UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA DE SISTEMAS Y ADMINISTRACIÓN DE EMPRESAS

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS

ARQUITECTURA DE RED BASADO EN EL MODELO JERÁRQUICO DE TRES CAPAS PARA MEJORAR EL TRÁFICO DE DATOS EN LA UNIVESIDAD NACIONAL TECNOLÓGICA DE LIMA SUR.

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER

LEON GAVINO, IVAN SANTOS

Villa el Salvador

2016

DEDICATORIA

A toda mi familia, por sus palabras de aliento y sus buenos deseos, especialmente a mi madre Andrea Gavino Flores, por todo su apoyo comprensión y sacrificio.

AGRADECIMIENTO

A Dios por haberme acompañado y cuidado a lo largo de toda mi carrera.

Al Ing. Hernán Cusi Chirapo por la orientación profesional que me brindo en el desarrollo de este proyecto. Además al Ing. Juan Ibarra, encargado de la jefatura de la Oficina de desarrollo de Tecnologías de la Información y Comunicación (ODTIC), por facilitarme los medios para el desarrollo del presente trabajo.

A la Universidad Nacional Tecnológica de Lima Sur que me ha permitido estudiar y ser un profesional.

ÍNDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS

INTRODUCCIÓN

En los últimos años, las redes de datos se han convertido en un factor muy importante para cualquier organización, es indudable el impacto social, económico y cultural que ha generado esta tecnología en nuestros tiempos.

Bajo este panorama en la actualidad las computadoras, el software, los protocolos y equipos de comunicación deben estar correctamente implementados y configurados para maximizar el rendimiento y la seguridad en las redes de datos.

Además, avances en las arquitecturas de redes, protocolos, servicios y tecnologías de acceso al medio, han sido utilizados en los sistemas de comunicación. Sin embargo algunos de estas ventajas no han sido aplicadas en esta institución, debido a la falta de iniciativa y los problemas de interoperabilidad entre los equipos existentes.

Actualmente la Universidad Nacional Tecnológica de Lima Sur no cuenta con una arquitectura de red bien definida, para tener el alto rendimiento a la hora de prestar servicios, tampoco está definida la seguridad de la red ya que esta debe estar implementada tanto en lo físico y lógico.

Ante esto, se necesita una infraestructura de red mucho más específica que cumpla con las características de una arquitectura de red estándar con la finalidad de satisfacer las expectativas de los usuarios finales.

Debido a ello, nace la propuesta de la arquitectura de red basado en el modelo jerárquico de tres capas para mejorar el tráfico de datos, con lo cual se busca mejorar la red conjunta y organizar el tráfico de datos de la universidad para responder a la congestión, seguridad y los cambios en el modelo de tráfico a implementarse en un futuro.

CAPÍTULO I:

PLANTEAMIENTO DEL PROBLEMA

1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

La universidad Nacional Tecnológica de Lima sur, viene funcionando desde hace diez años. Inicialmente contaba con una sola edificación que actualmente es el pabellón “A”, donde funcionaban las oficinas, biblioteca y laboratorios de cómputo. Debido a esto se planteó una topología de red básica para interconectar todas las áreas.

En la actualidad la universidad cuenta con una arquitectura de red diseñada y administrada con equipos propios del Proveedor de Servicios de Internet (ISP), bajo los términos de un contrato entre el proveedor y la universidad.

Puesto que la institución cuenta con una gran cantidad de computadoras conectadas a la red, ya sea de forma alámbrica o inalámbrica en los distintos pabellones dentro del campus, además el flujo masivo de usos de computadoras portátiles y equipos móviles que se conectan a la señal inalámbrica de la biblioteca durante todo el día. Esto genera un gran congestionamiento de tráfico de red (Degradación de la tasa de transferencia) debido a un direccionamiento ineficiente y una arquitectura mal definida.

Las causas que generan la congestión son:

- Diseño de red en clase C que origina una gran congestión de paquetes de mensajes de difusión causando que la red se vuelva lenta y reduzca el ancho de banda.
- La interconexión de equipos de comunicaciones entre el emisor y el receptor con cables UTP rectas que superan los límites establecidos.
- Falta de uso de estándares y normas generales para un diseño de red de campus.
- Ausencia de protocolos y servicios de calidad que distribuyan de manera eficiente el tráfico de datos. Debido que en la actualidad no basta con contar con un balanceador de ancho de banda.

