CSCI 7000-011 Introduction to Enterprise Networks

# Lab 2

## Wireless LANs

## Objectives

- This lab examines wireless networking technology, specifically the 802.11b protocol.
- The student will use a wireless router in conjunction with wireless enabled laptops/PCs to create their own network.
- The lab will explore the security concerns associated with wireless networking and allow the student to examine in detail the 802.11b protocol.
- We will then deal with the problem of creating a wireless environment that is able to support 2 different sets of users, users in each set must not be able to use each other's wireless domain but they can connect via the backbone network.

## INTRODUCTION

With the increased prevalence of mobile computers and PDAs, came an increased demand for mobile network connectivity. At this point, the most popular form of wireless networking is the IEEE standard

802.11b. 802.11 is the wireless working group within the 802 series, and 802.11b is one of several variants of 802.11.

The original 802.11 specification called for a data transfer rate of only 1 or 2 Mb/s. Today, 802.11b is currently the most popular 802.11 variant. There are a couple other variants in popular usage as well. Most notably, 802.11g has been increasing in popularity very rapidly over the past couple years. In addition, there are working groups within IEEE working on new 802.11 variants right now. For now, the three types of wireless most likely to be seen in use are 802.11b, 802.11a and 802.11g.

**802.11b –** 802.11b was originally released in 1999. It can support a data transfer rate of11 Mb/s but also has the ability to scale back as far as 1 Mb/s depending on conditions. 802.11b makes use of Direct Sequence Spread Spectrum (DSSS) to transfer bits. It operates in the unlicensed 2.4 GHz portion of the spectrum.

**802.11a –** 802.11a was released in 2001. It can run at a bit rate of up to 54 Mb/s. The standard also called for the use of a modulation technique called Orthogonal Frequency Division Multiplexing (OFDM). 802.11a operates in the 5GHz range of the spectrum.

**802.11g –** 802.11g actually operates in the 2.4 GHz portion of the spectrum like 802.11b. However, it uses OFDM like 802.11a. As far as data transfer rate, 802.11g falls in between 802.11a and b with a transfer rate of 22Mb/s.

Table 1 provides an overview of the 802.11 specifications.

| 802.11 PHY | Max Data Rate | Frequency | Modulation |
|---|---|---|---|
| 802.11 | 2Mb/s | 2.4GHz and IR | FHSS and DSSS |

| | | | |
|---|---|---|---|
| 802.11b | 11Mb/s | 2.4GHz | DSSS |
| 802.11g | 22Mb/s | 2.4GHz | OFDM |
| 802.11a | 54Mb/s | 5GHz | OFDM |

**Table 1 - 802.11 overview (802.11 security, Fleck and Potter)**

Because it is most widely deployed, this lab introduction will focus primarily on 802.11b. However, most of the concepts discussed should be transferable to any of the 802.11 variants.

**802.11 Architecture**

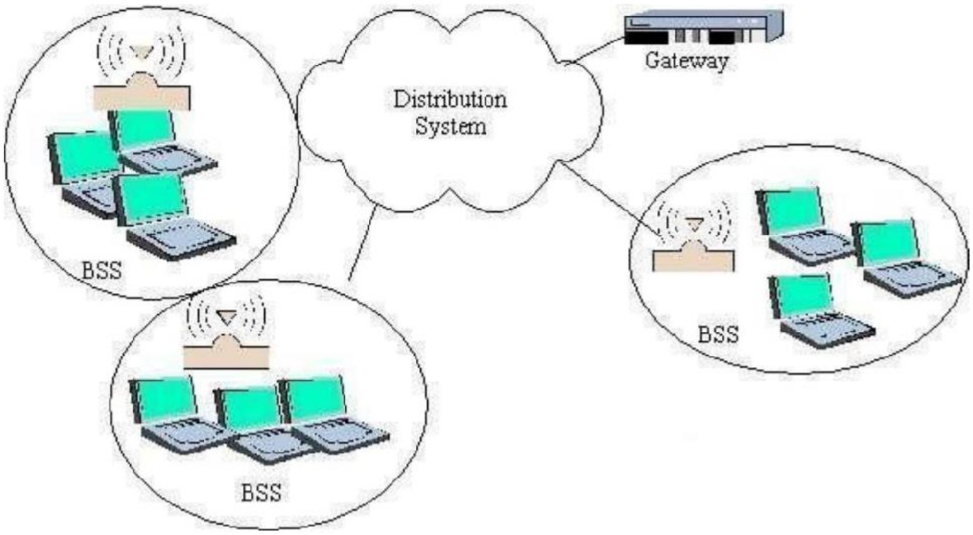
As with most things, there can be much more to an 802.11 network setup than simply a single AP. This is accomplished through a wireless LAN BSS (Basic Service Set). A BSS is identified by its service-set identifier (SSID). A BSS can be thought of in two different paradigms, an infrastructure network and an ad-hoc network.

