

# UNIVERSIDAD ALFONSO X EL SABIO

Red Inteligente para Campus Universitario con IoT y Servicios Multimedia

## 1. Definición del Modelo de Comunicación

### 1.1 Revisión de Modelos:

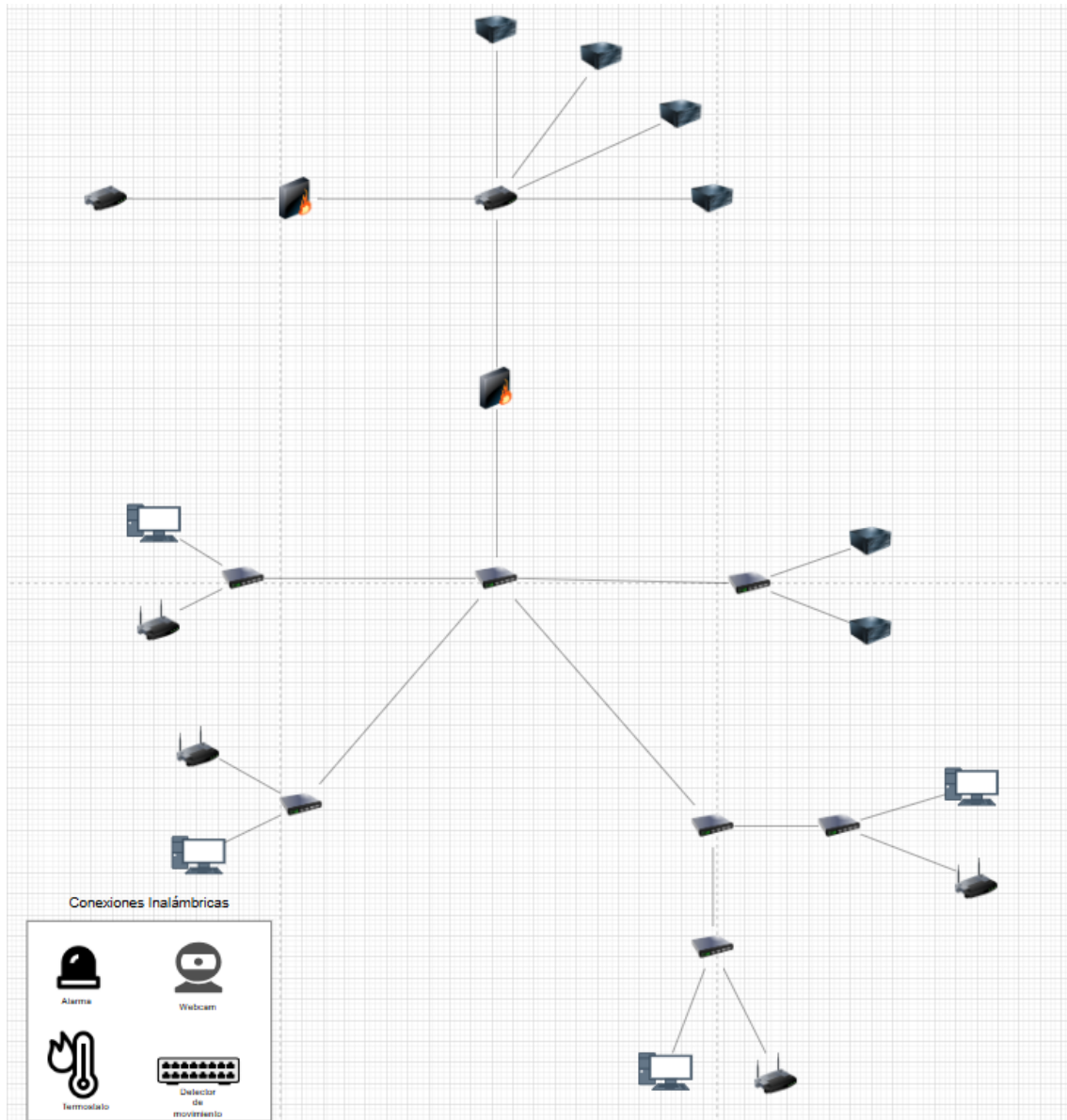
#### - Modelo OSI

1. Capa Física	Encargado de la transmisión real de bits a través de medios físicos. Tanto el cálculo de la fórmula de Shannon, las técnicas de modulación, el wifi y los cables ethernet del proyecto pertenecen a esta capa.
2. Capa de Enlace de datos	Colabora la transmisión libre de errores entre nodos, gestiona el direccionamiento a nivel de hardware. En el proyecto representa las direcciones MAC y el control de acceso al medio.
3. Capa de Red	Distribuye el direccionamiento lógico y la toma de decisiones de enrutamiento, por ejemplo, el Subneteo y esquema de rutas. En el proyecto esta capa se encarga de la direccion de broadcast, rango de host, Enrutamiento con Dijkstra, routers y configuraciones IP
4. Capa de Transporte	Se encarga de ejecutar una entrega confiable o en tiempo real, Usaremos TCP + SFTP para la transferencia de archivos y UDP + RTP para el streaming.
5. Capa de Sesión	Establece, administra y finaliza conexiones entre aplicaciones, para la gestión de diálogos entre diferentes sistemas. La multiplexación forma parte de esta capa
6. Capa de Presentación	Representa y codifica los datos, haciendo el cifrado, compresión y transformación de diferentes formatos.
7. Capa de Aplicación	Se comunica directamente con los programas que utiliza el usuario, por ejemplo, protocolos FTP/SFTP para transferir archivos, HTTP/HTTPS para los de multimedia, etc...

#### - Modelo TCP/IP

1. Capa de Acceso a Red	Sería igual que la capa física y enlace de datos en el modelo OSI. Se encarga de la transmisión de datos a nivel de hardware y de la comunican por medio físicos como el ethernet.
2. Capa de Internet	Se asemeja a la capa de red del modelo OSI. En este se gestiona las direcciones IP y el enrutamiento, por ejemplo, el algoritmo de Dijkstra.
3. Capa de Transporte	Parecida a la capa de transporte del modelo OSI. Gestiona los servicios de transporte ya sea confiable o sin conexión, TCP y UDP.
4. Capa de Aplicación	Equivalen a las capas 5, 6 y 7 del modelo OSI. Protocolos de transferencia, FTP y SFTP, manejo de contenidos HTTP y HTTPS, etc...

