

Diplomado de profundización en redes de nueva generación

fase 11

Juan Alberto Ortega Rojas

Asesor

Omar Albeiro Trejo

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Tecnología en Sistemas de Comunicación Inalámbrica

2022

Resumen

El siguiente trabajo tiene como fin ilustrar sobre la identificación, el reconocimiento y la configuración de los modelos y arquitecturas de redes NGN (Next Generation Network). Se pretende dar a conocer las capas, protocolos, funciones y ventajas de una arquitectura NGN utilizada en la interconexión de redes, mediante la comparación con las redes tradicionales y el uso de protocolos involucrados. También, busca Identificar los protocolos de IoT (Internet Of Things), mediante la investigación de los conceptos vigentes que responden a los estándares actuales.

Palabras clave: Red, Internet, modelo, arquitectura, Capa.

Abstract

The purpose of the following work is to illustrate the identification, recognition and configuration of NGN (Next Generation Network) network models and architectures. It is intended to make known the layers, protocols, functions and advantages of an NGN architecture used in the interconnection of networks, through comparison with traditional networks and the use of protocols involved. Also, it seeks to identify the IoT (Internet Of Things) protocols, through the investigation of current concepts that respond to current standards.

Keywords: Network, Internet, model, architecture, Layer.

Tabla de Contenido

Introducción	8
Justificación	9
Objetivos	10
Objetivo General	10
Objetivos Específicos.....	10
Diplomado de Profundización en Redes de Nueva Generación	11
Fase 11	11
Selección de Dos Mecanismos de QoS y Descripción del Proceso que Realiza Cada Uno Mediante un Diagrama de Bloques.	11
Documentación de los Pasos Requeridos para Definir un Plan de QoS	12
Planificación de Configuración IPQoS General	12
Planificación de la Distribución de la Red Diffserv	12
Estrategias de Hardware para la Red Diffserv	12
Distribuciones de Red IPQoS	13
Planificación de la Directiva de Calidad de Servicio.....	14
Lista de Comprobación de la Implementación de QoS.....	15
Consideraciones al Respecto de la Red Privada Virtual	16
IPTV Multicast.....	18
Clasificación y Marketing	19
Marcar los paquetes con el valor de IP Precedence	19
Configuración red MPLS	20
Configuración para habilitar CEF.....	20
Configuración para habilitar MPLS.....	22
Configuramos Multicast.....	24
Configuramos router con las redes globales	24
Simulación transmisor a receptor.....	31
Conclusiones	32
Recomendaciones	33
Referencias Bibliográficas	34

Lista de Tablas

Tabla 1 Direccionamiento IP en IPTV multicast	18
--	----

Lista de Figuras

Figura 1 <i>Diagrama de bloques sobre mecanismos QoS</i>	11
Figura 2 <i>Herramientas de gestión de la congestión</i>	12
Figura 3 <i>Distribuciones de red IPQoS</i>	13
Figura 4 <i>Topología IPTV multicast</i>	18
Figura 5 <i>Configuración para habilitar CEF paso 1</i>	20
Figura 6 <i>Configuración para habilitar CEF paso 2</i>	20
Figura 7 <i>Configuración para habilitar CEF paso 3</i>	21
Figura 8 <i>Configuración para habilitar CEF paso 4</i>	21
Figura 9 <i>Configuración para habilitar CEF paso 5</i>	21
Figura 10 <i>Configuración para habilitar CEF paso 6</i>	21
Figura 11 <i>Configuración para habilitar MPLS paso 1</i>	22
Figura 12 <i>Configuración para habilitar MPLS paso 2</i>	22
Figura 13 <i>Configuración para habilitar MPLS paso 3</i>	22
Figura 14 <i>Configuración para habilitar MPLS paso 4</i>	22
Figura 15 <i>Configuración para habilitar MPLS paso 5</i>	23
Figura 16 <i>Configuración para habilitar MPLS paso 6</i>	23
Figura 17 <i>Configuración para habilitar MPLS paso 7</i>	23
Figura 18 <i>Configuración para multicast paso 1</i>	24
Figura 19 <i>Configuración para multicast paso 2</i>	24
Figura 20 <i>Configuración para multicast paso 3</i>	24
Figura 21 <i>Configuración router con las redes globales paso 1</i>	24
Figura 22 <i>Configuración router con las redes globales paso 2</i>	25

Figura 23 <i>Configuración router con las redes globales paso 3</i>	25
Figura 24 <i>Configuración router con las redes globales paso 4</i>	25
Figura 25 <i>Configuración router con las redes globales paso 5</i>	25
Figura 26 <i>Configuración Router y DHCP paso 1</i>	26
Figura 27 <i>Configuración Router y DHCP paso 2</i>	26
Figura 28 <i>Configuración Router y DHCP paso 3</i>	26
Figura 29 <i>Configuración grupos de multicast paso 1</i>	26
Figura 30 <i>Configuración grupos de multicast paso 2</i>	27
Figura 31 <i>Configuración grupos de multicast paso 3</i>	27
Figura 32 <i>Configuración de enrutamiento paso 1</i>	28
Figura 33 <i>Configuración de enrutamiento paso 2</i>	28
Figura 34 <i>Configuración de enrutamiento paso 3</i>	29
Figura 35 <i>Configuración de enrutamiento paso 4</i>	29
Figura 36 <i>Configuración de enrutamiento paso 5</i>	30
Figura 37 <i>Configuración de comunicación paso 1</i>	30
Figura 38 <i>Configuración de comunicación paso 2</i>	30
Figura 39 <i>Configuración de comunicación paso 3</i>	30
Figura 40 <i>Configuración de comunicación paso 4</i>	30
Figura 41 <i>Configuración de comunicación paso 5</i>	31
Figura 42 <i>Simulación transmisor a receptor</i>	31

Introducción

En el presente documento se evidenciará el desarrollo de las actividades propuestas en la fase 11 del diplomado de profundización en redes de nueva generación, dicha actividad está compuesta por 3 puntos, los cuales se basan en identificar las capas y funciones de un modelo de red, a través de la investigación de los conceptos vigentes, los cuales son la base dentro de una arquitectura de red.

