ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ANÁLISIS DEL TRÁFICO EN UN AMBIENTE SIMULADO CON VLANS Y RECOMENDACIONES DE POLÍTICAS DE SERVICIO Y DISEÑO DE UNA RED SAI"

TRABAJO DE TITULACIÓN

Previo a la obtención del título de:

MAGÍSTER EN TELECOMUNICACIONES

PABLO ANDRÉS VALLEJO ZAMBRANO

GUAYAQUIL – ECUADOR

AÑO: 2019

AGRADECIMIENTO

Agradezco a las autoridades de la Escuela Superior Politécnica del Litoral por abrirme las puertas a esta prestigiosa universidad, a todos los profesores de la Maestría en Telecomunicaciones por haberme compartido sus conocimientos. De manera especial, al máster César Yépez Flores, tutor de mi proyecto de titulación, por toda su confianza en mi esfuerzo, quien me ha orientado y aconsejado con mucha claridad y paciencia durante todo el proceso de investigación.

DEDICATORIA

Esta Tesis está dedicada a:

A mis padres Dimas y Rosario, los pilares más importantes de mi familia, quienes siempre me han brindado su apoyo y cariño de manera incondicional durante toda mi vida.

A mi hermano Dimas, por siempre aconsejarme y brindarme siempre su entera confianza.

A todos mis amigos por siempre me han acompañado en mis luchas personales y han aportado en mi formación como ser humano.

Y una dedicatoria muy especial a mi hermana Sharon, quien ya paso a mejor vida y me hace mucha falta. Estoy seguro de que donde se encuentre, siempre está pendiente de mí.

TRIBUNAL DE EVALUACIÓN

_____

Ph.D. César Martín Moreno

SUBDECANO DE LA FIEC

_____

Ph.D. Boris Ramos Sánchez

DIRECTOR DEL TRABAJO DE TITULACIÓN

_____

Msig. Ronald Criollo Bonilla

MIEMBRO PRINCIPAL DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, me corresponde exclusivamente; y doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Pablo Andrés Vallejo Zambrano

RESUMEN

Para los proveedores de servicio de acceso a internet (SAI) es importante desarrollar procedimientos y llevar políticas de servicio y diseño, que permitan reducir problemas de red, usar eficientemente sus recursos y ofrecer a sus clientes un servicio con solidez, confiabilidad, seguridad y garantía.

Entre las practicas que un proveedor de SAI puede incorporar para optimizar el servicio que ofrece a sus clientes, se encuentra la implementación las redes virtuales de área local (VLAN), que segmentan la red de forma lógica en lugar de física, balanceando la carga de tráfico y permitiendo que los anchos de banda sean aprovechados eficientemente, disminuyendo considerablemente las consecuencias de tener un alto tráfico de broadcast en la red.

Esta investigación está orientada a realizar un escenario en el que se pueda medir el impacto del uso de VLANs en una red en crecimiento, en la que se realizará la segmentación de dominios de broadcast para la detección y análisis de envío y recepción de paquetes con esta solución implementada.

Las pruebas realizadas en un ambiente de simulación son de mucha utilidad para llegar a numerosos escenarios que pueden abarcar los principales problemas que ocurren dentro de la infraestructura física y principalmente la estructura lógica de los mismos, para aportar técnicamente a las soluciones con mejores prácticas dentro de la administración de los SAI.

Se propone, mediante simulación, realizar una configuración de VLAN en una de las redes principales del proveedor de SAI Celeritel Solutions S.A. con el fin de comprobar la eficiencia del tráfico dentro del ambiente simulado. Con los resultados obtenidos y las configuraciones de red determinadas, se implementa la solución de uso de VLANs en parte de la red del proveedor de SAI, posteriormente realizando la medición de trafico de red, para comprobar la efectividad y beneficios del uso de VLANs.

El resultado de esta investigación podrá ser utilizado en el área de las telecomunicaciones como aporte investigativo para el desarrollo de normativas que logren hacer de la administración de un SAI se pueda orientar a tener un espectro limpio de problemas relacionados al tráfico de difusión de red y ataques de seguridad, que pueden afectar el desempeño del servicio frente a los usuarios de internet.

ÍNDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

CAPÍTULO 1

1 PLANTEAMIENTO DE LA PROBLEMÁTICA

1.1 Descripción del problema

El broadcast es la difusión masiva de información o paquetes de datos a través de redes informáticas, considerada como la transferencia de información desde un nodo emisor a una multitud de nodos receptores. La Capa de Enlace de Datos o capa 2 del modelo OSI, actúa como intermediaria entre la capa de red y la capa física, codificando las tramas recibidas desde la capa de red para su transmisión desde la capa física, controlando el acceso al medio y los posibles errores en la transmisión.

También es considerada como un área de una red de computadoras formada por todas las computadoras y dispositivos de red que se pueden alcanzar enviando una trama a la dirección de difusión de la capa de enlace de datos.

En la actualidad la implementación de redes de área local (LAN) en empresas, negocios y otras instituciones se lo realiza a través de dispositivos físicos conectados a un mismo concentrador que comparten el ancho de banda disponible y forman parte del mismo dominio de broadcast.

Un dominio de broadcast es el área lógica en una red de computadoras en la que cualquier computadora conectada a la red puede transmitir directamente a cualquier otra computadora en el dominio sin precisar ningún dispositivo de encaminamiento.

En el caso de los proveedores de servicio de acceso a internet (SAI) es importante desarrollar procedimientos y llevar políticas de servicio o diseño que les permita reducir estos problemas, usar eficientemente sus recursos y ofrecer a sus clientes un servicio con solidez, confiabilidad, seguridad y garantía.

Usualmente, cada SAI cuenta con un equipo de técnicos que manejan la infraestructura física y lógica implementada, la misma que deben cumplir con estándares y normas internacionales para el manejo de redes ampliadas.

Entre estas prácticas se encuentra la tecnología de las redes virtuales de área local (VLAN), que segmentan la red de forma lógica en lugar de física, balanceando la carga de tráfico y permitiendo que los anchos de banda sean aprovechados eficiente y finalmente que las consecuencias del fenómeno broadcast sean disminuidas considerablemente, entre otras.

Esta investigación está orientada a realizar un escenario en el que se pueda medir el impacto de diversas formas de segmentación de redes para la detección de problemas en la red, mediante el análisis del del tráfico de broadcast.

1.2 Justificación

La infraestructura de los SAI puede robustecerse al contar con políticas de uso que permitirán la mejora incremental de la disponibilidad y accesibilidad de datos, haciendo que el tráfico se garantice para los consumidores de internet en cualquier momento del día.

El análisis de la pérdida de datos en las conexiones, las causas, tipos de interferencias y la consecuencia relacionada a omisión de datos, así como identificar los mejores aplicativos para llevar a cabo estas tareas permitirá tener insumos para lograr una buena administración de las conexiones dentro del SAI.

Las pruebas realizadas en un ambiente de simulación son de mucha utilidad para llegar a numerosos escenarios que pueden abarcar los principales problemas que ocurren dentro de la infraestructura física y principalmente la estructura lógica de los mismos, para aportar técnicamente a las soluciones con mejores prácticas dentro de la administración de los SAI.

El resultado de esta investigación podrá ser utilizado en el área de las telecomunicaciones como aporte investigativo para el desarrollo de aplicaciones que logren hacer de la administración de un SAI un conjunto adecuado de normas y aplicaciones que cumplan los estándares nacionales e internacionales orientándose principalmente a tener un espectro limpio de ciberataques y de espionaje cibernético que afecten el desempeño del servicio frente a los usuarios de internet.

1.3 Solución Propuesta

La propuesta de un escenario de simulación orientada a la medición de impacto de prácticas simuladas con VLANS y aplicativos en los SAI permitirá abrir las posibilidades de reforzar las medidas de acceso, distribución y control que actualmente tienen los proveedores de servicios con un costo mínimo de implementación, sin afectar al servicio actual ni a la implementación de nuevos proyectos de ampliación.

1.4 Objetivos de la tesis

1.4.1 Objetivos generales

Recomendar políticas de servicio y diseño de una red SAI apoyado por un ambiente simulado con VLANS.

1.4.2 Objetivos específicos

- Establecer un escenario de simulación con VLANS para una red SAI.
- Evaluar las características y cuantificación de los mensajes de broadcast dentro del escenario de simulación.
- Evaluar fenómenos e incidentes ocurridos dentro del escenario de simulación.
- Analizar los resultados obtenidos de tráfico, procesamiento de señales y características de los incidentes o mediciones realizados dentro del escenario de simulación.
- Desarrollar una propuesta de recomendaciones de políticas de servicios que permitan mejorar la eficiencia en el servicio que el SAI ofrece al usuario final.

1.5 Metodología

La metodología por utilizarse en esta investigación será de carácter aplicativo analítico con la finalidad de evaluar los distintos incidentes y resultados de las mediciones realizadas. Mediante la observación directa y la cuantificación de resultados en redes que proveen servicio, se desarrollarán recomendaciones de políticas de servicio para un SAI con el fin de mejorar su eficiencia y calidad.

1.6 Alcance

Esta investigación tiene como finalidad proponer recomendaciones para mejorar la eficiencia en el servicio que los proveedores de internet, en base a los resultados obtenidos de las mediciones que se realicen en un ambiente simulado y en una muestra de una red SAI mediante la implementación de VLANs.

CAPÍTULO 2

2 MARCO TEÓRICO

2.1 Red

Los clientes son los equipos que se conectan a una red para utilizar servicios como una conexión de Internet compartida, dispositivos de almacenamiento público e impresoras. Si tiene una red doméstica inalámbrica utilizando un enrutador o conmutador, cada equipo de la red es un cliente.

2.1.1 Controlador de tráfico

El controlador de tráfico es el dispositivo que administra la comunicación en una red. En una red doméstica, este dispositivo es típicamente un enrutador (router) o conmutador (switch). Un equipo llamado servidor también puede actuar como un controlador de tráfico. Los sistemas operativos orientados al servidor, como Windows Server y Linux, están diseñados específicamente para este trabajo. El controlador de tráfico en una red dirige información de clientes a Internet u otros dispositivos de la red y envía datos de vuelta a los clientes cuando sea necesario. El controlador de tráfico asigna un también un número de identificación único llamado "dirección IP" a cada equipo de la red. (Hernández & García, 2013)

La infraestructura por la cual se transfieren los datos entre los equipos terminales de red y otros dispositivos se conocen como medio de red. Por ejemplo, en una red de área local cableada, el medio de red comúnmente utilizado es el cable Ethernet. Otros medios de red son el cable coaxial, trasmisores de radio inalámbricos y fibra óptica.

2.1.2 Importancia de la red

Un computador es un equipo utilizado para manejar datos. El beneficio de vincular computadores entre sí surge de la necesidad de comunicación que los seres humanos tienen por naturaleza. (Pincay & Villagomez, 2015)

Una red de ordenadores puede tener varios propósitos:

- Compartir archivos, aplicaciones, hardware, conexión a Internet, etc.
- Envío y recepción de correo electrónico, discusiones en vivo, videoconferencias etc.
- La comunicación entre procesos como por ejemplo para equipos industriales.

- Garantizar el acceso a la información para un grupo determinado de personas, incluyendo bases de datos en red.

- Videojuegos Multijugador (Pincay & Villagomez, 2015).

Ventajas de la red

- Los archivos pueden ser almacenados en un ordenador central conocido como servidor de archivos, el cual permite compartir datos en la red.

- Los datos pueden ser administrados con más facilidad cuando están todos en un servidor de archivos central, en vez de cuando los datos se encuentran dispersados en varios ordenadores independientes.

- Las redes también permiten establecer la seguridad de acceso a la información, permitiendo que los usuarios de la red sólo puedan tener acceso a archivos y aplicaciones determinados. (Pincay & Villagomez, 2015)

Desventajas de la red

- Si se producen problemas con el servidor, toda la red puede quedar inoperativa.
- Se requiere de habilidades técnicas para gestionar eficazmente una red.
- Falta de conocimiento de la infraestructura de red. (Pincay & Villagomez, 2015)

2.1.3 Red de Servicio

Un servicio de red es un conjunto de operaciones implementado por un protocolo a través de una interfaz, y se ofrece a la capa inmediatamente superior. Se define lo que una capa puede ejecutar, sin preocuparse por la forma en la que se ejecutan las operaciones. Cada servicio es utilizado por aplicaciones diferentes, pudiendo una aplicación utilizar varios servicios, como un navegador como el Mozilla Firefox. Esta aplicación utiliza, por ejemplo, HTTP, HTTPS, DNS, etc.

Los servicios pueden ser orientados o no orientados a la conexión. Los servicios relacionados con la familia TCP se orientan a la conexión, mientras que los servicios relacionados con el protocolo UDP no son orientados a la conexión. (Moro Vallina, 2013)

Los procesos de una red de servicios son:

- **Red Multiservicio:** Permite Integrar los servicios de voz y de datos sobre la misma infraestructura" (Pincay & Villagomez, 2015)
- **Calidad de servicio:** Son tecnologías que le facilitan la capacidad para administrar el tráfico de red de manera eficaz y mejorar la experiencia del

usuario para una aplicación de red determinada (Pincay & Villagomez, 2015)

- **Seguridad:** El cliente debe contar con un servicio que le brinde una red totalmente privada. (Pincay & Villagomez, 2015)
- **Movilidad:** Permitirá el suministro constante de servicios para los usuarios, aunque estos se encuentren en movimiento dentro de un área o distancia determinada. (Hackbarth, y otros, 2009)
- **Fiabilidad:** Es la característica que deben tener los sistemas informáticos en la cual se mide el tiempo de funcionamiento sin errores (Vietes, 2015)
- **Escalabilidad:** Es la propiedad que puede tener un sistema para crecer, reaccionar y adaptarse sin perder calidad de los servicios que ofrece. (Vietes, 2015)

2.2 Infraestructura de red

La infraestructura de red es conformada por el hardware y recursos de software que hacen posible la conectividad de red, permitiendo la comunicación, operación y administración de una red. Proporciona la ruta que permite la comunicación entre usuarios, aplicaciones, procesos, servicios y redes externas. (Gallego, 2015)

La infraestructura de red suele formar parte de la infraestructura de tecnologías de la información (TI) que se encuentra en la mayoría de los entornos de TI empresariales. Toda la infraestructura de red está interconectada y puede utilizarse para comunicaciones internas, comunicaciones externas o ambas. Una infraestructura de red típica incluye: (Moro Vallina, 2013)

Hardware de red:

- Enrutadores
- Interruptores
- Tarjetas LAN
- Enrutadores inalámbricos
- Cables

Software de red:

- Operaciones y gestión de red
- Sistemas operativos
- Firewall
- Aplicaciones de seguridad de red
- Línea T-1
- DSL
- Satélite
- Protocolos inalámbricos
- Direccionamiento IP

2.2.1 Tipos y características

La forma de categorizar los distintos tipos de diseños de redes informáticas es por su alcance o escala, por este motivo, los tipos de redes de acuerdo con su diseño son conocidos como algún tipo de red de área. Los tipos de redes de área más comunes son: (Lindse & Simon, 2013)

- LAN - Red de área local
- WAN - Red de área amplia
- WLAN - Red de área local inalámbrica
- MAN - Red de Área Metropolitana
- CAN: red de área del campus, red de área del controlador o, a veces, red de área del clúster
- SAN: red de área de almacenamiento, red de área de sistema, red de área de servidor o, a veces, red de área pequeña
- PAN - Red de área personal

Las redes de área local (LAN) y de área amplia (WAN) son los dos tipos principales de redes de área y los más conocidos, mientras que los otros tipos de redes de área han surgido de acuerdo con los avances tecnológicos. (Lindse & Simon, 2013)

LAN: red de área local

Una LAN es una red que esta confinada a espacio limitado, tal como un edificio o una casa. Usa tecnologías de corto rango como Ethernet y Token Ring. Una LAN generalmente está bajo el control de la empresa, persona o entidad que requiere su uso. (Donahue, 2011)

WAN: red de área amplia

Una red de área amplia (WAN) permite la transmisión a larga distancia de datos, imágenes, audio y video sobre grandes áreas geográficas que pueden ser un país, un continente o incluso abarcar todo el planeta. Una red WAN puede ser muy compleja, como la infraestructura de conexión a internet, o muy simple, como una conexión de par trenzado que conecta una computadora residencial a internet. El primer ejemplo es una WAN conmutada y el segundo caso una WAN punto a punto.

La red WAN conmutada conecta a los equipos terminales, que puede ser un router que conecta a otra LAN o a una WAN.

La red WAN punto a punto es normalmente el medio de conexión como un par trenzado, cable coaxial o fibra óptica; que conecta una computadora residencial o una LAN pequeña al proveedor de internet (ISP). (Forouzan, 2007)

Otros tipos de redes de área

Aunque las redes LAN y WAN son los tipos de redes más populares, existen otros tipos de redes comunes:

- Red de área local inalámbrica: es una LAN que opera bajo tecnología de red inalámbrica Wi-Fi. (Donahue, 2011)
- Red de área del campus: es una red que conecta varias LANs o edificios en un área discreta controlada por una entidad, como por ejemplo una universidad o un campus comercial local. (Donahue, 2011)
- Red de área metropolitana: es una red que conecta varias LANs o edificios en un área que generalmente es más grande que un campus. (Donahue, 2011)
- Red de área de almacenamiento: permite la conexión entre servidores y dispositivos de almacenamiento de datos a través de una tecnología como canal de fibra (Castells, 2017)

Además de los tipos mencionados, las siguientes características son utilizadas también para categorizar los diferentes tipos de redes:

Topología: se refiere a la forma en la que una red se conecta físicamente, dos o más dispositivos se conectan por medio de un enlace; dos o más enlaces forman una topología. La topología de una red es la representación geométrica de la relación de todos los enlaces y dispositivos de red. Existen 4 tipos de topologías posibles: malla, estrella, bus y anillo. (Forouzan, 2007)

Protocolo: es un conjunto de reglas que gobiernan la comunicación de datos. Representa un acuerdo entre los dispositivos de comunicación. Sin un protocolo de por

medio, dos dispositivos pueden estar conectados físicamente sin poder comunicarse entre sí.

Arquitectura: la forma en la que se logra compartir recursos depende de la arquitectura lógica de la red. Los dos tipos de red según su arquitectura son punto a punto y cliente/servidor. (Groth, 2002)

Las computadoras en una red a veces se llaman clientes, y las computadoras y dispositivos que asignan recursos para una red se llaman servidores. (Castells, 2017)

2.2.2 Redes VLAN

Con la introducción de switches en un ambiente de LAN corporativo, surge la necesidad de administrar el flujo de trafico de manera más eficiente y de distintas maneras. Una de esas maneras fue la de permitir usuarios conectados en diferentes puertos de switch, participar en sus propias redes lógicamente separadas, pero físicamente conectadas, a otras estaciones en el mismo switch. Este concepto de "red dentro de una red" fue llamado tecnología de LAN virtual (VLAN). (Groth, 2002)

Las VLAN se implementan con el fin de lograr escalabilidad, seguridad y facilidad de administración de la red, las VLAN pueden adaptarse rápidamente a los cambios en los requisitos de la red y a la reubicación de las estaciones de trabajo y servidores (Duggan, 2014)

Las VLAN agrupan estaciones de trabajo pertenecientes a una o más LANs físicas en un dominio de broadcast. Las estaciones en una VLAN se comunican entre sí, como si estuvieran conectados en el mismo segmento físico. (Forouzan, 2007)

Una VLAN permite que varias redes funcionen virtualmente como una LAN. Uno de los elementos más beneficiosos de una VLAN es que elimina la latencia en la red, lo que ahorra recursos de red y aumenta la eficiencia de la red. Además, las VLAN se crean para proporcionar segmentación y ayudar en cuestiones como seguridad, administración de red y escalabilidad. Los patrones de tráfico también se pueden controlar fácilmente mediante el uso de VLAN.

Los beneficios clave de implementar VLAN incluyen:

- Permitir a los administradores de red aplicar seguridad adicional a las comunicaciones de red
- Facilitar la expansión y la reubicación de una red o un dispositivo de red
- Brinda flexibilidad porque los administradores pueden configurar en un ambiente centralizado mientras que los dispositivos pueden estar ubicados en diferentes ubicaciones geográficas

- Disminuir la latencia y la carga de tráfico en la red y los dispositivos de red, ofreciendo un mayor rendimiento

Las VLAN también tienen algunas desventajas y limitaciones, tal como se detalla a continuación:

- Alto riesgo de problemas de virus porque un sistema infectado puede diseminar un virus a través de toda la red lógica
- Limitaciones del equipo en redes muy grandes debido a que se podrían necesitar enrutadores adicionales para controlar la carga de trabajo
- Más eficaz para controlar la latencia que una WAN, pero menos eficiente que una LAN

2.2.3 Protocolos de seguridad

La seguridad de red está conformada por políticas y prácticas que permitan prevenir y controlar el acceso no autorizado, modificación, uso indebido o denegación de servicio de una red informática y recursos compartidos en la red. La seguridad de redes implica controlar autorización o denegación de acceso a usuarios a los datos de una red, la cual está bajo el control del administrador de red. Los usuarios se les asigna credenciales o información de autenticación que les permite acceder a programas o información dentro de su autoridad. (Gutierrez, 2013)

La seguridad de red se logra mediante el uso de criptografía, una ciencia basada en algebra abstracta. La criptografía es una palabra de origen griego que significa "escritura secreta". Sin embargo, se usa el termino para referirse a la ciencia y arte de transformar mensajes y convertirlos en seguros e inmunes a ataques. (Forouzan, 2007)

Los servicios de seguridad que son esperados dentro de una red, y que se logran mediante el uso de criptografía son los siguientes:

- **Confidencialidad de mensajes** significa existe privacidad entre el remitente y destinatario, es decir, que el mensaje trasmitido debe poderlo leer únicamente el destinatario. Para todos los demás, el mensaje debe ser ilegible.
- **Integridad de mensajes:** significa que los datos deben llegar a su destino exactamente como se enviaron. No deben existir cambios durante la transmisión, ni de manera accidental ni maliciosa.
- **Autenticación de mensajes:** es un servicio más allá de la integridad de mensajes. En la autenticación de mensajes el destinatario debe asegurarse de la identidad del remitente y que un impostor no haya sido quien envía el mensaje.

- **No repudio de mensaje:** significa que el remitente no debe poder negar que él ha enviado un mensaje que el haya enviado. La carga de la prueba recae en el destinatario.
- **Autenticación de entidad:** también llamado identificación de usuario, se produce cuando la entidad o el usuario es verificado antes de acceder a los recursos del sistema, por lo general por algún sistema verificación de credenciales. (Forouzan, 2007)

Los protocolos de seguridad de red definen la metodología y procesos que permiten proteger la información ante cualquier intento de acceso no autorizado a la red. Los protocolos de seguridad se aplican a todo tipo de información o datos, indistintamente del medio de red utilizado.

Los protocolos de seguridad de red generalmente implementan criptografía y técnicas de cifrado para proteger los datos, de modo que solo puedan descifrarse con un algoritmo especial, una clave lógica, una fórmula matemática y / o una combinación de todos ellos. Algunos de los protocolos de seguridad de red populares incluyen el Protocolo de transferencia segura de archivos (SFTP), el Protocolo seguro de transferencia de hipertexto (HTTPS) y la Capa de conexión segura (SSL). (Daimi, 2018)

2.2.4 Administración de redes

Se define a la administración de redes como el monitoreo, comprobación, configuración y resolución de problemas de componentes de la red, con el fin de cumplir con un conjunto de requerimientos definidos por una organización. Estos requerimientos incluyen la operación fluida y eficiente de la red que provee la calidad de servicio predefinida a los usuarios finales. Para cumplir con esta tarea, un sistema de administración utiliza hardware, software y personal humano.

Un sistema de administración de red tiene la función de administrar la configuración, los errores de red, el rendimiento de la red, la seguridad de la red y el registro de uso de los recursos de red. (Forouzan, 2007)

2.3 Protocolos de comunicación

Todo tipo de comunicación sigue un conjunto de reglas llamadas protocolos. Los protocolos se establecen específicamente de acuerdo con las características de la

conversación. La comunicación sobre redes sigue un protocolo similar a los usados en la comunicación entre seres humanos.
Los protocolos, son reglas utilizadas por cualquiera que se comunica con otro. En una conversación, las personas no piensan en los protocolos hasta que otra persona rompe alguno, pero muchos niveles de comportamiento son necesarios para una comunicación exitosa. Adicionalmente, si una persona intenta comunicarse en con otra, en un idioma que el receptor no entiende, los intentos de comunicación verbal fallarían.

Al igual que los seres humanos, los dispositivos de red también necesitan de protocolos para la comunicación. Los computadores no pueden aprender protocolos, por lo que los ingenieros de red desarrollaron reglas escritas de comunicación que deben seguirse de manera estricta para una comunicación entre hosts exitosa. Estas reglas se aplican en diferentes capas de sofisticación como en enlace físico usado, como los hosts escuchan, como hacer interrupciones, como terminar la comunicación, y muchos otros. Estas reglas, o protocolos, que trabajan en conjunto para asegurar la comunicación exitosa se agrupan en lo que se conoce como una suite de protocolos. (Dye, McDonald, & Rufi, 2008) .

Para que los dispositivos se puedan comunicar en una red, estos deben seguir diferentes protocolos, los cuales realizan distintas tareas para ser completados. Los protocolos definen lo siguiente:

- El formato del mensaje, como, por ejemplo, cuantos datos incluir en un segmento.
- La forma en la que disipativos intermedios comparten información sobre el camino al destinatario.
- El método para manejar mensajes de actualización entre disipativos intermedios.
- El proceso para iniciar y terminar comunicaciones entre hosts. (Dye, McDonald, & Rufi, 2008)

Personas de la industria de las telecomunicaciones se juntaron para estandarizar la forma en que las comunicaciones de red funcionan, definiendo protocolos comunes. Estos estándares son prácticas que cuentan con la aprobación de grupos representantes de la industria, y se siguen para asegurar la Inter operatividad entre fabricantes. La organización que estandariza los protocolos de red son el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) y el Grupo de trabajo de Ingeniería de Internet (IETF) Existen protocolos o suite de protocolos, que pueden ser específicos de un fabricante o de propiedad exclusiva. Algunos protocolos propietarios pueden ser

utilizados por distintas organizaciones con permiso del propietario. Otros, sólo se pueden implementar en equipos fabricados por el proveedor propietario. (Dye, McDonald, & Rufi, 2008)

Un ejemplo de la función de una suite de protocolos en redes de comunicación es la interacción entre un servidor web y un navegador web. Esta interacción utiliza un conjunto de protocolos y estándares en el proceso de intercambiar información entre ellos. Los diferentes protocolos trabajan en conjunto para asegurar que los mensajes son enviados y recibidos de manera exitosa. Por ejemplo, existen los siguientes protocolos:

- **Protocolo de transferencia de hipertexto (HTTP):** HTTP es un protocolo común que dicta la manera en la que un servidor web y un cliente interactúan. HTTP define el contenido y formato de los requerimientos y respuestas durante el cliente y el servidor, quienes deben tener HTTP como parte de su aplicación. A su vez, el protocolo HTTP depende de otros protocolos para determinar cómo los mensajes deben transportarse entre cliente y servidor.