## 1.2 Diagrama



Como se observa en el diagrama, se trata de una red donde hay un router con acceso a internet que lleva firewall con zona desmilitarizada donde se alojan los servidores `www/mail/dns`, después sale por un firewall interno que lleva a un switch núcleo que forma parte de un anillo de switches que recorre donde cada switch corresponde a su sala pertinente, como sala servidores, sala recepción, sala biblioteca, sala aula y sala laboratorio para finalmente volver al switch núcleo.

## 2. Capa Física – Capacidad, Modulación, Eficiencia

### 2.1 Cálculo de la Capacidad de Enlaces

Utilizamos la Formula de Shannon para calcular la capacidad necesaria en los enlaces cableados e inalámbricos del campus.

B=ancho de banda.                      C=Capacidad                      SNR=relación señal/ruido.

Formula de Shannon:  $C = B \log_2 (1 + SNR)$

$$SNR(lineal) = 10^{\left(\frac{SNR(db)}{10}\right)}$$

Una señal optima SNR esta entre el rango de 18db a 30db . Una buena señal empieza a partir de los 25 db. Por lo que usaremos 25 db como dato par la capacidad de Shanon.

Calculamos:

$$SNR = 10^{\frac{25}{10}} = 316.23$$

Cableado  $B = 100 \cdot 10^6 \text{ Hz} = 100\text{Mhz}$

$C = 100 \cdot 10^6 \cdot \log_2(1 + 316.23) = 831\text{Mbps}$

Inalámbrico  $B = 80 \cdot 10^6 = 80\text{Mhz}$

$C = 80 \cdot 10^6 \cdot \log_2(1 + 316.23) = 664.8\text{Mbps}$

En conclusión, Teniendo que tanto el cableado como el inalámbrico tienen un SNR de 25bp. El cableado con ancho de banda de 100Mhz tendrá capacidad de 831 Mbps y el inalámbrico de 80Mhz será de 664.8Mbps.

## 2.2 Selección de Modulación y Evaluación de Encapsulamiento.

En el campus universitario se cuenta con laptops, móviles, streaming, lot en una gran escala, por lo que buscamos una red capaz de soportar múltiples usuarios simultáneamente de forma eficiente a pesar del gran ruido.

Se hará uso del método OFDM, usando Wifi 5/6 y 5G, este método divide el canal en muchos subsánales con su propio símbolo y multiplexado en frecuencia, lo que permite la transmisión paralela de forma eficiente y sin interferencias.

En cuanto al encapsulamiento, la transmisión de archivos en una red pasa por varios capas OSI, en cada capa agregando nuevos headers para gestionar el envío y controlar los errores, aunque no forman parte de los datos útiles, afectando a la eficiencia de transmisión.

En el siguiente caso:

Se envían 1000 bytes que incluyen

-cabecera TCP=20 bytes

-cabecera IP=20 bytes

-cabecera MAC (802.11) =34 bytes

-Tráiler (FCS y otros) =4 bytes

Todos estos bytes no son utiles por lo que se consideran bytes de sobrecarga.

Por lo que hay una sobrecarga de  $20+20+34+4=78$  bytes

Por lo que el calculo seria de  $1000/(1000+78) =92.8\%$  de eficiencia, dicho de otra manera un 7.2% de sobrecarga.

### 3. Capa de Red – Diseño de Subredes y Enrutamiento

#### 3.1 Segmentación del Campus en Subredes

Partimos del bloque privado 10.1.0.0/16 y lo dividimos en cuatro grandes áreas lógicas, cada una con máscara /22 (1 022 hosts útiles) para permitir crecimiento:

Área	Bloque	Máscara	Hosts útiles	Uso principal
IoT	10.1.0.0/22	255.255.252.0	1 022	Sensores ambientales, cámaras IP
Usuarios	10.1.4.0/22	255.255.252.0	1 022	Estudiantes
	10.1.7.0/22	255.255.252.0	1022	Profesores
Multimedia	10.1.8.0/22	255.255.252.0	1 022	Streaming en aulas, señalización digital
Administración	10.1.12.0/22	255.255.252.0	1 022	Servidores corporativos, controladores, VPN

##### 1. Área IoT (10.1.0.0/22)

VLAN	Subred	Máscara	Hosts útiles	Puerta de enlace	Broadcast
IoT_P1	10.1.0.0/26	255.255.255.192	62	10.1.0.1	10.1.0.63
IoT_P2	10.1.0.64/26	255.255.255.192	62	10.1.0.65	10.1.0.127
IoT_Signal	10.1.0.128/27	255.255.255.248	30	10.1.0.129	10.1.0.159

IoT_Serv	10.1.0.16 0/28	255.255.255.2 40	14	10.1.0.161	10.1.0.175
----------	-------------------	---------------------	----	------------	------------

## 2. Área Usuarios (10.1.4.0/22)

VLAN	Subred	Máscara	Hosts útiles	Puerta de enlace	Broadcast
Users_P1	10.1.4.0/26	255.255.255.192	62	10.1.4.1	10.1.4.63
Users_P2	10.1.4.64/26	255.255.255.192	62	10.1.4.65	10.1.4.127
Users_Signal	10.1.4.128/27	255.255.255.224	30	10.1.4.129	10.1.4.159
Users_Serv	10.1.4.160/28	255.255.255.240	14	10.1.4.161	10.1.4.175

## 3. Área Multimedia (10.1.8.0/22)

VLAN	Subred	Máscara	Hosts útiles	Puerta de enlace	Broadcast
MM_Aulas_P1	10.1.8.0/26	255.255.255.192	62	10.1.8.1	10.1.8.63
MM_Aulas_P2	10.1.8.64/26	255.255.255.192	62	10.1.8.65	10.1.8.127
MM_Signal	10.1.8.128/27	255.255.255.224	30	10.1.8.129	10.1.8.159
MM_Serv	10.1.8.160/28	255.255.255.240	14	10.1.8.161	10.1.8.175

## 4. Área Administración (10.1.12.0/22)

VLAN	Subred	Máscara	Hosts útiles	Puerta de enlace	Broadcast
Admin_P1	10.1.12.0/26	255.255.255.192	62	10.1.12.1	10.1.12.63
Admin_P2	10.1.12.64/26	255.255.255.192	62	10.1.12.65	10.1.12.127
Admin_Signal	10.1.12.128/27	255.255.255.224	30	10.1.12.129	10.1.12.159
Admin_Serv	10.1.12.160/28	255.255.255.240	14	10.1.12.161	10.1.12.175

# 4: Capa de Transporte – Selección de Protocolos y Cálculo de Ventana

## 1. Definición de Protocolos

## TCP

Servicios críticos: acceso a sistemas administrativos, transferencias de archivos, portal del campus, bases de datos.

