3 Wireless Emulator (Challenges)

3.1 Introduction

The following relates to the wireless emulator challenges.

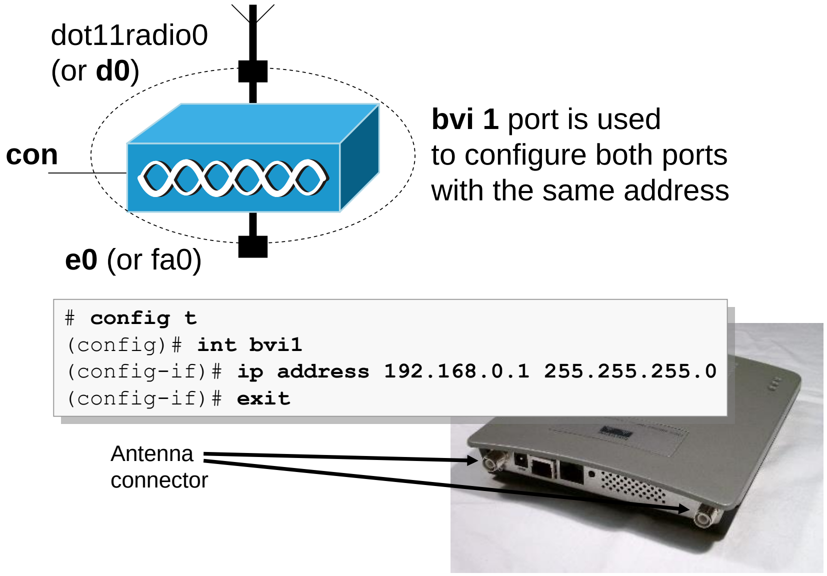
3.2 Challenge 1 (BVI 1)

The following sets up the BVI 1 port:

```
> enable
# config t
(config)# int bvi 1
(config-if)# ip address 158.234.223.7 255.192.0.0
(config-if)# description cisco
(config-if)# int e0
(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 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.



```
# config t
(config)# int bvi1
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# exit
```

Figure 1 Setting the IP address of the wireless access point

3.3 Challenge 2 (E0)

The following sets up the E0 port:

```
> enable
# config t
(config)# int bvi 1
(config-if)# ip address 158.234.223.7 255.192.0.0
(config-if)# description cisco
(config-if)# int e0
(config-if)# no shut
(config-if)# description production depart
(config-if)# speed 10
(config-if)# speed full
(config-if)# cpd enable
```

3.4 Challenge 3 (D0)

The following sets up the D0 port:

```
> 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
```

3.5 Challenge 4 (SSID and radio channel)

The following sets up the SSID and the radio channel:

```
> 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
```

Example IOS Version 12.3

```
> en
# config t
(config)# dot11 ssid minnesota
(config-ssid)# exit
(config)# int d0
(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 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.

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 1000 ms (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.

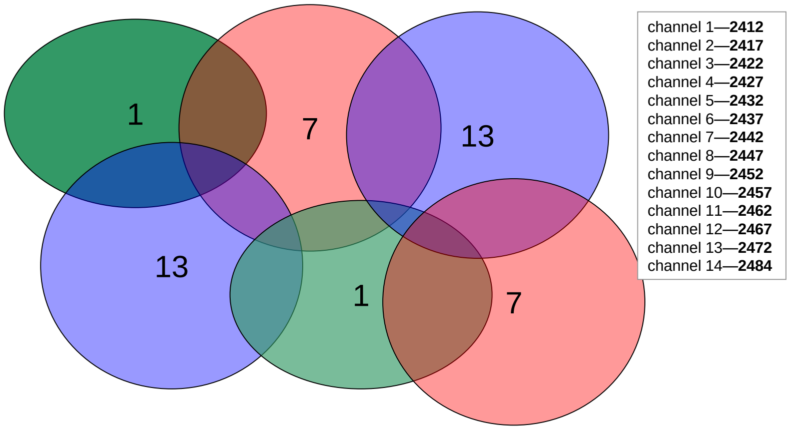


Figure 1   Channels in an area

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
```

3.6 Challenge 5

The following sets up radio port settings:

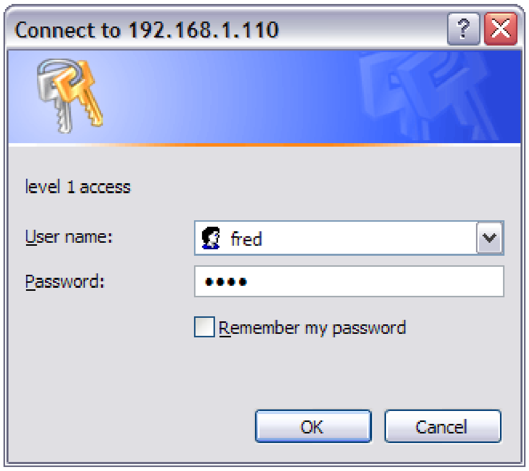
```
> en
# config t
(config)# enable ?
  last-resort  Define enable action if no TACACS servers respond
  password     Assign the privileged level password
  secret       Assign the privileged level secret
  use-tacacs   Use TACACS to check enable passwords
(config)# enable password hotel
(config)# enable secret hotel
(config)# username lynn password foxtrot
(config)# ip http server
```

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
```

This type of authentication is not the most secure but it offers a simple way to block access to the access point. Thus, when the user tries to access to the wireless access point they will not be allowed to connect, unless the have the correct username and password, such as shown in Figure 1. If the user has the correct username and password, the Web page will show the device settings (left-hand side of Figure 2), otherwise there will be an authentication failure (right-hand side of Figure 2).



Connect to 192.168.1.110

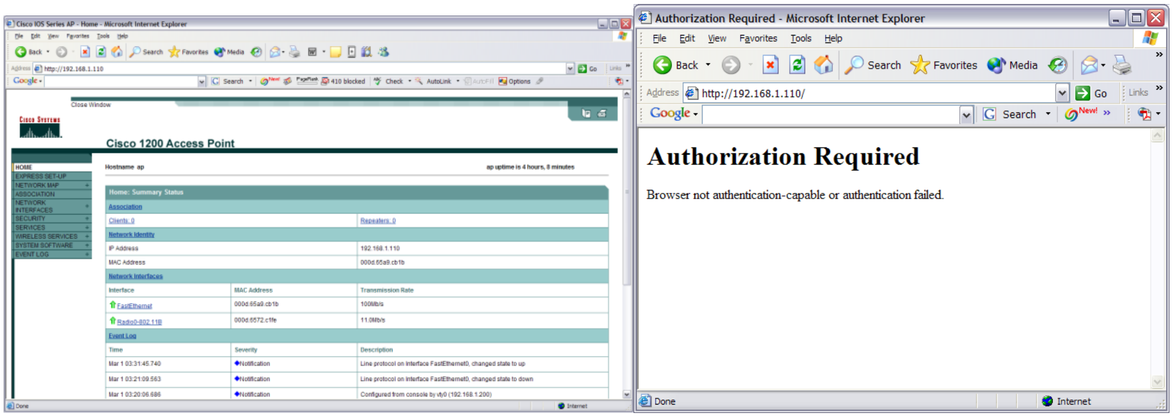
level 1 access

User name: fred

Password: ••••

□ Remember my password

Figure 1 Local authentication



Cisco IOS Series AP - Home - Microsoft Internet Explorer

Address http://192.168.1.110

Cisco 1200 Access Point

Hostname ap

ap uptime is 4 hours, 8 minutes

Home: Summary Status

Association	
Clients: 0	Repeaters: 0

Network Identity	
IP Address	192.168.1.110
MAC Address	000d.65a9.cb1b

Interface	MAC Address	Transmission Rate
FastEthernet	000d.65a9.cb1b	100Mb/s
Radio0-802.11B	000d.6572.c1fe	11.0Mb/s

Time	Severity	Description
Mar 1 03:31:45.740	◆Notification	Line protocol on Interface FastEthernet0, changed state to up
Mar 1 03:21:09.563	◆Notification	Line protocol on Interface FastEthernet0, changed state to down
Mar 1 03:20:06.686	◆Notification	Configured from console by vty0 (192.168.1.200)

Authorization Required - Microsoft Internet Explorer

Address http://192.168.1.110/

Authorization Required

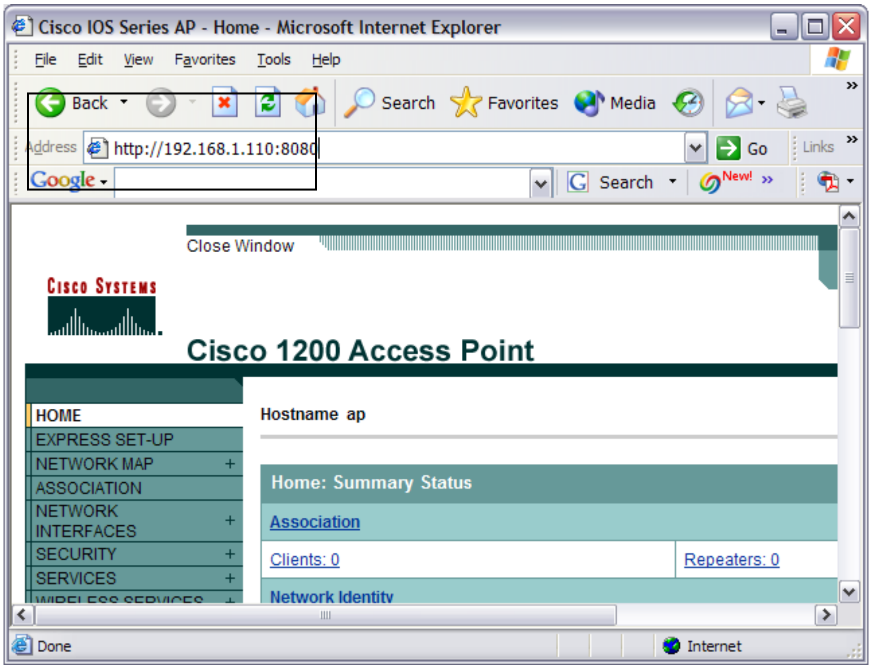
Browser not authentication-capable or authentication failed.

Figure 2 Web access success and failure

Often a new HTTP port is required (to stop users from trying to access the Web page). Thus to change the port:

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

Now we cannot access the Web page with the standard port (80), and we must change the address with a colon to define the port, such as shown in Figure 3.



