Tecnológico de Monterrey

Fundamentos de Redes Inalámbricas

TC3013-01 / Verano 2016

PROYECTO FINAL

El presente documento establece el alcance, los requisitos y los entregables que debe de cumplir el Proyecto Final del curso. Cualquier situación o evento no previsto en este documento será resuelto bajo el criterio exclusivo de los Instructores.

REQUERIMIENTOS GENERALES.

1. Los estudiantes se dividirán en 4 equipos de 4 integrantes cada uno.

2. La fecha de presentación del proyecto funcionando para todos los equipos es el miércoles **29 de junio**.

3. Los estudiantes tendrán máximo **90 minutos** para configurar e interconectar sus dispositivos. Después de ese tiempo habrá **20 minutos** para que cada equipo presente su proyecto.

4. Cada equipo entregará un reporte en formato PDF o Word (versión 2010 o anterior).

   4.1. La fecha límite de entrega del reporte es el viernes **1 de Julio**.

5. El reporte deberá ser un documento formal con la siguiente estructura:

   5.1. Portada.

      5.1.1. Nombre y clave del curso.
      5.1.2. Nombres de los integrantes y matrículas.

   5.2. Introducción.

      5.2.1. Presentación y descripción del proyecto.

   5.3. Desarrollo.

      5.3.1. Descripción de los requerimientos de interconexión de red.
      5.3.2. Plan de asignación de VLANs y subredes.
      5.3.3. Diagramas de topología lógica (capa 3) y física (capas 1 y 2).
      5.3.4. Configuración relevante de cada dispositivo (WLC, Routers, Switches y Servidores).
      5.3.5. Explicar que hace cada parte relevante de la configuración.
      5.3.6. Incluir evidencias del trabajo (fotos o capturas de pantalla).

   5.4. Conclusiones.

      5.4.1. Descripción de las experiencias y conocimientos adquiridos individualmente y en equipo.
      5.4.2. Descripción de los contratiempo encontrados y como los solucionaron.

5.5. Bibliografía o fuentes de información electrónica.

5.5.1. Las referencias, citas y bibliografía se anexarán siguiendo el estilo APA: http://www.library.cornell.edu/resrch/citmanage/apa

OBJETIVOS GENERALES.

1. Configurar, interconectar y administrar una red Wireless LAN usando Wireless LAN Controllers.
2. Configurar, interconectar y administrar la red LAN que dará servicio a la red Wireless LAN, implementando los protocolos EIGRP, HSRP y VTP.
3. Investigar como configurar un SSID con seguridad WPA2-Enterprise con un servidor RADIUS.

