Instituto Tecnológico y de Estudios Superiores de Monterrey
Campus Guadalajara

TC3013 Fundamentos de redes inalámbricas
Verano 2016

Ramiro Alejandro Bermúdez Uribe
Horacio Herrera González

Proyecto Final

Rafael López Peña - A01630163
Héctor Hurtado Felipe - A01228533
Erik Mendoza Ruiz- A01226009
Félix Amado Iniguez Iniguez-A01226058

Introducción

En el siguiente proyecto, como equipo, nos dedicamos a planear, simular e instalar físicamente en el laboratorio de redes, una infraestructura de red con la capacidad de soportar a clientes de manera inalámbrica, tolerancia a fallas mediante el protocolo HSRP con el cual los clientes no notarán si uno de los Switches capa 3 caen y una administración de los Access Point mediante una Wireless LAN Controller en un esquema FlexConnect.

En dicha infraestructura hay capacidad para 800 hosts mediante los Access Point. Estos 800 hosts se pueden distribuir en 4 diferentes SSIDs. Existen otros dos segmentos, uno donde se encuentran todos los servidores para que la red funcione y otro específico para la administración de los dispositivos de red.
Sin duda alguna la red puede salir a internet, y se asegura que aunque alguna conexión falle, el internet sigue disponible pues hay redundancia gracias al protocolo de ruteo y también al protocolo HSRP.

Así mismo, en el caso de los switches (capa dos y capa tres), se tiene activado VTP para facilitar el manejo de los segmentos de red existentes.La red está balanceada, esto quiere decir dos o más dispositivos se encargan de procesar la información y gracias a esto se ve aumentada la eficiencia de la red.

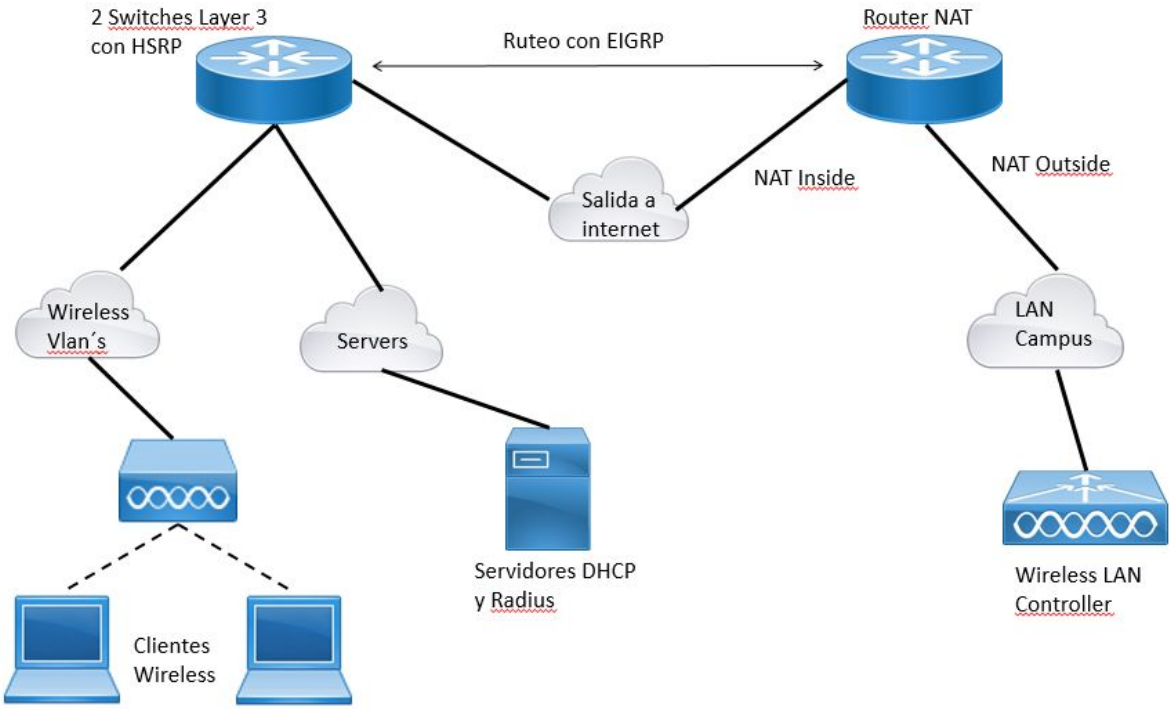
Para la parte inalámbrica se implementa cuatro tipos de seguridad para el acceso a la red y todo administrado bajo dos Wireless LAN Controllers, la controladora principal que se encarga de estar monitoreando los Access Point y la secundaria, la cual es un espejo de la primaria, que entra en funcionamiento si la controladora principal cae.

Objetivo(s)

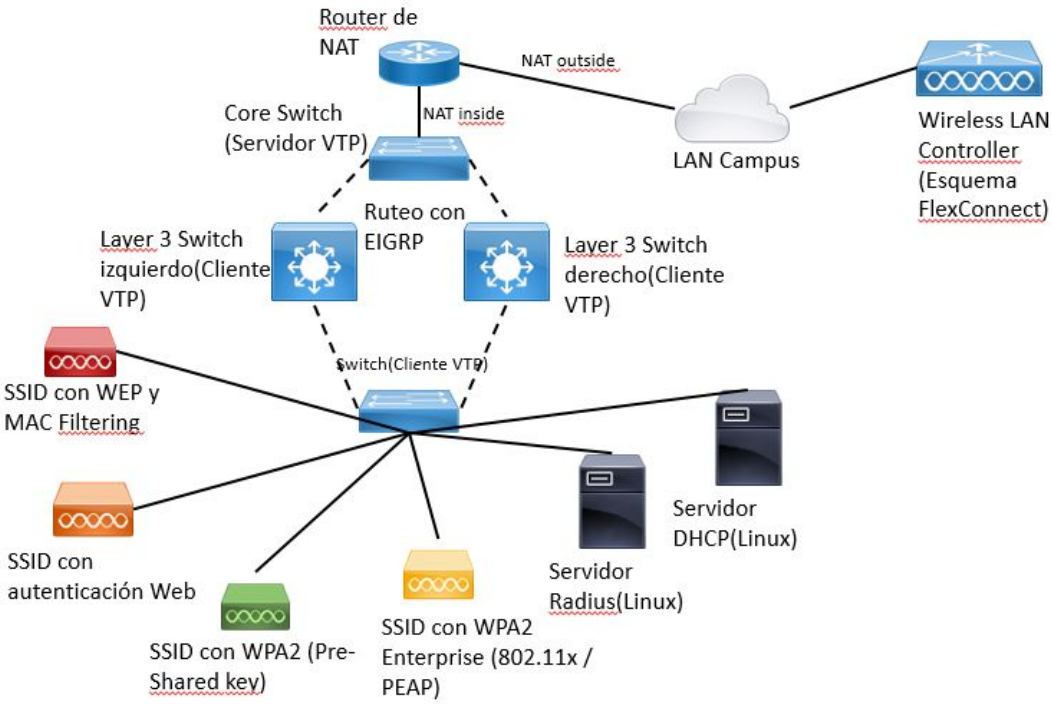
- Configurar, interconectar y administrar una red Wireless LAN usando Wireless LAN Controllers.
- Configurar, interconectar y administrar la red LAN que dará servicio a la red Wireless LAN, implementando los protocolos EIGRP, HSRP y VTP.
- Investigar cómo configurar un SSID con seguridad WPA2-Enterprise con un servidor RADIUS.
- Analizar y reparar fallas en la red.