Address http://192.168.1.110:8080

Hostname ap

Figure 3 Change of HTTP port

3.7 Challenge 6

The following sets up radio port settings:

```
> enable
# config t
(config)# int bvi1
(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
  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
  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
```

Example IOS Version 12.3

```
> enable
# config t
(config)# dot11 ssid fred
 (config-ssid)# max-assoc 9
(config-ssid)# exit
(config)# int bvi1
(config-if)# ip address 208.1.7.8 255.255.255.224
(config-if)# int d0
(config-if)# beacon period 2000
(config-if)# power local 5
(config-if)# power client 5
(config-if)#  world-mode
(config-if)# no shut
(config-if)# speed 1.0
(config-if)# ssid fred
```

3.8 Challenge 7

The following sets up radio port settings:

```
> enable
# config t
(config)# int bvi1
(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
```

Example IOS Version 12.3

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

(config)# int bvi1
(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
```

A major factor in wireless LANs is the multipath problem where waves can take differing paths to get to a destination. These multipaths can cause fading and distortion of the radio wave form. If different waves arrive at a receiver with different time delays they can distort the received signal. One of the way to overcome this problem is to use **diversity** which uses more than one antenna. It is likely that one of the antennas will experience less multipath problems than the other antennas. It is thus important that diversity antennas are physically separated from each other, and, so as to reduce the problem of null points, they can be moved around the physical space. The antenna can be set for both the transmit and receive options. These can be:

- **Diversity**. With this the WAP uses the antenna in which the best signal is being received.
- **Right**. This where the antenna is on the right of the WAP, and is highly directional.
- **Left**. This where the antenna is on the left of the WAP, and is highly directional.

3.9 Challenge 8

The following sets up radio port settings:

```
> 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
```

3.10 Challenge 9

The following sets up radio port settings:

```
> enable
# config t
(config)# int bvi1
(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)# premable-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
```

3.11 Challenge 10 (DHCP server)

The following sets up the DHCP server:

```
> en
# config t
(config)# ip dhcpd pool wyoming
(config-dhcp)# network 249.189.108.0 255.255.255.254
(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 249.189.108.26
(config)# ip dhcp ping ?
  packets  Specify number of ping packets
  timeout  Specify ping timeout
(config)# ip dhcp ping timeout 350
```

3.12 Challenge 11 (IP Hosts)

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 tennessee 211.99.108.9
montana (config)# ip host kirkcaldy 154.242.2.8
montana (config)# ip host edinburgh 64.2.249.2
```

3.13 Challenge 12 (CDP)

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
```

3.14 Challenge 13 (HTTP)

The following sets up HTTP settings:

```
> en
# config t
(config)# ip http server
(config)# ip http port ?
  <0-65535>  HTTP port
(config)# ip http port 1024
(config)# ip http ?
  access-class    Restrict access by access-class
  authentication  Set http authentication method
  help-path       HTTP help root URL
  path            Set base path for HTML
  port            HTTP port
  server          Enable HTTP server
(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
```

3.15 Challenge 14 (CON and VTY)

The following sets up CON and VTY settings:

```
> en
# config t
(config)# line con 0
(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)# log
 synchronous  Synchronized message output
(config-line)# log 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
```

3.16 Challenge 15 (Loopback)

The following sets up the loopback port:

```
> en
```

```
# config t
(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
```

3.17 Challenge 16 (Logging)

The following sets up logging:

```
> enable
# config t
(config)# logging on
(config)# logging 212.72.52.7
(config)# logging buffer 440240
(config)# logging host 138.24.170.8
(config)# logging trap emergency
(config)# logging monitor emergency
(config)# logging console emergency
(config)# logging buffer emergency
```

3.18 Challenge 17 (Services)

The following sets up services:

```
> 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)# sequence-numbers
  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
```

3.19 Challenge 18 (SNMP)

The following sets up SNMP:

```
> en
# 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
  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 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
```

3.20 Challenge 19 (Hot standby)

The following sets up hot standby:

```
> 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
  timeout         Standby polling timeout
(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
```

3.21 Challenge 20 (Repeater)

The following sets up a 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)# 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
(config-if)# ssid mississippi
(config-if-ssid)# infrastructure-ssid
```

3.22 Challenge 21 (Standard ACL)

The following sets up an ACL:

```
> 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
```

3.23 Challenge 22 (Extended ACL)

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
```

3.24 Challenge 23 (Encryption and LEAP)

The following sets up encryption and LEAP:

```
> en
# config t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# int bvi1
(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 ffffffffffffffffffffffffff
(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
```

3.25 Challenge 24 (AAA)

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)# user ?
  WORD  Client username
(config-radsrv)# user giraffe ?
  nthash    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
```

3.26 Challenge 25 (Mobile IP)

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 bvi1
(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
```

3.27 Challenge 27 (LBS)

The following sets up LBS:

```
> en
# config t
(config)# dot11 lbs test
(config-ssid)# server address 10.0.0.1 port 1024
(config-ssid)# int d0
(config-ssid)# 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.

3.28 Challenge 28 (AAA for Local Authentication)

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)# username test password bert
```

3.29 Challenge 29 (AAA)

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)# user ?
  WORD  Client username
(config-radsrv)# user giraffe ?
  nthash    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
```

3.30 Challenge 30 (RADIUS accounting on an SSID)

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

```
> en
# config t
(config)# aaa new-model
(config)# radius-server host 42.55.230.3 auth 1812 acct 1813
(config)# dot11 ssid test
(config-ssid)# accounting test-acc
```

3.31 Challenge 31 (HTTPS)

```
> en
# config t
(config)# hostname test
(config)# ip defaulf-gatway 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
```

3.32 Challenge 32 (TACACS+)

```
> 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
```

3.33 Challenge 33 (Security)

```
> enable
# config t
(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)# 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-priviledged 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
  systat           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.

3.34 Challenge 34 (Banners)

```
> 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
```

3.35 Challenge 34 (SNTP)

```
> enable
# config t
(config)# hostname amsterdam
amsterdam (config)# sntp server 192.168.1.100
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.
```

3.36 Challenge 36 (MAC filter)

```
> 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
```

3.37 Challenge 37 (MAC filter)

```
> 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 bridge-group-acl
(config-if) # bridge-group 1
(config-if) # bridge-group 1 output-address-list 701
```

3.38 Challenge 38 (MAC filter – extended)

```
> 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
```

3.39 Challenge 39 (MAC filter – extended)

```
> 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
```

3.40 Challenge 40 (MAC filter)

```
> 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 intput-address-list 701
```

3.41 Challenge 41 (Cisco Extensions)

```
> 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 aironet
```

Explanation

The Cisco Aironet extensions are:

- Cisco Key Integrity Protocol (CKIP). This uses a permutation method to renuew 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 again 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.

3.42 Challenge 42 (Cisco Extensions)

```
> 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
```

3.43 Challenge 43 (Beacon)

```
> enable
# config t
(config)# int bvi1
(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 50
```

Explanation

The beacon period is defined as the amount of time between access point beacons in Kilomicroseconds (1 Kμsec is 1,024 millseconds). The default is 100 Kμsec. 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).

3.44 Challenge 44 (RTS)

```
> 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 100
(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, tit 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
```

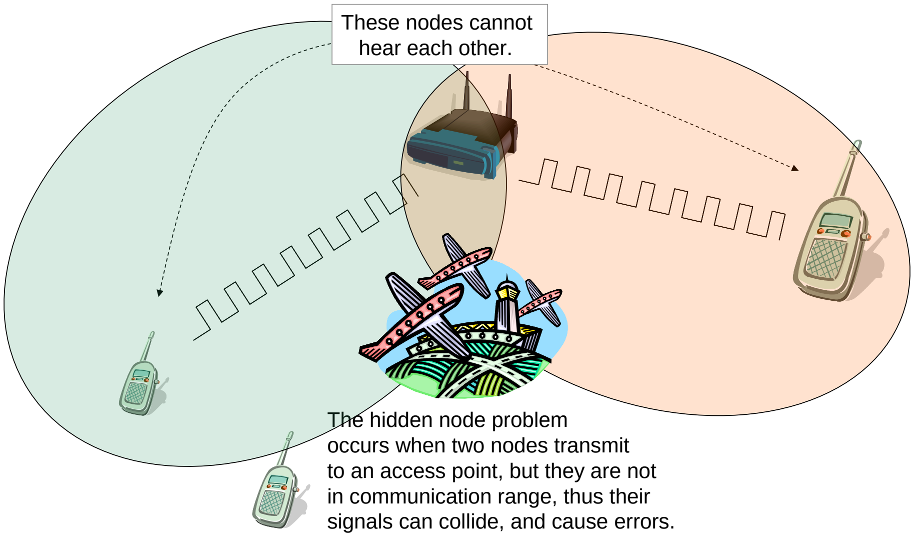

These nodes cannot hear each other.
The hidden node problem occurs when two nodes transmit to an access point, but they are not in communication range, thus their signals can collide, and cause errors.

Figure 1 Hidden node problem

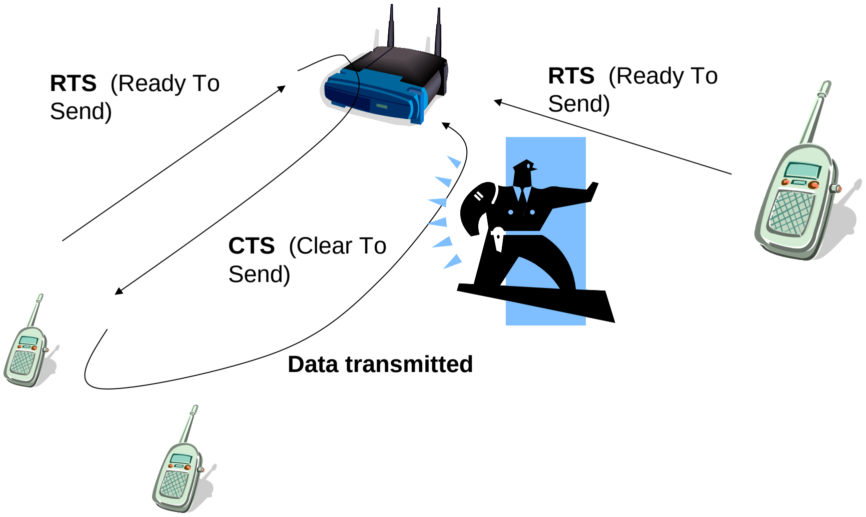


Figure 2 RTS/CTS operation

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
```

3.45 Challenge 45 (Fragmentation)

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

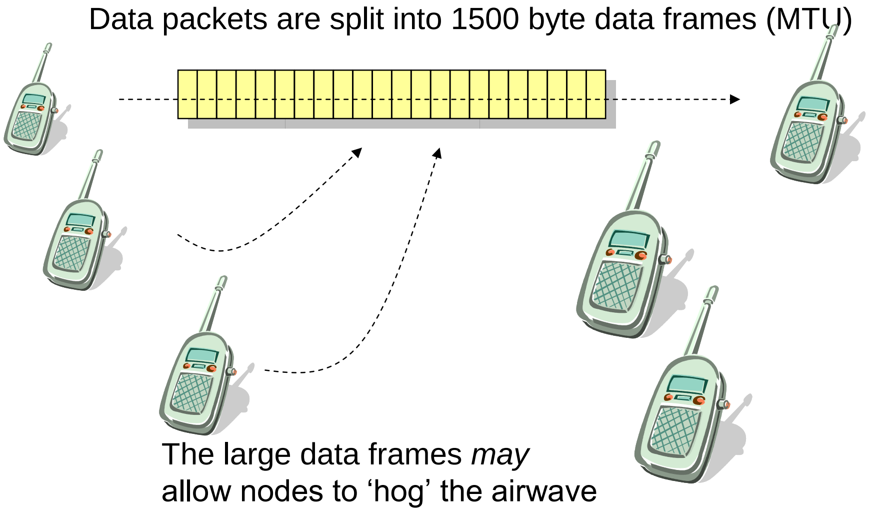

Data packets are split into 1500 byte data frames (MTU)
The large data frames *may* allow nodes to 'hog' the airwave

Figure 1 Transmission of large data frames

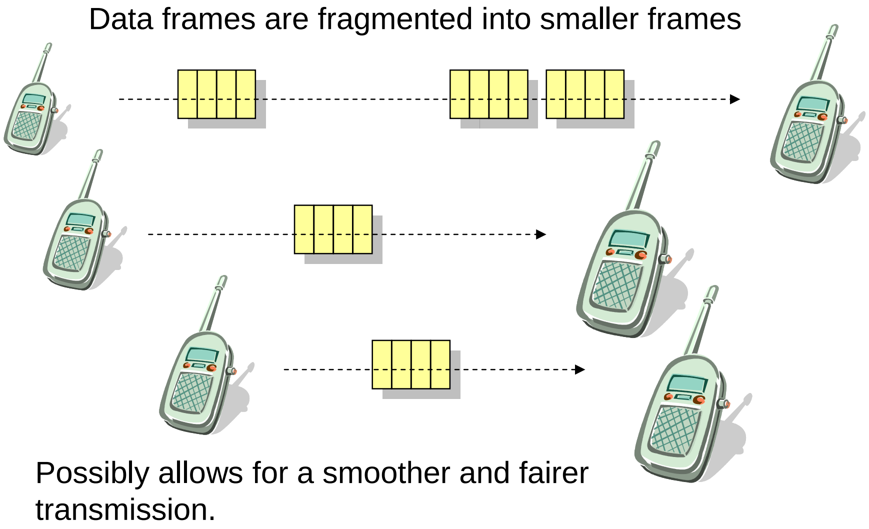

Data frames are fragmented into smaller frames
Possibly allows for a smoother and fairer transmission.

