ICCD353– FUNDAMENTOS DE REDES Y CONECTIVIDAD

FACULTAD DE INGENIERÍA DE SISTEMAS

Interworking del Hotel Temático de Disney

DOCENTE: Dra. Diana Yacchirema

Grupo: #10

Nombres: Elías Cazar

Roberth Gancino

Danny Iñaguazo

Fecha de entrega: 7/3/2024

Índice de Contenido

Introducción 3
Objetivos 4
1. Fundamentación teórica 5
2. Descripción de la Práctica 7
2.1 Configuración de la red 8
2.1.1 VLSM 8
2.1.2 Conexiones WAN 9
2.1.3 Switch principal y las Inter-VLANs 9
2.1.4 Routers Inalámbricos 11
2.1.5 Dispositivos IoT 12
2.1.6 Servidor Iot y Web 13
2.1.7 Conexión remota en el router de borde y switch principal del Hotel Temático de Disney. 15
3. Conclusiones 16
4. Recomendaciones 17
5. Bibliografía 18

Índice de Figuras

Figura 1. Topología- Hotel Temático de Disney 7
Figura 2. Conexiones WAN 9
Figura 3. Switch principal e Inter – VLANS 10
Figura 4. Subinterfaces 10
Figura 5. Routers inalámbricos 11
Figura 6. Configuración del router inalámbrico 11
Figura 7. Dispositivos IoT 12
Figura 8. Servidores web y IoT 13
Figura 9. Servidor IoT – IoT Monitor 13
Figura 10. Configuración – Servidor web 14
Figura 11. Página web – Menú del restaurante 14
Figura 12. Acceso remoto mediante ssh en el switch 15
Figura 13. Acceso remoto mediante ssh en el router de borde 15

Introducción

Este proyecto abarcó una amplia gama de conceptos y tecnologías de redes, con el objetivo de diseñar una infraestructura de red sólida y confiable que pueda satisfacer las necesidades de conectividad de un entorno hotelero de alto nivel.

La topología de red diseñada tuvo en cuenta aspectos clave como la gestión de direcciones IPv4, la segmentación de redes mediante el uso de VLSM (Variable Length Subnet Masking), la integración de dispositivos IoT (Internet of Things) para proporcionar servicios y comodidades avanzadas a los huéspedes, y la implementación de medidas de seguridad para proteger la administración de red contra posibles amenazas.

Se destacó también la importancia de métodos de control de acceso al medio para optimizar el rendimiento de la red y minimizar los problemas de congestión.

Un aspecto importante de este trabajo fue la implementación de protocolos de acceso remoto seguros, como SSH (Secure Shell), para administrar de manera eficiente los dispositivos de red desde ubicaciones remotas. Estas medidas de seguridad jugaron un papel significativo en la protección de la integridad y confidencialidad de los datos transmitidos a través de la red.

Objetivos

- Diseñar una topología de red que aborde los fundamentos de gestión de redes considerando las características de una red confiable que garantice la tolerancia a fallos, seguridad y la calidad de servicio (QoS).
- Implementar una estructura de subredes flexible que pueda adaptarse al crecimiento del hotel, permitiendo así la incorporación de nuevos dispositivos y servicios sin necesidad de rediseñar la arquitectura de red completa.
- Modelar una configuración escalable para dispositivos IoT, estableciendo conexiones inalámbricas flexibles en las instalaciones del hotel, y proveer servicios web y de IoT desde servidores remotos.
- Implementar el protocolo SSH para el acceso remoto seguro en los dispositivos, tanto de capa 2 (switches), como de capa 3 (routers).
- Establecer VLANs en la red con el objetivo de aislar el tráfico administrativo en los switches y el aumento del rendimiento de la red, reduciendo el número de dominios de broadcast.

1. Fundamentación teórica

Redes

Las redes constituyen interconexiones que pueden ser físicas o inalámbricas, enlazando diversos dispositivos informáticos como computadoras, celulares y servidores. Su propósito fundamental es facilitar la comunicación entre estos dispositivos, permitiendo el intercambio de datos y la prestación de diversos servicios de telecomunicaciones [1].

Al configurar una red, se define su topología, que se refiere a la disposición gráfica de los dispositivos dentro de la red. Esto abarca tanto la estructura física, que incluye los propios dispositivos, como la lógica, que implica las direcciones de red y direcciones IP. El objetivo es proporcionar un diseño de red optimizado, reduciendo redundancias en las conexiones y planificando la escalabilidad de la red.