En vista a la gran cantidad de departamentos administrativos, la red cuenta con VLANs creadas para cada uno de ellos y la asignación de IPs se da a través del protocolo DHCP, esto genera malestar entre los administrativos a la hora de empezar sus funciones diarias, debido que la IP correspondiente a su PC, es tomada por otro equipo externo (sea laptop, Tablet o Smartphone). Sucede porque se ha instalado un Access Point para emitir señal WiFi, sin autorización de la ODTIC. Debido a esto la cantidad de IPs asignadas para la respectiva área se reduce y la vez genera un gran congestionamiento de red, el 78% de los encuestados manifestó que tenía que lidiar frecuentemente con el icono amarillo, esto se debe a dos razones: El primero es porque no se tiene acceso al internet, por motivos de caída de algún equipo comunicación, la segunda sucede porque no cuenta con una dirección IP o existe duplicidad de IPs.

Además de esto el proveedor de servicios (ISP), proporciona la cantidad de 34 megas de internet, para la institución y esto no está reflejado a la hora de hacer uso de los equipos de acceso. Esto se debe a una configuración de red ineficiente, ya que balanceador de ancho de banda está proporcionando equitativamente los paquetes para cada VLAN para el consumo de datos. Cabe resaltar que el 78% de los usuarios encuestados afirma que la red es muy lenta, solo el 4% afirmó que la red tiene un comportamiento moderado a la hora de usar el acceso a internet (Véase en el anexo 1, resultados de la encuesta).

A analizar los datos capturados por el software Wireshark, se realizó un filtro de los 10 protocolos más frecuentes en los paquetes que circulan por la red de la Universidad.

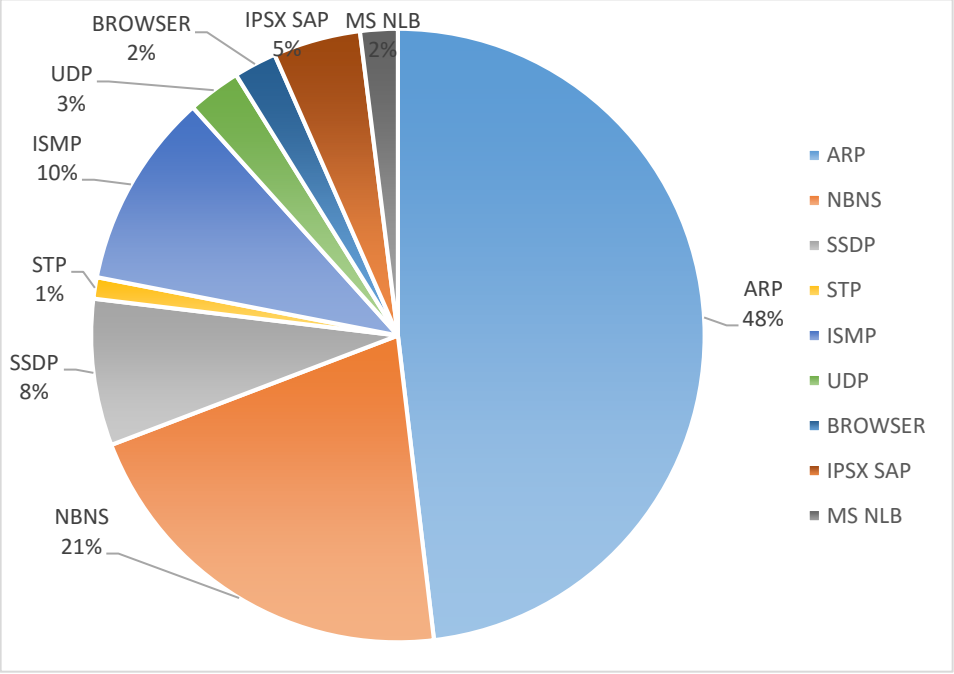


Figura 1-1: Principales protocolos que circulan por la red de datos de la UNIVERSIDAD.

