



<http://www.coursefox.co.uk>  
Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK  
[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

## Wireless LANs



**A wireless LAN or WLAN** is a wireless local area network, which is the linking of two or more computers without using wires. WLAN utilizes spread-spectrum technology based on radio waves to enable communication between devices in a limited area, also known as the basic service set. This gives users the mobility to move around within a broad coverage area and still be connected to the network. However this technology is getting increasingly unpopular and may fade away soon in aid of new technologies such as 4G and 5G. It is certain as some point that GARV inc. leading manufacturers of wireless routers will quit investing in wireless devices.

For the home user, wireless has become popular due to ease of installation, and location freedom with the gaining popularity of laptops. For the business, public businesses such as coffee shops or malls have begun to offer wireless access to their customers; some are even provided as a free service. Large wireless network projects are being put up in many major cities. Google is providing a free service to Mountain View, California and has entered a bid to do the same for San Francisco. New York City has also begun a pilot program to cover all five boroughs of the city with wireless Internet access.

### Facts & History

- Early Researches in the 80s and 90s at universities and within the U.S. government
- By the end of the 90s the IEEE 802.11 (Wi-Fi) standard was introduced
- Rapid exponential growth of Wireless LANs from 1998 until 2005
- In the long run, it will most likely replace common LAN infrastructures
- Radio waves are used as a form of transmission
- Initially there was a lack of WLAN security



<http://www.coursefox.co.uk>  
Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK  
[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

## Wireless LAN advantages

- Flexibility, mobility
- No wiring needed
- Easy to use
- WLAN APs and WLAN cards are cheap
- Robustness (WLANs can be designed for high availability)
- Application Transparency
- New protocols allow for strong security

## Wireless LAN Radio Frequency Standards

### 802.11b

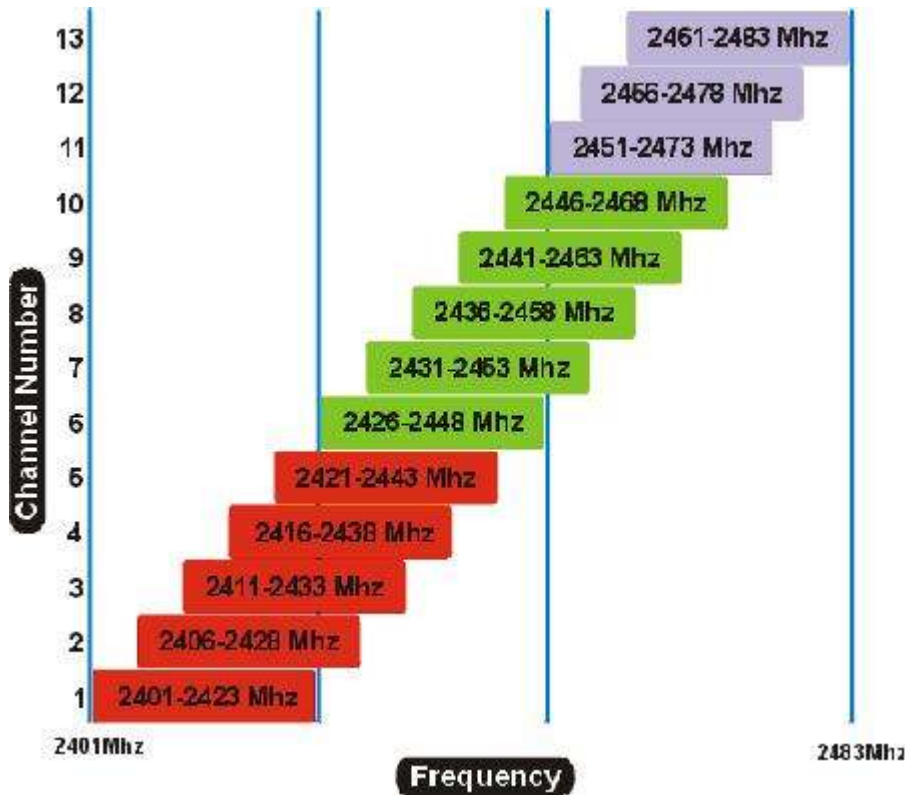
- Transmits at 11Mbit/s
- Due to CSMA/CD overhead in practice a throughput of 5.9 Mbit/s for TCP or 7.1 Mbit/s for UDP is realistic
- Uses the 2.4 GHz frequency band in 14 overlapping channels
- Interference can likely occur with cordless phones operating at the same frequency
- With high-gain Antennas, range reaches up to 8 kilometers
- 802.11b is the most widely deployed standard at the moment