En este proyecto de redes, se utilizaron dos tipos principales: las redes LAN (Local Area Network), que conectan dispositivos en áreas geográficas pequeñas, como hogares, edificios o habitaciones; y las redes WAN (Wide Area Network), que interconectan redes LAN ubicadas en diferentes ubicaciones físicas, permitiendo la comunicación a larga distancia.

VLSM

VLSM (Máscara de Subred de Longitud Variable) es una técnica de subneteo diseñada para crear subredes con diversas máscaras de red. Su principal objetivo es proporcionar flexibilidad en la asignación de hosts en cada red, permitiendo la creación de subredes de tamaños variados [2]. Esta estrategia previene el desperdicio de direcciones de host en redes que no requieren un gran número de hosts, como las conexiones de capa 3 (routers).

VLANs

Las VLANs (Virtual Local Area Networks) son una técnica que posibilita la subdivisión de una red física en redes lógicas [3]. Esta estrategia se implementa dentro de un switch, lo que permite segmentar la red mediante la asignación de puertos a los dispositivos. Este enfoque posibilita la segmentación de la red sin que los dispositivos cambien su ubicación física.

Adicionalmente, las VLANs posibilitan el aislamiento de dispositivos pertenecientes a subredes físicas distintas pero conectadas al mismo switch. Este proceso es análogo a dividir una red física, ya que separa los dispositivos conectados al switch a través de los puertos correspondientes. Este nivel de aislamiento facilita la administración de diversas redes dentro de una empresa mediante las VLAN creadas en el switch.

Enrutamiento estático y enrutamiento estático por defecto

Los routers desempeñan un papel crucial al dirigir paquetes de una red a otra, facilitando la comunicación entre dispositivos pertenecientes a distintas redes. Para lograr esto, los routers emplean técnicas especializadas que les permiten determinar la red de destino a la cual deben enviar un paquete.

El enrutamiento estático implica asignar manualmente al router una ruta fija, especificando la red de destino y la interfaz por la cual enviar el paquete. Esta técnica resulta eficaz en topologías de red simples, donde las rutas de paquetes son predecibles. En contraste, el enrutamiento estático por defecto permite dirigir paquetes sin la necesidad de especificar la red de destino, simplemente indicando la interfaz de salida. Esta práctica resulta particularmente beneficiosa al configurar routers de tipo "stub" o de borde, conectados a un único router vecino, generalmente de un proveedor de servicios de Internet (ISP). Esto simplifica la configuración de enrutamiento, delegando al router vecino la responsabilidad de gestionar el enrutamiento de las redes hacia Internet [4].

Router on stick

La configuración de un router "on stick" posibilita dirigir tráfico entre diferentes VLAN configuradas en un switch mediante una única conexión física. Este proceso implica la configuración de la interfaz física conectada a las VLANs mediante subinterfaces lógicas. Cada subinterfaz representa una VLAN, simulando una interfaz física única para cada red. Esta estrategia optimiza el enrutamiento hacia las VLANs, ofreciendo una solución eficiente al utilizar una sola conexión física con costos reducidos [5].

Conexiones Wireless

Las redes inalámbricas posibilitan la conexión de dispositivos a la red sin la necesidad de cables físicos, gracias a la tecnología IEEE 802.11 (WIFI) [6], que permite a los dispositivos conectarse a través de ondas de radio. Los routers inalámbricos, habilitados para conexiones wireless, operan estableciendo una red LAN privada y asignando direcciones IP específicas a los dispositivos. Además, para posibilitar que un dispositivo de la red creada por el router inalámbrico se conecte a la red principal asignada, este router ofrece la capacidad de traducción de direcciones IP hacia la red principal. Para lograrlo, es necesario asignar una dirección IP de la red principal al router. Esto permite que el router se encargue de la traducción de direcciones IP, facilitando la salida de paquetes desde los dispositivos inalámbricos hacia la red principal.

Servidores web y IoT

Los servidores desempeñan un papel crucial al facilitar el acceso a servicios para dispositivos tanto dentro como fuera de la red [7]. Estos servicios pueden abarcar desde protocolos HTTP/HTTPS para aplicaciones web hasta funciones específicas para el Internet de las cosas (IoT). Un servidor posibilita el hospedaje de páginas web, las cuales son accesibles desde cualquier ubicación mediante un navegador web conectado a la red o a Internet.

En el ámbito del IoT, el servidor actúa como un centro de mando centralizado que proporciona el control y la gestión de dispositivos IoT. Esto permite la configuración y el monitoreo de los dispositivos para que operen de diversas maneras. Además, el servidor ofrece servicios de cuentas de usuario, lo que facilita la administración remota de los dispositivos IoT de una organizacion desde cualquier dispositivo conectado a la red.

