universidade de aveiro

Departamento de Eletrónica, Telecomunicações e Informática
Mestrado Integrado em Eng. de Computadores e Telemática

Arquitetura de Redes

Laboratory Guide

Objectives

- Joining a BSS and communication.
- WLAN Filters.
- Wireless VLAN.
- Authentication.

NOTE: This lab guide should be performed with 2 student groups per Access Point. Use as #group ID the number of the first group.

Joining a BSS and Communication

1. Use a console/mirror cable to connect the serial/USB port of your PC to the AP console port and use the **password "Cisco"** the access the exec mode. Reset the device to default settings:

```
erase /all nvram:
write default-config
reload
```

Note:Your PC serial port should be configure without Software and Hardware Flow Control (set to NO).

2. Set up a network depicted below composed by 1 router, 1 AP and 2 PCs. Boot the PCs to Linux.
Using the AP console port and CLI, configure the virtual bridge 1 (bvi1) interface of the AP:

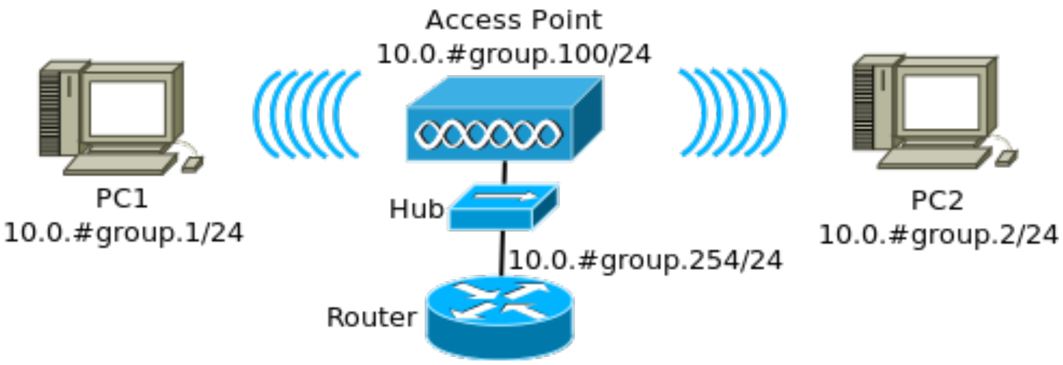
```
 AP(config)# interface bvi1
 AP(config-if)# ip address 10.0.#group.100 255.255.255.0
 AP(config-if)# no shutdown
```

After, configure the AP wireless interface with fixed wireless channel assigned to your group (**see table bellow**) and with SSID "rede#group":

```
 AP(config)# interface dot11radio 0
 AP(config-if)# channel <channelNumber>
 AP(config-if)# no shutdown
 AP(config-if)# ssid rede#group
 AP(config-if-ssid)# station-role root
```

Configure wireless authentication (start with `open`):

```
 AP(config)# dot11 ssid rede#group
 AP(config-ssid)# authentication open
 AP(config-ssid)# guest-mode
```



Groups	Channel
1-2	1
3-4	3
5-6	6
7-8	9
9-10	12

3. Using the Network Manager, create a new wireless connection with the correct parameters (SSID, Security – None, Manual IPv4 settings – according to figure) and connect PC1 to the wireless network and test connectivity with the AP and Router.

4. Configure PC2 as a wireless monitoring node by adding a monitoring virtual wireless device (mon0) listening a specific channel and start a capture with Wireshark in that interface. Connect again PC1 to the wireless network and using a visualization filter to capture all wireless frames from (or to) PC1 analyze the exchanged packets/frames and their content. Explain how the association process is performed.

Analyze the capabilities of your wireless interface:

```
iw phy phy0 info
```

To add a monitoring virtual wireless device (mon0) listening a specific channel (as root or with sudo):

```
iw phy phy0 interface add mon0 type monitor
rfkill unblock 0
ifconfig mon0 up
iw dev mon0 set channel <channel_number>
```

Note: Use `iw dev` and `rfkill list` commands to determine the wireless physical identifiers (if different from phy0 and 0, respectively).