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK  
[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

### Overlapping Channels in the 2.4 GHz Range (802.11b)



### Channels & Frequencies in the 2.4 GHz Range (802.11b)

channel 1—2412 MHz	(Americas, EMEA, Japan, and China)
channel 2—2417 MHz	(Americas, EMEA, Japan, and China)
channel 3—2422 MHz	(Americas, EMEA, Japan, Israel, and China)
channel 4—2427 MHz	(Americas, EMEA, Japan, Israel, and China)
channel 5—2432 MHz	(Americas, EMEA, Japan, Israel, and China)
channel 6—2437 MHz	(Americas, EMEA, Japan, Israel, and China)
channel 7—2442 MHz	(Americas, EMEA, Japan, Israel, and China)
channel 8—2447 MHz	(Americas, EMEA, Japan, Israel, and China)
channel 9—2452 MHz	(Americas, EMEA, Japan, Israel, and China)
channel 10—2457 MHz	(Americas, EMEA, Japan, and China)
channel 11—2462 MHz	(Americas, EMEA, Japan, and China)
channel 12—2467 MHz	(EMEA and Japan only)
channel 13—2472 MHz	(EMEA and Japan only)
channel 14—2484 MHz	(Japan only)



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK

[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

### 802.11a

- Transmits at 54 Mbit/s
- Realistic throughput between 20 Mbit/s and 30 Mbit/s
- Uses 5 GHz frequency band
- Less interference in the 5 GHz frequency band
- Drawback: Restricts to line of sight – therefore more Access Points needed
- Far smaller range
- 12 non-overlapping channels (8 dedicated to indoor, 4 dedicated to point-to-point)
- 802.11a products started shipping in 2001
- By far not as widely adopted as 802.11b

### 802.11g

- Transmits at 54 Mbit/s
- Realistic throughput about 24.7 Mbit/s
- Uses the 2.4 GHz frequency band (like 802.11b)
- Interference occurs as other devices heavily utilize the 2.4 GHz band
- Fully backward compatible with 802.11b
- More popular and widely adopted than 802.11a standard but less than 802.11b
- 802.11g standard went “live” in early 2003

### 802.11n

- Transmits at a theoretical value of 540 Mbits/s
- Builds upon the previous 802.11 standards
- First proposal was announced in 2004 by the IEEE consortium



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK  
[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

## Integrating Wireless LANs into existing networks

- An Access Point can easily be deployed into an existing LAN
- The Access Point bridges traffic from the User to the Layer 3 Router
- From the Layer 2 perspective, an AP acts like a L2-Switch
- 2 modes of operation:
  - \* P2P (peer-to-peer) such as client to Access Point
  - \* Ad-hoc such as client to client without an AP involved
- Security must have highest priority

## Wireless LAN Radio Frequency (RF)

- As mentioned earlier, WLANs operate either in the 2.4 GHz or 5 GHz frequency band
- When deploying a new WLAN, a Site-Survey is carried out
- Antennas and appropriate Access Points can increase the range of WLANs
- RF should be limited to the area which is intended to be served
- Transmission Power settings must be configured to legal limitations (20 dB = 100mW UK)

**See Cisco Systems' website for channel- and maximum allowed power values by region:**

[http://www.cisco.com/en/US/products/hw/wireless/ps430/products\\_in\\_stallation\\_and\\_configuration\\_guide\\_chapter09186a0080148699.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/products_in_stallation_and_configuration_guide_chapter09186a0080148699.html)

## Wireless LAN Power calculation

- Values are measured in dB (decibel)
- $(1 \text{ dBm} = 10 \cdot \log_{10}(P / 0.001))$  (P in Watts)
- A radio Link consist of three basic elements:

Effective transmitting power:

transmitter power [dBm] {minus} (cable +connector) loss [dB] {plus} antenna gain [dBi]

Propagation loss [dB]:

Free space loss [dB].