2. DESCRIPCIÓN DE LA PRÁCTICA

Con el fin de la creación y configuración de la red propuesta para el proyecto correspondiente, se siguió la siguiente topología de manera que cumpla los requisitos de un hotel de lujo con un gran flujo de huéspedes y distintas zonas como parqueadero, dormitorios, restaurante, salón de videojuegos y piscina.

Figura 1. Topología- Hotel Temático de Disney

En la Figura 1 se observan dos zonas adicionales: Centro de datos y salón de conferencias. Adicionalmente, se visualiza también parte de un segundo hotel ubicado en el parque temático Disney World en Orlando geográficamente distante del principal. Este se conforma por 3 habitaciones similares a las que se encuentran en el primer hotel.

Estos hoteles están conectados entre sí, además, se conectan a internet mediante enlaces redundantes hacia el router del ISP.

2.1 Configuración de la red

2.1.1 VLSM

Para la creación de la red se utilizó la siguiente dirección de red 139.0.0.0 /16. En adición, en la topología presente en la Figura 1 se tienen varias redes con diferente número de host, por lo que se utilizó VLSM.

Tabla 1. VLSM.

Redes	# Host	M	NT	N	MK prefijo	MK decimal	# Mágico
Hotel 2	2000	11	5	5	/21	255.255.248.0	8
Parqueadero Hotel 1	400	9	7	7	/23	255.255.254.0	2
Habitaciones Hotel 1	400	9	7	7	/23	255.255.254.0	2
Piscina Hotel 1	400	9	7	7	/23	255.255.254.0	2
Salón de Conferencias Hotel 1	400	9	7	7	/23	255.255.254.0	2
Restaurante Hotel 1	400	9	7	7	/23	255.255.254.0	2
Sala de videojuegos Hotel 1	400	9	7	7	/23	255.255.254.0	2
Centro de Datos Hotel 1	60	6	10	2	/26	255.255.255.192	64
WAN 1	2	2	14	6	/30	255.255.255.252	4
WAN 2	2	2	14	6	/30	255.255.255.252	4
WAN 3	2	2	14	6	/30	255.255.255.252	4
Administración	2	2	14	6	/30	255.255.255.252	4

Dirección de Red	1era Dir. Valida	Ultima Dir. Valida	Dirección de Broadcast
139.0.0.0	139.0.0.1	139.0.7.254	139.0.7.255
139.0.8.0	139.0.8.1	139.0.9.254	139.0.9.255
139.0.10.0	139.0.10.1	139.0.11.254	139.0.11.255
139.0.12.0	139.0.12.1	139.0.13.254	139.0.13.255
139.0.14.0	139.0.14.1	139.0.15.254	139.0.15.255
139.0.16.0	139.0.16.1	139.0.17.254	139.0.17.255
139.0.18.0	139.0.18.1	139.0.19.254	139.0.19.255
139.0.20.0	139.0.20.1	139.0.20.62	139.0.20.63
139.0.20.64	139.0.20.65	139.0.20.66	139.0.20.67
139.0.20.68	139.0.20.69	139.0.20.70	139.0.20.71

139.0.20.72	139.0.20.73	139.0.20.74	139.0.20.75
139.0.20.76	139.0.20.77	139.0.20.78	139.0.20.79

La Tabla 1 presenta los datos obtenidos mediante VLSM para las distintas subredes que se asignarón a las conexiones WAN, VLANs, entre otros.

2.1.2 Conexiones WAN

Se utilizó 3 routers con distintas finalidades como: router del ISP y 2 routers para cada hotel.