Fuente: Elaboración propia, con los datos capturados desde 25 al 30 de junio 2016

Como se aprecia en la figura 1-1, existe un alto porcentaje de ocurrencias del protocolo ARP y, este protocolo en un promedio del 97% es Broadcast (difusión). La acumulación de tráfico de Broadcast y Multicast de cada dispositivo en la red se denomina radiación de Broadcast. En ocasiones la circulación de radiación de Broadcast puede saturar la red, como consecuencia no hay ancho de banda disponible para los datos de aplicaciones.

Según los estándares de cisco, cuando el Broadcast supera el límite de 35% se considera que la red es plana y sus recursos están siendo desperdiciados en mensajes de difusión (Broadcast) que congestionan la red innecesariamente.

Otro gran problema es la seguridad de la red, ya que con el crecimiento de la internet, lo que se asumía que las redes eran seguras y controladas a través de usuarios autorizados, asignación de contraseñas, comprar un equipo firewall o su equivalente, no proporcionarían seguridad eficiente, ya que en la actualidad con esto no basta para tener una seguridad confiable y oportuna. El 67% de los encuestados afirmaron haber perdido información en alguna ocasión desde sus equipos, también 37% manifiesta que en alguna oportunidad pudo ingresar a equipos que no lo pertenecen.

De igual forma la arquitectura de red actual, no cuenta con un plan de contingencia ante cualquier evento que se genere (averías de switch, router o los equipos de seguridad instaladas), por motivos que no se planificó en la infraestructura inicial.

La red actualmente cuenta con una topología en estrella basada en los siguientes parámetros de direcciones:

- Dirección de Red 192.168.10.0
- Mascara 255.255.255.0
- Host 256.

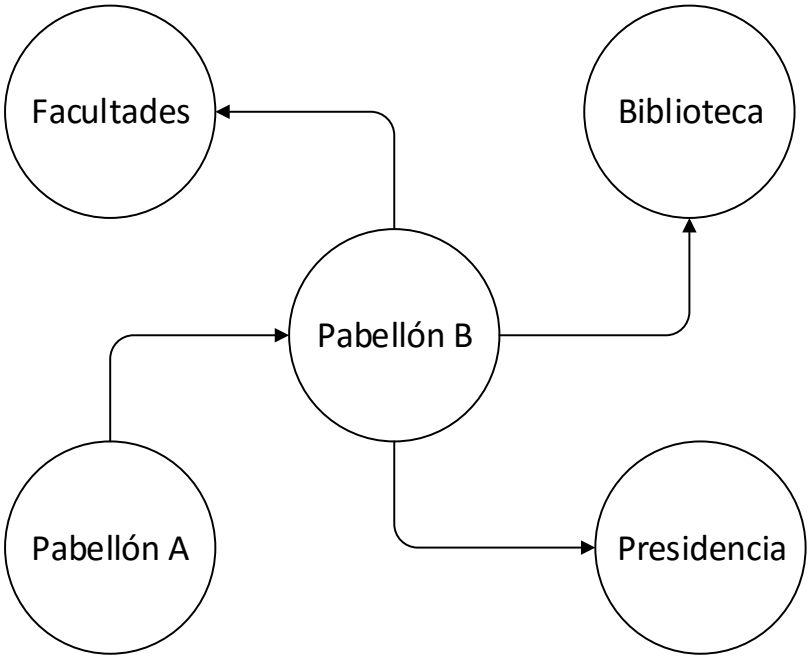


Figura 1-2: Topología en estrella de la UNTELS.

Fuente: Elaboración Propia.

Esta distribución permite que todos los nodos de la red se conecten a un solo concentrador que se encuentra el pabellón B, los datos de este fluyen del emisor hasta el concentrador por lo que ocasionan que se alarguen los tiempos de respuesta de los servicios que ofrece la red, además un fallo en concentrador provoca el aislamiento de todos los nodos que a el están conectados.

1.2. JUSTIFICACIÓN DEL PROYECTO

La Universidad Nacional Tecnológica de Lima Sur, a sus pocos años de iniciar su funcionamiento ya cuenta con gran prestigio entre todas las universidades existentes a nivel de Lima Sur. Por ello debe contar con una red de alto rendimiento y seguridad a la hora prestar servicios y más importante aún, una buena relación costo – rendimiento.