- **Protocolo de transporte:** Protocolo de control de transmisión (TCP) es el protocolo de transporte que administra las conversaciones individuales entre servidores web y clientes. TCP divide los mensajes HTTP en segmentos, para ser enviados a los destinatarios. es también responsable de contralar el tamaño y frecuencia a la que los mensajes son intercambiados entre servidor y cliente.

- **Protocolo de internetwork:** El protocolo más común en un protocolo de internetwork es el protocolo de internet (IP) quien es responsable de tomar los segmentos TCP, encapsularlos en paquetes, asignar las direcciones apropiadas, y seleccionar el mejor camino a su destino.

- **Protocolos de acceso a redes:** Los protocolos de acceso a redes describen dos funciones primarias: la administración del enlace de datos y la transmisión física de datos en el medio de red. Los protocolos de administración de enlaces de datos toman los paquetes desde IP y los organiza para ser transmitidos sobre el medio de red. Los estándares y protocolos para el medio físico dictan como las señales son enviadas por el medio de red y como deben ser interpretados por los destinatarios. Los transmisores y receptores de las interfaces de red implementan los estándares apropiados para el medio que utilizan. (Dye, McDonald, & Rufi, 2008

Los protocolos que guían la comunicación de los procesos de comunicación no dependen de ninguna tecnología específica para funcionar. Los protocolos describen que debe hacerse para comunicarse, mas no como la tarea se debe completar. esto permite que los diferentes tipos de dispositivos, como teléfonos y computadores, pueden usar la misma infraestructura de red para comunicarse. Cada dispositivo tiene su propia tecnología, pero es capaz de interactuar con diferentes dispositivos a nivel de red. (Dye, McDonald, & Rufi, 2008)

2.4 Incidentes en los SAI

Un incidente es un evento que podría conducir a la pérdida o interrupción de las operaciones, servicios o funciones de una organización. La gestión de incidentes es un término que describe las actividades de una organización para identificar, analizar y corregir los peligros a fin de evitar que vuelva a ocurrir en el futuro. Si no se gestiona, un incidente puede derivar en una emergencia, una crisis o un desastre (Fernandez, 2015). La gestión de incidentes es, por lo tanto, el proceso de limitar la posible interrupción causada por un evento de este tipo, seguido de un retorno al negocio como de costumbre. Sin una gestión efectiva de incidentes, un incidente puede interrumpir las operaciones comerciales, la seguridad de la información, los sistemas de TI, los empleados, los clientes u otras funciones comerciales vitales.

Actualmente, un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) desempeña un papel importante debido al aumento del crimen en Internet, y es un ejemplo común de incidentes que enfrentan las empresas en países desarrollados de todo el mundo. Por ejemplo, si una organización descubre que un intruso ha obtenido acceso no autorizado a un sistema informático, el CSIRT analizará la situación, determinará la amplitud del compromiso y tomará medidas correctivas. La informática forense es una tarea incluida en este proceso (Fernandez, 2015). En la actualidad, más de la mitad de los intentos de piratería en el mundo en las Corporaciones Transnacionales (ETN) tienen lugar en América del Norte (57%). El 23% de los intentos tienen lugar en Europa. Tener un equipo integral de respuesta a incidentes de seguridad informática es esencial para proporcionar un entorno seguro para cualquier organización, y se está convirtiendo en una parte fundamental del diseño general de muchos equipos modernos de redes.

2.4.1 Broadcast

Broadcast es cualquier forma de comunicación en la cual un único emisor transmite mensajes a muchos receptores a la vez, siendo los ejemplos más familiares los sistemas de televisión y radio pública. Lo contrario de la transmisión es la comunicación punto a punto o de transmisión restringida, entre un solo transmisor y un único receptor, una

conversación telefónica, por ejemplo. Cuando se realiza una conexión múltiple de este tipo a través de un cable de red en lugar de inalámbrico, dicha comunicación se denomina a menudo MULTIPOINT, en contraposición a un punto a punto o UNICAST. (Fiat, 2013)

En las redes de transmisión, cada estación receptora recibe todas las señales enviadas por los transmisores. El enrutamiento de las señales se realiza de forma pasiva. Cada estación puede transmitir en una longitud de onda separada. El receptor recibe la señal deseada para ser colocada en la longitud de onda correcta. Las dos topologías más convencionales son la estrella y el bus. En ambos casos, cada estación transmite hacia el área, lo que hace que la multiplexación por división de longitud de onda de todas las ondas lo alcance.

Por otro lado, en la teoría de las redes de computadoras, las telecomunicaciones y la información, la radiodifusión es un método de transferir un mensaje a todos los destinatarios simultáneamente. La radiodifusión se puede realizar como una operación de alto nivel en un programa, por ejemplo, transmitiendo una interfaz de paso de mensajes, o puede ser una operación de red de bajo nivel, por ejemplo, la transmisión en Ethernet. (Cover, 2015)

La comunicación todo-en-todo es un método de comunicación de computadora en el que cada emisor transmite mensajes a todos los receptores dentro de un grupo. Esto contrasta con el método punto a punto en el que cada emisor se comunica con un receptor.

Funcionamiento.

Análisis de impacto: tráfico y frecuencia.

En una red, el tráfico de mensajes se envía a todos los nodos de la red o a una parte de la red (segmento LAN). Las transmisiones se emiten para la resolución de la dirección cuando no se conoce la ubicación de un usuario o servidor. Pueden ocurrir cuando los clientes y servidores se conectan y se identifican. A veces, los dispositivos de red anuncian continuamente su presencia. En todos los casos, la transmisión debe llegar a todas las estaciones posibles que podrían responder. Ver resolución de dirección, ARP, SLP y difusión. (Guagalango, 2016)

No obstante, en Ethernet, todas las comunicaciones se basan en la transmisión. Por defecto, cada host debe procesar todos los paquetes de difusión en la red. El tráfico que los paquetes de difusión ocupan se llama tráfico de difusión. El tráfico excesivo de difusión puede provocar una depreciación del rendimiento de la red o incluso provocar fallas de la red como una red lenta e intermitencia.

La red estará menos influenciada si el tráfico de transmisión es pequeño. Sin embargo, la influencia de los paquetes de difusión en la red no se puede eliminar. En Ethernet, hay muchos protocolos, como ARP, RARP, NETBEUI, SMB, DHCP, RIP, SAP e IPX, hasta cierto punto funcionan en el modo de transmisión. Normalmente, el tráfico de difusión no debe superar el 20% del tráfico total. Para evitar la tormenta de difusión y otras fallas de red, los administradores de red deben verificar regularmente el tráfico de difusión en la red. (Guagalango, 2016)

2.4.2 Tormentas de Broadcast

Cuando un switch recibe un broadcast, este repite el broadcast en cada puerto (excepto el puerto por el cual se recibe). En un ambiente con bucles de conexiones, los broadcasts son repetidos eternamente. El resultado de este fenómeno es una tormenta de broadcast, y rápidamente dejara la red inoperativa.

El síntoma principal de una tormenta de broadcast implica que cada a dispositivo se le hará imposible enviar una trama en la red debido al tráfico de red constante. La única forma de resolver un daño causado por una tormenta de broadcast es romper el ciclo, apagar y reiniciar los equipos de red solo comenzarían el ciclo nuevamente. Detectar el causante de la tormenta de red en una red puede ser muy difícil especialmente en equipos no administrables.

Las tormentas de broadcast constituyen un gran inconveniente para la escalabilidad de las redes, la alta difusión de trafico de manera simultánea, enviada normalmente por los protocolos de arranque y configuración, no solo disminuye la eficacia de los sistemas debido al aumento de tráfico en la red, debido al gran número de paquetes recibidos por cada equipo, se reduce también el rendimiento de los equipos de red y terminales. (Valera, Prados, Ramos, & Navarro, 2017)

2.5 Principales herramientas para administrar

2.5.1 Administración física.

La topología física se refiere a la estructura interconectada de una red de área local (LAN). El método empleado para conectar los dispositivos físicos en la red con los cables y el tipo de cableado utilizado, todos constituyen la topología física. Esto contrasta con la topología lógica, que describe el rendimiento de la señal de medios de una red. (Castells, 2017)

La topología de red lógica no siempre se asigna a una topología física específica. Por ejemplo, Ethernet de par trenzado es la topología de bus lógico que se asigna a un plan de topología de estrella física, mientras que el anillo de token de IBM es una topología

de anillo lógica que se implementa físicamente como una topología en estrella. (Fiat, 2013)

Los tipos de topologías físicas incluyen:

- Topología de bus lineal: un solo cable al que todos los nodos de la red están conectados directamente. El cable tiene terminadores en cada extremo para evitar la pérdida de señal.
- Topología de estrellas: una topología con un solo punto de acceso o un interruptor en el centro de la topología; todos los otros nodos están conectados directamente a este punto.
- Topología de árbol (estrella extendida): combinación de las topologías de estrella y de bus lineal. Esta topología tiene múltiples puntos de acceso conectados al bus lineal, mientras que los nodos están conectados a sus respectivos puntos de acceso. (Fiat, 2013)

2.5.2 Administración lógica.

Una topología lógica es un concepto de red que define la arquitectura del mecanismo de comunicación para todos los nodos en una red. Mediante el uso de equipos de red como enrutadores y conmutadores, la topología lógica de una red se puede mantener y reconfigurar dinámicamente. (Vietes, 2015)

Las topologías lógicas contrastan con las topologías físicas, que se refieren a las interconexiones físicas de todos los dispositivos en la red.

La topología lógica define cómo deben transferirse los datos. Compare esto con la topología física, que consiste en el diseño de los cables, los dispositivos de red y el cableado. (Vietes, 2015)

Dos de las topologías lógicas más comunes son:

Topología de bus: Ethernet usa la topología de bus lógico para transferir datos. Bajo una topología de bus, un nodo transmite los datos a toda la red. Todos los demás nodos de la red escuchan los datos y verifican si los datos están destinados a ellos.

Topología de anillo: en esta topología, solo un nodo puede transferir los datos en una red en un momento determinado. Este mecanismo se logra mediante token (el nodo que tiene token solo puede transmitir los datos en una red) y, por lo tanto, la colisión se puede evitar en una red

2.6 Principales aplicativos

2.6.1 Packet Tracer

Packet Tracer es un software de simulación desarrollado por Cisco, para el aprendizaje de varios conceptos de redes de computadoras (Javid, 2014).

Cisco Packet Tracer es un robusto programa de simulación de redes que permite a estudiantes a experimentar con los comportamientos de red y a formularse preguntas sobre todos los posibles escenarios de red. Como una parte integral de la experiencia de aprendizaje de la Academia de Networking, Packet Tracer provee la simulación, visualización, creación, evaluación y capacidad de colaboración, facilitando la enseñanza y aprendizaje de conceptos de tecnología complejos (Dangwal & Kumar, 2014)

Como cualquier simulación, Packet Tracer se basa en un modelo simplificado de dispositivos y protocolos de red. Provee un entorno simulado donde los procesos entre varios dispositivos de red, como routers. switches, puntos de acceso inalámbricos, computadores, enlaces y aplicaciones, son visibles con animaciones y descripciones de fácil comprensión (Nazumudeen & Mahendran, 2014)

Este software soporta varios protocolos de red, soporte para múltiples plataformas, espacios de trabajo lógicos y físicos, en tiempo real y en modo de simulación e Interfaz de Línea de Comandos (CLI) (Janitor & Jakab, 2010)

2.6.2 Wireshark

Wireshark es un analizador de protocolo de red de fuente abierta y gratuita que permite a los usuarios navegar de manera interactiva el tráfico de datos en una red informática. El proyecto de desarrollo se inició con el nombre de Ethereal, pero cambió su nombre a Wireshark en 2006. (Orebaubg, 2016)

Muchos desarrolladores de redes de todo el mundo han contribuido a este proyecto con análisis de red, solución de problemas, desarrollo de software y protocolos de comunicación. Wireshark se utiliza en muchas instituciones educativas y otros sectores industriales.

Wireshark es un analizador de red o protocolo (también conocido como sniffer de red) disponible de forma gratuita en el sitio web de Wireshark. Se utiliza para analizar la estructura de diferentes protocolos de red y tiene la capacidad de demostrar la encapsulación. El analizador opera en los sistemas operativos Unix, Linux y Microsoft Windows, y emplea el juego de herramientas widget WK + y pcap para la captura de

paquetes. Wireshark y otras versiones de software libre basadas en terminales como Tshark se lanzan bajo la Licencia Pública General de GNU. (Orebaubg, 2016)

Wireshark comparte muchas características con tcpdump. La diferencia es que es compatible con una interfaz gráfica de usuario (GUI) y tiene características de filtrado de información. Además, Wireshark permite al usuario ver todo el tráfico que pasa por la red.

Las características de Wireshark incluyen:

- Los datos se analizan desde el cable a través de la conexión de red o desde archivos de datos que ya han capturado paquetes de datos.
- Admite la lectura y el análisis de datos en vivo para una amplia gama de redes (incluyendo Ethernet, IEEE 802.11, protocolo punto a punto (PPP) y loopback).
- Con la ayuda de GUI u otras versiones, los usuarios pueden navegar por las redes de datos capturados.
- Para editar y convertir de forma programática los archivos capturados a la aplicación editcap, los usuarios pueden usar los modificadores de línea de comando.
- Los filtros de visualización se utilizan para filtrar y organizar la visualización de datos.
- Los nuevos protocolos se pueden analizar creando complementos.
- El tráfico capturado también puede rastrear llamadas de voz por Internet (VoIP) a través de la red.
- Al usar Linux, también es posible capturar el tráfico USB sin formato.

Wireshark intentará capturar paquetes de red e intentará mostrar los datos de paquetes lo más detallados posible. Básicamente es una herramienta para ver los bits y bytes que fluyen a través de una red en forma humana legible. Sin él, entender un intercambio de comunicación de red sería prácticamente imposible. Como sabrá, el protocolo de red se divide en 7 capas. La parte que trata WireShark es la capa 2 hasta 7. La mayoría de los protocolos bien conocidos pueden decodificarse con WireShark (Chapelli, 2016)

Propósitos de Wireshark:

- Es utilizado por los administradores de red para analizar y solventar problemas de red
- Se usa para detectar errores de seguridad en la red.
- Permite a los desarrolladores depurar implementaciones de protocolos
- Se usa como medio de aprendizaje y visualización de protocolos y tráfico de red.

2.6.3 PRTG Network Monitor

PRTG es un software de monitoreo de red que puede ejecutarse en una máquina Windows dentro de la red y puede recopilar estadísticas de los hosts designados, como enrutadores, servidores, conmutadores y otros dispositivos o aplicaciones importantes (Llerena, 2016). El beneficio del software de administración de red es que puede detectar problemas antes de que se conviertan en fallas y al alertar de estos problemas a un administrador de la red, se pueden evitar muchas interrupciones costosas del servicio. Además, RPTG es gratuito para pequeñas empresas que rastrean menos de 25 dispositivos.

Muchas redes de pequeñas empresas no instalan aplicaciones de monitoreo de red, ya que a veces se consideran complicadas, innecesarias y/o costosas. Sin embargo, la supervisión de la red puede evitar la pérdida costosa de servicios, como el correo electrónico corporativo o el fallo del sitio web de comercio electrónico de una empresa. Además, la supervisión de la red ya no es costosa, compleja y complicada de instalar y configurar. En particular, PRTG es fácil de implementar y operar, de ahí su popularidad en entornos SMB (Aleaga, 2016).

Lo que hace que PRTG sea particularmente fácil de usar es que descubrirá automáticamente los dispositivos en la red y los configurará automáticamente. PRTG luego sondeará estos dispositivos a través de SNMP, WMI, detección de paquetes, flujo de red, jflow, sflow o IPFIX. La interfaz web fácil de usar de PRTG y la configuración de apuntar y hacer clic lo hacen adecuado para la resolución de problemas en tiempo real o para compartir datos con personal no técnico a través de gráficos en línea e informes personalizados.

La forma en que funciona PRTG es mediante el uso de sensores, que son entidades de monitoreo individuales configuradas para un propósito específico. Por ejemplo, hay sensores de aplicación HTTP, SMTP / POP3 (correo electrónico), así como sensores de hardware específicos para conmutadores, enrutadores y servidores. PRTG tiene más de 200 tipos de sensores preconfigurados que sondean las estadísticas de las entidades monitoreadas, como los tiempos de respuesta, el uso del procesador / memoria / ancho de banda (Chauchan, 2017).

El software de monitoreo de red es una herramienta administrativa importante cuando se trata de operar y mantener una red, independientemente del tamaño, ya que a menudo hay pocos síntomas o advertencias antes de una interrupción de la red. PRTG puede rastrear las anomalías del sistema y proporcionar alertas tempranas a eventos

de red potencialmente calamitosos, lo que le da al administrador el tiempo suficiente para tomar medidas correctivas.

Una solución de monitoreo fácil de usar para redes basadas en Windows PRTG Network Monitor se ejecuta en todos los sistemas operativos actuales y supervisa los sistemas Windows, Linux, UNIX y MacOS. PRTG se instala y configura en minutos; Viene con su propia base de datos y servidor web integrado, y un descubrimiento automático de la red. PRTG es por consiguiente optimizado para un fácil uso (Chauchan, 2017).

Un software para monitorear toda su red, dispositivos y aplicaciones, tráfico y disponibilidad PRTG Network Monitor admite SNMP, WMI, monitoreo de flujo, así como detección de paquetes, y ofrece más Más de 110 sensores especiales para monitoreo de VoIP, monitoreo de sitios web, monitoreo de correo electrónico, monitoreo de aplicaciones, Base de datos de monitoreo, monitoreo de entornos virtuales, y muchos otros.

Monitoreo de diferentes sitios desde una instalación central. PRTG Network Monitor viene con las llamadas 'sondas remotas' que se pueden instalar en distribuidos localmente Redes y luego envíe los datos de monitoreo cifrados SSL a través de Internet (no se requiere VPN) al servidor central de la instalación central. Una solución integral de monitoreo de red que se ajusta a su presupuesto PRTG Network Monitor ofrece una funcionalidad de monitoreo integral y se amplía hasta redes más grandes de Algunos miles de dispositivos e incluso más por el precio de un software de monitoreo de nivel de entrada (Chauchan, 2017).

CAPÍTULO 3

3 ESCENARIO DE ESTUDIO

3.1. Descripción del escenario

3.1.1 Caso real

El proveedor de servicios de acceso a internet SAI Celeritel Solutions S.A. ubicado en el cantón Playas, tiene conexión con sus proveedores externos de internet, estos se conectan al nodo o router principal mediante enlaces radioeléctricos punto a punto. De manera física, el nodo principal establece las rutas hacia los nodos secundarios, también mediante enlaces radioeléctricos punto a punto, el router principal está conectado por medio de un switch a varios nodos distribuidos en diferentes zonas geográficas, las rutas hacia los nodos secundarios también se encuentran establecidas mediante enlaces radioeléctricos punto a punto. En cada nodo secundario existen varios sistemas radio eléctricos punto-multipunto para proveer conectividad con el usuario final.

El router principal se encuentra dentro de la misma LAN que interconecta 6 nodos ubicados en distintos puntos geográficos dentro del cantón Playas, con el fin de llegar a cada uno de sus clientes, y brindarles conectividad a internet. Dentro de esta red de nodos, y bajo el mismo dominio de broadcast, se encuentran los equipos clientes del nodo 1 ubicados dentro del mismo edificio, donde se encuentra el rack con el router principal.

Se pueden destacar las siguientes características del proveedor de SAI Celeritel Solutions S.A:

Ancho de banda proveedores:

- Proveedor 1: 300 Mbps
- Proveedor 2: 70 Mbps

Clientes por nodo:

- Nodo 1: 25
- Nodo 2: 12
- Nodo 3: 32
- Nodo 4: 9
- Nodo 5: 36

- Nodo 6: 17

Distancia a los nodos:

Medida desde el Nodo 1 que es el principal

- Nodo 2: 5 Km
- Nodo 3: 9 Km
- Nodo 4: 12 Km
- Nodo 5: 19 Km
- Nodo 6: 0,4 Km

Direccionamiento IP:

- Nodo 1: 192.168.240.0
- Nodo 2: 192.168.240.0
- Nodo 3: 192.168.30.0 / 192.168.60.0
- Nodo 4: 192.168.90.0
- Nodo 5: 192.168.130.0
- Nodo 6: 192.168.120.0

Equipos:

- Router principal y de nodos: Zyxel USG-110
- Switch de Distribución por nodo y por red IP: Zyxel GS1900-24
- Enlaces radioeléctricos Punto a Punto: Cambium Networks Force-200 5GHz
- Punto de acceso: Cambium Networks ePMP-2000 5GHz, antena sectorial inteligente 120 grados
- Punto Cliente: Cambium Networks Force-180 5GHz

Conexión entre nodos al router principal

El router principal está conectado por medio de un switch Marca Zyxel modelo GS1900-24E y por medio de radio antenas Cambium Networks ePMP Force 200 5 GHz a varios routers también marca Zyxel modelo ZyWALL USG110 distribuidos en diferentes zonas geográficas, cada uno de estos routers son considerados nodos, de los cuales existen 6 en total, uno de los nodos está conectado directamente el switch sin el uso de radio enlaces, el diagrama de conexión entre nodos y clientes, se puede apreciar en la figura 3.1:

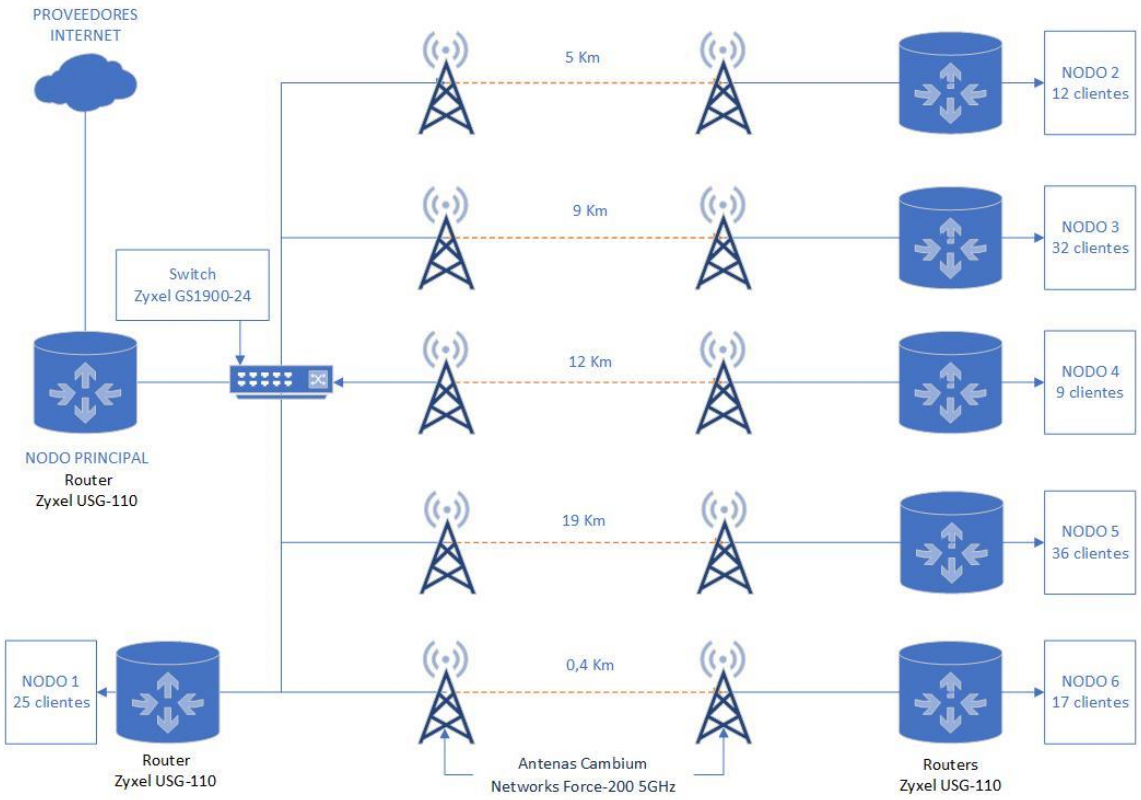


Figura 3.1 Diagrama de conexión a nodos – escenario actual

Al encontrarse todos los nodos conectados mediante un switch, la conexión entre el router principal, los equipos cliente del Nodo 1 y los routers en cada nodo se encuentran dentro de la misma LAN y, por lo tanto, el mismo dominio de broadcast.

Se debe tomar en cuenta que las antenas que conectan a cada uno de los nodos pueden considerarse hosts de la red dentro del dominio de broadcast de la red de nodos, debido a que, al ser administrables dentro de la red, poseen también direcciones MAC e IP; y, al igual que cualquier host dentro de una red, también generan tráfico de broadcast en la red.

En la figura 3.2 se puede apreciar la estructura física donde se encuentra el proveedor Celeritel Solutions S.A, donde también se encuentra el rack principal y los clientes del nodo 1 o nodo principal.

Figura 3.2 Ubicación física de proveedor de SAI - Nodo Principal

En la figura 3.3 se puede apreciar la torre con las radioantenas Cambium Networks ePMP Force 200 5 GHz para los enlaces punto a punto con los demás nodos.