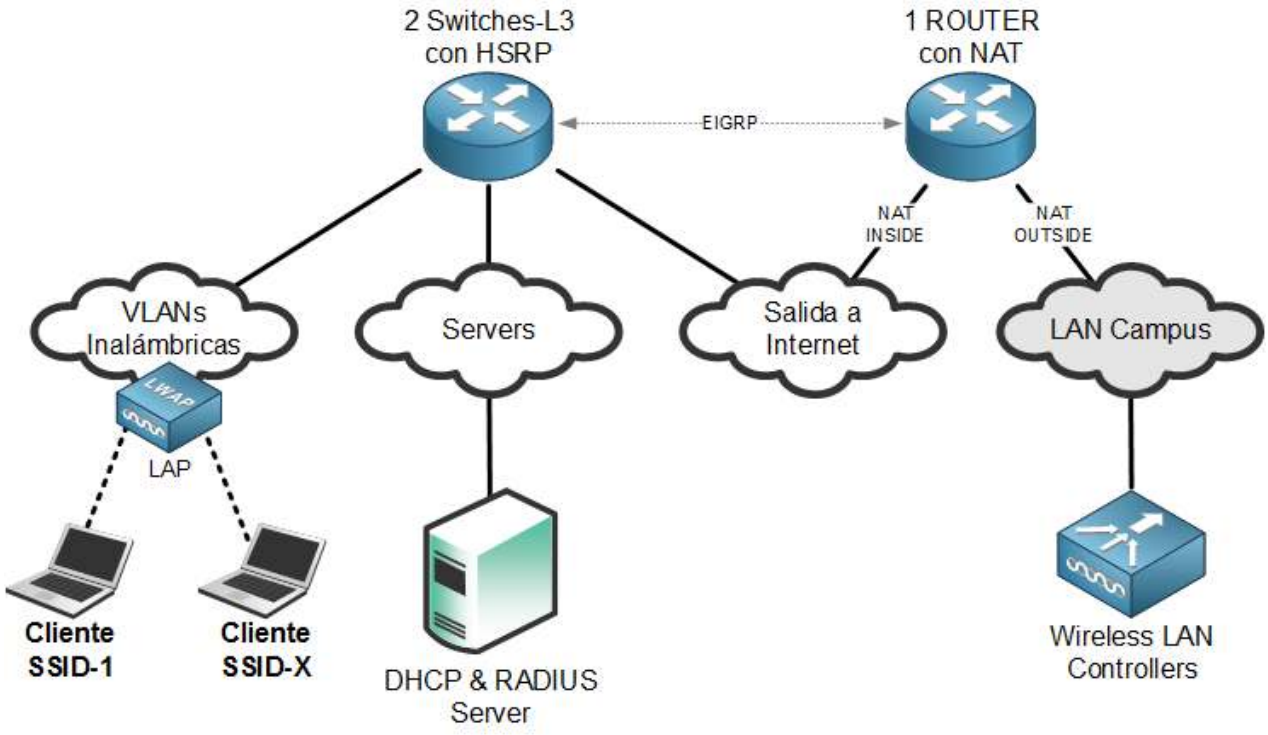
EQUIPO Y MATERIAL.

- Un dispositivo cliente por alumno para conectarse a la red inalámbrica (Laptop, Tablet, Celular, etc.).
- Al menos un servidor Linux (físico o virtual) por equipo para servicios de DHCP y RADIUS.
- Software: iperf, Wi-Fi Analyzer y Aruba Utilities.
- Un router de WAN para NAT.
- Dos switches con funciones de ruteo (para Core de la LAN).
- Un switch con Inline-Power o adaptadores de corriente directa para alimentar a los LAP.
- Dos Wireless LAN Controllers Virtuales (WLC).
- Al menos 4 Access-Points con imagen Light (LAP).
- Software de emulación de terminal (HyperTerminal, TeraTerm o Minicom).
- Cables UTP y cables de consola (rollover).

DESARROLLO.

1. Cada equipo conectará los dispositivos de red de la siguiente manera:

TOPOLOGÍA LÓGICA



2. A cada equipo le corresponde el siguiente direccionamiento:

EQUIPO	RED
1	172.20.120.0/21
2	172.20.160.0/21
3	172.20.200.0/21
4	172.20.240.0/21

2.1. La asignación de Subredes queda a elección de cada equipo dentro del rango designado.

2.2. Los estudiantes deberán aplicar las configuraciones necesarias en Switches y Routers para establecer comunicación interna (entre subredes) y hacia el exterior (LAN del Campus).

2.3. Todas las **PC** y **Servidores** deberán ser alcanzables por **ping** desde cualquier subred.

2.4. Todas las interfaces de los Routers y Switches-L3 deberán ser alcanzables por **ping** desde cualquier subred.

2.5. El ruteo de todas las Subredes debe tener redundancia por medio de HSRP (Entre Switches-L3).

2.5.1. El HSRP debe estar balanceado entre los dos Switches-L3.

2.6. El ruteo hacia la red externa debe ser por medio de EIGRP (Entre Switches-L3 y Router de NAT).

2.7. La configuración de ruteo debe ser eficiente.

3. Cada equipo tiene asignado el siguiente rango de VLANs:

EQUIPO	RANGO
1	760 - 769
2	770 - 779
3	780 - 789
4	790 - 799

3.1. Las VLANs deben propagarse entre Switches usando el protocolo VTP protegido.

3.2. Solo debe haber un Switch en modo servidor y los demás en modo cliente.

4. Deben configurar dos Wireless LAN Controllers (WLC) virtuales para administrar al menos 4 Access-Points Ligeros (LAP) en modo FlexConnect. Donde una controladora esté activa (Primaria) y la otra sea de respaldo (Secundaria).

