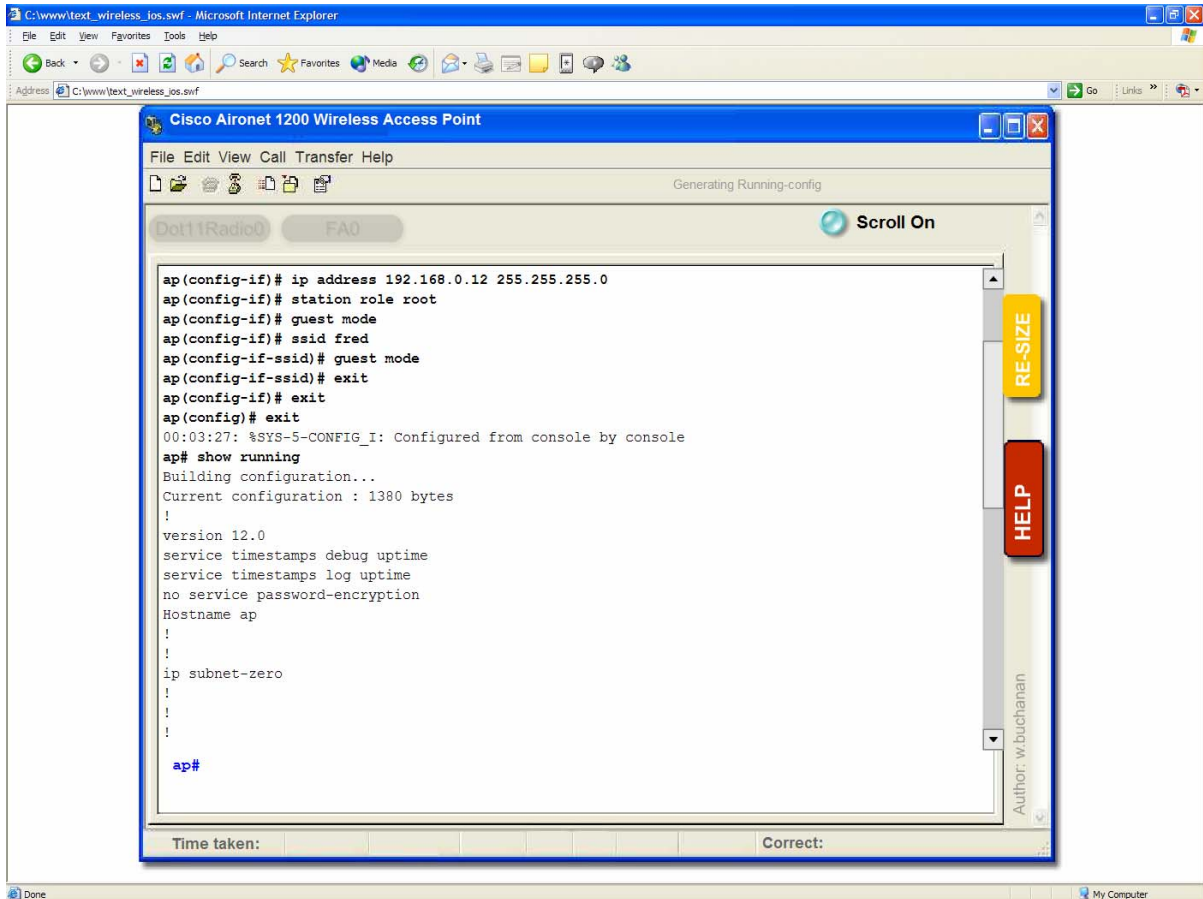


Wireless Access Point (WAP) Emulator (Aironet 1200 - Cisco IOS Version 12)

WWW page: <http://network-emulators.com> [then Select Wireless IOS]



Background

In a wireless system the main elements of the configuration are (Figure 1):

- **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 interoperability 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.

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:

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 stored in the Flash Memory:

Product/Model Number:

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 fred 172.14.10.11
(config)# ip host bert 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
```

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
```

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
Signal Quality : 81 %
Power-save    : Off
Connected for : 913 seconds
Activity Timeout : 31 seconds
Last Activity  : 28 seconds ago

Packets Input : 143
Bytes Input   : 16801
Duplicates Rcvd : 0
Decrypt Failed : 0
MIC Failed    : 0
MIC Missing   : 0

Packets Output : 5
Bytes Output   : 266
Data Retries   : 0
RTS Retries    : 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 Association 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_repeater             :0
cur_repeater                  :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 decrypt 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
```

Tutorial 4 (Authentication and Encryption)

48. **LOCAL AUTHENTICATION.** 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
```