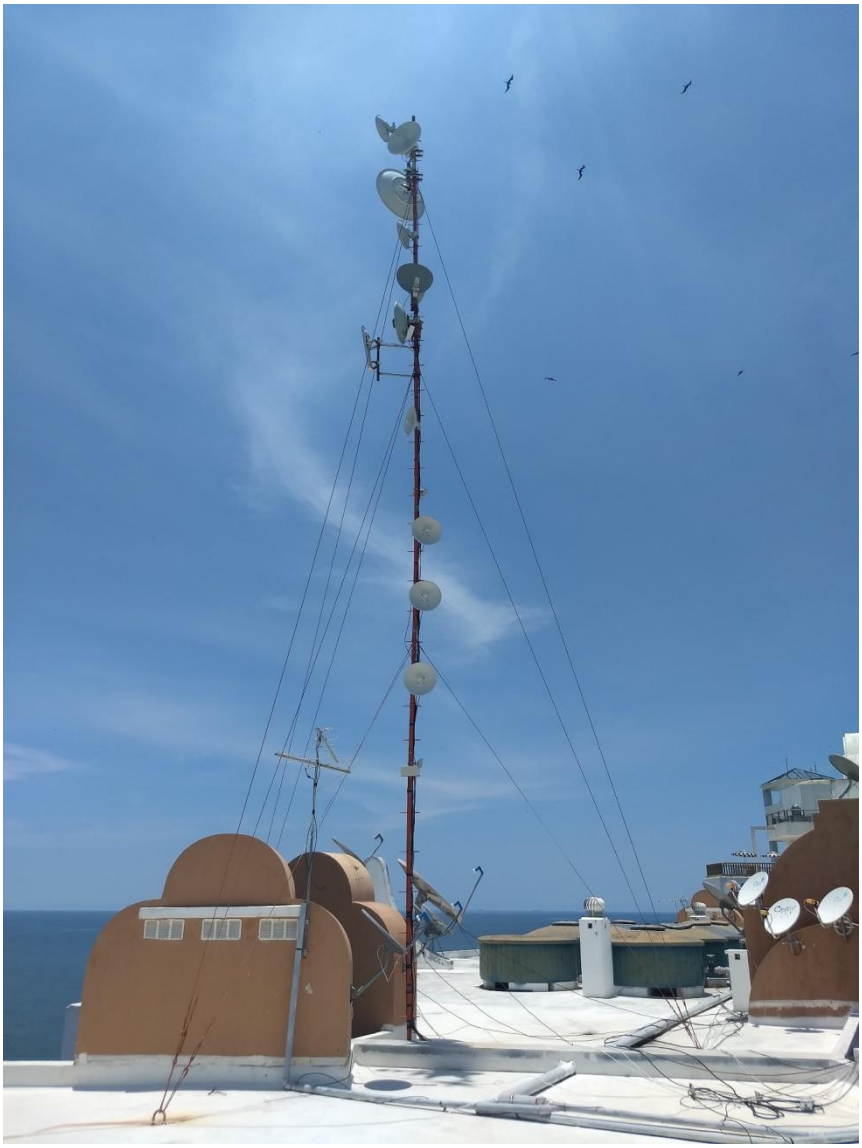


Figura 3.3 Torres con radioantenas Cambium Networks ePMP Force 200 5 GHz

Nodos conexión de usuario final a nodos

Los nodos tienen conexión directa al usuario final mediante el uso de switches, formando parte de la misma LAN y dominio de broadcast. Cada nodo tiene una infraestructura de

red interna diferente de acuerdo con el número de clientes en cada nodo y los medios de conexión empleados para llegar al usuario final. Un ejemplo de nodo se puede apreciar en la figura 3.4.

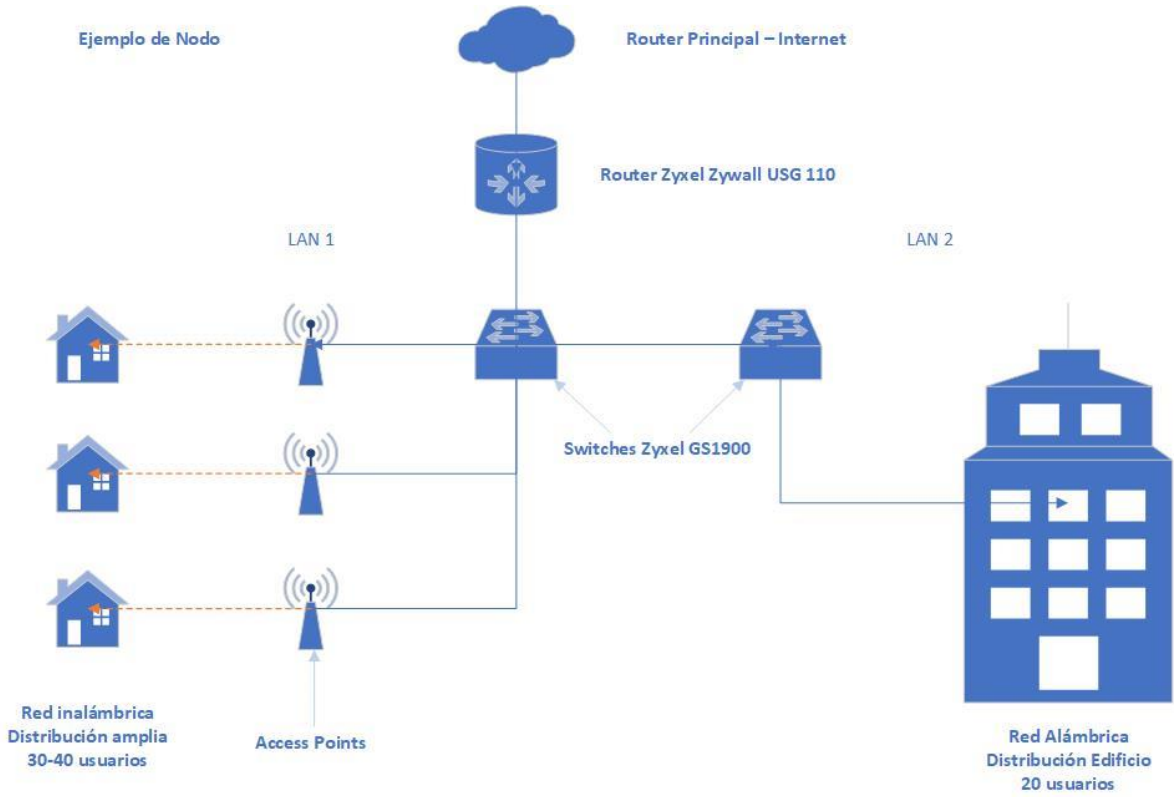


Figura 3.4 Ejemplo de nodo – conexión a clientes

3.1.2 Propuesta

Se propone verificar cual es el beneficio de limitar los dominios de broadcast en una red de un proveedor de servicios de acceso a internet (SAI), en el cual la conexión a nodos es compartida con ciertos clientes del proveedor ubicados en el mismo punto donde se encuentra el router principal. Compartir esta red con clientes sin la debida segmentación de los dominios de broadcast, podría presentar un gran riesgo a la red del proveedor, incluso afectando los demás nodos ubicados en los diferentes puntos geográficos.

Al tratarse de un proveedor de Servicio de Acceso a Internet, el cual tiene un alto potencial de expansión debido al aumento en el número de clientes a medida que transcurre el tiempo. El uso de VLANs es una solución viable para optimizar de manera significativa los recursos de red, los cuales, a medida que aumenta el número de nodos y clientes, a futuro, podrían presentar problemas de congestionamiento y afectación de la calidad de servicios al usuario final.

Actualmente la conexión entre nodos, y las conexiones internas dentro de cada nodo, funcionan bajo la misma LAN, y, por lo tanto, bajo el mismo dominio de broadcast. Por

lo que se realizará una medición de tráfico de red de Broadcast dentro de la red actual con el fin de tener una idea de cómo fluye el tráfico actualmente entre usuarios finales y su conexión a los nodos.

Una vez que se obtengan los resultados de la medición de la red sin VLANs, se realizará la implementación de VLANs dentro de las redes de nodos y se realizarán mediciones nuevamente, con el fin de comprobar los aspectos en los cuales se obtienen beneficios al hacer uso de VLANs en la red.

3.2 Descripción general del proceso de medición

Se realizará una medición mediante analizadores de red y sniffers por el tráfico que circula por la red, una medición sin VLANs y otra una vez creadas las VLANs.

3.2.1 Implementación y uso

Se utilizará el software de monitoreo PRTG Network Monitor y mediante Wireshark, se determinarán cuantos paquetes y bytes de broadcast son transmitidos en la red tanto sin VLANs y como con VLANs. El uso de VLANs debería reducir el número de paquetes de broadcast que se trasmiten en cada enlace y optimizar la conexión.

3.2.2 Equipos de medición

Para realizar la medición por Wireshark se hará uso de un computador portátil conectado a uno de los puntos de red cliente donde se implementará una de las VLANs.

La medición del software de monitoreo PRTG se encuentra actualmente implementado por el proveedor de SAI en uno de los servidores conectados a su red, donde se ejecutarán los análisis de tráfico antes y después de la implementación de las VLAN en la red.

CAPÍTULO 4

4 INFRAESTRUCTURA SIMULADA Y PROCEDIMIENTO DE MEDICIÓN

4.1 Proceso de simulación

Para el escenario de simulación con VLANs se usará, como punto de partida, el mismo esquema de red de la simulación sin VLANs. Para configurar VLANs es importante tener una planificación preliminar de las redes que se piensan utilizar, ya que al segmentar las redes y dominios de broadcast se hará uso de más subredes que si no se usan las VLANs. Es preferible que las redes de las VLANs tengan un orden fácil de identificar, para evitar confusiones al momento de gestionar la red.

En resumen, para implementar VLANs en la red dentro del packet tracer se seguirán los siguientes pasos:

1. Se empezará tomando como base la misma red en el escenario simulado sin VLAN.
2. Se definirán VLANs ID y redes para cada dominio de broadcast propuestos. Para el escenario actual se definirá una VLAN para cada red conectada a cada uno de los Access Points (AP); adicionalmente en el caso del edificio, una VLAN para cada piso del edificio.
3. Se llenará las bases de datos de VLAN de cada equipo de la red de acuerdo lo planteado en el punto anterior.
4. Se definirán los enlaces tipo trunk que en este caso son dos, el enlace de conexión entre switches, y el enlace de conexión al router.
5. En el router se configurará el enlace tipo trunk, base de datos de VLANs, subinterfaces de red IP y servicio de DHCP para cada VLAN.
6. Para efecto de la simulación se configurará cada router de cada nodo con protocolo de enrutamiento RIP para conexión a otros routers y al servidor DNS y HTTP.
7. Se revisará que cada equipo tipo cliente se encuentre dentro de su VLAN correspondiente, es decir, que el equipo obtenga dirección IP de la red de su VLAN, y que tenga conectividad con el servidor web simulado.

En la figura 4.1 se tiene el esquema de simulación del caso real en Packet Tracer, y en la figura 4.2 se presenta una configuración propuesta de VLANs sobre la misma red, en ambos casos, los colores denotan la cobertura de los dominios de broadcast.

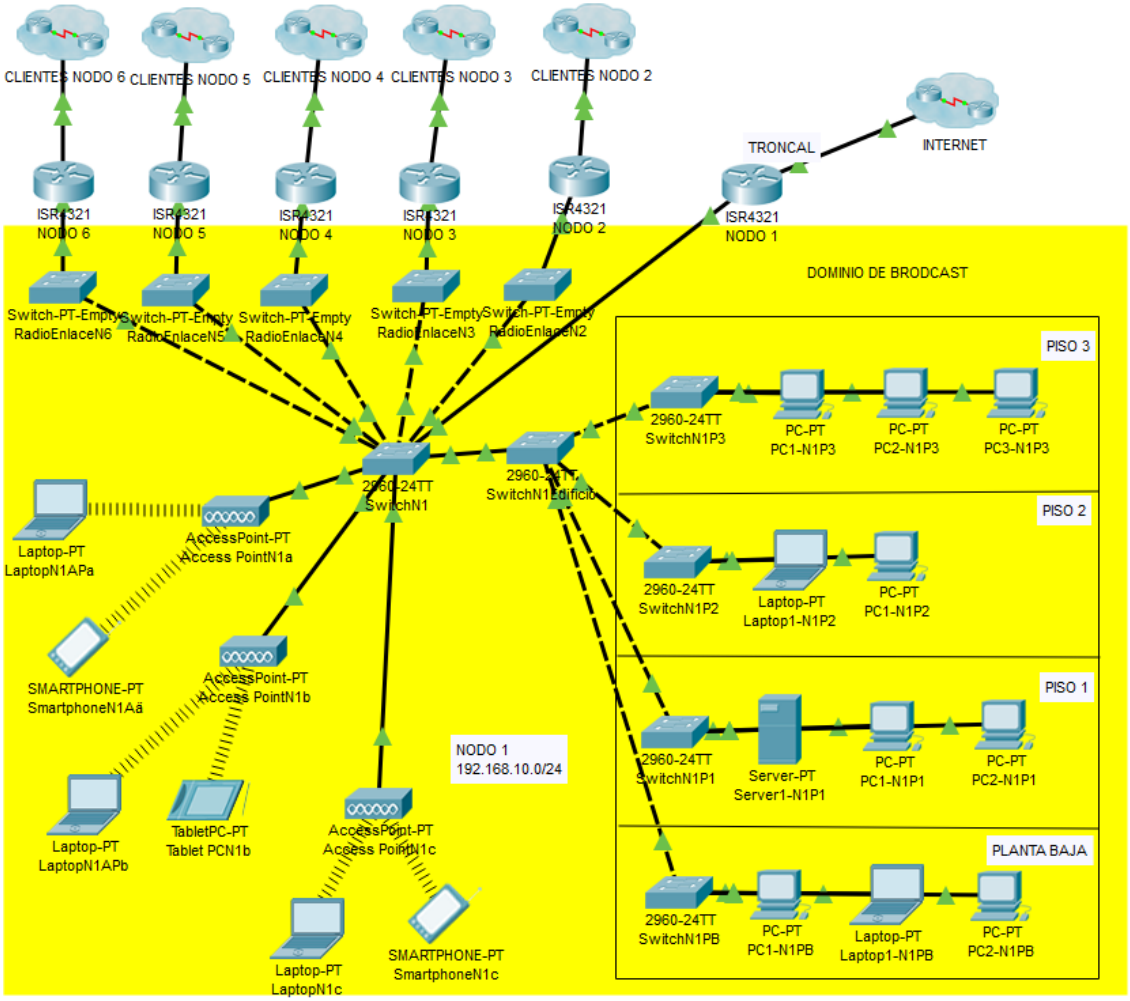


Figura 4.1 Esquema de escenario en Packet Tracer - sin VLANs

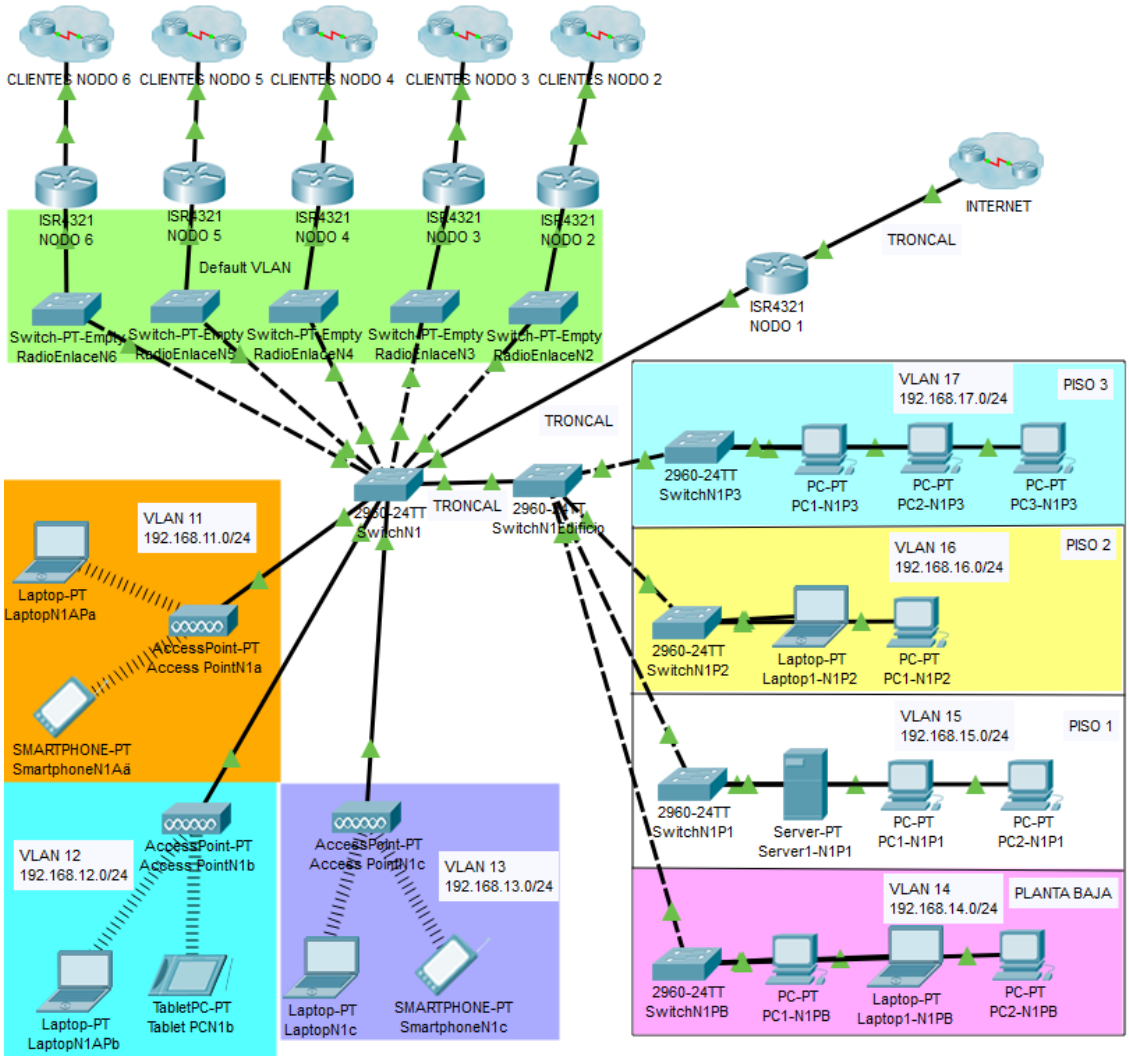


Figura 4.2 Propuesta de configuración de VLAN para simulación

En este diagrama se tienen dos switches principales en los que se configurarán las VLAN, los switches SwitchN1 y SwitchN1Edificio. Como la red usada en este nodo era la 192.168.10.0/24 se asignan las siguientes redes a las VLANs de acuerdo con lo indicado en la tabla 1:

SWITCH	INTERFAZ	VLAN ID	RED
SwitchN1	FastEthernet 0/1	11	192.168.11.0/24
SwitchN1	FastEthernet 0/2	12	192.168.12.0/24
SwitchN1	FastEthernet 0/3	13	192.168.13.0/24
SwitchN1Edificio	FastEthernet 0/1	14	192.168.14.0/24
SwitchN1Edificio	FastEthernet 0/2	15	192.168.15.0/24
SwitchN1Edificio	FastEthernet 0/3	16	192.168.16.0/24
SwitchN1Edificio	FastEthernet 0/4	17	192.168.17.0/24

Tabla 1 Asignación de VLANs a interfaces de Switches

Adicional a las VLAN mencionada, se debe realizar la configuración de los enlaces troncales por los que transmitirán las tramas de varias VLANs por sola una interfaz, en vista que los switches usados en la simulación, poseen dos interfaces Gigabit Ethernet (los dos puertos aislados ubicados en el área derecha del gráfico del switch), estas serán usadas para los enlaces troncales (Trunks).

Los enlaces troncales serán configurados como se detalla en la tabla 2:

DISPOSITIVO	INTERFAZ	VLANs permitidas	OBSERVACION
SwitchN1	GigabitEthernet 0/1	11 a 17	Conectado a Router NODO 1
SwitchN1	GigabitEthernet 0/2	14 a 17	Conectado a SwitchN1Edificio
SwitchN1Edificio	GigabitEthernet 0/1	14 a 17	Conectado a SwitchN1
Router NODO 1	GigabitEthernet 0/0/0	11 a 17	Conectado a SwitchN1

Tabla 2 Asignación de enlaces tipo troncal

En la conexión entre switches sólo se trasmitirán las VLAN 14 a las 17 debido a que son las únicas VLAN que están configuradas en el SwitchN1Edificio, para optimizar el tráfico de red no es necesario que por este enlace troncal se transmitan las VLAN 11 a la 13, sin embardo, en la conexión entre SwitchN1 y el Router Nodo1, si deben pasar todas las VLANs.

SwitchN1

Ya teniendo planificado como se configurarán las VLANs se procede a realizar la configuración en los switches, en el Switch N1 se deben configurar todas las VLANs que se van a utilizar en el nodo debido a que es el Switch que se conecta al router del nodo por medio del enlace troncal, por lo que la base de datos en el switch se muestra en la figura 4.3:

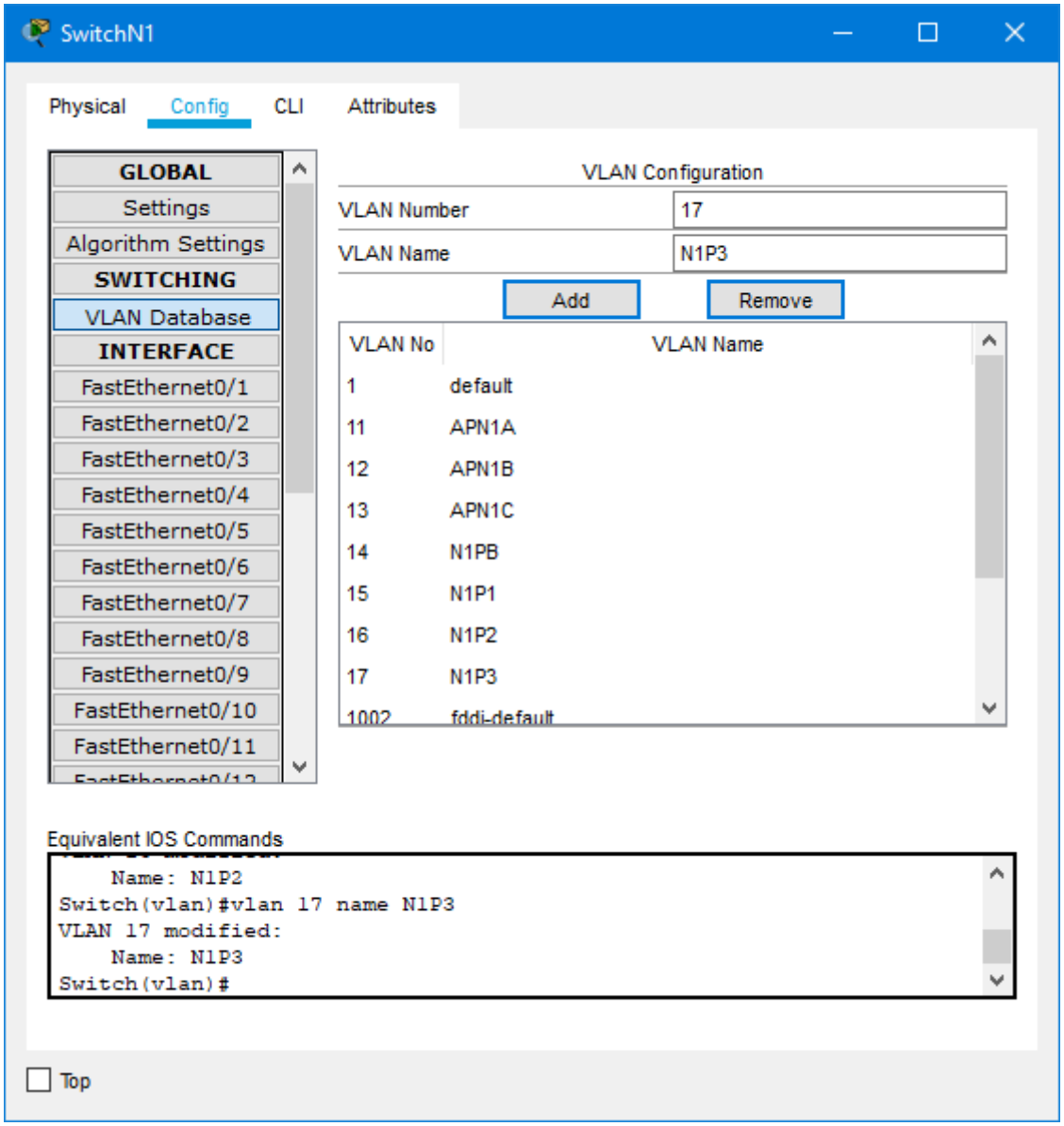


Figura 4.3 Base de datos SwitchN1

Adicionalmente, para cada interfaz se debe configurar su respectiva VLAN, por ejemplo, de acuerdo con la matriz de asignación de VLANs, la interfaz FastEthernet 0/1 tiene asignada la VLAN 11, quedando la configuración en el switch, como se presenta en la figura 4.4:

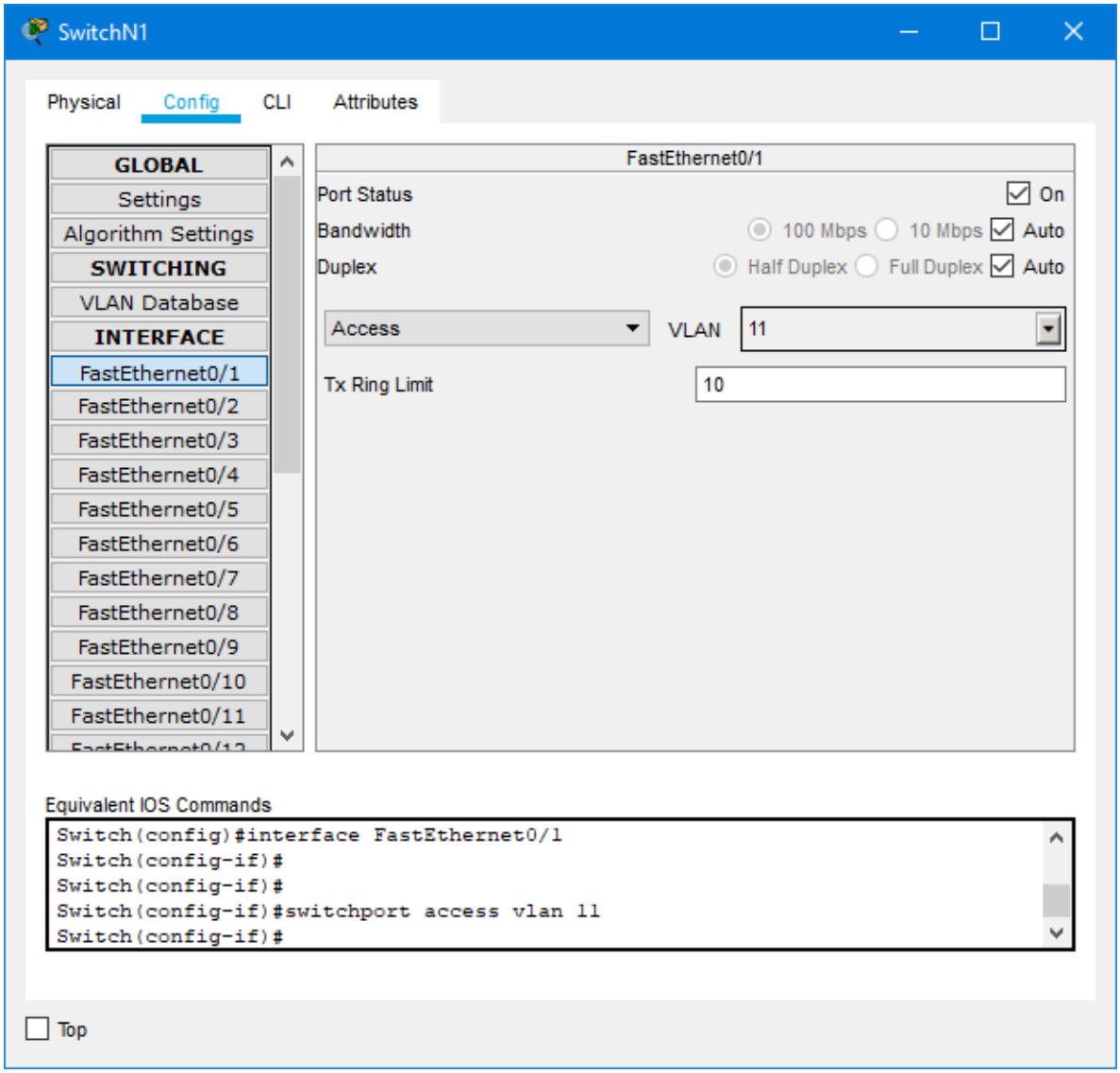


Figura 4.4 Asignación de VLAN a interfaz FastEthernet 0/1 de SwitchN1

Asi mismo se deben configurar las interfaces FastEthernet 0/2 y 0/3 de acuerdo a lo planificado.

