

Wireless

Cisco Wireless Challenge 1

Outline

This challenge involves the configuration of the BVI interface.

Objectives

The objectives of this challenge are to:

- Setup the IP address of the BVI interface.
- Setup the subnet mask of the BVI interface.
- Define the description of the BVI interface.
- Enable E0.
- Define the description of the E0 port.
- Define Ethernet details on the E0 port.

Example

```
> enable
ap# sh version
Cisco IOS Software, C1200 Software (C1200-K9W7-M), Version 12.3(8)JA, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 27-Feb-06 09:09 by ssearch

ROM: Bootstrap program is C1200 boot loader
BOOTLDR: C1200 Boot Loader (C1200-BOOT-M) Version 12.3(2)JA4, RELEASE SOFTWARE (fc1)

ap uptime is 28 minutes
System returned to ROM by power-on
System image file is "flash:/c1200-k9w7-mx.123-8.JA/c1200-k9w7-mx.123-8.JA"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

cisco AIR-AP1231G-E-K9 (PowerPC405GP) processor (revision A0) with 15038K/1336K bytes of memory.
Processor board ID FOC101311BH
PowerPC405GP CPU at 196Mhz, revision number 0x0145
Last reset from power-on
1 FastEthernet interface
1 802.11 Radio(s)

32K bytes of flash-simulated non-volatile configuration memory.

Base ethernet MAC Address: 00:17:59:67:5E:9D
Part Number : 73-8704-11
PCA Assembly Number : 800-23211-12
PCA Revision Number : A0
PCB Serial Number : FOC101311BH
Top Assembly Part Number : 800-23304-13
Top Assembly Serial Number : FCZ1019Z0T3
Top Revision Number : A0
Product/Model Number : AIR-AP1231G-E-K9

Configuration register is 0xF

ap# sh controller

!
interface Dot11Radio0
Radio AIR-MP21G, Base Address 0017.5ab7.ff60, BBlock version 0.00, Software version 5.90.8
Serial number: FOC1011C7A8
Number of supported simultaneous BSSID on Dot11Radio0: 8
Carrier Set: EMEA (EU)
Uniform Spreading Required: No
Current Frequency: 2417 MHz Channel 2
Allowed Frequencies: 2412(1) 2417(2) 2422(3) 2427(4) 2432(5) 2437(6) 2442(7) 2447(8) 2452(9) 2457(10) 2462(11) 2467(12) 2472(13)
Listen Frequencies: 2412(1) 2417(2) 2422(3) 2427(4) 2432(5) 2437(6) 2442(7) 2447(8) 2452(9) 2457(10) 2462(11) 2467(12) 2472(13) 2484(14)
Current CCK Power: 50 mW
Allowed CCK Power Levels: 1 5 10 20 30 50
Current OFDM Power: 30 mW
Allowed OFDM Power Levels: 1 5 10 20 30
Allowed Client Power Levels: 1 5 10 20 30 50
ERP settings: short slot time.
Neighbors in non-erp mode:

Current Rates: basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
Active Rates: basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
Allowed Rates: 1.0 2.0 5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Range Rates: basic-1.0 2.0 5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Throughput Rates: basic-1.0 basic-2.0 basic-5.5 basic-6.0 basic-9.0 basic-11.0 basic-12.0 basic-18.0 basic-24.0 basic-36.0 basic-48.0 basic-54.0
Default Rates: basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
Current Voice Rates: 5.5 6.0 11.0 12.0 24.0 [disabled until voice packet-discard enabled]
Default Voice Rates: 5.5 6.0 11.0 12.0 24.0
Channel / Max Power Table
1 O=15 D=17, 2 O=15 D=17, 3 O=15 D=17, 4 O=15 D=17, 5 O=15 D=17
6 O=15 D=17, 7 O=15 D=17, 8 O=15 D=17, 9 O=15 D=17, 10 O=15 D=17
11 O=15 D=17, 12 O=15 D=17, 13 O=15 D=17

Data Rate Sensitivity (rate, SNR dB, Contention dBm)
(1.0, 1, -98) (2.0, 7, -94) (5.5, 9, -92) (11.0, 16, -86)
(6.0, 7, -92) (9.0, 14, -87) (12.0, 12, -87) (18.0, 15, -84)

```

(24.0, 17, -82)   (36.0, 24, -76)   (48.0, 29, -73)   (54.0, 33, -69)
Radio Management (RM) Configuration:
Regular AP RM Mode 1   Temp Setting Disabled
Temp Settings: AP Tx Power 0   AP Tx Channel 0   Client Tx Power 0
ap# show running-config
Using 1413 out of 32768 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
enable secret 5 $1$a2Og$asLICPwL7.HnsvvykNOus1
!
ip subnet-zero
ip domain name test.com
!
!
username Cisco password 7 1531021F0725
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers tkip
!
ssid bill
!
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
world-mode legacy
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 FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
hold-queue 160 in
!
interface BVI1
ip address 10.0.0.1 255.255.255.0
no ip route-cache
!
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
!
!
control-plane
!
bridge 1 route ip
!

```

```

!
!
line con 0
line vty 0 4
  login local
!
end
# config t
(config)# int bvi 1
ap(config-if)# ip address ?
  A.B.C.D IP address
  pool IP Address autoconfigured from a local DHCP pool
ap(config-if)# ip address 158.234.223.7 ?
  A.B.C.D IP subnet mask
(config-if)# ip address 158.234.223.7 255.192.0.0
(config-if)# description cisco
(config-if)# int fa0
(config-if)# no shut
(config-if)# description production depart
(config-if)# speed 10
(config-if)# int d0
(config-if)# no shut

```

Explanation

One of the most popular access points for creating infrastructure networks is the Cisco Aironet 1200 device, which is an industry-standard wireless access point. It has two main networking ports: radio port named Dot11radio0 (**D0**) and an Ethernet one (**E0** or **FA0**). Each of these ports can be programmed with an IP address, but a special port named BVI1 is normally used to define the IP address for both ports. Figure 1 outlines this, and how the port is programmed.

... diagrams missed out in this version

Cisco Wireless Challenge 2

Outline

This challenge involves the configuration of the E0 interface.

Objectives

The objectives of this challenge are to:

- Setup the IP address of the BVI interface.
- Setup the subnet mask of the BVI interface.
- Enable E0.
- Define the description of the E0 port.
- Define Ethernet details on the E0 port.

- Enable CDP on E0.

Example

```
> enable
# config t
(config)# int bvi1
(config-if)# ip address 158.234.223.7 255.192.0.0
(config-if)# description cisco
(config-if)# int fa0
(config-if)# no shut
(config-if)# description production depart
(config-if)# speed 10
(config-if)# duplex full
(config-if)# cdp ?
    enable    Enable CDP on interface
    log       Log messages generated by CDP
(config-if)# cdp enable
```

Cisco Wireless Challenge 3

Outline

This challenge involves the configuration of a few details including the hostname and default gateway.

Objectives

The objectives of this challenge are to:

- Setup the IP address of the BVI interface.
- Setup the subnet mask of the BVI interface.
- Enable D0.
- Define the hostname.
- Define the default gateway.

Example

```
> en
# config t
(config)# int bvi1
(config-if)# ip address 202.86.171.1 255.255.255.254
(config-if)# int d0
(config-if)# no shut
(config-if)# exit
(config)# hostname oslo
oslo (config)# ip default-gateway ?
    A.B.C.D  IP address of default gateway
oslo (config)# ip default-gateway 136.182.33.11
```

```
oslo (config)#
```

Explanation

Another important configuration is the **default-gateway** which is used in order to redirect any data packets which are not destined for the local network. For this the wireless access point will send these data packets which have an unknown destination to the default gateway, which will, hopefully, find a destination for them, or at least know of another router which might be able to help on routing the packets. In most cases the default-gateway is defined as the IP address of the router port which connects to the Ethernet connection of the wireless access point. An example configuration is:

```
# config t
(config)# ip ?
(config)# ip default-gateway ?
(config)# ip default-gateway 192.168.1.254
(config)# exit
```

Cisco Wireless Challenge 4

Outline

This challenge involves the configuration an SSID and the radio channel. Also it defines the default gateway, the domain name and the hostname. Note there is a change in Cisco IOS 12.3.

Objectives

The objectives of this challenge are to:

- Define the SSID on the radio port.
- Define the radio channel.
- Define the default gateway.
- Define the domain name.
- Define the hostname.

Example IOS Version 12.3

```
> en
# config t
(config)# dot11 ssid minnesota
(config-ssid)# ?
ssid configuration commands:
  accounting          radius accounting
  admit-traffic       admit traffic
  authentication       authentication method
  exit                Exit from ssid sub mode
```

```

guest-mode          guest ssid
information-element Add information element
infrastructure-ssid ssid used to associate to other infrastructure devices
ip                  IP options
max-associations    set maximum associations for ssid
mbssid              Multiple BSSID
mobility            enable L3 mobility
no                  Negate a command or set its defaults
vlan                bind ssid to vlan
wpa-psk             Configure Wi-Fi Protected Access pre-shared key
(config-ssid)# exit
(config)# int d0
(config-if)# ssid ?
  LINE radio Service Set ID (Up to 32 characters)
(config-if)# ssid minnesota
(config-if)# int d0
(config-if)# channel ?
  <1-2472>          One of: 1 2 3 4 5 6 7 8 9 10 11 12 13 2412 2417 2422 2427
                    2432 2437 2442 2447 2452 2457 2462 2467 2472
                    least-congested Scan for best frequency
(config-if)# channel 1
(config-if)# exit
(config)# ip default-gateway 205.98.14.11
(config)# ip domain-name ?
  WORD Default domain name
(config)# ip domain-name moray.ll
(config)# hostname northdakota

```

Note that the setting of SSID is now done in the global configuration mode, and the SSID is then associated with the D0 port.

Example IOS Version 12.1

```

> en
# config t
(config)# int d0
(config-if)# ssid minnesota
(config-if-ssid)# exit
(config-if)# int d0
(config-if)# channel ?
  <1-2472>          One of: 1 2 3 4 5 6 7 8 9 10 11 12 13 2412 2417 2422 2427
                    2432 2437 2442 2447 2452 2457 2462 2467 2472
                    least-congested Scan for best frequency
(config-if)# channel 1
(config-if)# exit
(config)# ip default-gateway 205.98.14.11
(config)# ip domain-name moray.ll
(config)# hostname northdakota

```

Explanation

The radio SSID (Service Set ID) uniquely identifies a wireless network within a limited physical domain. It is setup within the access point with:

```

# config t
(config)# int dot11radio0
(config-if)# ssid fred
(config-if-ssid)# guest-mode

```

which sets up an SSID of **fred**, and allows guest-mode. Along with the SSID it is also possible to define a beacon time where a beacon signal is sent out at a given time interval, such as:

```
# config t
(config)# int dot11radio0
(config-if)# beacon ?
    dtim-period    dtim period
    period          beacon period
(config-if)# beacon period ?
    <20-4000>      Kusec (or msec)
(config-if)# beacon period 1000
```

which defines the beacon period of 1000ms (1 seconds).

The channel setting is an important one, as it defines the basic identification of the communications channel. In Europe there are 14 channels available which limits the number of simultaneous connections, where each channel is numbered from 1 to 14, each of which has their own transmission/reception frequency, as illustrated in Figure 1. Careful planning of these channels is important, especially in creating wireless domains which are overlapping as this allows users to roam around the physical space. The example in Figure 1 shows that it is possible to achieve good coverage, without overlapping domains with the same frequency, with just three channels.

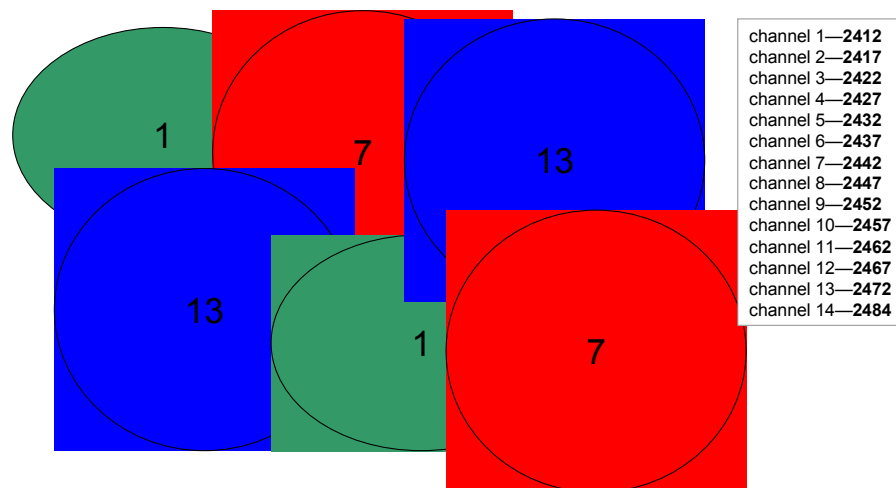


Figure 1 Channels in an area

The definition of the channel is defined within the D0 interface:

```
(config)# int dot11radio0
(config-if)# channel ?
    <1-2472>          One of: 1 2 3 4 5 6 7 8 9 10 11 12 13 2412 2417 2422 2427
                    2432 2437 2442 2447 2452 2457 2462 2467 2472
    least-congested Scan for best frequency
(config-if)# channel 7
(config-if)# no shutdown
```

Cisco Wireless Challenge 5

Outline

This challenge involves the configuration of passwords and a user.

Objectives

The objectives of this challenge are to:

- Define the privileged and secret passwords.
- Define a user and password.
- Enable the HTTP server.

Example

```
> en
# config t
(config)# enable ?
  last-resort  Define enable action if no TACACS servers respond
  password     Assign the privileged level password
  secret       Assign the privileged level secret
  use-tacacs   Use TACACS to check enable passwords
ap(config)# enable password ?
  0            Specifies an UNENCRYPTED password will follow
  7            Specifies a HIDDEN password will follow
  LINE        The UNENCRYPTED (cleartext) 'enable' password
  level       Set exec level password
(config)# enable password hotel
ap(config)# enable sec ?
  0            Specifies UNENCRYPTED password will follow
  5            Specifies an ENCRYPTED secret will follow
  LINE        The UNENCRYPTED (cleartext) 'enable' secret
  level       Set exec level password
(config)# enable secret hotel
(config)# username lynn password foxtrot
(config)# ip http server
(config)# ip subnetzero
```

Explanation

A wireless access point is typically accessible through the TELNET and/or HTTP proposal. The HTTP service is important as it allows remote access through a Web browser, and can be authenticated locally with:

```
# config t
(config) # username ?
(config) # username fred password bert
```

```
(config) # ip http ?
(config) # ip http server
(config) # ip http authentication local
(config) # exit
```

Cisco Wireless Challenge 6

Outline

This challenge involves the configuration of radio port settings. Note there is a change in Cisco IOS 12.3.

Objectives

The objectives of this challenge are to:

- Define the privileged and secret passwords.
- Define a user and password.
- Enable the HTTP server.

Example IOS Version 12.3

```
> enable
# config t

(config)# dot11 ssid fred
(config-ssid)# max-assoc ?
<1-255> association limit
(config-ssid)# max-assoc 9
(config-ssid)# exit

(config)# int bv11
(config-if)# ip address 208.1.7.8 255.255.255.224
(config-if)# int d0
(config-if)# beacon ?
    dtim-period dtim period
    period beacon period
(config-if)# beacon period ?
    <20-4000> Kusec (or msec)
(config-if)# beacon period 2000
(config-if)# power ?
    client Client radio transmitter power level
    local Local radio transmitter power level
(config-if)# power local ?
    <1-50> One of: 1 5 20 30 50
    maximum Set local power to allowed maximum

(config-if)# power local 5

(config-if)# power client ?
    <1-50> One of: 1 5 20 30 50
    maximum Set client power to allowed maximum
(config-if)# power client 5
```

(config-if)# ?

Interface configuration commands:

access-expression	Build a bridge boolean access expression
antenna	dot11 radio antenna setting
arp	Set arp type (arpa, probe, snap) or timeout
bandwidth	Set bandwidth informational parameter
beacon	dot11 radio beacon
bridge-group	Transparent bridging interface parameters
broadcast-key	Configure broadcast key rotation period
carrier-delay	Specify delay for interface transitions
cdp	CDP interface subcommands
channel	Set the radio frequency
countermeasure	countermeasure
custom-queue-list	Assign a custom queue list to an interface
dampening	Enable event dampening
default	Set a command to its defaults
delay	Specify interface throughput delay
description	Interface specific description
dot11	IEEE 802.11 config interface commands
dot1x	IEEE 802.1X subsystem
encryption	Configure dot11 encryption parameters
exit	Exit from interface configuration mode
fair-queue	Enable Fair Queuing on an Interface
fragment-threshold	IEEE 802.11 packet fragment threshold
help	Description of the interactive help system
hold-queue	Set hold queue depth
infrastructure-client	Reserve a dot11 virtual interface for a WGB client
--More----- press any key ---	
ip	Interface Internet Protocol config commands
keepalive	Enable keepalive
l2-filter	Set Layer2 ACL for packet received by upper layer protocols
load-interval	Specify interval for load calculation for an interface
logging	Configure logging for interface
loopback	Configure internal loopback on an interface
mac-address	Manually set interface MAC address
max-reserved-bandwidth	Maximum Reservable Bandwidth on an Interface
mtu	Set the interface Maximum Transmission Unit (MTU)
no	Negate a command or set its defaults
ntp	Configure NTP
packet	max packet retries
parent	Specify parents with which to associate
payload-encapsulation	IEEE 802.11 packet encapsulation
power	Set radio transmitter power levels
preamble-short	Use 802.11 short radio preamble
priority-group	Assign a priority group to an interface
random-detect	Enable Weighted Random Early Detection (WRED) on an Interface
rts	dot11 Request To Send
service-policy	Configure QoS Service Policy
shutdown	Shutdown the selected interface
snmp	Modify SNMP interface parameters
speed	Set allowed radio bit rates
--More----- press any key ---	
ssid	Configure radio service set parameters
station-role	role of the radio
timeout	Define timeout values for this interface
traffic-class	Radio traffic class parameters
transmit-interface	Assign a transmit interface to a receive-only interface
tx-ring-limit	Configure PA level transmit ring limit
world-mode	Dot11 radio world mode