Ventajas: control de flujo y congestión, fiabilidad (retransmisiones), garantía de orden.

## UDP

Transmisiones en tiempo real: cámaras IP, sensores IoT que envían datos de forma continua, streaming en vivo con RTP/RTCP.

Ventajas: baja sobrecarga, latencia reducida.

Gestión de calidad: implementar buffering adaptativo, FEC y control de tasa para compensar la ausencia de retransmisión.

## 2. Cálculo del Tamaño de Ventana:

Se utiliza el Bandwidth–Delay Product (BDP) para dimensionar la ventana:  
 $\text{BDP (bytes)} = \text{RTT (s)} \times \text{Ancho de banda (bytes/s)}$

$\text{Ventana (segmentos)} = \text{BDP} / \text{MSS}$

Parámetros:

Backbone (10 Gb/s, RTT 2 ms, MSS 1460 B):

$\text{BDP} = 0.002 \text{ s} \times 10 \times 10^9 \text{ bit/s} = 2.5 \times 10^6 \text{ B} \rightarrow \text{Ventana} \approx 1712 \text{ segmentos}$

Distribución–acceso (1 Gb/s, RTT 5 ms, MSS 1460 B):

$\text{BDP} = 0.005 \text{ s} \times 1 \times 10^9 \text{ bit/s} = 625\,000 \text{ B} \rightarrow \text{Ventana} \approx 428 \text{ segmentos}$

## 3. Contribución al Control de Congestión

Slow Start: crecimiento exponencial hasta ssthresh para evitar arranques bruscos.

Congestion Avoidance: crecimiento lineal tras alcanzar ssthresh.

Fast Retransmit / Fast Recovery: retransmisión rápida y ajuste de la ventana a la mitad en caso de pérdidas.

Un tamaño de ventana igual al BDP previene:

1. Subutilización (ventana muy pequeña) → desperdicio de ancho de banda.
2. Congestión excesiva (ventana muy grande) → alta latencia y pérdidas.

## 4. Gestión de Flujo en UDP

Sin control de congestión nativo: la aplicación debe limitar la tasa de envío (RTP/RTCP), usar jitter buffers y aplicar FEC.

Implementar buffering adaptativo en receptor para suavizar variaciones de retardo.

## **5. Capa de Aplicación y Multimedia – Servicios y Resolución de Nombres**

### **5.1 Diseño de Servicios**

Se usarán servicios basados en los protocolos HTTP/HTTPS y estarán destinados hacia dos propósitos dentro del campus universitario:

El Portal del Campus, que se tratará de un sitio web interactivo para los docentes, personal y alumnos. En dicho portal se proveerá información esencial como horarios de clases, eventos o recursos académicos entre otros. El HTTPS se destinará a mantener la seguridad y privacidad de información sensible con datos personales.

Un Distribuidor de Recursos Multimedia que se usará para alojar y distribuir recursos educativos y de otro tipo como:

- Acceso a grabaciones de clases.
- Material de apoyo (Apuntes, vídeos etc.).

Para esto se utiliza HTTP y HTTPS, y según la importancia del contenido, se priorizará con HTTPS que requiere autenticación.

Para la Resolución de Nombres (DNS):

- Se usará DNS como componente fundamental para el funcionamiento del campus.
- Cuando se ingrese un nombre de dominio, el sistema lo traduce a una dirección IP correspondiente.
- Para mejorar la eficiencia se usará un sistema de caché DNS local dentro del campus.

Para Autenticación de Usuarios:

Entre los métodos para controlar el acceso de los usuarios a los servicios de red están:

- Autenticación por credenciales: Los usuarios tendrán un usuario y contraseña.

### **5.2 Streaming y Multimedia**

Para el streaming y la distribución de contenido en el campus se hará uso de las siguientes UDP Streaming, HTTP Streaming y DASH:



Se utilizará el UDP para transmisiones en vivo con baja latencia de tal forma que pueda tolerar pérdidas de paquetes y se usarán protocolos RTP/RTCP para gestionar la entrega y calidad del streaming.

Para la distribución de contenido como grabaciones de clase, se usará el HTTP que dividirá el contenido en pequeños fragmentos que permiten una transmisión óptima con firewalls y proxies.

Se implementará DASH para técnicas de streaming adaptativo, ya que este permite al servidor proporcionar múltiples versiones del contenido a diferentes velocidades de bits, gracias a esto el cliente podrá cambiar entre estas versiones en función de su ancho de banda.

En cuanto al Ancho de Banda, la calidad del streaming se adaptará dinámicamente a la disponible para cada usuario, para esto el servidor codificará el contenido en múltiples velocidades de bits para que el cliente puede elegir la más óptima, se implementará buffering para suavizar las fluctuaciones del ancho de banda y así evitar interrupciones en la reproducción y por último se hará uso de controles de gestión para evitar sobrecargas en la red.