Para los enlaces troncales se configurarán tambien de acuerdo a la matriz de asignaciones, por lo que la interfaz que conecta al router debe permitir todas las VLAN, como se muestra en la ventana de la figura 4.5:

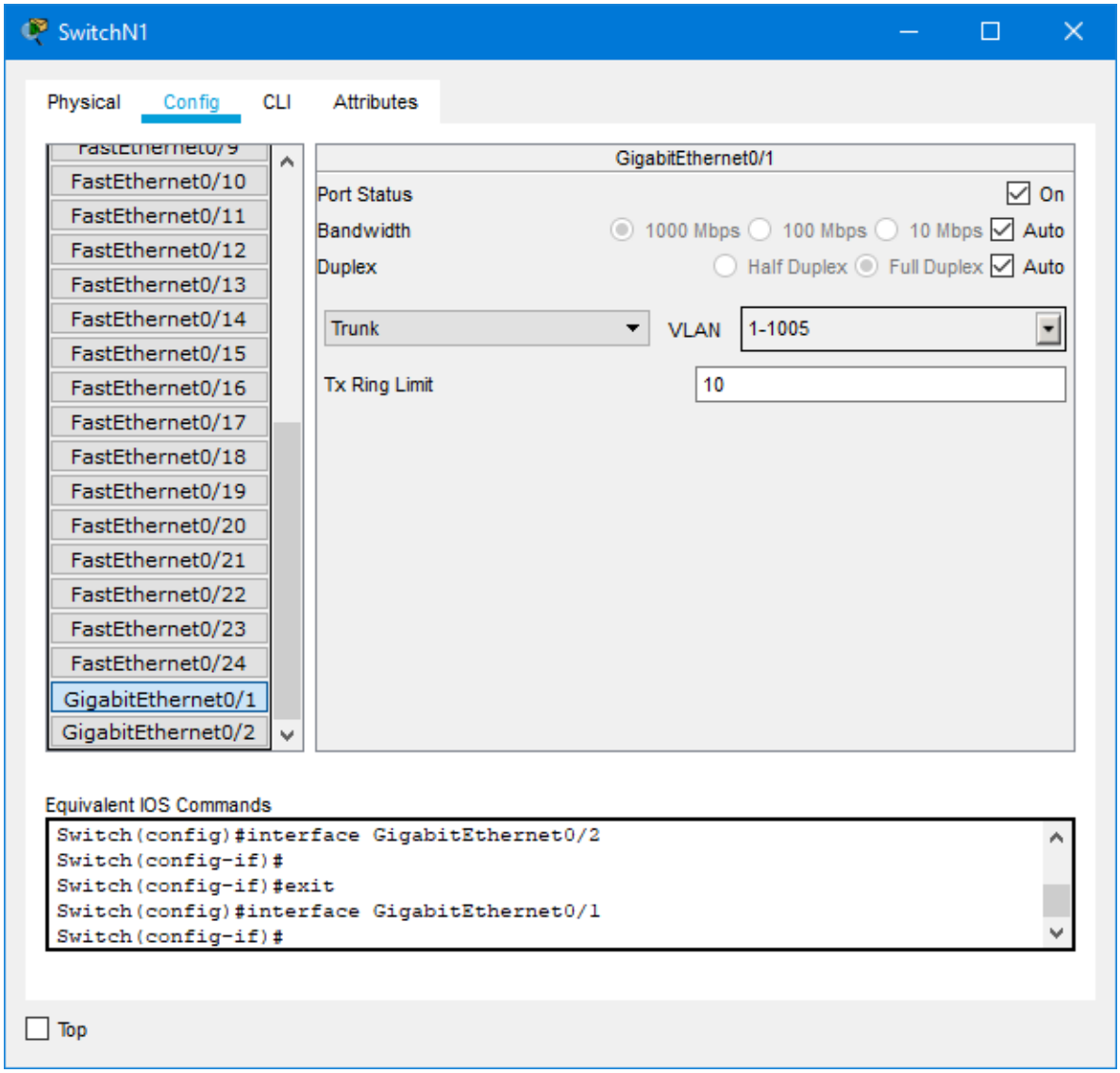


Figura 4.5 Asignación de enlace tipo troncal en interfaz GigabitEthernet 0/1 en SwitchN1 que conecta a Router Nodo 1

Y la interfaz GigabitEthernet 0/2 que conecta al SwitchN1Edificio, se omitiran las VLAN 11 hasta la 13, puesto que, como fue mencionado, no es necesario que por ese enlace se transmita informacion de dichas VLANs. En este caso se esta permitiendo las demas VLAN que tiene por defecto el Switch, por lo que solo se omitiran las VLAN 11 a la 13, quedando la configuracion como se muestra en la figura 4.6:

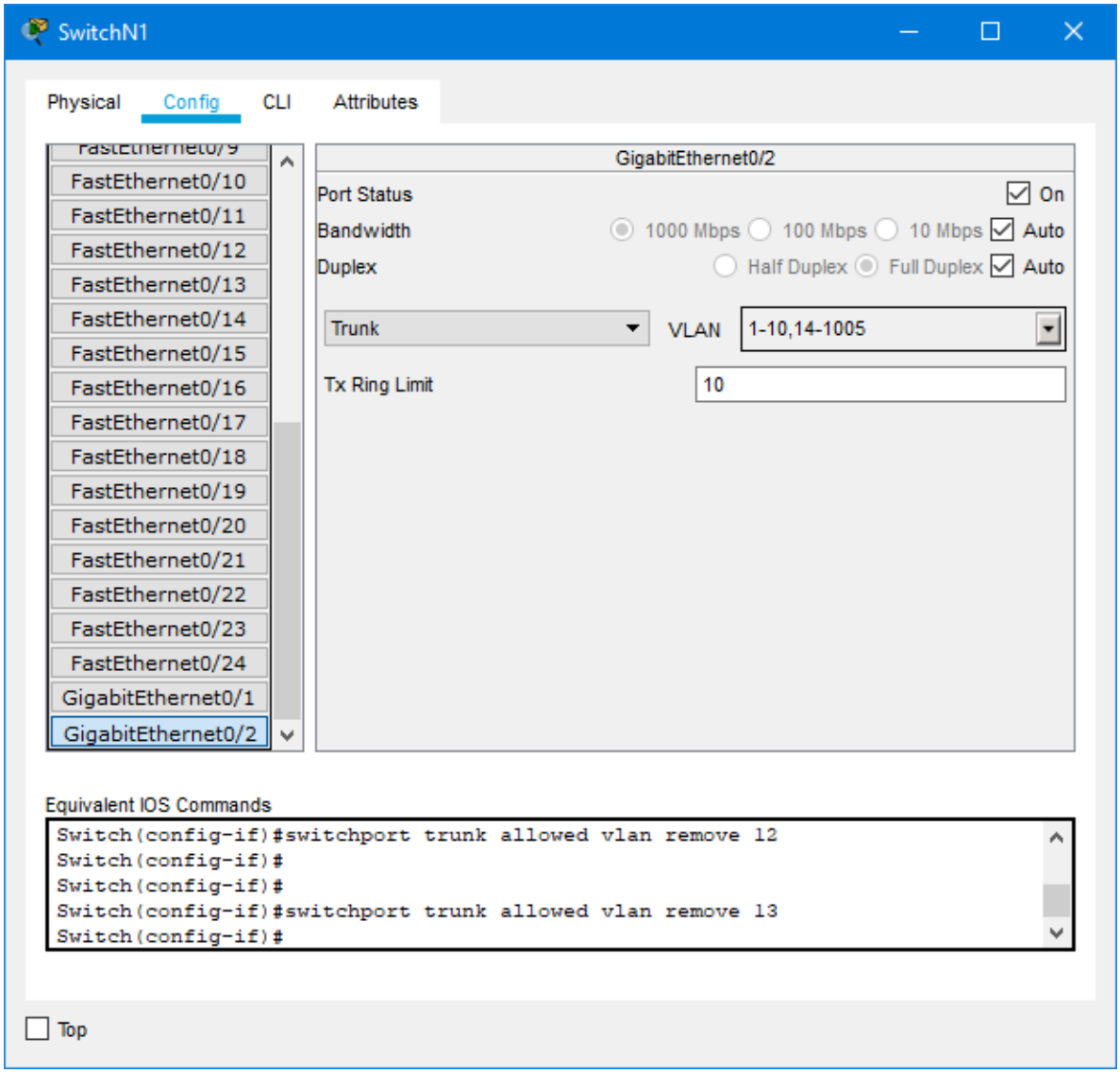


Figura 4.6 Asignación de enlace tipo troncal en interfaz GigabitEthernet 0/2 en SwitchN1 que conecta a SwitchN1Edificio

SwitchN1 Edificio

El Switch N1 Edificio también se configurará de acuerdo con la planificación de VLAN detallada en la matriz, y la configuración sería más sencilla que el Switch N1, se deben configurar todas las VLANs conectadas las interfaces de dicho switch, quedando la configuración como lo presentado en la figura 4.7:

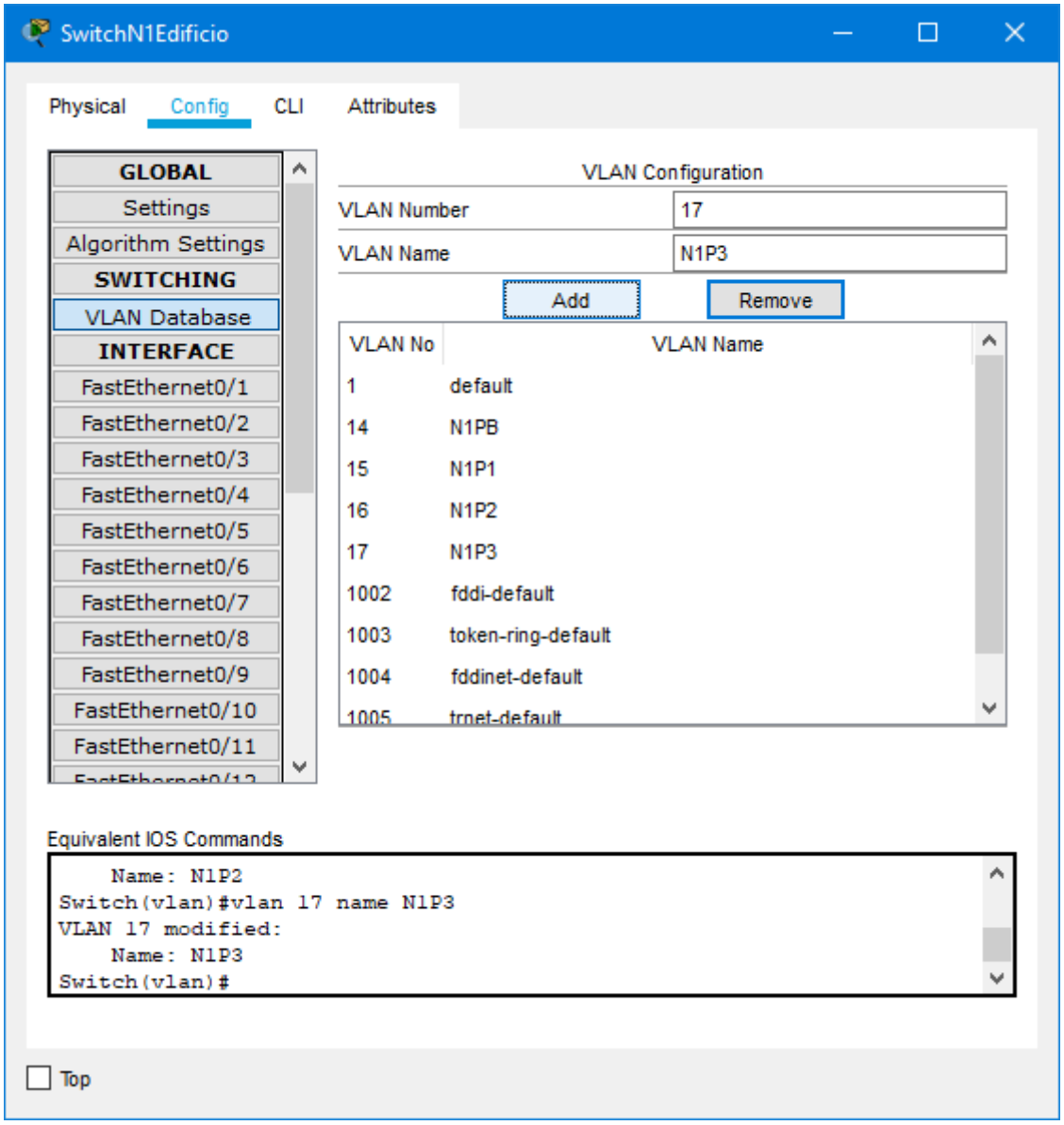


Figura 4.7 Base de datos de VLAN de SwitchN1Edificio

También se deben configurar las interfaces de acuerdo con cada VLAN, con los mismos principios del Switch N1, por ejemplo, la configuración de la interfaz FastEthernet 0/1 se muestra en la figura 4.8:

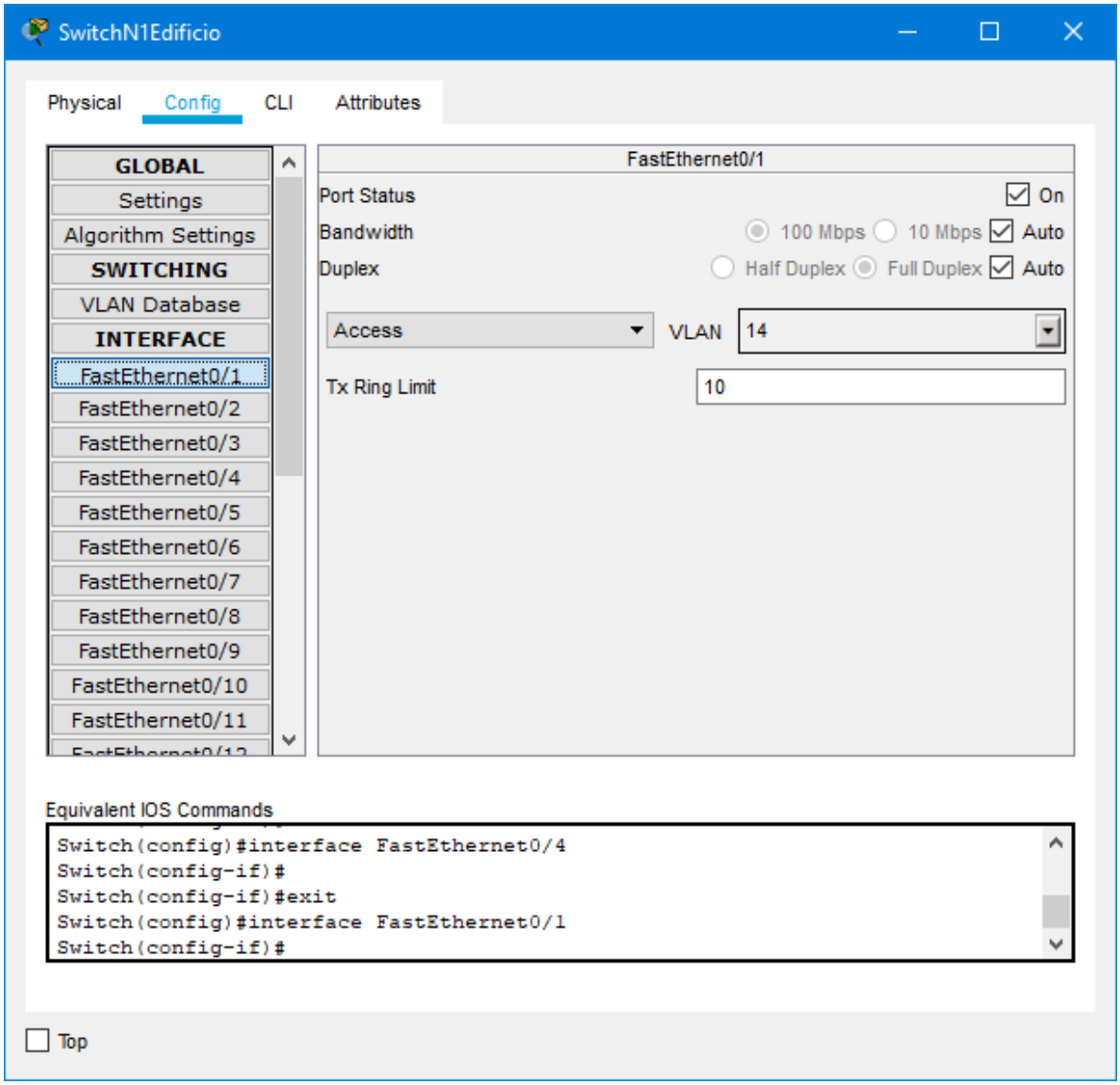


Figura 4.8 Asignación de VLAN a interfaz FastEthernet 0/1 de SwitchN1Edificio

Al igual que en el Switch N1 se deberán configurar del mismo modo las interfaces con sus VLAN correspondientes en este Switch de acuerdo con la matriz de asignación de VLANs.

La interfaz GigabitEthernet debe ser configurada en modo troncal con las VLANs 14 hasta la VLAN 17, que en este caso serian todas las que tiene configuradas este switch, como en la figura 4.9:

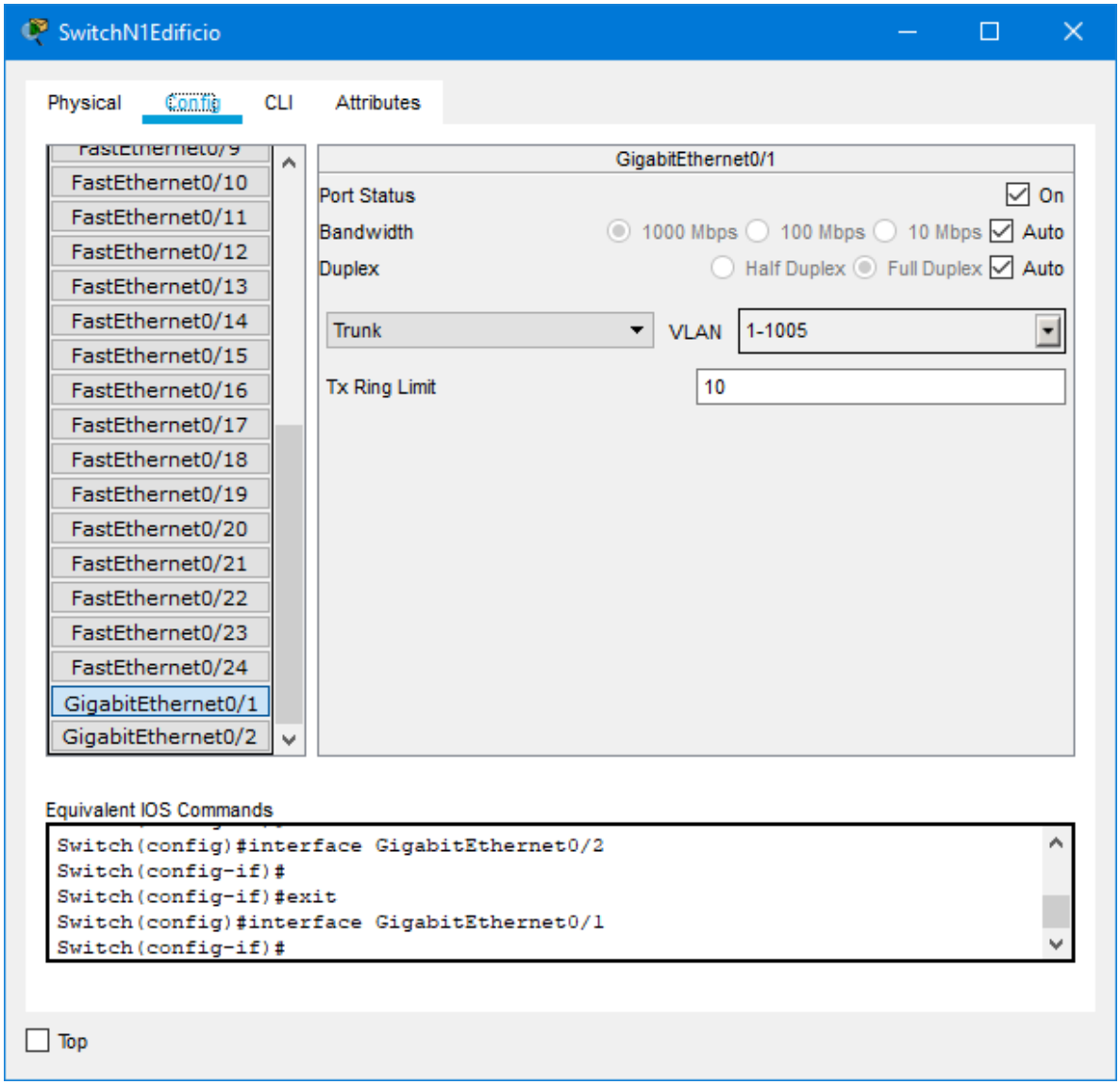


Figura 4.9 Asignación de enlace tipo troncal en interfaz GigabitEthernet 0/2 en SwitchN1 que conecta a SwitchN1

Router NODO 1

Una vez que se tienen configuradas las VLANs en los switches, se debe configurar el enlace troncal del Router Nodo 1, por donde serán transmitidas todas las VLANs, la base de datos de VLANs del router quedarían configuradas como se indica en la figura 4.10:

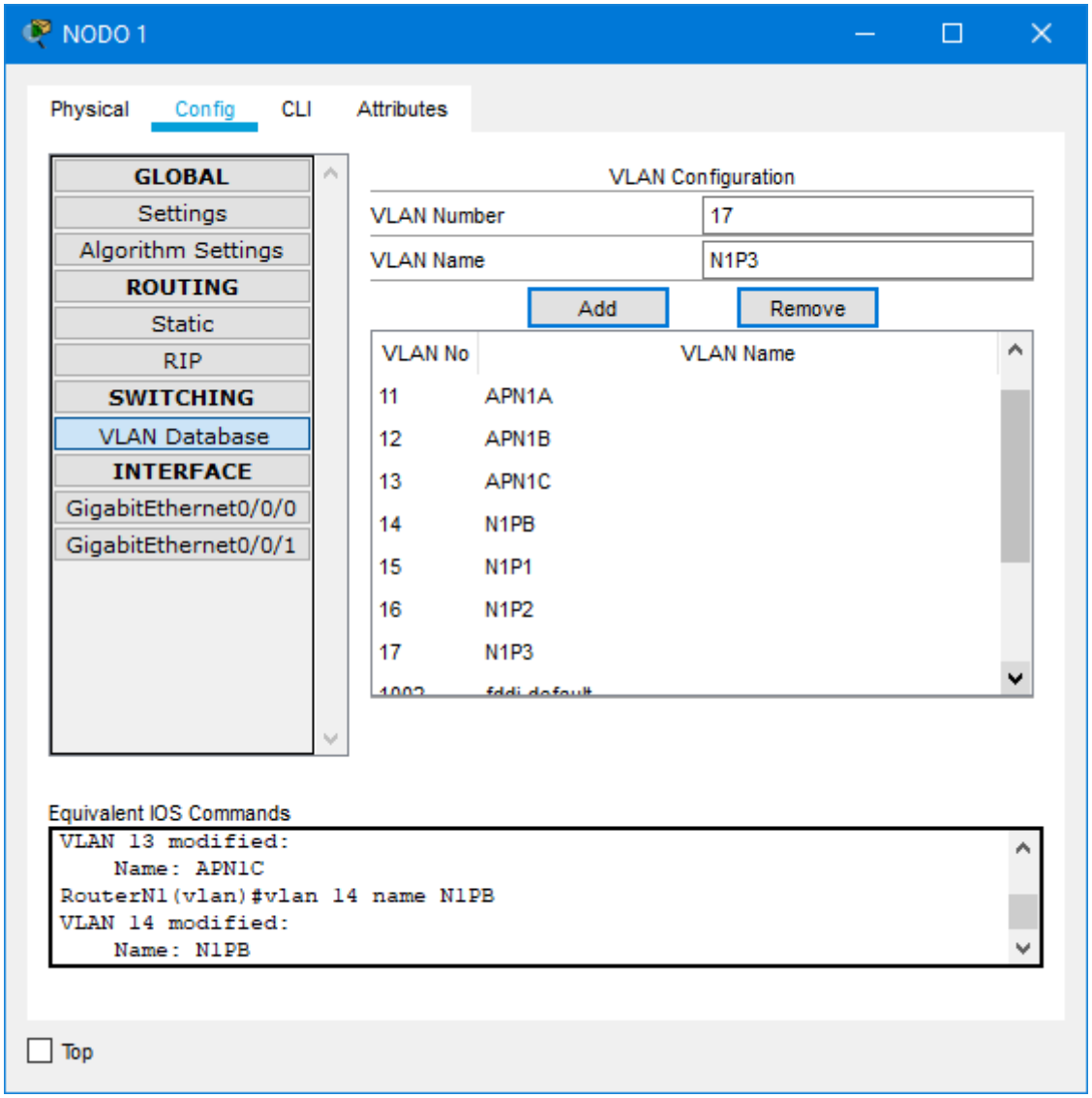


Figura 4.10 Base de datos de VLANs de Router NODO 1

Es necesario también configurar la tabla de direcciones de Red RIP para el enrutamiento correcto con los otros routers, que serían todas las redes de todas las VLANs de la red adicional a la red de nodos conectada directamente al router NODO 1 que es la red 192.168.240.0/24, quedando en la figura 4.11:

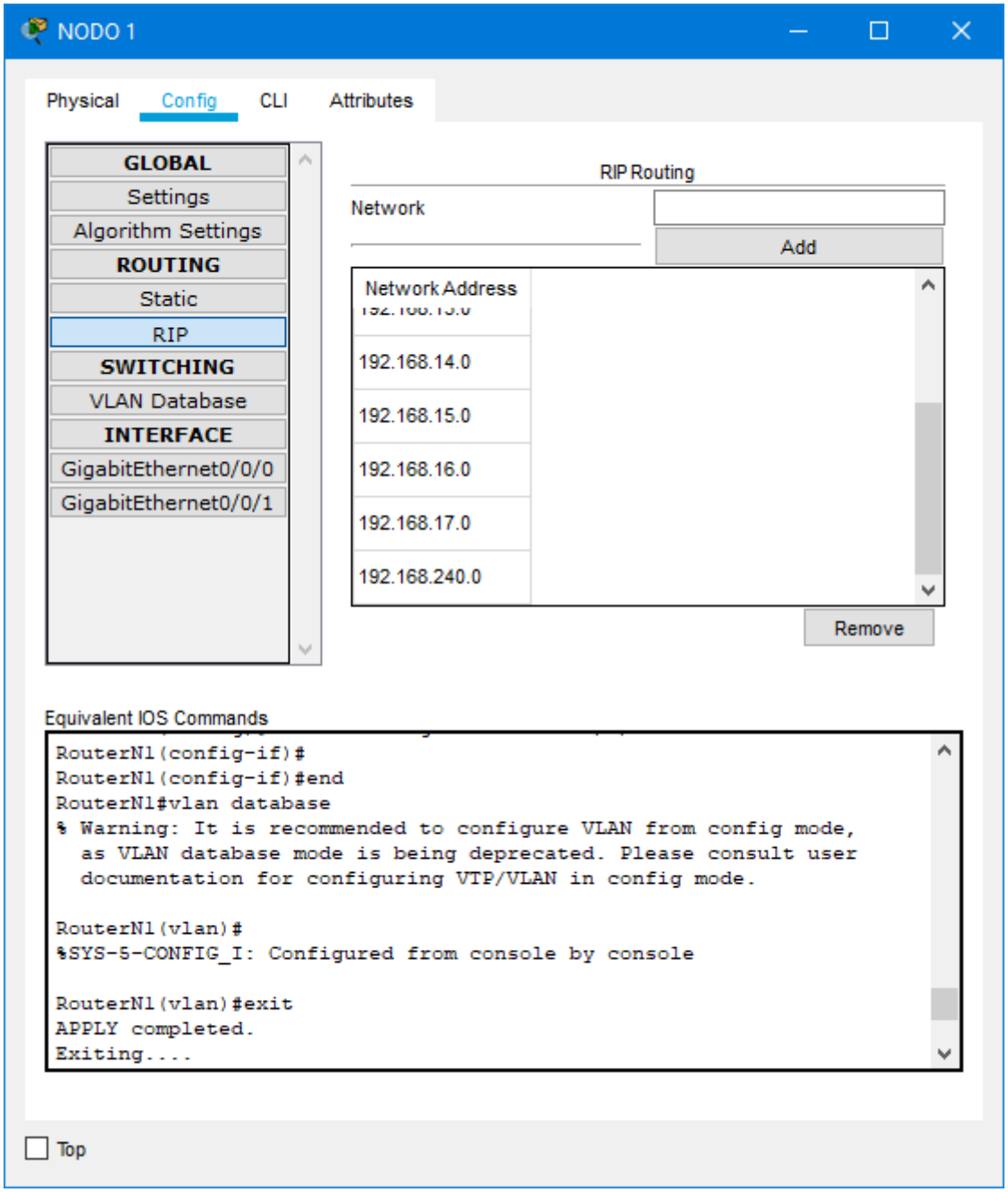


Figura 4.11 Configuración de protocolo de enrutamiento RIP en router NODO 1

En el router la configuración es más complicada porque debido a que opera en capa 3 y por la misma interfaz van a manejarse distintas redes debido a las VLAN, es necesario configurar la interfaz GigabitEthernet 0/0/0 con una subinterfaz para cada red IP correspondiente a cada VLAN, y asignarle una ip a dicha subinterfaz, que será la dirección de Gateway para cada VLAN, se debe también habilitar la encapsulación dot1Q (IEEE 802.1Q) para poder hacer uso de las subinterfaces y VLANs, para realizar estas configuraciones es necesario ingresar a la interfaz de comandos del router, para

facilitar la gestión se está configurando el número de subinterfaz correspondiente a la VLAN y red que utiliza, por ejemplo, para configurar la subinterface de la VLAN 11, se utilizan los siguientes comandos:

```
RouterN1#configure terminal
RouterN1(config)#interface GigabitEthernet 0/0/0.11
RouterN1(config-subif)#encapsulation dot1Q 11
RouterN1(config-subif)#ip address 192.168.11.1 255.255.255.0
```

Se deberá replicar los mismos comandos respectivamente para cada subinterfaz de acuerdo con su red y VLAN.

Para la simulación se activará el servicio DHCP en el router, se tendrá que configurar un pool de direcciones para cada red VLAN, por ejemplo, para configurar el pool DHCP de la VLAN 11, se utilizaran los siguientes comandos:

```
RouterN1#configure terminal
RouterN1(config)#ip dhcp pool dhcp-pool-vlan11
RouterN1(dhcp-config)#network 192.168.11.0 255.255.255.0
RouterN1(dhcp-config)#default-router 192.168.11.1
RouterN1(dhcp-config)#dns-server 220.220.220.220
```

Se deberá replicar los mismos comandos respectivamente para cada pool DHCP de acuerdo con su red y VLAN.

La configuración global del RouterN1 se la detalla dentro del Anexo B.

Con la configuración realizada, queda operativo el router para cada VLAN, si se realiza una prueba de conexión desde un equipo conectado al APN1a de la VLAN 11 perteneciente a la red 192.168.11.0/24, se tiene efectivamente conexión al router y al servidor web lo cual confirma que la configuración fue realizada correctamente, en la figura 4.12 se presenta una prueba de conexión desde uno de los equipos cliente:

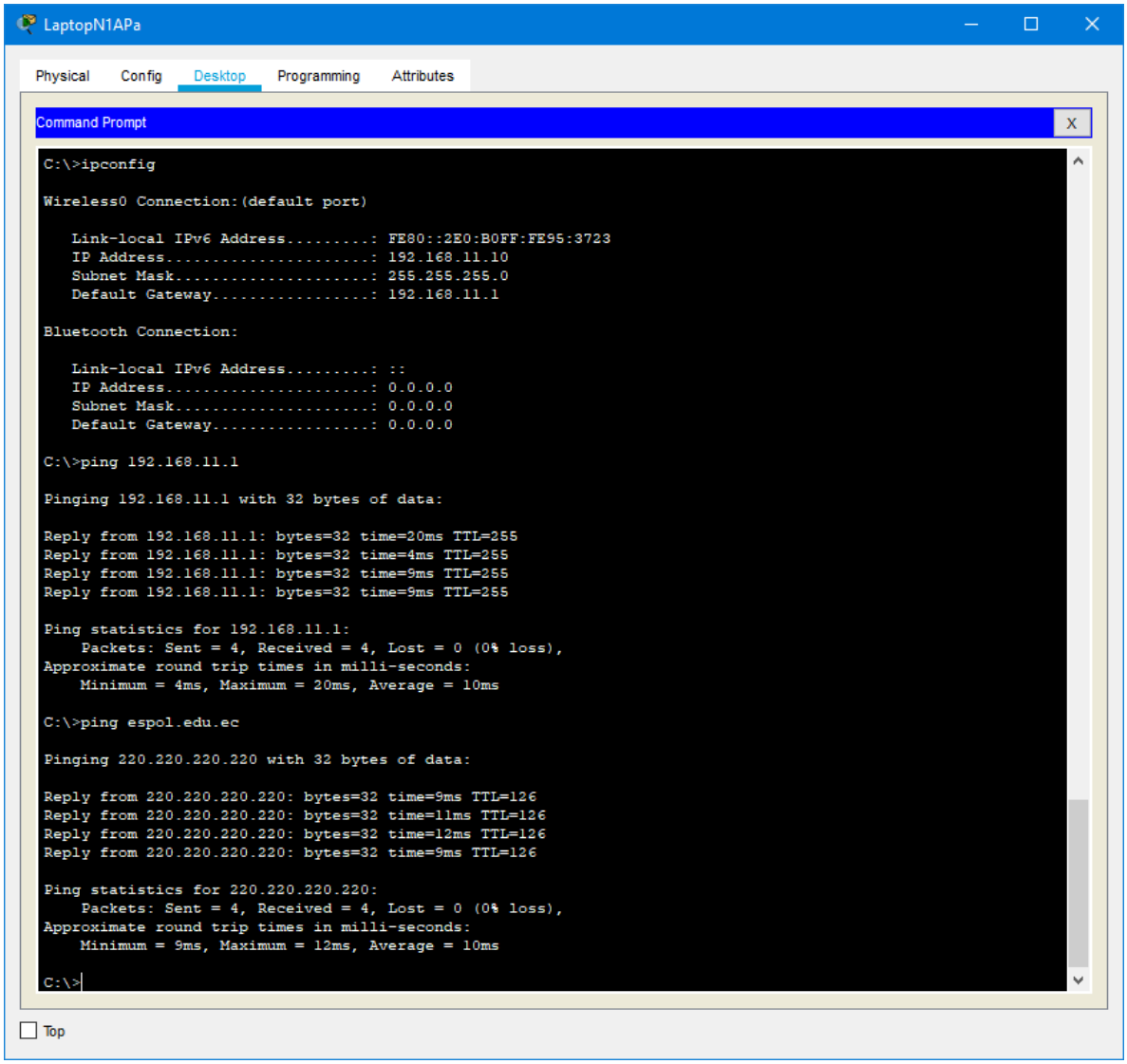


Figura 4.12 Prueba en host de asignación de IP vía DHCP, ping a router NODO 1 y a servidor HTTP

En la figura 4.13 se muestra una prueba de navegación al servidor http simulado:

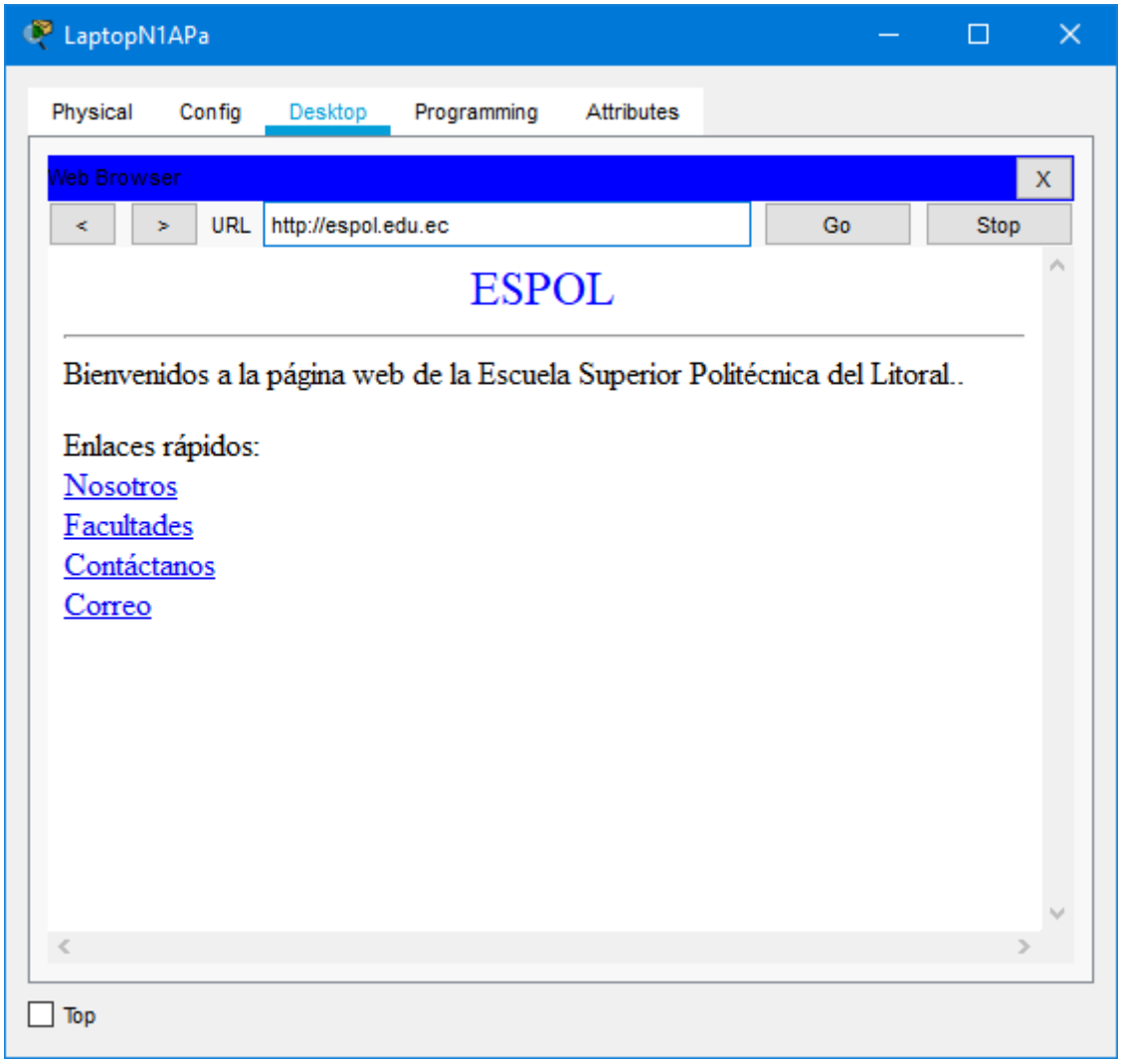


Figura 4.13 Prueba de navegación a servidor HTTP simulado

4.2 Comparacion de trafico en dominios de broadcast

Teniendo configurados el escenario sin VLAN y con VLAN en el Packet Tracer, se procede a realizar una comparación de trafico de broadcast utilizando la herramienta de simulación del Packet Tracer, en la cual se puede simular el fujo de paquetes en la red.

4.2.1 Simulación de trafico en dominios de broadcast sin VLANs

Utilizando la herramienta de simulación de tráfico en Packet Tracer, se origina un paquete de broadcast desde uno de los equipos cliente, se observará que los paquetes son enviados a todos los enlaces y equipos involucadros en el dominio de broadcast. En este caso, un paquete de broadcast emitido por el host PC1-N1P2 ubicado en el segundo piso de la red simulada en el edificio, una captura de la simulacion se encuentra ilustrado en la figura 4.14:

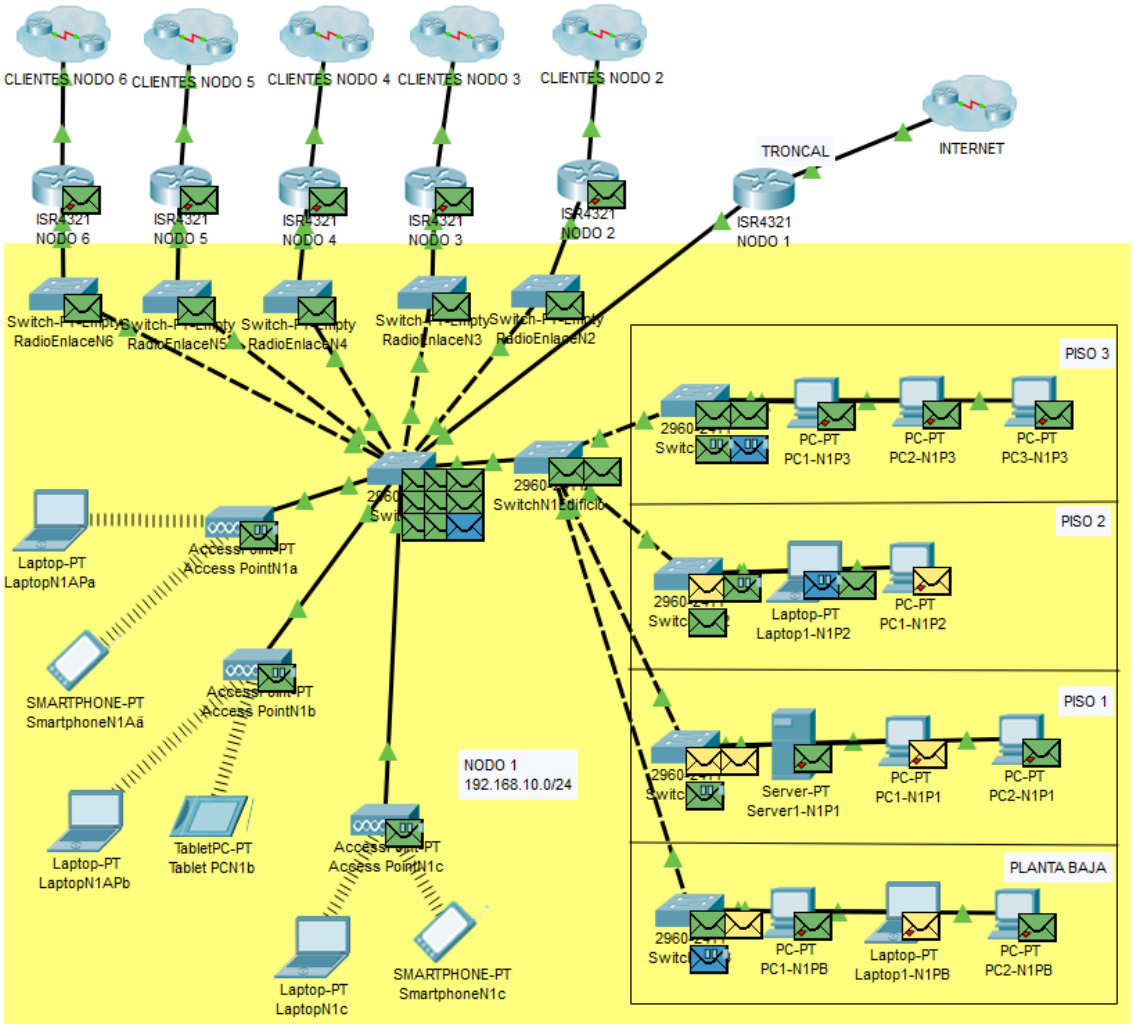


Figura 4.14 Simulación de broadcast en Packet Tracer - red sin VLAN

Como se puede observar, un paquete de broadcast puede llegar a otro grupo de equipos donde no es necesario que llegue, siempre y cuando los equipos se encuentren dentro de la misma LAN y el mismo dominio de broadcast, estos se verán afectados.

4.2.2 Simulación de trafico en dominios de broadcast con VLANs

Utilizando la herramienta de simulación de tráfico en Packet Tracer, se simula un paquete de broadcast emitido por el host PC1-N1P2 ubicado en el segundo piso de la red simulada en el Edificio, y ahora perteneciente a la VLAN 16 se trasmite de la siguiente manera en una red configurada VLANs, una captura de la simulación se encuentra en la figura 4.15, donde la línea color rojo denota la trayectoria del paquete de broadcast:

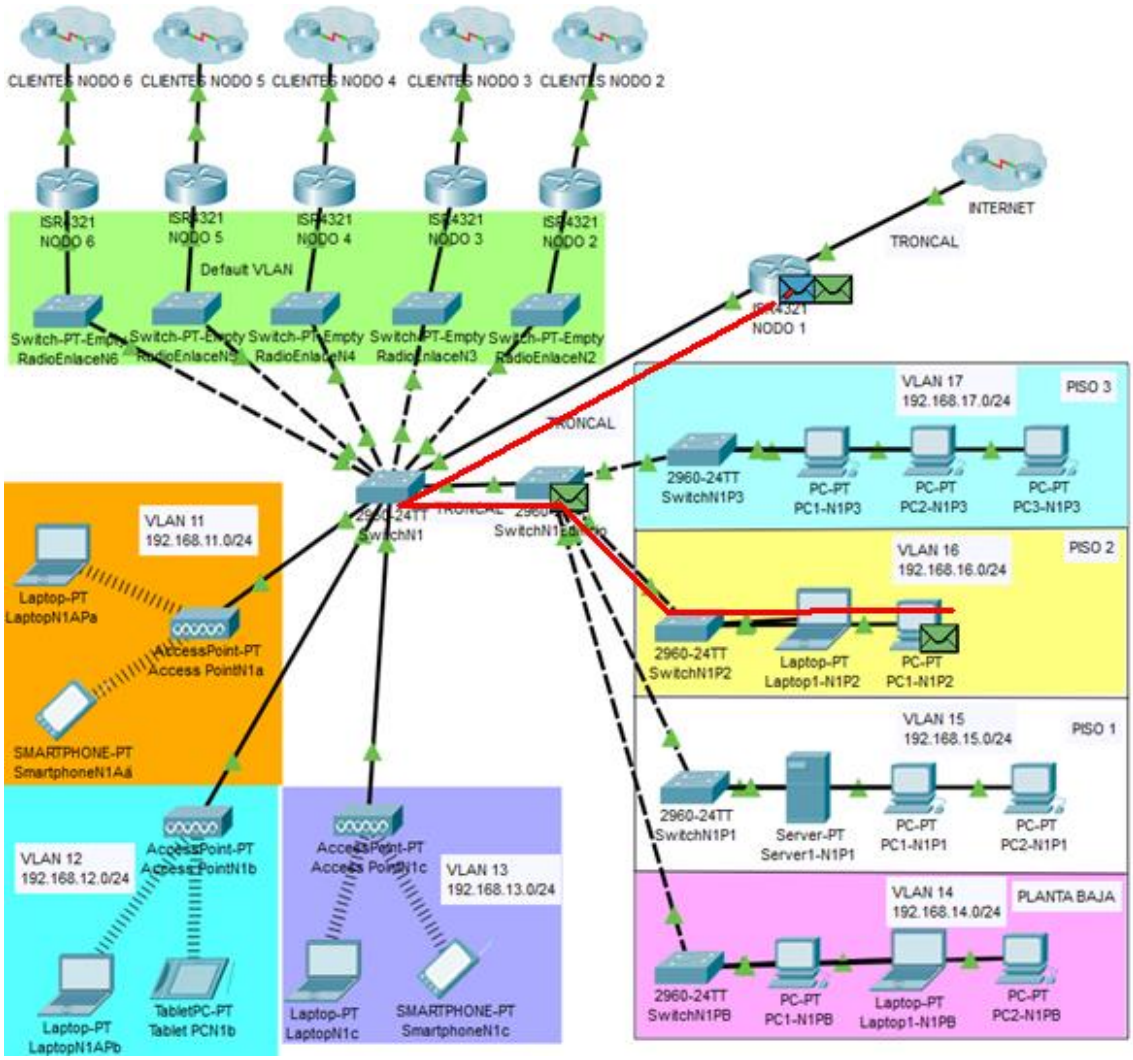


Figura 4.15 Simulación de trafico de broadcast con VLAN

4.2.3 Resultado de comparación de simulación de tráfico

A diferencia del escenario sin VLANs, en la simulación de una red con VLANs correctamente configuradas, se puede apreciar que el tráfico de broadcast enviado por el host PC1-N1P2 solo afecta a los equipos pertenecientes a su propia VLAN, y a los enlaces troncales que le permiten llegar al router que tiene la conexión al proveedor de internet, es decir, el tráfico de la red fluye únicamente por donde es necesario, y los equipos afectados por los tráfico de broadcast, pasan de ser todos los equipos clientes del nodo, a ser únicamente los equipos pertenecientes a la VLAN 16.

Se logra demostrar la optimización de red al crear VLANs en cada área y limitar el flujo de tráfico de los paquetes de broadcast a los dispositivos relevantes.

CAPÍTULO 5

5 EXPERIMENTACIÓN Y ANÁLISIS DE DATOS

5.1 Configuración del sistema

5.1.1 Localización geográfica y duración de la medición

La localización del rack donde se encuentran los equipos principales router principal y uno de los nodos del proveedor Celeritel Solutions S.A., se encuentran en el cantón Playas, mediante un switch Zyxel modelo GS1900-24E se conectan las radioantenas que permiten la conexión a los nodos ubicados en distintos puntos geográficos dentro del cantón Playas, este switch que conecta a los nodos a su vez, está conectado a usuarios finales que se encuentran en la misma ubicación al rack principal.

Se realizará una medición de tráfico y de paquetes de broadcast por una duración de 5 días aleatorios, en las redes de clientes del nodo 1 donde serán implementadas las VLANs, antes y después de la configuración de las VLAN en los equipos de red.