Topología

- *Topología lógica*



- *Topología física*



Direccionamiento

	Descripción	Red	Máscara	Default Gateway	Interface
Vlan 770	**Wep y MAC Filtering**	**172.20.160.0**	**255.255.255.0**	**172.20.160.254**	**Vlan 770**
Vlan 771	**Web authentication**	**172.20.161.0**	**255.255.255.0**	**172.20.161.254**	**Vlan 771**
Vlan 772	**Wpa2 PSK**	**172.20.162.0**	**255.255.255.0**	**172.20.162.254**	**Vlan 772**
Vlan 773	**Wpa2 enterprise**	**172.20.163.0**	**255.255.255.0**	**172.20.163.254**	**Vlan 773**
Vlan 774	**Administración**	**172.20.164.0**	**255.255.255.240**	**172.20.164.14**	**Vlan 774**
Vlan 775	**Servidores**	**172.20.164.16**	**255.255.255.248**	**172.20.164.22**	**Vlan 775**

Configuraciones

1. Configuraciones de los dispositivos.

Router de NAT

```
service password-encryption
hostname RouterNAT

enable secret cisco

clock timezone CST -6 0

no ip domain lookup

key chain quiero100
 key 1
  key-string 7 quiero100

username cisco privilege 15 secret cisco

interface Embedded-Service-Engine0/0
 no ip address
 shutdown

interface GigabitEthernet0/0
 ip address 172.20.164.1 255.255.255.240
 ip authentication mode eigrp 42 md5
 ip authentication key-chain eigrp 42 quiero100
 ip nat inside

interface GigabitEthernet0/1
 description NAT
 ip address dhcp
 ip nat outside
```

```
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000

interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000

router eigrp 42
 network 172.20.160.0 0.0.7.255
 network 172.20.164.0 0.0.0.15
 passive-interface default
 no passive-interface GigabitEthernet0/0

ip nat inside source list 1 interface GigabitEthernet0/1 overload
ip nat inside source static udp 172.20.164.18 1812 interface GigabitEthernet0/1
1812

access-list 99 permit 172.20.164.0 0.0.0.15
access-list 99 permit 172.20.164.16 0.0.0.7
access-list 99 permit 172.20.163.0 0.0.0.255
access-list 99 permit 172.20.162.0 0.0.0.255

line con 0
 exec-timeout 5 0
 login local

line vty 0 4
 access-class 99 in
 exec-timeout 5 0
 login local

line vty 5 15
 access-class 99 in
 exec-timeout 5 0
 login local

end
```

Configuración del Router de NAT.

Switch server

```
service password-encryption

hostname SwitchServer

enable secret cisco

username cisco privilege 15 secret cisco
```

```
clock timezone CST -6

no ip domain-lookup

interface range FastEthernet0/1 - 20
 spanning-tree portfast

interface FastEthernet0/21
 description Puerto Trunk para SwitchL3 Derecho
 switchport mode trunk

interface FastEthernet0/22
 description Puerto Trunk para SwitchL3 Izquierdo
 switchport mode trunk

interface FastEthernet0/23
 description Puerto Trunk para Router NAT
 switchport access vlan 774
 switchport mode access

interface FastEthernet0/24

interface GigabitEthernet0/1

interface GigabitEthernet0/2

interface Vlan1
 no ip address
 no ip route-cache
 shutdown

interface Vlan774
 ip address 172.20.164.2 255.255.255.240
 no ip route-cache

ip default-gateway 172.20.164.1

access-list 3 permit 172.20.162.0 0.0.0.255
access-list 3 permit 172.20.163.0 0.0.0.255
access-list 3 permit 172.20.164.0 0.0.0.15
access-list 3 permit 172.20.164.16 0.0.0.7

line con 0
 exec-timeout 5 0
 login local

line vty 0 4
 access-class 3 in
 exec-timeout 5 0
 login local

line vty 5 15
 access-class 3 in
 exec-timeout 5 0
 login local

end
```

Configuración del Switch server.

Layer 3 Switch izquierdo.

```
service password-encryption
hostname SwitchL3-IZQ

enable secret cisco

username cisco privilege 15 secret cisco

clock timezone CST -6
ip routing
no ip domain-lookup

key chain quiero100
 key 1
   key-string quiero100

interface range FastEthernet0/1 - 21
 switchport mode dynamic desirable
 spanning-tree portfast

interface FastEthernet0/22
 description Puerto Trunk para SwitchCliente
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/23
 description Puerto Trunk para SwitchServer
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/24
 switchport mode dynamic desirable

interface GigabitEthernet0/1
 switchport mode dynamic desirable

interface GigabitEthernet0/2
 switchport mode dynamic desirable

interface Vlan1
 no ip address
 shutdown

interface Vlan770
 bandwidth 20000
 ip address 172.20.160.2 255.255.255.0
 ip helper-address 172.20.164.18
 standby 1 ip 172.20.160.254
 standby 1 preempt
 standby 1 authentication md5 key-string 7 02050D480809

interface Vlan771
 bandwidth 20000
```

```
 ip address 172.20.161.2 255.255.255.0
 ip helper-address 172.20.164.18
 standby 2 ip 172.20.161.254
 standby 2 priority 110
 standby 2 preempt
 standby 2 authentication md5 key-string 7 045802150C2E

interface Vlan772
 bandwidth 20000
 ip address 172.20.162.2 255.255.255.0
 ip helper-address 172.20.164.18
 standby 3 ip 172.20.162.254
 standby 3 preempt
 standby 3 authentication md5 key-string 7 121A0C041104

interface Vlan773
 bandwidth 20000
 ip address 172.20.163.2 255.255.255.0
 ip helper-address 172.20.164.18
 standby 4 ip 172.20.163.254
 standby 4 priority 110
 standby 4 preempt
 standby 4 authentication md5 key-string 7 00071A150754

interface Vlan774
 bandwidth 20000
 ip address 172.20.164.3 255.255.255.240
 ip authentication mode eigrp 42 md5
 ip authentication key-chain eigrp 42 quiero100
 standby 5 ip 172.20.164.14
 standby 5 preempt
 standby 5 authentication md5 key-string 7 110A1016141D

interface Vlan775
 ip address 172.20.164.20 255.255.255.248
 standby 6 ip 172.20.164.22
 standby 6 priority 110
 standby 6 preempt
 standby 6 authentication md5 key-string 7 121A0C041104

router eigrp 42
 passive-interface default
 no passive-interface Vlan774
 no auto-summary
 network 172.20.0.0

ip default-gateway 172.20.164.1
ip route 0.0.0.0 0.0.0.0 Vlan774

access-list 3 permit 172.20.162.0 0.0.0.255
access-list 3 permit 172.20.163.0 0.0.0.255
access-list 3 permit 172.20.164.0 0.0.0.15
access-list 3 permit 172.20.164.16 0.0.0.7

line con 0
 exec-timeout 5 0
 login local
```

```
line vty 0 4
 access-class 3 in
 exec-timeout 5 0
 login local

line vty 5 15
 access-class 3 in
 exec-timeout 5 0
 login local

end
```

Configuración del Layer 3 Switch izquierdo.