An ad-hoc wireless network is composed of two or more nodes. In this setup, there is no central AP by which the nodes are connected. Instead, the nodes are related to each other in a single BSS by the common SSID. This ad-hoc type of configuration is relatively quick to setup, and thus is good for small areas where individual nodes need to communicate.

In most situations, however, an infrastructure network will be used. In a wireless infrastructure network, a BSS is composed of a central access point and a set of clients. This is advantageous to an ad-hoc setup for several reasons. The clients can be much simpler and will only have to worry about communication with the AP. In addition, the AP can provide a connection to networks outside of the wireless network, such as the Internet. With dedicated APs, the APs can be used for authentication, logging and a host of other functionality.

When an organization grows to the point that it needs more than one AP to cover the Desired area, it is necessary to establish an ESS (Extended service set). An ESS is essentially two or more BSSs that are connected through a distribution system. The distribution system could be either wired or wireless.

Figure 3 illustrates how three BSSs could be combined into a single ESS.



When a client wants to join a BSS, it will look for available APs. This can be done either actively or passively. An AP can broadcast its SSID periodically using broadcast beacons.

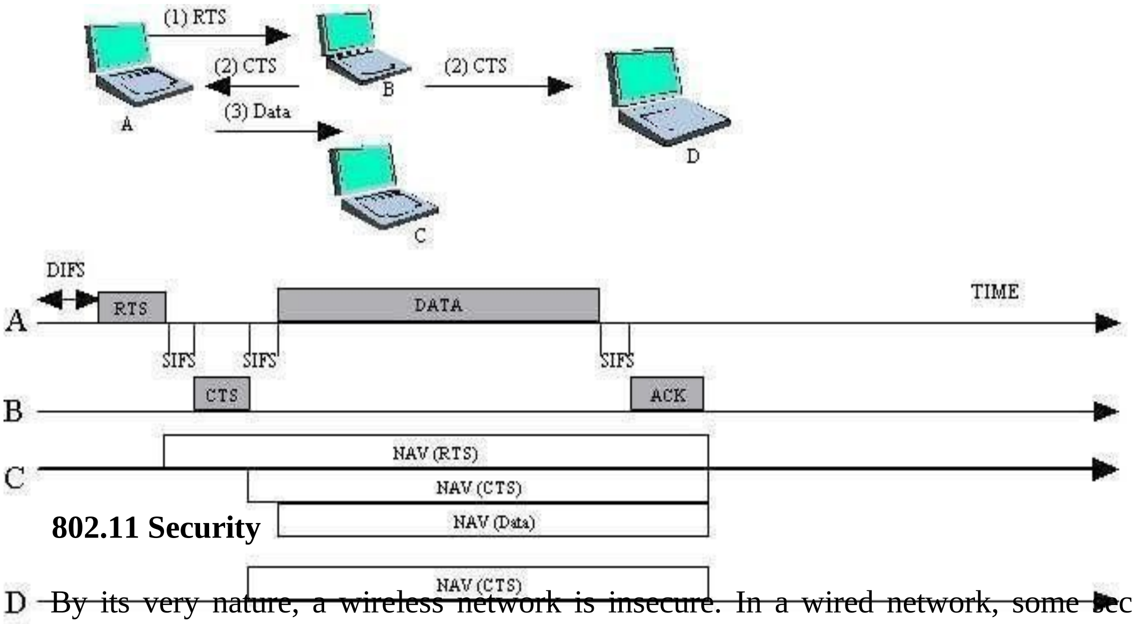
### Joining a BSS

The first thing a client wishing to join a BSS must do is find the SSID of the BSS. Sometimes the AP will periodically use broadcast beacons to announce the name its presence and SSID. If this is the case, then the client can simply use the SSID from the broadcast beacon. The client could also try actively sending Probe Request Frames and waiting for Probe Responses from APs. For security reasons, it is usually not a good reason to broadcast the SSID. In this case, the client would have to know the SSID. Once the client knows the SSID of the desired AP, it sends an association request to the AP. The station and the AP will go through a handshake process and exchange any authentication information that may be required by the AP. Once the client is associated with the AP, it is officially a part of the network. The AP may relay traffic between the client and other clients, or act as a bridge to the wired network. When a client is finished using the wireless network, it should disassociate which allows the AP to clear up any resources committed to that client. However, since clients can’t always disassociate, the AP will time out associations that haven’t been used.

### 802.11 MAC

Since 802.11 is an 802 protocol, it is a shared medium protocol. Thus, it must use some process to deal with collisions. Recall that 802.3 (Ethernet) uses Carrier Sense Multiple Access/Collision Detection (CSMA/CD). However, in the wireless domain, collision detection is not feasible because radios that do full duplex would be much more expensive and not all nodes may be able to hear each other. Because of this, 802.11 use CSMA/CA (Collision Avoidance). Instead of sending and then listening for a collision, CA will first listen and then back off for a random period if the medium is busy. CA must acknowledge every packet to ensure the packet has arrived.