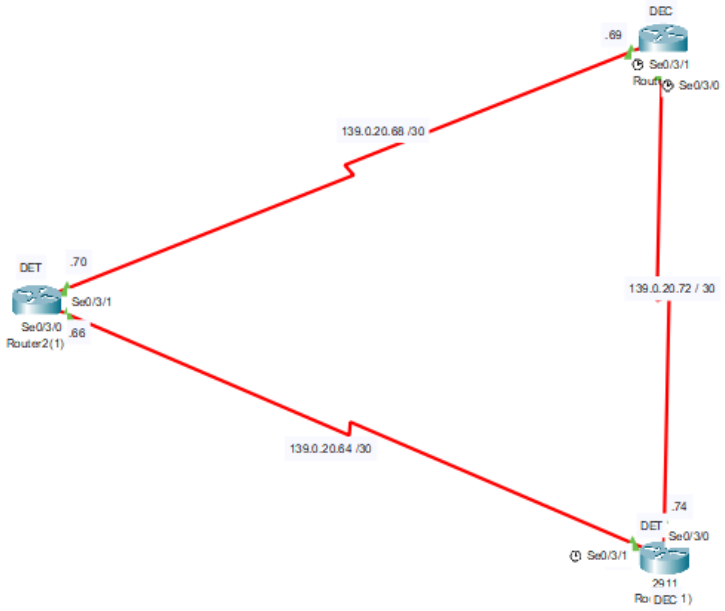

Figura 2. Conexiones WAN

En la Figura 2 se tiene el router dedicado al ISP trabaja como un dispositivo DCE en ambas interfaces seriales utilizadas, debido a sus altas prestaciones, mientras que, en la conexión entre los routers de los hoteles, uno de los routers trabaja como DCE y el otro como DTE. Dicha configuración fue realizada debido a que las redes de los hoteles son parecidas y no existe un router con una mayor capacidad o prestaciones significativas para designar alguno en específico como DCE. Este paso es importante para el enrutamiento de paquetes hacia otras subredes.

2.1.3 Switch principal y las Inter-VLANs

En la división de VLANs y distribución de dispositivos intermedios y finales dentro del hotel se necesita de un nodo principal siendo este un switch.


```
10   parqueadero                    active    Fa0/1
20   piscina                        active    Fa0/2
30   dormitorio                     active    Fa0/3
40   datacenter                     active    Fa0/4
50   videojuegos                    active    Fa0/5
60   conferencia                    active    Fa0/6
70   restaurante                    active    Fa0/7
100  manage                         active    Fa0/24
```

Figura 3. Switch principal e Inter – VLANS

El router del hotel principal se conecta al switch principal como se muestra en la Figura 3, para que controle eficazmente el tráfico de paquetes de VLANs entre las distintas interfaces. Entonces creamos 7 VLANs para cada zona existente, la 8va se destina al manejo remoto del switch (Manager), se pueden visualizar en la Figura 3.

```
!
interface GigabitEthernet0/0.1
 encapsulation dot1Q 10
 ip address 139.0.10.1 255.255.254.0
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 20
 ip address 139.0.8.1 255.255.254.0
!
interface GigabitEthernet0/0.3
 encapsulation dot1Q 30
 ip address 139.0.14.1 255.255.254.0
!
interface GigabitEthernet0/0.4
 encapsulation dot1Q 40
 ip address 139.0.20.1 255.255.255.192
!
interface GigabitEthernet0/0.5
 encapsulation dot1Q 50
 ip address 139.0.18.1 255.255.254.0
!
interface GigabitEthernet0/0.6
 encapsulation dot1Q 60
 ip address 139.0.16.1 255.255.254.0
!
interface GigabitEthernet0/0.7
 encapsulation dot1Q 70
 ip address 139.0.12.1 255.255.254.0
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 100
 ip address 139.0.20.77 255.255.255.252
!
```

Figura 4. Subinterfaces

En la Figura 4 se puede notar que en el router se realizó la creación de subinterfaces a partir de la Gigabit Ethernet 0/0 con el objetivo de permitir la comunicación entre

VLANs. En cada subinterfaz se encapsula respecto al ID de la VLAN correspondiente para luego asignar una dirección IP y máscara de red.

2.1.4 Routers Inalámbricos

Los routers inalámbricos son una parte fundamental para configurar y gestionar una red privada debido a la distribución de redes IP hacia los dispositivos finales. Estos dispositivos forman la red privada local.