Layer 3 Switch derecho.

```
service password-encryption

hostname SwitchL3-DER
enable secret cisco

username cisco privilege 15 secret cisco

ip routing
no ip domain-lookup

key chain quiero100
 key 1
   key-string quiero100

interface range FastEthernet0/1 - 21
 switchport mode dynamic desirable
 spanning-tree portfast

interface FastEthernet0/22
 description Puerto Trunk para SwitchCliente
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/23
 description Puerto Trunk para SwitchServer
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/24
 switchport mode dynamic desirable

interface GigabitEthernet0/1
 switchport mode dynamic desirable

interface GigabitEthernet0/2
 switchport mode dynamic desirable

interface Vlan1
 no ip address
```

```
 shutdown

interface Vlan770
 bandwidth 20000
 ip address 172.20.160.3 255.255.255.0
 ip helper-address 172.20.164.18
 standby 1 ip 172.20.160.254
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string 7 030752180500

interface Vlan771
 bandwidth 20000
 ip address 172.20.161.3 255.255.255.0
 ip helper-address 172.20.164.18
 standby 2 ip 172.20.161.254
 standby 2 preempt
 standby 2 authentication md5 key-string 7 070C285F4D06

interface Vlan772
 bandwidth 20000
 ip address 172.20.162.3 255.255.255.0
 ip helper-address 172.20.164.18
 standby 3 ip 172.20.162.254
 standby 3 priority 110
 standby 3 preempt
 standby 3 authentication md5 key-string 7 110A1016141D

interface Vlan773
 bandwidth 20000
 ip address 172.20.163.3 255.255.255.0
 ip helper-address 172.20.164.18
 standby 4 ip 172.20.163.254
 standby 4 preempt
 standby 4 authentication md5 key-string 7 045802150C2E

interface Vlan774
 bandwidth 20000
 ip address 172.20.164.4 255.255.255.240
 ip helper-address 172.20.164.18
 ip authentication mode eigrp 42 md5
 ip authentication key-chain eigrp 42 quiero100
 standby 5 ip 172.20.164.14
 standby 5 priority 110
 standby 5 preempt
 standby 5 authentication md5 key-string 7 00071A150754

interface Vlan775
 bandwidth 20000
 ip address 172.20.164.21 255.255.255.248
 standby 6 ip 172.20.164.22
 standby 6 preempt
 standby 6 authentication md5 key-string 7 05080F1C2243

router eigrp 42
 passive-interface default
 no passive-interface Vlan774
```

```
 no auto-summary
 network 172.20.0.0

ip default-gateway 172.20.164.1
ip route 0.0.0.0 0.0.0.0 Vlan774

access-list 3 permit 172.20.162.0 0.0.0.255
access-list 3 permit 172.20.163.0 0.0.0.255
access-list 3 permit 172.20.164.0 0.0.0.15
access-list 3 permit 172.20.164.16 0.0.0.7

line con 0
 exec-timeout 5 0
 login local
line vty 0 4
 access-class 3 in
 exec-timeout 5 0
 login local
line vty 5 15
 access-class 3 in
 exec-timeout 5 0
 login local

end
```

Configuración del Layer 3 Switch derecho.

Switch cliente

```
service password-encryption
hostname SwitchCliente

enable secret cisco

username cisco privilege 15 secret 5 $1$fsV9$4zEoLmeN4uwdtgFBkcRBW.
no ip domain-lookup

interface FastEthernet0/1
 description Puerto Trunk para AP
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 774
 switchport trunk allowed vlan 1,770-779
 switchport mode trunk

interface FastEthernet0/2
 description Puerto Trunk para AP
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 774
 switchport trunk allowed vlan 1,770-779
 switchport mode trunk

interface FastEthernet0/3
 description Puerto Trunk para AP
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 774
 switchport trunk allowed vlan 1,770-779
```

```
 switchport mode trunk

interface FastEthernet0/4
 description Puerto Trunk para AP
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 774
 switchport trunk allowed vlan 1,770-779
 switchport mode trunk

interface FastEthernet0/5
 description Puerto de acceso para servidor DHCP
 switchport access vlan 775
 switchport mode access
 no cdp enable
 spanning-tree portfast

interface FastEthernet0/6
 description Puerto de acceso para servidor Radius
 switchport access vlan 775
 switchport mode access
 no cdp enable
 spanning-tree portfast

interface FastEthernet0/7
 switchport access vlan 771
 switchport mode access
 no cdp enable
 spanning-tree portfast

interface FastEthernet0/8
 switchport access vlan 772
 switchport mode access
 no cdp enable
 spanning-tree portfast

interface FastEthernet0/9
 description AP
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 774
 switchport trunk allowed vlan 1,770-779
 switchport mode trunk
 spanning-tree portfast

interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 774
 switchport trunk allowed vlan 1,770-779
 switchport mode trunk

interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 774
 switchport trunk allowed vlan 1,770-779
 switchport mode trunk

interface FastEthernet0/12
 switchport mode dynamic desirable
```

```
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 774
 switchport trunk allowed vlan 1,770-779
 switchport mode trunk

interface FastEthernet0/14
 switchport mode dynamic desirable

interface FastEthernet0/15
 switchport mode dynamic desirable

interface FastEthernet0/16
 switchport mode dynamic desirable

interface FastEthernet0/17
 switchport mode dynamic desirable

interface FastEthernet0/18
 switchport mode dynamic desirable

interface FastEthernet0/19
 switchport mode dynamic desirable

interface FastEthernet0/20
 switchport mode dynamic desirable

interface FastEthernet0/21
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,770-779
 switchport mode trunk

interface FastEthernet0/22
 description Puerto Trunk SwitchL3 Derecho
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/23
 description Puerto Trunk SwitchL3 Izquierdo
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/24
 switchport mode dynamic desirable

interface GigabitEthernet0/1
 switchport mode dynamic desirable

interface GigabitEthernet0/2
 switchport mode dynamic desirable

interface Vlan1
 no ip address
 shutdown

interface Vlan774
```

```
 ip address 172.20.164.6 255.255.255.240

ip default-gateway 172.20.164.1
ip route 0.0.0.0 0.0.0.0 Vlan774

access-list 3 permit 172.20.162.0 0.0.0.255
access-list 3 permit 172.20.163.0 0.0.0.255
access-list 3 permit 172.20.164.0 0.0.0.255


line con 0
 exec-timeout 5 0
 login local

line vty 0 4
 access-class 3 in
 exec-timeout 5 0
 login local

line vty 5 15
 access-class 3 in
 exec-timeout 5 0
 login local

end
```

Configuración del switch cliente.

2. Servidor DHCP

Para hacer un servidor de DHCP en un Linux se puede hacer de dos maneras, la manera tradicional y la manera rápida. La manera tradicional es bajar un archivo de la página de isc.org, descomprimir, compilar e instalar el servicio desde Linux. La manera rápida es utilizar el comando apt-get.

```
sudo apt-get -y install isc-dhcp-server
```

Después de hacer la instalación en un archivo seleccionamos la interfaz por donde se repartirán las direcciones.

```
sudo nano /etc/default/isc-dhcp-server
```

```
INTERFACES=”eth2"
```

Después de haber configurado la interfaz por donde se repartirán las direcciones, editamos el archivo de configuración del DHCP que se encuentra en el directorio: `/etc/dhcp/dhcpd.conf`

```
# /etc/dhcp/dhcpd.conf

ddns-update-style none;
ddns-updates off;
default-lease-time 300;
max-lease-time 300;

# Para cuando se usa Syslog:
# log-facility local7;

option netbios-node-type 8;
option netbios-name-servers 172.20.164.18;
option domain-name "barco.mx";
option domain-name-servers 10.40.42.76;
option space Cisco_LWAPP_AP;
option Cisco_LWAPP_AP.server-address code 241 = array of ip-address;

shared-network Vlan_770{
        subnet 172.20.160.0 netmask 255.255.255.0 {
                range 172.20.160.10 172.20.160.254;
                option broadcast-address 172.20.160.255;
                option routers 172.20.160.254;
        }
}

shared-network Vlan_771{
        subnet 172.20.161.0 netmask 255.255.255.0 {
                range 172.20.161.10 172.20.161.254;
                option broadcast-address 172.20.161.255;
                option routers 172.20.161.254;
        }
}

shared-network Vlan_772{
        subnet 172.20.162.0 netmask 255.255.255.0 {
                range 172.20.162.10 172.20.162.254;
                option broadcast-address 172.20.162.255;
                option routers 172.20.162.254;
        }
}

shared-network Vlan_773{
        subnet 172.20.163.0 netmask 255.255.255.0 {
                range 172.20.163.10 172.20.163.254;
                option broadcast-address 172.20.163.255;
                option routers 172.20.163.254;
        }
}

shared-network Vlan_774{
        subnet 172.20.164.0 netmask 255.255.255.240{
                range 172.20.164.7 172.20.164.14;
                option broadcast-address 172.20.164.15;
                option routers 172.20.164.14;
                class "Cisco AP c3500"{
```

```
                        match if option vendor-class-identifier = "Cisco AP
c3500";
                        option vendor-class-identifier "Cisco AP c3500";
                        vendor-option-space Cisco_LWAPP_AP;
                        option Cisco_LWAPP_AP.server-address 10.40.72.33;
                }
        }
}
shared-network Vlan_775{  # Servidores
        subnet 172.20.164.16 netmask 255.255.255.248 {
                range 172.20.164.20 172.20.164.22;
                option broadcast-address 172.20.164.23;
                option routers 172.20.164.22;
        }
}
```

Configuración del DHCP.