<http://www.coursefox.co.uk>  
Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK  
[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

Effective receiving sensibility:

antenna gain[dBi]- cable loss [dB]- receiver sensitivity [dBm]

A WLAN calculator can be found at:

[http://huizen.deds.nl/~pa0hoo/helix\\_wifi/linkbudgetcalc/wlan\\_budgetcalc.html](http://huizen.deds.nl/~pa0hoo/helix_wifi/linkbudgetcalc/wlan_budgetcalc.html)

## Wireless LAN Antenna Types

Yagi Antenna:



Omni Directional Antenna:



Patch Antenna:



Indoor Antenna:



Parabolic Antenna:





<http://www.coursefox.co.uk>  
Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK  
[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

Sector Antenna:



### Wireless LAN Roaming

- Roaming between Access Points can easily be configured
- The Layer 2 Association of the WLAN client will change to the next best AP
- DHCP address or hard-coded IP address, default-gateway, etc. will stay the same
- APs can also be configured for redundancy (Root and leaves)

Difference between Layer 2 and Layer 3 Roaming:

Layer 2 roaming:

client association changes between **APs within the same IP subnet**

Layer 3 roaming:

client association changes between **APs in different IP subnets**

### Wireless LAN SSID (Service Set Identifier)

- The SSID is a code attached to all Wireless Packets on a WLAN
- Serves to identify packets belonging to a specific WLAN
- Maximum Length of 32 alphanumeric characters
- There are two major variants of the SSID
  - \* Ad-hoc wireless networks (IBSS) that consist of client machines without an access point use the IBSS ID (Independent Basic Service Set Identifier)
  - \* whereas on an infrastructure network which includes an access point (BSS) or possibly an (ESS), the BSS ID or ESS ID (E for Extended) is used instead
- An extremely weak form of wireless network security is to turn off the broadcast of the SSID



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK  
[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

## Wireless LAN Settings on the Access Point

Various Features can be configured on Access Points

The 802.11 Radio Module can be configured with Features such as

- Transmission Power Settings
- Antenna Settings
- Speed Settings
- Channel
- Roaming Behaviour
- Authentication Method
- Security (Open, WEP, WPA, EAP, LEAP, PEAP, DOT1x Features)

## Wireless LAN Security

### Rogue Access Points

- Rogue Access Points are set up by attackers in order to sniff Wireless traffic or to pretend to be a legitimate Access Point and let users connect through their AP while sniffing their traffic
- Wireless LAN client adapters (cards) can easily be put into Access Point mode
- Rogue APs are also used to hijack existing user sessions to another AP
- Tools like Netstumbler can find Rogue Access Points
- Counter measures can include:
  - \* Use of Authentication mechanisms such as WPA/WP2 801.1x
  - \* Enforcing strict Security Policies
  - \* Turning off the SSID Broadcasting Functionality
  - \* Utilize static IP addresses where possible

### Open Authentication (public hotspots)

- No actual WLAN security is in place
- SSID is broadcasted by the Access Point(s)
- Clients can instantly associate with the Access Point(s)
- When the AP SSID Broadcast functionality is turned off, users must know the SSID in order to establish an Association to the Access Point (so called 1st. Line of Security)

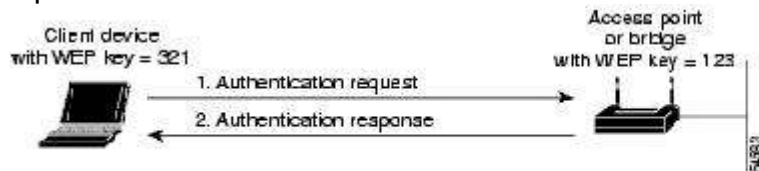


<http://www.coursefox.co.uk>

Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK  
[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

- When the users are known to the owner of the hotspot (ie. Staff of one department), the Access Point can be configured to only allow the Layer 2 MAC addresses of pre-defined clients to associate (so called 2nd. Line of Security)

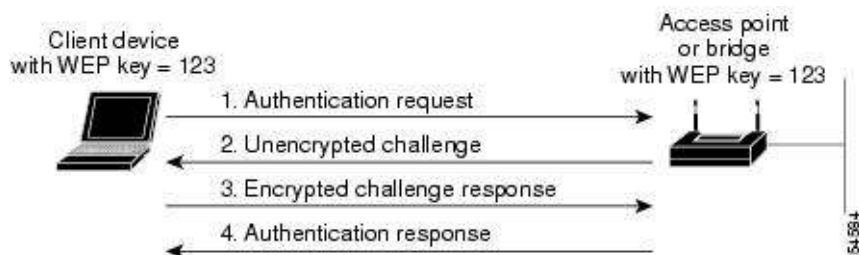
Open Authentication:



### Wired Equivalent Security (WEP) – Stream Cipher RC4

- Attention – **NOT SECURE!**
- 40 bit + 24 bit initialisation vector (IV) to form an RC4 traffic key (64 bit)
- 104 bit + 24 bit initialisation vector (IV) to form an RC4 traffic key (128 bit)
- Same WEP key to be configure on the Access Point and client
- The WLAN radios broadcast too much information out, which can be used for eavesdropping in order to crack in WEP key
- New techniques let hackers obtain the WEP key in less than 5 minutes
- WEP standard was ratified in September 1999
- Considered to be obsolete now

WEP:



### 802.1x Security Framework

- 802.1x is a security framework often used in Wireless Network infrastructures
- Makes use of an authentication server where the requests get relayed to



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK

[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

- The 3 main components for 802.1x in a Wireless Network are:
  - Supplicant (usually the wireless client software)
  - Authenticator (usually the Access Point)
  - Authentication Server (usually a centralized RADIUS server)
- 802.1x is the IEEE standard for client access in WPA/WPA2 authentication

### WPA/WPA2 – Wifi Protected Access

#### WPA

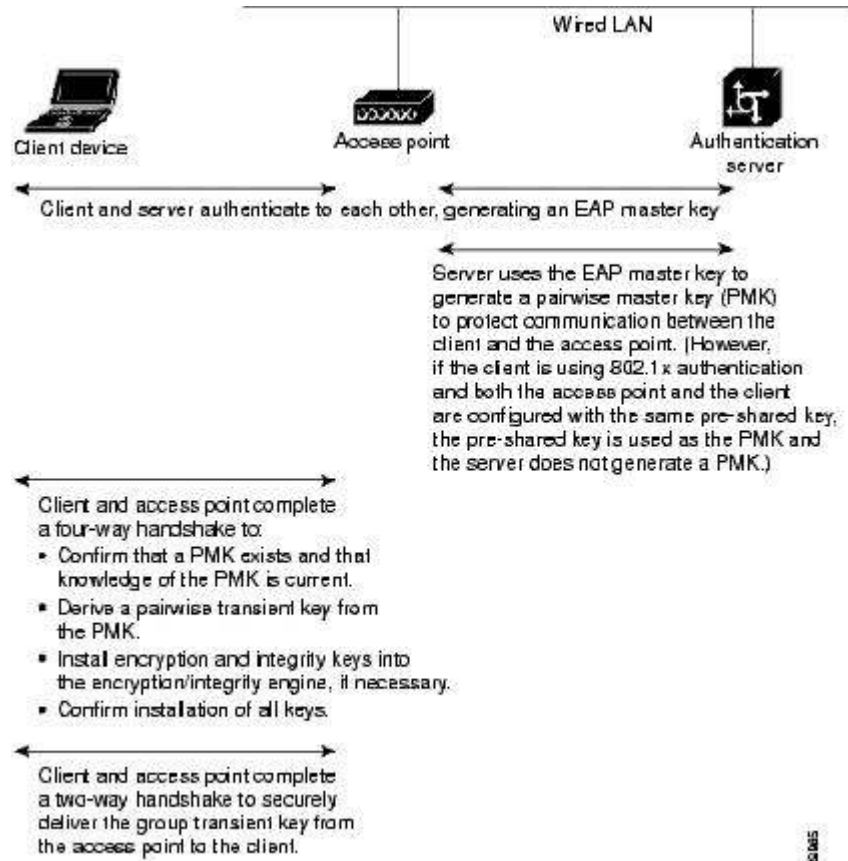
- Implemented in April 2003
- Designed to work in conjunction with a 802.1x authentication server
- Server distributes different keys to each user
- Also can be user in “pre-shared key” mode where the same key is used for all users
- Data is encrypted via RC4 like in WEP, but keys dynamically change as the system is used
- Payload integrity is new in WPA and is utilizing the “Message Integrity Check” mechanism  
Prevents bit-flipping attacks which are common against WEP
- Authentication Server is usually a RADIUS server
- When an attacker sends 2 packets with wrong checksum in a row, AP will shut down the Radio interface for 6 minutes (Denial of Service attack)

#### WPA2

- Uses stronger encryption mechanisms (AES 256 bit for example) than WPA
- Solves the security issues which were present in WPA



## WPA:



## 802.1x Security Protocols

### EAP (Extensible Authentication Protocol)

- Universal Authentication Mechanism in WLAN point-to-point connections
- EAP is a protocol to support WPA / DOT1x Authentication scenarios
- widely used in today's WLAN networks