Figure 2 Fragmentation of data frames

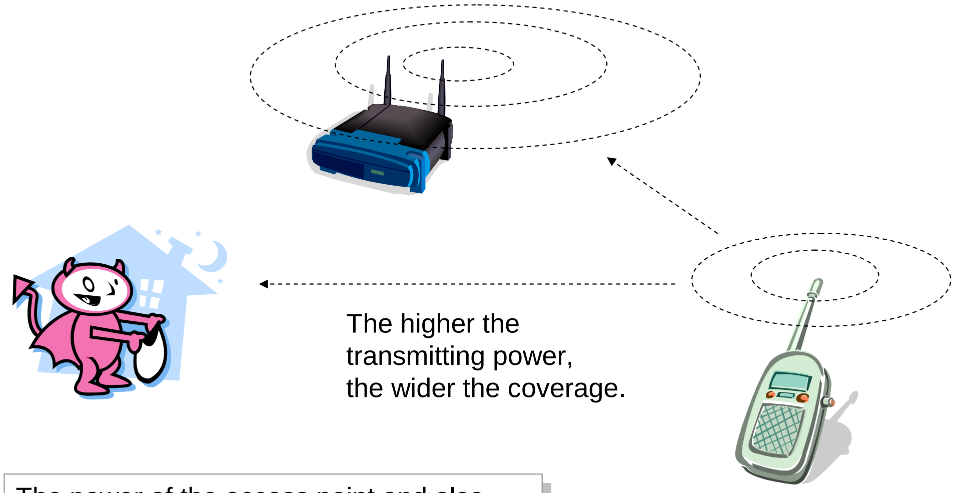
3.46 Challenge 46 (Power)

```
> enable
# config t
(config)# int bvi1
(config-if)# ip address 208.1.7.8 255.255.255.224
(config-if)# int d0
(config-if)# power local 50
(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
```



The power of the access point and also of the client are important as they will define the coverage of the signal, and must also be within the required safety limits.

Figure 1 Power transmission

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.

3.47 Challenge 47 (Association)

```
> enable
# config t
(config)# int bvi1
(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
```

3.48 Challenge 48 (Preamble)

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 interoperatablity problems. To set short preamble:

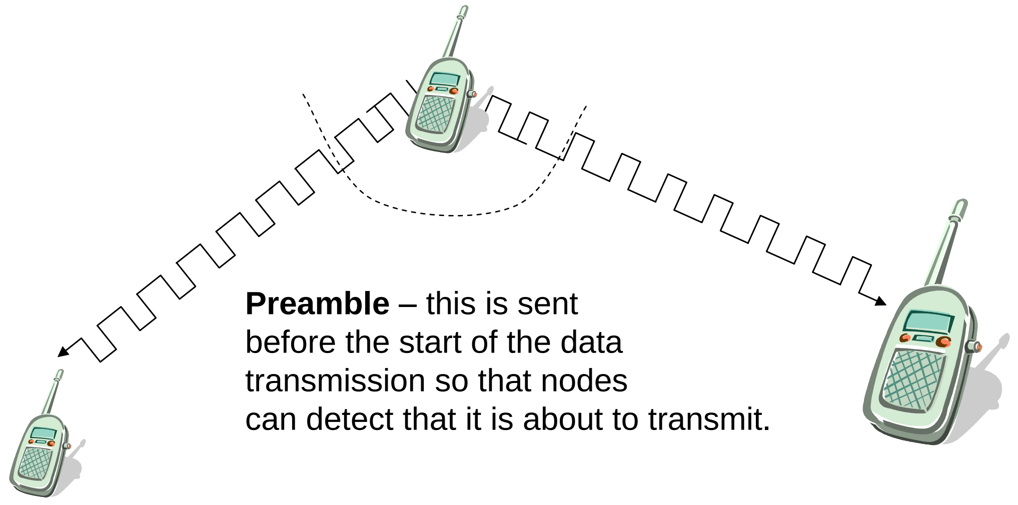
```
# config t
(config)# int dot11radio0
(config-if)# preamble-short
(config-if)# end
```

3.49 Challenge 49 (Station role)

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)# 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.



Preamble – this is sent before the start of the data transmission so that nodes can detect that it is about to transmit.

Figure 1 Preamble

3.50 Challenge 50 (Slot time)

The throughout 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 avialable in IEEE 802.11g. By default it is disabled.

3.51 Challenge 51 (MAC authentication)

```
> 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 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.

3.52 Challenge 52 (Wireless IDS)

```
> 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 scanner
(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
```

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
```

3.53 Challenge 53 (Fallback)

```
> 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:

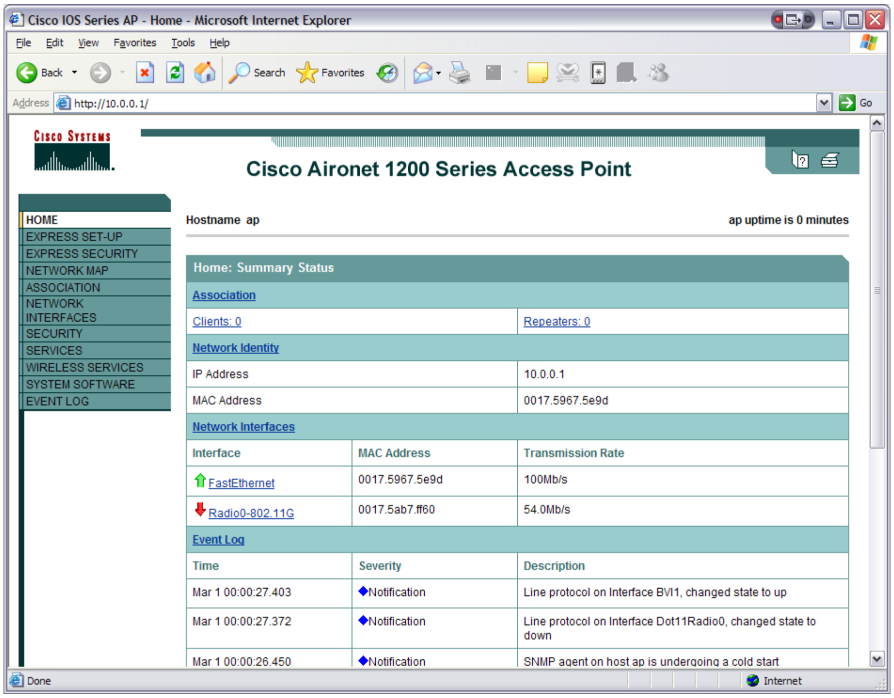
```
(config-if)# station root fallback shutdown
```

3.54 Challenge 54 (Web server)

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):



Hostname ap

ap uptime is 0 minutes

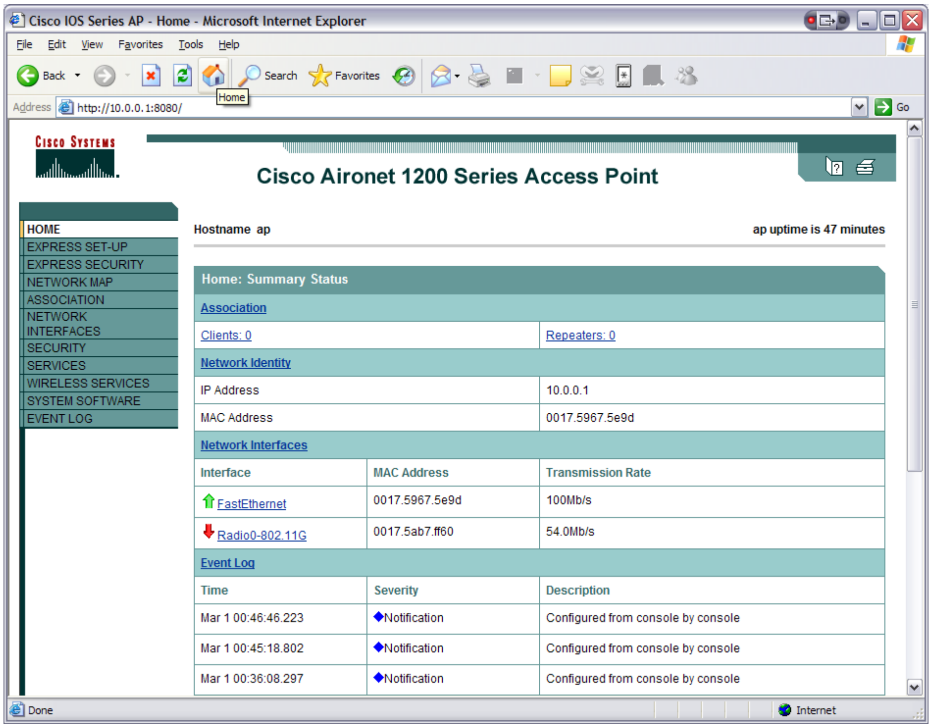
Home: Summary Status

Association		
Clients: 0		Repeaters: 0
Network Identity		
IP Address		10.0.0.1
MAC Address		0017.5967.5e9d
Network Interfaces		
Interface	MAC Address	Transmission Rate
FastEthernet	0017.5967.5e9d	100Mb/s
Radio0-802.11G	0017.5ab7.ff60	54.0Mb/s
Event Log		
Time	Severity	Description
Mar 1 00:00:27.403	Notification	Line protocol on Interface BVI1, changed state to up
Mar 1 00:00:27.372	Notification	Line protocol on Interface Dot11Radio0, changed state to down
Mar 1 00:00:26.450	Notification	SNMP agent on host ap is undergoing a cold start

Sometimes another port is used, such as 8080 with:

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

which is accessed with:



Hostname ap

ap uptime is 47 minutes

Home: Summary Status

Association		
Clients: 0		Repeaters: 0
Network Identity		
IP Address		10.0.0.1
MAC Address		0017.5967.5e9d
Network Interfaces		
Interface	MAC Address	Transmission Rate
FastEthernet	0017.5967.5e9d	100Mb/s
Radio0-802.11G	0017.5ab7.ff60	54.0Mb/s
Event Log		
Time	Severity	Description
Mar 1 00:46:46.223	Notification	Configured from console by console
Mar 1 00:45:18.802	Notification	Configured from console by console
Mar 1 00:36:08.297	Notification	Configured from console by console

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 ?
  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
```

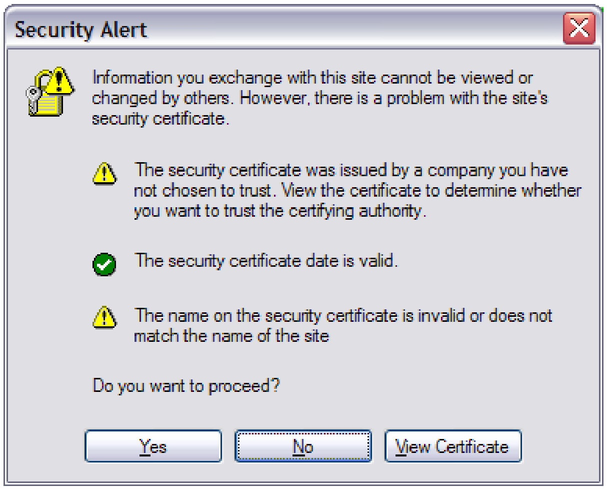
```
HTTP server status: Enabled
HTTP server port: 8080
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path: flash:/c1200-k9w7-mx.123-8.JA/html/level/1;zflash:/c1200-k9w7-
     mx.123-8.JA/html/level/1;flash:/c1200-k9w7-mx.123-
     8.JA/html/level/15;zflash:/c1200-k9w7-mx.123-8.JA/html/level/15;flash:/c1200-k9w7-
     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-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:
```

3.55 Challenge 55 (Secure Web server)

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:



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

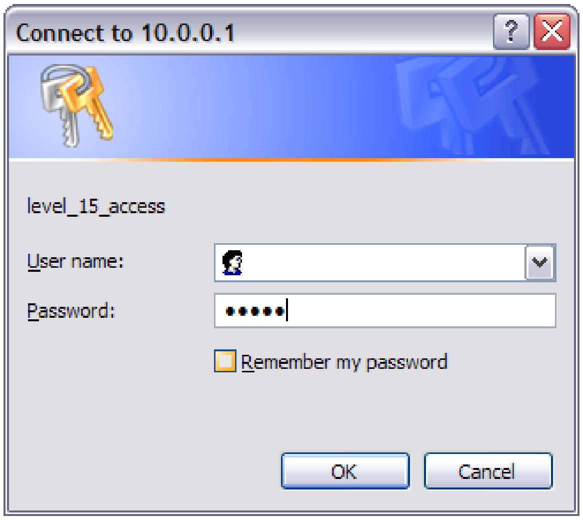
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

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



Connect to 10.0.0.1

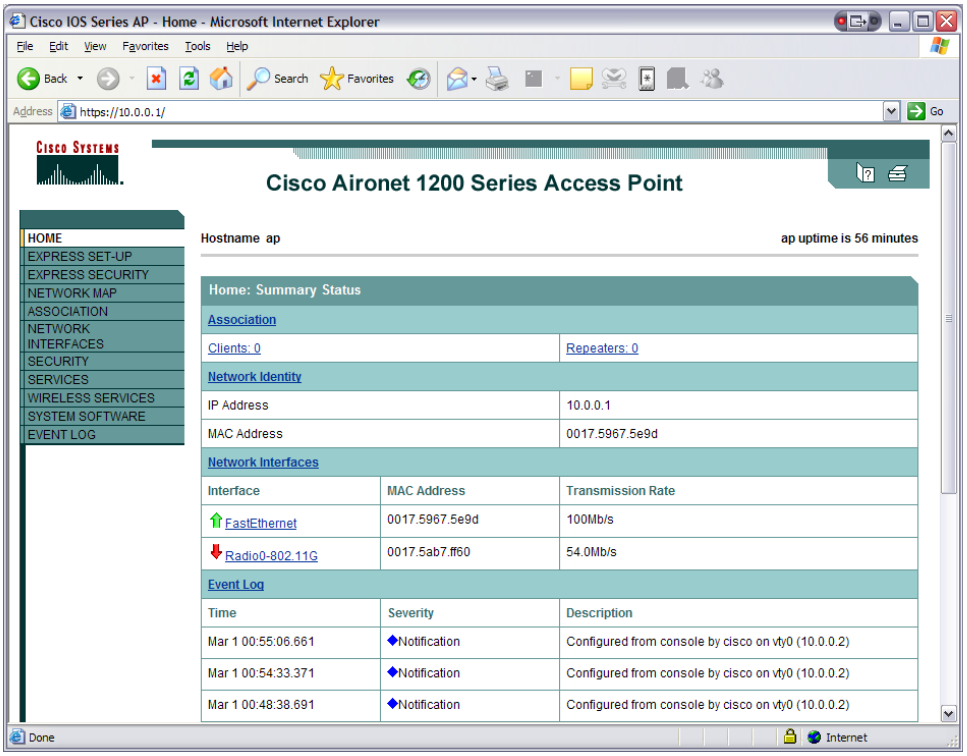
level_15_access

User name:

Password: •••••

□ Remember my password

and then:



Cisco IOS Series AP - Home - Microsoft Internet Explorer

Address https://10.0.0.1/

Cisco Aironet 1200 Series Access Point

Hostname ap — ap uptime is 56 minutes

Home: Summary Status

Association	
Clients: 0	Repeaters: 0
Network Identity	
IP Address	10.0.0.1
MAC Address	0017.5967.5e9d

Network Interfaces		
Interface	MAC Address	Transmission Rate
FastEthernet	0017.5967.5e9d	100Mb/s
Radio0-802.11G	0017.5ab7.ff60	54.0Mb/s

Event Log		
Time	Severity	Description
Mar 1 00:55:06.661	Notification	Configured from console by cisco on vty0 (10.0.0.2)
Mar 1 00:54:33.371	Notification	Configured from console by cisco on vty0 (10.0.0.2)
Mar 1 00:48:38.691	Notification	Configured from console by cisco on vty0 (10.0.0.2)

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:
```

3.56 Challenge 56 (QoS)

The Aironet advertise their QoS parameters so that WLAN clients which require a certain QoS requirement can 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 choose if this was the best rate for the best effort.

3.57 Challenge 57 (SSH)

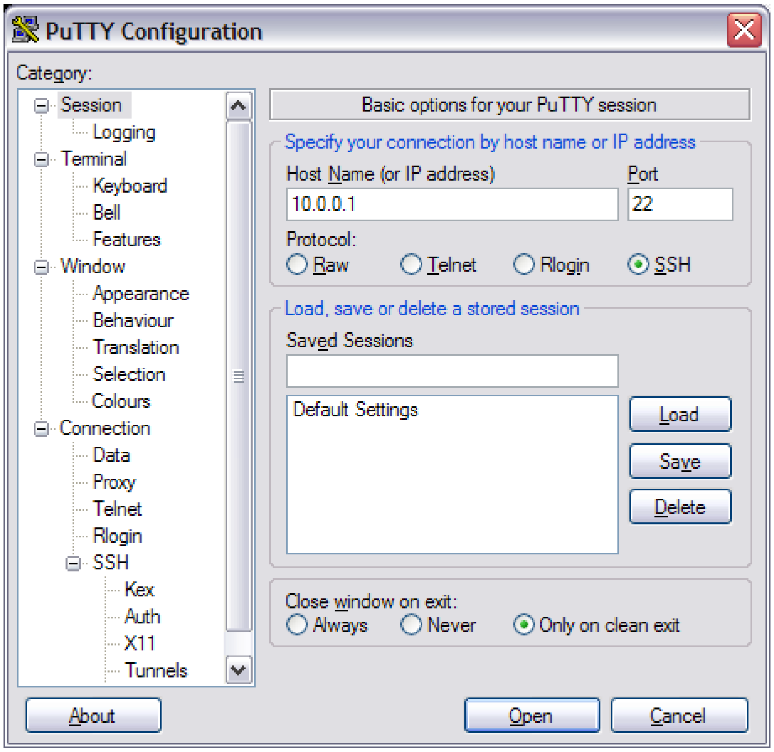
The TELNET protocol is insecure as the text is passed as plain text. An improved method is to use SSH, which encrypts data. It requires that the domain-name and an RSA key pair:

```
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:



PuTTY Configuration

Category:

Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 10.0.0.1

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

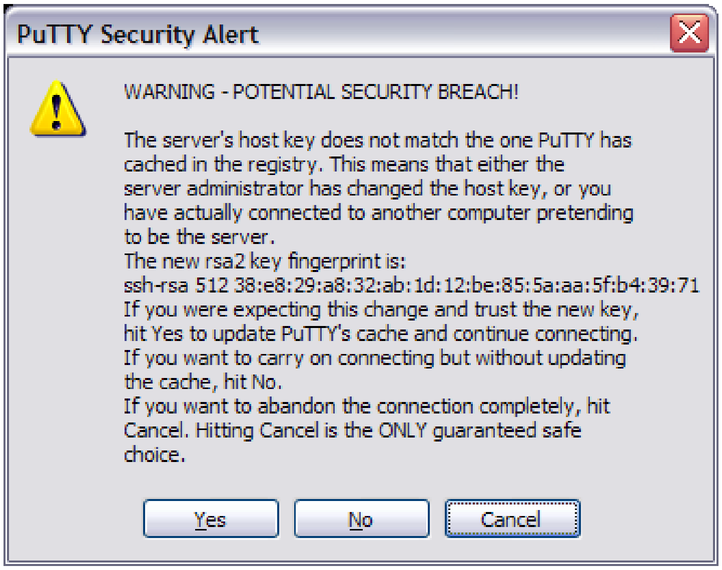
Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

after which the client shows the message:

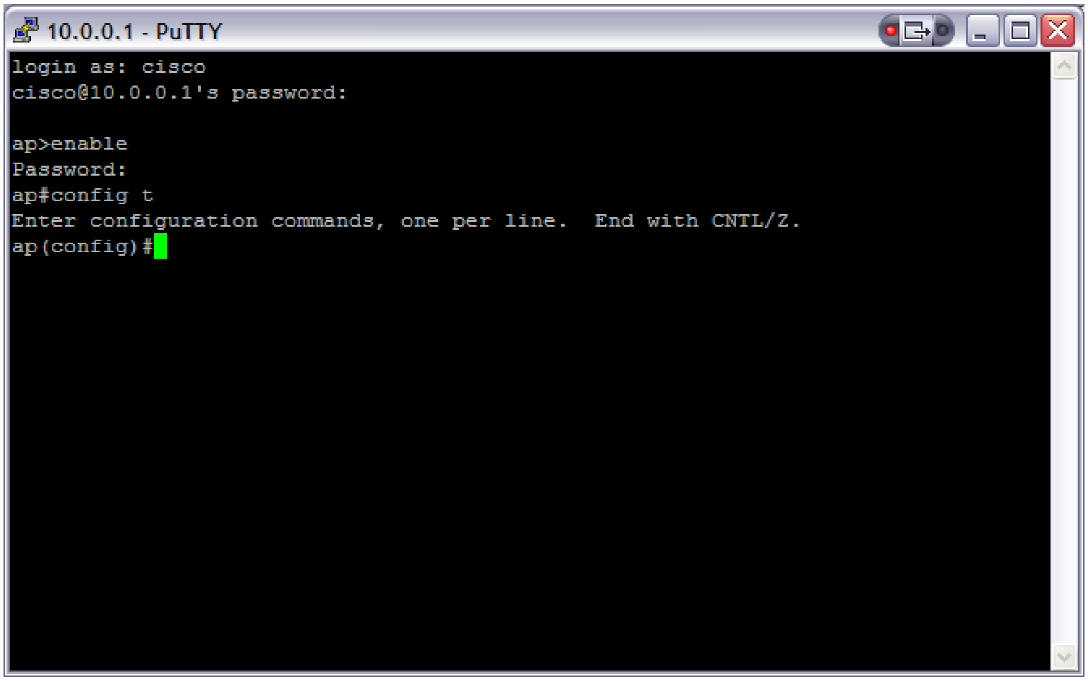


PuTTY Security Alert

WARNING - POTENTIAL SECURITY BREACH!

