Lab 2

Wireless LANs & HSRP redundancy

Fall 2014

OBJECTIVES

1. To **assign IP addresses to hosts using a DHCP server**
2. To **familiarize the student with 802.11 protocols and their practical uses. Students will be exposed to the basic 802.11b protocol, and will understand the ramifications that go along with setting up a wireless network**
3. Having **a comprehension of good wireless security practices**

Scenario

- 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. Figure 1 shows the 802 structure.

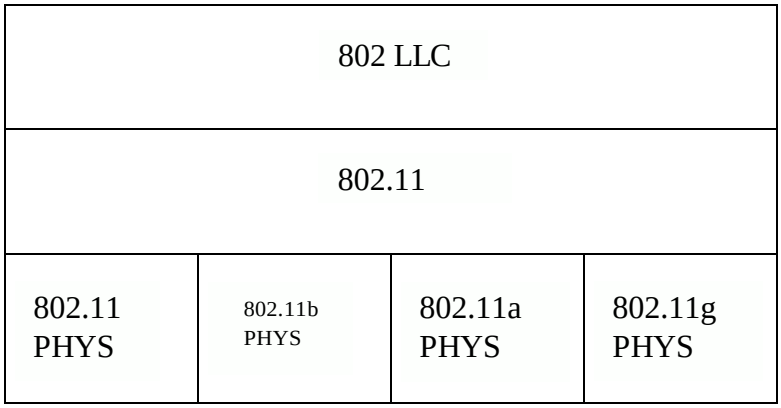


Figure 1 - 802 Structure (802.11 security, Fleck and Potter)

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 of 11 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.

Within the United States, 802.11b can use one of 11 channels which are located in the 2.4 GHz range. Please see the required reading section for a link to an article which discusses the placement of access points on non-overlapping channels.

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.

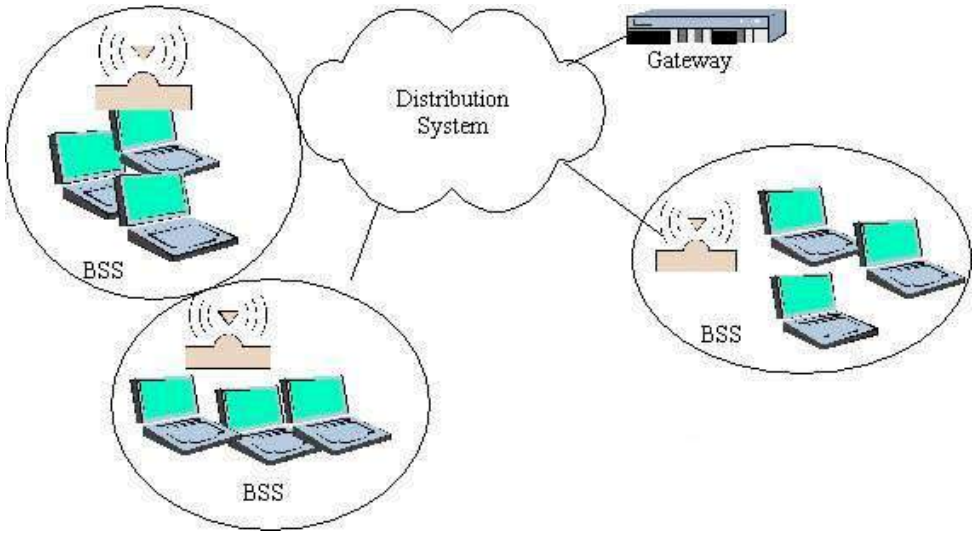


Figure 3 - (http://www-ee.uta.edu/online/wang/Wireless%20LAN.pdf)

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.