```

(config-if)# world-mode ?
<cr>
(config-if)# world-mode

(config-if)# no shut
(config-if)# speed ?
 1.0      Allow 1 Mb/s rate
11.0     Allow 11 Mb/s rate
 2.0     Allow 2 Mb/s rate
 5.5     Allow 5.5 Mb/s rate
basic-1.0 Require 1 Mb/s rate
basic-11.0 Require 11 Mb/s rate
basic-2.0 Require 2 Mb/s rate
basic-5.5 Require 5.5 Mb/s rate
range    Set rates for best range
throughput Set rates for best throughput
<cr>
(config-if)# speed 1.0
(config-if)# ssid fred

```

Example IOS Version 12.1

```

> enable
# config t
(config)# int bvl1
(config-if)# ip address 208.1.7.8 255.255.255.224
(config-if)# int d0
(config-if)# beacon ?
 dtim-period dtim period
 period      beacon period
(config-if)# beacon period ?
 <20-4000> Kusec (or msec)
(config-if)# beacon period 2000
(config-if)# power ?
 client Client radio transmitter power level
 local  Local radio transmitter power level
(config-if)# power local ?
 <1-50> One of: 1 5 20 30 50
 maximum Set local power to allowed maximum

(config-if)# power local 5

(config-if)# power client ?
 <1-50> One of: 1 5 20 30 50
 maximum Set client power to allowed maximum
(config-if)# power client 5
(config-if)# ?
Interface configuration commands:
 access-expression Build a bridge boolean access expression
 antenna           dot11 radio antenna setting
 arp               Set arp type (arpa, probe, snap) or timeout
 bandwidth         Set bandwidth informational parameter
 beacon            dot11 radio beacon
 bridge-group      Transparent bridging interface parameters
 broadcast-key     Configure broadcast key rotation period
 carrier-delay     Specify delay for interface transitions
 cdp               CDP interface subcommands
 channel           Set the radio frequency
 countermeasure    countermeasure
 custom-queue-list Assign a custom queue list to an interface
 dampening         Enable event dampening

```

```

default          Set a command to its defaults
delay            Specify interface throughput delay
description      Interface specific description
dot11            IEEE 802.11 config interface commands
dot1x            IEEE 802.1X subsystem
encryption       Configure dot11 encryption parameters
exit             Exit from interface configuration mode
fair-queue       Enable Fair Queuing on an Interface
fragment-threshold IEEE 802.11 packet fragment threshold
help             Description of the interactive help system
hold-queue       Set hold queue depth
infrastructure-client Reserve a dot11 virtual interface for a WGB client
--More----- press any key ---
ip               Interface Internet Protocol config commands
keepalive        Enable keepalive
l2-filter        Set Layer2 ACL for packet received by upper layer
                  protocols
load-interval    Specify interval for load calculation for an
                  interface
logging          Configure logging for interface
loopback         Configure internal loopback on an interface
mac-address      Manually set interface MAC address
max-reserved-bandwidth Maximum Reservable Bandwidth on an Interface
mtu              Set the interface Maximum Transmission Unit (MTU)
no               Negate a command or set its defaults
ntp              Configure NTP
packet           max packet retries
parent           Specify parents with which to associate
payload-encapsulation IEEE 802.11 packet encapsulation
power            Set radio transmitter power levels
preamble-short   Use 802.11 short radio preamble
priority-group   Assign a priority group to an interface
random-detect    Enable Weighted Random Early Detection (WRED) on an
                  Interface
rts              dot11 Request To Send
service-policy   Configure QoS Service Policy
shutdown         Shutdown the selected interface
snmp             Modify SNMP interface parameters
speed            Set allowed radio bit rates
--More----- press any key ---
ssid             Configure radio service set parameters
station-role     role of the radio
timeout          Define timeout values for this interface
traffic-class    Radio traffic class parameters
transmit-interface Assign a transmit interface to a receive-only
                  interface
tx-ring-limit    Configure PA level transmit ring limit
world-mode       Dot11 radio world mode

(config-if)# world-mode ?
<cr>
(config-if)# world-mode

(config-if)# no shut
(config-if)# speed ?
 1.0          Allow 1 Mb/s rate
11.0          Allow 11 Mb/s rate
 2.0          Allow 2 Mb/s rate
 5.5          Allow 5.5 Mb/s rate
basic-1.0     Require 1 Mb/s rate
basic-11.0    Require 11 Mb/s rate
basic-2.0     Require 2 Mb/s rate
basic-5.5     Require 5.5 Mb/s rate

```

```

range      Set rates for best range
throughput Set rates for best throughput
<cr>
(config-if)# speed 1.0
(config-if)# ssid fred
(config-if-ssid)# max-assoc ?
<1-255> association limit
(config-if-ssid)# max-assoc 9

```

Cisco Wireless Challenge 7

Outline

This challenge involves the configuration of the D0 parameters, such as the role of the station, the antenna settings, the SSID and guest-mode. Note there is a change in Cisco IOS 12.3.

Objectives

The objectives of this challenge are to:

- Define the station role.
- Define the antenna settings.
- Define the SSID.
- Enable guest-mode on the SSID.

Example IOS Version 12.3

```

> enable
# config t
(config)# dot11 ssid michigan
(config-ssid)# guest-mode
(config-ssid)# exit

(config)# int bv11
(config-if)# ip address 208.1.7.8 255.255.255.224
(config)# int d0
(config-if)# station ?
  repeater Repeater access point
  root     Root access point
(config-if)# station root
(config-if)# antenna ?
  receive  receive antenna setting
  transmit transmit antenna setting
(config-if)# antenna receive ?
  diversity antenna diversity
  left     antenna left
  right    antenna right
(config-if)# antenna receive diversity
(config-if)# antenna transmit left
(config-if)# ssid michigan

```

Example IOS Version 12.1

```

> enable
# config t

(config)# int bv11
(config-if)# ip address 208.1.7.8 255.255.255.224
(config)# int d0
(config-if)# station ?
    repeater  Repeater access point
    root      Root access point
(config-if)# station root
(config-if)# antenna ?
    receive   receive antenna setting
    transmit  transmit antenna setting
(config-if)# antenna receive ?
    diversity antenna diversity
    left      antenna left
    right     antenna right
(config-if)# antenna receive diversity
(config-if)# antenna transmit left
(config-if)# ssid michigan
(config-if-ssid)# guest-mode

```

Cisco Wireless Challenge 8

Outline

This challenge involves the configuration of the D0 parameters, such as the rts settings, fragmentation settings, and the radio channel. Note there is a change in Cisco IOS 12.3.

Objectives

The objectives of this challenge are to:

- Define RTS (ready to send) settings.
- Define the SSID.
- Define the maximum associations for the SSID.
- Define the radio channel.

Example IOS Version 12.3

```

> enable
# config t
(config)# dot11 ssid oklahoma
(config-ssid)# max-assoc 24
(config-ssid)# exit

(config)# int bv11
(config-if)# ip address 208.1.7.8 255.255.255.224
(config)# int d0
(config-if)# ssid oklahoma
(config-if)# rts ?
    retries   RTS max retries
    threshold RTS threshold
(config-if)# rts threshold ?

```

```
<0-2347> threshold in bytes
(config-if)# rts threshold 19
(config-if)# rts retries 24
(config-if)# fragment ?
<256-2346>
(config-if)# fragment 1091
(config-if)# channel 4
```

Example IOS Version 12.1

```
> enable
# config t
(config)# int bvi1
(config-if)# ip address 208.1.7.8 255.255.255.224
(config)# int d0
(config-if)# ssid oklahoma
(config-if)# rts ?
    retries    RTS max retries
    threshold  RTS threshold
(config-if)# rts threshold ?
    <0-2347> threshold in bytes
(config-if)# rts threshold 19
(config-if)# rts retries 24
(config-if)# ssid oklahoma
(config-if-ssid)# max-assoc 24
(config-if-ssid)# exit
(config-if)# fragment ?
    <256-2346>
(config-if)# fragment 1091
(config-if)# channel 4
```

Cisco Wireless Challenge 9

Outline

This challenge involves the configuration of the D0 parameters, such as for packet retries, preamble settings, fragment limit and the radio channel. Note there is a change in Cisco IOS 12.3.

Objectives

The objectives of this challenge are to:

- Define packet retry settings.
- Define the SSID.
- Define the maximum associations for the SSID.
- Define the radio channel.

Example IOS Version 12.3

```
> enable
# config t
(config)# dot11 ssid oklahoma
```

```

(config-ssid)# max-assoc 24
(config-ssid)# exit

(config)# int bv11
(config-if)# ip address 208.1.7.8 255.255.255.224
(config)# int d0
(config-if)# packet ?
    retries  retries
(config-if)# packet retries ?
    <1-128>  max packet retries before giving up
(config-if)# packet retries 7
(config-if)# preamble-short
(config-if)# ssid oklahoma
(config-if)# fragment ?
    <256-2346>
(config-if)# fragment 1091
(config-if)# channel 4

```

Example IOS Version 12.1

```

> enable
# config t
(config)# int bv11
(config-if)# ip address 208.1.7.8 255.255.255.224
(config)# int d0
(config-if)# packet ?
    retries  retries
(config-if)# packet retries ?
    <1-128>  max packet retries before giving up
(config-if)# packet retries 7
(config-if)# preamble-short
(config-if)# ssid oklahoma
(config-if-ssid)# max-assoc 24
(config-if-ssid)# exit
(config-if)# fragment ?
    <256-2346>
(config-if)# fragment 1091
(config-if)# channel 4

```

Cisco Wireless Challenge 10

Outline

This challenge involves the configuration of the DHCP server on the wireless access point.

Objectives

The objectives of this challenge are to:

- Define the DHCP pool.
- Define the network addresses.
- Define the DNS server.
- Define the NetBIOS server.
- Define the lease time.

- Define the default router.
- Define excluded addresses.

Example

The following sets up the DHCP server:

```
> en
# config t
(config)# ip dhcpd pool Wyoming
(dhcp-config)# ?
DHCP pool configuration commands:
  accounting          Send Accounting Start/Stop messages
  bootfile            Boot file name
  class               Specify a DHCP class
  client-identifier   Client identifier
  client-name         Client name
  default-router      Default routers
  dns-server          DNS servers
  domain-name         Domain name
  exit                Exit from DHCP pool configuration mode
  hardware-address    Client hardware address
  host                Client IP address and mask
  import              Programatically importing DHCP option parameters
  lease               Address lease time
  netbios-name-server NetBIOS (WINS) name servers
  netbios-node-type   NetBIOS node type
  network             Network number and mask
  next-server         Next server in boot process
  no                  Negate a command or set its defaults
  option              Raw DHCP options
  origin              Configure the origin of the pool
  subnet              Subnet allocation commands
  update              Dynamic updates
  utilization         Configure various utilization parameters
  vrf                 Associate this pool with a VRF
(dhcp-config)# n?
netbios-name-server netbios-node-type network next-server
no
(dhcp-config)# network ?
  A.B.C.D Network number in dotted-decimal notation
(config-dhcp)# network 249.189.108.0 255.255.255.254
(dhcp-config)# dns ?
  Hostname or A.B.C.D Server's name or IP address
(config-dhcp)# dns-server 249.189.108.58
(config-dhcp)# netbios-name-server 249.189.108.61
(config-dhcp)# lease 3
(config-dhcp)# default-router 249.189.108.87
(config-dhcp)# exit
(config)# ip dhcp ?
  conflict            DHCP address conflict parameters
  database            Configure DHCP database agents
  excluded-address    Prevent DHCP from assigning certain addresses
  limited-broadcast-address Use all 1's broadcast address
  ping                Specify ping parameters used by DHCP
  pool                Configure DHCP address pools
  relay               DHCP relay agent parameters
  smart-relay        Enable Smart Relay feature
(config)# ip dhcp excluded-address ?
  A.B.C.D Low IP address
```

```
(config)# ip dhcp excluded-address 249.189.108.26 ?
  A.B.C.D  High IP address
  <cr>
(config)# ip dhcp excluded-address 249.189.108.26
(config)# ip dhcp ping ?
  packets  Specify number of ping packets
  timeout  Specify ping timeout

(config)# ip dhcp ping timeout 350
```

Cisco Wireless Challenge 11

Outline

This challenge involves the configuration of an IP hosts table.

Objectives

The objectives of this challenge are to:

- Define a default gateway.
- Define a hostname.
- Define a hosts table.

Example

The following sets up an IP hosts table:

```
> en
# config t
(config)# ip default-gateway 36.125.171.9
(config)# hostname Montana
montana (config)# ip host ?
  WORD  Name of host
montana (config)# ip host tennessee ?
  <0-65535>  Default telnet port number
  A.B.C.D   Host IP address
  additional Append addresses
montana (config)# ip host tennessee 211.99.108.9
montana (config)# ip host kirkcaldy 154.242.2.8
montana (config)# ip host edinburgh 64.2.249.2
```

Cisco Wireless Challenge 12

Outline

This challenge involves the configuration of CDP (Cisco Discovery Protocol).

Objectives

The objectives of this challenge are to:

- Enable CDP.
- Define CDP holdtime.
- Define CDP timer.
- Apply CDP onto E0.

Example

The following sets up CDP:

```
# config t
(config)# cdp ?
  advertise-v2      CDP sends version-2 advertisements
  holdtime          Specify the holdtime (in sec) to be sent in packets
  source-interface  Insert the interface's IP in all CDP packets
  timer             Specify the rate at which CDP packets are sent (in sec)
run
(config)# cdp run
(config)# cdp holdtime ?
  <10-255> Length of time (in sec) that receiver must keep this packet
(config)# cdp holdtime 66
(config)# cdp timer ?
  <5-254> Rate at which CDP packets are sent (in sec)
(config)# cdp timer 94
(config)# int e0
(config-if)# cdp enable
```

Explanation

CDP (Cisco Discovery Protocol) is used to discover Cisco devices which connect to a given port. It is set globally on the device with **cdp run**, and then the timers are set as:

```
# config t
(config)# cdp ?
(config)# cdp holdtime ?
(config)# cdp holdtime 120
(config)# cdp timer ?
(config)# cdp timer 50
(config)# end
```

To enable CDP on the wireless access point:

```
# config t
(config)# cdp run
(config)# end
```

To enable CDP on an interface:

```
# config t
(config)# int fa0
(config-if)# cdp ?
(config-if)# cdp enable
(config-if)# end
```

To show CDP information:

```
# show cdp ?
# show cdp neighbors
# show cdp neighbors detail
# show cdp neighbors traffic
```

Cisco Wireless Challenge 13

Outline

This challenge involves the configuration of HTTP server details.

Objectives

The objectives of this challenge are to:

- Enable the HTTP server.
- Define the HTTP server port.
- Define the HTTP authentication.
- Enable various banners.

Example

The following sets up the HTTP server parameters:

```
> en
# config t
(config)# ip http ?
  access-class      Restrict http server access by access-class
  authentication    Set http server authentication method
  client            Set http client parameters
  help-path         HTTP help root URL
  max-connections   Set maximum number of concurrent http server connections
  path              Set base path for HTML
  port              Set http server port
  secure-ciphersuite Set http secure server ciphersuite
  secure-client-auth Set http secure server with client authentication
  secure-port       Set http secure server port number for listening
  secure-server     Enable HTTP secure server
  secure-trustpoint Set http secure server certificate trustpoint
  server            Enable http server
  timeout-policy    Set http server time-out policy parameters
(config)# ip http server
(config)# ip http port ?
```

```

<0-65535> HTTP port
(config)# ip http port 1024
(config)# ip http authentication ?
    enable Use enable passwords
    local Use local username and passwords
    tacacs Use tacacs to authorize user
(config)# ip http authentication local
(config)# ip http help-path ?
    WORD root URL for help pages
(config)# ip http help-path file:///c:\wireless\help
(config)# ip http access-class 10
(config)# banner motd gorgie home
(config)# banner login welcome
(config)# banner exec admin device

```

Cisco Wireless Challenge 14

Outline

This challenge involves the configuration of console and Telnet parameters.

Objectives

The objectives of this challenge are to:

- Define the console password.
- Define the timeout for the console.
- Define the Telnet password.
- Define the timeout for Telnet sessions.

Example

The following sets up the CON and VTY settings:

```

> en
# config t
(config)# line con 0
(config-line)# ?
Line configuration commands:
  access-class           Filter connections based on an IP access list
  activation-character   Define the activation character
  autocommand           Automatically execute an EXEC command
  autocommand-options   Autocommand options
  data-character-bits   Size of characters being handled
  databits              Set number of data bits per character
  default               Set a command to its defaults
  domain-lookup         Enable domain lookups in show commands
  editing               Enable command line editing
  escape-character      Change the current line's escape character
  exec                  Configure EXEC
  exec-banner           Enable the display of the EXEC banner
  exec-character-bits   Size of characters to the command exec
  exec-timeout          Set the EXEC timeout
  exit                  Exit from line configuration mode

```

```

flowcontrol          Set the flow control
full-help           Provide help to unprivileged user
help               Description of the interactive help system
history            Enable and control the command history function
international      Enable international 8-bit character support
ip                 IP options
length             Set number of lines on a screen
location           Enter terminal location description
logging            Modify message logging facilities
login              Enable password checking
modem              Configure the Modem Control Lines
monitor            Copy debug output to the current terminal line
motd-banner        Enable the display of the MOTD banner
no                 Negate a command or set its defaults
notify             Inform users of output from concurrent sessions
padding            Set padding for a specified output character
parity             Set terminal parity
password           Set a password
privilege          Change privilege level for line
refuse-message     Define a refuse banner
rotary             Add line to a rotary group
rxspeed            Set the receive speed
session-timeout    Set interval for closing connection when there is no
                  input traffic
special-character-bits Size of the escape (and other special) characters
speed              Set the transmit and receive speeds
start-character    Define the start character
stop-character     Define the stop character
stopbits          Set async line stop bits
terminal-type     Set the terminal type
timeout            Timeouts for the line
transport          Define transport protocols for line
txspeed            Set the transmit speeds
vacant-message     Define a vacant banner
width              Set width of the display terminal
(config-line)# password lothian
(config-line)# timeout ?
    login Timeouts related to the login sequence
(config-line)# timeout login ?
    response Timeout for any user input during login sequences
(config-line)# timeout login response ?
    <0-300> Timeout in seconds
(config-line)# timeout login response 19
(config-line)# exec-timeout ?
    <0-35791> Timeout in minutes
(config-line)# exec-timeout 11
(config-line)# logging ?
    synchronous Synchronized message output
(config-line)# logging synchronous
(config-line)# line vty 0 8
(config-line)# login
(config-line)# password mississippi
(config-line)# timeout login response 12
(config-line)# exec-timeout 10

```

Cisco Wireless Challenge 15

Outline

This challenge involves the configuration of a loopback address, and a few other settings.

Objectives

The objectives of this challenge are to:

- Set the clock.
- Allow zero subnets.
- Define a DHCP pool.
- Define the E0 IP address and subnet mask.
- Define a loopback address and subnet mask.

Example

The following sets up loopback settings:

```
> en
# clock ?
  set Set the time and date
# clock set 03:52
# config t
(config)# ip subnet-zero
(config)# ip dhcp pool ion
(config)# int e0
(config-if)# ip address 80.24.45.1 255.255.252.0
(config-if)# no shutdown
(config-if)# exit
(config)# int loopback ?
  <0-2147483647> Loopback interface number
(config)# int loopback 45
(config-if)# ip address 195.253.209.21 255.255.128.0
```

Cisco Wireless Challenge 16

Outline

This challenge involves the configuration of logging.

Objectives

The objectives of this challenge are to:

- Enable logging.
- Define logging levels.

Example

The following sets up the CON and VTY settings:

```

> enable
# config t
(config)# logging on
(config)# logging 212.72.52.7
(config)# logging buffer ?
<0-7> Logging severity level
<4096-2147483647> Logging buffer size
alerts Immediate action needed (severity=1)
critical Critical conditions (severity=2)
debugging Debugging messages (severity=7)
emergencies System is unusable (severity=0)
errors Error conditions (severity=3)
informational Informational messages (severity=6)
notifications Normal but significant conditions (severity=5)
warnings Warning conditions (severity=4)
xml Enable logging in XML to XML logging buffer
<cr>
(config)# logging buffer 440240
(config)# logging host 138.24.170.8
(config)# logging trap ?
<0-7> Logging severity level
alerts Immediate action needed (severity=1)
critical Critical conditions (severity=2)
debugging Debugging messages (severity=7)
emergencies System is unusable (severity=0)
errors Error conditions (severity=3)
informational Informational messages (severity=6)
notifications Normal but significant conditions (severity=5)
warnings Warning conditions (severity=4)
<cr>
(config)# logging trap emergency
(config)# logging monitor emergency
(config)# logging console emergency
(config)# logging buffer emergency

```

Cisco Wireless Challenge 17

Outline

This challenge involves the configuration of services.

Objectives

The objectives of this challenge are to:

- Define logging timestamps.
- Disable UDP small servers.
- Disable TVP small servers.
- Define that passwords are encrypted.

Example

The following sets up the CON and VTY settings:

```

> en
# config t
(config)# service ?
compress-config      Compress the configuration file
config               TFTP load config files
dhcp                 Enable DHCP server and relay agent
disable-ip-fast-frag Disable IP particle-based fast fragmentation
exec-callback        Enable exec callback
exec-wait            Delay EXEC startup on noisy lines
finger              Allow responses to finger requests
hide-telnet-addresses Hide destination addresses in telnet command
linenumber           enable line number banner for each exec
nagle                Enable Nagle's congestion control algorithm
old-slip-prompts     Allow old scripts to operate with slip/ppp
pad                  Enable PAD commands
password-encryption Encrypt system passwords
prompt               Enable mode specific prompt
pt-vty-logging       Log significant VTY-Async events
sequence-numbers    Stamp logger messages with a sequence number
slave-log            Enable log capability of slave IPs
tcp-keepalives-in    Generate keepalives on idle incoming network
                    connections
tcp-keepalives-out   Generate keepalives on idle outgoing network
                    connections
tcp-small-servers   Enable small TCP servers (e.g., ECHO)
telnet-zeroidle      Set TCP window 0 when connection is idle
timestamps          Timestamp debug/log messages
udp-small-servers   Enable small UDP servers (e.g., ECHO)
(config)# service timestamps ?
debug   Timestamp debug messages
log     Timestamp log messages
<cr>
(config)# service timestamps log ?
datetime Timestamp with date and time
uptime   Timestamp with system uptime
<cr>
(config)# service timestamps log datetime
(config)# service ?
compress-config      Compress the configuration file
config               TFTP load config files
dhcp                 Enable DHCP server and relay agent
disable-ip-fast-frag Disable IP particle-based fast fragmentation
exec-callback        Enable exec callback
exec-wait            Delay EXEC startup on noisy lines
finger              Allow responses to finger requests
hide-telnet-addresses Hide destination addresses in telnet command
linenumber           enable line number banner for each exec
nagle                Enable Nagle's congestion control algorithm
old-slip-prompts     Allow old scripts to operate with slip/ppp
pad                  Enable PAD commands
password-encryption Encrypt system passwords
prompt               Enable mode specific prompt
pt-vty-logging       Log significant VTY-Async events
sequence-numbers     Stamp logger messages with a sequence number
slave-log            Enable log capability of slave IPs
tcp-keepalives-in    Generate keepalives on idle incoming network
                    connections
tcp-keepalives-out   Generate keepalives on idle outgoing network
                    connections
tcp-small-servers    Enable small TCP servers (e.g., ECHO)
telnet-zeroidle      Set TCP window 0 when connection is idle
timestamps           Timestamp debug/log messages
udp-small-servers    Enable small UDP servers (e.g., ECHO)

```

```
(config)# service sequence-numbers
(config)# service dhcp
(config)# service finger

(config)# no service tcp-small-servers
(config)# no service udp-small-servers
(config)# service password-encryption
```

Cisco Wireless Challenge 18

Outline

This challenge involves the configuration of the SNMP server.

Objectives

The objectives of this challenge are to:

- Define SNMP community string.
- Define SNMP contact.
- Define SNMP location.
- Enable SNMP traps.

Example

The following sets up the SNMP settings:

```
# config t
(config)# snmp-server ?
  chassis-id      String to uniquely identify this chassis
  community       Enable SNMP; set community string and access privs
  contact         Text for mib object sysContact
  enable          Enable SNMP Traps or Informs
  engineID        Configure a local or remote SNMPv3 engineID
  group           Define a User Security Model group
  host            Specify hosts to receive SNMP notifications
  ifindex         Enable ifindex persistence
  inform          Configure SNMP Informs options
  location        Text for mib object sysLocation
  manager         Modify SNMP manager parameters
  packet-size     Largest SNMP packet size
  queue-length    Message queue length for each TRAP host
  system-shutdown Enable use of the SNMP reload command
  tftp-server-list Limit TFTP servers used via SNMP
  trap            SNMP trap options
  trap-source     Assign an interface for the source address of all traps
  trap-timeout    Set timeout for TRAP message retransmissions
  user            Define a user who can access the SNMP engine
  view            Define an SNMPv2 MIB view
(config)# snmp-server community popup
(config)# snmp-server contact june
(config)# snmp-server location glasgow
```

```

(config)# snmp-server ?
  chassis-id      String to uniquely identify this chassis
  community       Enable SNMP; set community string and access privs
  contact         Text for mib object sysContact
  enable          Enable SNMP Traps or Informs
  engineID        Configure a local or remote SNMPv3 engineID
  group           Define a User Security Model group
  host            Specify hosts to receive SNMP notifications
  ifindex         Enable ifindex persistence
  inform          Configure SNMP Informs options
  location        Text for mib object sysLocation
  manager         Modify SNMP manager parameters
  packetSize      Largest SNMP packet size
  queue-length    Message queue length for each TRAP host
  system-shutdown Enable use of the SNMP reload command
  tftp-server-list Limit TFTP servers used via SNMP
  trap           SNMP trap options
  trap-source     Assign an interface for the source address of all traps
  trap-timeout    Set timeout for TRAP message retransmissions
  user           Define a user who can access the SNMP engine
  view           Define an SNMPv2 MIB view
(config)# snmp-server enable ?
  informs Enable SNMP Informs
  traps   Enable SNMP Traps
(config)# snmp-server enable traps
(config)# snmp-server chassis-id brighton

```

Explanation

SNMP (Simple Network Management Protocol) is a well-supported standard which can be used to monitor and control devices. It typically runs of hubs, switches and bridges. Many SNMP devices provides both general network management and device management through a serial cable, modem, or over the network from a remote computer. It involves a primary management station communicating with different management processes. Figure 1 shows an out-line of an SNMP-based system. A SNMP agent runs SNMP management software. An SNMP server sends commands to the agent which responses back with the results. In this figure the server asks the agent for its routing information and the agent responds with its routing table. These responses can either be polled (the server sends a request for information) or interrupt-driven (where the agent sends its information at given events). A polled system tends to increase network traffic as the agent may not have any updated information (and the server must re-poll for the information).

The SNMP (Simple Network Management Protocol) protocol is initially based in the RFC1157 document. It defines a simple protocol which gives network element management information base (MIB). There are two types of MIB: MIB-1 and MIB-2. MIB-1 was defined in 1988 and has 114 table entries, divided into two groups. MIB-2 is a 1990 enhancement which has 171 entries organized into 10 groups (RFC 1213). Most devices are MIB-1 compliant and newer one with both MIB-1 and MIB-2.

The database contains entries with four fields:

- Object type. Defines the name of the entry.
- Syntax. Gives the actual value (as string or an integer).
- Access field. Defines whether the value is read-only, read/write, write-only and not

accessible.

- Status field. Contains an indication on whether the entry in the MIB is mandatory (the managed device must implement the entry), optional (the managed device may implement the entry) or obsolete (the entry is not used).

SNMP is a very simple protocol but suffers from the fact that it is based on connectionless, unreliable, UDP. The IAB have recommended that the Common Management Information Services (CMIS) and Common Management Information Protocol (CMIP) be accepted as standard for future TCP/IP systems. The two main version of SNMP are SNMP Ver1 and SNMP Ver2. SNMP has added security to stop intruders determining network loading or the state of the network.

The SNMP architecture is based on a collection of:

- Network management stations. These execute management applications which monitor and control network elements.
- Network elements. These are devices such as hosts, gateways, terminal servers, and so on and have management agents which perform network management functions replying to requests from network management stations.

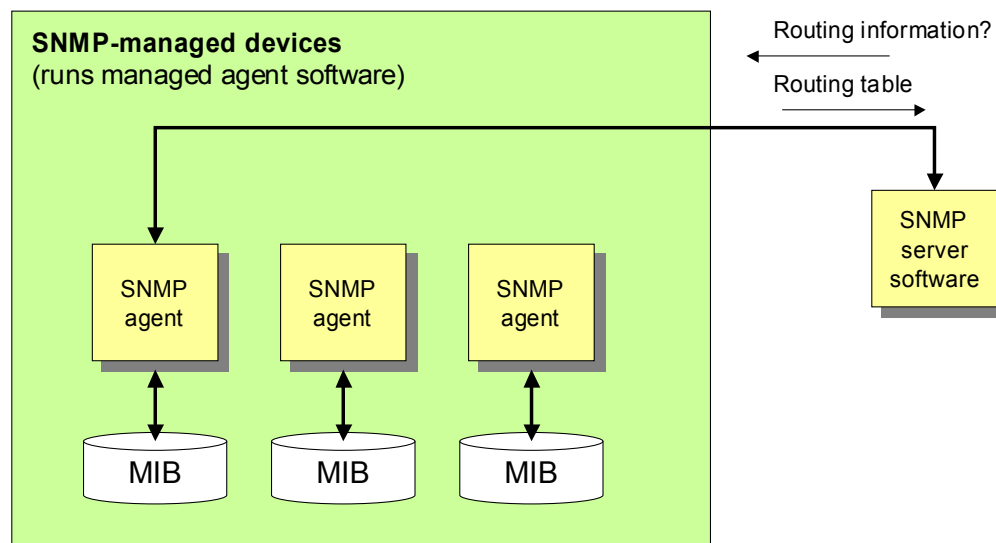


Figure 1 SNMP architecture

SNMP on a wireless access point

The SNMP (Simple Network Management Protocol) is a powerful method of gaining information on the operation of the network. The **snmp-server** command is used to enable SNMP monitoring. The **snmp-server community** command is used to initialise SNMP, and set the community string (which is basically used as a type of password for the SNMP access). For example to define the read-only string to public:

```
# config t
(config)# snmp-server community public RO
```

The RO defines read-only access, while RW defines read-write access. To setup the SNMP contact, the location:

```
(config)# snmp-server contact fred smith
(config)# snmp-server location room c6
```

SNMP contains a database of monitored network conditions, such as the number of errors in data packets, the IP addresses of the interfaces, and so on. It can also be setup to trigger on certain traps, such as on syslog traps. To enable all of SNMP traps so that all the data is monitored:

```
(config)# snmp-server enable traps
```

Then to send these traps to a remote host (to www.myhost.com):

```
# config t
(config)# snmp-server host www.myhost.com public
```

To determine the status of the SNMP communications:

```
# show snmp
```

and to display the SNMP engine and remote engines:

```
# show snmp engine
```

and to display the SNMP group:

```
# show snmp group
```

SNMP uses an MIB database to store its values. To display its contents:

```
# show snmp mib
```

SNMP tree structure

The MIB tree structure is defined by a long sequence of numbers separated by dots, such as .1.3.6.1.2.1.1.4.0 (where the .0 represents an end node). This number is called an **Object Identifier (OID)**. The OID is a numerical representation of the MIB tree structure. Each digit represents a node in this tree structure. The trunk of the tree is on the left; the leaves are on the right, as illustrated in Figure 2 and Figure 3.

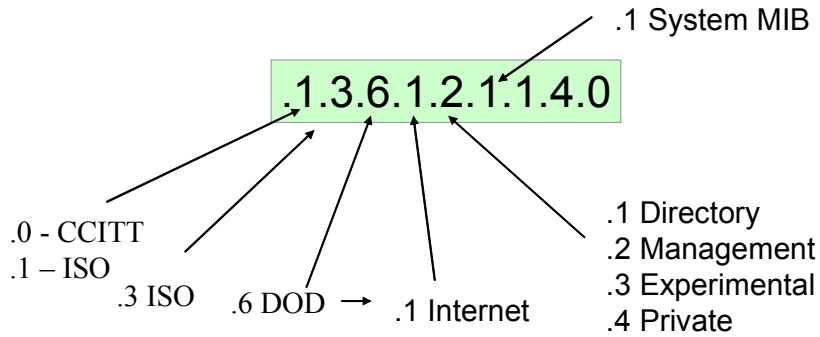
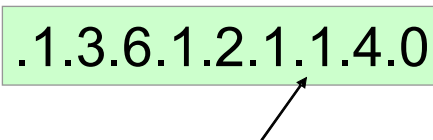


Figure 2 SNMP object ID



sysDescr (1), *sysObjectID* (2),
sysUpTime (3), *sysContact* (4),
sysName (5), *sysLocation* (6),
sysServices (7),

Figure 3 SNMP object ID

For example a node with an ID of 1.3.6.1.2.1.5.1.0 has the following structure:

- iso(1).
- org(3).
- dod(6).
- internet(1).
- mgmt(2).
- mib-2(1).
- icmp(5).
- icmpInMsgs(1).

For a router, example objects are:

MIB name	Description	Object ID
sysName	Hostname	.1.3.6.1.2.1.1.5.0
sysUpTime	Uptime	.1.3.6.1.2.1.1.3.0
sysDescr	System Description	.1.3.6.1.2.1.1.1.0
sysContact	System Contact	.1.3.6.1.2.1.1.4.0
sysLocation	System Location	.1.3.6.1.2.1.1.6.0
ciscoImageString	IOS Version	.1.3.6.1.4.1.9.9.25.1.1.1.2.5
avgBusy1	1-Minute CPU Util.	.1.3.6.1.4.1.9.2.1.57.0
avgBusy5	5-Minute CPU Util.	.1.3.6.1.4.1.9.2.1.58.0

freeMem	Free memory	.1.3.6.1.4.1.9.2.1.8.0
ciscoImageString.4	IOS feature set	.1.3.6.1.4.1.9.9.25.1.1.1.2.4

Cisco Wireless Challenge 19

Outline

This challenge involves the configuration of the hot standby.

Objectives

The objectives of this challenge are to:

- Define the BVI IP address and subnet mask.
- Define the MAC address of the device to monitor.
- Define the poll-time for the hot standby.
- Define the timeout for the host standby.

Example

The following sets up the hot standby function:

```
> en
# config t
(config)# int bvi1
(config-if)# ip address 202.86.171.1 255.255.255.254
(config-if)# int d0
(config-if)# no shut
(config-if)# int e0
(config-if)# no shut
(config-if)# exit
(config)# iapp ?
  standby  Configure AP standby mode parameters
(config)# iapp standby ?
  mac-address      MAC address of the primary AP
  poll-frequency   Standby polling frequency
  primary-shutdown Shutdown primary radios on failover
  timeout          Standby polling timeout
<cr>
(config)# iapp standby mac ?
  H.H.H  MAC address of the primary AP Radio
(config)# iapp standby mac-address 00e0.9143.5615
(config)# iapp standby timeout ?
  <5-600> Standby polling timeout in seconds
(config)# iapp standby timeout 234
(config)# iapp standby poll-frequency ?
  <1-30> Standby polling frequency in seconds
(config)# iapp standby poll-frequency 11
(config)# iapp standby primary-shutdown ?
<cr>
```

Explanation

The hot standby function is used to provide a backup to another access point, and is configured in the same way, so that if it fails, the hot standby device can become active, and associates the active clients, automatically. The only setting that will differ is the IP address of the device. In the following configuration, the MAC address of the device to be monitored is **1111.abcd.ef10**. The timeout period in which the device will determine if the monitored device has stopped working is five seconds, and the poll time is two seconds:

```
# config t
(config)# iapp standby mac 1111.abcd.ef10
(config)# iapp standby timeout 5
(config)# iapp standby polltime 2
```

The hot standby device has a different IP address (as it may cause a conflict when the two devices are operating at the same time, but, for the sake of seamless operation, the hot standby device must be setup with the following settings by identical:

- SSID.
- IP Subnet Mask.
- Default gateway.
- Data rates.
- Encryption and authentication settings.

... diagrams missed out in demo version

Cisco Wireless Challenge 20

Outline

This challenge involves the configuration of a repeater.

Objectives

The objectives of this challenge are to:

- Define the BVI address and subnet mask.
- Define a repeater role.
- Define the parent MAC address.
- Setup infrastructure-SSID.

Example IOS Version 12.3

The following sets up the repeater:

```

> en
# config t
(config)# dot11 ssid mississippi
(config-ssid)# infrastructure-ssid
(config-ssid)# exit
(config)# int bvi1
(config-if)# ip address 160.51.42.9 255.255.128.0
(config-if)# int d0
(config-if)# no shut
(config-if)# ssid mississippi
(config-if)# station ?
    non-root          Non-root (bridge)
    repeater          Repeater access point
    root              Root access point or bridge
    scanner           Scanner access point
    workgroup-bridge Workgroup Bridge
(config-if)# station repeater
(config-if)# parent ?
    <1-4>             Parent number
    timeout           Time in seconds to look for parent
(config-if)# parent 1 ?
    H.H.H            Parent MAC addr
(config-if)# parent 1 00e0.4e3d.c533 ?
    <cr>
(config-if)# parent 1 00e0.4e3d.c533
(config-if)# parent timeout ?
    <0-65535>        Timeout in seconds

```

Example IOS Version 12.2

The following sets up the repeater:

```

> en
# config t
(config)# int bvi1
(config-if)# ip address 160.51.42.9 255.255.128.0
(config-if)# int d0
(config-if)# no shut
(config-if)# ssid mississippi
(config-if-ssid)# infrastructure-ssid
(config-if-ssid)# exit
(config-if)# station ?
    repeater          Repeater access point
    root              Root access point
(config-if)# station repeater
(config-if)# parent ?
    <1-4>             Parent number
    timeout           Time in seconds to look for parent
(config-if)# parent 1 ?
    H.H.H            Parent MAC addr
(config-if)# parent 1 00e0.4e3d.c533 ?
    <cr>
(config-if)# parent 1 00e0.4e3d.c533

```

Cisco Wireless Challenge 21

Outline

This challenge involves the configuration of a standard access-list

Objectives

The objectives of this challenge are to:

- Define a standard access-list
- Apply it on E0.

Example

The following sets up a standard access-list:

```
> en
# config t
(config)# access-list 3 permit ?
  Hostname or A.B.C.D  Address to match
  any                  Any source host
  host                 A single host address
(config)# access-list 3 permit host 199.237.96.4

(config)# access-list 3 deny host 163.209.141.8

(config)# access-list 3 permit 48.13.112.0 ?
  A.B.C.D  Wildcard bits
  log      Log matches against this entry
  <cr>
(config)# access-list 3 permit 48.13.112.0 0.15.255.255

(config)# access-list 3 deny 208.147.31.0 1.255.255.255

(config)# int e0

(config-if)# ip access-group 3 ?
  in  inbound packets
  out outbound packets
(config-if)# ip access-group 3 in
```

Cisco Wireless Challenge 22

Outline

This challenge involves the configuration of an extended ACL.

Objectives

The objectives of this challenge are to:

- Create an extended ACL.

- Apply it onto the incoming port of E0.

Example

The following sets up an extended ACL:

```
> en
# config t
(config)# access-list 106 ?
  deny      Specify packets to reject
  dynamic   Specify a DYNAMIC list of PERMITs or DENYS
  permit    Specify packets to forward
  remark    Access list entry comment
(config)# access-list 106 permit tcp host 202.33.249.1 host 162.97.253.5 eq
          syslog
(config)# access-list 106 deny tcp host 197.85.151.8 host 196.123.113.4 eq
          syslog
(config)# access-list 106 permit tcp 123.183.27.0 255.255.255.0 110.233.17.0
          255.255.255.0 eq syslog

(config)# access-list 106 deny tcp 24.81.208.0 255.255.255.0 127.46.93.0
          255.255.255.0 eq syslog

(config)# int e0
(config-if)# ip access-group 106 in
```

Cisco Wireless Challenge 23

Outline

This challenge involves the configuration of an encryption.

Objectives

The objectives of this challenge are to:

- Define the BVI address and subnet mask.
- Define the encryption key.
- Define LEAP.

Example IOS Version 12.3

The following sets up encryption and LEAP:

```
> en
# config t
(config)# dot11 ssid ohio
(config-ssid)# dot11 ssid ohio
(config-ssid)# authentication ?
  client          LEAP client information
```

```

key-management    key management
network-eap       leap method
open              open method
shared            shared method
(config-ssid)# authentication network-eap ?
WORD leap list name (1 -- 31 characters)
(config-ssid)# auth net newhamphshire ?
mac-address mac-address authentication method
<cr>
(config-ssid)# authentication network-eap newhamphshire
(config-ssid)# exit

(config)# int bvil
(config-if)# ip address 143.224.21.9 255.240.0.0
(config-if)# int d0
(config-if)# encry ?
key Set one encryption key
mode encryption mode
vlan vlan
(config-if)# encry key ?
<1-4> key number 1-4
(config-if)# encry key 1
size Key size
(config-if)# encry key 1 size ?
128bit 128-bit key
40bit 40-bit key
(config-if)# encry key 1 size 128bit ?
0 Specifies an UNENCRYPTED key will follow
7 Specifies a HIDDEN key will follow
Hex-data 26 hexadecimal digits
(config-if)# encry key 1 size 128bit ffffffffffffffffffffffffffff
(config-if)# encryp mode ?
ciphers Optional data ciphers
wep Classic 802.11 privacy algorithm
(config-if)# encryp mode ciphers ?
ckip Cisco Per packet key hashing
ckip-cmic Cisco Per packet key hashing and MIC (MMH)
cmic Cisco MIC (MMH)
tkip WPA Temporal Key encryption
wep128 128 bit key
wep40 40 bit key
(config-if)# encryp mode ciphers ckip
(config-if)# ssid ohio

```

Example IOS Version 12.1

The following sets up encryption and LEAP:

```

> en
# config t
Enter configuration commands, one per line. End with CNTL/Z.
(config)# int bvil
(config-if)# ip address 143.224.21.9 255.240.0.0
(config-if)# int d0
(config-if)# encry ?
key Set one encryption key
mode encryption mode
vlan vlan
(config-if)# encry key ?
<1-4> key number 1-4
(config-if)# encry key 1

```

```

size Key size
(config-if)# encry key 1 size ?
  128bit 128-bit key
  40bit 40-bit key
(config-if)# encry key 1 size 128bit ?
  0 Specifies an UNENCRYPTED key will follow
  7 Specifies a HIDDEN key will follow
  Hex-data 26 hexadecimal digits
(config-if)# encry key 1 size 128bit ffffffffffffffffffffffffffff
(config-if)# encryp mode ?
  ciphers Optional data ciphers
  wep Classic 802.11 privacy algorithm
(config-if)# encryp mode ciphers ?
  ckip Cisco Per packet key hashing
  ckip-cmic Cisco Per packet key hashing and MIC (MMH)
  cmic Cisco MIC (MMH)
  tkip WPA Temporal Key encryption
  wep128 128 bit key
  wep40 40 bit key
(config-if)# encryp mode ciphers ckip
(config-if)# ssid ohio
(config-if-ssid)# authentication ?
  client LEAP client information
  key-management key management
  network-eap leap method
  open open method
  shared shared method
(config-if-ssid)# authentication network-eap ?
  WORD leap list name (1 -- 31 characters)
(config-if-ssid)# authentication network-eap newhampshire

```

Cisco Wireless Challenge 24

Outline

This challenge involves the configuration of mobile IP.

Objectives

The objectives of this challenge are to:

- Enable proxy-mobile on the device, and on the interface ports.

Example

The following sets up mobile IP:

```

> en
# config t
(config)# ip proxy-mobile ?
  aap Authoritative AP
  enable Enable WLAN Proxy Mobile IP
  pause Disables Proxy Mobile IP without removing configuration
  secure Security association
(config)# ip proxy-mobile enable
(config)# int bv11

```

(config-if)# ?

Interface configuration commands:

access-expression	Build a bridge boolean access expression
arp	Set arp type (arpa, probe, snap) or timeout
bandwidth	Set bandwidth informational parameter
bridge-group	Transparent bridging interface parameters
carrier-delay	Specify delay for interface transitions
cdp	CDP interface subcommands
custom-queue-list	Assign a custom queue list to an interface
dampening	Enable event dampening
default	Set a command to its defaults
delay	Specify interface throughput delay
description	Interface specific description
duplex	Configure duplex operation.
exit	Exit from interface configuration mode
fair-queue	Enable Fair Queuing on an Interface
full-duplex	Configure full-duplex operational mode
half-duplex	Configure half-duplex and related commands
help	Description of the interactive help system
hold-queue	Set hold queue depth
ip	Interface Internet Protocol config commands
keepalive	Enable keepalive
l2-filter	Set Layer2 ACL for packet received by upper layer protocols
load-interval	Specify interval for load calculation for an interface
logging	Configure logging for interface
--More----- press any key ---	
loopback	Configure internal loopback on an interface
mac-address	Manually set interface MAC address
max-reserved-bandwidth	Maximum Reservable Bandwidth on an Interface
mtu	Set the interface Maximum Transmission Unit (MTU)
no	Negate a command or set its defaults
ntp	Configure NTP
priority-group	Assign a priority group to an interface
random-detect	Enable Weighted Random Early Detection (WRED) on an Interface
service-policy	Configure QoS Service Policy
shutdown	Shutdown the selected interface
snmp	Modify SNMP interface parameters
speed	Configure speed operation.
timeout	Define timeout values for this interface
transmit-interface	Assign a transmit interface to a receive-only interface
tx-ring-limit	Configure PA level transmit ring limit

(config-if)# ip proxy-mobile ?

<cr>

(config-if)# ip proxy-mobile

(config-if)# int d0

(config-if)# ip proxy-mobile

(config-if)# int e0

(config-if)# ip proxy-mobile

Cisco Wireless Challenge 25

Outline

This challenge involves the configuration of a VLAN.

Objectives

The objectives of this challenge are to:

- Define a VLAN.
- Enable 802.1q on sub-interfaces.

Example

```
> en
# config t
(config)# dot11 ssid test
(config-ssid)# vlan 10
(config-ssid)# exit
(config)# int d0.1
(config-subif)# ?
Interface configuration commands:
  arp          Set arp type (arpa, probe, snap) or timeout
  bandwidth    Set bandwidth informational parameter
  bridge-group Transparent bridging interface parameters
  cdp          CDP interface subcommands
  default      Set a command to its defaults
  delay        Specify interface throughput delay
  description  Interface specific description
  encapsulation Set encapsulation type for an interface
  exit         Exit from interface configuration mode
  ip          Interface Internet Protocol config commands
  keepalive    Enable keepalive
  logging      Configure logging for interface
  mtu          Set the interface Maximum Transmission Unit (MTU)
  no          Negate a command or set its defaults
  service-policy Configure QoS Service Policy
  shutdown     Shutdown the selected interface
  timeout      Define timeout values for this interface
(config-subif)# encapsulation?
  dot1Q IEEE 802.1Q Virtual LAN

(config-subif)# encapsulation dot1q ?
  <1-4094> IEEE 802.1Q VLAN ID

(config-subif)# encapsulation dot1q 1 ?
  native      Make this as native vlan
  second-dot1q Configure this subinterface as a 1Q-in-1Q subinterface
  <cr>
(config-subif)# encapsulation dot1q 10 native
(config-subif)# exit
(config)# int fa0.1
(config-subif)# encapsulation dot1q 10 native
(config-if)# exit
```

Cisco Wireless Challenge 26

Outline

This is an intermediate test, which revises some of the main principles of Wireless configuration. It will show knowledge of:

- Hostname
- BVI settings.
- Gateway setting.
- Domain name setting.
- D0 settings.
- SSID settings.
- Username and password.
- HTTP enable.

Cisco Wireless Challenge 27

Outline

This challenge involves the configuration of location based services (LBS).

Objectives

The objectives of this challenge are to:

- Define an LBS profile.
- Define the LBS server address and port.
- Define LBS interface.

Example

```
> en
# config t
(config)# dot11 lbs test
(dot11-lbs)#?
lbs configuration commands:
  channel-match  only reports tag packet in the same tx & rx channel
  exit           Exit from LBS sub mode
  interface      enable LBS on radio interface
  method         method used for AP to locate tag
  multicast      multicast MAC address of LBS TAGs
  no             Negate a command or set its defaults
  packet-type    packet type used by the LBS tag and server
  server         remote LBS server IP address and UDP port number
(dot11-lbs)# server a ?
  A.B.C.D  IP address

(dot11-lbs)# server a 1.2.3.4 ?
  port    server UDP port number

(dot11-lbs)# server a 1.2.3.4 p ?
  <1024-65535>  port number
```

```
(dot11-lbs)# server a 10.0.0.1 port 1024 ?
<cr>
(dot11-lbs)# server address 10.0.0.1 port 1024
(dot11-lbs)# interface d0
(dot11-lbs)# method ?
    rssi  received signal strength identification
(dot11-lbs)# method r ?
<cr>
(dot11-lbs)# method rssi
```

Description

With LBS, access points monitor location packets sent by LBS positioning tags, and thus allow assets to be tracked. On receiving a positioning packet, the access point determines the received signal strength indication (RSSI). It then creates a UDP packet with the RSSI value and the current time, which it then forwards to a location server. Next the location server determines the position of the tag based on the information received.

Cisco Wireless Challenge 28

Outline

This challenge involves the configuration of AAA for local authentication.

Objectives

The objectives of this challenge are to:

- Enable AAA.
- Define local authentication.

Example

The following sets up AAA:

```
> en
# config t
(config)# aaa new-model
(config)# aaa authentication login default local
(config)# aaa authorization exec local
(config)# aaa authorization network local
(config)# user ?
    WORD  User name
(config)# user test ?
    access-class      Restrict access by access-class
    autocommand       Automatically issue a command after the user logs in
    callback-dialstring  Callback dialstring
    callback-line      Associate a specific line with this callback
    callback-rotary    Associate a rotary group with this callback
    dnis               Do not require password when obtained via DNIS
    nocallback-verify  Do not require authentication after callback
    noescape          Prevent the user from using an escape character
```

```

nohangup          Do not disconnect after an automatic command
nopassword        No password is required for the user to log in
password          Specify the password for the user
privilege         Set user privilege level
secret           Specify the secret for the user
user-maxlinks     Limit the user's number of inbound links
view             Set view name
<cr>
(config)# user test password ?
 0      Specifies an UNENCRYPTED password will follow
 7      Specifies a HIDDEN password will follow
LINE   The UNENCRYPTED (cleartext) user password
(config)# username test password bert

```

Cisco Wireless Challenge 29

Outline

This challenge involves the configuration of AAA.

Objectives

The objectives of this challenge are to:

- Enable AAA.
- Define local RADIUS.
- Define RADIUS settings.

Example

The following sets up AAA:

```

> en
# config t
(config)# aaa new-model
(config)# radius-server ?
 attribute          Customize selected radius attributes
 authorization      Authorization processing information
 challenge-noecho   Data echoing to screen is disabled during
                   Access-Challenge
 configure-nas     Attempt to upload static routes and IP pools at startup
 deadtime          Time to stop using a server that doesn't respond
 directed-request  Allow user to specify radius server to use with '@server'
 domain-stripping  Strip the domain from the username
 host              Specify a RADIUS server
 key               encryption key shared with the radius servers
 local             Configure local RADIUS server
 optional-passwords The first RADIUS request can be made without requesting a
                  password
 retransmit        Specify the number of retries to active server
 timeout           Time to wait for a RADIUS server to reply
 unique-ident      Higher order bits of Acct-Session-Id
 vsa               Vendor specific attribute configuration

```

```

(config)# radius-server local
(config-radsrv)#?
Local RADIUS server configuration commands:
 authentication supported authentication
 eapfast          EAP-FAST configurations
 exit             Exit from local radius server sub mode
 group           Configure client groups
 nas            Configure allowed Network Access Servers
 no             Negate a command or set its defaults
 user           Configure client usernames and passwords
(config-radsrv)# user ?
 WORD Client username
(config-radsrv)# user giraffe ?
 nhash          Set NT hash of clientpassword
 password       Set client password
(config-radsrv)# user giraffe password root
(config-radsrv)# nas ?
 A.B.C.D IP address of the NAS
(config-radsrv)# nas 42.55.230.3 ?
 key           Set NAS shared secret
(config-radsrv)# nas 42.55.230.3 key coconut
(config-radsrv)# exit
(config)# radius-server ?
 attribute      Customize selected radius attributes
 authorization   Authorization processing information
 challenge-noecho Data echoing to screen is disabled during
                Access-Challenge
 configure-nas  Attempt to upload static routes and IP pools at startup
 deadtime      Time to stop using a server that doesn't respond
 directed-request Allow user to specify radius server to use with '@server'
 domain-stripping Strip the domain from the username
 host          Specify a RADIUS server
 key           encryption key shared with the radius servers
 local        Configure local RADIUS server
 optional-passwords The first RADIUS request can be made without requesting a
                password
 retransmit    Specify the number of retries to active server
 timeout       Time to wait for a RADIUS server to reply
 unique-ident  Higher order bits of Acct-Session-Id
 vsa          Vendor specific attribute configuration
(config)# radius-server host ?
 Hostname or A.B.C.D IP address of RADIUS server
(config)# radius-server host 42.55.230.3
 acct-port     UDP port for RADIUS accounting server (default is 1646)
 alias        1-8 aliases for this server (max. 8)
 auth-port    UDP port for RADIUS authentication server (default is 1645)
 key         per-server encryption key (overrides default)
 non-standard Parse attributes that violate the RADIUS standard
 retransmit  Specify the number of retries to active server (overrides
                default)
 timeout     Time to wait for this RADIUS server to reply (overrides
                default)
<cr>
(config)# radius-server host 42.55.230.3 auth 1812 acct 1813

```

Cisco Wireless Challenge 30

Outline

This challenge involves the configuration of and RADIUS account on an SSID.

Objectives

The objectives of this challenge are to:

- Enable AAA.
- Define RADIUS.
- Define an SSID.
- Associate RADIUS account with an SSID.

Example