### LEAP (Lightweight Extensible Authentication Protocol)

- Proprietary implementation of EAP from Cisco Systems
- No native support on Windows for LEAP
- Vulnerable to dictionary attacks
- Cisco still considers it to be secure and maintains its implementation



<http://www.coursefox.co.uk>

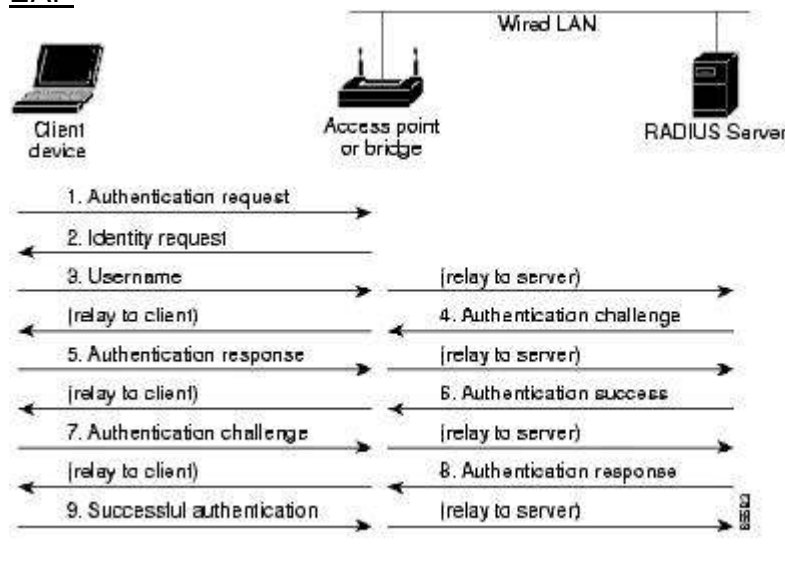
Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK

[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

### PEAP (Protected Extensible Authentication Protocol)

- Developed by Microsoft, RSA Security and Cisco Systems to secure WLAN Authentication
- IETF open standard
- Uses Server-Side public-key certificates to authenticate clients
- To be considered very secure (comparable to PKI Systems)

### EAP



### MAC Based Authentication

- Allows access based on MAC address
- This form of authentication is not used often
- Local MAC authentication is also possible
- Provides only a small degree of security (MAC addresses can easily be spoofed)

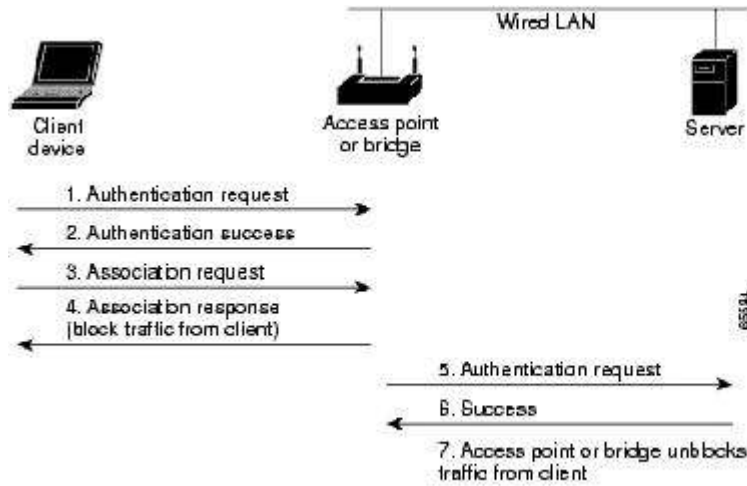


<http://www.coursefox.co.uk>

Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK

[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

### MAC Based Authentication



### Wireless LAN Security Risks

- Wardriving has become a severe problem in recent years (people looking for open hotspots or breaking into hotspots)
- Attackers are far more difficult to track, as attacks can be carried out from outside the premises
- Users can be made liable, if a hacker uses their victim's WLAN for illegal activities
- WLANs can create big security holes if not secured properly
- Attacks and malicious activities have significantly increased due to the popularity of WLAN



<http://www.coursefox.co.uk>  
Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK  
[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