Tomando como base figura 2 previamente presentada, dentro del área de equipos cliente, se detallan 2 puntos clientes en los cuales se propone configurar las VLAN y realizar las mediciones. En la figura 5.1 se presenta la ubicación de los equipos de medición, indicados por los cuadros color rojo, y puntos a clientes dentro del nodo, para el escenario sin VLAN implementadas:

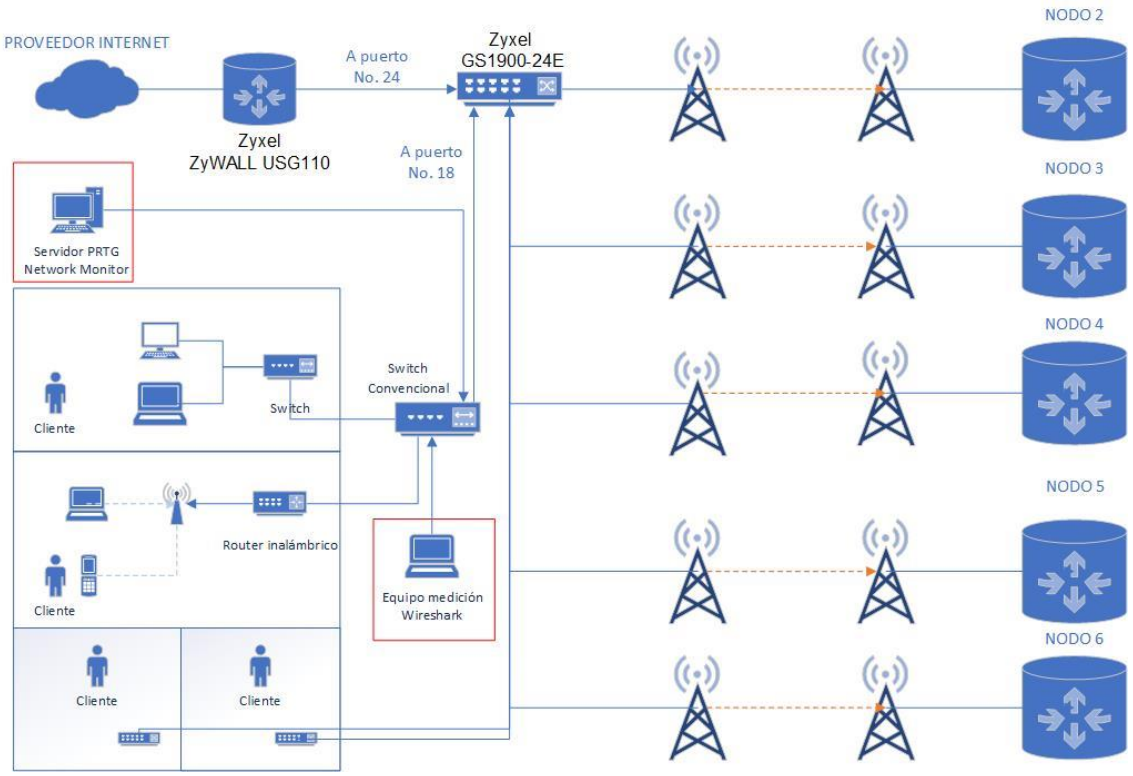


Figura 5.1 Ubicación de equipos de medición en red de clientes

La medición tendrá una duración mínima de 10 días, separadas en 5 días antes de la implementación de VLANs y 5 días después de la implementación de VLANs.

5.1.2 Parámetros de configuración

Para implementar VLANs en la red, es necesario realizar configuraciones tanto en el router principal Zyxel modelo ZyWALL USG110 como en el Switch Zyxel modelo GS1900-24E, de hecho, al ser las VLANs una tecnología de capa 2, la mayor parte de la configuración debe realizarse en el switch.

Las especificaciones técnicas del router Zyxel modelo ZyWALL USG110 se encuentra detalla en el Anexo C, y las especificaciones del switch Zyxel modelo GS1900-24E se encuentran en el Anexo D.

Será necesario crear la VLAN a la que pertenecen los usuarios finales con el identificador de VLAN 11 (VLAN ID 11), a partir de ahora llamada sólo VLAN 11, y habilitarla en unos de los puertos del switch Zyxell GS1900-24E. Para este caso se seleccionará el puerto 18, también será necesario habilitar la VLAN 11 en el puerto 24 que será el enlace tipo troncal que conectará el switch al router principal y por el cual deben fluir el tráfico tanto de la VLAN 1 como de las VLAN 11.

Parámetros de configuración de Switch Zyxel modelo GS1900-24E

En el caso real, se ingresa a la administración del switch por medio de la dirección IP de administración, y se lo configura con los siguientes parámetros:

- Se agregará la VLAN 11 a la base de datos de VLANS y se comprueba que la VLAN creada este dentro de la base de VLANs del switch, esta configuración se presenta en las figuras 5.2 y 5.3.

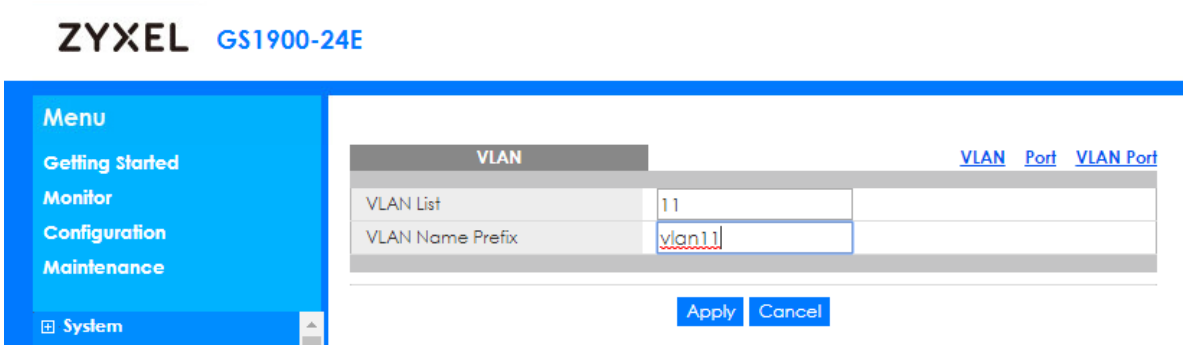


Figura 5.2 Interfaz de administración del switch GS1900-24E - creación de VLAN

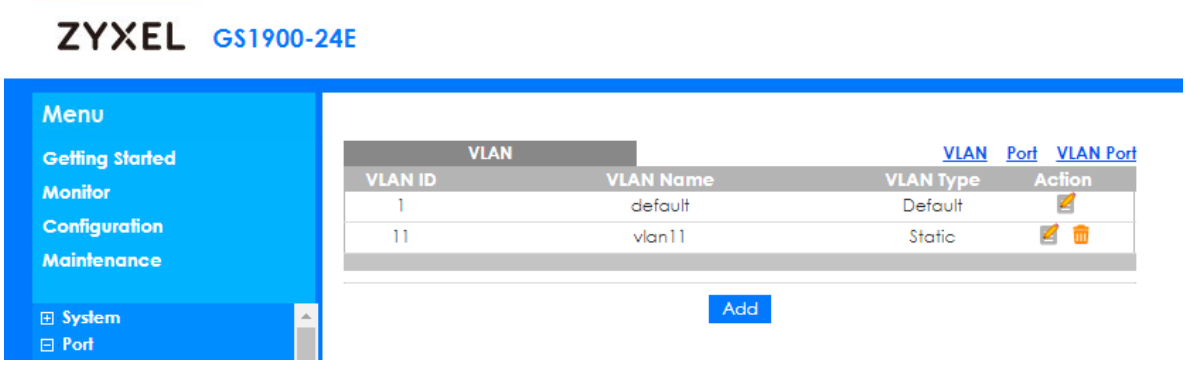


Figura 5.3 Interfaz de administración del switch GS1900-24E – Base de VLANs

- Para este escenario se configura el puerto 18 del switch para el uso de la VLAN 11, primero es recomendable denominar el puerto para uso de la VLAN y después es necesario vincular el puerto 18 de la VLAN 11, en el caso de los equipos marca Zyxel el número de VLAN está indicado por el campo PVID (Port VLAN ID) como en la muestra en las figuras 5.4 y 5.5.

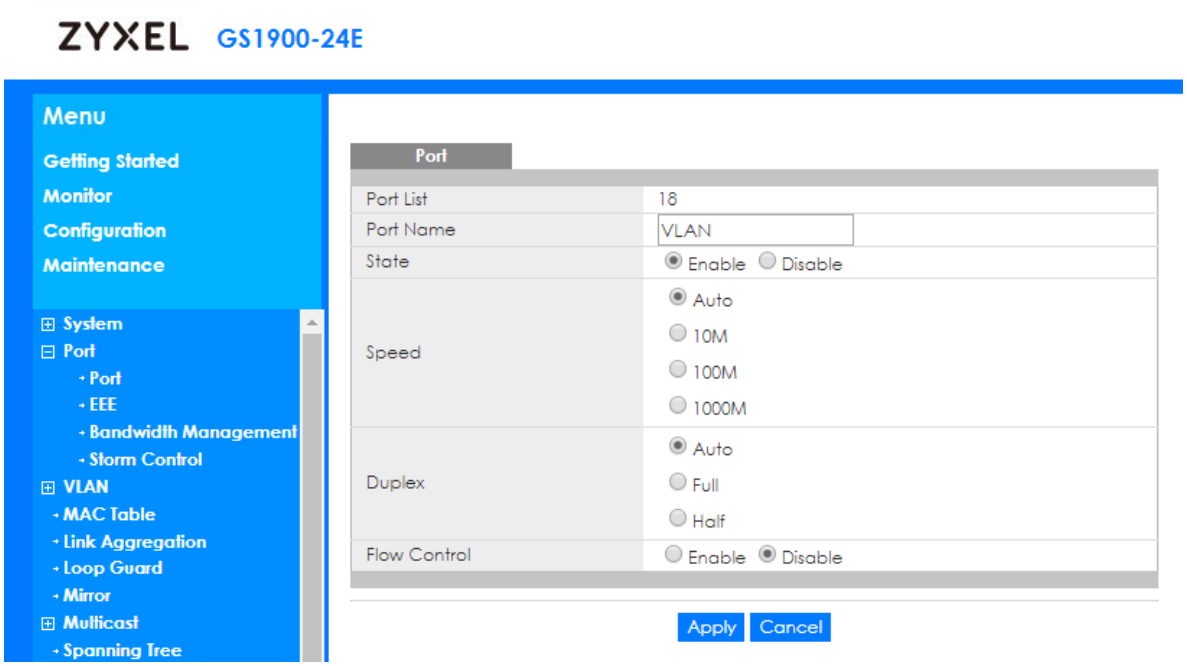


Figura 5.4 Interfaz de administración del switch GS1900-24E – configuración de puerto 18

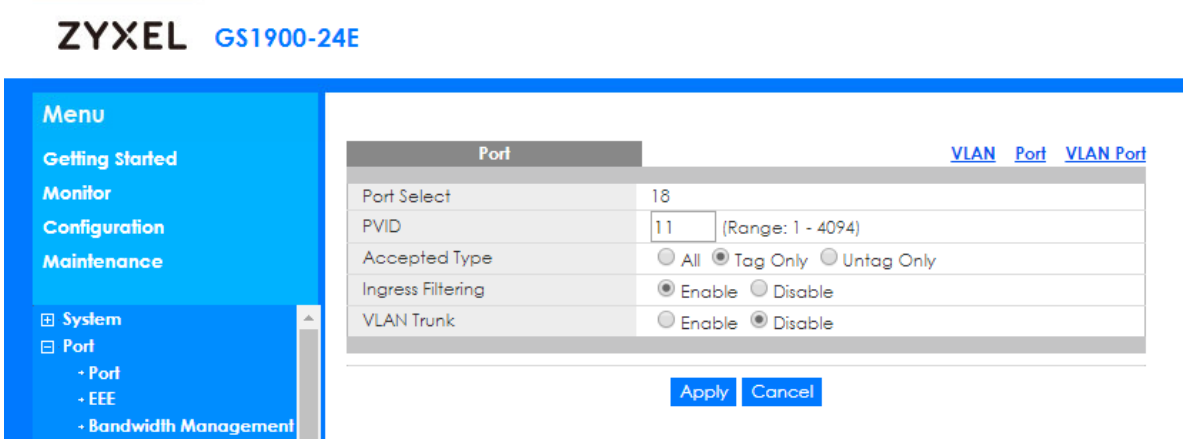


Figura 5.5 Interfaz de administración del switch GS1900-24E – vinculación de puerto 18 a VLAN 11

- Se debe habilitar el tráfico de la VLAN 11 por los puertos 18 y 24, por lo que será necesario especificar en la interfaz de administración del switch que por esos puertos solo se permita el tráfico de tramas debidamente etiquetadas como pertenecientes a la VLAN 11, para mejor control, se especificará que todos los demás puertos, se prohíba el acceso a tráfico de la VLAN 11. La configuración realizada se muestra en la figura 5.6:

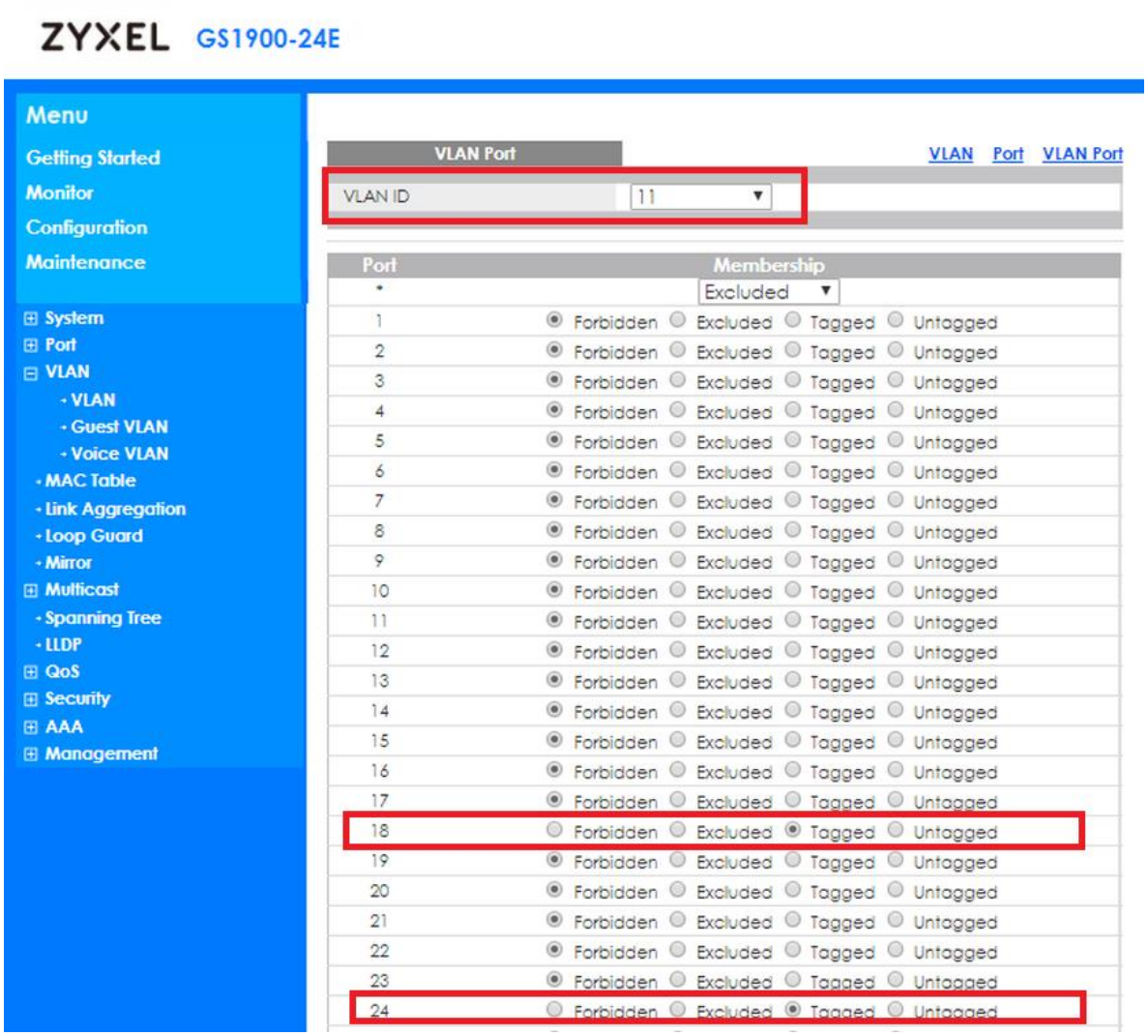


Figura 5.6 Interfaz de administración del switch GS1900-24E – Habilitar tráfico de VLAN 11 por los puertos 18 y 24.

- Para el caso particular de los switches marca Zyxel, con la configuración mencionada en el punto anterior realizada, el puerto 18 quedaría operativo tanto dentro de las VLAN 11 y como de la VLAN 1 (la VLAN por defecto); es decir, por medio del puerto 18 se trasmitirá tráfico de broadcast de la VLAN 1 y la VLAN 11, como lo que se propone es segmentar los dominios de broadcast. es necesario especificar dentro de la interfaz de administración, que se prohíba el tráfico de la VLAN 1 por el puerto 18. Debido a que el puerto 24 será un enlace tipo troncal, es correcto que se trasmita el tráfico de ambas VLANs. Se realiza la configuración como se muestra en la figura 5.7.

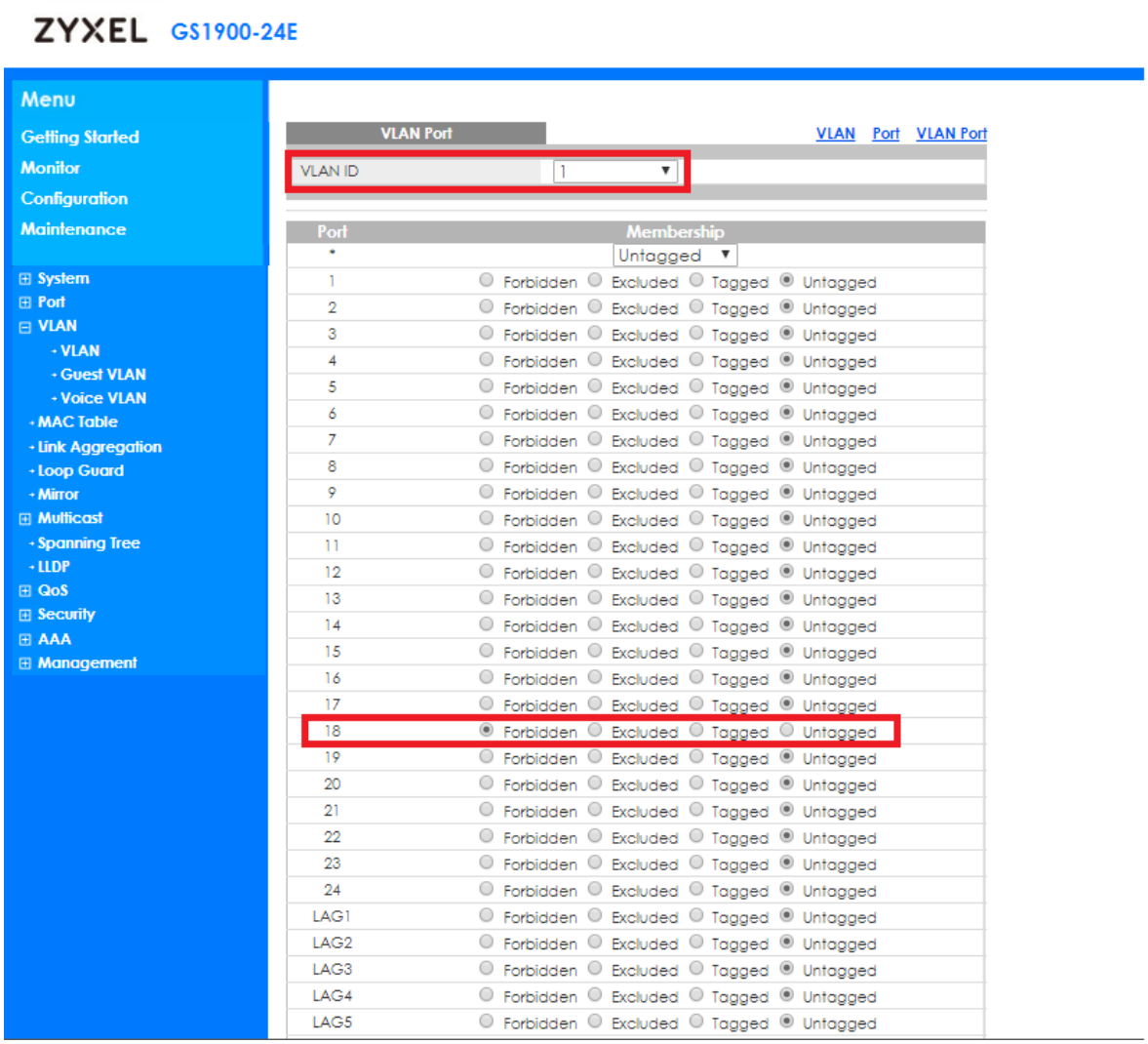


Figura 5.7 Interfaz de administración del switch GS1900-24E – Prohibición de trafico de VLAN 1 por el puerto 18.

Parámetros de configuración de router Zyxel modelo ZyWALL USG110

Para poder tener comunicación con la VLAN 11 ya configurada en switch GS1900-24E, se debe también agregar esta VLAN ID dentro de la base de VLANs del router, así como establecer el enlace tipo troncal que conecta el router ZyWALL USG110 al switch GS1900-24E ya configurado, las configuraciones se las realizarán mediante la interfaz gráfica del router presentada en la figura 5.8:

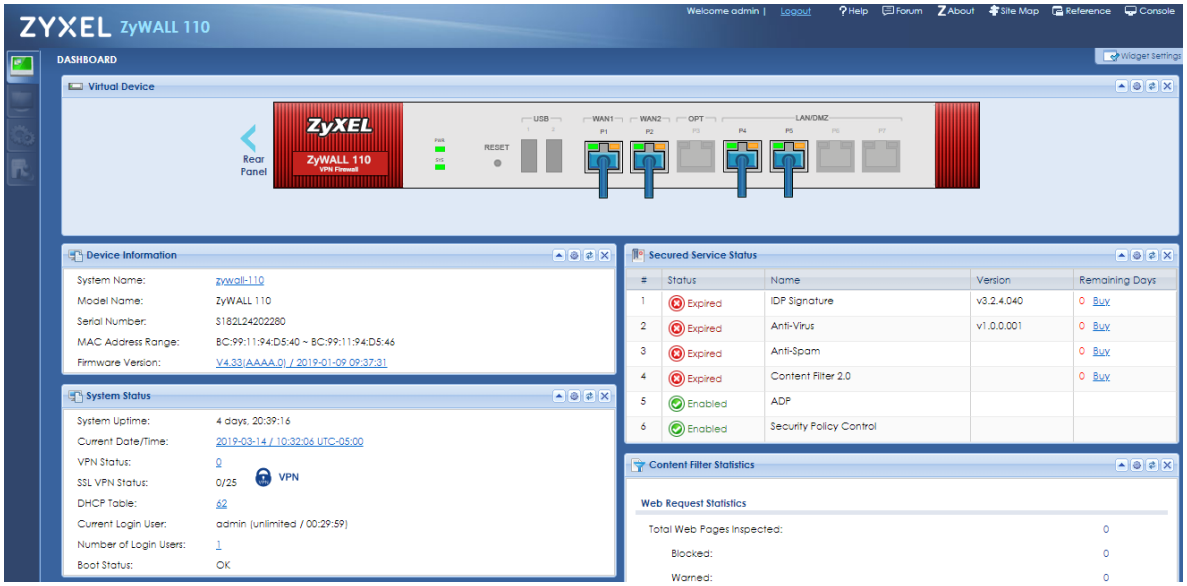


Figura 5.8 Interfaz de administración de router Zyxel modelo ZyWALL USG110

- Primero se deberá agregar la VLAN 11, esto automáticamente agregará la subinterfaz para esta VLAN por lo que será necesario especificar una IP que será el Gateway al router de los equipos pertenecientes a la VLAN 11, se indicara que la interfaz es interna debido a que la conexión se realizara mediante uno de los puertos LAN del router. Debido a que la red de la VLAN 11 es la 192.168.241.0/24, la IP de la interfaz VLAN 11 del router será 192.168.241.1/24. como se muestra en la figura 5.9:

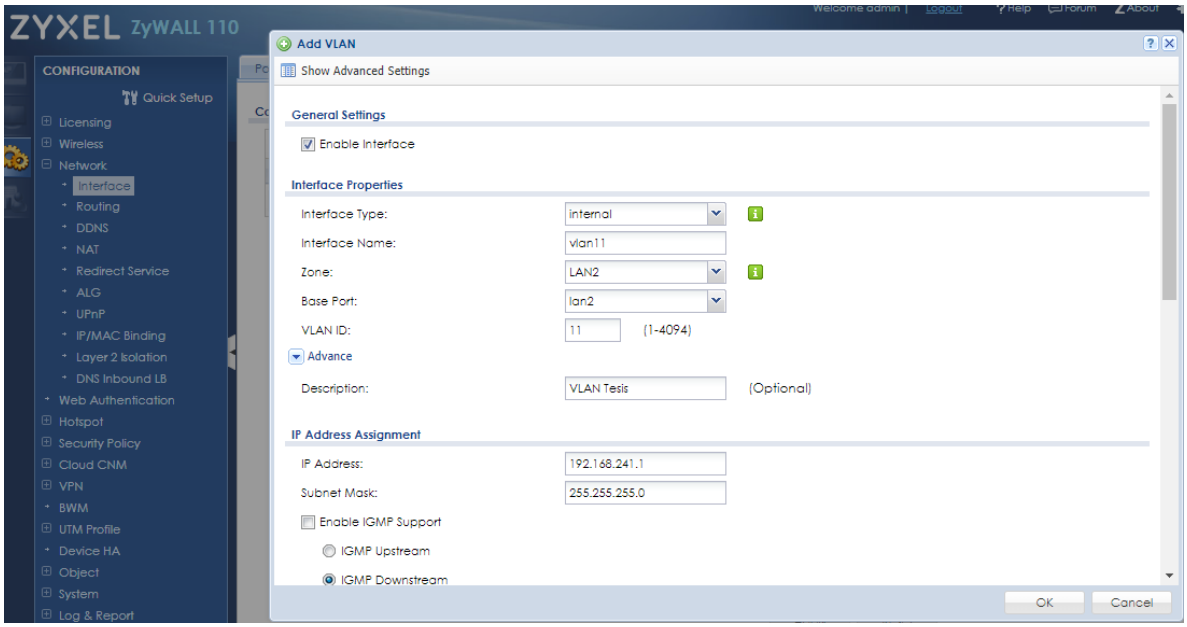


Figura 5.9 Interfaz de administración router USG110 – creación de VLAN 11 y asignación de IP