```
> en
# config t
(config)# aaa new-model
(config)# radius h ?
  Hostname or A.B.C.D  IP address of RADIUS server
(config)# rad h 1.2.3.4 ?
  acct-port           UDP port for RADIUS accounting server (default is 1646)
  alias               1-8 aliases for this server (max. 8)
  auth-port           UDP port for RADIUS authentication server (default is 1645)
  backoff             Retry backoff pattern (Default is retransmits with constant
                    delay)
  key                 per-server encryption key (overrides default)
  non-standard        Parse attributes that violate the RADIUS standard
  retransmit          Specify the number of retries to active server (overrides
                    default)
  timeout             Time to wait for this RADIUS server to reply (overrides
                    default)
  <cr>
(config)# radius-server host 42.55.230.3 auth 1812 acct 1813
(config)# dot11 ssid test
(config-ssid)# accounting test-acc
```

Cisco Wireless Challenge 31

Outline

This challenge involves the configuration of a secure HTTP server (HTTPS), which is more secure than normal Web access to the access point (HTTP). In an HTTPS connection the data transmitted is encrypted.

Objectives

The objectives of this challenge are to:

- Define a host name.
- Define the domain name.
- Define the gateway.
- Define an HTTPS server.
- Define the HTTPS port (default: 443).

Example

```
> en
# config t
(config)# hostname test
(config)# ip default-gateway 192.168.0.1
(config)# ip domain-name perth.cc
(config)# ip http ?
  access-class          Restrict http server access by access-class
  authentication        Set http server authentication method
  client                Set http client parameters
  help-path             HTTP help root URL
  max-connections       Set maximum number of concurrent http server connections
  path                  Set base path for HTML
  port                  Set http server port
  secure-ciphersuite    Set http secure server ciphersuite
  secure-client-auth    Set http secure server with client authentication
  secure-port           Set http secure server port number for listening
  secure-server         Enable HTTP secure server
  secure-trustpoint     Set http secure server certificate trustpoint
  server                Enable http server
  timeout-policy        Set http server time-out policy parameters
(config)# ip http secure-server
(config)# ip http secure-port ?
  <0-65535> Secure port number(above 1024 or default 443)
(config)# ip http secure-port 443
```

Cisco Wireless Challenge 32

Outline

This challenge involves the configuration of TACACS+ for the Aironet.

Objectives

The objectives of this challenge are to:

- Define a host name.
- Define AAA.
- Define Tacacs+

Example

```
> en
```

```
# config t
(config)# hostname test
(config)# aaa new-model
(config)# tacacs-server host 39.100.234.1
(config)# tacacs-server key krinkle
(config)# aaa authentication login default group tacacs
(config)# aaa authentication ppp default group tacacs
(config)# aaa authorization network default group tacacs
(config)# aaa authorization exec default group tacacs
```

Cisco Wireless Challenge 33

Outline

This challenge involves the configuration of security of the wireless access point.

Objectives

The objectives of this challenge are to:

- Define usernames and passwords.
- Define privilege levels.
- Restrict access of users to a single host.

Example

```
> enable
# config t
(config)# username fred ?
access-class          Restrict access by access-class
autocommand           Automatically issue a command after the user logs in
callback-dialstring   Callback dialstring
callback-line         Associate a specific line with this callback
callback-rotary       Associate a rotary group with this callback
dnis                  Do not require password when obtained via DNIS
nocallback-verify    Do not require authentication after callback
noescape              Prevent the user from using an escape character
nohangup              Do not disconnect after an automatic command
nopassword            No password is required for the user to log in
password              Specify the password for the user
privilege              Set user privilege level
secret                Specify the secret for the user
user-maxlinks         Limit the user's number of inbound links
view                  Set view name
<cr>
(config)# username fred password bert
(config)# username test nopassword
(config)# username fred privilege 15
(config)# username test privilege 1
(config)# username test user-maxlinks 2
```

```
(config)# access-list 9 permit host 192.168.0.1
(config)# user fred access-class ?
  <1-199>      Access-class number
  <1300-2699>  Expanded Access-class number
(config)# username fred access-class 9
```

Explanation

The privilege levels go from level 0 to level 15, such as:

- **Level 0.** This only includes five commands: disable, enable, exit, help and logout.
- **Level 1.** This is the non-privileged mode with a prompt of **wap>**.
- **Level 15.** This is the highest level of privilege, and has a prompt of **wap#**.

Typical 1 commands are:

access-enable	Create a temporary Access-List entry
clear	Reset functions
connect	Open a terminal connection
disable	Turn off privileged commands
disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
exit	Exit from the EXEC
help	Description of the interactive help system
lock	Lock the terminal
login	Log in as a particular user
logout	Exit from the EXEC
name-connection	Name an existing network connection
ping	Send echo messages
rcommand	Run command on remote switch
resume	Resume an active network connection
show	Show running system information
sysstat	Display information about terminal lines
telnet	Open a telnet connection
terminal	Set terminal line parameters
traceroute	Trace route to destination
tunnel	Open a tunnel connection
where	List active connections

Thus:

```
(config)# username fred privilege 15
(config)# username test privilege 1
```

sets the maximum privilege level for **fred** at 15, while **test** will only be able to enter the non-privileged mode. Also:

```
(config)# access-list 9 permit host 192.168.0.1
(config)# username fred access-class 9
```

restricts the access for fred to a single host (192.168.0.1), so that the user will not be able to log-in from any other host. The following:

```
(config)# username test user-maxlinks 2
```

restricts the number of connections for **test** to two.

Cisco Wireless Challenge 34

Outline

This challenge involves the configuration of the banner messages.

Objectives

The objectives of this challenge are to:

- Setup the Message-of-the-day (MOTD) message.
- Setup the Login message.
- Setup the EXEC message.

Example

```
> enable
# config t
(config)# hostname amsterdam
amsterdam (config)# banner motd my device
amsterdam (config)# banner login how are you
amsterdam (config)# banner exec main device
amsterdam (config)# ip http server
```

Cisco Wireless Challenge 35

Outline

This challenge involves the configuration of Simple Network Time Protocol (SNTP).

Objectives

The objectives of this challenge are to:

- Setup SNTP to receive time updates from a specific server.
- Setup device to receive SNTP broadcasts.

- Set the system clock (this would not be required if an SNTP server is used, obviously).

Example

```

> enable
# config t
(config)# hostname amsterdam
amsterdam (config)# sntp ?
  broadcast  Configure SNTP broadcast services
  logging    Enable SNTP message logging
  server     Configure SNTP server
amsterdam (config)# sntp s ?
  Hostname or A.B.C.D Name or IP address of server
amsterdam (config)# sntp server 192.168.1.100 ?
  version    Configure NTP version
<cr>
amsterdam (config)# sntp server 192.168.1.100
amsterdam (config)# sntp broadcast ?
  client     Enable SNTP broadcast client mode
amsterdam (config)# sntp broadcast client
amsterdam (config)# exit
amsterdam # clock set 05:44
amsterdam # show sntp
SNTP server      Stratum   Version   Last Receive
192.168.1.100    16        1         never

```

Broadcast client mode is enabled.

Cisco Wireless Challenge 36

Outline

This challenge involves the configuration of filtering incoming MAC addresses for D0.

Objectives

The objectives of this challenge are to:

- Setup MAC filters.
- Implement MAC filters on the outgoing port of D0.

Example

```

> enable
# config t
(config) # access-list ?
<1-99>          IP standard access list
<100-199>      IP extended access list
<1100-1199>    Extended 48-bit MAC address access list
<1300-1999>    IP standard access list (expanded range)

```

```

<200-299>          Protocol type-code access list
<2000-2699>        IP extended access list (expanded range)
<700-799>          48-bit MAC address access list
dynamic-extended  Extend the dynamic ACL absolute timer
(config) # access-list 701 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
(config) # access-list 701 deny ?
  H.H.H   48-bit hardware address
(config) # access-list 701 deny 1111.2222.3333 ?
  H.H.H   48-bit hardware address mask
<cr>
(config) # access-list 701 deny 1111.2222.3333 ffff.ffff.ffff
(config) # access-list 701 deny 1112.2222.3333 ffff.ffff.ffff
(config) # access-list 701 deny 1113.2222.3333 ffff.ffff.ffff
(config) # access-list 701 permit 0.0.0 ffff.ffff.ffff
(config) # int d0
(config-if) # l2-filter bridge-group-acl
(config-if) # bridge-group ?
  <1-255> Assign an interface to a Bridge Group.
(config-if) # bridge-group 1
(config-if) # bridge-group 1 ?
<cr>
circuit-group          Associate serial interface with a circuit group
input-address-list     Filter packets by source address
input-lat-service-deny Deny input LAT service advertisements matching a
                       group list
input-lat-service-permit Permit input LAT service advertisements matching a
                       group list
input-lsap-list        Filter incoming IEEE 802.3 encapsulated packets
input-type-list        Filter incoming Ethernet packets by type code
lat-compression        Enable LAT compression over serial or ATM
                       interfaces
output-address-list    Filter packets by destination address
output-lat-service-deny Deny output LAT service advertisements matching a
                       group list
output-lat-service-permit Permit output LAT service advertisements matching
                       a group list
output-lsap-list       Filter outgoing IEEE 802.3 encapsulated packets
output-type-list       Filter outgoing Ethernet packets by type code
port-protected         There will be no traffic between this interface
                       and other protected
                       subscriber-loop-control Configure subscriber loop control
                       port interface in this bridge group
block-unknown-source   block traffic which come from unknown source MAC
                       address
input-pattern-list     Filter input with a pattern list
output-pattern-list    Filter output with a pattern list
path-cost              Set interface path cost
priority              Set interface priority
source-learning        learn source MAC address
spanning-disabled     Disable spanning tree on a bridge group
unicast-flooding       flood packets with unknown unicast destination MAC
                       addresses

(config-if) # bridge-group 1 input-address-list 701

```

Cisco Wireless Challenge 37

Outline

This challenge involves the configuration of filtering outgoing MAC addresses for D0.

Objectives

The objectives of this challenge are to:

- Setup MAC filters.
- Implement MAC filters on the outgoing port of D0.

Example

```
> enable
# config t
(config) # access-list 701 deny 1111.2222.3333 ffff.ffff.ffff
(config) # access-list 701 deny 1112.2222.3333 ffff.ffff.ffff
(config) # access-list 701 deny 1113.2222.3333 ffff.ffff.ffff
(config) # access-list 701 permit 0.0.0 ffff.ffff.ffff
(config) # int d0
(config-if)# l2-filter ?
    block-arp          avoid arp attack
    bridge-group-acl   Use bridge-group ACLs
(config-if)# l2-filter bridge-group-acl ?
<cr>
(config-if) # l2-filter bridge-group-acl
(config-if)# bridge- ANY ?
<cr>
circuit-group          Associate serial interface with a circuit group
input-address-list     Filter packets by source address
input-lat-service-deny Deny input LAT service advertisements matching a
                        group list
input-lat-service-permit Permit input LAT service advertisements matching a
                        group list
input-lsap-list        Filter incoming IEEE 802.3 encapsulated packets
input-type-list        Filter incoming Ethernet packets by type code
lat-compression        Enable LAT compression over serial or ATM
                        interfaces
output-address-list    Filter packets by destination address
output-lat-service-deny Deny output LAT service advertisements matching a
                        group list
output-lat-service-permit Permit output LAT service advertisements matching
                        a group list
output-lsap-list       Filter outgoing IEEE 802.3 encapsulated packets
output-type-list       Filter outgoing Ethernet packets by type code
port-protected         There will be no traffic between this interface
                        and other protected
subscriber-loop-control Configure subscriber loop control
                        port interface in this bridge group
block-unknown-source   block traffic which come from unknown source MAC
                        address
input-pattern-list     Filter input with a pattern list
output-pattern-list    Filter output with a pattern list
path-cost              Set interface path cost
priority              Set interface priority
source-learning        learn source MAC address
spanning-disabled     Disable spanning tree on a bridge group
unicast-flooding       flood packets with unknown unicast destination MAC
                        addresses
```

```
(config-if) # bridge-group 1
(config-if)# bridge- ANY output-a ?
<700-799> Ethernet address access list
(config-if) # bridge-group 1 output-address-list 701
```

Cisco Wireless Challenge 38

Outline

This challenge involves the configuration of filtering outgoing MAC addresses for D0 for a source and destination MAC address.

Objectives

The objectives of this challenge are to:

- Setup an extended MAC address filter.
- Implement MAC filter on the outgoing port of D0.

Example

```
> enable
# config t
(config) # access-list 1102 deny 1111.2222.3333 0.0.0 1112.2222.3333 0.0.0
(config) # access-list 1102 permit 0.0.0 ffff.ffff.ffff 0.0.0 ffff.ffff.ffff
(config) # int d0
(config-if) # l2-filter bridge-group-acl
(config-if) # bridge-group 1
(config-if) # bridge-group 1 output-pattern-list ?
<1100-1199> Pattern access list number
(config-if) # bridge-group 1 output-pattern-list 1102
```

Cisco Wireless Challenge 39

Outline

This challenge involves the configuration of filtering outgoing MAC addresses for D0 for a source and destination MAC address.

Objectives

The objectives of this challenge are to:

- Setup an extended MAC address filter.
- Implement MAC filter on the incoming port of D0.

Example

```
> enable
# config t
(config) # access-list 1102 deny 1111.2222.3333 0.0.0 1112.2222.3333 0.0.0
(config) # access-list 1102 permit 0.0.0 ffff.ffff.ffff 0.0.0 ffff.ffff.ffff
(config) # int d0
(config-if) # l2-filter bridge-group-acl
(config-if) # bridge-group 1
(config-if) # bridge-group 1 input-pattern-list ?
<1100-1199> Pattern access list number
(config-if) # bridge-group 1 input-pattern-list 1102
```

Cisco Wireless Challenge 40

Outline

This challenge involves the configuration of filtering incoming MAC addresses for D0.

Objectives

The objectives of this challenge are to:

- Setup MAC filters.
- Implement MAC filters on the outgoing port of D0.

Example

```
> enable
# config t
(config) # access-list 701 permit 1111.2222.3333 ffff.ffff.ffff
(config) # access-list 701 permit 1112.2222.3333 ffff.ffff.ffff
(config) # access-list 701 permit 1113.2222.3333 ffff.ffff.ffff
(config) # access-list 701 deny 0.0.0 ffff.ffff.ffff
(config) # int d0
(config-if) # l2-filter bridge-group-acl
(config-if) # bridge-group 1
(config-if) # bridge-group 1 input-address-list 701
```

Cisco Wireless Challenge 41

Outline

This challenge involves the configuration of ARP caching for connected wireless nodes, and to enable Cisco Aironet extensions.

Objectives

The objectives of this challenge are to:

- Setup BVI port.
- Enable ARP caching for connected wireless nodes.
- Enable Cisco Aironet extensions.

Example

```
> enable
# config t
(config)# int bvi 1
(config-if)# ip address 158.234.223.7 255.192.0.0
(config-if)# exit
(config)# dot11 arp-cache
(config)# int d0
(config-if)# dot11 ?
  extension  Cisco IEEE 802.11 extension
  qos        Dot11 QOS configuration

(config-if)# dot11 ex ?
  aironet    Cisco Aironet extension
  power      Enable Cisco proprietary native power management
(config-if)# dot11 extension aironet
```

Explanation

The Cisco Aironet extensions are:

- Cisco Key Integrity Protocol (CKIP). This uses a permutation method to renew the WEP key. If TKIP is used, CKIP is not required.
- Limiting power level. This allows the Aironet to control the power level of the clients, once they associate.
- Load balancing. This allows the access point to select the best access point in terms of signal strength, load requirements, and so on.
- Message Integrity Check (MIC). This enhances WEP security against a number of attacks.
- Repeater mode. This allows the access point to support repeater access points.
- World mode. This allows for carrier information from the wireless device and adjust their settings automatically.

Cisco Wireless Challenge 42

Outline

This challenge involves the disabling of ARP caching for connected wireless nodes, and to disable Cisco Aironet extensions.

Objectives

The objectives of this challenge are to:

- Setup BVI port.
- Disable ARP caching for connected wireless nodes.
- Disable Cisco Aironet extensions.

Example

```
> enable
# config t
(config)# int bvi 1
(config-if)# ip address 158.234.223.7 255.192.0.0
(config-if)# exit
(config)# no dot11 arp-cache
(config)# int d0
(config-if)# no dot11 extension aironet
```

Explanation

The Cisco Aironet extensions are:

- Cisco Key Integrity Protocol (CKIP). This uses a permutation method to renew the WEP key. If TKIP is used, CKIP is not required.
- Limiting power level. This allows the Aironet to control the power level of the clients, once they associate.
- Load balancing. This allows the access point to select the best access point in terms of signal strength, load requirements, and so on.
- Message Integrity Check (MIC). This enhances WEP security against a number of attacks.
- Repeater mode. This allows the access to support repeater access points.
- World mode. This allows for carrier information from the wireless device and adjust their settings automatically.

Cisco Wireless Challenge 43

Outline

This challenge involves the configuration of the beacon settings for the beacon period and for the DTIM (delivery traffic indication message).

Objectives

The objectives of this challenge are to:

- Define the beacon period.
- Define the beacon DTIM.

Example

```
> enable
# config t
(config)# int bv11
(config-if)# ip address 208.1.7.8 255.255.255.224
(config-if)# int d0
(config-if)# beacon ?
    dtim-period  dtim period
    period       beacon period
(config-if)# beacon period ?
    <20-4000>  Kusec (or msec)
(config-if)# beacon period 2000
(config-if)# beacon dtim?
    <1-100>  dtim count
(config-if)# beacon dtim 50
```

Explanation

The beacon period is defined as the amount of time between access point beacons in Kilomicroseconds (1 K μ sec is 1,024 milliseconds). The default is 100 K μ sec. If the beacon period is 1000, the time between beacons is approximately 1 second (1.024 seconds).

The Data Beacon Rate defines how often the DTIM (delivery traffic indication message) appears in a beacon, where the DTIM tells power-save client devices that a packet is waiting for them. The default DTIM is 2. If the DTIM is set at 5, and the beacon period is 1000, a packet with a DTIM will be sent every 5 seconds (approx).

RTS Explained

Outline: This challenge involves an analysis of RTS.

Objectives: The objectives of this challenge are to explain RTS.

Example

```
> enable
# config t
(config)# int bvi1
(config-if)# ip address 208.1.7.8 255.255.255.224
(config-if)# int d0
(config-if)# rts ?
    retries    RTS max retries
    threshold  RTS threshold

(config-if)# rt re ?
    <1-128>    max retries

(config-if)# rts retries 100
(config-if)# rt th ?
    <0-2347>   threshold in bytes
(config-if)# rts threshold 1000
```

Explanation

The RTS threshold prevents the *Hidden Node* problem, where two wireless nodes are within range of the same access point, but are not within range of each other, as illustrated in Figure 1. As they do not know that they both exist on the network, they may try to communicate with the access point at the same time. When they do, their data frames may collide when arriving simultaneously at the access point, which causes a loss of data frames from the nodes. The RTS threshold tries to overcome this by enabling the handshaking signals of Ready To Send (RTS) and Clear To Send (CTS). When a node wishes to communicate with the access point it sends a RTS signal to the access point. Once the access point defines that it can then communicate, it sends a CTS signal. The node can then send its data, as illustrated in Figure 2. RTS threshold determines the data frame size that is required, in order for it send an RTS to the WAP. The default value is 4000.