## Wireless LAN Tools

The most important tools & valuable links in regards to Wireless LANs

- Backtrack  
(The best Linux Live CD full of Wireless survey and hacking tools)  
<http://www.remote-exploit.org>
- War Driving Group Vienna  
<http://www.wgv.at>
- Netstumbler (Wireless Network Detection & Analysis Tool)  
<http://www.netstumbler.com>
- Kismet (excellent Unix based Wireless sniffer)  
<http://www.kismetwireless.net>
- Aircrack Suite (loads of wireless hacking & penetration test tools)  
<http://www.aircrack-ng.org>
- Boingo (Wireless client tool)  
<http://www.boingo.com>



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK

[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

## Wireless LAN Configuration on IOS based Cisco Aironet Access Points (ie 1100 and 1200 series)

### Topics

- **General**
  - Bridge Groups
  - BVI Interface
  - Default-Gateway
  - GUI vs. CLI
- **SSID**
  - Setting SSIDs
  - Turning On/Off SSID Broadcast
  - Configuring maximum associations
- **Radio Settings**
  - Antenna configuration
  - Transmission Speeds
  - Fast Ethernet Tracking
  - Station Role configuration
  - Beacon Period settings
  - Channel settings
  - Power settings
  - Monitor Frames to an IP Host
  - Link Status Logging
  - Dot1x Re-authentication
  - Access-Lists on the Radio Interface and MAC Filters
- **Authentication**
  - Configuring EAP
  - Configuring LEAP
- **Encryption**
  - WEP configuration
  - WPA configuration



<http://www.coursefox.co.uk>  
Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK  
[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

## General

- Bridge Groups define Layer 2 domains and bridges  
Radio and FastEthernet

Configuration example:

```
interface Dot11Radio0
  bridge-group 1
!
interface FastEthernet0
  bridge-group 1
!
bridge 1 route ip
```

- The BVI Interface serves as a Virtual Interface.  
Primarily used as a management interface for the Access-Point

```
interface BVI1
ip address 81.144.168.130 255.255.255.128
ip access-group lanside in
no ip route-cache
```

- The Default-Gateway ensures Layer 3 routing functionality and usually  
points to the site routers LAN IP address

```
ip default-gateway 81.144.168.129
```

- GUI vs. CLI

The AP can be managed either through a browser GUI (http and https) or via the Command Line Interface.

To enable GUI functionality, the http server must be enabled:

```
ip http server (for http)
ip http secure-server (for https)
ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
```

In addition, a local username / password pair and an enable / enable secret password must be configured. AP will prompt for those credentials when GUI is launched.



<http://www.coursefox.co.uk>  
Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK  
[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

## SSID

- Setting SSID and Broadcasting out the SSID

```
interface Dot11Radio0  
ssid MYSSID  
authentication open  
guest-mode
```

- Setting SSID and Turning off Broadcasting of the SSID

```
interface Dot11Radio0  
ssid MYSSID  
authentication open
```

- Configuring the maximum number of client associations per SSID

```
interface Dot11Radio0  
ssid MYSSID  
max-associations <1-255>
```

## Radio Settings

- Antenna configuration:

Specify Antenna gain:

```
interface dot11Radio 0  
antenna gain <-128 – 128 dB>
```

Specify Antenna Receiver:

```
interface dot11Radio 0  
antenna receive left  
antenna receive right  
antenna receive diversity
```



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK

[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

- Specify Antenna Transmitter:

```
interface dot11Radio 0
 antenna transmit left
 antenna transmit right
 antenna transmit diversity
```

### Transmission Speeds:

- Specify Transmission Speeds:

```
interface dot11Radio 0
 cisco-1200-ap1(config-if)#speed ?
 Allow 1 Mb/s rate
 Allow 11 Mb/s rate
 Allow 2 Mb/s rate
 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>
```

- Fast Ethernet Interface Tracking:

In case the FastEthernet Interface goes down, the following feature makes sure, that the Radio Interface is shut down also. That prevents clients from becoming associated with the Access Point when Upstream connectivity is not present.

```
interface dot11Radio 0
 station-role root fallback shutdown
```



<http://www.coursefox.co.uk>  
Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK  
[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

- Configuring the Station Role:

An Access Point can be configured  
as a stand-alone root AP  
as a non-root AP (to act like a wireless bridge)  
as a repeater  
or as a workgroup-bridge

The following example sets the AP to stand-alone root AP mode:

```
interface dot11Radio 0  
station-role root
```

- Beacon Period Settings:

A Beacon frame is around 50 bytes long  
and is sent to all 1's (broadcast MAC address).  
It is the "Heartbeat" of any Wireless LAN and