5. El Router de NAT, además de tener reglas para permitir que los dispositivos internos puedan salir a exterior, debe tener una regla para que las WLC (outside) se puedan comunicar con el servidor de RADIUS (inside) en el puerto UDP 1812.

6. Configure 4 SSID's con los siguientes nombres y requerimientos de seguridad:

NOTA: La "X" corresponde al número del equipo.

SSID	RADIO	SEGURIDAD
equipoX-wep	11g/n	MAC Filtering + WEP de 104 ó 128 bits
equipoX-webauth	11g/n	Web Authentication
equipoX-wpa2psk	11a/n	WPA2-PSK
equipoX-wpa2sec	11a/n	WPA2-Enterprise (Dot1x/PEAP)

7. Cada SSID debe estar asociado a una subred diferente.

8. Documente el canal y la potencia que la WLC le asigna a cada LAP en cada radio:

NOMBRE DEL AP	RADIO (2.4/5GHz)	CANAL	POTENCIA

9. Realice y documente al menos una prueba de desempeño en cada SSID usando **iperf**:

NOMBRE DEL SSID	DESEMPEÑO (Mbps)	ANCHO DEL CANAL (MHz)	INTENSIDAD DE SEÑAL (dBm)	NIVEL DE SNR (dB)

9.1. Explique bajo qué condiciones se obtiene un mejor desempeño.

10. Los clientes inalámbricos deben obtener IP por DHCP del servidor Linux y tienen permitido comunicarse a cualquier dirección IP externa.

11. Los LAP solo tienen permitido comunicarse con direcciones IP internas y con las WLC. NO tiene permitido comunicarse con ningún otra IP externa.

12. Los LAP deben ir conectados a Switches con Power-Inline o con adaptadores.

13. Todos los Switches, Routers y Access-Points deben tener una dirección IP de administración en la VLAN/Subred de Servidores.

14. Solamente está permitido hacer telnet a los Switches y Routers desde la subred de servidores y las subredes inalámbricas con seguridad WPA2.

15. Los dispositivos de red deben tener aplicadas las configuraciones generales de administración y seguridad (usuarios y contraseñas).

GUÍA EXPRESS PARA CONFIGURACIÓN DE SERVIDOR RADIUS.

1. Instalar el servicio RADIUS usando el comando:

```
sudo –i

aptitude install freeradius
```

2. Editar el archivo "**/etc/freeradius/clients.conf**" para agregar la IP de la WLC y una contraseña.

```
client 10.40.72.X {
        secret                          = mylittleradius
        shortname                       = wlc
        nastype                         = cisco
}
```

3. Editar el archivo "**/etc/freeradius/eap.conf**".

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

4. Editar el archivo "**/etc/freeradius/users**".

```
### MAC FILTERING
e08871182218   Service-Type == Call-Check, Auth-Type := Accept
DEFAULT        Service-Type == Call-Check, Auth-Type := Reject
### WEB-AUTH & WPA2/Dot1x/PEAP/MSCHAPv2
user1          Cleartext-Password := "redes1"
user2          Cleartext-Password := "redes2"
```

5. En la WLC:

   5.1. ir al menú **SECURITY** > **AAA** > **RADIUS** > **Authentication** y dar click en **NEW** para dar de alta la IP externa del servidor de RADIUS (No olvide que es la IP externa del NAT) y la misma contraseña que puso en el archivo de "clients.conf".

   5.2. Crear un **SSID** y en menú de **SECURITY** configurar los siguiente en las pestañas correspondientes:

      5.2.1. LAYER 2 – Seguridad=**WPA2**, Encription=**AES** y Key Management=**802.1X**.

      5.2.2. AAA SERVERS – Authentication Servers=**Enabled**; Server 1=**Seleccionar IP del Servidor RADIUS**.

FIN DEL DOCUMENTO.