También es importante tener en cuenta los protocolos de IoT (Internet Of Things), mediante la investigación de los conceptos vigentes que responden a los estándares actuales y como se configuran los servicios multimedia para un escenario de NGN a nivel de simulación, aplicando los conceptos de arquitectura funcional y definiendo políticas de Calidad de Servicio (QoS, Quality of Service).

Justificación

El presente trabajo se enfocará en el estudio de las capas, protocolos, funciones y ventajas de una arquitectura NGN utilizada en la interconexión de redes, mediante la comparación con las redes tradicionales y el uso de protocolos involucrados.

Este trabajo permitirá mostrar qué tipo de modificaciones se han desarrollado en las capas, protocolos, funciones y ventajas de una arquitectura NGN utilizada en la interconexión de redes. Además se identificarán los protocolos y funciones de la capa de red, mediante el uso de los principios de direccionamiento IP, enmarcados dentro de los estándares.

Objetivos

Objetivo General

Evidenciar el desarrollo de las actividades propuestas en la fase 11 del diplomado de profundización en redes de nueva generación, la cual se basa en identificar las capas y funciones de un modelo de red, a través de la investigación de los conceptos vigentes, los cuales son la base dentro de una arquitectura de red.

Objetivos Específicos

Identificar los protocolos y funciones de la capa de red, mediante el uso de los principios de direccionamiento IP, enmarcados dentro de los estándares.

Reconocer las capas, protocolos, funciones y ventajas de una arquitectura NGN utilizada en la interconexión de redes, mediante la comparación con las redes tradicionales y el uso de protocolos involucrados.

Configurar servicios multimedia para un escenario de NGN a nivel de simulación, aplicando los conceptos de arquitectura funcional y definiendo políticas de Calidad de Servicio (QoS, Quality of Service).

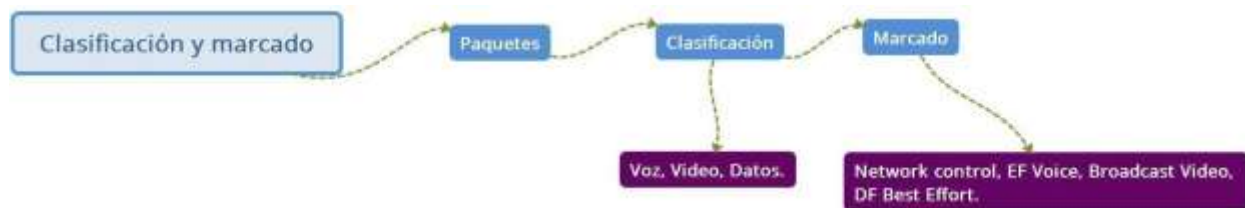
Diplomado de Profundización en Redes de Nueva Generación

Fase 11

Selección de Dos Mecanismos de QoS y Descripción del Proceso que Realiza Cada Uno Mediante un Diagrama de Bloques.

Clasificación y marcado. Estas herramientas diferencian entre aplicaciones y clasifican los paquetes en diferentes tipos de tráfico. El marcado indica que cada paquete es miembro de una clase de red, lo que permite que los dispositivos de la red reconozcan la clase del paquete. La clasificación y el marcado se implementan en dispositivos de red como enrutadores, conmutadores y puntos de acceso.

Figura 1 Diagrama de bloques sobre mecanismos QoS



Fuente. Autoría Propia.

Gestión de la congestión. Estas herramientas utilizan la clasificación y el marcado de paquetes para determinar en qué cola colocar los paquetes. Las herramientas de gestión de la congestión incluyen las colas de prioridad, las primeras en entrar, las primeras en salir y las de baja latencia.

Figura 2 *Herramientas de gestión de la congestión*



Fuente. Autoría Propia.

Documentación de los Pasos Requeridos para Definir un Plan de QoS

Planificación de Configuración IPQoS General

Utilizar servicios diferenciados, como IPQoS, en una red requiere una planificación exhaustiva. Debe considerarse no sólo la posición y función de cada sistema con IPQoS, sino también la relación de cada sistema con el enrutador de la red local. El mapa de tareas siguiente muestra las principales tareas de planificación para implementar IPQoS en la red, y contiene vínculos a procedimientos para realizar las tareas.

Planificación de la Distribución de la Red Diffserv

Para proporcionar servicios diferenciados en la red, necesita al menos un sistema con IPQoS y un enrutador con Diffserv. Puede expandir esta configuración básica de diferentes modos, como se explica en esta sección.

Estrategias de Hardware para la Red Diffserv

Normalmente, los clientes utilizan IPQoS en servidores y consolidaciones de servidores, como Sun Enterprise™ 0000. También puede utilizar IPQoS en sistemas de sobremesa, como UltraSPARC®, según las necesidades de la red. La siguiente lista contiene posibles sistemas para una configuración IPQoS:

Sistemas Oracle Solaris que ofrecen varios servicios, como servidores web o de base de datos Servidores de aplicaciones que ofrecen servicios de correo electrónico, FTP y otras

aplicaciones de red comunes Servidores de caché web o proxy. Redes de conjuntos de servidores con IPQoS administradas por equilibradores de carga con Diffserv.

Cortafuegos que administran el tráfico de una red heterogénea sistemas IPQoS que forman parte de una red de área local (LAN) virtual puede integrar sistemas IPQoS en una distribución de red que ya tenga enrutadores con Diffserv en funcionamiento.