3. Servidor Radius

Para instalar un servidor Radius en Linux Ubuntu,la manera más sencilla es instalar los repositorios de forma directa, mediante el siguiente comando:

```
sudo –i
apt-get install freeradius
```

Una vez instalado el servicio,se necesitarán configurar los clientes que utilizarán el servicio de Radius (controladoras).

En el archivo ubicado en /etc/freeradius/clients.conf se configurarán las direcciones de las controladoras clientes, así como su llave de autenticación entre el servidor y la controladora.

```
client 10.40.72.33 {
      secret    = eri
      shortname = wlc
      nastype   = cisco
}

client 10.40.72.34 {
        secret    = eri
        shortname = wlc
        nastype   = cisco
}
```

Después procedimos a modificar el archivo /etc/freeradius/eap.conf en el cual especificamos el protocolo de autenticación de usuarios que se utilizará para acceder a la red inalambrica WPA Enterprise.

```
eap {
     default_eap_type = peap
     …
     peap {
           default_eap_type = mschapv2
           copy_request_to_tunnel = yes
           use_tunneled_reply = yes
     ...
}
```

Al final se configura el archivo /etc/freeradius/user,dónde estará el registro de los usuarios y contraseñas,para acceder a la red.

```
### WEB-AUTH & WPA2/Dot1x/PEAP/MSCHAPv2

rafa   Cleartext-Password := "rafa"

felix  Cleartext-Password := "felix"
```

Después de editar los archivos se reiniciará el servidor para aplicar los cambios,El comando es felix@felix:~$ sudo service freeradius restart.

4. Acceso a internet NAT/PAT

En la red existe un router que es específico para hacer la salida hacia internet mediante NAT/PAT. Mediante esto el router convierte nuestras direcciones privadas en direcciones públicas. En caso de PAT convierte una ip privada en una pública y para PAT; una ip pública para toda la red, pero lo hace por diferentes puertos. Para configurar esto se debe tener una interfaz la cual dará salida y otra que dará entrada. Para esto debemos usar una configuración como la siguiente:

```
RouterNAT# configure terminal
RouterNAT(config)# no access-list 1
RouterNAT(config)# access-list 1 permit 172.20.0.0 0.0.255.255
RouterNAT(config)# ip nat inside source list 1 Interface GigabitEthernet
0/1 overload
RouterNAT(config)# interface GigabitEthernet 0/1
RouterNAT(config-if)# ip address dhcp
RouterNAT(config-if)# ip nat outside
RouterNAT(config)# interface GigabitEthernet 0/0
RouterNAT(config-if)# ip nat inside
```

Configuración de NAT en el RouterNAT.

Básicamente lo que hacen los siguientes comandos son crear una ACL (Access-list) la cual permitirá la salida de toda la red y después se aplica la ACL en la configuración de NAT y le declaramos que la interfaz, por donde saldrá nuestro tráfico. El overload hace referencia al PAT para que nuestra red saliga con una misma ip pero por diferentes puertos.

Para probar que esto nos funcionó correctamente debemos checar el status de la interfaz. Para esto utilizamos el comando `show interfaces` + la interfaz a verificar.

```
RouterNAT#show interfaces gigabitEthernet 0/1

GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is c464.139a.7ee9 (bia
c464.139a.7ee9)

  Description: NAT
  Internet address is 10.40.72.98/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
      reliability 255/255, txload 1/255, rxload 1/255

  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1Gbps, media type is RJ45
  output flow-control is XON, input flow-control is XON
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:03, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 307000 bits/sec, 26 packets/sec
  5 minute output rate 32000 bits/sec, 11 packets/sec
      1038104 packets input, 973071358 bytes, 0 no buffer
      Received 28276 broadcasts (0 IP multicasts)
      0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 watchdog, 0 multicast, 0 pause input
      797019 packets output, 149641497 bytes, 0 underruns
      0 output errors, 0 collisions, 1 interface resets
      60 unknown protocol drops
      0 babbles, 0 late collision, 0 deferred
      4 lost carrier, 0 no carrier, 0 pause output
      0 output buffer failures, 0 output buffers swapped out
```

Staus de la interfaz GigabitEthernet 0/1 en el Router de NAT.

En la parte superior nos debe aparecer una dirección dada por la red del campus. En caso que esta no nos haya entregado dirección nos mostrará un mensaje: `the ip address will be negotiated`.

5. Ruteo con el Protocolo EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) es un protocolo de ruteo vector distancia creado por Cisco. Este nos permite hacer el ruteo basado en la mejor ruta. Esto se determina con 4 parámetros o métricas: Bandwidth, Delay, Confiabilidad y carga.

Para este caso no usamos otro protocolo como OSPF, ya que solo estamos trabajando con dispositivos Cisco y por lo tanto conocen y hablan EIGRP. Pero eso no indica que no sea posible utilizar OSPF u otro protocolo distinto.

Para configurar EIGRP debemos hacer que todos nuestros dispositivo estén en el mismo sistema autónomo y luego de haber definido es utilizamos la siguiente configuración.

```
RouterNAT(config-router)# router eigrp 42
RouterNAT(config-router)# network 172.20.160.0 0.0.7.255
RouterNAT(config-router)# network 172.20.164.0 0.0.0.15
RouterNAT(config-router)# passive-interface default
RouterNAT(config-router)# no passive-interface GigabitEthernet0/0
```

Configuración de EIGRP en RouterNAT

Lo que hace esa configuración es declarar que se usará EIGRP con el sistema autónomo 42 y que conoce las redes `172.20.160.0/21` y `172.20.164.0/28`. El comando passive-interface hace que las interfaces seleccionadas dejen de enviar mensajes de EIGRP. Lo que se hace aquí es aplicar lógica negada y negamos todas la interfaces y después negamos las interfaces que queremos que manden mensajes de EIGRP. Al hacer la doble negación esta queda activa y manda mensajes de EIGRP.

Para agregar seguridad en el ruteo se le pueden colocar llaves para que se autentiquen entre los vecinos EIGRP. Para crear un llavero debemos entrar al modo configuración y utilizar los siguientes comandos.

```
RouterNAT(config)#key chain quiero100
RouterNAT(config-keychain)#key 1
RouterNAT(config-keychain-key)# key-string quiero100
```

Configuración de llaves.

Aquí declaramos un llavero con el nombre “Quiero100”. Después decimos que la llave uno será un String con encriptación y luego ponemos el String. En este caso la llave ya está encriptada por el algoritmo md5.

Para aplicar la llave debemos colocarla en las interfaces que hablan EIGRP.

```
RouterNAT(config-if)# ip authentication mode eigrp 42 md5
RouterNAT(config-if)# ip authentication key-chain eigrp 42 quiero100
```

Aplicación de las llaves en las interfaces.

Para aplicar la llave accedemos a la interfaz y dentro de ella le decimos que se debe autentificar cuanto esté el protocolo EIGRP con su respectivo sistema autónomo y al final se le pone md5 el cual es el algoritmo de encriptación utilizado.

Por último solo le indicamos que se debe autenticar con la llave generada y su respectivo sistema autónomo.

6. Layer 3 Switch y Lightweight Access Point.

Algunos dispositivos de red pueden trabajar en más de una capa del modelo OSI. En este caso un Switch trabaja solo en la capa de enlace de datos (Layer 2), según Cisco. Para que un Switch Cisco trabaje en capa 3 se le debe cambiar el sistema operativo. Para hacer esto hay dos formas. La manera rápida es hacerlo mediante TFTP. Nos ponemos una dirección estática en una PC y otra en una interfaz Vlan. Probamos la conexión mediante un ping y utilizamos el siguiente comando.

```
Switch# archive download-sw /overwrite /reload
tftp://10.0.0.2/c3550-ipservices-tar.122-44.SE2.tar
```

Comando para cambiar el IOS del Dispositivo.