CA must first do virtual carrier sensing. The client will send a short Ready to Send (RTS) message that contains source and destination addresses plus the duration of the message. This lets other nodes know they should back off for that duration. The destination will respond to the RTS with a Clear to Send (CTS) message. All nodes that hear either the RTS or CTS message will set their Network Allocation Vector (NAV), or basically their timer, for the given duration and not send during that period of time. This process is illustrated in figure 4.



**802.11 Security**

By its very nature, a wireless network is insecure. In a wired network, some security can be assumed because the data is flowing across wires that are located in a physically secure location (your building). In a wireless setting, the data is traveling across the airwaves for anyone to see (a hacker in the parking lot can see the same wireless traffic as a legitimate user). Because of this, there are some basic security steps that should always be considered when setting up a wireless network.

Recall that an SSID must be known in order to connect to that access point. Be sure to disallow that AP from broadcasting its SSID unless there are other authentication measures in place. Most APs ship with their SSID set to a default value. This default value should always be changed, and the default values are widely known to the hacker community.

(This also goes for the default administrator password for the AP).

**WEP**

With traffic whizzing through the air, it makes it easy for an unscrupulous user to sniff and read that traffic. For that reason, APs should always use Wired Equivalent Privacy (WEP). The idea behind WEP is that wireless LANs should be as secure as their wired counterparts. With WEP, the AP and the client share a key that is used to encrypt the transmitted data with the RC4 cipher. The 802.11 standard specifies a 40-bit key, but most vendors have also implemented a 104-bit or greater key.

It should be noted that WEP has some serious issues. First, it does not deal with the issue of key management at all. Either the keys have to be manually given to end users, or they have to be distributed in some other authentication method. Since WEP is a shared key system, the AP uses the same key as all the clients and the clients also share the same key with each other. A hacker would only have to compromise the key from a single user, and he would then know they key for all users.

In addition to key management, a recently published paper describes ways in which WEP can actually be broken ("Weaknesses in the Key Scheduling Algorithm of RC4" by Fluhrer, Mantin and Shamir). This is due to a weakness in RC4 as it is implemented in WEP. If enough traffic can be intercepted, then it can be broken by brute force in a matter of an hour or two. If that weren't bad enough, the time it takes to crack WEP only grows linearly with key length, so a 104-bit key doesn't provide any significant protection over a 40-bit key when faced against a determined hacker. There are several freely available programs that allow for the cracking of WEP. WEP is indeed a broken solution, but it should be used as it is better than nothing. In addition, higher layer encryption (SSL, etc) should be used when possible.

**Refer to this links for CISCO 1800 before coming to lab:**

https://www.cisco.com/c/en/us/td/docs/routers/access/1800/1801/software/configuration/guide/scg/wireless.html