Si el enrutador que utiliza no admite Diffserv, considere las soluciones Diffserv que ofrecen Cisco Systems, Juniper Networks y otros fabricantes de enrutadores. Si el enrutador local no utiliza Diffserv, se limita a transferir los paquetes marcados al siguiente salto sin evaluar las marcas.

Distribuciones de Red IPQoS

En esta sección se ilustran estrategias IPQoS para redes con diferentes requisitos. IPQoS en hosts individuales. La siguiente figura ilustra una red de sistemas con IPQoS.

Figura 3 *Distribuciones de red IPQoS*



Fuente. Autoría Propia.

Planificación de la Directiva de Calidad de Servicio

Al planificar la directiva de calidad de servicio (QoS) debe revisar, clasificar y después priorizar los servicios que proporciona la red. También debe evaluar la cantidad de ancho de banda disponible para determinar la tasa a la que cada clase de tráfico se transfiere en la red.

Sin Algún Tipo de QoS, Podrían Surgir los Sigüientes Problemas:

Inestabilidad: paquetes del RDP que llegan a velocidades diferentes, lo que puede generar problemas de audio y visuales.

Pérdida de paquetes: paquetes descartados, lo que produce una retransmisión que requiere más tiempo.

Tiempo de ida y vuelta (RTT) con retraso: paquetes del RDP que tardan mucho tiempo en llegar a sus destinos, lo que provoca retrasos perceptibles entre la entrada y la reacción de la aplicación remota.

La forma menos complicada de solucionar estos problemas es aumentar el tamaño de las conexiones de datos, tanto internas como de salida por Internet. Dado que a menudo el costo de esto es prohibitivo, QoS proporciona una manera de administrar los recursos de los que dispone, en lugar de agregar ancho de banda de forma más eficaz. Para solucionar los problemas de calidad, se recomienda usar QoS en primer lugar y agregar ancho de banda solo cuando sea necesario.

Para que QoS sea eficaz, es preciso aplicar una configuración de QoS coherente en toda la organización. Cualquier parte de la ruta de acceso que no admita las prioridades de QoS puede degradar la calidad de la sesión de RDP.

Introducción a las Colas de QoS

Para proporcionar QoS, los dispositivos de red deben tener una manera de clasificar el tráfico y deben poder distinguir RDP de otro tráfico de red.

Cuando el tráfico de red entra en un enrutador, el tráfico se coloca en una cola. Si no se configura una directiva de QoS, hay solo una cola y todos los datos se tratan con el método "el primero en llegar es el primero en salir" con la misma prioridad. Esto significa que el tráfico del RDP puede quedar atascado detrás de tráfico en el que unos pocos milisegundos adicionales no serían un problema.

Al implementar QoS, se definen varias colas y para ello se usa una de las distintas características de administración de la congestión, como la puesta en cola de prioridades y la espera equitativa ponderada basada en clases (CBWFQ) de Cisco, y las características de prevención de congestiones, como la detección anticipada aleatoria ponderada (WRED).

Una analogía sencilla es que QoS crea "carriles para vehículos compartidos" virtuales en la red de datos. Por eso, algunos tipos de datos nunca, o casi nunca, sufren ningún retraso. Una vez que se crean esos carriles, se puede ajustar su tamaño relativo y administrar de forma mucho más eficaz el ancho de banda de la conexión, y todo ello sin dejar de proporcionar experiencias de nivel empresarial a los usuarios de una organización.

Lista de Comprobación de la Implementación de QoS

A nivel general, siga estos pasos para implementar QoS:

Asegúrese de que la red está preparada, Asegúrese de que RDP Shortpath para redes administradas está habilitado (las directivas de QoS no se admiten para el transporte de conexión inversa).

Implemente la inserción de marcadores de DSCP en los hosts de sesión.

Cuando se prepare para la implementación de QoS, tenga en cuenta las siguientes directrices:

La ruta de acceso más corta al host de sesión es la mejor. No se recomienda que haya ningún obstáculo, como servidores proxy o dispositivos de inspección de paquetes. Asegúrese de que la red está preparada

Si se plantea la posibilidad de realizar una implementación de QoS, ya debe haber determinado los requisitos de ancho de banda y los demás requisitos de red.

La congestión del tráfico en una red afectará significativamente a la calidad de los medios. La falta de ancho de banda conduce a la degradación del rendimiento y a una mala experiencia del usuario. A medida que crece el uso y la adopción de Azure Virtual Desktop, use Log Analytics para identificar los posibles problemas y, después, realice los ajustes necesarios mediante QoS y las adiciones de ancho de banda selectivo.

Consideraciones al Respecto de la Red Privada Virtual

QoS solo funciona según lo esperado cuando se implementa en todos los vínculos entre los clientes y los hosts de la sesión. Si QoS se usa en una red interna y un usuario inicia sesión desde una ubicación remota, solo se pueden asignar prioridades dentro de la red interna administrada. Aunque las ubicaciones remotas pueden recibir una conexión administrada mediante la implementación de una red privada virtual, una VPN implica intrínsecamente una sobrecarga de paquetes y crea retrasos en el tráfico en tiempo real.

En una organización global con vínculos administrados que abarcan continentes, se recomienda encarecidamente usar QoS, ya que el ancho de banda para esos vínculos está limitado, en comparación con la LAN. Inserción de marcadores de DSCP

Para implementar QoS se puede usar un objeto de directiva de grupo (GPO) para indicar a los hosts de sesión que inserten un marcador de DSCP en los encabezados de paquetes IP que lo identifiquen como un tipo determinado de tráfico. Tanto los enrutadores como otros dispositivos de red se pueden configurar para que reconozcan estas marcas y coloquen el tráfico en una cola independiente de mayor prioridad.

Las marcas de DSCP se pueden comparar con los sellos de franqueo que indican a los trabajadores de Correos el grado de urgencia de la entrega y cual es la mejor forma de ordenar los paquetes para entregarlos lo más rápidamente posible. Una vez que se haya configurado la red para dar prioridad a las secuencias de RDP, tanto los paquetes perdidos como los que van con retraso deberían disminuir considerablemente.