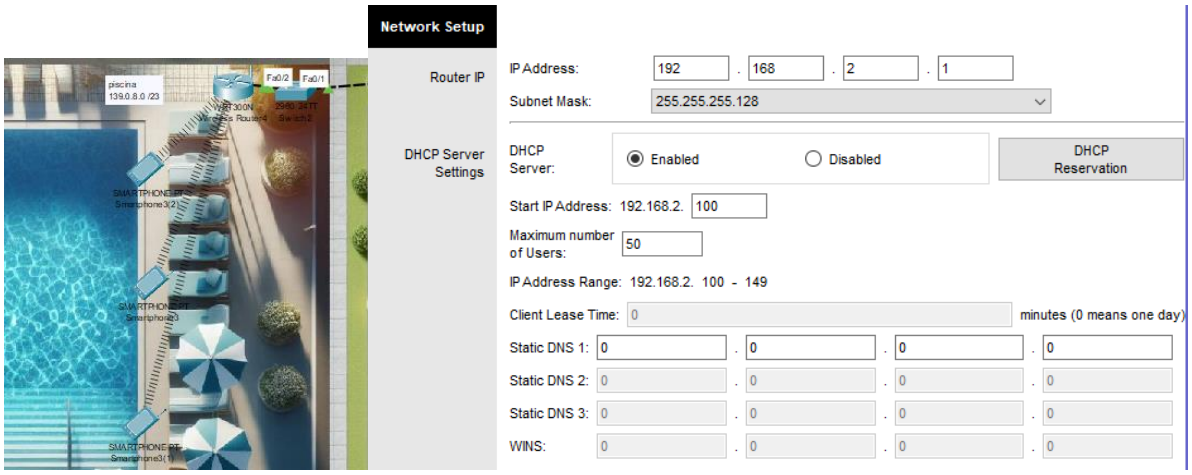

Figura 5. Routers inalámbricos

Como siguiente punto, en algunas VLANs se presenta este dispositivo junto con un switch. Para configurarlo, se asigna una dirección IP de la red en la que se encuentra, su máscara y un gateway, permitiendo así el enrutamiento de paquetes.

EL protocolo DCHP se encarga de asignar direcciones IP privadas a los dispositivos que se conecten al router, posteriormente en la Figura 5 se muestra un ejemplo con un numero de 50 usuarios a asignar.

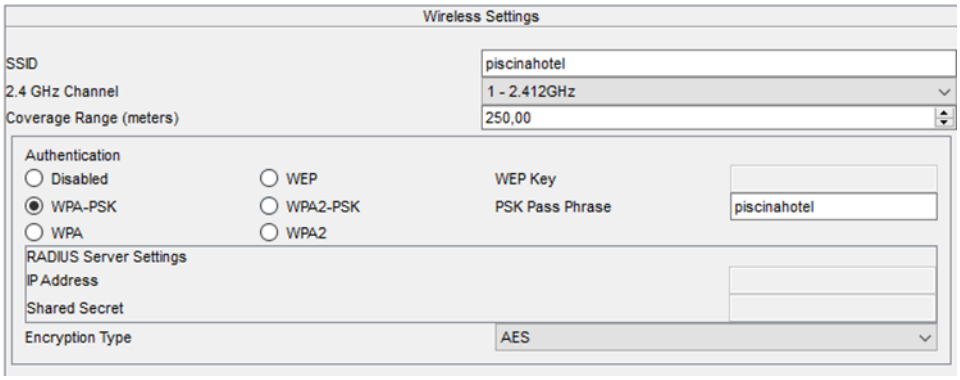

Figura 6. Configuración del router inalámbrico

En el mismo dispositivo se debe configurar el método de acceso a la red privada, en la Figura 6 se asignó como SSID (Nombre de la red inalámbrica) “piscinahotel” y la contraseña “piscinahotel”. Con las credenciales mencionadas, un dispositivo inalámbrico puede conectarse sin problemas.

2.1.5 Dispositivos IoT

Las habitaciones presentes en ambos hoteles poseen dispositivos IoT como: Lámparas, puertas y sensores. Dichos dispositivos se encuentran conectados a un router inalámbrico mediante el protocolo DHCP, el cual a su vez se conecta a un servidor iot que contiene las condiciones e instrucciones para las interacciones entre los dispositivos iot.

Figura 7. Dispositivos IoT

En la Figura 7 se puede visualizar que en cada habitación existe un sensor, una puerta y una lámpara. El funcionamiento que poseen dichos dispositivos corresponde al siguiente: Cuando el sensor es activado, la puerta pasa de estar bloqueada a desbloqueada y cuando la puerta es abierta, la lámpara se enciende. Por otra parte, cuando el sensor no es activado, la puerta se bloquea y además la lámpara se apaga debido a dicho estado de la puerta.

2.1.6 Servidor Iot y Web

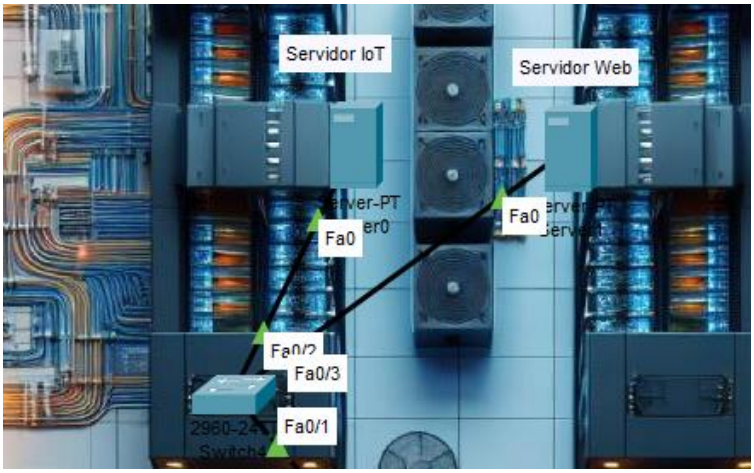

Figura 8. Servidores web y IoT

En la Figura 8 se puede apreciar la red perteneciente a la VLAN “Datacenter”, la cual contiene los dos servidores importantes que ofrecerán servicios a los huéspedes. El servidor IoT tiene como objetivo controlar, procesar y monitorear los datos que un dispositivo IoT envía.