- La plataforma de administración permite habilitar el servicio DHCP en la interfaz VLAN 11, para facilitar la conexión de equipos clientes se habilitará el servicio DHCP como se muestra en la figura 5.10:

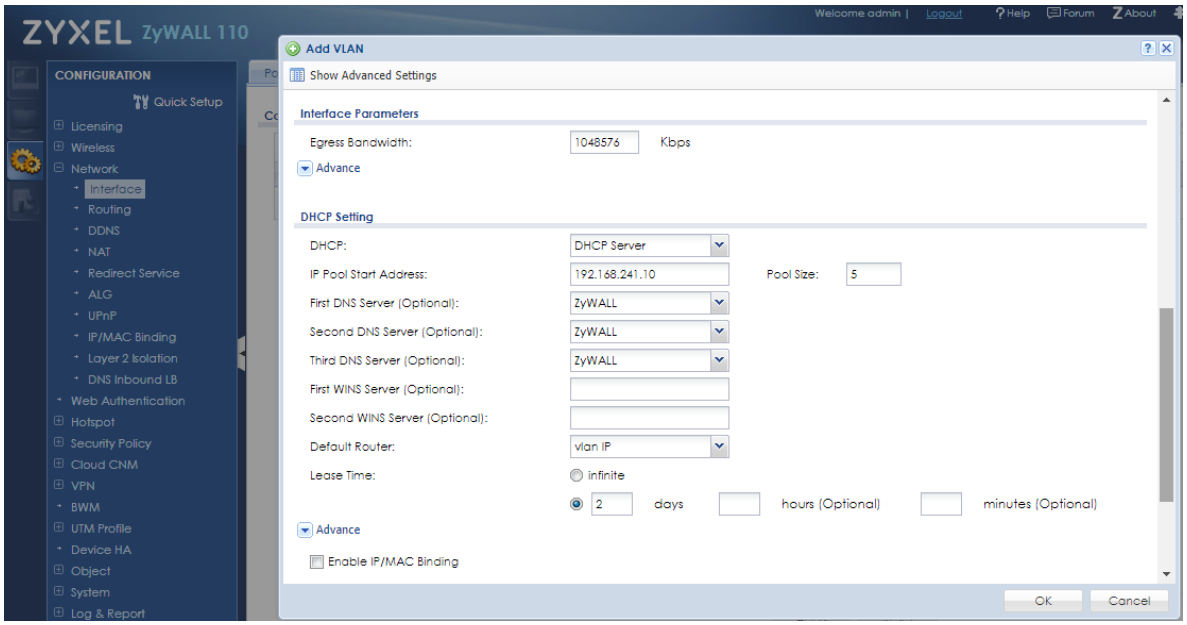


Figura 5.10 Interfaz de administración router USG110 – habilitación de servidor DHCP en interfaz VLAN 11

- Se verifica que la VLAN 11 se encuentra dentro de la base de VLANs del router, en la figura 5.11 se muestra la base de VLANs en el router:

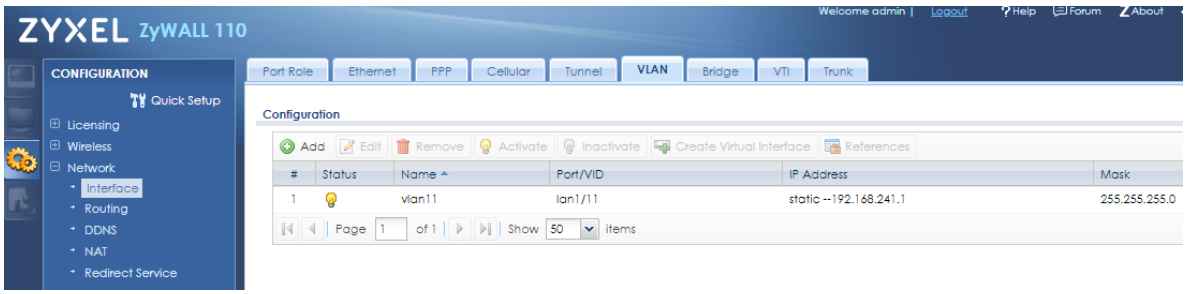


Figura 5.11 Interfaz de administración router USG110 – base de VLANs

Para corregir problemas de configuración y comprobar que la VLAN 11 se encontraba operativa de manera correcta, fue muy útil la utilización del análisis de tráfico de Wireshark mediante un equipo portátil conectado directamente al rack de equipos para la verificación, como se aprecia en la fotografía de la figura 5.12:

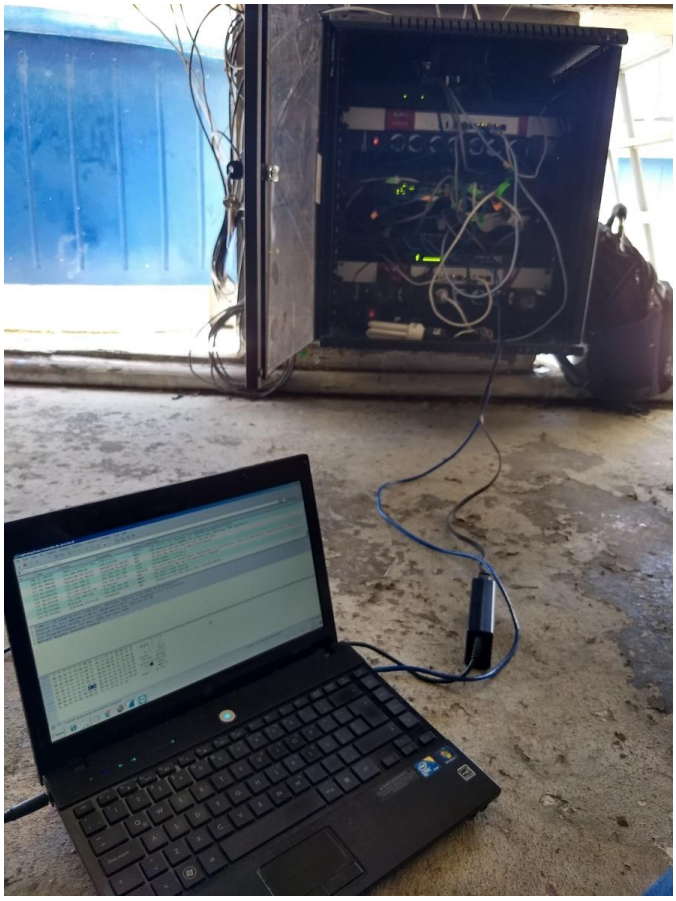


Figura 5.12 Medición de Tráfico con Wireshark de red entre nodos

Una vez terminada la configuración de la VLAN 11 en dos de los puntos clientes, el diagrama de conexión de la figura 5.13 detalla qué equipos pertenecen a las VLAN 11, la cual se resalta de color amarillo en el gráfico.

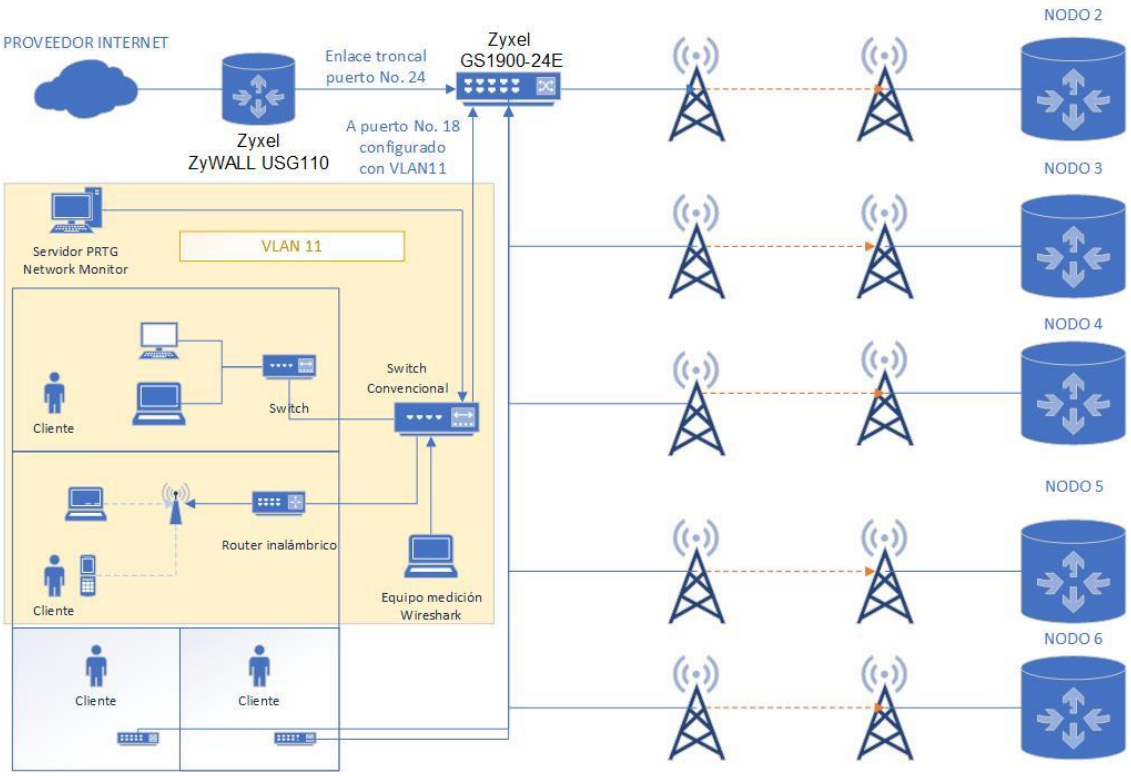


Figura 5.13 Cobertura de VLAN 11 en escenario real

Configurada correctamente la VLAN 11 se procede a realizar las mediciones respectivas.

5.2 Medición de datos

Se configurarán sensores mediante el protocolo simple de administración de red (SNMP) dentro del sistema de monitoreo PRTG, instalado en uno de los servidores de la red, que permiten monitorear el tráfico de broadcast que se trasmita en la red LAN. Adicionalmente se realizará la captura de paquetes de broadcast mediante la aplicación Wireshark, de donde se obtendrá detalles del número de paquetes de broadcast, ancho de banda ocupado y el número de equipos que generan broadcast en la red.

Dentro de las figuras 5.1 y 5.13 ya presentadas, se muestra la ubicación de los equipos de medición dentro de la red antes de implementar la VLAN y después de implementarla respectivamente.

La captura de paquetes de Wireshark se la realizará desde uno de los puntos de los clientes residenciales donde se implementó la VLAN 11, como se demuestra en la fotografía de la figura 5.14.

Figura 5.14 Medición de tráfico y broadcast mediante Wireshark en punto residencial

5.3 Recopilación de datos

Dentro de PRTG y dentro de Wireshark, una vez obtenido el resultado del proceso de sniffing por un total de 10 días, separados en dos escenarios: 5 días en el estado actual de la red, y 5 días después de la implementación de las VLAN, se filtrarán los paquetes de broadcast para sacar los totales enviados por uno de los enlaces.

Para realizar las mediciones se utilizó un computador con Wireshark instalado dentro de uno de los puntos cliente, una vez que se verificó que se estaba capturando el tráfico, se programaron las mediciones para capturar todo el tráfico y almacenarlo en archivos secuenciales cada 12 horas, se deja ejecutando la captura de tráfico durante 5 días consecutivos en cada escenario, obteniendo al menos 10 archivos por escenario, con información de tráfico de 12 horas cada uno como se muestra en la figura 5.15.

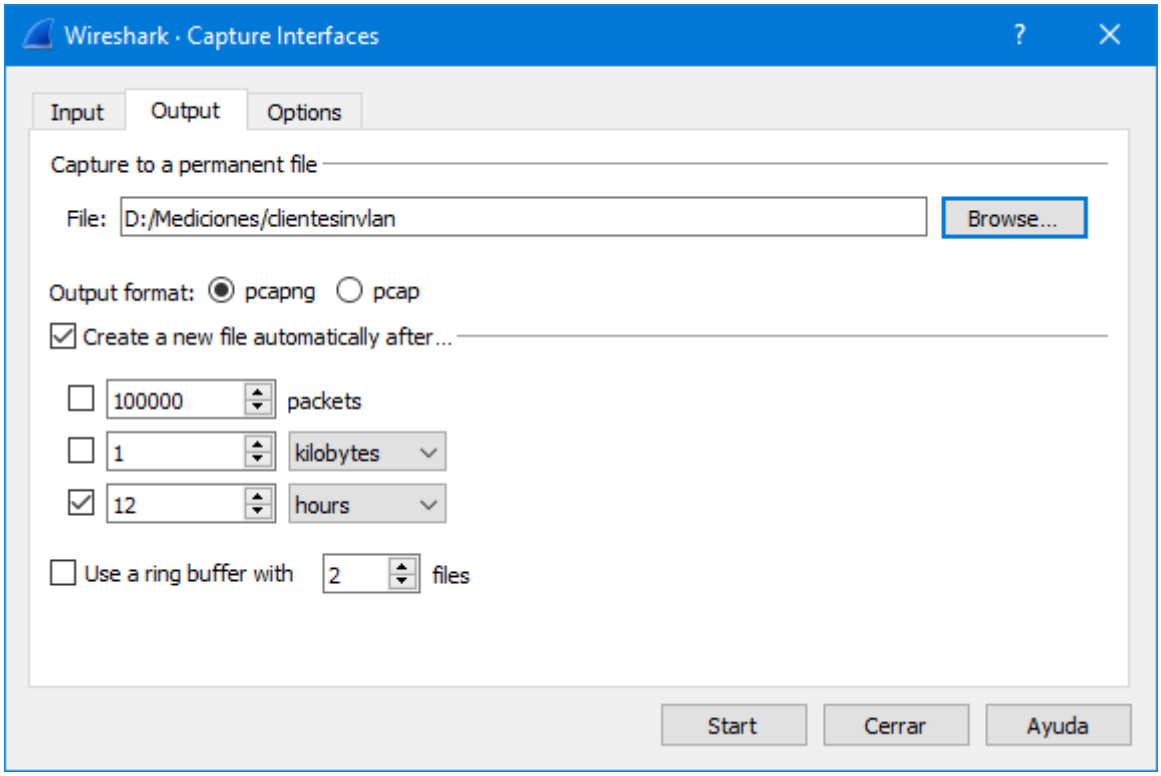


Figura 5.15 Interfaz de Wireshark para configuración de captura de tráfico

5.3.1 Escenario sin VLAN implementada

En la figura 5.16 se muestra un ejemplo de una estadística de medición de tráfico realizada en Wireshark, se puede observar que 124 equipos de red se encuentran generando tráfico, de los cuales más de 30 equipos se encuentran generando tráfico de broadcast al momento de la medición.

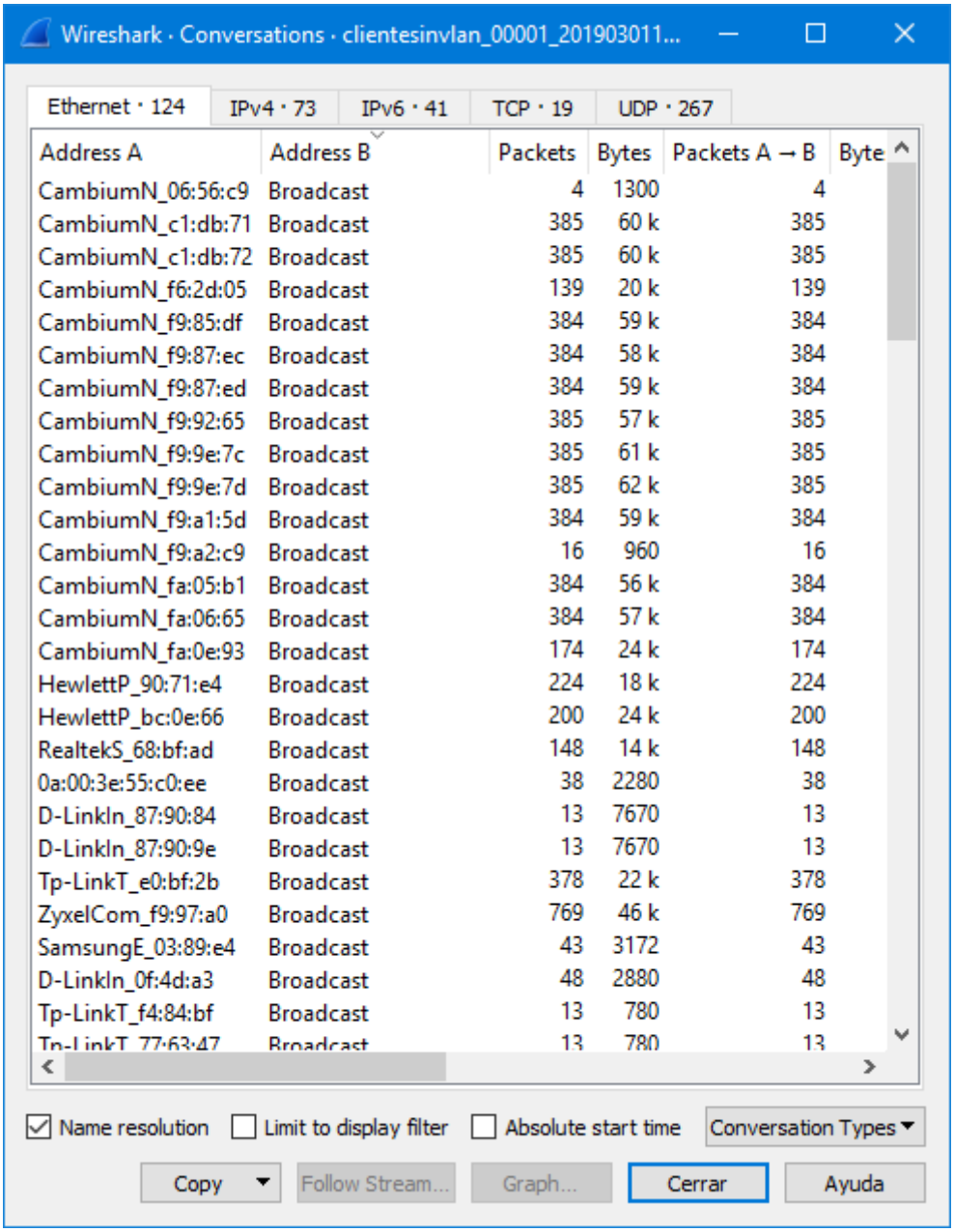


Figura 5.16 Estadísticas de tráfico de broadcast

Compilando la información de los 10 archivos que contenían información de los 5 días de mediciones se obtuvieron los siguientes resultados totales:

Escenario sin VLAN implementada

Número de paquetes de broadcast en la red: 188.307

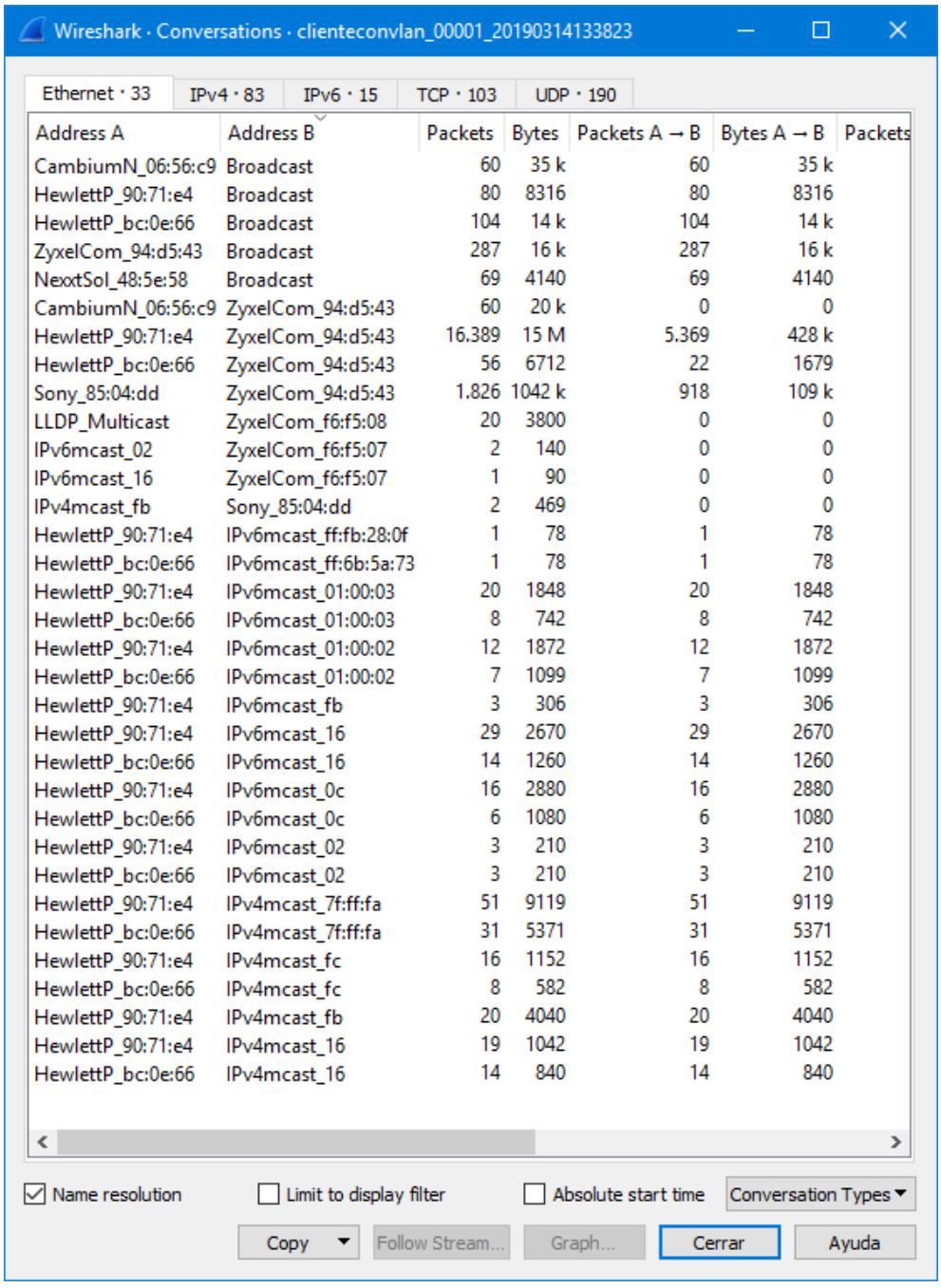
Total de bytes generados por broadcast: 20’751.197

Numero de dispositivos únicos en red realizando broadcasts en la red: 77

5.3.2 Mediciones en escenario con VLAN implementada

La medición en el escenario con VLAN se la realizar en el mismo punto donde se lo realizo en el caso de la red sin VLAN, es decir, en uno de los puntos de un cliente o usuario final.

En la figura 5.17 se puede apreciar una de las mediciones realizadas en Wireshark sobre la red con dentro de la VLAN ya implementada, como se puede observar, sólo intervienen 33 equipos que generan tráfico, y sólo 5 equipos se encuentran generando tráfico de broadcast al momento de la medición.



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets
CambiumN_06:56:c9	Broadcast	60	35 k	60	35 k	
HewlettP_90:71:e4	Broadcast	80	8316	80	8316	
HewlettP_bc:0e:66	Broadcast	104	14 k	104	14 k	
ZyxelCom_94:d5:43	Broadcast	287	16 k	287	16 k	
NexxtSol_48:5e:58	Broadcast	69	4140	69	4140	
CambiumN_06:56:c9	ZyxelCom_94:d5:43	60	20 k	0	0	
HewlettP_90:71:e4	ZyxelCom_94:d5:43	16.389	15 M	5.369	428 k	
HewlettP_bc:0e:66	ZyxelCom_94:d5:43	56	6712	22	1679	
Sony_85:04:dd	ZyxelCom_94:d5:43	1.826	1042 k	918	109 k	
LLDP_Multicast	ZyxelCom_f6:f5:08	20	3800	0	0	
IPv6mcast_02	ZyxelCom_f6:f5:07	2	140	0	0	
IPv6mcast_16	ZyxelCom_f6:f5:07	1	90	0	0	
IPv4mcast_fb	Sony_85:04:dd	2	469	0	0	
HewlettP_90:71:e4	IPv6mcast_ff:fb:28:0f	1	78	1	78	
HewlettP_bc:0e:66	IPv6mcast_ff:6b:5a:73	1	78	1	78	
HewlettP_90:71:e4	IPv6mcast_01:00:03	20	1848	20	1848	
HewlettP_bc:0e:66	IPv6mcast_01:00:03	8	742	8	742	
HewlettP_90:71:e4	IPv6mcast_01:00:02	12	1872	12	1872	
HewlettP_bc:0e:66	IPv6mcast_01:00:02	7	1099	7	1099	
HewlettP_90:71:e4	IPv6mcast_fb	3	306	3	306	
HewlettP_90:71:e4	IPv6mcast_16	29	2670	29	2670	
HewlettP_bc:0e:66	IPv6mcast_16	14	1260	14	1260	
HewlettP_90:71:e4	IPv6mcast_0c	16	2880	16	2880	
HewlettP_bc:0e:66	IPv6mcast_0c	6	1080	6	1080	
HewlettP_90:71:e4	IPv6mcast_02	3	210	3	210	
HewlettP_bc:0e:66	IPv6mcast_02	3	210	3	210	
HewlettP_90:71:e4	IPv4mcast_7f:ff:fa	51	9119	51	9119	
HewlettP_bc:0e:66	IPv4mcast_7f:ff:fa	31	5371	31	5371	
HewlettP_90:71:e4	IPv4mcast_fc	16	1152	16	1152	
HewlettP_bc:0e:66	IPv4mcast_fc	8	582	8	582	
HewlettP_90:71:e4	IPv4mcast_fb	20	4040	20	4040	
HewlettP_90:71:e4	IPv4mcast_16	19	1042	19	1042	
HewlettP_bc:0e:66	IPv4mcast_16	14	840	14	840	

Figura 5.17 Estadísticas de trafico de broadcast en red 12 Horas con VLAN

Compilando la información de los 10 archivos que contenían información de los 5 días de mediciones sobre la red con la VLAN implementada se obtuvieron los siguientes resultados totales:

Número de paquetes de broadcast en la red: 89.878

Total de bytes generados por broadcast: 16’574.747

Numero de dispositivos únicos en red realizando broadcasts en la red: 7

5.4 Comparación de trafico de broadcast en red sin VLAN y con VLAN

Tomando los resultados de las mediciones de la red sin VLAN y con VLAN se obtuvieron los resultados de la siguiente tabla, donde el valor de optimización de red es el porcentaje en el que se ve reducido el resultado de la red con VLAN implementada en comparación a la red sin VLAN utilizando la siguiente formula:

Optimización de red = 100 – (*valor con vlan* x 100) / *valor sin vlan*

Los resultados del cálculo para cada uno de los puntos de medición realizados se presentan en la tabla 3.