Esta propuesta presentará una arquitectura de red basada en el modelo jerárquico de tres capas propuesta por Cisco, para diseño de redes LAN. Para proporcionar un transporte eficiente y tolerante a fallas que pueda diferenciar el tráfico de aplicaciones para tomar decisiones inteligentes sobre el uso compartido de cargas cuando la red está temporalmente congestionada. Independientemente de que el acceso a la red de un usuario sea por cable o inalámbrico, la red ofrecerá priorización inteligente y colas de tráfico junto con las rutas más eficientes posibles a través de las diferentes capas que maneja.

Los resultados obtenidos en esta investigación beneficiaran a la comunidad universitaria permitiendo tener una mejor disponibilidad de ancho de banda para cada uno de los equipos de acceso a la red, aportando seguridad y confiabilidad. Además permitirán comprender nuevas soluciones tecnológicas en el área de administración de redes, porque estos hoy en día constituyen un recurso importante como soporte logístico sea cual fuere el área de servicio, por lo que ha pasado a formar parte de una línea de negocio muy importante en área de TI para cualquier organización.

En conclusión esta propuesta, estará diseñada con una adecuada topología, velocidad, costo, seguridad, disponibilidad, escalabilidad y fiabilidad para tener un alto rendimiento y seguridad en la red de la universidad.

1.3. DELIMITACIÓN DEL PROYECTO

1.3.1. Espacial

La investigación se desarrollará en el campus de la Universidad Nacional Tecnológica de Lima Sur.

1.3.2. Temporal

El periodo bajo estudio comprende desde:

Inicio: 4 de abril 2016

Término: 31 de julio de 2016

1.3.3. Conceptual

Direccionamiento.

En una red de datos se requiere la identificación de los usuarios que participan en la conexión mediante las direcciones de origen y destino. Estas direcciones pueden ser físicas o lógicas. El direccionamiento provoca una característica denominada Latencia: Un switch no puede direccionar un paquete hasta recibir el campo de control de errores y verificar su correcto estado.

Dirección IP

La dirección IP es el identificador de cada nodo dentro de su red. Cada nodo conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host. En el caso de Internet, no puede haber dos computadores con 2 direcciones IP

(públicas) iguales. Pero sí podríamos tener dos computadores con la misma dirección IP siempre y cuando pertenezcan a redes independientes entre sí. Las direcciones IP se clasifican en: direcciones IP públicas, direcciones IP privadas (reservadas).

Máscara de Red

Una máscara de red o máscara de subred es aquella dirección que enmascarando la dirección IP, nos indica si otra dirección IP pertenece a nuestra subred o no, es decir, nos sirve para separar los bits de identificación de red (van bits en 1) y los bits de identificación de hosts (van bits en 0).

Segmentación de red

Una de las cuestiones a la que las empresas no suelen prestar especial atención es a la red de comunicaciones interna. Segmentar y dimensionar tu red LAN de comunicaciones puede ayudar a resolver muchos de los problemas que se producen a nivel de comunicaciones en las empresas. Para ello es imprescindible identificar que departamentos requieren un mayor ancho de banda para trabajar y medir el flujo de datos de la red interna.

Gestión de red

La gestión de red describe como el sistema, incluyendo las otras funciones de la red se controla y gestiona. Este consiste en un modelo de información que describe los tipos de datos que se utilizan para controlar y gestionar cada uno de los elementos del sistema, los mecanismos para conectar los dispositivos con el fin de gestionar los flujos de datos a

través de la red. Los mecanismos de administración de red incluyen la supervisión y recopilación de datos a través los instrumentos para acceder, transmitir, actuar y modificar los datos.

Seguridad

La seguridad es un requisito para garantizar la confidencialidad, integridad y disponibilidad del usuario, la aplicación, los dispositivos y redes de información. La seguridad describe como los recursos del sistema se encuentran protegidos contra robos, daños, denegación de servicios (DoS) o acceso no autorizado. La seguridad se implementa en regiones o zonas de seguridad que representan un determinado nivel de sensibilidad y control de acceso.

Router.