## 6. Seguridad en Redes – Plan y Configuración

### 6.1 Plan Integral de Seguridad

Control	Tecnología / Protocolo	Objetivo
<b>Perímetro</b>	Cisco ASA 5505	Filtrado de tráfico malicioso, DDoS, IPS/IDS
<b>Acceso remoto seguro</b>	VPN IPsec (AES-256/SHA-2)	Cifrado de administración y teletrabajo
<b>Cifrado extremo a extremo</b>	TLS 1.3 y SRTP	Protección de HTTP/HTTPS, SIP y streaming multimedia
<b>Autenticación usuarios</b>	AAA	Control de puerto y doble factor para acceso a la red
<b>Protección DNS</b>	DNSSEC	Firmas digitales en zonas internas y públicas para evitar spoofing

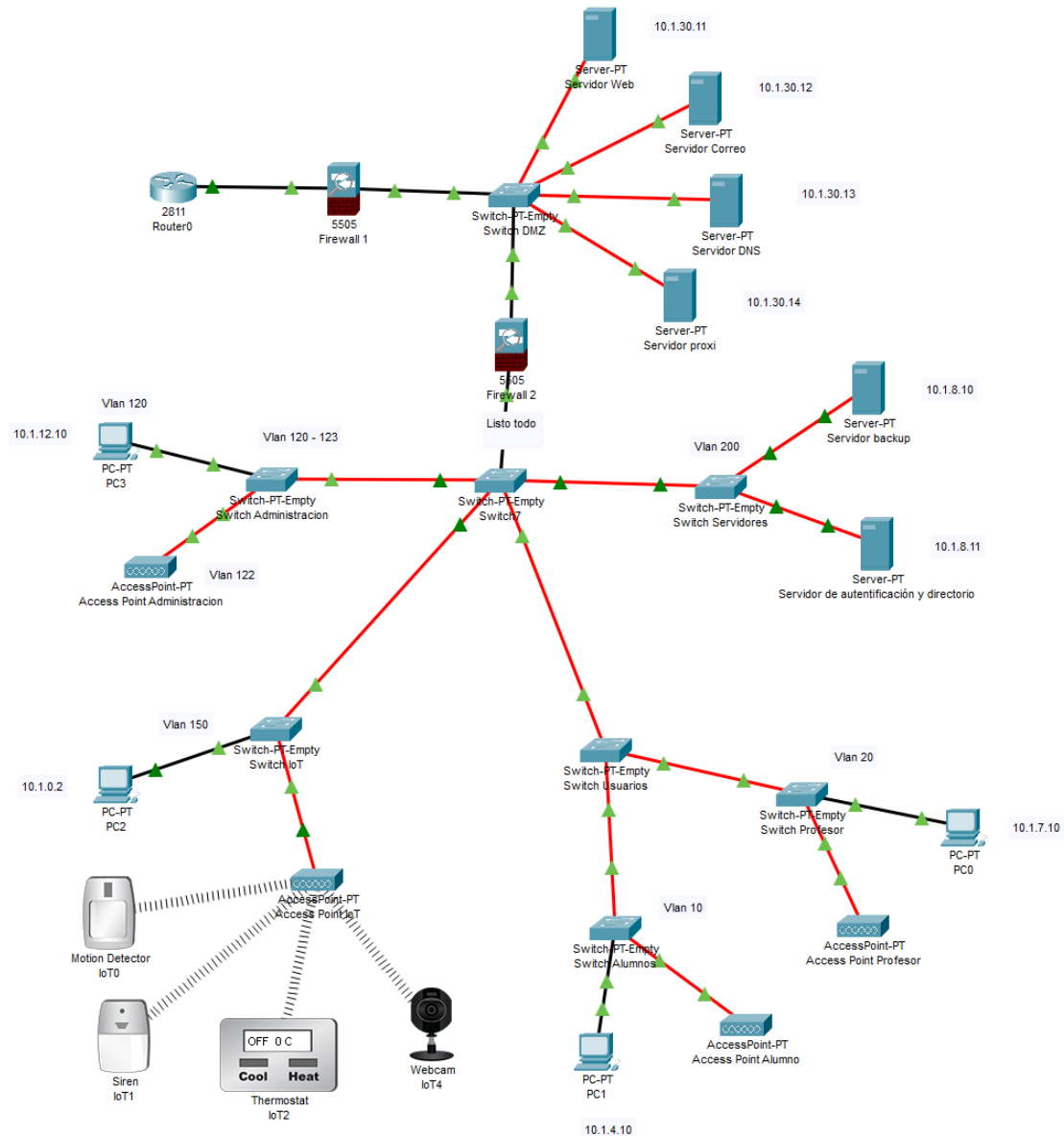
## 6.2 Configuración y justificación

Para asegurar el campus, se implementa un plan en capas. Cada nivel de la red cuenta con controles específicos:

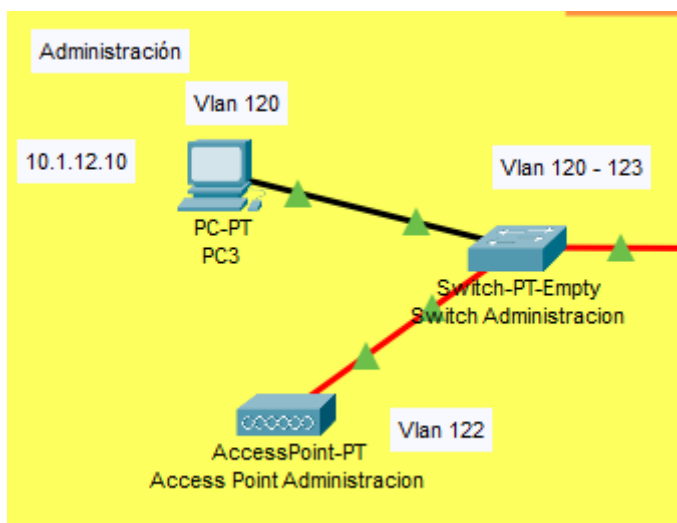
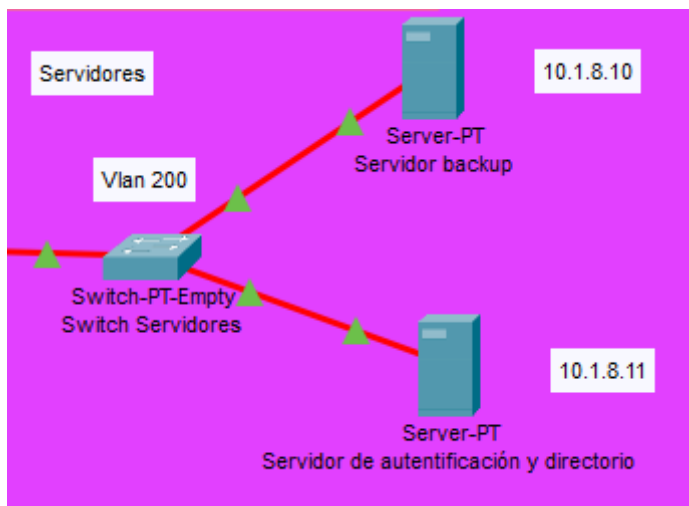
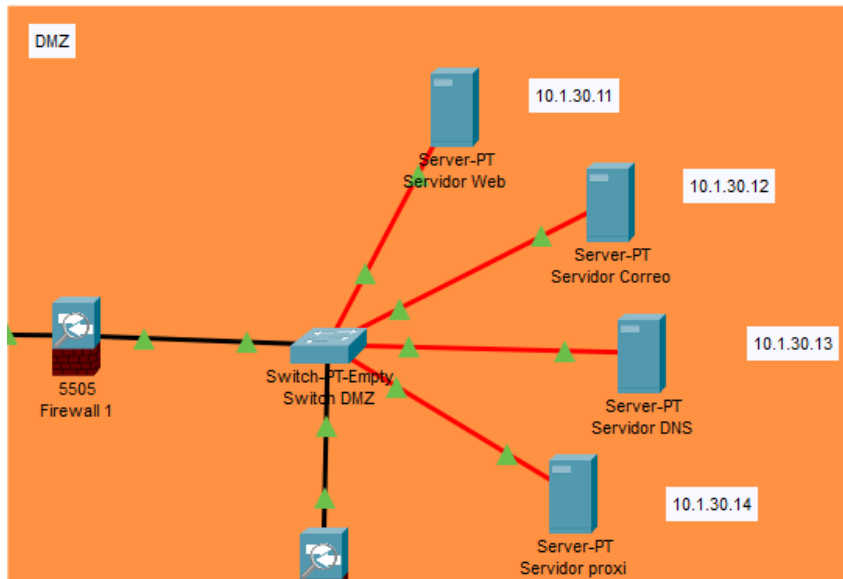
- **Perímetro:** Se configuran firewalls Cisco FPR 5505 en alta disponibilidad. Se aplican políticas de filtrado, inspección profunda de paquetes (IPS) y protección DDoS. Justificación: mitigar amenazas externas antes de que ingresen a la red interna.
- **Red Interna:** Segmentación por VLAN y switches L3 para aislar tráfico según función (IoT, usuarios, multimedia, administración). Justificación: evitar movimientos laterales y contener posibles infecciones.
- **Acceso Remoto:** Se activa VPN IPsec con cifrado AES-256 y autenticación SHA-2. Solo usuarios autorizados acceden a servicios administrativos desde fuera. Justificación: proteger la integridad de la red durante el teletrabajo o tareas remotas.
- **DNS Seguro:** Se despliega DNSSEC en los servidores DNS internos. Justificación: prevenir ataques de suplantación (DNS spoofing) y garantizar integridad en la resolución de nombres.
- **Control de Usuarios y Dispositivos:** Implementación de NAC para identificar dispositivos y aplicar políticas según perfil. Integración con servidores con protocolo AAA para autenticación centralizada. Justificación: asegurar que solo usuarios válidos accedan a la red.

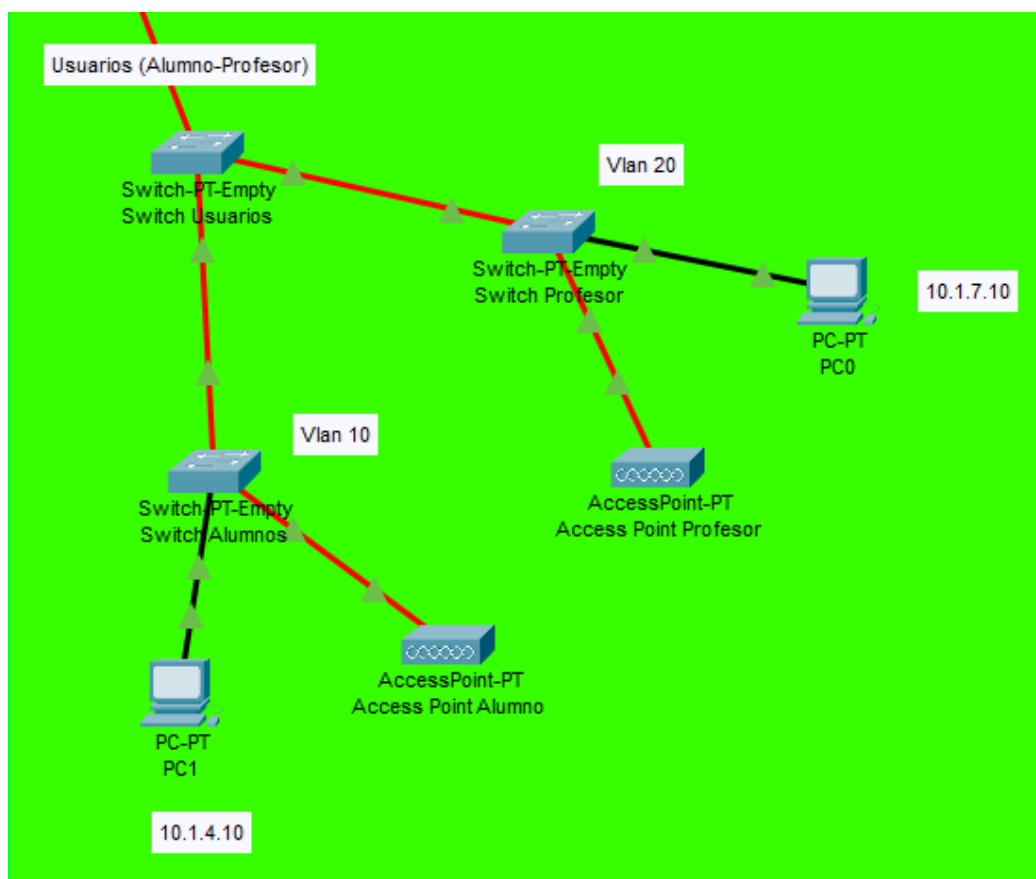
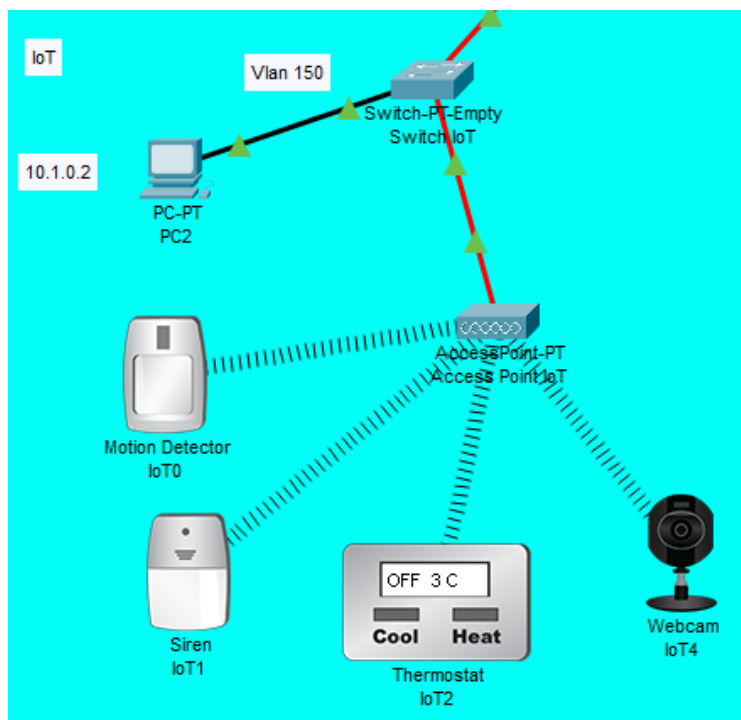
## 7. Implementación Cisco Packet Tracer