The server's host key does not match the one PuTTY has cached in the registry. This means that either the server administrator has changed the host key, or you have actually connected to another computer pretending to be the server.
The new rsa2 key fingerprint is:
ssh-rsa 512 38:e8:29:a8:32:ab:1d:12:be:85:5a:aa:5f:b4:39:71
If you were expecting this change and trust the new key, hit Yes to update PuTTY's cache and continue connecting.
If you want to carry on connecting but without updating the cache, hit No.
If you want to abandon the connection completely, hit Cancel. Hitting Cancel is the ONLY guaranteed safe choice.

and the SSH connection is made, such as:



```
login as: cisco
cisco@10.0.0.1's password:

ap>enable
Password:
ap#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#
```

To get rid of keys:

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

and to set the timeout and authentication retries:

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

and to prevent Telnet sessions:

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

3.58 Challenge 58 (LEAP)

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

```
(config)# hostname ap
(config)# aaa new-model
(config)# int bvi1
(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.

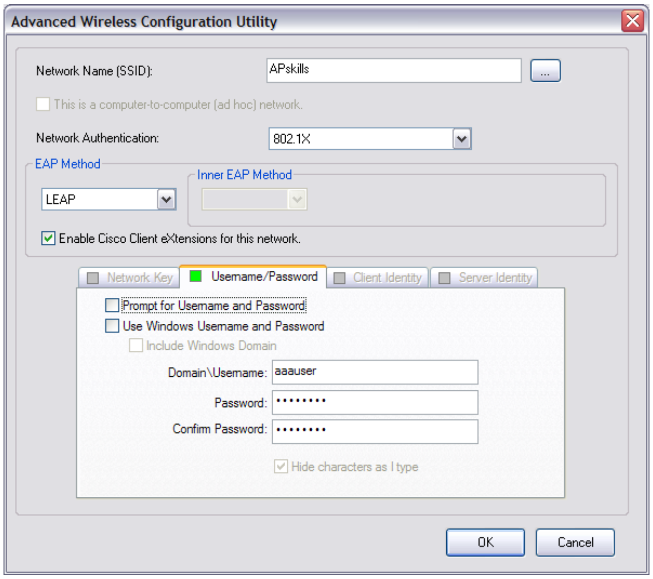
Next setup the clients to support LEAP authentication, as shown in Figure 1. Once the client has associated, determine the associated devices with:

```
# 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)
```



Advanced Wireless Configuration Utility

Network Name (SSID): APskills

□ This is a computer-to-computer (ad hoc) network.

Network Authentication: 802.1X

EAP Method: LEAP

Inner EAP Method:

☑ Enable Cisco Client eXtensions for this network.

□ Prompt for Username and Password

□ Use Windows Username and Password

□ Include Windows Domain

Domain\Username: aaauser

Password: ••••••••

Confirm Password: ••••••••

☑ Hide characters as I type

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]

3.59 Challenge 59 (Encapsulaion)

The following sets up SNAP encapsulation:

```
(config)# hostname ap
(config)# aaa new-model
(config)# int bvi1
(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
```

3.60 Challenge 60 (Output filter)

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
```

3.61 Challenge 61 (Filtering)

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
```

3.62 Challenge 62 (PSPF)

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
```

3.63 Challenge 63 (MBSSID)

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.

3.64 Challenge 66 (SSID redirect)

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
```

3.65 Challenge 67 (SSID redirect with ACLs)

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
```

3.66 Challenge 68 (SSIDL)

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
```

3.67 Challenge 69 (VLAN encryption)

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.

3.68 Challenge 70 (VLAN encryption)

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

3.69 Challenge 71 (VLAN broadcast)

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.

3.70 Challenge 72 (MAC authentication)

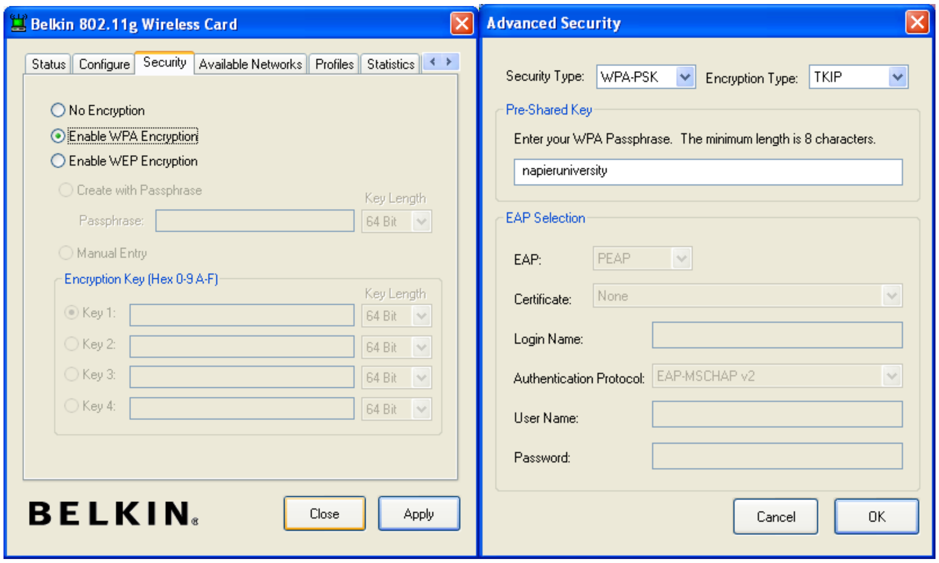
```
# config t
```

```
(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
```

3.71 Challenge 73 (WPA-PSK)

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 client (Figure 1) 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
```



○ No Encryption
● Enable WPA Encryption
○ Enable WEP Encryption
○ Create with Passphrase
Passphrase: Key Length 64 Bit
○ Manual Entry
Encryption Key (Hex 0-9 A-F) Key Length
● Key 1: 64 Bit
○ Key 2: 64 Bit
○ Key 3: 64 Bit
○ Key 4: 64 Bit

Security Type: WPA-PSK Encryption Type: TKIP
Pre-Shared Key
Enter your WPA Passphrase. The minimum length is 8 characters.
napieruniversity
EAP Selection
EAP: PEAP
Certificate: None
Login Name:
Authentication Protocol: EAP-MSCHAP v2
User Name:
Password:

Figure 1:

3.72 Challenge 74 (Authentication holdtimes)

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.

3.73 Challenge 75 (WLCCP)

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 bvi1
(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.

3.74 Challenge 76 (Test)

This is a wireless test

3.75 Challenge 77 (Tacacs+)

```
> en
# config t
(config)# hostname test
(config)# aaa new-model
(config)# tacacs-server ?
  administration    Start tacacs+ deamon 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 accouting network default ?
  none        No accounting.
  start-stop  Record start and stop without waiting
  stop-only   Record stop when service terminates.

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

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

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

3.76 Challenge 78 (Multiple SSIDs)

```
> 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
```

3.77 Challenge 79 (Multiple SSIDs)

```
> 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
```

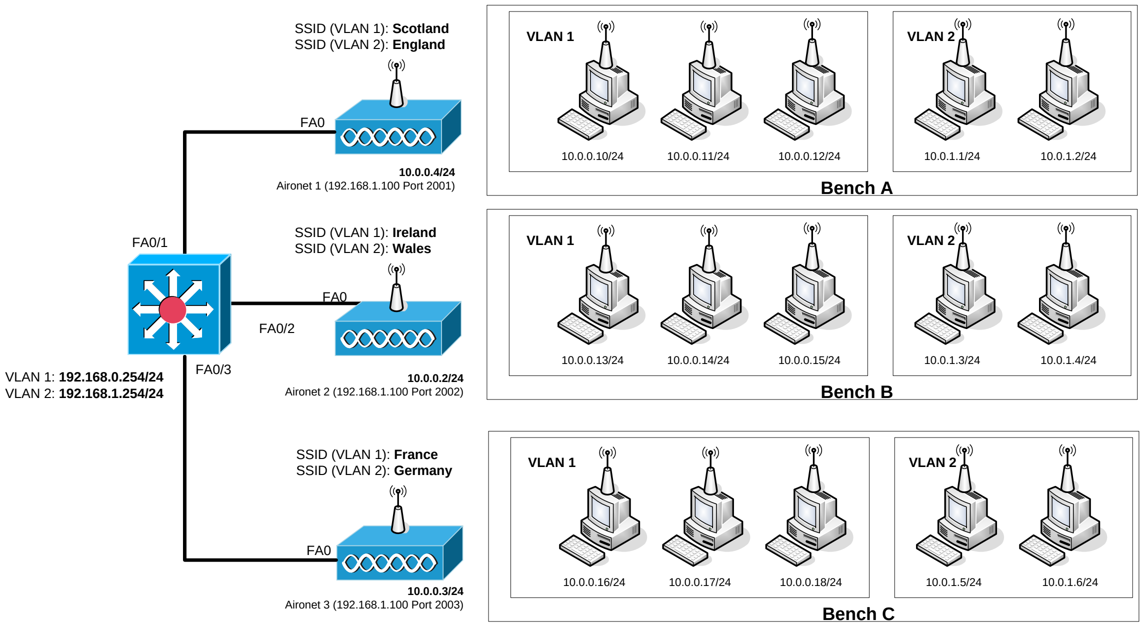
This assigns three VLANs. The first is allowed to the network1 SSID, the second to network2 and the third to network3.

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 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 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 vlan 1,2
(config-if)# switchport mode trunk
(config-if)# switchport nonegotiate
```



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"
```

3.78 Challenge 80 (QoS)

```
> 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.

4 Wireless (Tutorial)

4.1 Introduction

In a wireless system the main elements of the configuration are:

- **Authentication algorithm**. This sets whether the adapter uses an open system (where other nodes can listen to the communications), or uses encryption (using either a WEP key, or a shared key).
- **Channel**. If an ad-hoc network is used, then the nodes which communicate must use the same channel.
- **Fragmentation threshold**. This can be used to split large data frames into smaller fragments. The value can range from 64 to 1500 bytes. This is used to improve the efficiency when there is a high amount of traffic on the wireless network, as smaller frames make more efficient usage of the network.
- **Network type**. This can either be set to an infrastructure network (which use access points, or wireless hubs) or Ad-hoc, which allows nodes to interconnect without the need for an access point.
- **Preamble mode**. 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 interoperatablity problems.
- **RTS/CTS threshold**. 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 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, the access point sends a CTS message. The node can then send its data.

4.2 Tutorial 1 (Basic Configuration)

1. You should start in the user mode:

```
>
```

2. Go into the EXEC mode using the enable command.

```
> enable
```

How does the prompt change?

3. From the EXEC mode go into the Global Configuration Mode, and use the hostname command to change the hostname to MyWireless.

```
# ?
# config t
(config) # hostname MyWireless
```

How does the prompt change?

4. Exit from the Global Configuration Mode using exit, and list the current running-config with show running-config.

```
(config) # exit
# show running-conf
```

Outline some of the settings in the running-config:

4.2.1 Using the show command

5. Complete the following command:

```
# ?
# show buffers
# show memory
# show stacks
# show hosts
# show arp
# show flash
# show history
# show version
# show interfaces
# show interface fa0
# show interface dot11radio0
```

Using the information from above what are the following:

Processor Board ID:

Processor Type:

Processor Clock Speed:

System image file:

Operating System Version:

File names shored in the Flash Memory:

Product/Model Number:

4.2.2 History commands

The main commands for history are:

```
# terminal ?
# terminal history ?
# terminal history size ?
# terminal history size 100
# show history
```

4.2.3 Clock commands

The main commands for clock are:

```
# clock ?
# clock set ?
# clock set 11:00 ?
# clock set 11:00 11 ?
# clock set 11:00 11 jun ?
# clock set 11:00 11 jun 2006
```

4.2.4 Programming the WAP ports

6. Program the two ports of the WAP with:

```
# config t
(config)# int ?
(config)# int fa0
(config-if)# ?
(config-if)# ip address ?
(config-if)# ip address 207.11.12.10 ?
(config-if)# ip address 207.11.12.10 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
```

```
(config)# int dot11radio0
(config-if)# ?
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# station-role ?
(config-if)# station-role root
(config-if)# channel ?
(config-if)# channel 7
(config-if)# no shutdown
(config-if)# ssid fred
(config-if-ssid)# ?
(config-if-ssid)# guest-mode
(config-if-ssid)# exit
(config-if)# exit
(config)# exit
```

WAP is the root of the wireless network (other option: `repeater`)

Set radio channel to 7 (2.442GHz)

Ping the newly defined ports (`207.11.12.10` and `192.168.0.1`). Are they responding?

Next go back to the ports and shut them down:

```
# config t
(config)# int ?
(config)# int fa0
(config-if)# shutdown
(config-if)# exit
(config)# int dot11radio0
(config-if)# shutdown
(config-if)# exit
(config)# exit
```

Ping the newly defined ports (`207.11.12.10` and `192.168.0.1`) again. Are they responding?