	Sin VLAN	**Con VLAN**	**Optimización de red (%)**
Número de paquetes de broadcast	188,307	89,878	52.27
Total de bytes generados por broadcast	20,751,197	16,574,747	20.13
Numero de dispositivos únicos en red realizando broadcasts	77	7	90.91

Tabla 3 Comparación de mediciones de Broadcast con VLAN y sin VLAN

Se puede observar que se reduce el número de paquetes que se trasmiten en la VLAN, esto es debido a que el número de equipos que trasmiten broadcast en la red se ha segmentado de manera significativa.

Del mismo modo el tráfico en bytes con la VLAN implementada es menor debido a que el número de equipos de la red únicos que generan broadcast se reduce a sólo los que son necesarios, no se aprecia una gran reducción en comparación a la que hay con el número de paquetes.

Analizando el tráfico por Wireshark se pudo apreciar que esto es posiblemente debido al tráfico DHCP, el cual no cambia de manera significativa en comparación a la red sin VLAN, pues la mayoría de los equipos de la red de nodos utilizaban direcciones IP estáticas, por lo que no había tanta diferencia en cuanto a tráfico tipo DHCP en la red.

Realizando un análisis más a detalle la configuración del servidor DHCP, se detectó que durante las mediciones se tenía configurado un tiempo de concesión de direcciones IP de 1 hora, lo cual explicaría el alto tráfico de broadcast de DHCP.

Mediante la interfaz del PRTG Network Monitor instalado en uno de los servidores de la red, se realiza la medición de tráfico en broadcast en los escenarios sin VLAN y con VLAN.

Como se puede apreciar en el ejemplo de análisis de tráfico de broadcast de la figura 5.18, en la red sin VLAN, el tráfico de broadcast alcanza como máximo 2,96 kb/s, y mantienen una tendencia de aproximadamente 1,8 kb/s.

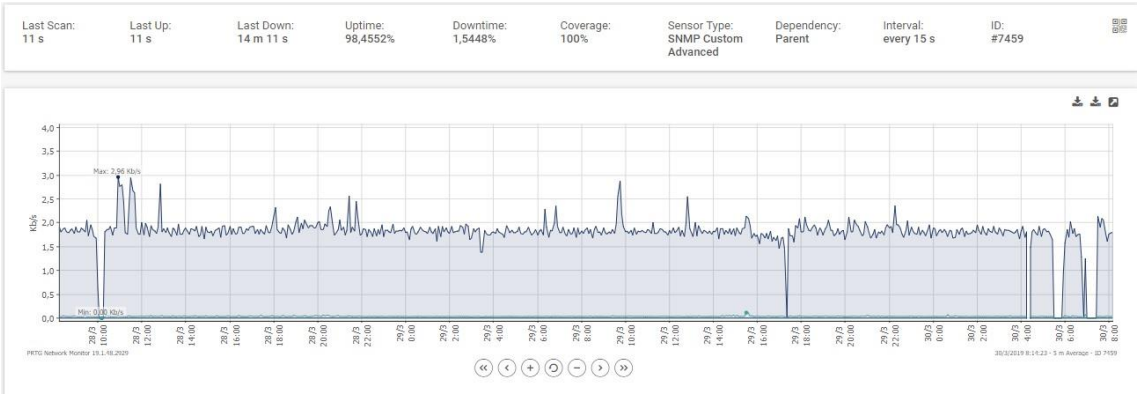


Figura 5.18 Análisis de tráfico por PRTG Network Monitor - Sin VLAN

En el ejemplo de tráfico de broadcast en la red con VLAN ilustrado en la figura 5.19, se puede apreciar una optimización de ancho de banda, obteniendo un tráfico máximo de 2,15 kb/s y teniendo una tendencia aproximada de 1,2 kb/s.

Figura 5.19 Análisis de tráfico por PRTG Network Monitor - Con VLAN

Comparando ambos resultados se puede determinar que limitando los dominios de broadcast mediante VLANs, se aprecia una optimización significativa de ancho de banda y de tráfico de broadcast en la red del proveedor de SAI.

CONCLUSIONES

Trabajando en ambos escenarios se han obtenido las siguientes conclusiones:

1. Se comprueba que el tráfico de broadcast es menor en una red que implementa VLANs, debido a que se reduce el número de equipos en cada dominio de broadcast, al segmentar la red física en redes virtuales.

2. En el caso del escenario real, sin importar el tráfico de red que se haya tenido en la VLAN donde se realizaron las mediciones, es importante tomar en cuenta que ese tráfico no afectará la red entre los nodos ya que los nodos ahora pertenecen a otro dominio de broadcast y ya no se ven afectados por lo que suceda en la VLAN de los clientes.

3. Existen paquetes que son transmitidos con frecuencia con direcciones de broadcast como paquetes DHCP. ARP y STP, pero existe también tráfico de broadcast producido por ataques maliciosos o accidentales, como un equipo switch en mal estado o algún bucle de conexiones entre de switches, que pueden provocar tormentas de broadcast. Este tipo de tráfico puede provocar retrasos en la red, congestionarla e incluso puede colapsarla lo cual requeriría intervención de los componentes afectados y causaría la perdida momentánea de servicio a los usuarios finales. Se debe tomar en cuenta que el riesgo y daño serian aún mayores, si se tiene un gran número de equipos en un mismo dominio de broadcast, configurar VLANs en una red ayudaría a aislar y evitar este tipo de problemas de red.

4. El uso de VLANs puede mantener una red aislada de otros dominios de broadcast, por lo que se puede optimizar el tráfico de dicha red al evitar que fluya tráfico innecesario de otro grupo de equipos.

5. Al implementar VLANs en una red grande, se obtendrá un beneficio económico, al ser una alternativa viable para limitar los dominios de broadcast, se evitaría la compra de routers adicionales para lograr el mismo efecto.

6. La propuesta de segmentar los dominios de broadcast mediante la implementación de VLANs en la red de un proveedor SAI mediante un switch tiene beneficios adicionales que utilizar un router, pues un switch administrable

cuenta con más puertos para configurar VLANs, y al ser una red de un proveedor que tiene tendencia a crecer en cuanto a número de clientes, tener un switch con capacidad de VLANs permitirá crear dominios de broadcast adicionales, y optimizar la red a medida que va creciendo.

7. Se debe tener una planificación adecuada para configurar VLANs en la red, identificar cuáles son los enlaces por los que se desea circule el tráfico de cada VLAN, de manera que afecte lo menos posible el tráfico de otras redes.

RECOMENDACIONES

Las recomendaciones en la implementación de VLANs en una red de SAI son las siguientes

1. Para la implementación óptima de VLANs es necesario realizar una planificación de las subredes que se utilizarán, VLAN IDs a utilizarse, interfaces a configurar y cuáles serán los enlaces tipo troncales de la red.

2. Para configurar VLANs es necesario tener equipos Switches que soporten esta funcionalidad, usando switches tradicionales todos los paquetes de broadcast pasan por cada uno de sus puertos. Al configurar correctamente equipos que soportan VLANs, los broadcasts se pueden segmentar hacia un dominio de broadcast especifico.

3. Configurar una VLAN ID específica para administración de equipos, y vincularla a una de las interfaces del switch

4. Si se desea implementar servicio de telefonía IP, se debe configurar una VLAN específicamente para ese servicio, y así evitar interferencias causadas por broadcast en las llamadas telefónicas, muchos switches tienen configuraciones de VLANs específicas para este escenario.

5. Es recomendable contar con una aplicación o sistema de monitoreo dentro de una red de proveedor SAI. Es de gran utilidad tener una herramienta que permita analizar el tráfico e identificar cualquier error de la red, especialmente para redes grandes. Adicionalmente, las herramientas utilizadas para las mediciones en este estudio cuentan con muchas funciones útiles para la verificación de la configuración de red a medida que se realizan cambios en la red.

6. Mediante listas de acceso, es posible bloquear la comunicación entre VLANs dentro del router, esto se puede configurar para impedir que un grupo de usuarios puedan acceder a las redes de otro grupo de usuarios en la misma red.
7. Contar con políticas de frecuencia de cambio claves de administración de los equipos de red por motivos de seguridad.

8. Para evitar excesos de paquetes de broadcast en la red, como en el caso presentado en este documento, es recomendable no tener un tiempo muy bajo de concesión de direcciones IPs dentro del servicio de DHCP, se debe considerar la frecuencia de conexión de los equipos nuevos en la red para determinar el tiempo óptimo de concesión.

9. Wireshark es una herramienta muy útil para verificar si una VLAN se encuentra configurada correctamente, es una práctica recomendable realizar una medición una vez configurada la VLAN para verificar que el tráfico fluye correctamente.

10. Configurar varias VLAN en una red puede ser un trabajo muy meticuloso, por lo que es recomendable tener documentada toda la red y su configuración en el mayor detalle posible, y mantener esta documentación siempre actualizada cada vez que se realice algún cambio en la red. Esto facilitará en gran medida los futuros cambios en la red.

11. El router Zyxel Zywall USG110 que fue utilizado para el escenario de estudio tienen una limitante, sólo soporta un número máximo de 16 VLANs, si se desea tener la opción a futuro de implementar un mayor número de VLANs en la red de clientes, se debería considerar actualizar el equipo a un modelo que soporte más VLANs, como el modelo USG210 o USG310, como se puede observar en documento de especificaciones técnicas en el anexo 2.

BIBLIOGRAFÍA

Aleaga, F. (2016). *Analisis y elaboracion de un plan de optimizacion para los recursos.* Guayaquil: Universidad Salesiana.

Andreu, J. (2014). *Instalación de equipos de red. Configuración (Redes locales).* Editex.

Ávila, A. (2006). *Iniciación a la red Internet.* Madrid: Ideas Propias Editorial.

Bertolin, J. (2018). *Seguridad de la informacion.* Madrid : Diaz de Santos.

Castells, M. (2017). *La era de la información.* Madrdi: Alianza.

Chapelli, L. (2016). *Analisi de red de Wireshark.* Mexico: Limusa.

Chauchan, M. (2017). *Ubuntu Using Hacking.* California: Esic.

Cover, T. (2015). *Canales de broadcast.* Bogota: Norma.

Daimi, K. (2018). *Computer and Network Security Essentials.* Detroit: Springer.

Dangwal, K., & Kumar, V. (2014). Comparative study of EIGRP and RIP using Cisco Packet Tracer. *International Journal of Engineering Sciences & Journal of Computer Science and Information Emerging Technologies (IJESET)*, 6.

Donahue, G. (2011). *Network Warrior.* O'Reilly Media.

Dordoigne, J. (2015). *Redes informacitcas, redes inalambricas.* Madrid: Panorama.

Duggan, M. (2014). *Cisco CCIE Routing and Switching v5.0 Configuration Practice Labs.* Cisco Press.

Dye, M., McDonald, R., & Rufi, A. (2008). *CCNA Exploration Companion Guide.* Indianapolis: Cisco Press.

Fernandez, B. (2015). *Estado actual de euiqpos de respuesta a incidentes de seguridad informatica.* Mexico: Diaz de Santos.

Fiat, A. (2013). *Cifrado de broadcast.* Madrid: Diaz de Santos.

Forouzan, B. (2007). *Data Communications and Networking.* McGraw-Hill.

Frey, J. (2016). *Redes de sensores inalambricos.* Mexico: Esic.

Gallego, J. C. (2015). *FPB - Instalación y mantenimiento de redes para transmisión de datos.* Editex. .

Groth, D. (2002). *Network+ Study Guide.* London: Sybex.

Guagalango, R. (2016). *Evaluacion tecnica de la seguridad informatica.* Guayaquil: ESPE.

Gutierrez, J. (2013). *Protocolos criptograficos.* Mexico: Limusa.

Hackbarth, K., Vogelsang, I., Marcus, J., Rendon Schneir, J., Neu, W. &., Fuentes, F., . . . Plueckebaum, T. (2009). Interconexión en Redes de Siguiente Generación (NGNs). *Estudio para el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL)*. Perú.

Hernández, J. V., & García, R. G. (2013). *Prácticas de Redes de Área Local e Interconexión de Redes.* Valencia: Lulu.

Janitor, & Jakab. (2010). Visual learning tools for teaching/learning computer networks: Cisco networking academy and packet tracer. *Sixth International Conference on Networking and Services.*

Javid, S. (2014). Role of Packet Tracer in learning Computer Networks. *International Journal of Advanced Research in Computer and Communication Engineering*.

Lindse, W. C., & Simon, M. K. (2013). *Telecommunication Systems Engineering.* New York: Courier Corporation.

Llerena, C. (2016). *Implementación de un sistema de monitoreo de servicios de datos e internet.* Guayaquil: Universidad Politecnica del Litoral.

Monter, L., & Rios, D. (2016). *Apuntes de Comunicaciones en Redes - UAEH.* Obtenido de Centro de Innovación para el Desarrollo y la Capacitación en Materiales Educativos - Universidad Autónoma del Estado de Hidalgo: http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro27/index.html

Moro Vallina, M. (2013). *Infraestructuras de redes de datos y sistemas de telefonía.* Madrid: Paraninfo.

Nazumudeen, & Mahendran. (2014). Performance Analysis of Dynamic Routing Protocol Using Packet Tracer. *International Journal of Innovative research in Science*.

Orebaubg, A. (2016). *Kit de herramientas del analizados de protocolo de red.* Madrid: Diaz de Santos.

Pincay, C., & Villagomez, F. (2015). *Estructuración de una red de servicios y transferencias de dinero llamado PAGOTODOYFACIL ubicado en la isla Trinitaria, sector marginal de la ciudad de Guayaquil*. Guayaquil, Guayas, Ecuador.

Ramos, N. (2015). *Seguridad informatica.* Madrid: Esic.

Saez, F. (2014). *Más alla de internet.* Mexico: Novatica.

Valera, B., Prados, J., Ramos, J., & Navarro, J. (2017). *Implementación de mecanismos de mitigación de tormentas de broadcast en redes de área local mediante Redes Definidas por Software.* Valencia: Editorial Universitat Politècnica de València.

Vietes, A. (2015). *Enciclopedia de la seguridad informática.* Madrid: Esic.

ANEXOS

ANEXO A: ABREVIATURAS Y SIMBOLOGIA

AP	Punto de acceso
ARP	Protocolo de resolución de direcciones
ATM	Modo de transferencia asíncrona
CAN	Red de área de campus
CLI	Interfaz de Línea de Comandos
CSIRT	Equipo de Respuesta a Incidentes de Seguridad Informática
DHCP	Protocolo de configuración dinámica de host
DNS	Sistema de nombres de dominio
ETN	Corporaciones Transnacionales
GUI	Interfaz gráfica de usuario
HTTP	Protocolo de transferencia de hipertexto
HTTPS	Protocolo seguro de transferencia de hipertexto
IBM	Corporación de Máquinas de Negocio Internacional
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
IETF	Grupo de trabajo de ingeniería de Internet
IP	Protocolo de Internet
IPFIX	Protocolo de exportación de flujo de información de protocolo de internet
IPX	Intercambio de paquetes interred
ISP	Proveedor de servicios de Internet
LAN	Red de área local
MAC	Control de acceso a medios
MAN	Red de Área Metropolitana
NETBEUI	Interfaz extendida de usuario de NetBIOS
NETBIOS	Sistema de Entrada Salida Básica

OSI	Interconexión de sistemas abiertos
PAN	Red de área personal
PCAP	Captura de paquetes
POP3	Protocolo de oficina de correo
PPP	Protocolo punto a punto
RARP	Protocolo de resolución de direcciones inverso
RIP	Protocolo de Información de Encaminamiento
SAI	Servicios de acceso a internet
SAN	Red de área de almacenamiento
SAP	Protocolo de Aviso de Sesión
SFTP	Protocolo de transferencia de archivos Secure Shell
SLP	Protocolo de ubicación de servicios
SMB	Bloque de mensajes de servidor
SMTP	Protocolo para transferencia simple de correo
SNMP	Protocolo simple de administración de red
SSL	Capa de puertos seguros
TCP	Protocolo de control de transmisión
TI	Tecnologías de la Información
USB	Bus universal en serie
VLAN	Red de área local virtual
VOIP	Voz por Internet
VPN	Red privada virtual
WAN	Red de área amplia
WI-FI	Fidelidad Inalámbrica
WLAN	Red de área local inalámbrica
WMI	Instrumentación de administración Windows

ANEXO B CONFIGURACIÓN GLOBAL DE ROUTERN1 PARA PROPUESTA DE VLANS EN PACKET TRACER

Dentro de la interfaz de línea de comandos del RouterN1 dentro de la red de simulación de VLANs en packet tracer, se tiene la configuración global presentada a continuación:

```
RouterN1#show running-config
Building configuration...

Current configuration : 2459 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname RouterN1
!
!
!
!
!
ip dhcp pool dhcp-pool-vlan11
network 192.168.11.0 255.255.255.0
default-router 192.168.11.1
dns-server 220.220.220.220
ip dhcp pool dhcp-pool-vlan12
network 192.168.12.0 255.255.255.0
default-router 192.168.12.1
dns-server 220.220.220.220
ip dhcp pool dhcp-pool-vlan13
network 192.168.13.0 255.255.255.0
default-router 192.168.13.1
dns-server 220.220.220.220
ip dhcp pool dhcp-pool-vlan14
network 192.168.14.0 255.255.255.0
default-router 192.168.14.1
dns-server 220.220.220.220
ip dhcp pool dhcp-pool-vlan15
network 192.168.15.0 255.255.255.0
default-router 192.168.15.1
dns-server 220.220.220.220
```

```
ip dhcp pool dhcp-pool-vlan16
network 192.168.16.0 255.255.255.0
default-router 192.168.16.1
dns-server 220.220.220.220
ip dhcp pool dhcp-pool-vlan17
network 192.168.17.0 255.255.255.0
default-router 192.168.17.1
dns-server 220.220.220.220
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
!
interface GigabitEthernet0/0/0.11
encapsulation dot1Q 11
ip address 192.168.11.1 255.255.255.0
!
interface GigabitEthernet0/0/0.12
encapsulation dot1Q 12
ip address 192.168.12.1 255.255.255.0
!
interface GigabitEthernet0/0/0.13
encapsulation dot1Q 13
ip address 192.168.13.1 255.255.255.0
!
interface GigabitEthernet0/0/0.14
encapsulation dot1Q 14
ip address 192.168.14.1 255.255.255.0
!
interface GigabitEthernet0/0/0.15
encapsulation dot1Q 15
ip address 192.168.15.1 255.255.255.0
!
interface GigabitEthernet0/0/0.16
encapsulation dot1Q 16
```

```
ip address 192.168.16.1 255.255.255.0
!
interface GigabitEthernet0/0/0.17
encapsulation dot1Q 17
ip address 192.168.17.1 255.255.255.0
!
interface GigabitEthernet0/0/1
ip address 192.168.240.11 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router rip
network 192.168.11.0
network 192.168.12.0
network 192.168.13.0
network 192.168.14.0
network 192.168.15.0
network 192.168.16.0
network 192.168.17.0
network 192.168.240.0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

ANEXO C CARACTERÍSTICAS ROUTER MARCA ZYXEL MODELOS USGX10

Specifications

Model	USG110	USG210	USG310
Product photo			
Hardware Specifications			
Interfaces	4 x LAN/DMZ, 2 x WAN, 1 x OPT	4 x LAN/DMZ, 2 x WAN, 1 x OPT	8 x GbE(configurable)
USB ports	2	2	2
Console port	Yes (DB9)	Yes (DB9)	Yes (DB9)
Rack-mountable	Yes	Yes	Yes
Fanless	-	-	-
System Capacity & Performance*1			
SPI firewall throughput (Mbps)*2	1600	1,900	5000
VPN throughput (Mbps)*3	400	500	650
IDP throughput (Mbps)*4	590	660	900
AV throughput (Mbps)*4	450	500	550
UTM throughput (AV and IDP)*4	450	500	550
Max. TCP concurrent sessions*5	150,000	200,000	500,000
Max. concurrent IPsec VPN tunnels*6	100	200	300
Concurrent SSL VPN users (default/max.)*7	25 / 150	35/150	50/150
VLAN interface	16	32	64
Concurrent devices logins (default/max.)*7*8	200/300	200/300	500 / 800
WLAN Management			
Managed AP number (default/max.)*7	2/34	2/34	2/34
Security Service			
Anti-Virus (AV)*7	Yes	Yes	Yes
Intrusion Detection and Prevention (IDP) & Application Patrol*7	Yes	Yes	Yes
Anti-Spam*7	Yes	Yes	Yes
Content Filtering (CF 2.0)*7*9	Yes	Yes	Yes
Key Features			
VPN	IKEv2, IPSec, SSL, L2TP/ IPSec	IKEv2, IPSec, SSL, L2TP/ IPSec	IKEv2, IPSec, SSL, L2TP/ IPSec
SSL (HTTPS) inspection	Yes	Yes	Yes
EZ Mode	-	-	-
Hotspot Management*7	Yes	Yes	Yes
Ticket printer support*10 / Support Q'ty (max.)	Yes (SP350E) / 10	Yes (SP350E) / 10	Yes (SP350E) / 10
Amazon VPC	Yes	Yes	Yes
Facebook WiFi	Yes	Yes	Yes
Device HA Pro	Yes*7	Yes*7	Yes*7
Link Aggregation (LAG)	-	-	Yes

ANEXO D CARACTERÍSTICAS SWITCH ZYXEL MODELOS GS1900

Specifications

Model		GS1900-8	GS1900-8HP	GS1900-10HP	GS1900-16	GS1900-24E
Product name		8-port GbE Smart Managed Switch	8-port GbE Smart Managed PoE Switch	8-port GbE Smart Managed PoE Switch with GbE Uplink	16-port GbE Smart Managed Switch	24-port GbE Smart Managed Switch
						
Port Density						
10/100/1000BASE-T, fixed		8	-	-	16	24
10/100/1000BASE-T, PoE, fixed		-	8	8	-	-
SFP 100/1000 Mbps		-	-	2	-	-
Performance						
Switching capacity (Gbps)		16	16	20	32	48
Forwarding rate (Mpps)		11.9	11.9	14.88	23.8	35.7
Packet buffer (byte)		525 K	525 K	525 K	525 K	525 K
MAC address table		8 K	8 K	8 K	8 K	8 K
Jumbo frame (byte)		9 K	9 K	9 K	9 K	9 K
Power						
Input		100 - 240 V AC, 50/60 Hz	100 - 240 V AC, 50/60 Hz	100 - 240 V AC, 50/60 Hz	100 - 240 V AC, 50/60 Hz	100 - 240 V AC, 50/60 Hz
Max. power consumption (watt)		6.2	84.3	96.2	10.5	15.1
PoE power budget (watt)		-	70	77	-	-
Physical Specifications						
Item	**Dimensions (WxDxH) (mm/in.)**	250 x 104 x 27/ 9.84 x 4.10 x 1.06	250 x 104 x 27/ 9.84 x 4.10 x 1.06	250 x 104 x 27/ 9.84 x 4.10 x 1.06	216 x 133 x 42/ 8.50 x 5.23 x 1.65	267 x 162 x 42/ 10.51 x 6.37 x 1.65
	Weight (kg/lb.)	0.65/1.43	0.71/1.57	0.72/1.59	0.97/2.13	1.56/3.44
Packing	**Dimensions (WxDxH) (mm/in.)**	302 x 227 x 64/ 11.89 x 8.94 x 2.52	302 x 227 x 64/ 11.89 x 8.94 x 2.52	302 x 227 x 64/ 11.89 x 8.94 x 2.52	325 x 223 x 71/ 12.80 x 8.78 x 2.80	325 x 223 x 71/ 12.80 x 8.78 x 2.80
	Weight (kg/lb.)	1.04/2.30	1.51/3.33	1.53/3.37	1.80/3.97	2.05/4.52
Included accessories		• Power adapter • Wall mount kit	• Power cord • Power adapter • Wall mount kit	• Power cord • Power adapter • Wall mount kit	• Power cord • Wall mount kit • Rack mounting kit	• Power cord • Wall mount kit • Rack mounting kit
Green Feature						
Fanless		Yes	Yes	Yes	Yes	Yes
Environmental Specifications						
Operating temperature		0°C to 50°C/ 32°F to 122°F	0°C to 50°C/ 32°F to 122°F	0°C to 50°C/ 32°F to 122°F	0°C to 50°C/ 32°F to 122°F	0°C to 50°C/ 32°F to 122°F
Storage temperature		-40°C to 70°C/ -40°F to 158°F	-40°C to 70°C/ -40°F to 158°F	-40°C to 70°C/ -40°F to 158°F	-40°C to 70°C/ -40°F to 158°F	-40°C to 70°C/ -40°F to 158°F
Operating humidity		10% to 95% (non-condensing)	10% to 95% (non-condensing)	10% to 95% (non-condensing)	10% to 95% (non-condensing)	10% to 95% (non-condensing)
Storage humidity		10% to 95% (non-condensing)	10% to 95% (non-condensing)	10% to 95% (non-condensing)	10% to 95% (non-condensing)	10% to 95% (non-condensing)
MTBF (hr)		862,561	926,199	801,113	843,668	804,714
Heat dissipation (BTU/hr)		21.14	48.763	65.472	35.81	51.49
Acoustic noise (dBA)		0	0	0	0	0