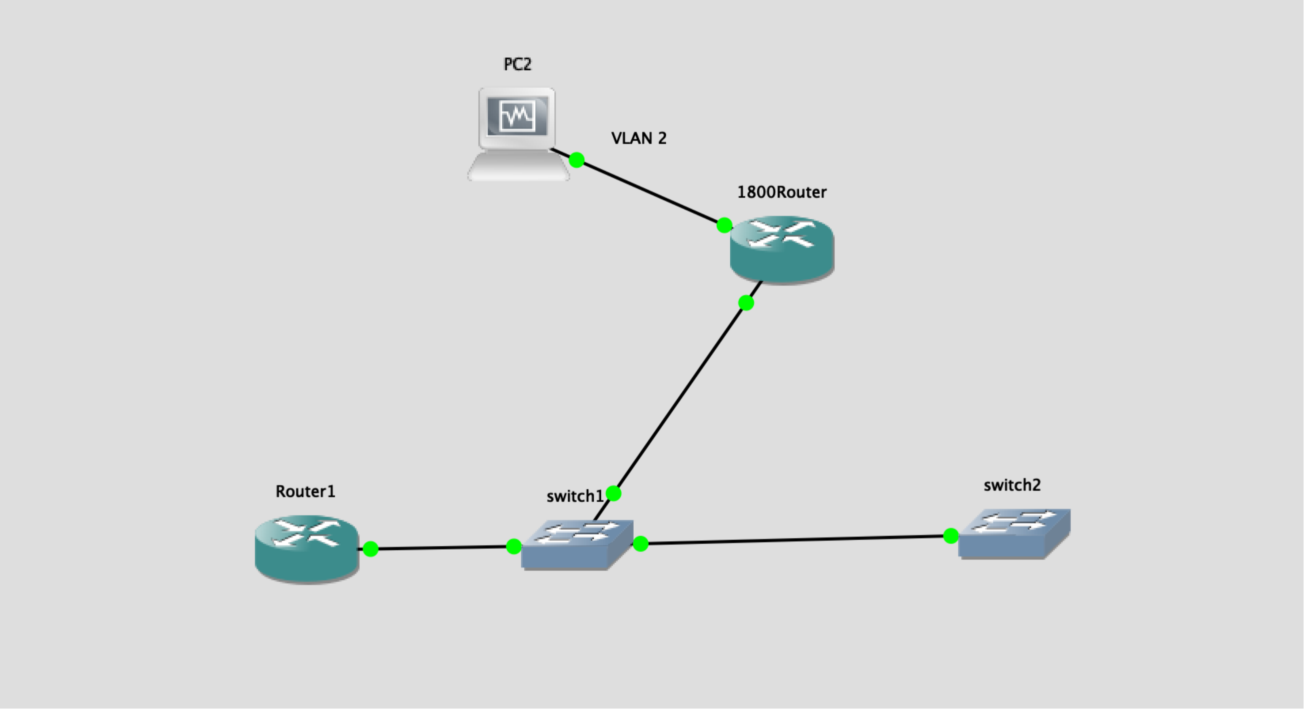
## LAB SETUP

In this part of the lab, we will address the problem of creating separate wireless networks for two sets of users. Users in each set should not have access to the others' wireless networks but should be able to communicate via the backbone network.

### NETWORK DIAGRAM

This is in continuation to your previous lab. Remove switch 3. Connect the Cisco 1800 wireless router to switch 1.

Connect the PC 1 in the later part of the objective.

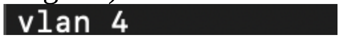


**Design Considerations:**

1. All the Links to switch 1 are trunk. Choose any type of encapsulation.

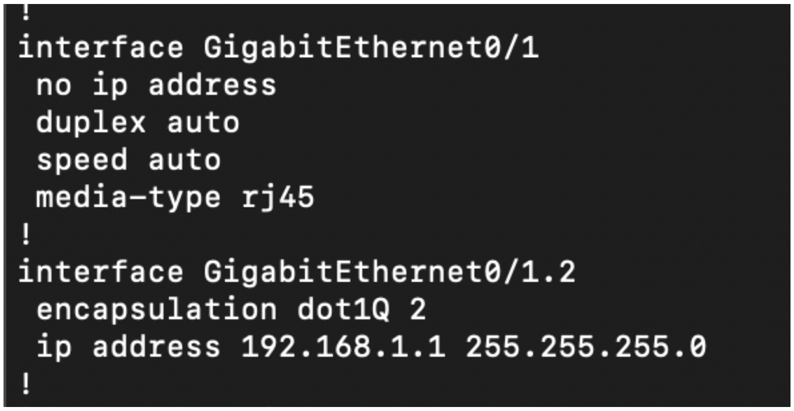
## 1. Creating a DHCP server and implementing wired LANs

a) Create a VLAN named wired1 on the Cisco 1800 Wireless router (VLAN 2 in the network diagram)



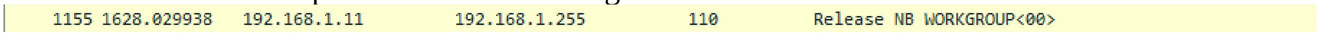
```
vlan 4
```

b) Create sub-interfaces on router 1 and give it an IP address in the subnet that you assign to VLAN 2



```
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1.2
 encapsulation dot1Q 2
 ip address 192.168.1.1 255.255.255.0
!
```

c) The DHCP server for host in VLAN 2 will be hosted on switch 2. The DHCP pool will also provide the hosts with the IP of their default gateway (router sub-interface) and DNS server IP. Sniff and capture the DHCP messages.