Este comando sobreescribe el sistema operativo que tiene actualmente y luego se reinicia después de haber terminado. El archivo `c3550-ipservices-tar.122-44.SE2.tar` es el IOS que se le cargará. Mediante esto podemos hacer el cambio del IOS al Switch.

Para el Access Point es el mismo caso y el mismo comando solo cambia el archivo a cargar. Esto se le hace al Access Point para que se convierta en un Lightweight Access Point y pueda ser administrado por la controladora.

7. Tolerancia a fallas mediante HSRP

Hot Standby Router Protocol (HSRP) es un protocolo de Cisco. Se ponen dos o más routers para que exista redundancia, se activa este protocolo para que tenga un router preferido (el de mayor prioridad) y si este falla, se activa el segundo que tenga mayor prioridad.

Para activarlo, se ponen los siguientes comandos (ejemplo de la subinterfaz de administración de un switch capa tres):

```
SwitchL3(config-subif)# standby 5 ip 172.20.164.14
SwitchL3(config-subif)# standby 5 priority 110
SwitchL3(config-subif)# standby 5 preempt
SwitchL3(config-subif)# standby 5 authentication md5 key-string quiero100
```

Lo que se hizo fue poner una dirección IP virtual (para que la comparta con la misma subinterfaz del otro router o switch capa tres), se le da la máxima prioridad para que se tenga preferencia sobre el otro dispositivo (al otro se le dejó en 100), se pone el comando preempt para que el switch intente convertirse en active y finalmente se le coloca una llave para permitir el acceso a esta interfaz solo a ciertos dispositivos. Ahora hay que poner lo mismo en la subinterfaz del otro switch, excepto la prioridad que ya se mencionó.

8. Administración de VLANs mediante VTP

VLAN Trunking Protocol (VTP) tiene como función administrar VLANs de manera más sencilla entre varios switches Cisco. Tiene que existir un switch servidor, que es el que tiene derecho a crear, modificar y eliminar las VLANs; puede haber un switch transparente, que simplemente deja pasar la información; y finalmente el switch cliente, que no puede hacer nada respecto a VLANs mas que recibirlas por parte del switch servidor. Para nuestro proyecto, se nos solicitó establecer un switch como servidor y el resto como clientes. Para el switch servidor, se pusieron los siguientes comandos:

```
SwitchServer(config)# vtp mode transparent
SwitchServer(config)# vtp version 2
SwitchServer(config)# vtp domain HijosDeHoracio
SwitchServer(config)# vtp password cisco
SwitchServer(config)# vtp mode server
```

Todas las configuraciones se tienen que llevar a cabo con el switch en modo transparente (está en modo servidor por default), se pone la versión dos y se establece un dominio y una contraseña que tendrán en común con el resto de los switches asociados al mismo. Para los switches clientes, es colocar exactamente los mismos comandos, exceptuando el último, ya que ahora será *vtp mode client*.

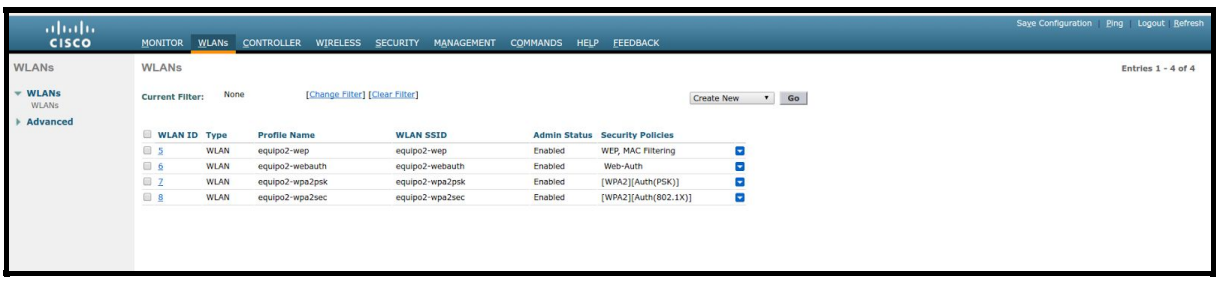
Así de esta forma creamos las VLANs de la 770 a la 779 en el switch servidor y no tenemos que hacer lo mismo en los dos switches capa tres y el switch con los puertos de acceso, puesto que ahora son clientes y las heredarán directamente.

9. Opción 43 en DHCP.

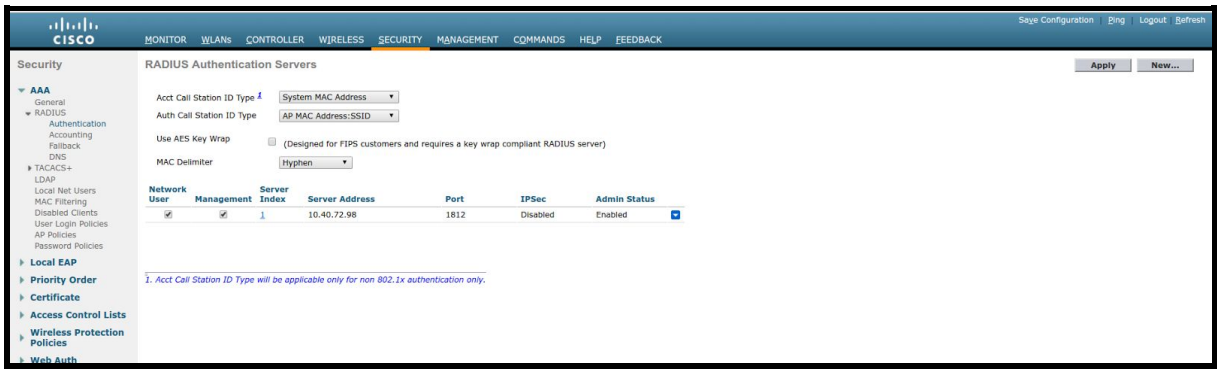
Para que los Access Point LAP puedan conectarse a una controladora en específico, en el servidor del DHCP de Linux se habilitó la opción 43, en el archivo de configuración, donde se especifica la dirección ip de la controladora y que se dará este servicio de configuración a un AP c3500.

```
shared-network Vlan_774{
        subnet 172.20.164.0 netmask 255.255.255.240{
                range 172.20.164.7 172.20.164.14;
                option broadcast-address 172.20.164.15;
                option routers 172.20.164.14;
                class "Cisco AP c3500"{
                        match if option vendor-class-identifier = "Cisco AP
c3500";
                        option vendor-class-identifier "Cisco AP c3500";
                        vendor-option-space Cisco_LWAPP_AP;
                        option Cisco_LWAPP_AP.server-address 10.40.72.33;
                }
        }
}
```

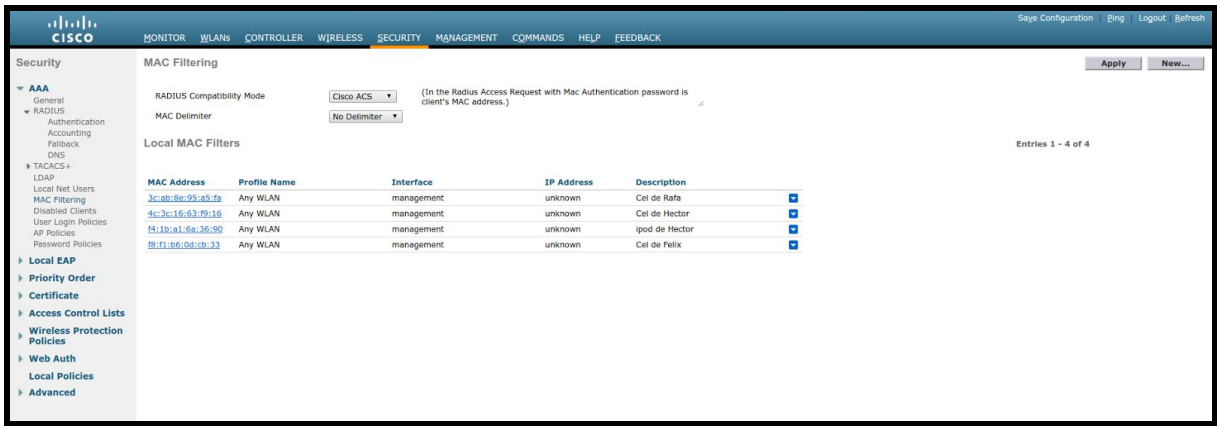
10. Administración de los Access Point.