Una vez que todos los dispositivos de red usan las mismas clasificaciones, marcas y prioridades, es posible reducir o eliminar retrasos, paquetes descartados e inestabilidad. Desde la perspectiva de RDP, el paso de configuración esencial es la clasificación y el marcado de paquetes. Sin embargo, para que la QoS completa se realice correctamente, también es preciso alinear meticulosamente la configuración de RDP con la configuración de red subyacente. El valor de DSCP indica a una red configurada correspondiente qué prioridad se debe proporcionar a un paquete o secuencia.

Se recomienda usar el valor 46 de DSCP que se asigna a la clase de DSCP Expedited Forwarding (EF) .

IPTV Multicast

Configuración de dispositivos y servidor TVIP, habilitación de protocolos de enrutamiento, Multicast, RTP, configuración de cliente de video VLC y pruebas funcionales.

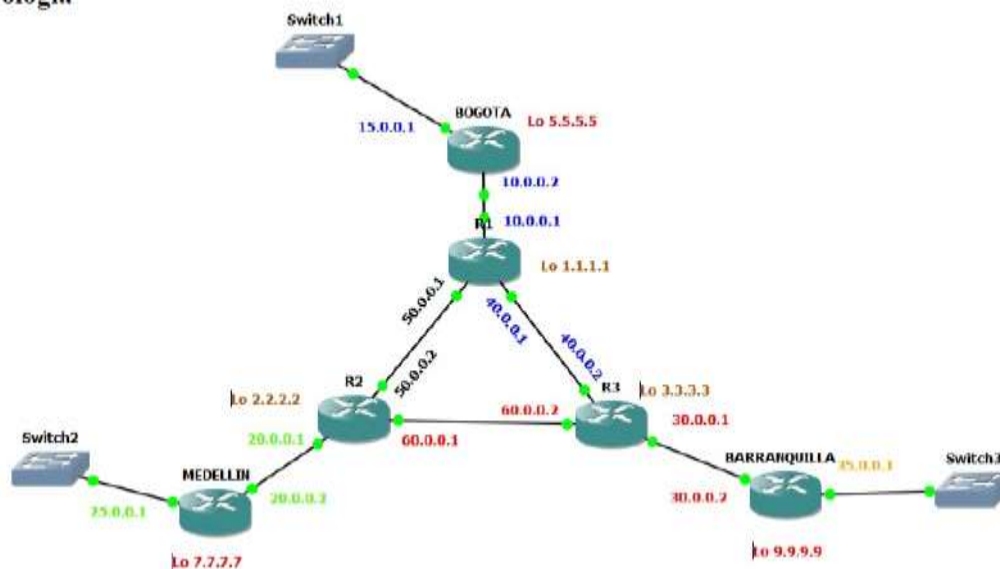
Tabla 1 *Direccionamiento IP en IPTV multicast*

Direccionamiento IP	Bogotá	Medellín	Barranquilla
WAN	10.0.1.1	10.0.2.2	10.0.3.3
Máscara	255.0.0.0	255.0.0.0	255.0.0.0
Router	201.168.1.1	201.168.2.1	201.168.3.1
Máscara	255.255.255.0	255.255.255.0	255.255.255.0
PC1	201.168.1.2	201.168.2.2	201.168.3.2
Máscara	255.255.255.0	255.255.255.0	255.255.255.0
PC2	201.168.1.3	201.168.2.3	201.168.3.3
Máscara	255.255.255.0	255.255.255.0	255.255.255.0

Nota. Transmisión de información a un grupo de receptores (clientes) que están configurados.

Figura 4 *Topología IPTV multicast*

Topología



Fuente. Autoría Propia.

Clasificación y Marketing

Class-Based Packet Marking proporciona un modo fácil mediante CLI para un marcado eficiente de los paquetes. Marca los paquetes de una determinada clase definida por el usuario previamente mediante el MQC. Se puede activar cuando se configura la política para una clase. Esta herramienta permite a los usuarios ejecutar las siguientes acciones:

Marcar los paquetes poniendo los bits del IP Precedence o el DSCP en el byte ToS de la cabecera IP.

Marcar los paquetes poniendo el valor de Clase de Servicio (CoS) de la Capa 2.

Asociar un valor de grupo local de calidad de servicio a un paquete.

Poner los bits de la prioridad de pérdida de celda (Cell Loss Priority CLP) en la cabecera ATM de un paquete de 0 a 1.

Poner el bit de Frame Relay Discard Eligibility (DE) en el campo dirección del marco frame relay de 0 a 1.

Class-Based Packet Marking se puede configurar sobre una interfaz, subinterfaz, o un circuito virtual permanente (PVC) ATM. Pero no se soporta en las siguientes interfaces:

Fast EtherChannel.

Tunnel.

Primary Rate Interface (PRI) de la Red Digital de Servicios Integrados (RDSI).

ATM switched virtual circuit (SVC).

Frame Relay data-link connection identifier (DLCI).

Marcar los paquetes con el valor de IP Precedence

En la siguiente configuración se pone el valor de IP Precedence a 5 de los paquetes que satisfagan los criterios de selección de la clase class1. Todos los paquetes que satisfagan los

criterios de selección de la clase 1 se marcarán con el valor de IP Precedence 5. El tratamiento que reciban los paquetes dependerá de la configuración de la red. Nótese que para marcar los paquetes de una determinada clase, primero se debe de haber creado la clase con el comando class-map y después la política para esa clase con el comando policy-map.

Configuración red MPLS

Aquí Habilitamos el IP CEF, Habilitamos el protocolo LDP para el intercambio de etiquetas, luego utilizamos una interfaz Loopback como router-id para LDP y utilizar la Loopback como identificador del router y por último habilitamos MPLS en cada interface.