Filtering Wireless Layer 2 Information

Configure a Wireshark visualization filter to analyse the management packets:

```
wlan.fc.type_subtype==x
      x=0 association request
        10 diassociation
        2 reassociation request
        1 association response
        3 reassociation response
        4 probe request
        5 probe response
        8 beacon
        11 authentication
        12 deauthentication
        13 ACK
        27 RTS
        28 CTS
```

To analyze all the management packets but the beacons, configure the following Wireshark visualization filter (remove beacons and analyze packets from or to PC1):

```
not wlan.fc.type_subtype==8 && wlan.addr == mac_pc
```

5. Reconnect PC1 to the wireless network and test the connectivity with the AP through wireless. Analyze the exchanged packets/frames and their content. Explain how the transmission is performed. If you have another available computer (laptop), you can join this SSID and ping between the several computers that joined this SSID. Analyze the exchanged packets/frames and their content. Explain how the packet transmission is performed. If you have different concurrent pings in different PCs, analyze the sequence of packets exchange of the several pings.

6. Configure the AP to enable RTS and CTS packets (with a RTS threshold value of 1000):

```
 AP(config)# interface dot11radio 0
 AP(config-if)# rts threshold 1000    !RTS threshold (0 to 2339)
 AP(config-if)# rts retries 2         !RTS retries (1 to 128)
```

Exchange pings between PC1 and the router and between the PCs (laptops). Analyze the exchanged packets/frames and their content. Explain how the transmission is performed and analyze the differences between this and the previous experience.

7. Now exchange very large pings (e.g. 2000 bytes), with increased length (ping –s length IP_address). Analyze the exchanged packets/frames and their content. Explain how the transmission is now performed and analyze the differences between this and the previous experiences.

Wireless VLANs

8. Configure two different VLANs using two different SSIDs:

```
 AP(config)# interface dot11radio 0
 AP(config-if)# ssid rede#group 
 AP(config-if)# ssid rede#group_2
 AP(config-if)# mbssid                  !to support multiple SSIDs
```

Configure the authentication to this SSID to be open:

```
 AP(config)#dot11 ssid rede#group
 AP(config-ssid)# vlan 1
 AP(config-ssid)# authentication open
 AP(config-ssid)# mbssid guest-mode
--
 AP(config)# dot11 ssid rede#group_2
 AP(config-ssid)# vlan 2
 AP(config-ssid)#authentication open
 AP(config-ssid)#mbssid guest-mode
```

Define Wireless and Wired sub-interfaces, ans assign VLAN numbers (bridge groups):

```
 AP(config)# interface dot11radio0.1
 AP(config-subif)# encapsulation dot1q 1 native
 AP(config-subif)# bridge-group 1
 AP(config-subif)# exit
 AP(config)# interface fastEthernet0.1
 AP(config-subif)# encapsulation dot1q 1 native
 AP(config-subif)# bridge-group 1
--
 AP(config)# interface dot11radio0.2
 AP(config-subif)# encapsulation dot1q 2
 AP(config-subif)# bridge-group 2
 AP(config-subif)# exit
 AP(config)# interface fastEthernet0.2
 AP(config-subif)# encapsulation dot1q 2
 AP(config-subif)# bridge-group 2
```

Connect PCs to the wireless network using different SSIDs/VLANs. Start pings between PCs in the same and in different VLANs, and pings with the router. If you are able to capture the packets/frames using a different PC, analyze the sequence of packets exchange and their content, and explain how VLANs are distinguished in the network.

9. Configure the router to perform inter-VLAn routing:

```
Router(config)# interface f0/0.1
Router(config-if)# encapsulation dot1q 1 native
Router(config-if)# ip address 10.0.#group.254 255.255.255.0
Router(config-if)# no shutdown
Router(config)# interface f0/0.2
Router(config-if)# encapsulation dot1q 2
Router(config-if)# ip address 10.0.#group+10.254 255.255.255.0
Router(config-if)# no shutdown
```

Re-test the connectivity between terminals in different VLANs.