```
# config t
(config)# int dot11radio0
(config-if)# rts ?
    retries    RTS max retries
    threshold  RTS threshold
(config-if)# rts threshold ?
    <0-2347>   threshold in bytes
(config-if)# rts threshold 2000
```

... diagrams not shown in Demo version.

RTS retries defines the number of times that an access point will transmit an RTS signal before it stops sending the data frame. Values range from 1 to 128. For example:

```
# config t
(config)# int dot11radio0
(config-if)# rts retries ?
    <1-128> max retries
(config-if)# rts retries 10
(config-if)# end
```

Fragment-threshold Explained

Outline: This challenge involves an analysis of the fragment-threshold.

Objectives: The objectives of this challenge are to explain fragment-threshold.

Example

```
> enable
# config t
(config)# int bv11
(config-if)# ip address 208.1.7.8 255.255.255.224
(config-if)# int d0
(config-if)# fragment-threshold ?
    <256-2346>
(config-if)# fragment-threshold 1000
```

Explanation

A wireless data frame can have up to 2312 data bytes in the data payload. This large amount could hog the bandwidth too much, and not give an even share to all the nodes on the network, as illustrated in Figure 1. Research has argued that creating smaller data frames, often known as cells, is more efficient in using the available bandwidth, and also for switching data frames. Thus wireless systems provides a fragment threshold, in which the larger data frames are split into smaller parts, as illustrated in Figure 2. An example of the configuration is:

```
# config t
(config)# int dot11radio0
(config-if)# fragment-threshold ?
    <256-2346>
(config-if)# fragment-threshold 700
```

... diagrams missed out in demo version

Power Settings Explained

Outline: This challenge involves an analysis of the power settings.

Objectives: The objectives of this challenge are to explain power settings.

Example

```
> enable
# config t
(config)# int bvi1
(config-if)# ip address 208.1.7.8 255.255.255.224
(config-if)# int d0
(config-if)# po lo cc ?
<1 - 50> One of: 1 5 10 20 30 50
maximum Set local power to allowed maximum
(config-if)# power local 50
(config-if)# power client ?
<1 - 50> One of: 1 5 10 20 30 50
local Set client power to Access Point local power
maximum Set client power to allowed maximum
(config-if)# power client 10
```

Explanation

The power of the access point and also of the clients are important as they will define the coverage of the signal, and must also be within the required safety limits. Thus, the more radio power that is used to transmit the signal, the wider the scope of the wireless network. Unfortunately, the further that the signal goes, the more chance that an intruder can pick up the signal, and, possibly, gain access to its contents, as illustrated in Figure 1. To control this power, the access point can set up its own radio power, and also is able to set the power transmission of the client adapter. An example in setting the local power, and the client is shown next:

```
# config t
(config)# int dot11radio0
(config-if)# power ?
(config-if)# power local ?
<1-50> One of: 1 5 20 30 50
maximum Set local power to allowed maximum
(config-if)# power local 30
(config-if)# power client ?
<1-50> One of: 1 5 20 30 50
maximum Set client power to allowed maximum
(config-if)# power client 10
```

... diagrams missed out in demo version

One the client, especially with portable devices, the power usage of the radio port is important. Thus there are typically power settings, such as:

- **CAM** (Constant awake mode). Used when power usage is not a problem.
- **PSP** (Power save mode). Power is conserved as much as possible. The card will typically go to sleep, and will only be awoken by the access point, or if there is activity.
- **FastPSP** (Fast power save mode). This uses both CAM and PSP, and is a compromise between the two.

Max-associations Explained

Outline: This challenge involves an analysis of the power settings.

Objectives: The objectives of this challenge are to explain the maximum associations.

Example (12.3)

```
> enable
# config t
(config)# dot11 ssid fred
(config-ssid)# max ?
    <1-255> association limit
(config-ssid)# max-assoc 9
(config-ssid)# exit

(config)# int bv11
(config-if)# ip address 208.1.7.8 255.255.255.224
(config-if)# int d0
(config-if)# ssid fred
```

Example

```
> enable
# config t
(config)# int bv11
(config-if)# ip address 208.1.7.8 255.255.255.224
(config-if)# int d0
(config-if)# ssid fred
(config-if-ssid)# max-assoc ?
<1-255> association limit
(config-if-ssid)# max-assoc 9
```

Explanation

A particular problem in wireless networks is that the access point may become overburdened with connected clients. This could be due to an attack, such as **DoS** (Denial of Service), or due to **poor planning**. To set the maximum number of associations, the max-associations command is used within the SSID setting:

```
# config t
(config)# int dot11radio0
(config-if)# ssid fred
(config-if-ssid)# max ?
    <1-255> association limit
(config-if-ssid)# max 100
(config)# exit
```

and to show the associations for the wireless access point:

```
# show dot11 ?
# show dot11 association
```

```
# show dot11 statistics client-traffic
```

and for associated access points:

```
# show dot11 adjacent-ap
```

Preamble Explained

Outline: This challenge involves an analysis of the preamble.

Objectives: The objectives of this challenge are to explain the preamble.

Explanation

This can either be set to Long (which is the default) or short. A long preamble allows for interoperatively with 1Mbps and 2Mbps DSSS specifications. The shorter allows for faster operations (as the preamble is kept to a minimum) and can be used where the transmission parameters must be maximized, and that there are no interoperability problems. To set short preamble:

```
# config t
(config)# int dot11radio0
(config-if)# preamble-short
(config-if)# end
```

... diagrams missed out in demo version

Station-role Explained

Outline: This challenge involves an analysis of the station role.

Objectives: The objectives of this challenge are to explain the station role.

Explanation

A root access point is used to connect a wireless client to a fix network, whereas a repeater access point does not connect to a wired LAN, and basically forwards the data packets to another repeater or to a wireless access point which is connected to a wired network (Figure 1). With a repeater, of course, the Ethernet port will not operate. The repeater access point typically associates with an access point which has the best connectivity, however they can be setup to connect to a specific access point. In the following case, the access point will associate with the parent with the specified MAC address (1111.2222.3333):

```
# config t
```

```

(config)# dot11 ssid napier
(config-ssid)# infr ?
    optional  turn off infrastructure restrictions
    <cr>
(config-ssid)# infrastructure-ssid
(config-ssid)# exit

(config)# interface d0
(config-if)# ssid napier
(config-if)# station-role repeater
(config-if)# dot11 extensions aironet
(config-if)# parent ?
    <1-4>      Parent number
    timeout   Time in seconds to look for parent
(config-if)# parent 1 ?
    H.H.H     Parent MAC addr
(config-if)# parent 1 1111.2222.3333
(config-if)# parent 2 2222.aaaa.bbbb
(config-if)# end

```

Or

```

# config t
(config)# interface d0
(config-if)# ssid napier
(config-ssid)# infrastructure-ssid
(config-ssid)# exit
(config-if)# station-role repeater
(config-if)# dot11 extensions aironet
(config-if)# parent 1 1111.2222.3333
(config-if)# parent 2 2222.aaaa.bbbb
(config-if)# end

```

It is possible to define up to four parents, so that if one fails to association, it can use others. In most cases the Cisco Aironet extensions must be enabled, as it aids the association process, but this can cause incompatibility problems with non-Cisco devices.

... diagrams missed out in demo version

The repeater will start with the first parent, and, if it cannot connect, it will then try the next parent, and so on. Overall, repeaters are fairly good at extending the range of a wireless network, but reduce the throughput, as bandwidth is wasted in relaying the data from repeaters. As an approximation the actual throughput will be reduced by at least half.

Short-time Slot Explained

Outline: This challenge involves an analysis of the short-time slot.

Objectives: The objectives of this challenge are to explain the short-time slot.

Explanation

The throughput of a wireless network can be reduced by enabling short slot time. When enabled it reduces the slot time from 20 microseconds to 9 microseconds. The backoff time is the time that wireless nodes and is a random multiple of the slot-time. Thus reducing the slot time will typically reduce the backoff time. To enable it:

```
(config)# int d0
(config-if)# short-time-short
```

Note that short slot time is only available in IEEE 802.11g. By default it is disabled.

MAC Authentication Explained

Outline: This challenge involves an analysis of the MAC authentication cache.

Objectives: The objectives of this challenge are to explain MAC authentication cache.

Example

```
> enable
# config t
(config)# int bvi1
(config-if)# ip address 208.1.7.8 255.255.255.224
(config-if)# exit
(config)# aaa new-model
(config)# dot11 aaa ?
  authentication  Authentication
  csid            Calling and Called station ID format
  dot1x          802.1x
(config)# dot11 aaa authentication ?
  attributes     Configure Dot11 AAA authentication attributes
  mac-authen     Configure Mac Authentication details
(config)# dot11 aaa authentication mac-authen filter-cache
```

Explanation

MAC authentication cache on the access points is typically used where MAC-authenticated clients roam around the network. When it is enabled it reduces the time overhead in re-authenticating the nodes with an authentication server. When a node is initially authenticated, its MAC address is added to the cache.

Wireless IDS Explained

Outline: This challenge involves an analysis of WIDS.

Objectives: The objectives of this challenge are to explain WIDS.

Example

```
> enable
# config t
(config)# int bv11
(config-if)# ip address 208.1.7.8 255.255.255.224
(config-if)# int d0
(config-if)# st ?
    non-root          Non-root (bridge)
    repeater          Repeater access point
    root              Root access point or bridge
    scanner           Scanner access point
    workgroup-bridge Workgroup Bridge
(config-if)# station scanner
(config-if)# monitor ?
    frames Monitor dot11 frames

(config-if)# monitor frames ?
    endpoint endpoint station where the captured traffic is

(config-if)# monitor frames endpoint ?
    ip IP address

(config-if)# monitor frames endpoint ip ?
    address IP address

(config-if)# monitor frames endpoint ip address ?
    A.B.C.D Destination IP Address xxx.xxx.xxx.xxx

(config-if)# monitor frames endpoint ip address 10.0.0.1 ?
    port UDP port number

(config-if)# monitor frames endpoint ip address 10.0.0.1 port ?
    <1024-65535> Destination UDP port number 1024 to 65535

(config-if)# monitor frames endpoint ip address 10.0.0.1 port 1111
(config-if)# exit
(config)# wlccp ?
    ap                  Enable WLCCP AP
    authentication-server Authentication Server
    wds                 Enable Wireless Domain Service Manager
    wnm                 Configure Wireless Network Manager
(config)# wlccp ap ?
    username Specify the AP's WLCCP username
    wds        IP address of WDS

(config)# wlccp au ?
    client          For Clients
    infrastructure For Infrastructure Nodes

(config)# wlccp wd ?
    aaa            Authentication, Authorization, and Accounting
    interface      Interface to send WDS Adv
    priority        Priority of WDS
    recovery        WDS Graceful Recovery
    statistics      Roaming statistics
```

```
(config)# wlccp wn ?
ip IP configuration commands
```

Explanation

The scanner mode is used in WIDS where the access point listens on all of the radio channels and reports activity. As it is used as a WIDS, it does not accept any associations. The monitor command can then be used to forward all of the data packets received to a specific address on a certain port, such as for 10.0.0.1 on UDP port 1111 :

```
(config-if)# monitor frames endpoint ip address 10.0.0.1 port 1111
```

To show the captured packets:

```
# sh wl ap rm monitor stat
Dot11Radio0
=====
WLAN Monitoring           : Enabled
Endpoint IP address      : 10.0.0.1
Endpoint port            : 1111
Frame Truncation Length  : 128 bytes

Dot11Radio1
=====
WLAN Monitoring           : Disabled

WLAN Monitor Statistics
=====
Total No. of frames rx by DOT11 driver      : 0
Total No. of Dot11 no buffers               : 0
Total No. of Frames Q Failed                : 0
Current No. of frames in SCAN Q             : 0

Total No. of frames captured                 : 0
Total No. of data frames captured            : 0
Total No. of control frames captured         : 0
Total No. of Mgmt frames captured           : 0
Total No. of CRC errored frames captured     : 0

Total No. of UDP packets forwarded           : 0
Total No. of UDP packets forward failed     : 0
```

and to clear the statistics:

```
# clear wlccp ap rm statistics
```

Wireless Shutdown Explained

Outline: This challenge involves an analysis of wireless shutdown.

Objectives: The objectives of this challenge are to explain wireless shutdown.

Example

```
> enable
# config t
(config)# int bvi1
(config-if)# ip address 208.1.7.8 255.255.255.224
(config-if)# int d0
(config-if)# station root fallback shutdown
```

Explanation

A major problem occurs when the Ethernet/Radio port fails, and in some situations the radio port of the access-point should shutdown. The following shuts down the D0 port when the Ethernet connection fails:

```
(config-if)# station ?
non-root          Non-root (bridge)
repeater          Repeater access point
root              Root access point or bridge
scanner           Scanner access point
workgroup-bridge Workgroup Bridge
(config-if)# station root ?
access-point      Access point
ap-only           Bridge root in access point only mode
bridge            Bridge root (without wireless client)
fallback          Root AP action if Ethernet port fails
(config-if)# station root fallback ?
repeater          Become a repeater
shutdown          Shutdown the radio
(config-if)# station root fallback shutdown
```

Web Server Explained

Outline: This challenge involves an analysis of the Web server.

Objectives: The objectives of this challenge are to explain the Web server.

Explanation

By default the Web server is not enabled. To enable it:

```
# config t
(config)# int bvi1
(config-if)# ip address 10.0.0.1 255.255.255.0
(config-if)# exit
(config)# ip http server
```

By default the Web page is then accessed by the client with (<http://10.0.0.1>):

... graphic missed out on version see help file.

Sometimes another port is used, such as 8080 with:

```
(config)# ip http port 8080
```

which is accessed with (http://10.0.0.1:8080):

... graphic missed out on version see help file.

The details are then displayed with:

```
# sh ip http server all
HTTP server status: Enabled
HTTP server port: 8080
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path: flash:/c1200-k9w7-mx.123-8.JA/html/level/1;zflash:/c1200-
k9w7-mx.123-8.JA/html/level/1;flash:/c1200-k9w7-
mx.123-8.JA/html/level/15;zflash:/c1200-k9w7-mx.123-8.JA/html/level/15;flash:/c1200-
k9w7-mx.123-8.JA/html;zflash:/c1200-k9w7-mx.123-8.JA/html;flash:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 120 seconds
Server life time-out: 120 seconds
Maximum number of requests allowed on a connection: 60
HTTP secure server capability: Present
HTTP secure server status: Disabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-128-sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
```

```
HTTP server application session modules:
  Session module Name  Handle  Description
Homepage_Server       3       IOS Homepage Server
HTTP_IFS_Server       1       HTTP based IOS File Server
WEB_EXEC              2       HTTP based IOS EXEC Server
tti-petitioner        4       TTI Petitioner
```

```
HTTP server current connections:
local-ipaddress:port  remote-ipaddress:port  in-bytes  out-bytes
10.0.0.1:8080        10.0.0.2:4066         5197      50720
```

```
HTTP server statistics:
Accepted connections total: 10
```

```
HTTP server history:
local-ipaddress:port  remote-ipaddress:port  in-bytes  out-bytes  end-time
10.0.0.1:80          10.0.0.2:4046         396       192        00:00:46 03/01
10.0.0.1:80          10.0.0.2:4047         427       192        00:00:52 03/01
10.0.0.1:80          10.0.0.2:4049         5352      52152     00:01:59 03/01
10.0.0.1:80          10.0.0.2:4048         4885      85094     00:02:04 03/01
10.0.0.1:80          10.0.0.2:4051         396       192        00:25:23 03/01
10.0.0.1:80          10.0.0.2:4052         4878      86257     00:26:30 03/01
```

```

10.0.0.1:80          10.0.0.2:4053  5041          50737          00:26:35 03/01
10.0.0.1:8080       10.0.0.2:4064  401           192            00:47:16 03/01
10.0.0.1:8080       10.0.0.2:4065  4343          85878          00:48:21 03/01

```

```
# sh ip http server conn
```

```
HTTP server current connections:
```

```
local-ipaddress:port  remote-ipaddress:port  in-bytes  out-bytes
```

```
ap# sh ip http server conn
```

```

all          HTTP server all information
connection   HTTP server connection information
history      HTTP server history information
secure       HTTP secure server status information
session-module HTTP server application session module information
statistics   HTTP server statistics information
status       HTTP server status information

```