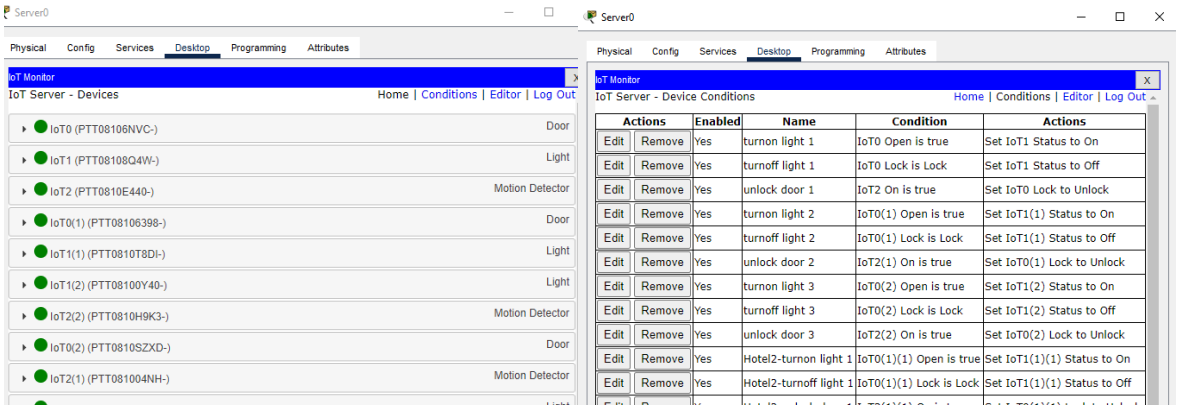

Figura 9. Servidor IoT – IoT Monitor

La figura 9 contienen información del servidor que muestra los dispositivos IoT conectados, y las acciones que tienen configurados con alguna condición. Se implementaron acciones que familiarizan al huésped y se hablaron el en apartado 2.1.5. Dichas condiciones incluyen también los dispositivos ubicados en el Hotel Disney Orlando.

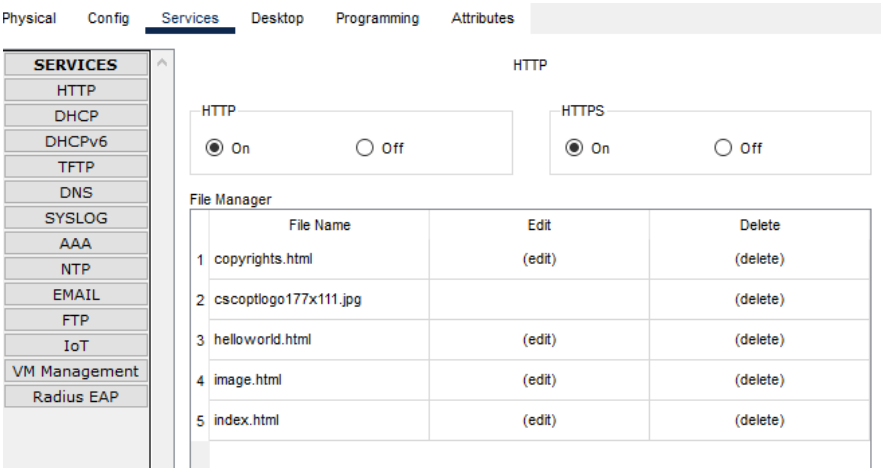

Figura 10. Configuración – Servidor web

En la Figura 10 se puede apreciar que en el servidor web se levantaron los servicios HTTPS para que los dispositivos finales puedan acceder al menú del restaurante, específicamente el archivo “index.html”.