MAC Filtering

10. Put PC2 wireless card in managed mode. Connect both PC1 and PC2 to the wireless network and make sure that both PCs are associated to the AP through pings to the AP and between the PCs. These pings should be continuous to show the MAC filtering effects.

Configure a filter for one of the two PCs and then apply this MAC-based filter to the radio interface:

```
!Configure a filter for PC with MAC address xxxx.xxxx.xxxx:
AP(config)# access-list 700 deny xxxx.xxxx.xxxx 0000.0000.0000
AP(config)# access-list 700 permit 0000.0000.0000 ffff.ffff.ffff
!Apply the MAC-based filter to the radio interface:
AP(config)#interface Dot11Radio 0
AP(config-if)#dot11 association mac-list 700
```

What happens to the ping of the filtered PC? If you are able to capture the packets/frames through a different PC, analyze the sequence of packets exchange.

IP filtering

12. Again, make sure that both PCs are associated to the AP and using pings to the AP and between the PCs verify full connectivity. These pings should be continuous to show the IP filtering effects.

Configure a filter for one of the two PCs and then apply this IP-based filter to the radio interface.

```
!Configure a filter for PC with IP address x.x.x.x:
AP(config)#access-list 1 deny host x.x.x.x
AP(config)#access-list 1 permit any
!Apply the IP-based filter to the radio interface:
AP(config)#interface Dot11Radio 0
AP(config-if)#ip access-group 1 in
```

What happens to the pings of the filtered PC?

Remove the IP filters and comment the results.

WPA for Home Wireless Networks

13. WPA also provides a Pre-Shared Key version (WPA-PSK) that is intended for use in small small or home wireless networks. This experiment will test this simpler WPA mode. In WPA-PSK the Encryption Mode needs to be configured as Cipher Temporal Key Integrity Protocol (TKIP), with the authentication mode WPA, introducing a shared key.

Configure the AP with WPA-PSK to enable WPA authentication:

```
AP(config)#interface dot11Radio 0
AP(config-if)#encryption vlan 1 mode ciphers tkip
AP(config-if)#dot11 ssid rede#group
AP(config-ssid)#authentication open
AP(config-ssid)#authentication key-management wpa
AP(config-ssid)#wpa-psk ascii pre-shared_key
      !Example of a pre-shared key: ARGROUP00#
```

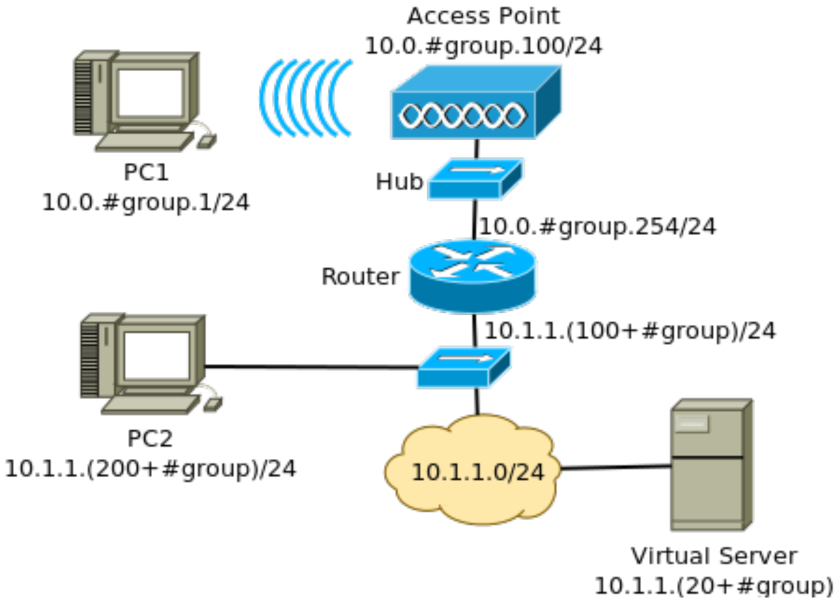
Then, configure PC2 as a wireless monitor node and start a capture. Connect PC1 to the wireless network with the corresponding key and analyze the captured packets during the phase of WPA enforcement. Check the connectivity between the PC and the router through a set of pings, and analyze the exchanged packets.