Se configuraron 4 SSID, cada uno debe estar asociado a una subred diferente. Estos cuentan con seguridad diferente (MAC Filtering + WEP, Web Authentication, WPA2-PSK, WPA2-Enterprise) .



Aquí está la parte del Radius Authentication donde agregaremos la dirección del servidor para validar si estaban los usuarios y las contraseñas.



Esta es la parte de MAC filtering donde agregamos las mac address que seran permitidas para conectarse a la red.

11. Power Over Ethernet

Power Over Ethernet (PoE) es una tecnología implementada en algunos dispositivos de red para alimentar a otros dispositivos de red. Este está regularizado por el estándar IEEE 802.3af. En nuestra infraestructura el Switch cliente tiene el PoE y este fue utilizado para alimentar a los Access Point. Para esto simplemente se necesita conectar el Access Point al Switch y el puerto donde se conecta debe tener el protocolo CDP activo, ya que mediante este negocía la potencia con la que se alimentará. Esto aplica solo si el Access Point es Cisco.

Si queremos verificar que puerto está alimentando y cual es la potencia que se suministra podemos usar el siguiente comando en el Switch.

```
SwitchCliente# show power inline

Available:360(w)   Used:46(w)   Remaining:314(w)
```

```
Interface Admin  Oper    Power   Device           Class Max
                         (Watts)
--------- ------ ---------- ------- ------------------ ----- ----
Fa0/1 auto   off         0.0   n/a                n/a   15.4
Fa0/2 auto   off         0.0   n/a                n/a   15.4
Fa0/3 auto   off         0.0   n/a                n/a   15.4
Fa0/4 auto   off         0.0   n/a                n/a   15.4
Fa0/5 auto   off         0.0   n/a                n/a   15.4
Fa0/6 auto   off         0.0   n/a                n/a   15.4
Fa0/7 auto   off         0.0   n/a                n/a   15.4
Fa0/8 auto   off         0.0   n/a                n/a   15.4
Fa0/9 auto   on          15.4  AIR-CAP3502I-A-K9        15.4
Fa0/10auto   on          15.4  AIR-CAP3502I-A-K9        15.4
Fa0/11auto   off         0.0   n/a                n/a   15.4
Fa0/12auto   off         0.0   n/a                n/a   15.4
Fa0/13auto   on          15.4  AIR-CAP3502I-A-K9        15.4
Fa0/14auto   off         0.0   n/a                n/a   15.4
Fa0/15auto   off         0.0   n/a                n/a   15.4
Fa0/16auto   off         0.0   n/a                n/a   15.4
Fa0/17auto   off         0.0   n/a                n/a   15.4
Fa0/18auto   off         0.0   n/a                n/a   15.4
Fa0/19auto   off         0.0   n/a                n/a   15.4
Fa0/20auto   off         0.0   n/a                n/a   15.4
Fa0/21auto   off         0.0   n/a                n/a   15.4
Fa0/22auto   off         0.0   n/a                n/a   15.4
Fa0/23auto   off         0.0   n/a                n/a   15.4
Fa0/24auto   off         0.0   n/a                n/a   15.4
```

Comando Show power inline.

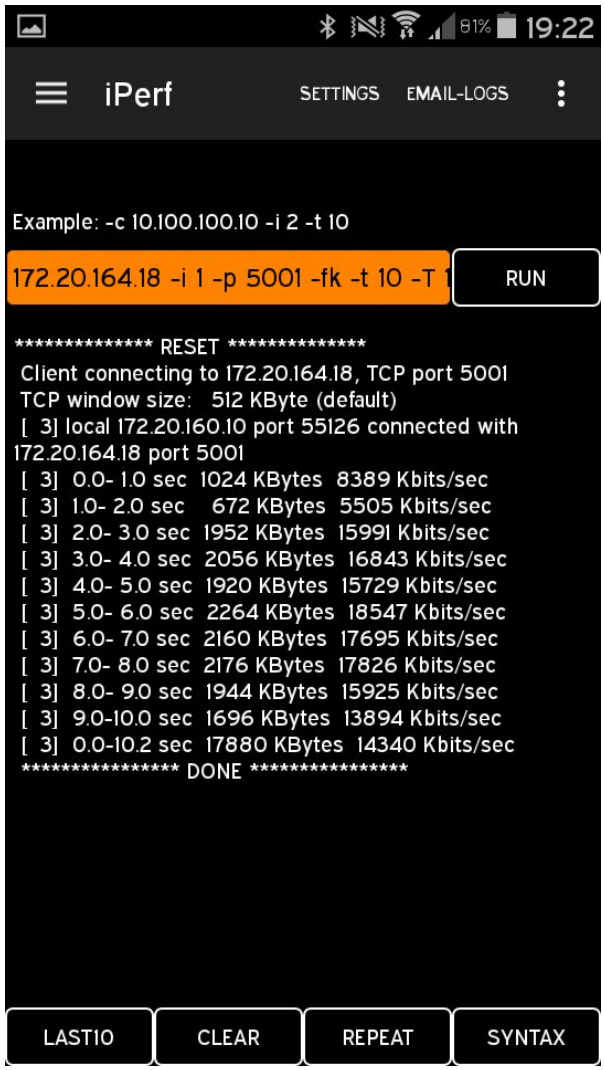
Aquí se muestra la potencia que puede entregar en total el dispositivo; la que está en uso y la restante. Allí se muestra que a los Access Point se les entrega 15.4 Watts. Esta potencia está definida por el estándar IEEE 802.3af, ya mencionado antes. Un detalle con esta tecnología es que al llegar al límite de potencia entregada pueden pasar dos cosas: no le entrega potencia al último dispositivo conectado o simplemente deja de entregar potencia a todos los dispositivos.