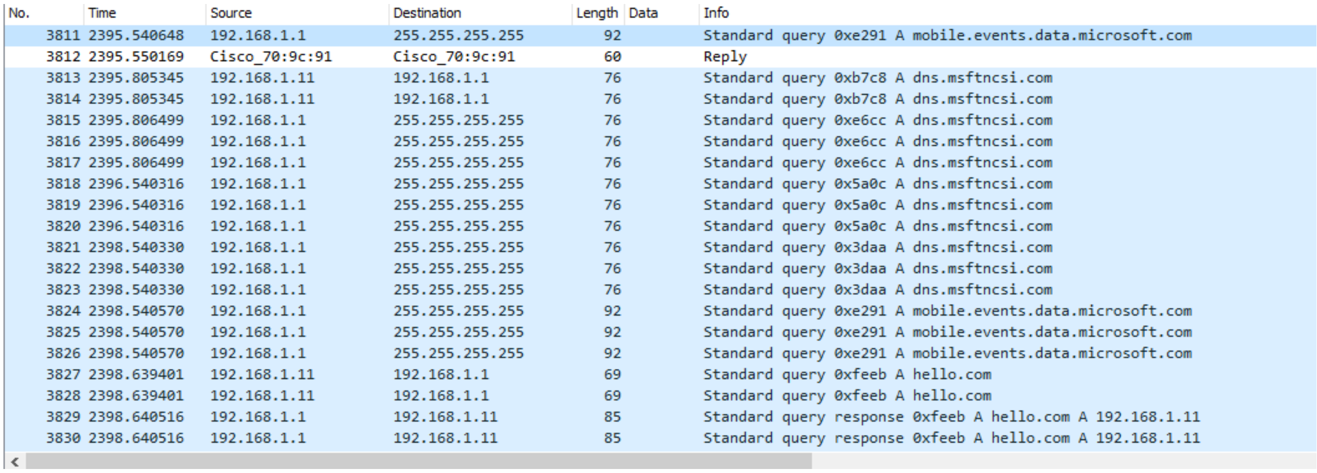


```
1155 1628.029938    192.168.1.11         192.168.1.255          110         Release NB WORKGROUP<00>
```

d) Connect a PC to the Cisco 1800 Router as shown in the network diagram and verify that it gets an IP address from the DHCP server.

Shown above

e) Create entries on the DNS server i.e. router 1 for the IP addresses obtained on the hosts. Sniff and capture the DNS messages

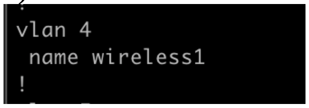


| No. | Time | Source | Destination | Length | Data | Info |
|---|---|---|---|---|---|---|
| 3811 | 2395.540648 | 192.168.1.1 | 255.255.255.255 | 92 | | Standard query 0xe291 A mobile.events.data.microsoft.com |
| 3812 | 2395.550169 | Cisco_70:9c:91 | Cisco_70:9c:91 | 60 | | Reply |
| 3813 | 2395.805345 | 192.168.1.11 | 192.168.1.1 | 76 | | Standard query 0xb7c8 A dns.msftncsi.com |
| 3814 | 2395.805345 | 192.168.1.11 | 192.168.1.1 | 76 | | Standard query 0xb7c8 A dns.msftncsi.com |
| 3815 | 2395.806499 | 192.168.1.1 | 255.255.255.255 | 76 | | Standard query 0xe6cc A dns.msftncsi.com |
| 3816 | 2395.806499 | 192.168.1.1 | 255.255.255.255 | 76 | | Standard query 0xe6cc A dns.msftncsi.com |
| 3817 | 2395.806499 | 192.168.1.1 | 255.255.255.255 | 76 | | Standard query 0xe6cc A dns.msftncsi.com |
| 3818 | 2396.540316 | 192.168.1.1 | 255.255.255.255 | 76 | | Standard query 0x5a0c A dns.msftncsi.com |
| 3819 | 2396.540316 | 192.168.1.1 | 255.255.255.255 | 76 | | Standard query 0x5a0c A dns.msftncsi.com |
| 3820 | 2396.540316 | 192.168.1.1 | 255.255.255.255 | 76 | | Standard query 0x5a0c A dns.msftncsi.com |
| 3821 | 2398.540330 | 192.168.1.1 | 255.255.255.255 | 76 | | Standard query 0x3daa A dns.msftncsi.com |
| 3822 | 2398.540330 | 192.168.1.1 | 255.255.255.255 | 76 | | Standard query 0x3daa A dns.msftncsi.com |
| 3823 | 2398.540330 | 192.168.1.1 | 255.255.255.255 | 76 | | Standard query 0x3daa A dns.msftncsi.com |
| 3824 | 2398.540570 | 192.168.1.1 | 255.255.255.255 | 92 | | Standard query 0xe291 A mobile.events.data.microsoft.com |
| 3825 | 2398.540570 | 192.168.1.1 | 255.255.255.255 | 92 | | Standard query 0xe291 A mobile.events.data.microsoft.com |
| 3826 | 2398.540570 | 192.168.1.1 | 255.255.255.255 | 92 | | Standard query 0xe291 A mobile.events.data.microsoft.com |
| 3827 | 2398.639401 | 192.168.1.11 | 192.168.1.1 | 69 | | Standard query 0xfeeb A hello.com |
| 3828 | 2398.639401 | 192.168.1.11 | 192.168.1.1 | 69 | | Standard query 0xfeeb A hello.com |
| 3829 | 2398.640516 | 192.168.1.1 | 192.168.1.11 | 85 | | Standard query response 0xfeeb A hello.com A 192.168.1.11 |
| 3830 | 2398.640516 | 192.168.1.1 | 192.168.1.11 | 85 | | Standard query response 0xfeeb A hello.com A 192.168.1.11 |