Funciona en el ámbito de capa 3 y por ello requiere un análisis del protocolo Internet IP. Debe soportar distintos tipos de protocolos; por ejemplo TCP/IP, DECnet, IPX (Novell), AppleTalk, XNS (Xerox). Interconectan LAN entre sí o una LAN con WAN (X.25, Frame Relay, ATM). Permiten mejorar la eficiencia de la red ya que toleran distintos caminos dentro de la red. El Router puede segmentar datagramas muy largos en caso de congestión, en cambio no pueden ensamblar datagramas. Un router se utiliza muchas veces como conversor de interfaz (LAN hacia G.703 para 2 Mb/s o V.35 para Nx64 kb/s). Los router se pueden interconectar a alta velocidad mediante interfaces de 100 Mb/s (mediante pares o fibra óptica) y 1000 Mb/s (mediante Gigabit Ethernet) para formar redes de alta velocidad. En este caso el medio de transporte entre router es una conexión LAN extendida (MAN). Normalmente el

protocolo IP usado en una LAN puede ser transportado mediante una red SDH, una red ATM o directamente sobre interfaz LAN por fibra óptica. Cuando la estructura de red usada es la descripta se observa una unión entre el concepto de switch LAN y router.

Switch

El switch funciona en el ámbito de capa 2 (MAC), procesan las direcciones MAC en una LAN y no modifican el contenido del paquete. Inspecciona la dirección de fuente y destino del paquete para determinar la ruta de conmutación. La tabla de rutas se realiza mediante un compilador de direcciones MAC. La misma es dinámica y se actualiza sobre la base de la lectura de las direcciones contenidas en los paquetes que ingresan al switch. Cuando un switch recibe un paquete con dirección desconocida lo emite a todas las puertas (técnica conocida como Flooding).

Switch de capa 3

Se entiende por switch de capa 3 al equipo que realiza la operación de enrutamiento mediante acciones de hardware; en tanto que es un router cuando las mismas se realizan mediante acciones de software. El switch de capa 3 se fundamenta en circuitos custom del tipo ASIC (Application-Specific Integrated Circuit). Una diferencia de importancia entre un switch y un router es que este último permite optimizar la ruta cuando la red es muy grande. Permite además disponer de caminos alternativos y reconfigurar la tabla de rutas.

Ether – channel

Una redundancia interesante se logra mediante la función Ether-channel. En este caso dos switch pueden ser unidos mediante líneas paralelas con tráfico distinto. De esta forma, en caso de corte una sola línea abastece al medio, reduciendo la performance pero manteniendo el servicio.

DHCP (Dynamic Host Configuration Protocol).

El protocolo DHCP fue diseñado por el IETF (standard en RFC-2131) para reducir los requerimientos de configuración. Además de asignar la dirección IP realiza una configuración automática de los parámetros necesarios para funcionar en la red donde se encuentra. DHCP trabaja sobre TCP y está basado en el protocolo BOOTP (Bootstrap Protocol) de RFC-0951, con algunas diferencias. Se utiliza un modelo Client/Server por lo que se dispone de uno o varios servidores DHCP. No se requiere de un servidor por subred por lo que el protocolo DHCP debe trabajar a través de Router. Más de un servidor pueden realizar las tareas de asignación de direcciones con el propósito de mejorar la eficiencia del sistema.

Vlan (Red de área local virtual o LAN virtual).

Una VLAN es una red de área local que agrupa un conjunto de equipos de manera lógica y no física. Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento de equipos según determinados criterios (direcciones MAC, números de puertos, protocolo, etc.).

1.4. FORMULACIÓN DEL PROBLEMA

¿De qué manera la arquitectura de red basada en el modelo jerárquico de tres capas mejorará el tráfico de datos en la Universidad Nacional Tecnológica de Lima Sur?

1.5. OBJETIVOS

1.5.1. Objetivos General

Implementar una arquitectura de red basado en el modelo jerárquico de tres capas en la Universidad Nacional Tecnológica de Lima Sur.

1.5.2. Objetivos específicos

- Determinar el estado actual de la red de datos existentes.
- Realizar el estudio detallado del modelo de red jerárquico de tres capas para diseño de la red LAN cableada de campus.
- Crear VLANs, para las diferentes áreas o jefaturas con el fin incrementar la seguridad y el rendimiento de la red.
- Diseñar la arquitectura de red de datos de acuerdo al modelo propuesto.

CAPÍTULO II:

MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN.