To get rid of guest-mode:

```
# config t
(config)# int dot11radio0
(config-if)# ?
(config-if)# ssid fred
(config-if-ssid)# no guest-mode
(config-if-ssid)# exit
(config-if)# exit
(config)# exit
```

7. Go to the EXEC mode, and view the running-config:

```
# show running-config
```

8. The WAP can access a domain server and DNS, using the ip name-server and ip domain-lookup commands:

```
# config t
(config)# ip ?
(config)# ip domain-name ?
(config)# ip domain-name mydomain.com
(config)# ip name-server ?
(config)# ip name-server 160.10.11.12
(config)# ip domain-lookup
(config)# ip default-gateway ?
(config)# ip default-gateway 10.11.12.11
```

Enable DNS lookup on the WAP

9. To get rid of any of these settings, insert a “no” in front of them, such as:

```
# config t
(config)# no ip domain-name mydomain.com
(config)# no ip name-server 160.10.11.12
(config)# no ip domain-lookup
(config)# no ip default-gateway 10.11.12.11
(config)# exit
# show running
```

10. Setting passwords for the line console and for telnet access:

```
# config t
(config)# line con 0
(config-line)# login
(config-line)# password fred
(config-line)# exit
(config)# line vty 0 15
(config-line)# login
(config-line)# password fred
(config-line)# exit
(config)# exit
```

11. Setting up a WWW server on the wireless access point:

```
# config t
(config)# ip http server
(config)# exit
# show running
```

12. If we need to change the port and the max number of connections on the WWW server:

```
# config t
(config)# ip http port 8080
(config)# ip http max-connections 2
(config)# exit
```

```
# show running
```

13. And to disable the WWW server:

```
# config t
(config)# no ip http server
(config)# exit
# show running
```

14. Setting up a user on the wireless access point:

```
# config t
(config)# username ?
(config)# username fred ?
(config)# username fred password bert
(config)# exit
# show running
```

15. To get rid of a user:

```
# config t
(config)# no username fred password bert
(config)# exit
# show running
```

16. To setup the host table on the wireless access point:

```
# config t
(config)# ip host freds 172.14.10.11
(config)# ip host berts 172.14.10.12
(config)# ip host slappi 10.15.1.100
```

17. It is possible to run a DHCP server to assign IP parameters to wireless nodes:

```
# config t
(config)# ip ?
(config)# ip dhcp ?
(config)# ip dhcp pool socpool
(config-dhcp)# ?
(config-dhcp)# network 192.168.0.0 255.255.255.0
(config-dhcp)# lease 10
(config-dhcp)# exit
(config)# exit
# show running-config
```

Sets the range of addresses to be allocated, and sets the lease for 10 days

18. Then to get rid of DHCP:

```
# config t
(config)# no ip dhcp pool socpool
```

```
(config)# exit
# show running-config
```

19. To create a banner:

```
# config t
(config)# banner motd # hello #
(config)# exit
# show running
```

20. To get rid of the banner:

```
# config t
(config)# no banner motd # hello #
```

21. To set the ARP method:

```
# config t
(config)# int dot11radio0
(config-if)# arp ?
(config-if)# arp arpa
```

22. CDP (Cisco Discovery Protocol) is set with the following:

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

Using the show cdp command, determine the settings for CDP:

23. To enable CDP on the WAP:

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

24. To enable CDP on an interface:

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

25. To show CDP information:

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

26. To setup a local hosts table:

```
(config)# ip host LAB_A 192.5.5.1 205.7.5.1 201.100.11.1
(config)# ip host LAB_B 201.100.11.2 219.17.100.1 199.6.13.1
(config)# ip host LAB_C 223.8.151.1 204.204.7.1
(config)# ip host LAB_D 210.93.105.1 204.204.7.2
(config)# ip host LAB_E 210.93.105.2
(config)# exit
# show hosts
# show running
```

4.3 Tutorial 2 (Enhancing the radio port setup)

27. The power level of the access point can be set with the power command, and the speed can be set with the speed command:

```
# config t
(config)# int dot11radio0
(config-if)# power ?
(config-if)# power local ?
(config-if)# power local 30
(config-if)# power client 10
(config-if)# speed ?
(config-if)# speed 1.0
(config-if)# exit
(config)# exit
```

The access point can be used to set the power levels of the clients (in this case, 10mW)

Using the information from above what are the following:

Available power levels for access point:

Available speeds for access point:

28. With world mode, the access point adds channel carrier set information to its beacon. This allows client devices with world mode to receive the carrier set information and adjust their settings automatically. World mode is disabled by default, to enable it:

```
# config t
(config)# int dot11radio0
(config-if)# ?
(config-if)# world-mode
```

```
(config-if)# exit
(config)# exit
```

29. The antenna can be set for both the transmit and receive options. These can be :

- **Diversity**. With this the WAP uses the antenna in which the best signal is being received.
- **Right**. This where the antenna is on the right of the WAP, and is highly directional.
- **Left**. This where the antenna is on the left of the WAP, and is highly directional.

```
# config t
(config)# int dot11radio0
(config-if)# antenna ?
(config-if)# antenna transmit ?
(config-if)# antenna transmit diversity
(config-if)# antenna receive left
(config-if)# exit
(config)# exit
```

30. The WAP can be setup to transmit a beacon signal on which devices can connect to (using a delivery traffic indication message - DTIM). The time period on which it transmits is defined in Kilomicroseconds, which is 1 millisecond (one thousands of a second). For example to set the beacon period to once every second:

```
# config t
(config)# int dot11radio0
(config-if)# beacon ?
(config-if)# beacon period ?
(config-if)# beacon period 1000
(config-if)# exit
(config)# exit
```

To get rid of the beacon signal:

```
# config t
(config)# int dot11radio0
(config-if)# no beacon period 1000
(config-if)# exit
(config)# exit
```

31. **PAYLOAD-ENCAPSULATION**. If packets are received which are not defined in IEEE 802.3 format, the WAP must format them using the required encapsulation. The methods are:

- 802.1H (**dot1h**). This is the default, and is optimized for Cisco Aironet wireless products.

- RFC1042. This is used by many wireless manufacturers (SNAP), and is thus more compatible than 802.1H.

For example:

```
# config t
(config)# int dot11radio0
(config-if)# payload-encapsulation ?
(config-if)# payload-encapsulation rfc1042
(config-if)# exit
(config)# exit
```

32. **CARRIER TEST**. The WAP can show the activity on certain channels using the carrier busy test (note that the connections to devices are dropped for about 4 seconds when these tests are made).

For example:

```
# show dot11 ?
# show dot11 carrier ?
# show dot11 carrier busy
```

33. **RTS**. The RTS (Ready To Send) is used to handshake data between the client and the WAP. RTS threshold is used to set the packet size at which the access point issues a request to send (RTS) before sending the packet. Low RTS Threshold values are useful in areas where there are many clients, or where the clients are far apart and cannot reach each other (the hidden node problem). The Maximum RTS Retries (1-128) defines the maximum number of times the access point issues an RTS before abandoning the send. For example to set the threshold at 1000 Bytes and the number of retries to 10:

```
# config t
(config)# int dot11radio0
(config-if)# rts ?
(config-if)# rts threshold ?
(config-if)# rts threshold 1000
(config-if)# rts retries ?
(config-if)# rts retries 10
(config-if)# exit
(config)# exit
```

To set the preamble to short:

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

To get rid of it:

```
# config t
(config)# int dot11radio0
(config-if)# no preamble-short
(config-if)# exit
(config)# exit
```

34. **PACKET RETRIES**. The maximum data retries value (1-128) defines the number of attempts that a WAP makes before dropping the packet.

```
# config t
(config)# int dot11radio0
(config-if)# packet retries 5
(config-if)# exit
(config)# exit
```

35. **FRAGMENT-THRESHOLD**. The fragmentation threshold value sets the size at which packets are fragmented (256 B to 2338 B). Low values are good when there are many errors in the transmitted data, as there will be more chance that each of the fragments will be received correctly. An example is:

```
# config t
(config)# int dot11radio0
(config-if)# fragment-threshold 1000
(config-if)# exit
(config)# exit
```

36. **IP PROXY-MOBILE**. This command is applied to the interface command to enable proxy Mobile IP operations. For example:

```
# config t
(config)# int dot11radio0
(config-if)# ip proxy-mobile
(config-if)# exit
(config)# exit
```

The basic details of the wireless access point is:

FA0 - Fast Ethernet connection to the network.
DOT11RADIO0 - 2.4GHz radio connection.
DOT11RADIO1 - 5GHz radio connection.

37. A particular problem can be were there are too many associations with the wireless device. To limit the number of associations, the max-association value is set. For example to set the maximum number of associations to 20:

```
# config t
(config)# int d0
(config-if)# ssid fred
(config-if-ssid)# ?
(config-if-ssid)# max-associations ?
(config-if-ssid)# max-associations 20
(config-if-ssid)# exit
```

4.4 Tutorial 3 (Showing associations and controllers)

38. To determine wireless nodes that have been associated with the WAP:

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

What is the IP address and the MAC address of the node has been associated with the WAP:

What is the transmitted signal strength:

What is the signal quality:

39. To list controllers

```
# show controllers
```

```
!
interface Dot11Radio0
Radio 350 Series, Address 0007.50d5.bf4c, BBlock version 1.59, Software version 5.30.17
Serial number: vms061904jc
Carrier Set: EMEA (EU)
Current Frequency: 2452 Mhz  Channel 9
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)
Current Power: 50 mW
Allowed Power Levels: 1 5 20 30 50
Current Rates:  basic-1.0 basic-2.0 basic-5.5 basic-11.0
Allowed Rates:  1.0 2.0 5.5 11.0
Best Range Rates:  basic-1.0 2.0 5.5 11.0
Best Throughput Rates:  basic-1.0 basic-2.0 basic-5.5 basic-11.0
Default Rates:  no
Radio Management (RM) Configuration:
      Beacon State      1     RM Tx Setting Enabled FALSE
      RM Tx Power Level 0     RM Tx Channel Number  0
      Saved Tx Power    0     Saved Tx Channel      0
Priority 0 cw-min 5 cw-max 10 fixed-slot 6
Priority 1 cw-min 5 cw-max 10 fixed-slot 2
Priority 2 cw-min 4 cw-max 5 fixed-slot 1
Priority 3 cw-min 3 cw-max 4 fixed-slot 1
Radio running mobile:  temp 0 C tx_power 50 bb_code 0x0
    rssi_threshold 0x0 last alarm code 0x0 gain offset 0
```

40. **SHOW CONTROLLERS**. The Show Controllers Dot11Radio0 command is used to show the status of radio interface. For example:

```
# show controllers dot11radio0
```

An example of the output is:

```
!
interface Dot11Radio0
Radio 350 Series, Address 0007.50d5.bf4c, BBlock version 1.59, Software version 5.30.17
Serial number: vms061904jc
Carrier Set: EMEA (EU)
Current Frequency: 2432 Mhz  Channel 5
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)
Current Power: 50 mW
Allowed Power Levels: 1 5 20 30 50
Current Rates:  basic-1.0 basic-2.0 basic-5.5 basic-11.0
Allowed Rates:  1.0 2.0 5.5 11.0
Best Range Rates:  basic-1.0 2.0 5.5 11.0
Best Throughput Rates:  basic-1.0 basic-2.0 basic-5.5 basic-11.0
Default Rates:  no
Radio Management (RM) Configuration:
      Beacon State      1     RM Tx Setting Enabled FALSE
      RM Tx Power Level 0     RM Tx Channel Number  0
      Saved Tx Power    0     Saved Tx Channel      0
```

41. **SHOW CLIENTS**. This command is used to show the details of all the associated clients, and uses:

```
# show dot11 associations all-clients
```

An example of the output is:

```
Address           : 0003.6dff.2a51     Name             :
IP Address        : 192.168.0.11       Interface        : Dot11Radio 0
Device            :    -                Software Version :

State             : Assoc              Parent           : self
SSID              : tsunami            VLAN             : 0
Hops to Infra     : 1                  Association Id   : 3
Clients Associated: 0                  Repeaters associated: 0
Key Mgmt type     : NONE               Encryption     Rate      : 11.0
Capability       :  ShortHdr
Supported Rates   : 1.0 2.0 5.5 11.0
Signal Strength   : -29  dBm           Connected for    : 913 seconds
Signal Quality    : 81 %               Activity Timeout : 31 seconds
Power-save        : Off                Last Activity    : 28 seconds ago

Packets Input     : 143                Packets Output   : 5
Bytes Input       : 16801              Bytes Output     : 266
Duplicates Rcvd   : 0                  Data Retries     : 0
Decrypt Failed    : 0                  RTS Retries      : 0
MIC Failed        : 0
MIC Missing       : 0
```