WPA with EAP Authentication (through RADIUS server)

14. Disable WPA-PSK:

```
AP(config-ssid)#no wpa-psk ascii pre-shared_key
```

In this final experiment, you will configure your network to work with a WPA with EAP authentication. This new scheme builds on current EAP/802.1x authentication and dynamic key management, and adds stronger cipher encryption. After the client device and the authentication server make an EAP/802.1x association, WPA key management is negotiated between the AP and the WPA-compliant client device. The following is an example of a LEAP configuration (EAP from Cisco).



15. Connect an interface of the router 10.1.1.(100+#group) to a hub and to the rack. Physically connect PC2 to network 10.1.1.0/24 with IP address 10.1.1.(200+#group).

In PC2 start a Virtual Machine with a Linux Server, connect it to the Internet and install the RADIUS server (freeradius): `sudo apt-get install freeradius`.

After, configure the network interface configured as **bridged adapter** to the Ethernet interface, and configure your Linux Server with the IPv4 address 10.1.1.20+#group.

Configure the RADIUS server. Edit the file /etc/freeradius/clients.conf and add the access credentials for the AP (10.0.#.100):

```
       client 10.0.#.100 {
              secret = 'key'
       }
```

Where # is your group number and an example of key is: `ARGROUP00#` .

Define the user credentials by editing the file /etc/freeradius/users and adding the line

```
       "labredes"   Cleartext-Password := "labcom"
```

Note: confirm that this is not the last line of the configuration file.

Restart the radius server:

```
       sudo service freeradius restart
```

Configure the default gateways of the AP:

```
       ip default-gateway 10.0.#.254
```

and, at the server, add an IPv4 static route to the wireless network:

```
       route add -net 10.0.#group.0/24 gw 10.1.1.(100+#group)
```

16. Configure the AP with WPA-EAP to enable WPA Enterprise (with LEAP) authentication in VLAN 1 (SSID rede#group).

```
 AP(config)#aaa new-model
!Configure information about the server and its authentication/authorization ports:
 AP(config)#aaa group server radius name_server
 AP(config-sg-radius)#server 10.1.1.20+#group auth-port 1812 acct-port 1813
 AP(config)#aaa authentication login name_eap_methods group name_server
!Configure TKIP in the wireless interface:
 AP(config)#interface dot11Radio 0
 AP(config-if)#encryption mode ciphers tkip
!This defines the method for the underlying EAP when third-party clients are in use.
 AP(config-if)#dot11 ssid rede#group
 AP(config-ssid)#authentication open eap name_eap_methods
!This defines the method for the underlying EAP when Cisco clients are in use.
 AP(config-ssid)#authentication network-eap name_eap_methods
!Configure the engagement of WPA key management.
 AP(config-ssid)#authentication key-management wpa
!Associate the Interface associated to the router to the Radius Server and include the default gateway
 AP(config)#ip default-gateway 10.1.#group.254
 AP(config)#ip radius source-interface f0/0    !or f0/0.1 with VLANs
!Configure where the RADIUS server is and the key between the AP and server.
 AP(config)#radius-server host 10.1.1.20+#group auth-port 1812 acct-port 1813 key key
       !Example of a key: ARGROUP00# (Use the key configured in the RADIUS server)
```

Then, configure the PC1 to access the network (SSID rede#group) with the corresponding key. With PC2 in wireless monitor mode capture and analyze the phase of WPA enforcement. Check the connectivity between the PC1 and the network elements through a set of pings, and analyze the exchanged packets. Disconnect PC1 from the wireless network.

17. With PC2 in network 10.1.1.0/24, start an Ethernet capture with Wireshark. Connect PC1 to the wireless network (SSID rede#group). Analyze the RADIUS packets exchanged between your AP and the RADIUS server.