## 2. Configuring Wireless for IPv4 VLANs

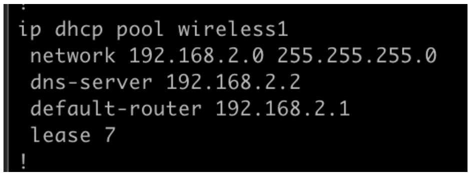
(Command are given in the following page)

a) Create 1 more VLAN named wireless1 i.e. VLAN 4



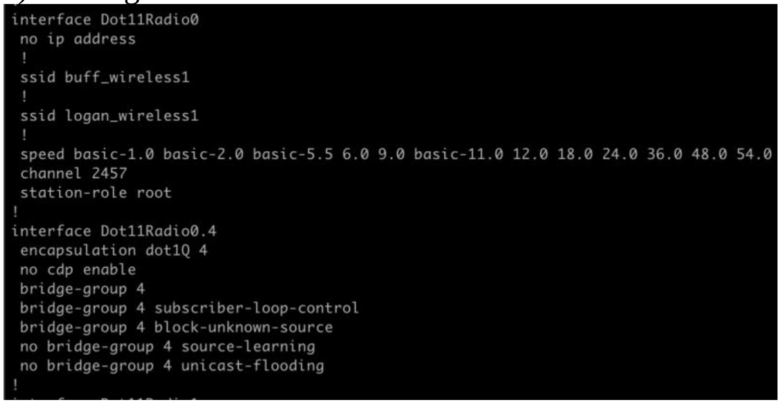
```
vlan 4
 name wireless1
!
```

b) Create a DHCP pool for the hosts on this VLAN on the CISCO 1800 device with the default gateway as the IP on the VLAN.



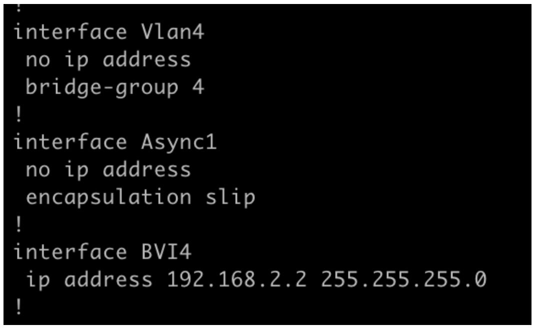
```
ip dhcp pool wireless1
 network 192.168.2.0 255.255.255.0
 dns-server 192.168.2.2
 default-router 192.168.2.1
 lease 7
!
```

c) Configure the Root Radio Station.



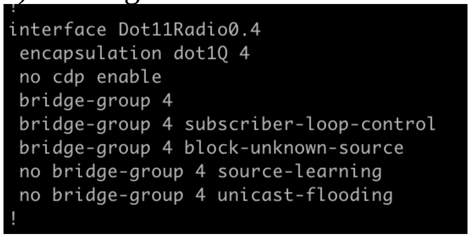
```
interface Dot11Radio0
 no ip address
 !
 ssid buff_wireless1
 !
 ssid logan_wireless1
 !
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 channel 2457
 station-role root
!
interface Dot11Radio0.4
 encapsulation dot1Q 4
 no cdp enable
 bridge-group 4
 bridge-group 4 subscriber-loop-control
 bridge-group 4 block-unknown-source
 no bridge-group 4 source-learning
 no bridge-group 4 unicast-flooding
!
```

d) Configure Bridging on VLAN.



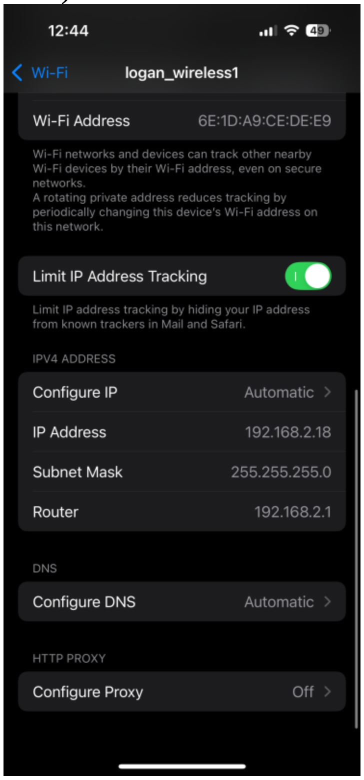
```
interface Vlan4
 no ip address
 bridge-group 4
!
interface Async1
 no ip address
 encapsulation slip
!
interface BVI4
 ip address 192.168.2.2 255.255.255.0
!
```

e) Configure Radio Station Sub-interfaces.



```
interface Dot11Radio0.4
 encapsulation dot1Q 4
 no cdp enable
 bridge-group 4
 bridge-group 4 subscriber-loop-control
 bridge-group 4 block-unknown-source
 no bridge-group 4 source-learning
 no bridge-group 4 unicast-flooding
!
```

f) Connect a device to the respective SSID’s and paste relevant screenshots.



logan_wireless1

Wi-Fi Address 6E:1D:A9:CE:DE:E9

Wi-Fi networks and devices can track other nearby Wi-Fi devices by their Wi-Fi address, even on secure networks.
A rotating private address reduces tracking by periodically changing this device's Wi-Fi address on this network.