42. **SHOW DOT11 ASSOCIATIONS STATISTICS**. This command shows the statistics for the associations. For example:

```
# show dot11 associations statistics
```

An example of the output is:

```
---- DOT11 Assocation Statistics -------------

On Interface Dot11Radio0:
cDot11AssStatsAssociated        :2
cDot11AssStatsAuthenticated     :2
cDot11AssStatsRoamedIn          :0
cDot11AssStatsRoamedAway        :0
cDot11AssStatsDeauthenticated   :1
cDot11AssStatsDisassociated     :1
cur_bss_associated              :1
cur_associated                  :1
cur_bss_repeaters               :0
cur_repeaters                   :0
cur_known_ip                    :1
dot11DisassociateReason         :2
dot11DisassociateStation        :0003.6dff.2a51
dot11DeauthenticateReason       :2
dot11DeauthenticateStation      :0003.6dff.2a51
dot11AuthenticateFailStatus     :0
dot11AuthenticateFailStation    :0000.0000.0000
```

43. **SHOW INTERFACES DOT11RADIO0 STATISTICS**. This command shows the statistics for the radio port. For example:

```
# show interfaces dot11radio0 statistics
```

An example of the output is:

```
  DOT11 Statistics (Cumulative Total/Last 5 Seconds):
RECEIVER                               TRANSMITTER
Host Rx Bytes:          41758 /   0    Host Tx Bytes:            135270 /   0
Unicasts Rx:              450 /   0    Unicasts Tx:                1258 /   0
Unicasts to host:         450 /   0    Unicasts by host:             11 /   0
Broadcasts Rx:           1247 /   0    Broadcasts Tx:             30329 /  49
Beacons Rx:                 0 /   0    Beacons Tx:                29773 /  49
Broadcasts to host:         0 /   0    Broadcasts by host:          556 /   0
Multicasts Rx:              0 /   0    Multicasts Tx:                77 /   0
Multicasts to host:         0 /   0    Multicasts by host:           77 /   0
Mgmt Packets Rx:         1247 /   0    Mgmt Packets Tx:            1247 /   0
RTS received:               0 /   0    RTS transmitted:               0 /   0
Duplicate frames:          65 /   0    CTS not received:              0 /   0
CRC errors:                57 /   0    Unicast Fragments Tx:       1258 /   0
WEP errors:                 0 /   0    Retries:                       0 /   0
Buffer full:                0 /   0    Packets one retry:             0 /   0
Host buffer full:           0 /   0    Packets > 1 retry:             0 /   0
Header CRC errors:        656 /   0    Protocol defers:               0 /   0
Invalid header:             0 /   0    Energy detect defers:         52 /   0
Length invalid:             0 /   0    Jammer detected:               0 /   0
Incomplete fragments:       0 /   0    Packets aged:                  0 /   0
Rx Concats:                 0 /   0    Tx Concats:                    0 /   0

RATE 11.0 Mbps
Rx Packets:               450 /   0    Tx Packets:                    8 /   0
Rx Bytes:                 41664 /    0    Tx Bytes:                   764 /    0
RTS Retries:                  0 /    0    Data Retries:                 0 /    0
```

The full list of key interfaces are:

```
# show interface ?
# show interface fa0
# show interface dot11radio0
# show interface bvi
```

44. **SHOW DOT11 NETWORK-MAP**. This command shows the radio network map. For example:

```
# show dot11 ?
# show dot11 network-map
# config t
(config)# dot11 network-map
(config)# exit
# show dot11 network-map
# show dot11 carrier ?
# show dot11 carrier busy
```

Which frequency is the most utilized:

45. A few other show commands are:

```
# show ip
# show ip ?
# show led
# show led ?
# show led flash
# show line
# show log
```

```
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns)
    Console logging: level debugging, 31 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 32 messages logged
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 35 message lines logged

Log Buffer (4096 bytes):

*Mar  1 00:00:04.103: soap_pci_subsys_init: slot 3 found radio
*Mar  1 00:00:04.405: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
reset
*Mar  1 00:00:05.429: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0,
changed state to down
```

```
*Mar  1 00:00:06.432: %LINK-3-UPDOWN: Interface FastEthernet0, changed state to up
*Mar  1 00:00:07.432: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0, changed state to up
*Mar  1 00:00:15.384: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0, changed state to down
*Mar  1 00:00:25.435: %SYS-5-RESTART: System restarted --
```

```
# show vlans
```

46. Some other show commands are:

```
# show aliases
# show caller
# show cca
# show class-map
# show clock
# show crash
# show dhcp ?
# show dot11 ?
```

```
  adjacent-ap        Display adjacent AP list
  antenna-alignment  Display recent antenna alignment results
  arp-cache          Arp Cache
  associations       association information
  carrier            Display recent carrier test results
  linktest           Display recent linktest results
  network-map        Network Map
  statistics         statistics information
```

```
# show dot11 adjacent-ap
# show dot11 arp-cache
# show dot11 associations
```

```
802.11 Client Stations on Dot11Radio0:

SSID [tsunami] :

MAC Address    IP address      Device        Name            Parent         State
0090.4b54.d83a 192.168.2.2     4500-radio    -               self           Assoc


Others:  (not related to any ssid)
```

```
# show dot11 carrier ?
# show dot11 carrier busy
# show dot11 network-map
# show dot11 statistics
# show dot11 statistics ?
# show dot11 statistics client-traffic
```

```
Clients:
3-0090.4b54.d83a pak in 372 bytes in 31151 pak out 3 bytes out 262
      dup 0 decrpyt err 0 mic mismatch 0 mic miss 0
      tx retries 0 data retries 0 rts retries 0
      signal strength 43 signal quality 83
```

47. For radio tests:

```
# dot11 ?
# dot11 dot11radio0 ?
# dot11 dot11radio0 carrier ?
# dot11 dot11radio0 carrier busy
# dot11 dot11radio0 linktest
```

4.5 Tutorial 4 (Authentication and Encryption)

48. **LOCAL ATHENTICATION**. Large networks require a separate RADIUS server to authenticate nodes. For smaller networks it is possible to run a local authenticator. The steps are:

- The local WAP is defined as a RADIUS-SERVER (radius-server local).
- The WAP is defined as a NAS (Network Authentication Server).
- Local users are defined, along with passwords (up to 50 users can normally be created).

```
# config t
(config)# aaa new-model
(config)# radius-server ?
(config)# radius-server local
(config-radsvr)# ?
(config-radsvr)# nas 192.168.0.1 key fred
(config-radsvr)# user michael password none
(config-radsvr)# exit
(config)# exit
# show radius local-server statistics
```

Sets the shared key between devices.

Examine the running-config. Which lines have been added related to AAA?

Examine the running-config. How has the password been changed for the user?

To remove AAA:

```
# config t
(config)# no aaa new-model
(config)# exit
```

49. **WEP (40-bit)**. WEP is the basic encryption method used for wireless. Unfortunately the 40-bit version can be cracked within 5 hours, but it can be used as a barrier to stop users from initially connecting to the WAP. For the key to be generated the user must define a 10-digit hexadecimal code:

```
# config t
(config)# int dot11radio0
```

```
(config-if)# encryption ?
(config-if)# encryption mode wep optional
(config-if)# encryption key 1 size 40bit 1122334455 transmit-key
(config)# exit
```

Key number 1 (three other keys are possible)

Key

Examine the running-config. How has the encryption key been changed?

How many digits does the hashed encryption key have?

Note, as 64-bit expects 10 hexadecimal digits, the following error results if the key is less than or more than 10 hexadecimal digits it will not accept the key.

Try entering a 40-bit WEP key which is not 10 digits. What message does the system show?

The basic format of the encryption command is:

```
[no] encryption
[vlan vlan-id ]
key 1-4
size {40bit | 128Bit}
encryption-key
[transmit-key]
```

50. **WEP (128-bit)**. The same can be done for 128-bit encryption, which is more secure. In this case we require 26 hexadecimal digits.

```
# config t
(config)# int dot11radio0
(config-if)# encryption mode wep optional
(config-if)# encryption key 1 size 128bit 12345678901234567890123456
   transmit-key
(config)# exit
```

Examine the running-config. How has the encryption key been changed?

How many digits does the hashed encryption key have?

Try entering a 128-bit WEP key which is not 26 digits. What message does the system show?

51. Set authentication to EAP:

```
# config t
(config)# int dot11radio0
(config-if)# ssid fred
(config-if-ssid)# ?
(config-if-ssid)# authentication ?
(config-if-ssid)# authentication network-eap joe
(config-if-ssid)# exit
```

52. Set key management:

```
# config t
(config)# int dot11radio0
(config-if)# ssid fred
(config-if-ssid)# ?
(config-if-ssid)# authentication key-management ?
(config-if-ssid)# authentication key-management wpa
(config-if-ssid)# wpa-psk ?
(config-if-ssid)# wpa-psk ascii ?
```

53. Set authentication to LEAP:

```
# config t
(config)# int dot11radio0
(config-if)# ssid fred
(config-if-ssid)# ?
(config-if-ssid)# authentication ?
```

54. Set authentication to shared:

```
# config t
(config)# int dot11radio0
(config-if)# ssid fred
(config-if-ssid)# ?
(config-if-ssid)# authentication shared ?
(config-if-ssid)# authentication shared eap ?
(config-if-ssid)# authentication shared eap eap1
```

55. Set authentication to client:

```
# config t
(config)# int dot11radio0
(config-if)# ssid fred
(config-if-ssid)# ?
(config-if-ssid)# authentication client ?
(config-if-ssid)# authentication client username ?
(config-if-ssid)# authentication client username fred password bert
```

56. Enable an encryption key:

```
# config t
(config)# int dot11radio0
(config-if)# encryption ?
(config-if)# encryption mode ?
(config-if)# encryption mode wep ?
(config-if)# encryption mode cipher tkip wep128
(config-if)# encryption key ?
(config-if)# encryption key 3 size 128bit 12345678901234567890123456
transmit-key
```

57. TACACS+.

```
# config t
(config)# aaa new-model
(config)# tacacs-server host 192.168.0.10
(config)# tacacs-server key mypass
```

4.6 Tutorial 5 (Show file systems and controllers)

58. To show file system information:

```
# show file ?
# show file descriptions
# show file info
# show file info ?
# show file info bs:
# show file info flash:
# show file info ftp:
# show file systems
```

A sample run is:

```
File Systems:

     Size(b)     Free(b)      Type  Flags  Prefixes
*    7741440     4049408     flash     rw   flash:
           -           -    opaque     rw  bs:
     7741440     4049408   unknown     rw   zflash:
       32768       32716     nvram     rw   nvram:
           -           -   network     rw   tftp:
           -           -    opaque     rw   null:
           -           -    opaque     rw   system:
           -           -    opaque     ro   xmodem:
           -           -    opaque     ro   ymodem:
           -           -   network     rw   rcp:
           -           -   network     rw   ftp:
           -           -   network     rw   scp:
```

```
# show hosts
# show html
# show html ?
# show iapp
# show iapp ?
# show iapp rogue-ap-list
# show iapp standby-parms
# show iapp standby-status
# show iapp statistics
# show idb
```

59. To list the directory:

```
# dir
```

```
Directory of flash:/

    2  -rwx          27   Mar 01 1993 00:26:58  private-config
    4  -rwx          97   Mar 01 1993 00:00:25  env_vars
    6  drwx         384   Jan 01 1970 00:12:27  c1200-k9w7-mx.122-13.JA2

7741440 bytes total (4049408 bytes free)
```

60. To list the boot:

```
# show boot
```

```
BOOT path-list:
Config file:          flash:/config.txt
Private Config file:  flash:/private-config
Enable Break:         yes
Manual Boot:          no
HELPER path-list:
NVRAM/Config file
      buffer size:    32768
```

4.7 Tutorial 6 (Security settings)

61. To generate a public and a private key, the domain name must first be set:

```
# config t
(config)# ip domain-name test.com
```

62. Next a username can be setup with a password for the login:

```
# config t
```

```
(config)# username ?
(config)# username fred ?
(config)# username fred password bert
(config)# exit
# show running
```

63. Telnet is a weak protocol in that it sends userIDs and passwords in a plain text format. An improved protocol is SSH, which encrypts the transmitted data. To generate a key:

```
(config)# crypto key generate ?
(config)# crypto key generate rsa ?
```

What is the default RSA key size?