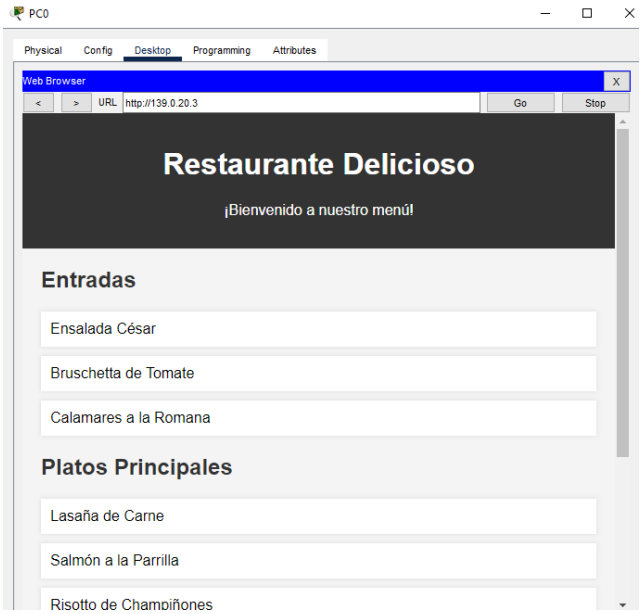

Figura 11. Página web – Menú del restaurante

Cuando un dispositivo final solicita la información del servidor en el browser, será respondido en la manera de la Figura 11.

2.1.7 Conexión remota en el router de borde y switch principal del Hotel Temático de Disney.

El acceso remoto hacia el router y el switch fue realizado mediante ssh, ya que este método proporciona una alta seguridad debido a la autenticación y comunicación cifrada que posee.

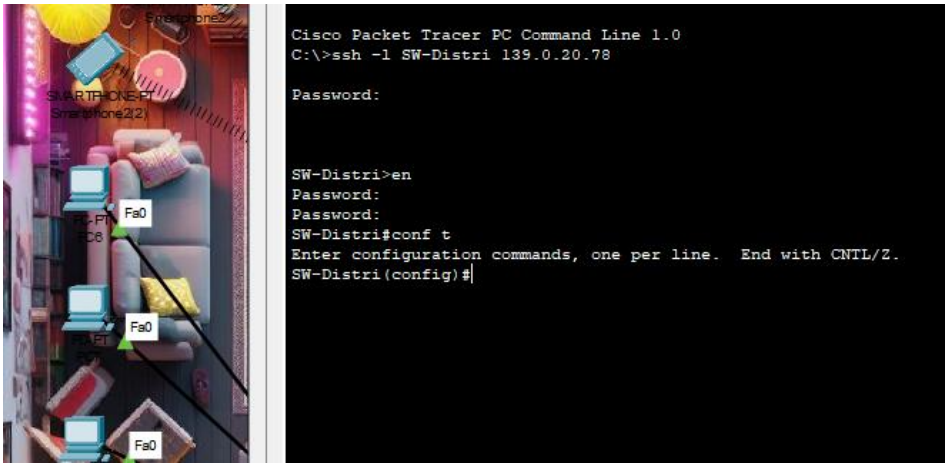

Figura 12. Acceso remoto mediante ssh en el switch

En la Figura 12 se puede visualizar el acceso remoto hacia el switch desde la PC6 mediante ssh, donde la contraseña es “grupo10”. Además, la contraseña para acceder al modo EXEC Privilegiado es “fis”.

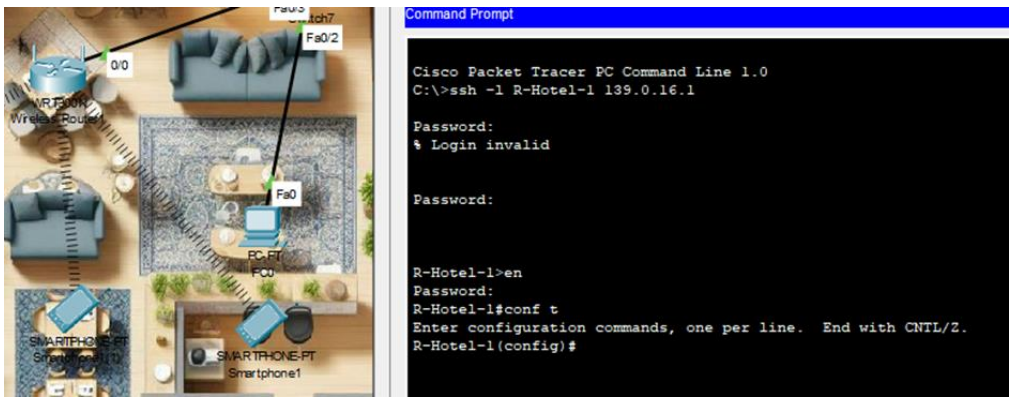

Figura 13. Acceso remoto mediante ssh en el router de borde

En la Figura 13 se puede visualizar el acceso remoto hacia el router desde la PC0 mediante ssh, donde la contraseña es “grupo10”. Además, la contraseña para acceder al modo EXEC Privilegiado es “fis”.