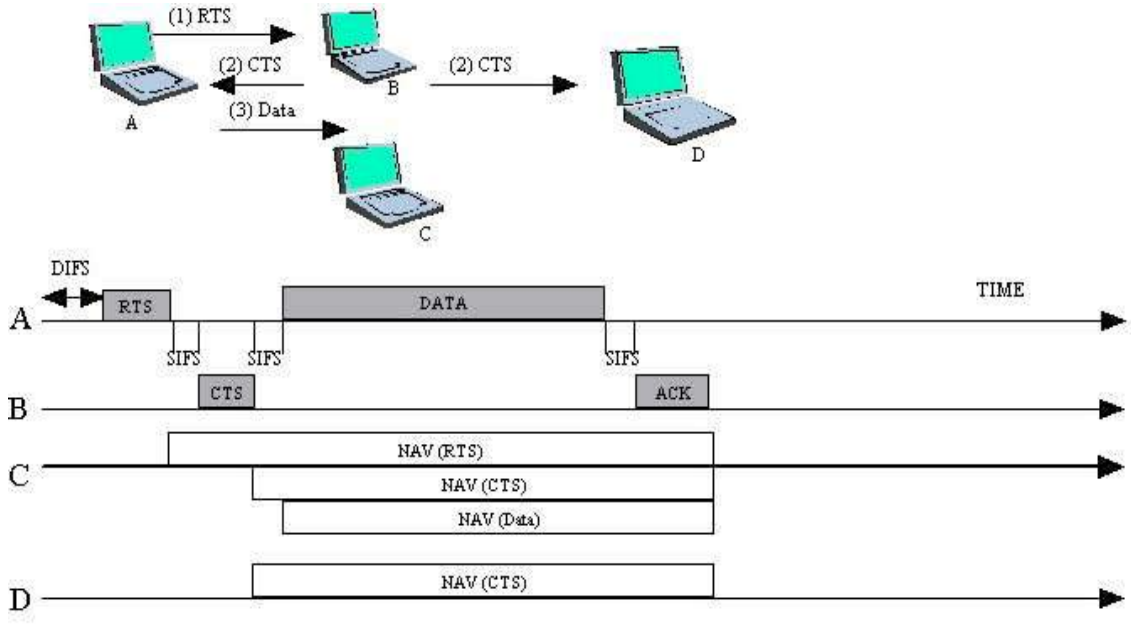


Figure 4 - (http://www-ee.uta.edu/online/wang/Wireless%20LAN.pdf)

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 values. 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.

Lab Scenarios

Infrastructure network configuration

A typical infrastructure configuration for a home user includes a central access point (AP) or wireless router and clients associated with that AP. Such distributed configurations provide minimum control over network devices and place a burden on the network administrator with regards to manageability, monitoring and security profiles since each AP needs to be individually managed. Hence, such configurations are rarely used in corporate wireless data networks.

Corporate wireless networks use a centralized administrative model in which several access points and their associated networks can be managed, monitored and configured centrally and remotely. This is achieved by using Wireless LAN Controller (WLC) devices. A WLC essentially serves to create an ESS by connecting several BSSs together and can be thought of as being part of the Distribution System (DS) (see 802.11 architecture above). Using these devices, the administrator can manage several hundred Access Points deployed system wide and control aspects such as security profiles, QoS, RF management and VLAN management. Using WLCs, companies can construct and deploy scalable, reliable, secure and cost effective WLANs, thus bridging the gap between wired and wireless network management and administration. A typical WLAN configuration using WLCs is as shown in figure 5.