If the domain-name is not set the result will be:

% Please define a domain-name first.

64. To show the crypto:

```
# show crypto ?
```

```
  ca      Show certification authority policy
  engine  Show crypto engine info
  key     Show long term public keys
  mib     Show Crypto-related MIB Parameters
```

```
# show crypto key ?
# show crypto key mypubkey ?
# show crypto key mypubkey rsa
```

```
% Key pair was generated at: 00:14:48 UTC Mar 1 1993
Key name: ap.test.com
 Usage: General Purpose Key
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00B27F21 A211CE00
  A55D2E0C EBB17A00 9907759D C382C96F A18E4E9D CE6A2F38 6B027304 23AE59BE
  DB51CD68 BB2C9806 6E3AC744 771C55D7 F674C948 0C958D76 7D020301 0001
% Key pair was generated at: 00:14:49 UTC Mar 1 1993
Key name: ap.test.com.server
 Usage: Encryption Key
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00A63184 72A118C4
  24F17831 59CDCD87 00503594 A168D881 83E444CE E9C63D63 40D2BB26 6887503F
  5378ADB8 BF32FE06 B8910BC8 0FB0BAE1 3D60FA35 F17220D1 7C8BDA55 B96266E6
  F8BA639B FEAA5936 6ABF3C82 AD93CC73 E960E3D8 53640AE1 7B020301 0001
```

65. A key to enhance the security of the system is to limit the number of retries of the password, and also to provide a time-out for the session. The following sets the time-out to 15 seconds, and the number of retries to 3:

```
# config t
(config)# ip ssh ?
(config)# ip ssh time-out ?
(config)# ip ssh time-out 15
(config)# ip ssh authentication-retries ?
(config)# ip ssh authentication-retries 3
```

What is the maximum timeout value?

What is the number of authentication-retries?

66. A key to enhance the security of the system is to limit the number of retries of the password, and also to provide a time-out for the session. The following sets the time-out to 15 seconds, and the number of retries to 3:

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

Which transport protocols are available?

67. Along with setting the SSH parameters it is a good idea to encrypt passwords:

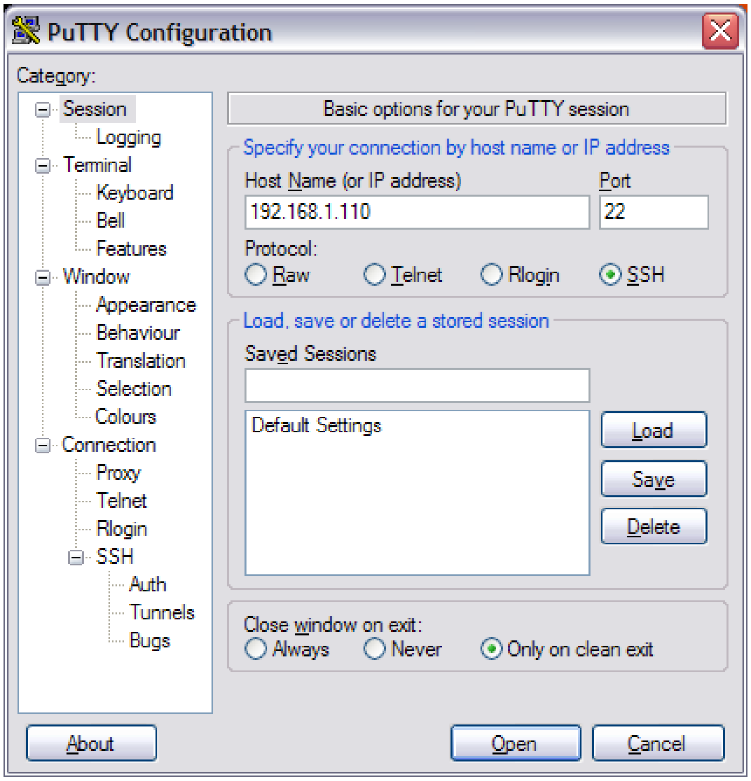
```
# config t
(config)# service ?
(config)# service password-encryption
```

To get rid of it:

```
# config t
(config)# no service password-encryption
```

4.8 Creating a TELNET connection

Once the WAP has been setup, it can then be connected to by the client using SSH. The following shows an example connection using PuTTY:



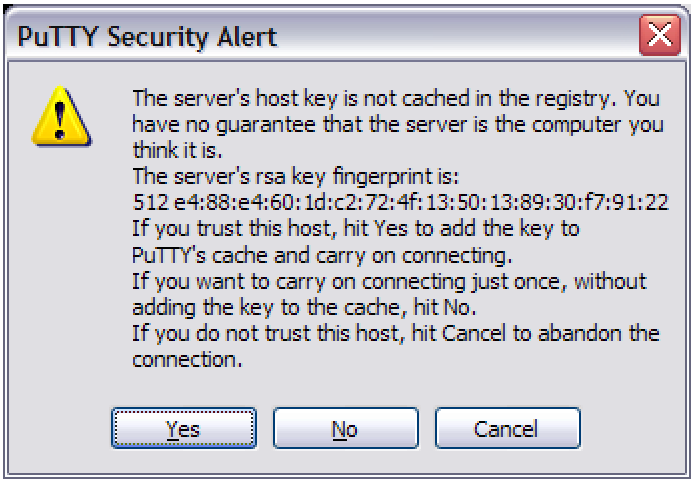
Host Name (or IP address): 192.168.1.110

Port: 22

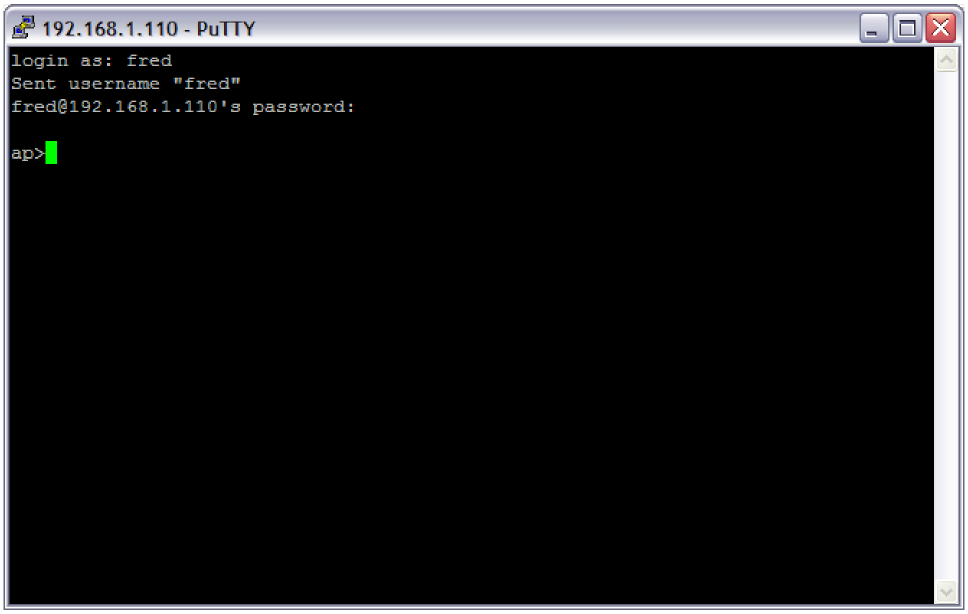
Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Close window on exit: ○ Always ○ Never ● Only on clean exit

after which the following alert is shown on the client:



The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa key fingerprint is:
512 e4:88:e4:60:1d:c2:72:4f:13:50:13:89:30:f7:91:22
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.



```
login as: fred
Sent username "fred"
fred@192.168.1.110's password:

ap>
```

To show ssh connections:

```
# show ssh
```

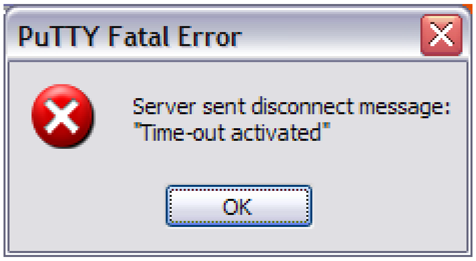
A sample result is:

```
Connection        Version Encryption        State                     Username
 5                1.5     3DES              Session started           fred
```

68. Often the creation of a WWW server on the WAP can create a security issue. To disable the WWW server:

```
# config t
(config)# no ip http server
```

If a time-out occurs, the client shows something like:



Server sent disconnect message:
"Time-out activated"

4.9 Tutorial 7 (Logging and SNMP)

69. To setup that the wireless access point should send system messages to a syslog server (for centralized monitor):

```
# config t
(config)# logging ?
(config)# logging 10.11.12.13
```

This uses the UDP port 514 to send the messages.

70. To enable traps on logging:

```
# config t
(config)# logging trap ?
(config)# logging trap debugging
```

Outline some of the traps that are available?

71. To show the logging:

```
# show logging
```

Outline some of the contents of the log?

72. To activate service timestamps and sequence numbers on the WAP:

```
# config t
(config)# service timestamps log uptime
(config)# service sequence-numbers
```

4.10 SNMP configuration

73. SNMP. The snmp-server community command is used to initialise SNMP. For example to define the read-only string to public:

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

or for read-write access use RW instead of RO. The community access string (in this case, public) acts as a password for the access to the SNMP information. To setup the SNMP contact:

```
(config)# snmp-server contact fred smith
```

and to set the location:

```
(config)# snmp-server location room c27
```

To enable SNMP traps so that all the data is monitored:

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

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

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

Go back to the user executive mode with the command exit

Show the main system configuration with show running-config.

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
```

To show the currently pending SNMP requests:

```
# show snmp pending
```

To show the SNMP sessions:

```
# show snmp sessions
```

4.11 Tutorial 8 (Firewalls and VLANs)

74. Initially an encryption key is generated for the VLAN:

```
# config t
(config)# int dot11radio0
(config-if)# encryption ?
(config-if)# encryption vlan ?
(config-if)# encryption vlan 104 ?
(config-if)# encryption vlan 104 key ?
(config-if)# encryption vlan 104 key 1 size 40bit 7 4604392EE307 transmit-
key
(config-if)# encryption vlan 104 mode wep mandatory
```

75. Next the radio devices can be associated with a VLAN using:

```
# config t
(config)# int dot11radio0
(config-if)# ssid fred
(config-if-ssid)# ?
(config-if-ssid)# vlan ?
(config-if-ssid)# vlan 104
```

Check the running-config to see if the VLAN is set. Is it there?

76. Access Control Lists (ACLs) allow for incoming and outgoing data to be filtered, and are used to implement firewalls. To deny access from the incoming dot11radio0 port to every host on the 156.1.1.0 subnet:

```
(config)# access-list ?
(config)# access-list 1 ?
(config)# access-list 1 deny 156.1.1.0 0.0.0.255
(config)# interface dot11radio0
(config-if)# ip access-group 1 in
(config-if)# exit
(config)# exit
# show running
```

To deny access to port 888:

```
(config)# access-list 100 deny tcp 192.5.5.0 0.0.0.255 any eq 8888 log
(config)# access-list 100 deny udp 192.5.5.0 0.0.0.255 any eq 8888 log
(config)# interface e0
(config-if)# ip access-group 100 out
```