### 7.1 Construcción de la Topología del Campus



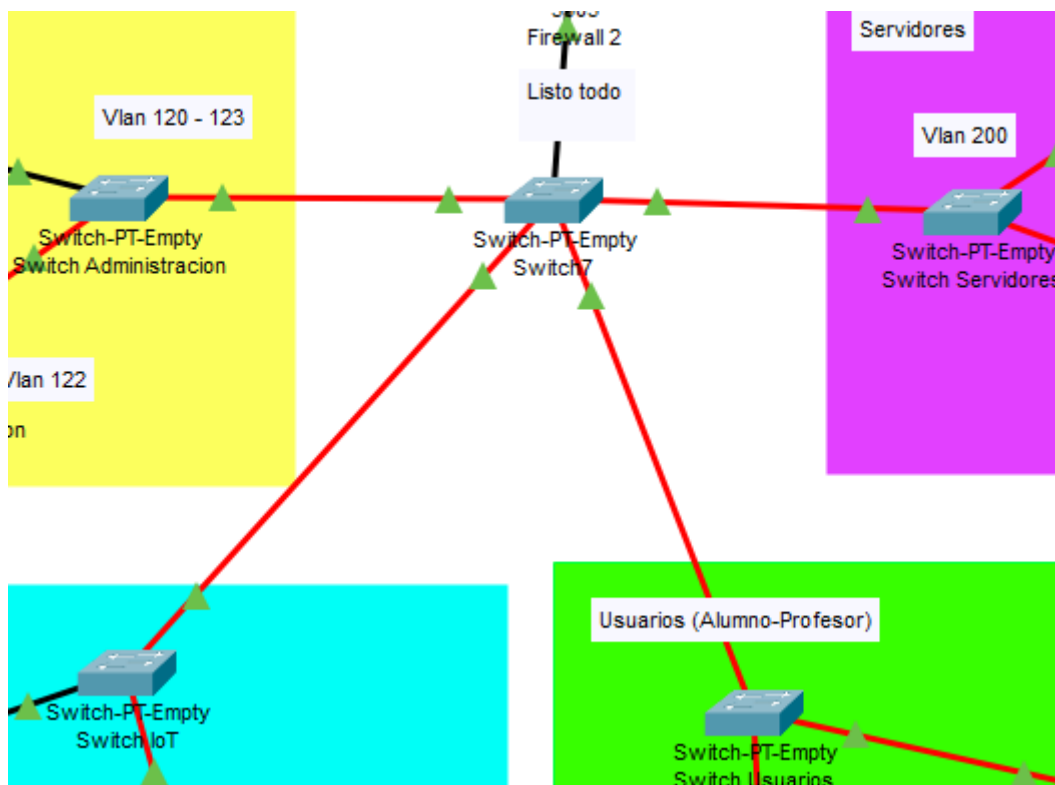
La red dividida en segmentos:





## 7.2 Configuración de Rutas y Políticas de Seguridad

Topología de los switches:



Hemos creado una red con una topología denominada topología de estrella, todos los switches están como cliente menos el primero de usuario que está como transparente ya que pasa al de profesor y alumno.