Configuración para habilitar CEF

Configuración para habilitar CEF Ingresamos a la consola de cada uno de los router e ingresamos a la configuración general.

Figura 5

Configuración para habilitar CEF paso 1

```
EOGOTA#config t
Enter configuration commands, one per line. End with CNTL
EOGOTA(config)#ip CEF
EOGOTA(config)#ip C?
casa cef classless community-list
EOGOTA(config)#ip C
```

Fuente. Autoría Propia.

Figura 6

Configuración para habilitar CEF paso 2

```
MEDELLIN#config t
Enter configuration commands, one per line. End w
MEDELLIN(config)#ip CEF
MEDELLIN(config)#ip C?
casa cef classless community-list
```

Fuente. Autoría Propia.

Figura 7

Configuración para habilitar CEF paso 3

```
BARRANQUILLA#config t
Enter configuration commands, one per line. End with
BARRANQUILLA(config)#ip CEF
BARRANQUILLA(config)#ip C?
casa cef classless community-list
```

Fuente. Autoría Propia.

Figura 8

Configuración para habilitar CEF paso 4

```
R1#config t
Enter configuration commands, one per line.
R1(config)#ip CEF
R1(config)#ip C?
casa cef classless community-list
```

Fuente. Autoría Propia.

Figura 9

Configuración para habilitar CEF paso 5

```
R2#config t
Enter configuration commands, one per line.
R2(config)#ip CEF
R2(config)#ip C?
casa cef classless community-list
```

Fuente. Autoría Propia.

Figura 10

Configuración para habilitar CEF paso 6

```
old start
R3#config t
Enter configuration commands, one per line.
R3(config)#ip CEF
R3(config)#ip c?
casa cef classless community-list
```

Fuente. Autoría Propia.

Configuración para habilitar MPLS

Ingresamos a la consola de cada uno de los router e ingresamos a la configuración.

Figura 11

Configuración para habilitar MPLS paso 1

```
BOGOTA(config)#MPLS ip
BOGOTA(config)#MPLS label protocol LDP
BOGOTA(config)#MPLS label range 21 99
BOGOTA(config)#exit
BOGOTA#
```

Fuente. Autoría Propia.

Figura 12

Configuración para habilitar MPLS paso 2

```
BARRANQUILLA(config)#MPLS ip
BARRANQUILLA(config)#MPLS label protocol LDP
BARRANQUILLA(config)#MPLS label range 21 99
BARRANQUILLA(config)#^Z
BARRANQUILLA#wr
```

Fuente. Autoría Propia.

Figura 13

Configuración para habilitar MPLS paso 3

```
R1(config)#MPLS ip
R1(config)#MPLS label protocol LDP
R1(config)#MPLS label range 21 99
R1(config)#^Z
R1#
```

Fuente. Autoría Propia.

Figura 14

Configuración para habilitar MPLS paso 4

```
R2(config)#MPLS ip
R2(config)#MPLS label protocol LDP
R2(config)#MPLS label range 21 99
R2(config)#^Z
R2#
```

Fuente. Autoría Propia.

Configuramos los puertos de interface Ingresamos a la consola de cada uno de los router e ingresamos a la configuración general. Verificamos la Configuramos los puertos de interface ingresamos a la consola de cada uno de los router revisamos el loopback y la interface.

Figura 15*Configuración para habilitar MPLS paso 5*

```

BOGOTA#config t
Enter configuration commands, one per line. End with
BOGOTA(config)#interface f0/0
BOGOTA(config-if)#ip address 10.0.0.2 255.255.255.252
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#
*Mar 1 00:39:35.087: %LINK-3-UPDOWN: Interface FastE
*Mar 1 00:39:36.087: %LINEPROTO-5-UPDOWN: Line proto
BOGOTA(config-if)#interface f0/1
BOGOTA(config-if)#ip address 15.0.0.1 255.255.255.252
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#
*Mar 1 00:40:12.223: %LINK-3-UPDOWN: Interface FastE
*Mar 1 00:40:13.223: %LINEPROTO-5-UPDOWN: Line proto
BOGOTA(config-if)#^Z

```

*Fuente. Autoría Propia.***Figura 16***Configuración para habilitar MPLS paso 6*

```

MEDELLIN#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#interface f0/0
MEDELLIN(config-if)#ip address 10.0.0.2 255.255.255.252
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#
*Mar 1 00:40:09.183: %LINK-3-UPDOWN: Interface FastEthernet0/0, c
*Mar 1 00:40:10.183: %LINEPROTO-5-UPDOWN: Line protocol on Interf
MEDELLIN(config-if)#interface f0/1
MEDELLIN(config-if)#ip address 15.0.0.1 255.255.255.252
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#
*Mar 1 00:40:32.651: %LINK-3-UPDOWN: Interface FastEthernet0/1, c
*Mar 1 00:40:33.651: %LINEPROTO-5-UPDOWN: Line protocol on Interf
MEDELLIN(config-if)#
MEDELLIN(config-if)#^Z
MEDELLIN#

```

*Fuente. Autoría Propia.***Figura 17***Configuración para habilitar MPLS paso 7*

```

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface f0/0
R1(config-if)#ip address 50.0.0.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#interface f0/1
*Mar 1 00:25:49.715: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed
*Mar 1 00:25:50.715: %LINEPROTO-5-UPDOWN: Line protocol on Interface Fa
R1(config-if)#interface f0/1
R1(config-if)#ip address 40.0.0.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#
*Mar 1 00:26:11.995: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed
*Mar 1 00:26:12.995: %LINEPROTO-5-UPDOWN: Line protocol on Interface Fa
R1(config-if)#interface f1/0
R1(config-if)#ip address 10.0.0.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#

```

Fuente. Autoría Propia.

Configuramos Multicast

Habilitamos Multicast los router Ingresamos a la consola de cada uno de los router e ingresamos a la configuración general.