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	nvrn	rw	nvrn:
	-	-	network	rw	tftp:
	-	-	opaque	rw	null:
	-	-	opaque	rw	system:
	-	-	opaque	ro	xmodem:
	-	-	opaque	ro	yndem:
	-	-	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
```

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:

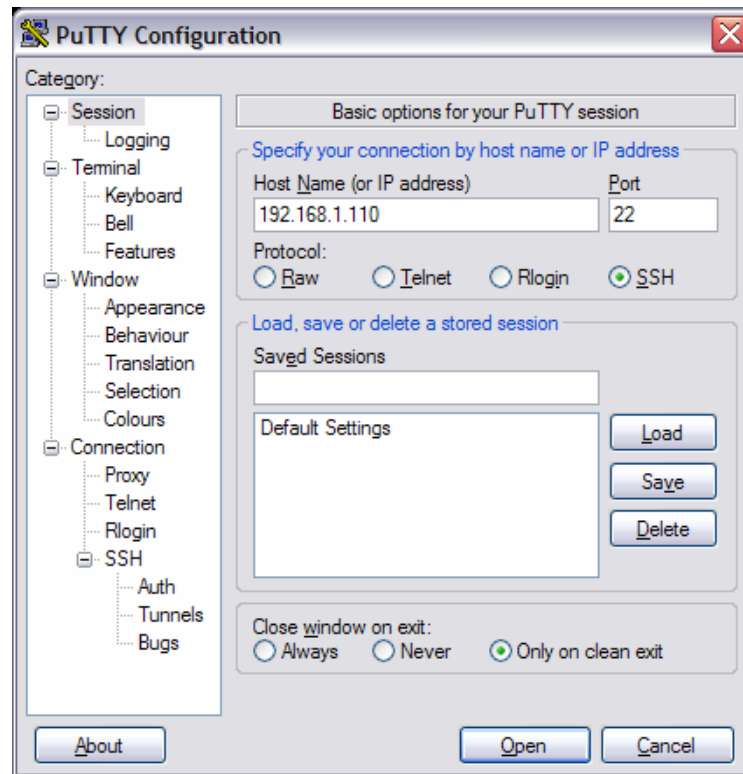
```
# config t
(config)# service ?
(config)# service password-encryption
```

To get rid of it:

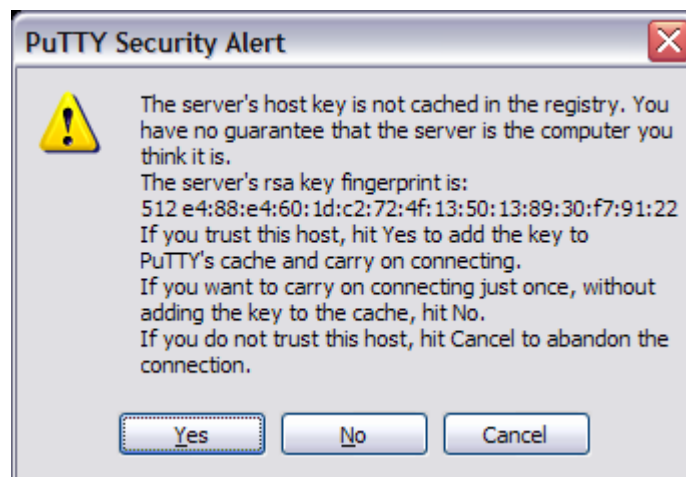
```
# config t
(config)# no service password-encryption
```

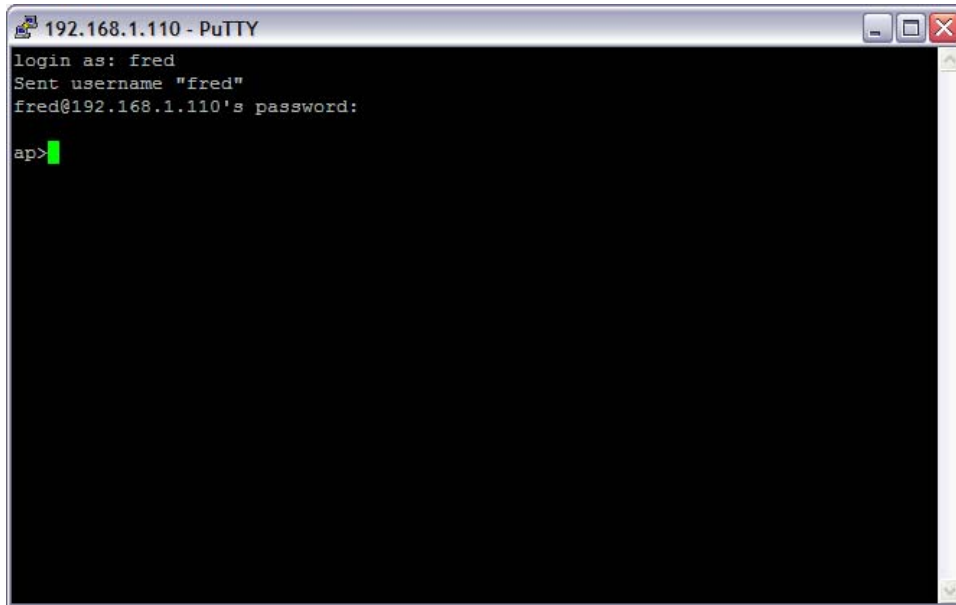
Creating a TELNET connection

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:



after which the following alert is shown on the client:





To show ssh connections:

```
# show ssh
```

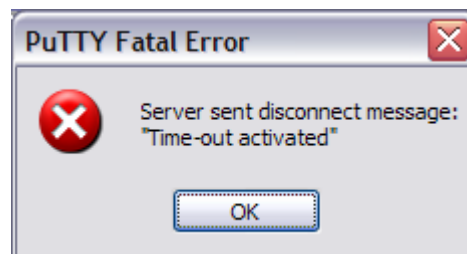
A sample result is:

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:



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
```

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
```

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
```

Copyright information

© William Buchanan 2004

All rights reserved. No reproduction, copy or transmission of this publication may be made without written permission.

No paragraph of this publication may be reproduced, copied or transmitted save with written permission or in accordance with the provision of the Copyright, Designs and Patents Act 1988, or under the terms of any licence permitting limited copying issued by the Copyright Licensing Agency, 90 Tottenham Court Road, London W1T4LP.

Any person who does any unauthorised act in relation to this publication may be liable to criminal prosecution and civil claims for damages.

The author(s) have asserted their rights to be identified as the author(s) of this work in accordance with the Copyright, Designs and Patents Act 1988.