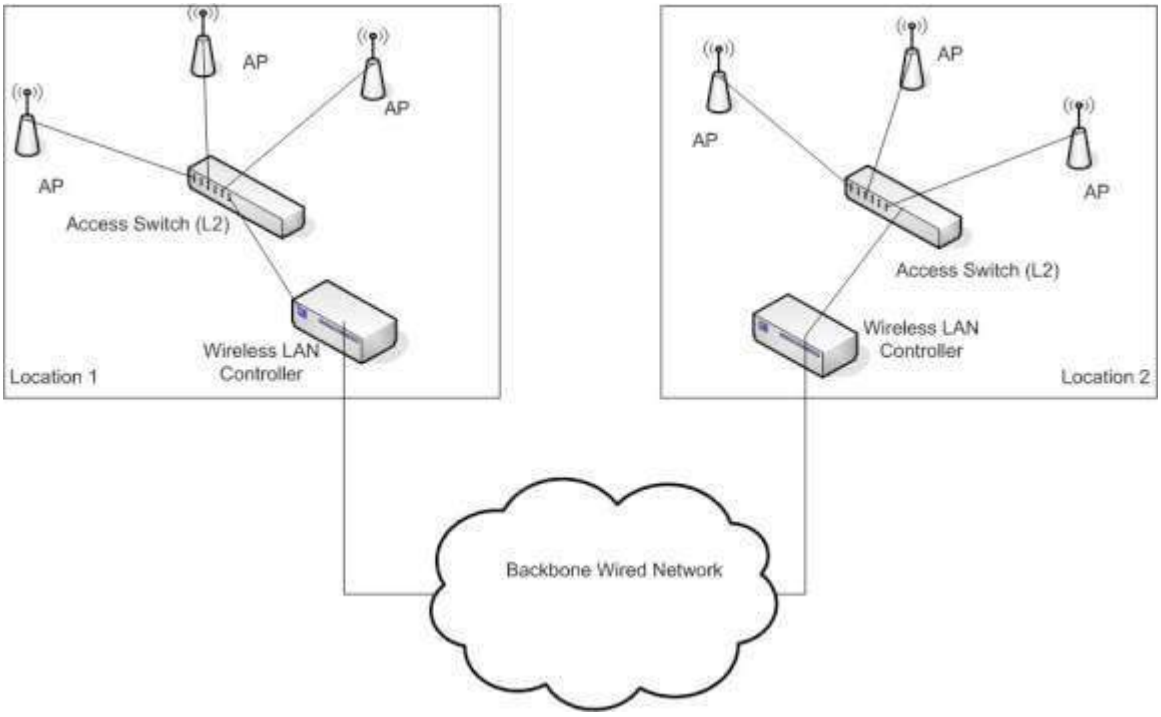


Figure 4 - Typical configuration using WLCs

This was an old setup. Nowadays, we have WLC, AP, access switch all built in one. Such as the one that you use at home i.e. Linksys

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.

The following component will be used to demonstrate the concepts of centralized WLANs.

Cisco 1800 Series Fixed-Configuration Routers

The Cisco 1800 Series fixed-configuration routers provide:

• Secure broadband access with concurrent services for branch and small offices

• Integrated ISDN Basic Rate Interface (BRI), analog modem, or Ethernet backup port for redundant WAN links and load balancing

• Secure wireless LAN for simultaneous 802.11a and 802.11b/g operation with use of multiple antennas

• Advanced security including:

– Sophisticated Firewall features including Application Inspection, Transparent and Stateful Firewall

– SSL and IP Security (IPSec) VPNs (Triple Data Encryption Standard [3DES] or Advanced Encryption Standard [AES])

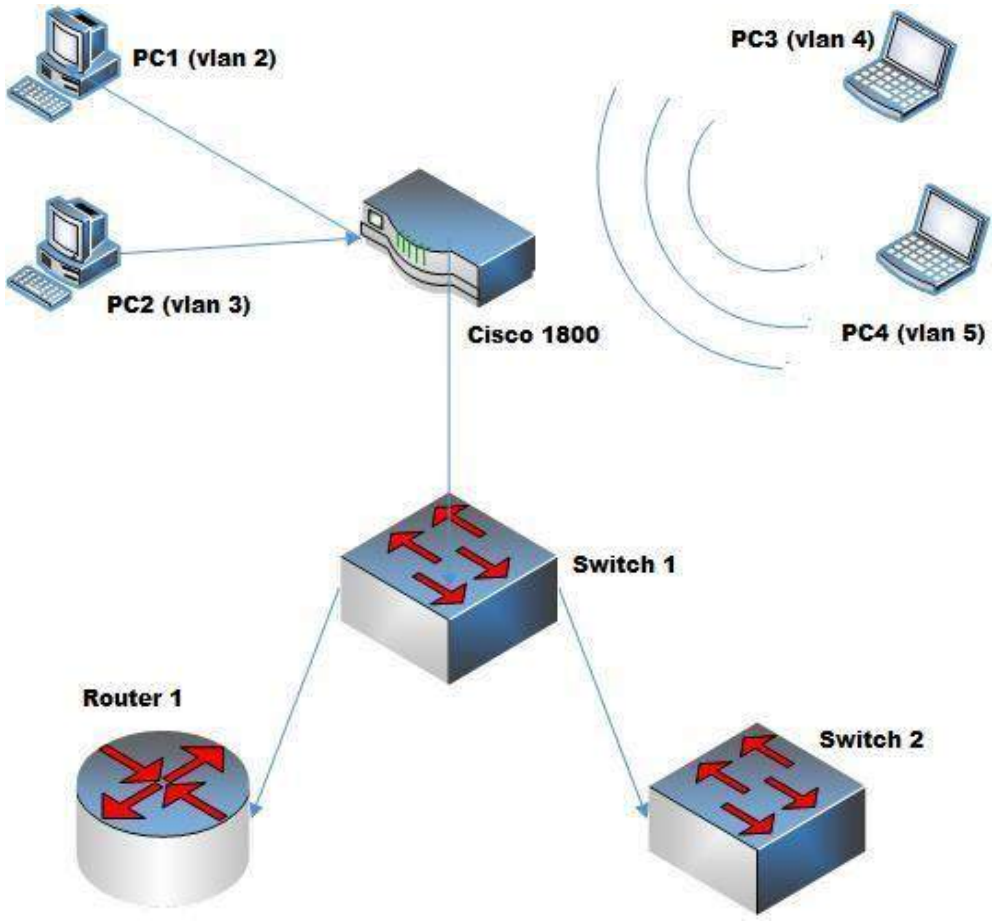
– Intrusion Prevention System (IPS)