Figura 18

Configuración para multicast paso 1

```
BOGOTA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#ip multicast-routing
BOGOTA(config)#^Z
BOGOTA#wr
```

Fuente. Autoría Propia.

Figura 19

Configuración para multicast paso 2

```
MEDELLIN#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#ip multicast-routing
MEDELLIN(config)#^Z
MEDELLIN#w
```

Fuente. Autoría Propia.

Figura 20

Configuración para multicast paso 3

```
BARRANQUILLA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BARRANQUILLA(config)#ip multicast-routing
BARRANQUILLA(config)#^Z
BARRANQUILLA#
```

Fuente. Autoría Propia.

Configuramos router con las redes globales

Ingresamos a la consola de cada uno de los router e ingresamos a la configuración general.

Figura 21 *Configuración router con las redes globales paso 1*

```
router ospf 3
mpls ldp autoconfig
router-id 5.5.5.5
log-adjacency-changes
network 5.5.5.5 0.0.0.0 area 0
network 10.0.0.0 0.0.0.3 area 0
network 15.0.0.0 0.0.0.3 area 0
```

Fuente. Autoría Propia.

Figura 22

Configuración router con las redes globales paso 2

```
router ospf 3
mpls ldp autoconfig
router-id 7.7.7.7
log-adjacency-changes
network 7.7.7.7 0.0.0.0 area 0
network 20.0.0.0 0.0.0.3 area 0
network 25.0.0.0 0.0.0.3 area 0
```

Fuente. Autoría Propia.

Figura 23

Configuración router con las redes globales paso 3

```
router ospf 3
mpls ldp autoconfig
router-id 9.9.9.9
log-adjacency-changes
network 9.9.9.9 0.0.0.0 area 0
network 30.0.0.0 0.0.0.3 area 0
network 35.0.0.0 0.0.0.3 area 0
```

Fuente. Autoría Propia.

Figura 24

Configuración router con las redes globales paso 4

```
R1(config)#router ospf 3
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 1.1.1.1 0.0.0.0 area 0
R1(config-router)#network 10.0.0.0 0.0.0.3 area 0
R1(config-router)#network 10.0.0.0 0.0.0.3 area 0
*Mar 1 00:58:35.455: %OSPF-5-ADJCHG: Process 3, Nbr
rom LOADING to FULL, Loading Done
R1(config-router)#network 40.0.0.0 0.0.0.3 area 0
*Mar 1 00:58:42.667: %LDP-5-NBRCHG: LDP Neighbor 5.1
R1(config-router)#network 40.0.0.0 0.0.0.3 area 0
R1(config-router)#network 50.0.0.0 0.0.0.3 area 0
R1(config-router)#^Z
```

Fuente. Autoría Propia.

Figura 25 Configuración router con las redes globales paso 5

```
R2(config)#router ospf 3
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 2.2.2.2 0.0.0.0 area 0
R2(config-router)#network 50.0.0.0 0.0.0.3 area 0
R2(config-router)#network 50.0.0.0 0.0.0.3 area 0
*Mar 1 01:07:15.499: %OSPF-5-ADJCHG: Process 3, Nbr
om LOADING to FULL, Loading Done
R2(config-router)#network 60.0.0.0 0.0.0.3 area 0
R2(config-router)#network 60.0.0.0 0.0.0.3 area 0
*Mar 1 01:07:28.899: %LDP-5-NBRCHG: LDP Neighbor 1.1
R2(config-router)#network 20.0.0.0 0.0.0.3 area 0
R2(config-router)#
*Mar 1 01:07:42.675: %OSPF-5-ADJCHG: Process 3, Nbr
```

Fuente. Autoría Propia.

Router y DHCP

Figura 26

Configuración Router y DHCP paso 1

```
ip dhcp pool BOGOTA
  network 201.168.1.0 255.255.255.0
  default-router 201.168.1.1
```

Fuente. Autoría Propia.

Figura 27

Configuración Router y DHCP paso 2

```
MEDELLIN(config)#
MEDELLIN(config)#ip dhcp pool MEDELLIN
MEDELLIN(dhcp-config)#network 201.168.2.0 255.255.255.0
MEDELLIN(dhcp-config)#default-router 201.168.2.1
MEDELLIN(dhcp-config)^Z
MEDELLIN#
```

Fuente. Autoría Propia.

Figura 28

Configuración Router y DHCP paso 3

```
ip dhcp pool BARRANQUILLA
  network 201.168.3.0 255.255.255.0
  default-router 201.168.3.1
```

Fuente. Autoría Propia.

Grupos de multicast

Figura 29 *Configuración grupos de multicast paso 1*

```
BOGOTA(config)#int Lo0
BOGOTA(config-if)#ip pim sparse-mode
BOGOTA(config-if)#
"Mar 1 02:57:20.939: %PIM-5-DRCHG: DR change from neighbo
BOGOTA(config-if)#int f0/0
BOGOTA(config-if)#ip pim sparse-mode
BOGOTA(config-if)#
"Mar 1 02:58:01.811: %PIM-5-DRCHG: DR change from neighbo
BOGOTA(config-if)#int f0/1
BOGOTA(config-if)#ip pim sparse-mode
BOGOTA(config-if)^Z
BOGOTA#
```

Fuente. Autoría Propia.

Figura 30

Configuración grupos de multicast paso 2

```
MEDELLIN#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#int Lo0
MEDELLIN(config-if)#ip pim sparse-mode
MEDELLIN(config-if)#int
*Mar 1 02:57:11.135: %PIM-5-DRCHG: DR change from neighbor 0
MEDELLIN(config-if)#int f0/0
MEDELLIN(config-if)#ip pim sparse-mode
MEDELLIN(config-if)#
*Mar 1 02:57:32.779: %PIM-5-DRCHG: DR change from neighbor 0
MEDELLIN(config-if)#int f0/1
MEDELLIN(config-if)#ip pim sparse-mode
MEDELLIN(config-if)#
*Mar 1 02:57:46.063: %PIM-5-DRCHG: DR change from neighbor 0
MEDELLIN(config-if)#^Z
MEDELLIN#
*Mar 1 02:57:51.015: %SYS-5-CONFIG: 2: Configuration saved
```

Fuente. Autoría Propia.