The Beacon period is the time between 2 of these frames.  
It can be set between 20 and 4000ms.

```
interface dot11Radio 0  
beacon period <20 – 4000ms>
```

- Channel Settings:

Channels are not configured by simply entering the channel number.  
The actual frequency band matching the corresponding channels  
needs to be configured:

```
interface dot11Radio 0  
channel <frequency from 1 – 2462 MHz for 802.11b>
```



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK

[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

- Power Settings:

The Power settings specify the transmission power the AP will transmit on.

```
interface dot11Radio 0
power local ?
<1 - 100> One of: 1 5 20 30 50 100
maximum Set local power to allowed maximum
```

Table shows dB to mW conversion:

dBm	-1	2	5	6	7	8	8	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
mW	1	2	3	4	5	6	8	10	12	15	20	25	30	40	50	80	80	100	125	150	200	250

- Monitor frames to an IP host:

For centralized monitoring purposes, frames can be sent to an IP host

```
interface dot11Radio 0
monitor frames endpoint ip address 141.1.1.1 port 3000
```

- Monitor the interface link / sub-interface link status of the Radio Interface:

```
interface dot11Radio 0
logging event link-status <subif-link-status>
```

- Dot1x Re-authentication period:

Where dot1x is used, the re-authentication period can be specified. For example how often an AP has to re-authenticate with its RADIUS server.

```
interface dot11Radio 0
dot1x reauth-period ?
<1-65555> Seconds
server use server provided reauthentication interval
```



<http://www.coursefox.co.uk>

Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK

[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

- Layer 2 MAC ACLs for client MAC authentication

This feature enables the administrator to allow only pre-defined MAC addresses on clients to associate with an AP. That provides a “certain” degree of security.

```
access-list 700 permit 0002.a52d.5e4c 0000.0000.0000
access-list 700 permit 0008.02d2.570b 0000.0000.0000
access-list 700 permit 00c0.4955.eeb4 0000.0000.0000
access-list 700 permit 0007.40fa.efe6 0000.0000.0000
```

```
interface dot11Radio 0
bridge-group 1 input-address-list 700
l2-filter bridge-group-acl
```

- Access-Lists on the Radio Interface on L3/L4 basis for traffic from the clients:

```
interface Dot11Radio0
no ip address
ip access-group radioside in
no ip route-cache
!
```

## Authentication & Encryption

- Configuring EAP

```
AP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AP(config)#aaa group server radius rad_eap
AP(config-sg-radius)#server 10.0.0.3 auth-port 1645 acct-port 1646
AP(config-sg-radius)#exit
AP(config)#aaa new-model
AP(config)#aaa authentication login eap_methods group rad_eap
AP(config)#radius-server host 10.0.0.3 auth-port 1645 acct-port 1646
key labap1200ip102
AP(config)#end
AP#write memory
```



<http://www.coursefox.co.uk>  
Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK  
[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

- Configuring LEAP:

```
aaa new-model
!
aaa group server radius rad_eap
server 192.168.2.108 auth-port 1812 acct-port 1813
!
aaa authentication login eap_methods group rad_eap
!
interface Dot11Radio0
 encryption key 1 size 128bit 12345678901234567890123456 transmit-
key
!
 encryption mode wep mandatory
!
ssid labap1200
 authentication network-eap eap_methods
!
radius-server local
!
nas 192.168.2.108 key shared_secret
!
user user1 nhash password1 group testgroup
!
radius-server host 192.168.2.108 auth-port 1812 acct-port 1813 key
shared_secret
```

- Configuring WEP:

```
interface dot11Radio 0
 encryption key 1 size 128bit 7 5C3A6F2CD518A27CF72C5C207F2C
transmit-key
 encryption mode wep mandatory
```



<http://www.coursefox.co.uk>  
Be a smart fox...book at course fox  
Your Cisco Training Course Provider in the UK  
[info@coursefox.co.uk](mailto:info@coursefox.co.uk)

- Configuring WPA:

```
aaa new-model
!
aaa group server radius rad_eap
server 192.168.2.100 auth-port 1645 acct-port 1646
!
aaa authentication login eap_methods group rad_eap
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers tkip
!
ssid WPAlabap1200
authentication open eap eap_methods
authentication open network-eap eap_methods
authentication key-management wpa
!
radius-server host 192.168.2.100 auth-port 1645 acct-port 1646 key
shared_secret
```