```
ap# sh ip http server status
```

```

HTTP server status: Enabled
HTTP server port: 8080
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path: flash:/c1200-k9w7-mx.123-8.JA/html/level/1;zflash:/c1200-
k9w7-mx.123-8.JA/html/level/1;flash:/c1200-k9w7-
mx.123-8.JA/html/level/15;zflash:/c1200-k9w7-mx.123-8.JA/html/level/15;flash:/c1200-
k9w7-mx.123-8.JA/html;zflash:/c1200-k9w7-mx.123-8.JA/html;flash:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 120 seconds
Server life time-outs: 120 seconds
Maximum number of requests allowed on a connection: 60
HTTP secure server capability: Present
HTTP secure server status: Disabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-edc-cbc-sha des-cbc-sha rc4-128-md5 rc4-128-sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:

```

Secure Web Server Explained

Outline: This challenge involves an analysis of a secure Web server.

Objectives: The objectives of this challenge are to explain the secure Web server.

Explanation

Unfortunately Web servers do not use encrypted data, thus they are a security risk, where intruders could detect information in the data packets for the transmission of the Web page from the device to a client. An improved method is to use a secure HTTP protocol such as HTTPS. The configuration is thus:

```

# config t
(config)# int bvi1
(config-if)# ip address 10.0.0.1 255.255.255.0

```

```

(config-if)# exit
(config)# ip http secure-server
% Generating 1024 bit RSA keys ...[OK]
(config)# ip http secure-port ?
    <0-65535> Secure port number(above 1024 or default 443)
(config)# ip http secure-port 443

```

By default the Web page is then accessed by the client with (<https://10.0.0.1>), afterwhich the client responds with:

... graphic missed out on version see help file.

and then (the password is the default enable password):

... graphic missed out on version see help file.

and then:

... graphic missed out on version see help file.

The data transferred between the client and server will then be encrypted. To verify the details:

```

ap#sh ip http server status
HTTP server status: Enabled
HTTP server port: 80
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path: flash:/c1200-k9w7-mx.123-8.JA/html/level/1;zflash:/c1200-
k9w7-mx.123-8.JA/html/level/1;flash:/c1200-k9w7-
mx.123-8.JA/html/level/15;zflash:/c1200-k9w7-mx.123-8.JA/html/level/15;flash:/c1200-
k9w7-mx.123-8.JA/html;zflash:/c1200-k9w7-mx.123-8.JA/html;flash:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 120 seconds
Server life time-out: 120 seconds
Maximum number of requests allowed on a connection: 60
HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-128-sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:

```

```

ap#sh ip http server conn

HTTP server current connections:
local-ipaddress:port  remote-ipaddress:port  in-bytes  out-bytes
      10.0.0.1:443           10.0.0.2:1082    266       52587
      10.0.0.1:443           10.0.0.2:1083    2493      67032

```

```

ap#sho ip http server secure status
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-128-sha
HTTP secure server client authentication: Disabled

```

HTTP secure server trustpoint:

User Priority Explained

Outline: This challenge involves an analysis of QoS..

Objectives: The objectives of this challenge are to explain QoS.

Explanation

The Aironet advertise their QoS parameters so that WLAN clients which require a certain QoS requirement can use these advertisements to associate with the required access-point. The traffic-stream command is used to configure the radio interface for the CAC (Call Admission Control – used in Voice over Wireless) traffic stream properties. The Aironet support traffic streams, such as:

```
ap# config t
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)# int d0
ap(config-if)#traffic-stream ?
    priority  Apply to Priority

ap(config-if)# traffic-stream pri ?
    <0-7>  UP Value
```

where the UP (user priority) is defined as:

- 0 (Best Effort)
- 1 (Background)
- 2 (Spare)
- 3 (Excellent)
- 4 (Controlled Load)
- 5 (Video)
- 6 (Voice)
- 7 (Network Control)

```
ap(config-if)# traffic-stream pri 0 ?
    sta-rates  Set rates to allow for traffic-stream
ap(config-if)# traffic-stream pri 0 sta ?
    1.0        Allow 1 Mb/s rate
    11.0       Allow 11 Mb/s rate
    12.0       Allow 12 Mb/s rate
    18.0       Allow 18 Mb/s rate
    2.0        Allow 2 Mb/s rate
    24.0       Allow 24 Mb/s rate
    36.0       Allow 36 Mb/s rate
    48.0       Allow 48 Mb/s rate
    5.5        Allow 5.5 Mb/s rate
    54.0       Allow 54 Mb/s rate
    6.0        Allow 6 Mb/s rate
```

```

9.0      Allow 9  Mb/s rate
nom-1.0  Allow Nominal 1 Mb/s rate
nom-11.0 Allow Nominal 11 Mb/s rate
nom-12.0 Allow Nominal 12 Mb/s rate
nom-18.0 Allow Nominal 18 Mb/s rate
nom-2.0  Allow Nominal 2 Mb/s rate
nom-24.0 Allow Nominal 24 Mb/s rate
nom-36.0 Allow Nominal 36 Mb/s rate
nom-48.0 Allow Nominal 48 Mb/s rate
nom-5.5  Allow Nominal 5.5 Mb/s rate
nom-54.0 Allow Nominal 54 Mb/s rate
nom-6.0  Allow Nominal 6 Mb/s rate
ap(config-if)#traffic-stream pri 0 sta 1.0

```

Thus the best effort for this access point is a rate of 1.0Mbps. If this was advertised to client, they would choice if this was the best rate for the best effort.

SSH Explained

Outline: This challenge involves an analysis of SSH.

Objectives: The objectives of this challenge are to explain SSH.

Explanation

The TELNET protocol is insecure as the text is passed as plain text. An improved method is to use SSH, which encrypts data. It requires that the domain-name and an RSA key pair:

```

ap# config t
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)# ip domain-name test.com
ap(config)# crypto key generate rsa
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]

```

To view the public key:

```

ap#show crypto key mypubkey rsa
% Key pair was generated at: 00:42:19 UTC Mar 1 2002
Key name: ap.test.com
Usage: General Purpose Key
Key is not exportable.
Key Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DDD8C6 4B744520
 F1499B01 49C485A2 20C9FB37 8CD11053 039D344B 3C5BD55E E84E17C8 FD62DA08
 32020F80 910AFBCC 6D402F90 96E8A59B 40467A3E 8FEED18B B1020301 0001
% Key pair was generated at: 00:42:21 UTC Mar 1 2002
Key name: ap.test.com.server
Usage: Encryption Key
Key is not exportable.
Key Data:
 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00B435A4 C007251B
 312319CA 0E919F76 72D2D5A9 36B4710C CC4DE0C4 080D2B47 55970CA5 39F21170
 D07C0000 832F6A1C 81411423 BE52CBF4 ECBE417E 1C3C09D1 2BBC90DF 8DA398DB

```

```
AE8EFA46 282AEC54 F0909F82 466A19DD EBEFAEDE 7B4B992F 5F020301 0001
```

An SSH client such as putty can then be used to connect to the access point:

... graphic missed out on version see help file.

after which the client shows the message:

... graphic missed out on version see help file.

and the SSH connection is made, such as:

... graphic missed out on version see help file.

To get rid of keys:

```
ap(config)# crypto key zero
```

and to set the timeout and authentication retries:

```
ap(config)# ip ssh time-out 60
ap(config)# ip ssh authentication-retries 2
```

which sets the timeout to 60 seconds, and a maximum of two retries. Finally, to prevent Telnet sessions:

```
ap(config)#line vty 0 4
ap(config-line)# transport input ssh
```

LEAP Explained

Outline: This challenge involves an analysis of LEAP.

Objectives: The objectives of this challenge are to explain LEAP.

Explanation

The following uses a local RADIUS server to authenticate using LEAP authentication:

```
(config)# hostname ap
(config)# aaa new-model
(config)# int bv11
(config-if)# ip address 192.168.1.110 255.255.255.0
(config-if)# exit
(config)# dot11 ssid APskills
```

```

(config-ssid)# authentication network-eap eap_methods
(config-ssid)# guest-mode
(config-ssid)# exit
(config)# radius-server local
(config-radsrv)# nas 192.168.1.110 key sharedkey
(config-radsrv)# user aaauser password aaauser
(config-radsrv)# exit
(config)#radius-server host 192.168.1.110 auth 1812 acct 1813 key sharedkey
(config-if)interface d0
(config-if) channel 11
(config-if) station-role root
(config-if) encryption key 1 size 40bit aaaaaaaaaa transmit-key
(config-if) encryption mode ciphers tkip wep40
(config-if) ssid APskills

```

In this case the user login for LEAP will be **aaauser** with a password of **aaauser**. Notice that the NAS is set to the local IP address, and that the Radius server is set also as the local IP address.

Notice also that the shared key (in this case named **sharedkey**) must be set the same for the NAS and the Radius server.

Next setup the clients to support LEAP authentication, as shown in Figure 1. Once the client has associated, determine the associated devices with:

```

# show dot assoc

802.11 Client Stations on Dot11Radio0:
SSID [APskills] :

MAC Address      IP address      Device          Name      Parent      State
0090.4b54.d83a  192.168.1.111  4500-radio     -        self       EAP-Assoc

Others:  (not related to any ssid)

```

... graphic missed out on version see help file.

Figure 1: LEAP setup

After which the WAP will display a message such as the following on a successful association:

```

*Mar 1 00:00:51.750: %DOT11-6-ASSOC: Interface Dot11Radio0, Station 0090.4b54.d83a
Associated KEY_MGMT[WPA]

```

D0 Encapsulation

Outline: This challenge involves setting up the encapsulation on D0.

Objectives: The objectives of this challenge are to outline encapsulation on D0.

Explanation

The following sets up SNAP encapsulation on D0:

```
(config)# hostname ap
(config)# aaa new-model
(config)# int bv11
(config-if)# ip address 192.168.1.110 255.255.255.0
(config-if)# exit
(config)# dot11 ssid APskills
(config-ssid)# authentication open
(config-ssid)# exit
(config-if)interface d0
(config-if) channel 11
(config-if) encapsulation snap
(config-if) ssid APskills
```

Command Filtering Explained

Outline: This challenge involves filtering the output of the show command.

Objectives: The objectives of this challenge are to outline the usage of the filtering of the output in the show command.

Explanation

The filtering output includes:

```
show "command" | include "word" this finds all lines with "word"
show "command" | begin "word"      this finds all lines which begin with "word"
show "command" | exclude "word" this finds all lines without "word"
```

An example is:

```
# show running | include udp
# show running | include tcp
# show running | include !
# show running | begin version
# show running | exclude int
```

Command Filtering Explained

Outline: This challenge involves filtering the output of the show command.

Objectives: The objectives of this challenge are to outline the usage of the filtering of the output in the show command.

Explanation

The filtering output includes:

```
show "command" | include "word" this finds all lines with "word"  
show "command" | begin "word"      this finds all lines which begin with "word"  
show "command" | exclude "word" this finds all lines without "word"
```

An example is:

```
# show version | include cisco  
# show version | include product  
# show version | include ver  
# show version | begin power  
# show version | exclude pca
```

Public Secure Packet Forwarding (PSPF) Explained

Outline: This challenge involves enabling PSPF.

Objectives: The objectives of this challenge are to outline the usage of PSPF.

Explanation

Public Secure Packet Forwarding (PSPF) is used to prevent clients from associating with an access point and inadvertently communicating with other clients which are associated to the access point. It thus allows the clients to connect to the Internet, without being part of the local network. Often this facility is used in public wireless networks, such as on university campuses.

An example is:

```
# config t  
(config)# int d0
```

```

(config-if)# bridge-port 1 ?
<cr>
circuit-group          Associate serial interface with a circuit group
input-address-list     Filter packets by source address
input-lat-service-deny Deny input LAT service advertisements matching a
                       group list
input-lat-service-permit Permit input LAT service advertisements matching a
                       group list
input-lsap-list        Filter incoming IEEE 802.3 encapsulated packets
input-type-list       Filter incoming Ethernet packets by type code
lat-compression        Enable LAT compression over serial or ATM
                       interfaces
output-address-list    Filter packets by destination address
output-lat-service-deny Deny output LAT service advertisements matching a
                       group list
output-lat-service-permit Permit output LAT service advertisements matching
                       a group list
output-lsap-list       Filter outgoing IEEE 802.3 encapsulated packets
output-type-list       Filter outgoing Ethernet packets by type code
port-protected         There will be no traffic between this interface
                       and other protected
subscriber-loop-control Configure subscriber loop control
                       port interface in this bridge group
block-unknown-source   block traffic which come from unknown source MAC
                       address
input-pattern-list     Filter input with a pattern list
output-pattern-list    Filter output with a pattern list
path-cost              Set interface path cost
priority              Set interface priority
source-learning        learn source MAC address
spanning-disabled     Disable spanning tree on a bridge group
unicast-flooding       flood packets with unknown unicast destination MAC
                       addresses
(config-if)# bridge-group 1 port-protected

```

Multiple Basic SSIDs (MBSSID) Explained

Outline: This challenge involves setting up MBSSID.

Objectives: The objectives of this challenge are to outline the usage of PSPF.

Explanation

Up to eight basic SSIDs (BSSIDs) can be assigned, and are similar to MAC addresses. This allows MBSSIDs to assign a DTIM setting for each SSID, and then to broadcast multiple SSIDs in a single beacon message. Using MBSSID makes the access-point more accessible to guests.

An example is:

```
# config t
(config)# dot11 ssid fred
(config-ssid)# mbssid guest-mode dtim 10
(config-ssid)# exit
(config)# int d0
(config-if)# mbssid
```

Note:

Large DTIM values are useful for increasing the battery life for power-save client devices.

Cisco Wireless Challenge 64 (Test)

Outline

This is an intermediate test, which revises some of the main principles of Wireless configuration.

Cisco Wireless Challenge 65 (Test)

Outline

This is an intermediate test, which revises some of the main principles of Wireless configuration.

SSID Redirection Explained

Outline: This challenge involves defining SSID redirection.

Objectives: The objectives of this challenge are to outline the usage of SSID redirection.

Explanation

With IP redirection on an SSID, all the packets from clients are sent to a specific IP address. This is typically used in applications which use handhelds, where specific software is used to handle the data packets. For example an SSID might be HANDHELDS, which handheld scanners connect to. When redirection is used on this SSID, all the data packets will be set to the specified IP address, where software can be setup to handle this. It is also possible to redirect on specific types of traffic, but this requires ACLs.

An example is:

```
# config t
(config)# dot11 ssid fred
(config-ssid)# ip ?
    redirection Redirect client data to alternate IP address
(config-ssid)# ip redirection ?
    host Destination host to forward data
(config-ssid)# ip redirection host ?
    A.B.C.D IP redirect destination host address
(config-ssid)# ip redirection host 192.168.1.1
(config-ssid)# exit
```

SSID Redirection with ACL Explained

Outline: This challenge involves defining SSID redirection with ACLs.

Objectives: The objectives of this challenge are to outline the usage of SSID redirection with ACLs.

Explanation

With IP redirection on an SSID, all the packets from clients are sent to a specific IP address. This is typically used in applications which use handhelds, where specific software is used to handle the data packets. For example an SSID might be HANDHELDS, which handheld scanners connect to. When redirection is used on this SSID, all the data packets will be set to the specified IP address, where software can be setup to handle this. It is also possible to redirect on specific types of traffic, which requires the setup of an ACL which defines the traffic which will be redirected. **Note: All other traffic that isn't redirected will be dropped!**

An example is:

```
# config t
(config)# access-list 1 permit 10.0.0.0 0.0.0.255
(config)# dot11 ssid fred
(config-ssid)# ip ?
    redirection Redirect client data to alternate IP address
(config-ssid)# ip redirection ?
    host Destination host to forward data
(config-ssid)# ip redirection host ?
    A.B.C.D IP redirect destination host address
(config-ssid)# ip red host 1.2.3.4 ?
    access-group Optional group access-list to apply
    <cr>
(config-ssid)# ip red host 1.2.3.4 access-group ?
    WORD Access-list number or name
```

```
(config-ssid)#ip red host 1.2.3.4 access-group 1 ?
  in Apply to input interface
(config-ssid)#ip red host 1.2.3.4 access-group 1 in ?
  <cr>
(config-ssid)#ip red host 1.2.3.4 access-group 1 in
(config-ssid)# exit
```

SSID in an SSIDL IE Explained

Outline: This challenge involves using an SSID in an SSIDL IE (Information-element).

Objectives: The objectives of this challenge are to outline the usage of an SSID in an SSIDL IE.

Explanation

There is only one broadcast SSID contained within a beacon from the access point. An SSIDL information elements (SSIDL IEs) is contained within the beacon and can contain additional SSIDs, thus clients can detect other SSIDs, along with the security settings for that SSID.

An example is:

```
# config t
(config)# dot11 ssid fred
(config-ssid)# information-element ssidl ?
  advertisement include SSID name in SSIDL IE
  wps advertise WPS capability in SSID IE
  <cr>
(config-ssid)# information-element ssidl advertisement
(config-ssid)# exit
```

VLAN Encryption Explained

Outline: This challenge involves using an encryption key for a VLAN.

Objectives: The objectives of this challenge to use an encryption key for a VLAN.

Explanation

An encryption key can be set for each VLAN, so that the traffic is encrypted over the interconnected ports of the VLAN. Up to four keys can be defined for the encryption key. An example is:

```
# config t
(config)# dot11 ssid fred
(config-ssid)# vlan 22
(config-ssid)# exit
(config)# int d0
(config-if)# encryption vlan 22 key 1 size 40 aaaaaaaaaa
```

which defines a 40-bit encryption key of aaaaaaaaaa (which is a hexadecimal value). The other option is for a 128-bit key which has 32 hexadecimal digits. In this case the interface is assigned to VLAN 22, so that all the other nodes in this VLAN will receive broadcasts from a node in the VLAN.

VLAN Encryption Explained

Outline: This challenge involves using an encryption key for a VLAN.

Objectives: The objectives of this challenge to use an encryption mode for a VLAN.

Explanation

An encryption key can be set for each VLAN, so that the traffic is encrypted over the interconnected ports of the VLAN. Most hosts now use WPA as it allows for TKIP encryption. WEP suffers from many security problems, but TKIP overcomes most of these, and is still compatible with most currently available IEEE 802.11 wireless interfaces. The CKIP and CMIC are Cisco-derived methods, and sometimes lack compatibility. An example for WPA using TKIP is:

```
# config t
(config)# dot11 ssid fred
(config-ssid)# vlan 22
(config-ssid)# exit
(config)# int d0
(config-if)# ssid fred
(config-if)# encryption vlan 22 mode cipers tkip
```

The two main cipher suites for authenticated key management:

CCKM (Cisco Centralized Key Management). This uses either:

- wep128
- wep40
- ckip
- cmic
- ckip-cmic
- tkip

WPA. This uses either:

- tkip
- tkip wep128
- tkip wep40

VLAN Broadcast-key Explained

Outline: This challenge involves defining the change time for the broadcast key.

Objectives: The objectives of this challenge to change the time for the broadcast key.

Explanation

The broadcast key rotation allows for a new key to be broadcast to the network. It is disabled by default. It is used with 802.1x authentication, such as with LEAP, EAP-TLS, or PEAP). The broadcast-key is change time is defined with:

```
# config t
(config)# dot11 ssid fred
(config-ssid)# vlan 22
(config-ssid)# exit
(config)# int d0
(config-if)# ssid fred
(config-if)# broadcast-key vlan 22 change 100
```

which enables the broadcast-key on VLAN 22, and defines that the broadcast key is changed every 100 seconds.

Authentication based on MAC-address Explained

Outline: This challenge involves defining authentication based on MAC addresses.

Explanation

```
# config t
(config)# dot11 ssid fred
(config-ssid)# authentication open mac-address maclist
(config-ssid)# exit
(config)# aaa new-model
(config)# aaa authentication login maclist group radius
```

WPA-PSK Explained

Outline: This challenge involves defining the pres shared key for WPA-PSK.

Explanation

Unfortunately, WEP suffers from many problems, and should not be used for sensitive data. An improvement which keeps compatibility with WEP is TKIP. One method is WPA-PSK (Pre-shared key), where the users defines a pre-share key, which is setup on both the access point and the client. An example setup of the WPA-PSK on a Linksys access point (Figure 1) is shown, and on a client (Figure 2) with the same shared key of **napieruniversity**.