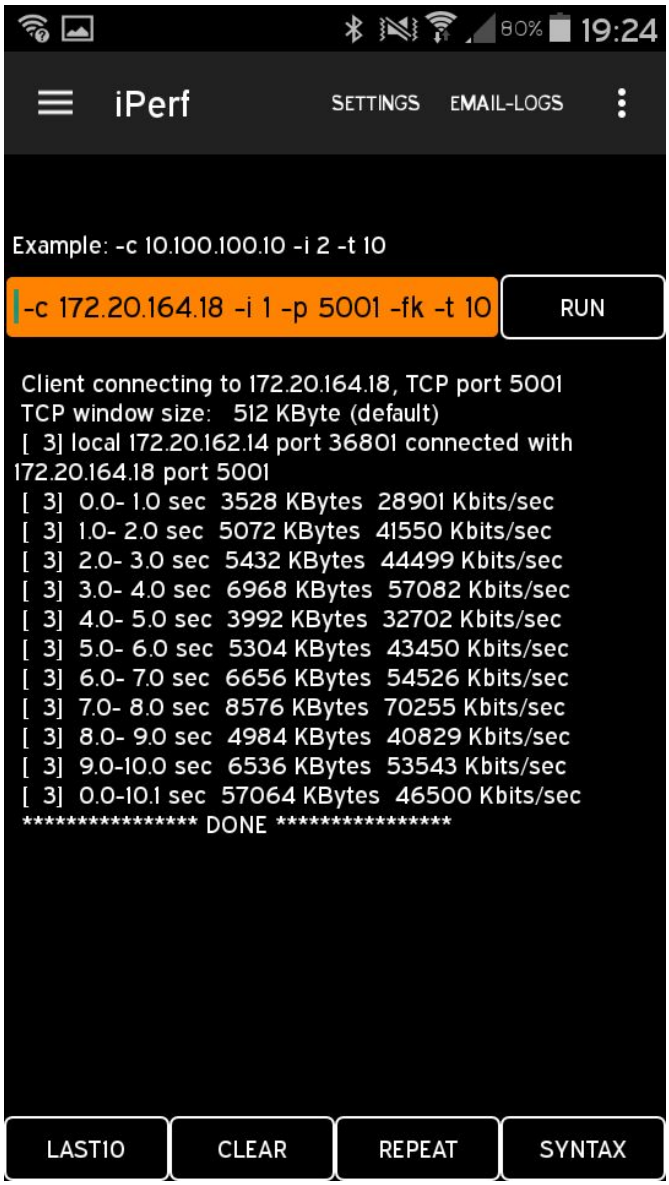
Desempeño de la red

Una vez terminada la construcción de la red, se procedió a analizar algunos datos tanto de los Access Points como de los cuatro SSIDs creados, como su canal y potencia en el caso de los APs y su desempeño e intensidad de señal en el caso de los SSIDs. Algunos de estos datos se obtenían directamente de la controladora, pero otros solo se podían conseguir con algún programa de análisis, como iperf. En nuestro caso, utilizamos WiFi Analyzer y Aruba Utilities. Para utilizar este último, era obligatorio estar conectado al SSID que se quería analizar, asimismo tener una dirección IP de algún equipo conectado a la misma red para poder hacerle ping y

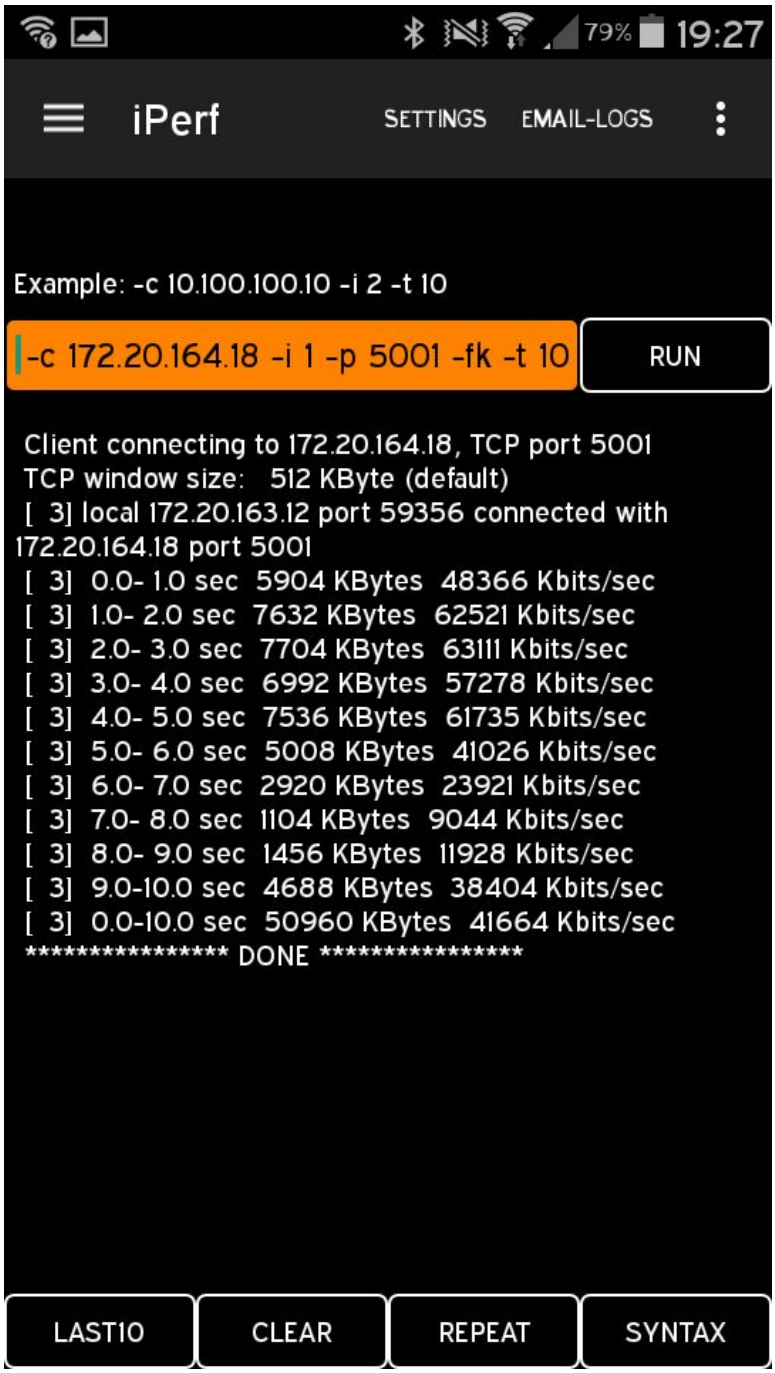
obtener la información deseada. A continuación, las capturas de pantalla de un teléfono celular con la aplicación de Aruba Utilities abierta y conectado a los SSIDs que creamos.

Análisis del SSID con autenticación WEP + MAC Filtering





Análisis del SSID con autenticación WPA2-PSK



Análisis del SSID con autenticación WPA2-Enterprise

NOMBRE DEL AP	RADIO	CANAL	POTENCIA
AP3502 MEDIOS AUD1B	2.4 GHz	11	7
AP3502 MEDIOS AUD1B	5 GHz	64	6
AP3502 AUL3 2B	2.4 GHz	1	7
AP3502 AUL3 2B	5 GHz	56	7
APe8b7.482c.6772	2.4 GHz	1	8
APe8b7.482c.6772	5 GHz	56	7
AP3502_MEDIOS_1B	2.4 GHz	6	8
AP3502_MEDIOS_1B	5 GHz	149	7

NOMBRE DEL SSID	DESEMPEÑO (Mbps)	ANCHO DEL CANAL (MHz)	INTENSIDAD DE SEÑAL (dBm)	NIVEL DE SNR (dB)
equipo2-wep	15.5	20	-36	39
equipo2-webauth	19.5	20	-42	41
equipo2-wpa2psk	53.7	20	-48	44
equipo2-wpa2sec	56.2	20	-59	33

Resolución de problemas

1. Nuestro servidor DHCP estaba configurado de manera correcta en Linux, sin embargo el equipo contaba con una ruta estática que mandaba nuestros request a internet. Para eso borramos le cambiamos la ruta para que salga por la interfaz correcta.
2. Cuando planeamos la arquitectura de la red tomamos los dispositivos de tal forma que no teníamos ninguno con power inline, así que al tratar de conectar los Access Points ninguno encendía. Para esto tuvimos que sacar un puerto trunk por un reflejo del rack y pasarlo a otro switch y mediante VTP hacer que aprendiera las Vlan configuradas de la red.

3. Configurada la opción 43 en el DHCP Linux este no enviaba la dirección de la controladora a los Access Point. El detalle de esto es que tenía una línea mal escrita y esto hacía que no mandara la dirección.
4. Los puertos que llevan a los mirrors de la mesa del laboratorio C no sirven, específicamente, los MC01-1,2,3 los demás si funcionan.