– Antivirus support through Network Admission Control (NAC) and enforcement of secure access policies

• 8-port 10/100 managed switch with VLAN support and optional Power over Ethernet (PoE)

• Easy deployment and remote-management capabilities through Web-based tools and Cisco IOS® Software

Network Diagram



Design Considerations:

1. All the Links to switch 1 are trunk . Choose any type of encapsulation
2. Vlan information should propagate through VTP between the 1800 device and switch 1 and 2. Router 1 will have sub-interfaces for communication between the vlans.

1. Creating a DHCP server and implementing wired LANs

a) Enter the CLI mode of Cisco 1800

b) Create 2 VLANs say wired1 and wired2 i.e. Vlan 2 and Vlan 3

c) Give IP addresses to the sub-interfaces of the router and make it the default gateway to the hosts of vlan 2 and vlan 3

d) The Dhcp server for hosts in Vlan 2 will be hosted on switch 2. The Dhcp pool will also provide the hosts with the IP of their default gateway. The default gateway in this scenario is that of the router sub-interface

e) Create DHCP pool for hosts in Vlan 3 is created on Router 1 which will also provide all the hosts on Vlan 3 with their default gateway i.e. router sub-interface

f) Connect hosts to the 2 VLANs and verify that the pool is working.

g) Achieve connectivity between these 2 VLANs

***Use the commands given in Command Reference to configure DHCP**

Troubleshooting DHCP:

https://supportforums.cisco.com/servlet/JiveServlet/previewBody/13740-102-1-31644/DNSDHCP.pdf

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

http://www.petri.co.il/troubleshoot-dhcp-problem.htm

2. Configuring Wireless for IPv4 VLANs

Perform the following tasks to configure this network scenario:

a) Create 2 more VLANs named wireless1 and wireless2 i.e Vlan 4 and Vlan 5
b) Create a DHCP pool for the hosts on these Vlans on the CISCO 1800 device with the default gateway as the IP on the vlans
c) Configure the Root Radio Station
d) Configure Bridging on VLANs
e) Configure Radio Station Sub-interfaces
f) Configure clients

a) Create 2 more VLANs named wireless1 and wireless2

b) 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

i. Enter the global configuration mode

ii. **interface dot11radio** *interface_number*

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)

iii. **ssid** *name*

This command specifies the name of the wireless network that can 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.

iv. **vlan** *vlan_no*

This command binds the particular vlan with that ssid

v. **authentication** *open*

vi. **exit**

Out of ssid configuration mode

vii. **station – role** *root*

Specifies the role of this wireless interface. You must specify at least one root interface.

viii. **channel** *channel_number*

Determines the channel on which the configuration occurs.

ix. Similarly create other SSID's for other VLANs. We can create multiple SSIDs on the same radio interface.

c) 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 ieee
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.

Note: Remember to remove that address from the VLAN, if not than it will generate an error as overlapping subnet.

- ***Explain in report why you require bridging interfaces and not simply give an IP address to VLANs as we do in wired LANs)***
- ***Explain the two commands used in step ii***
- ***Explain in detail what will happen when you use bridge irb in your network. Why is it required?***
- ***What is the purpose of a BVI ?***

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) Configuring Clients

i. Open your laptop and go to an option called add non-broadcast networks.
ii. Enter SSID of the wireless LAN
iii. Connect to the network
iv. Do this for second wireless LAN also
v. Verify connectivity between all 4 VLANs

3. Securing WLANs:

a) Configure VLAN wireless1 so that only one Laptop is allowed to connect to the VLAN and all others are rejected.
b) Configure VLAN wireless2 with encryption wep128
c) Configure another VLAN say wireless3 with authentication WPA-Personal using TKIP