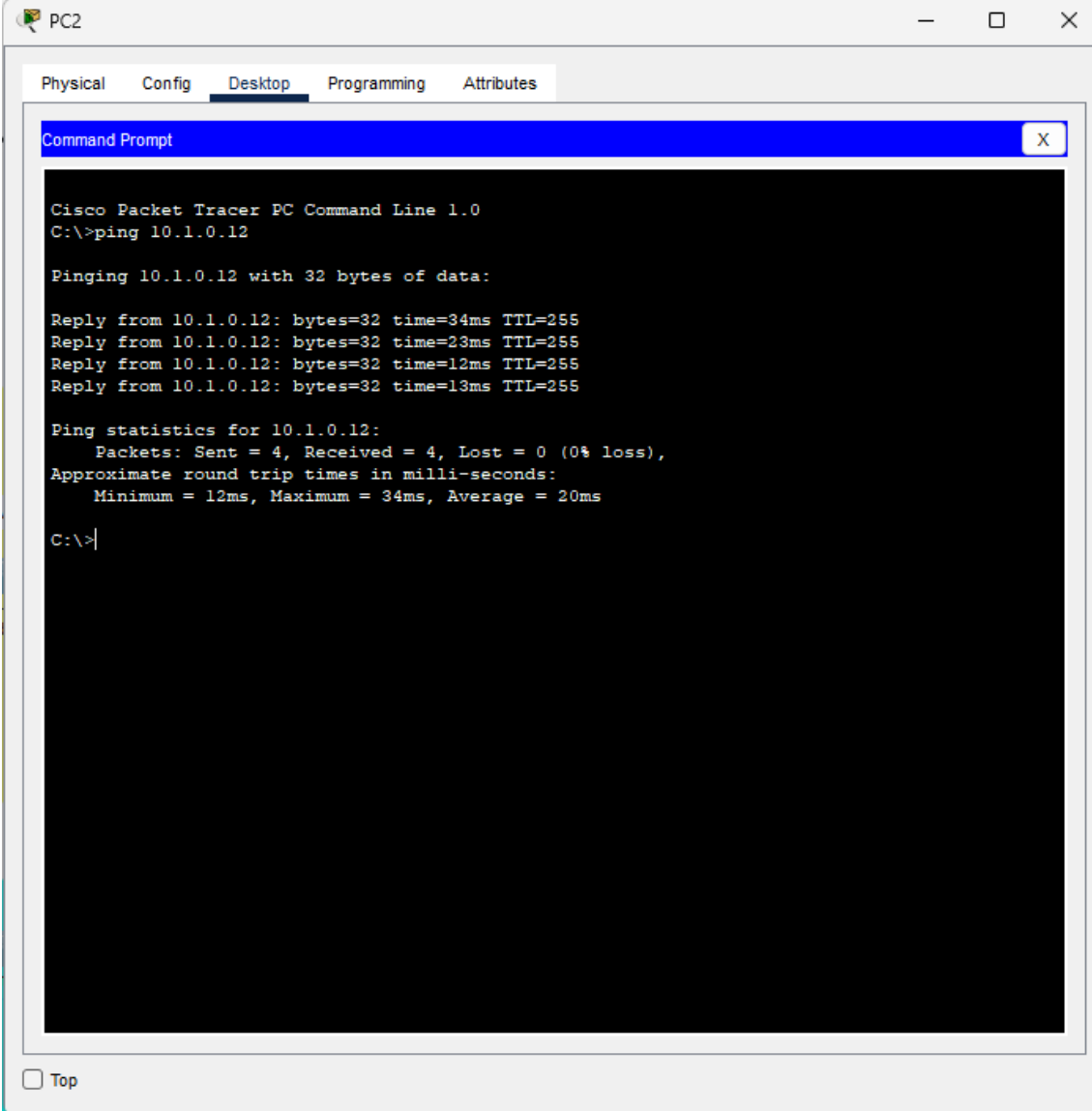
En este caso no puedo calcular el enrutamiento de Dijkstra por el simple hecho de que cada switch maneja vlans diferentes haciendo que no se pueda hacer un ping entre ellas.

No hemos configurado el VPN, pero el firewall 2 que se encuentra entre la dmz y la red interna, tiene un security-level 50 para lo que entra desde la red interna a la dmz y un security-level 100 para lo que entra desde la dmz a la red interna impidiendo su conexión al principio quería poner 100 solo a los segmentos de servidores y IoT pero no supe hacerlo y se lo coloque a todos, el firewall 1 situado entre el router y la dmz, tiene un security-level 0 para lo que sale hacia el router y un 50 para lo que entra desde el router a la dmz.

Tampoco hemos puesto ACLs por el momento, aunque el firewall mirara cada bits de información que pase por la red.

## 7.3 Pruebas de funcionamiento

Ping entre el pc que administra los IoT y el detector de monitoreo:



The screenshot shows a Cisco Packet Tracer PC Command Line window for a device named PC2. The window has tabs for Physical, Config, Desktop, Programming, and Attributes, with Desktop selected. The Command Prompt shows the execution of the command 'ping 10.1.0.12'. The output indicates that the ping was successful, with 4 packets sent and received, 0% loss, and round trip times ranging from 12ms to 34ms. The window also includes a 'Top' button at the bottom left.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.1.0.12

Pinging 10.1.0.12 with 32 bytes of data:

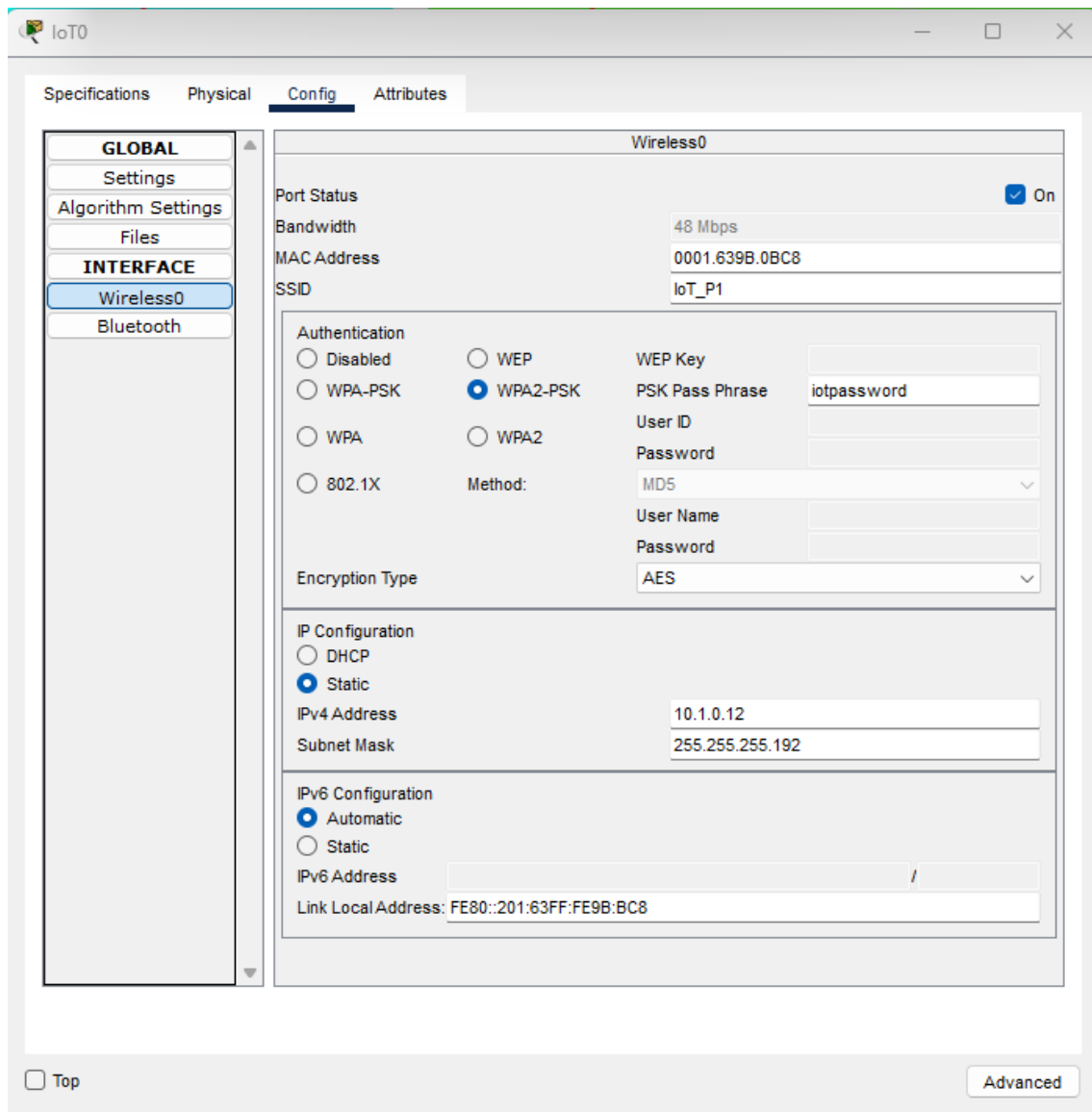
Reply from 10.1.0.12: bytes=32 time=34ms TTL=255
Reply from 10.1.0.12: bytes=32 time=23ms TTL=255
Reply from 10.1.0.12: bytes=32 time=12ms TTL=255
Reply from 10.1.0.12: bytes=32 time=13ms TTL=255