Resolución de problemas (Examen final)

En lo que respecta al examen final, las cosas que detectamos que fueron cambiadas para que la red no funcionara de la forma correcta son las siguientes:

1. El primer error que se detectó fue en una interfaz del router. Había una lista de acceso que negaba ciertas direcciones. Simplemente se procedió a eliminar esta lista.
2. Posteriormente, tratamos de hacer Telnet a los switches, pero vimos que esto no era posible. Al analizar por qué no eran alcanzables (a través de varios comandos *show*) nos percatamos con *show standby* que la VLAN 774 (la de administración) estaba en estado Init. Con esto sabíamos que no estaba haciendo HSRP. Al ver el porqué de esta situación, con el comando *show vlan*, vimos que la VLAN 774 había desaparecido. Esto se solucionó accediendo al Switch Server y volviendo a levantar la VLAN caída. Así, por VTP, el resto de los switches también la obtuvieron y todo volvió a la normalidad.

Conclusiones

Rafael López Peña

Este proyecto fue bastante interesante ya que utilizamos todo lo visto durante el curso y lo juntamos para hacer una red funcional. Esto no significa que fuese fácil concluirlo, ya que tuvimos bastantes controversias al momento de la elaboración tanto en capa física con los cables que flapeaban o que simplemente no funcionaban y en capa de red con algunas direcciones mal asignadas. Esto en general fue bastante interesante ya que nos enfocamos bastante en la parte wireless mediante el uso de una Wireless LAN Controller. Gracias a esta podiamos hacer cambios a los Access Point mediante una interfaz gráfica y verificar datos que no se veían tan fácil en la terminal de los mismos.

Otro punto que quiero tocar aquí es el trabajo en equipo, ya que considero que es fundamental en cualquier organización. Formar un equipo de trabajo puede resultar difícil al inicio del mismo ya que cada persona que integrará al equipo de trabajo tiene pensamientos y cultura diferente es por ello que el comprometerse con un equipo de trabajo se deberá involucrar completamente para todas las actividades que se desarrollen.

La verdad sobre este proyecto es que lo logramos concluir pese a todas los topes encontrados y gracias a estos pude aprender bastante sobre las posibles fallas que se puedan encontrar en las redes.

Héctor Hurtado Felipe

Me gustó mucho este proyecto, ya que aplicamos todo lo visto durante el curso, además de lo ya visto en Redes I y II. Tuvimos varios contratiempos al construir la red, como cables o puertos que fallaban, comandos que se nos olvidaban colocar o poníamos de manera incorrecta y nos llevaba varios minutos o incluso horas darnos cuenta de esto, conectar los APs a la controladora correcta, e incluso tuvimos que lidiar con un apagón provocado por la fuerte lluvia que se registró en la madrugada e hizo que algunos de los dispositivos se reiniciaran.

Pero al final, ya con el proyecto completado con éxito, siento que los problemas que tuvimos nos hacen aprender todavía más que si no hubiéramos tenido ninguno, ya que te puedes dar cuenta de para qué sirve cada comando y qué es lo que sucedió cuando el mismo no se pone o se pone de manera equivocada.

Pese a que nos llevó algo de tiempo entenderla y hacerla funcionar adecuadamente, también me agradó que tuvimos que involucrar a la controladora para administrar los LAPs, quizá hubiera sido más tedioso configurar los cuatro APs uno por uno.

Así que, en conclusión, siento que el proyecto fue retador pero definitivamente fue el adecuado para nosotros, ya que así fue una excelente manera de reforzar todo lo visto en estos tres cursos de Redes.

Erik Raul Mendoza Ruiz

En lo personal el proyecto fue muy retador, ya que integramos todos los conocimientos de las otras dos clases de redes, tambien existian concepto que ya no recordaba de dichas clases por ejemplo el comando de ip route 0.0.0.0 0.0.0.0, para que nos resolviera la salida a internet cuando no conocia la ruta. Creo que al principio configuramos el router de NAT mal, lo que nos ocasionó una serie de problemas, también duramos mucho tiempo tratando de hacer que funcionara el radius authentication, el problema principal fue que la controladora hacia la petición pero se quedaba en el Router de NAT, ya que no sabia como mandarselo al servidor, ya que no teníamos configurado el puerto 1812, la dirección del servidor de radius, ni que fuera por el protocolo udp.

Otra falla fue la conexión de los access points ya que los conectabamos en puertos consecutivos y el profesor Horacio nos explicó que por conjunto de puertos existían diferentes fuentes de poder entonces existía la posibilidad de que alcanzara a levantar todos los access points.

El éxito del proyecto fue que trabajamos en equipo, nos preocupamos de la configuración de todos los dispositivos (Router,Switch, WLC, Server), si uno fallaba nos reunimos y dábamos ideas de las posibles fallas, eso ayudó bastante porque logramos encontrar una solución a cada problema. Todos teníamos conocimientos distintos, lo que complemento bastante al equipo, en lo personal yo me especialice más en el área de wireless.
Considero que la clase estuvo muy completa porque llegamos a cubrir más del material del curso, aparte los profesores hacían la clase muy retadora con teoría al principio y complementándola con práctica al final. Aparte el dejar de lado el simulador del packet tracer y hacer todas las configuraciones de manera física y con el material adecuado, hacía más enriquecedora la clase.

Felix Amado Iniguez Iniguez
Durante este curso de redes inalámbricas tenía muchas expectativas,en este proyecto incorporamos todos los conocimientos adquiridos durantes redes 1,redes 2 y redes inalámbricas.Considero que el proyecto fue retador e integró completamente todo lo esencial en el diseño de una red compleja,de alto desempeño y aplicable a un laboratorio o empresa.

Redes inalámbricas es toda una ciencia,donde solo hemos explorado sus fundamentos,no obstante considero que con los conocimientos adquiridos somos capaces de diseñar una red de alto nivel y de manera profesional.Al momento de integrar el proyeto y el diseno, tuvimos complicaciones y errores;Las configuraciones y diseno del ruteo lo aplicamos de forma incorrecta,tambien muchos de los conceptos y comando aplicados en redes 2 fueron necesarios.Esto nos limito y consumio tiempo,en recordar y poder aplicar, para solucionar nuestros errores.Por ejemplo, la lista de acceso que permita en el router NAT el paso y descubrimiento del servidor Radius por el puerto 1812.

```
ip nat inside source static udp 172.20.164.18 1812 interface GigabitEthernet0/1 1812
```

Otra complicación fue que en los switches de capa 3 faltaba el ruteo,el nat y el acceso a internet si estaba activo;sin embargo,los usuarios sólo conocían las rutas internas y al querer salir a internet no conocían su DNS ni forma de llegar a él y a los sitios solicitados.Para solucionar aplicamos una ruta por default.

```
ip route 0.0.0.0 0.0.0.0 Vlan774
```

En cuanto el área inalámbrica,despeje muchas dudas y preguntas que tenía de las redes inalámbricas,no conocía prácticamente nada del funcionamiento,de la seguridad y autenticación y de cómo administrarlas.Al incio pense que seria muy complicado el manejo de los AP, de la administracion de vlans y puertos.Sin embargo,fui entendiendo poco a poco como se asignaban las subredes y como era la logica.Descubrir que esta ultima era muy similar a lo visto previamente en alambrico,solo necesitamos equipos especializados para la tranmision inalambrica.

La administración de los AP mediante una controladora me pareció una herramienta excelente para el diseño y trabajo de una red.Con estas cajas se pueden diseñar y mantener en control redes realmente complejas,con diferentes SSID,Usuarios y recursos específicos.

Referencias

"Ubuntu Documentation." *Isc-dhcp-server*. n.d. Web. 01 July 2016. Available at: https://help.ubuntu.com/community/isc-dhcp-server.

"Power over Ethernet (PoE) Power Requirements FAQ." *Cisco*. Cisco Technical Support, 26 June 2008. Web. 01 July 2016. Available at: http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-ip-phone-7900-series/97869-poe-requirement-faq.html.

"Configuring EIGRP." *Cisco*. Cisco Technical Support, 23 Mar. 2008. Web. 01 June 2016. Available at: http://www.cisco.com/cisco/web/support/LA/7/75/75043_eigrp-toc.html.

Seccion de Autógrafos

Rafael López Peña

Héctor Hurtado Felipe

Erik Mendoza Ruiz

Félix Amado Iniguez Iniguez