Limit IP Address Tracking

Limit IP address tracking by hiding your IP address from known trackers in Mail and Safari.

IPV4 ADDRESS

Configure IP Automatic

IP Address 192.168.2.18

Subnet Mask 255.255.255.0

Router 192.168.2.1

DNS

Configure DNS Automatic

HTTP PROXY

Configure Proxy Off

## Configuring the Root Radio Station

For this, we need to enable dot11radio interfaces and enable bridging. Create different SSIDs for different VLANs and associate them appropriately

Configuration

- conf t
- Interface dot11radio *0 or 1or sub interface*
  Cisco 1800 ISRs have interfaces on which wireless can be configured. This command is used to enter the interface configuration mode for that interfaces. (0 for 2.4 Ghz and 1 for 5 Ghz)
- ssid *name*

This command specifies the name of the wireless network that can be seen by all. Also places the router in ssid configuration mode. There are encryption and authentication commands before this command. Since we are using open authentication and no encryption, we haven't mentioned the commands here.

- Vlan#

  This command binds the particular vlan with that ssid

- Channel #

  Determines the channel on which the configuration occurs
- Exit

**Next**
**Similarly create other SSID's for other VLANs. We can create multiple SSIDs on the same radio interface. (if you want to configure multiple wireless VLAN's)**

- Conf t
- dot11 ssid name
- guest-mode
- channel #
- exit

! Notes
- Do not enter vlan # under global config mode
- Do not enter authentication under global config mode

### Configure Bridging on VLANs

Now, we have to configure integrated routing and bridging on VLANs

i. **bridge** *irb*

*Specifies the type of bridging. Here we are using the integrated bridging and routing*

ii. In global configuration mode enter the commands:

**bridge x protocol ieeee**
**bridge x route ip**

iii. Assign IP address to that virtual bridge group interface (BVI) from the subnet of the VLAN that you will be using for wireless.

- **Explain in report why you require bridging interfaces and not simply give an IP address to VLANs as we do in wired LANs)**

Wireless interface don't support layer 3 devices. Allows for wired and wireless clients to share a subnet.

- **Explain the two commands used in step ii** bridge x protocol ieeee: This enables STP for the bridge.

bridge x route ip: allows ip traffic to be routed between bridge groups

- **Explain in detail what will happen when you use bridge irb in your network. Why is it required?**

Allows layer 2 bridging and layer 3 routing to work on the same device. So not only does it allow for traffic to be forwarded on the same subnet, but it also routes traffic between different VLANs/subnets. It is required for multiple users to connect to different networks on wifi.

- **What is the purpose of a BVI?**

  It allows different management on traffic segments while having one IP.

### d) Configuring Radio station Sub-interfaces

Now, we have to configure radio station sub-interface for each VLAN

**i.** **interface dot11radio** *0.x*

*This command will enable the user to configure the radio station sub-interface.*

**ii.** **encapsulation dot1q** *vlan_no*

*This command will enable IEEE 802.11q encapsulation on that sub-interface.*

**iii.** **no cdp enable**

*Disables the Cisco Discovery Protocol for the wireless interface.*

**iv.** **bridge-group** *number*

*This command assigns bridge group to the sub-interface.*

### e) <u>Configuring Clients</u>

i. Connect a laptop/phone to the SSID
ii.

iii. Verify connectivity between the wired and wireless VLAN. (Ping between the devices connected to the wired and wireless VLANs)

All screenshots are shown above proving the configuration that is also provided above in the lab itself.

### 3. Securing WLANs:

a) Configure VLAN wireless1 (VLAN 4) so that only one Laptop is allowed to connect to the VLAN, and all others are rejected.

```
!
```

b) Configure VLAN wireless1 with encryption wep128

```
encryption mode wep mandatory
```

c) Change the authentication to WPA-Personal using TKIP

```
dot11 ssid logan_wireless1
vlan 4
authentication open
guest-mode
wpa-psk ascii 0 password
!
interface Dot11Radio0
no ip address
!
encryption mode ciphers tkip
!
ssid buff_wireless1
!
ssid logan_wireless1
!
```

### 4. VLAN.

**Implement the wired host into the wireless VLAN so that the wired host is in the same subnet as that of the wireless**

For this just associate the router interface of 1800 with appropriate bridge group and assign an IP address in the same subnet. (Don’t forget to exclude this address from the pool.) Verify connectivity.

```
interface BVI4
ip address 192.168.2.2 255.255.255.0
!
```

As you can see, I have achieved connectivity within the wireless vlan between this wired computer and the phone connected to wireless.