Figura 31

Configuración grupos de multicast paso 3

```
BARRANQUILLA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BARRANQUILLA(config)#int Lo0
BARRANQUILLA(config-if)#ip pim sparse-mode
BARRANQUILLA(config-if)#
*Mar 1 02:53:11.543: %PIM-5-DRCHG: DR change from neighbor
BARRANQUILLA(config-if)#int f0/0
BARRANQUILLA(config-if)#ip pim sparse-mode
BARRANQUILLA(config-if)#
*Mar 1 02:53:24.847: %PIM-5-DRCHG: DR change from neighbor
BARRANQUILLA(config-if)#int f0/1
BARRANQUILLA(config-if)#ip pim sparse-mode
BARRANQUILLA(config-if)#
*Mar 1 02:53:38.751: %PIM-5-DRCHG: DR change from neighbor
BARRANQUILLA(config-if)#^Z
BARRANQUILLA#
```

Fuente. Autoría Propia.

Enrutamiento

Figura 32

Configuración de enrutamiento paso 1

```
BOGOTA#
BOGOTA#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

 5.0.0.0/32 is subnetted, 1 subnets
C       5.5.5.5 is directly connected, Loopback0
 10.0.0.0/30 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, FastEthernet0/0
 15.0.0.0/30 is subnetted, 1 subnets
C       15.0.0.0 is directly connected, FastEthernet0/1
BOGOTA#
```

Fuente. Autoría Propia.

Figura 33

Configuración de enrutamiento paso 2

```
MEDELLIN#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

 20.0.0.0/30 is subnetted, 1 subnets
C       20.0.0.0 is directly connected, FastEthernet0/0
  7.0.0.0/32 is subnetted, 1 subnets
C       7.7.7.7 is directly connected, Loopback0
 25.0.0.0/30 is subnetted, 1 subnets
C       25.0.0.0 is directly connected, FastEthernet0/1
MEDELLIN#
```

Fuente. Autoría Propia.

Figura 34

Configuración de enrutamiento paso 3

```

BARRANQUILLA#
BARRANQUILLA#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

 35.0.0.0/30 is subnetted, 1 subnets
C       35.0.0.0 is directly connected, FastEthernet0/1
  9.0.0.0/32 is subnetted, 1 subnets
C       9.9.9.9 is directly connected, Loopback0
 30.0.0.0/30 is subnetted, 1 subnets
C       30.0.0.0 is directly connected, FastEthernet0/0
BARRANQUILLA#

```

Fuente. Autoría Propia.

Figura 35

Configuración de enrutamiento paso 4

```

R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

 1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
 50.0.0.0/30 is subnetted, 1 subnets
C       50.0.0.0 is directly connected, FastEthernet0/0
 40.0.0.0/30 is subnetted, 1 subnets
C       40.0.0.0 is directly connected, FastEthernet0/1
 10.0.0.0/30 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, FastEthernet1/0
R1#

```

Fuente. Autoría Propia.

Figura 36*Configuración de enrutamiento paso 5*

```

R2#show ip route
Codes: C - connected, S - static, R - RTP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

 50.0.0.0/30 is subnetted, 1 subnets
C    50.0.0.0 is directly connected, FastEthernet0/0
 2.0.0.0/32 is subnetted, 1 subnets
C    2.2.2.2 is directly connected, Loopback0
 20.0.0.0/30 is subnetted, 1 subnets
C    20.0.0.0 is directly connected, FastEthernet1/0
 60.0.0.0/30 is subnetted, 1 subnets
C    60.0.0.0 is directly connected, FastEthernet0/1
R2#

```

*Fuente. Autoría Propia.***Comunicación****Figura 37***Configuración de comunicación paso 1*

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.1	1	FULL/BDR	00:00:34	10.0.0.1	FastEthernet0/0

BOGOTA#

*Fuente. Autoría Propia.***Figura 38 Configuración de comunicación paso 2**

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	1	FULL/BDR	00:00:36	20.0.0.1	FastEthernet0/0

MEDELLIN#

*Fuente. Autoría Propia.***Figura 39 Configuración de comunicación paso 3**

Neighbor ID	Pri	State	Dead Time	Address	Interface
9.9.9.9	1	FULL/BDR	00:00:39	30.0.0.1	FastEthernet0/0

BARRANQUILLA#

*Fuente. Autoría Propia.***Figura 40 Configuración de comunicación paso 4**

```

R1#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
9.9.9.9          1    FULL/DR         00:00:39   40.0.0.2    FastEthernet0/1
15.0.0.1         1    FULL/DR         00:00:30   10.0.0.2    FastEthernet1/0
R1#

```

Fuente. Autoría Propia.