SIDNEI DE OLIVERA GUERRA, en su tesis “UNA PROPUESTA DE ARQUITECTURA MPLS/DIFFSERV PARA PROVEER MECANISMOS DE CALIDAD DE SERVICIO (QoS) EN EL TRANSPORTE DE LA TELEFONIA IP”, menciona que una arquitectura de red, debe proporcionar eficiencia, fiabilidad, escalabilidad y supervivencia orientada a la comunicación. Además dicha arquitectura de red debe responder de manera favorable, a la congestión y los cambios en el modelo de tráfico para los servicios, proporcionando eficiencia en la entrega de paquetes en tiempo real.

También menciona que una arquitectura propuesta debe tener una política de gestión que garantice la factibilidad de la red, para un perfil de tráfico determinado de manera que se pueda disponer de recursos de red suficientes con niveles aceptables de calidad, fiabilidad y supervivencia (Tolerancia a fallos).(Madrid – España 2004).

XAVIER FRANCISCO LOPEZ ANDRADE, en su tesis “REDISEÑO DE LA RED CON CALIDAD DE SERVICIOS PARA DATOS Y TECNOLOGIA DE VOZ

SOBRE IP EN EL ILUSTRE MUNICIPIO DE AMBATO", destaca una metodología que es el diseño de redes de arriba hacia abajo, trabajada básicamente en referencia al modelo OSI, que empieza por la capa superior terminando en la capa inferior que es el nivel físico. Básicamente trata de un diseño con redes virtuales (VLANs) con la posibilidad de incrementar una red voz basada en tecnología IP y reducir la congestión de tráfico. (Ecuador 2008).

MARCELO ALEJANDRO RIFFO GUTIERREZ, en su tesis "VULNERABILIDADES DE LAS REDES TCP/IP Y PRINCIPALES MECANISMOS DE SEGURIDAD", muestra la poca seguridad con que cuenta el modelo TCP/IP, ya que con el manejo de ciertas variables, herramientas o software, se puede establecer una manipulación de servicios asociados a la hora de transmitir los datos, se puede inhabilitar los servicios y crear conflictos en las aplicaciones web. Destaca además que los sistemas Cortafuegos no entregan una respuesta de denegación personalizada, es por ello destaca que se debe insertar los sistemas criptográficos como complemento a los cortafuegos. Porque la criptografía mediante algoritmos y métodos matemáticos puede resolver los problemas de autenticidad, privacidad, integridad en la trasferencia de información. También el objetivo de implementar la criptografía en la red es envió de información secreta usando transformaciones en el mensaje, las cuales se conocen como el cifrado, dicho envío puede ser variable de acuerdo al tipo de cifrado que se utilice, nivel de autenticidad, contraseñas e inserción de protocolos se seguridad a nivel de red y de transporte que permitirán brindar seguridad en una red. (Chile, 2009).

TAYLOR IVAN BARRENECHEA ZAVALA en su tesis “DISEÑO DE UNA RED LAN INALAMBRICA PARA UNA EMPRESA DE LIMA” cabe destacar de esta tesis el estudio de las principales tecnologías y estándar de comunicaciones inalámbricas de la actualidad tales como: IEEE 802.11, en sus especificaciones 802.11a, 802.11b y 802.11g. Permitiendo así mejorar rendimiento del sistema de comunicaciones dentro de una organización, además se debe mencionar la configuración de seguridad para el acceso a la red inalámbrica, en conjunto con las asignaciones de las VLANs en el Switch y las listas de control de acceso en el router principal. Se debe mencionar además el uso del software para la adecuada simulación y diseño de la red LAN que permitieron la correcta ubicación de los equipos inalámbricos basándose en los indicadores emitidos por el software de diseño (Lima, 2009).

MOLINA RUIZ JULIO EDGAR, en su tesis “PROPUESTA DE SEGMENTACION CON REDES VIRTUALES Y PRIORIZACION DEL ANCHO DE BANDA CON QoS PARA LA MEJORA DEL RENDIMIENTO Y SEGURIDAD DE LA RED LAN EN LA EMPRESA EDITORA EL COMERCIO PLANTA NORTE”, destaca la importancia de segmentar las áreas de una institución en subredes para tener una mayor seguridad en la estructura de la red, dicha seguridad debe estar implementada con las listas de accesos(ACL), nivel de autentificación – Radius, además destaca la importancia de mejorar el ancho de banda con calidad de servicio, implementar nuevos protocolos en tecnología CISCO, con el propósito de disminuir los costos y elevar la productividad de la institución que lo implemente.(Chiclayo, 2012).