```
> enable
# config t
(config)# dot11 ssid texas
(config-ssid)# wpa-psk ascii napieruniversity
(config-ssid)# exit
(config)# int d0
(config-if)# ssid texas
```

diagram not included in this version

Figure 1: WPA-PSK (Linksys configuration)

diagram not included in this version

Figure 2: WPA-PSK (client)

Authentication Holdtimes Explained

Outline: This challenge involves defining the timeouts for authentication.

Explanation

An example is

```
> enable
# config t
(config)# dot11 holdoff-time 15
(config)# dot1x timeout supp-response 10
(config)# int d0
(config-if)# dot1x reauth-period 10
(config-if)# countermeasure tkip hold-time
```

where:

```
(config)# dot11 holdoff-time x
```

This is the time that a client device must wait before it can reattempt to authenticate, after it has failed an authentication. This occurs when the client device fails three logins or does not reply to three authentication requests. 1-65,545 seconds.

```
(config)# dot1x timeout supp-response 10
```

This is the time that the access point waits for a reply to an EAP/dot1x message from a client before the authentication is failed.

```
(config-if)# dot1x reauth-period 10
```

This is the time that the access point waits before it asks the client to reauthenticate itself.

```
(config-if)# countermeasure tkip hold-time
```

This defines the TKIP MIC failure holdtime, and is caused when the access point detects two MIC failures in a period of 60 seconds. It will then, for the holdtime period, blocks all TKIP clients on the interface.

WLCCP Explained

Outline: This challenge involves defining WLCCP (Wireless LAN Context Communication Protocol).

Explanation

In large campus area networks, it is important that mobile nodes are able to migrate from one access point to another. If possible they must hand the current context from one access point to the other.

WLCCP establishes and manages wireless network topologies in a SWAN (Smart Wireless Architecture for Networking). It securely manages an *operational context* for mobile clients, typically in a campus-type network. In the registration phase, it can automatically create and delete network link, and securely distribute operational context, typically with Layer 2 forwarding paths.

With WLCCP, a sole infrastructure node is defined as the central control point within each subnet, and allows access points and mobile nodes to select a parent node for a *least-cost path* to the backbone connection. An example is

```
> enable
# config t
(config)# aaa new-model
```

```
(config)# aaa authentication login testi group radius
(config)# aaa authentication login testc group radius

(config)# wlccp wds priority 200 interface bv11
(config)# wlccp authentication-server infrastructure testi
(config)# wlccp authentication-server client any testc
(config-wlccp-auth)# ssid testing
```

which defines that the authentication of infrastructure devices is done using the server group testi, and that client devices using the testing SSID are authenticated using the server group of testc.

Cisco Wireless Test

Outline

This challenge involves taking a Wireless test.

Cisco Wireless Challenge 77

Outline

This challenge involves the configuration of TACACS+ accounting and authentication for the Aironet.

Objectives

The objectives of this challenge are to:

- Define a host name.
- Define AAA.
- Define Tacacs+ account for network and exec.

The commands used are:

```
> en
# config t
(config)# hostname test
(config)# aaa new-model
(config)# tacacs-server host 39.100.234.1
(config)# tacacs-server key krinkle
(config)# aaa authentication login default group tacacs
(config)# aaa authentication ppp default group tacacs
(config)# aaa authorization network default group tacacs
(config)# aaa authorization exec default group tacacs
(config)# aaa authorization exec default group tacacs
```

```
(config)# aaa accounting exec default start-stop group tacacs+
(config)# aaa accounting network default start-stop group tacacs+
```

Example

```
> en
# config t
(config)# hostname test
(config)# aaa new-model
(config)# tacacs-server ?
  administration    Start tacacs+ daemon handling administrative messages
  cache             AAA auth cache default server group
  directed-request  Allow user to specify tacacs server to use with '@server'
  dns-alias-lookup Enable IP Domain Name System Alias lookup for TACACS
                   servers
  host              Specify a TACACS server
  key               Set TACACS+ encryption key.
  packet           Modify TACACS+ packet options
  timeout          Time to wait for a TACACS server to reply
(config)# tacacs-server host ?
  Hostname or A.B.C.D IP address of TACACS server
  <cr>
(config)# tacacs-server host 39.100.234.1
ap(config)# tacacs-server key ?
  0      Specifies an UNENCRYPTED key will follow
  7      Specifies HIDDEN key will follow
  LINE   The UNENCRYPTED (cleartext) shared key
(config)# tacacs-server key crinkle
(config)# aaa authentication ?
  arap          Set authentication lists for arap.
  attempts     Set the maximum number of authentication attempts
  banner       Message to use when starting login/authentication.
  dot1x        Set authentication lists for IEEE 802.1x.
  enable       Set authentication list for enable.
  eou          Set authentication lists for EAPoUDP
  fail-message Message to use for failed login/authentication.
  login        Set authentication lists for logins.
  password-prompt Text to use when prompting for a password
  ppp          Set authentication lists for ppp.
  sgbp        Set authentication lists for sgbp.
  username-prompt Text to use when prompting for a username
(config)# aaa authentication login ?
  WORD        Named authentication list.
  default     The default authentication list.

(config)# aaa authentication login default ?
  cache      Use Cached-group
  enable     Use enable password for authentication.
  group      Use Server-group
  line       Use line password for authentication.
  local      Use local username authentication.
  local-case Use case-sensitive local username authentication.
  none       NO authentication.

(config)# aaa authentication login default group ?
  WORD        Server-group name
```

```

radius    Use list of all Radius hosts.
tacacs+   Use list of all Tacacs+ hosts.
(config)# aaa authentication login default group tacacs
(config)# aaa authentication ppp default group tacacs

(config)# aaa authorization ?
auth-proxy    For Authentication Proxy Services
cache         For AAA cache configuration
commands     For exec (shell) commands.
config-commands For configuration mode commands.
configuration For downloading configurations from AAA server
console       For enabling console authorization
exec          For starting an exec (shell).
network       For network services. (PPP, SLIP, ARAP)
reverse-access For reverse access connections
template      Enable template authorization

(config)# aaa authorization network ?
WORD         Named authorization list.
default      The default authorization list.

(config)# aaa author n d ?
cache        Use Cached-group
group        Use server-group.
if-authenticated Succeed if user has authenticated.
local        Use local database.
none         No authorization (always succeeds).

(config)# aaa author n d g ?
WORD         Server-group name
radius       Use list of all Radius hosts.
tacacs+     Use list of all Tacacs+ hosts.

(config)# aaa authorization network default group tacacs
(config)# aaa authorization exec default group tacacs
(config)# aaa authorization exec default group tacacs

(config)# aaa accounting ?
auth-proxy    For authentication proxy events.
commands     For exec (shell) commands.
connection    For outbound connections. (telnet, rlogin)
delay-start   Delay PPP Network start record until peer IP address is
              known.
exec          For starting an exec (shell).
gigawords     64 bit interface counters to support Radius attributes 52 &
              53.
nested        When starting PPP from EXEC, generate NETWORK records
              before EXEC-STOP record.
network       For network services. (PPP, SLIP, ARAP)
resource      For resource events.
send          Send records to accounting server.
session-duration Set the preference for calculating session durations
suppress      Do not generate accounting records for a specific type of
              user.
system        For system events.
update        Enable accounting update records.
(config)# aaa accounting exec ?

```

```

WORD      Named Accounting list.
default   The default accounting list.

(config)# aaa accounting exec default ?
none      No accounting.
start-stop Record start and stop without waiting
stop-only Record stop when service terminates.

(config)# aaa accounting exec default start-stop ?
broadcast Use Broadcast for Accounting
group      Use Server-group

(config)# aaa accounting exec default sta group ?
WORD      Server-group name
radius    Use list of all Radius hosts.
tacacs+   Use list of all Tacacs+ hosts.

(config)# aaa accounting exec default start-stop group tacacs+

(config)# aaa accounting net ?
WORD      Named Accounting list.
default   The default accounting list.

(config)# aaa accounting network default ?
none      No accounting.
start-stop Record start and stop without waiting
stop-only Record stop when service terminates.

(config)# aaa accounting network default start-stop ?
broadcast Use Broadcast for Accounting
group      Use Server-group

(config)# aaa accounting exec default group ?
WORD      Server-group name
radius    Use list of all Radius hosts.
tacacs+   Use list of all Tacacs+ hosts.

(config)# aaa accounting network default start-stop group tacacs+

```

Cisco Wireless Challenge 78

Outline

This challenge involves the configuration of multiple SSIDs.

Objectives

The objectives of this challenge are to:

- Create multiple SSIDs.

The commands used are:

```
> en
# config t
(config)# dot11 ssid network1
(config-ssid)# mbssid guest-mode
(config-ssid)# exit
# config t
(config)# dot11 ssid network2
(config-ssid)# exit
# config t
(config)# dot11 ssid network3
(config-ssid)# exit

(config)# int d0
(config-if)# mbssid
(config-if)# ssid network1
(config-if)# ssid network2
(config-if)# ssid network3
```

Example

```
> en
# config t
(config)# dot11 ssid network1
(config-ssid)# mbssid guest-mode
(config-ssid)# exit
# config t
(config)# dot11 ssid network2
(config-ssid)# exit
# config t
(config)# dot11 ssid network3
(config-ssid)# exit

(config)# int d0
(config-if)# mbssid
(config-if)# ssid network1
(config-if)# ssid network2
(config-if)# ssid network3
```

Cisco Wireless Challenge 79

Outline

This challenge involves the configuration of multiple SSIDs which are associated with VLANs.

Objectives

The objectives of this challenge are to:

- Define sub-interfaces.
- Create VLANs.
- Define multiple SSIDs.

The commands used are:

```
> en
# config t
(config)# dot11 ssid network1
(config-ssid)# mbssid guest-mode
(config-ssid)# vlan 1
(config-ssid)# exit
# config t
(config)# dot11 ssid network2
(config-ssid)# vlan 2
(config-ssid)# exit
# config t
(config)# dot11 ssid network3
(config-ssid)# vlan 3
(config-ssid)# exit

(config)# int d0
(config-if)# mbssid
(config-if)# ssid network1
(config-if)# ssid network2
(config-if)# ssid network3

(config)# int d0.1
(config-if)# encapsulation dot1q 1 native
(config-if)# exit
(config)# int e0.1
(config-if)# encapsulation dot1q 1 native
(config-if)# exit
(config)# int d0.2
(config-if)# encapsulation dot1q 2
(config-if)# exit
(config)# int e0.2
(config-if)# encapsulation dot1q 2
(config-if)# exit
(config)# int d0.3
(config-if)# encapsulation dot1q 3
(config-if)# exit
(config)# int e0.1
(config-if)# encapsulation dot1q 3
(config-if)# exit
```

Example

```
> en
# config t
(config)# dot11 ssid network1
(config-ssid)# vlan 1
(config-ssid)# exit
```

```

# config t
(config)# dot11 ssid network2
(config-ssid)# vlan 2
(config-ssid)# exit
# config t
(config)# dot11 ssid network3
(config-ssid)# vlan 3
(config-ssid)# exit

(config)# int d0.1
(config-if)# encapsulation dot1q 1 native
(config-if)# exit
(config)# int e0.1
(config-if)# encapsulation dot1q 1 native
(config-if)# exit
(config)# int d0.2
(config-if)# encapsulation dot1q 2
(config-if)# exit
(config)# int e0.2
(config-if)# encapsulation dot1q 2
(config-if)# exit
(config)# int d0.3
(config-if)# encapsulation dot1q 3
(config-if)# exit
(config)# int e0.1
(config-if)# encapsulation dot1q 3
(config-if)# end

```

show vlan

Virtual LAN ID: 1 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interfaces: Dot11Radio0.1
Virtual-Dot11Radio0.1

This is configured as native Vlan for the following interface(s) :
Dot11Radio0
Virtual-Dot11Radio0

Protocols Configured:	Address:	Received:	Transmitted:
Bridging	Bridge Group 1	17	9
Bridging	Bridge Group 1	17	9

Virtual LAN ID: 2 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interfaces: Dot11Radio0.2
Virtual-Dot11Radio0.2

Protocols Configured:	Address:	Received:	Transmitted:
Bridging	Bridge Group 2	1	0
Bridging	Bridge Group 2	1	0

Virtual LAN ID: 3 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interfaces: Dot11Radio0.3
Virtual-Dot11Radio0.3

Protocols Configured:	Address:	Received:	Transmitted:
Bridging	Bridge Group 2	1	0
Bridging	Bridge Group 2	1	0

This assigns three VLANs. The first is allowed to the network1 SSID, the second to network2 and the third to network3.

Theory

In the following example VLAN 1 is associated to Scotland on the first Aironet, Ireland on the next, and France on the third one. Each of the nodes which connect to VLAN 1 will all be part of the same network, even though they connect to different Aironets. The same applies to VLAN 2, where nodes connecting to England, Wales and Germany, will be in the same network. The key factor is that the switch supports 802.1q which will trunk between the ports on the switch.

An example of trunking on the switch is:

```
# config t
(config)# int vlan 1
(config-vlan)# exit
(config)# int vlan 2
(config-vlan)# exit
(config)# int fa0/1
(config-if)# switchport trunk encapsulation dot1q
(config-if)# switchport trunk native vlan 1
(config-if)# switchport trunk allowed add vlan 1,2
(config-if)# switchport mode trunk
(config-if)# switchport nonegotiate
(config-if)# int fa0/2
(config-if)# switchport trunk encapsulation dot1q
(config-if)# switchport trunk native vlan 1
(config-if)# switchport trunk allowed add vlan 1,2
(config-if)# switchport mode trunk
(config-if)# switchport nonegotiate
(config-if)# int fa0/3
(config-if)# switchport trunk encapsulation dot1q
(config-if)# switchport trunk native vlan 1
(config-if)# switchport trunk allowed add vlan 1,2
(config-if)# switchport mode trunk
(config-if)# switchport nonegotiate
```

Diagram has been left-out in this version... see e-Book.

When the bridge group is added to the radio port the following are added:

```
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"
```

Cisco Wireless Challenge 80

Outline

This challenge involves defining precedence of QoS Settings. If QoS is enabled, the device then queues packets based on the Layer 2 class of service value for each packet. This can either be:

- **Packets already classified.** This is typical from a QoS-enabled device, such as a switch or router. These contain values in the 802.1P field, and take priority over all other policies.
- **QoS from Wireless Phones.** This allows wireless phone traffic to get a higher priority than other traffic. In addition, a QoS Basic Service Set (QBSS) can be enabled to advertise channel load information in the beacon and probe response frames. This can then be used by the phones to determine the best access point to associate to, such as for their traffic load.

This example shows how to enable IEEE 802.11 phone support with the legacy QBSS Load element:

```
AP(config)# dot11 phone
```

Objectives

The objectives of this challenge are to:

- Enable IEEE 802.11 phone support for the legacy QBSS load element.

The commands used are:

```
> en
# config t
(config)# dot11 phone
(config)# int d0
(config-if)# traffic-class best-effort cw-min 4 cw-max 10 fixed-slot 2
```

Example

```
> en
# config t
(config)# dot11 phone
```

```

(config)# int d0
(config-if)# traffic-control ?
0          Parameters for priority 0
1          Parameters for priority 1
2          Parameters for priority 2
3          Parameters for priority 3
4          Parameters for priority 4
5          Parameters for priority 5
6          Parameters for priority 6
7          Parameters for priority 7
background Parameters for the background access class
best-effort Parameters for the best effort access class
video      Parameters for the video access class
voice      Parameters for voice access class
(config-if)# traffic-c best-effort ?
cw-max     802.11 contention window maximum
cw-min     802.11 contention window minimum
fixed-slot 802.11 fixed backoff slot time
<cr>
(config-if)# traffic-c be cw-min ?
<0-10> CwMin will be ( 2 to the power of the entered value ) - 1

(config-if)# traffic-c best cw-min 4 ?
cw-max     802.11 contention window maximum
fixed-slot 802.11 fixed backoff slot time
<cr>

(config-if)# traffic-c best cw-min 4 cw-max ?
<0-10> CwMax will be ( 2 to the power of the entered value ) - 1

(config-if)# traffic-c best cw-min 4 cw-max 10 ?
fixed-slot 802.11 fixed backoff slot time
<cr>

(config-if)# traffic-c best cw-min 4 cw-max 10 fixed-slot ?
<0-16> 802.11 fixed backoff slot time
(config-if)# traffic-class best-effort cw-min 4 cw-max 10 fixed-slot 2

```

This configuration enables 802.11-compliant phone support and configures the best effort traffic class for contention windows and fixed-slot backoff values. In this case the backoff for best effort is started, where it waits a minimum of the 802.11 Short Inter-Frame Space time plus two backoff slots.