Ping statistics for 10.1.0.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 34ms, Average = 20ms

C:\>|
```

☐ Top

Dejo aquí la muestra de cuál es el ping del sensor de monitoreo:

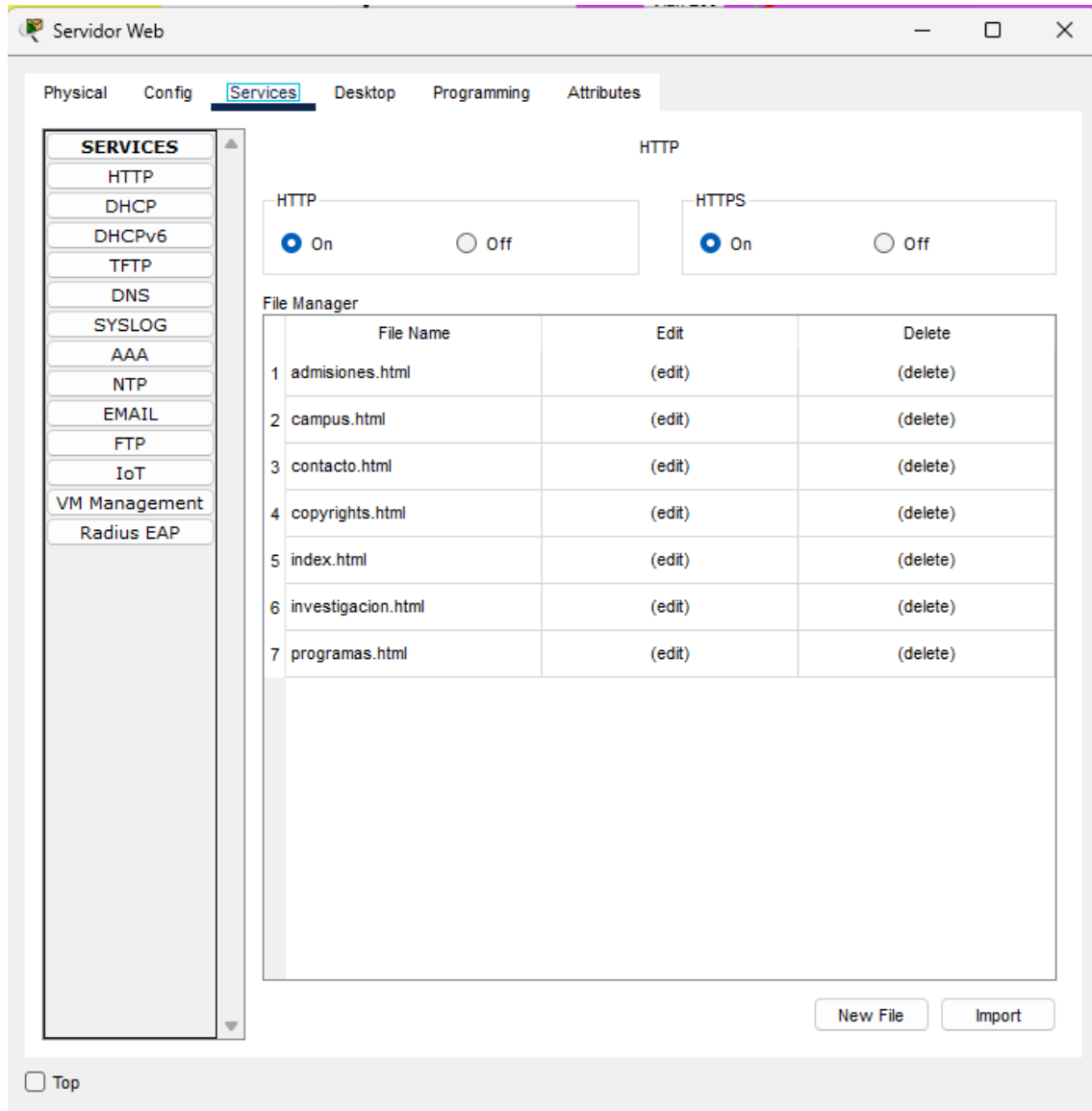


En esta imagen, también vera que los Access Point están todos configurados de la misma manera, todos tienen como contraseña el <nombre del segmento>password y como SSID <nombre del segmento>AC menos el de IoT que se llama IoT\_P1-



## Servidor

## Web:



En este servidor solo tenemos activado el HTTP y HTTPS con sus file creados emulando una web completa de una universidad, también hacemos una “falsa simulación” con el Proxi y el DNS. Supuestamente lo que haría el DNS sería enviar al servidor proxi y luego al servidor web para protegerlo.