[redacted]

i. Enter the VLAN for which you want to bridge wireless interface to the physical interfaces.

ii. Give the following command

**bridge-group 4**

*Associates a bridge group to an interface.*

Achieve full network connectivity!

## Study Questions:

1. In what situations would an ad-hoc network be useful?

An ad hoc network is useful for disaster recovery. Also, IoT devices could benefit from ad-hoc networks as they can create those networks without help of a central device.

2. In what situations would you use an infrastructure network?

Unlike an ad hoc network, an infra network is more permanent and usually has more compute. These are used for enterprise and business networks. Home networks also benefit from this type of network. This extends to any other application that requires a stable reliable internet connection.

3. What is the difference between a Layer 2 and a Layer 3 switch? Can Layer 3 switches be used to completely substitute routers in a network?

It is in the name. A layer 2 switch operates only on layer 2, forwarding frames. A layer 3 switch operates on the packet level, being able to forward packets to other networks and also forward frames. L3 switches can be used to completely substitute routers in a network. It really depends on the swtich or router and what features they have.

4. What is DHCP and why would you use it in a wireless network?

DHCP is dynamic host configuration protocol that hands out an IP to devices that want connectivity to a network. You would use it in a wireless network when you have many hosts that connect to one SSID and do not know there specific device address.

5. What is WEP? Why is it insecure? What are the different ways to break WEP? What are some of the other security options available for 802.11 networks?

Wired Equivalent Privacy is an outdated wirelsess security protocol. Provides encryption and security for Wi-Fi networks. Its encryption is not secure and is easily crackable. All users share the same static key, allowing users to break WEP. Wireshark can crack WEP. WPA, WPA2, and WPA3 are other security options.

6. Explain the meaning of Integrated Bridging and routing (IRB) and why is it required when creating wireless LANs

It allows layer 2 bridging and layer 3 routing in a device within the same VLAN. It allows for seamless connections between the wired and wireless network.

7. Explain the differences between WPA and WPA2.

WPA uses TKIP, which does have exploits. WPA is vulnerable to brute force attacks. WPA2 uses AES-CCMP. Different modes for different applications.

8. The wireless networks that we implemented did not broadcast their SSIDs. Find if there is any command to broadcast the SSID or at least see the network (similar to the probe feature explained in the ICND1)

Guest-mode

9. Explain in detail the DHCP messages you have captured in Objective 1.

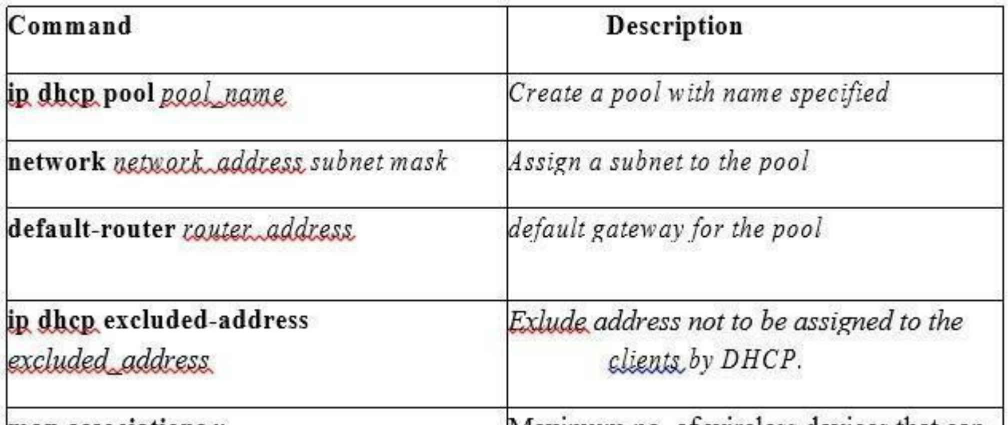
Discover – A broadcast message on UDP 67 that sends a message trying to find a DHCP server

Offer – A DHCP server found this broadcast and now sends a unicast back to the sender saying I am now your DHCP server.

Request – Now that host knows DHCP server, host will send a unicast back asking for needed IP information

Acknowledge – Finally, the DHCP server will send back the needed information and take note of the IP and other information given out to the host.

**Command Reference:**



| Command | Description |
|---|---|
| **ip dhcp pool** *pool_name* | *Create a pool with name specified* |
| **network** *network address subnet mask* | *Assign a subnet to the pool* |
| **default-router** *router address* | *default gateway for the pool* |
| **ip dhcp excluded-address** *excluded_address* | *Exlude address not to be assigned to the clients by DHCP.* |
| max-associations n | Maximum no. of wireless devices that can |