***For all the 3 parts, refer to the command reference**

4. VLAN. Implement one wired host into any of the wireless VLANs 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.

i. Enter the VLAN for which you want to bridge wireless interface to the physical interfaces.
ii. Give the following command

bridge-group *number*

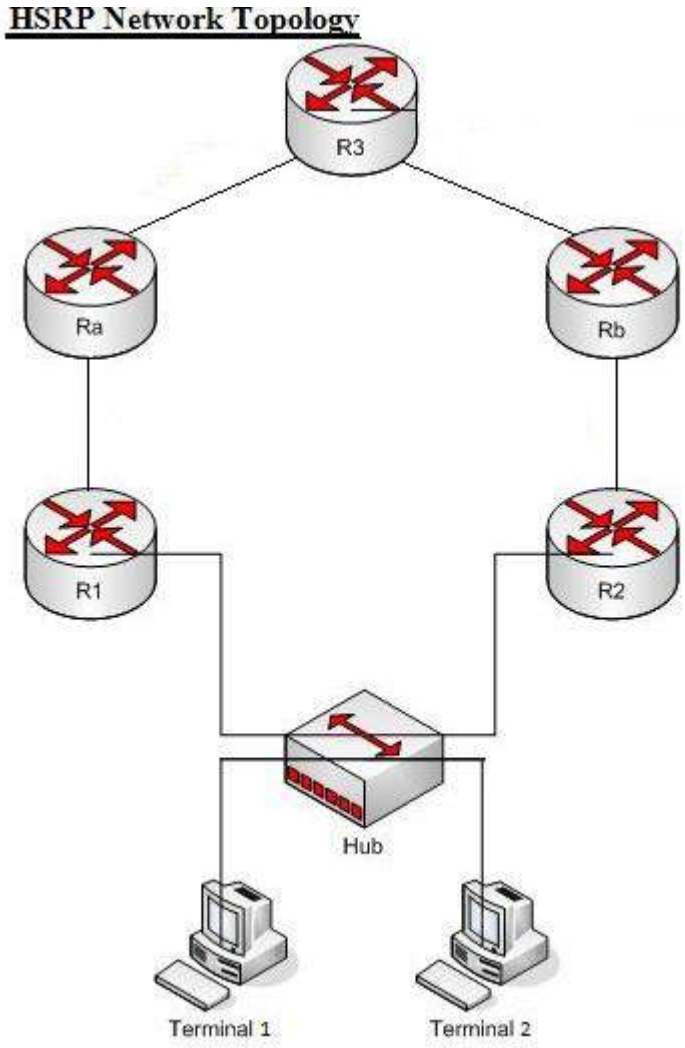
Associates a bridge group to an interface.

Achieve full network connectivity!

5. HSRP redundancy

Create the redundancy in the network by using HSRP in the R1 and R2. R1 should be the active router while R2 will act as the standby router in case of R1 failure. Configure R3 with the loopback to test the end connectivity of the network. Verify the network end-to-end connectivity and proper routing of packets. Then purposely fail the R1 by disconnecting the serial interface. R2 will automatically assume the active router role and will forward the packets.

Note: You can use switch in place of hub.



Refer to these links before coming to lab:

http://www.cisco.com/en/US/docs/routers/access/1800/1801/software/configuration/guide/scg.html

http://www.cisco.com/en/US/docs/routers/access/1800/wireless/configuration/guide/s37rf.html

http://www.cisco.com/warp/public/102/1800_isr_wireless.pdf

- From the first link study CONFIGURING A WIRELESS LAN CONNECTION.
- From the second link you must study till the end of configuring Authentication types.
- From third link study everything.

Study Questions:

1. In what situations would an ad-hoc network be useful? Give me the configurations to form an Ad-hoc network.

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

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?

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

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?

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

7. Give me the differences between WPA and WPA2.

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)

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 *x*	Maximum no. of wireless devices that can be connected
encryption vlan *x* **mode ? ? ?**	Select type of encryption
encryption vlan *x* **key** *y* **? ? ? ?**	select key for the encryption
authentication open	
authentication key-management wpa optional	WPA-personal authentication
authentication network-eap	To provide authentication with RADIUS server
wpa-psk ? ? ?	key for authentication
Show dot11 associations	**----------**
Show ip dhcp binding	**-----------**
Debug ip dhcp server packet	**---------**