3. Conclusiones

- La planificación de la topología de red resultó en un entorno altamente escalable y seguro para la gestión de la red del hotel. Al priorizar la estabilidad y la calidad del servicio, hemos garantizado que la infraestructura de red pueda soportar el crecimiento constante y mantener un rendimiento constante en todo momento.
- La configuración escalable para dispositivos IoT permite una gran experiencia en el huésped dentro de las instalaciones. Al establecer conexiones inalámbricas y proporcionar servicios web y de IoT, se creó un atractivo ecosistema tecnológico que facilita las tareas domésticas del huésped.
- La implementación del protocolo SSH para el acceso remoto aseguró un nivel de seguridad para la administración de nuestra red. Al proporcionar un método de acceso cifrado y autenticado, se garantiza que solo el personal autorizado pueda acceder a los dispositivos de red. Esta capa adicional de seguridad es esencial para proteger la integridad de los datos sensibles del hotel.
- Al segmentar el tráfico y aislar las áreas administrativas y recreativas, hemos reducido la congestión, mejorando así, el rendimiento de la red. Esta optimización no solo mejora la experiencia del usuario, sino que también reduce la carga en nuestros dispositivos de red, por lo que como resultado minimiza el riesgo de fallos y maximiza la confiabilidad.
- Se han establecido conexiones redundantes utilizando rutas estáticas flotantes en los routers, lo que asegura la disponibilidad continua de la red incluso en caso de fallo de enlaces principales y la Integridad de los paquetes a enviar.

4. Recomendaciones

- Al configurar VLANs en la red, es importante tener en cuenta las configuraciones de trunking y etiquetado VLAN para evitar problemas de aislamiento o interferencia de tráfico entre diferentes VLANs. Además, se debe prestar especial atención a la asignación de puertos a las VLANs para garantizar que los dispositivos estén correctamente segmentados según sus funciones.
- Se recomienda encarecidamente priorizar el uso del protocolo SSH sobre Telnet para el acceso remoto a los dispositivos de red en Cisco Packet Tracert, debido a las preocupaciones de seguridad asociadas con Telnet. SSH proporciona un acceso remoto seguro mediante la autenticación y el cifrado, lo que protege los datos sensibles transmitidos durante las sesiones de administración. En contraste, Telnet transmite información de inicio de sesión y otros datos en texto plano.
- Evitar superposiciones de direcciones IP y diseñar subredes con suficiente espacio para la expansión futura ayudará a evitar problemas de direccionamiento y congestión de red.
- Los dispositivos DCE, en cuestión de routers, controlan la velocidad de transmisión de datos en la conexión WAN, mientras que los dispositivos DTE, son responsables de enviar y recibir datos a través de la conexión. Se recomienda asegurarse de que los dispositivos DCE y DTE estén correctamente configurados y conectados considerando la configuración de parámetros como la velocidad de transmisión, el tipo de encapsulación y los protocolos.

5. Bibliografía

[1] Cisco. "SMB Redes", s/f. [Online] Disponible en: https://www.cisco.com/c/dam/global/es_mx/solutions/small-business/pdfs/smb-redes-mx.pdf
[2] GeeksforGeeks. (Año). Implementation of VLSM in Cisco. GeeksforGeeks. [Online] Disponible en: https://www.geeksforgeeks.org/implementation-of-vlsm-in-cisco/
[3] Cisco, "Configuring Service-Specific Parameters for Location Tracking VLANS," Cisco Systems, [Online]. Disponible en: https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/alolh/sp/svc_5.html
[4] Cisco, "Static Routing Configuration Guide for Cisco RV160 and RV260 Series Routers," Cisco Support, [Online]. Disponible en: https://www.cisco.com/c/es_mx/support/docs/smb/routers/cisco-rv-series-small-business-routers/kmgmt-2334-Static-Routing-RV160-RV260.html
[5] OpenAI, "Router on Stick", OpenAI Chat, [Online]. Disponible en: https://chat.openai.com/c/ff53bfba-1f81-409d-bb6e-219bb509cdef
[6] Cisco, "Wireless Networking Solutions for Small Business," Cisco Small Business Resource Center, [Online]. Disponible en: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/wireless-network.html
[7] Zoostock, "Servidores de almacenamiento de Cisco Web - IoT," Zoostock, [Online]. Disponible en: https://www.zoostock.com/cisco-system/conoce-los-servidores-de-almacenamiento-de-ciscog