Figura 41

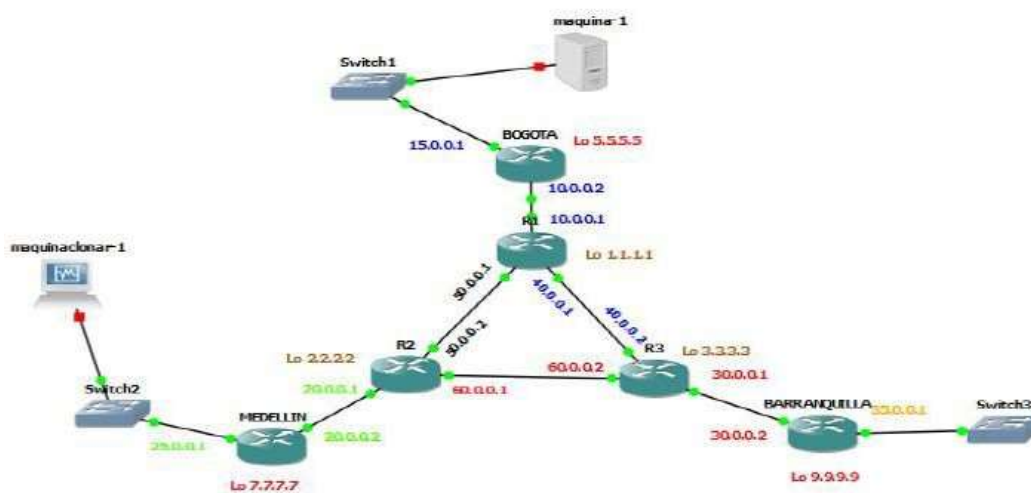
Configuración de comunicación paso 5

Neighbor ID	Pri	State	Dead Time	Address	Interface
25.0.0.1	1	FULL/DR	00:00:31	20.0.0.2	FastEthernet1/0
9.9.9.9	1	FULL/BDR	00:00:33	60.0.0.2	FastEthernet0/1
1.1.1.1	1	FULL/DR	00:00:34	50.0.0.1	FastEthernet0/0

R2#

Fuente. Autoría Propia.

Simulación transmisor a receptor

Figura 42 Simulación transmisor a receptor

Fuente. Autoría Propia.

Conclusiones

Para concluir, el desarrollo de las actividades propuestas en la fase 11 del diplomado de profundización en redes de nueva generación, me ha permitido identificar las capas y funciones de un modelo de red, a través de la investigación de los conceptos vigentes, los cuales son la base dentro de una arquitectura de red.

También he identificado los protocolos y funciones de la capa de red, mediante el uso de los principios de direccionamiento IP, enmarcados dentro de los estándares, así como reconocer las capas, protocolos, funciones y ventajas de una arquitectura NGN utilizada en la interconexión de redes, mediante la comparación con las redes tradicionales y el uso de protocolos involucrados.

En el desarrollo de la actividad se identificaron los protocolos de IoT (Internet Of Things), mediante la investigación de los conceptos vigentes que responden a los estándares actuales y configurar servicios multimedia para un escenario de NGN a nivel de simulación, aplicando los conceptos de arquitectura funcional y definiendo políticas de Calidad de Servicio (QoS, Quality of Service).

Recomendaciones

El surgimiento de nuevos servicios y tecnologías de las telecomunicaciones requieren adquirir el compromiso por parte de los actores involucrados en el sector de las telecomunicaciones de obtener nuevos conocimientos y la adaptabilidad de infraestructuras para la implementación de los nuevos cambios tecnológicos basándose en la identificación de los protocolos y funciones de las capas de redes, mediante el uso de los principios de direccionamiento IP, enmarcados dentro de los estándares, así como funciones y ventajas de una arquitectura NGN utilizada en la interconexión de redes, mediante la comparación con las redes tradicionales y el uso de protocolos involucrados en la implementación de un servicio IPTV.

Referencias Bibliográficas

- Aguirre, E., Calva, J., Guerrero, A., Hernández, A., Hernández, S., y Hernández, G. (2017). Comparación de los modelos OSI y TCP/IP. *Ciencia Huasteca Boletín Científico De La Escuela Superior De Huejutla*, 5(10). Recuperado de <https://bibliotecavirtual.unad.edu.co/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.DCE36D6C&lang=es&site=eds-live&scope=site>
- Álvarez Mise, L. F., & Romero Gallardo, C. G. (2012) Evaluación del desempeño de los sistemas de autenticación del estándar de seguridad IEEE 802.1 X para la integración de un portal cautivo bajo el protocolo de RADIUS. <http://repositorio.espe.edu.ec/bitstream/21000/32161/1/T-ESPE-052448.pdf>
- Cedeño Tumbaco, L. L., & Peñaherrera Espín, K. E. (2017). *Implementación de una red lan con la utilización de cableado estructurado basado en las normas internacionales ANSI/TIA/EIA 568-B, en el Laboratorio de Investigación de Ingeniería de Software en la Universidad Técnica De Cotopaxi, Extensión La Maná, en el año 2017* (Bachelor's thesis, Ecuador: La Mana: Universidad Técnica de Cotopaxi; Facultad de Ciencias de la Ingeniería y Aplicadas; Carrera de Ingeniería en Informática y Sistemas Computacionales). <http://repositorio.utc.edu.ec/handle/27000/4621>
- Contero Ramos, W. M. (2019). Diseño de una política de seguridad de la información basada en la norma ISO 27002: 2013, para el sistema de botones de seguridad del Ministerio del Interior. <https://repositorio.uisek.edu.ec/handle/123456789/3345>
- Guerrero Cadena, J. A. (2015). Diseñar un modelo de red de comunicación de voz, datos y televisión para conjuntos habitacionales basado en la normativa iso 11801. <https://repositorio.uisek.edu.ec/handle/123456789/3197>

López Caro, J. J., & Hernández Pastrana, L. (2012). Guía para diseñar instalaciones eléctricas domiciliarias según NTC 2050 y Retie.

<https://repositorio.utb.edu.co/handle/20.500.12585/664>

Ortiz, F. L. (2010). El estándar IEEE 802.11 wireless lan. *Univ. Politécnica Madr.*

<http://www.dit.upm.es/~david/tar/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf>

Rubio, G. A., Díaz, E. A. M., Alfonso, A., VarónCristian, A. O. F., & Rubio, C. E. (2020).

Evaluación de la reglamentación interna para las redes de telecomunicaciones (ritel) y su uso en la construcción de una ciudad inteligente en el ámbito smartliving. *Memorias.*

<https://hemeroteca.unad.edu.co/index.php/memorias/article/view/4177>