2.2. BASES TEÓRICAS

2.2.1. Arquitectura de red de datos.

Lo primero que tenemos que saber es, a que nos referimos cuando mencionamos una arquitectura de red, pues bien nos referimos a las tecnologías que admiten la infraestructura, servicios y protocolos que transmiten los mensajes a través de la red, para que esta sea fiable y funcione correctamente. Pues a continuación detallaremos las características básicas que deben cumplir una arquitectura de red bien definida, para su correcto funcionamiento.

2.2.1.1. Tolerante a fallas.

Una red tolerante a fallas es la que limita el impacto de una falla del software o hardware y puede recuperarse rápidamente cuando se produce dicha falla. Estas redes dependen de enlaces o rutas redundantes entre el origen y el destino del mensaje. Si un enlace o ruta falla, los procesos garantizan que los mensajes pueden enrutarse en forma instantánea en un enlace diferente transparente para los usuarios en cada extremo. Tanto las infraestructuras físicas como los procesos lógicos que direccionan los mensajes a través de la red están diseñados para adaptarse a esta redundancia.

2.2.1.2. Escalabilidad

Una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio enviado a los usuarios actuales. Miles de nuevos usuarios y proveedores de servicio se conectan a Internet cada semana. La capacidad de la red de admitir

estas nuevas interconexiones depende de un diseño jerárquico en capas para la infraestructura física subyacente y la arquitectura lógica. El funcionamiento de cada capa permite a los usuarios y proveedores de servicios insertarse sin causar disrupción en toda la red. Los desarrollos tecnológicos aumentan constantemente las capacidades de transmitir el mensaje y el rendimiento de los componentes de la estructura física en cada capa.

2.2.1.3. Calidad de Servicios (QoS)

Internet actualmente proporciona un nivel aceptable de tolerancia a fallas y escalabilidad para sus usuarios. Pero las nuevas aplicaciones disponibles para los usuarios en internetworks crean expectativas mayores para la calidad de los servicios enviados. Las transmisiones de voz y video en vivo requieren un nivel de calidad consistente y un envío ininterrumpido que no era necesario para las aplicaciones informáticas tradicionales. La calidad de estos servicios se mide con la calidad de experimentar la misma presentación de audio y video en persona. Las redes de voz y video tradicionales están diseñadas para admitir un único tipo de transmisión y, por lo tanto, pueden producir un nivel aceptable de calidad. Los nuevos requerimientos para admitir esta calidad de servicio en una red convergente cambian la manera en que se diseñan e implementan las arquitecturas de red.

2.2.1.4. Seguridad

Internet evolucionó de una internetworks de organizaciones gubernamentales y educativas estrechamente controlada a un medio

ampliamente accesible para la transmisión de comunicaciones personales y empresariales. Como resultado, cambiaron los requerimientos de seguridad de la red. Las expectativas de privacidad y seguridad que se originan del uso de internetworks para intercambiar información empresarial crítica y confidencial exceden lo que puede enviar la arquitectura actual. La rápida expansión de las áreas de comunicación que no eran atendidas por las redes de datos tradicionales aumenta la necesidad de incorporar seguridad en la arquitectura de red.

2.2.2. Diseño Jerárquico de la red.

Las redes deben satisfacer las necesidades actuales de las organizaciones y admitir tecnologías emergentes a medida que se adoptan nuevas tecnologías. Los principios y los modelos de diseño de red pueden ayudar a un ingeniero de red a diseñar y armar una red que sea flexible, resistente y fácil de administrar.

2.2.2.1. Requisito de la red.

Cuando se analiza el diseño de red, es útil categorizar las redes según la cantidad de dispositivos que se atienden:

- Red pequeña: proporciona servicios para hasta 200 dispositivos.
- Red mediana: proporciona servicios para 200 a 1000 dispositivos.
- Red grande: proporciona para más de 1000 dispositivos.

Los diseños de red varían según el tamaño y las necesidades de las organizaciones. Por ejemplo, las necesidades de infraestructura de red de una organización pequeña con menos dispositivos son menos complejas

que la infraestructura de una organización grande con una cantidad importante de dispositivos y conexiones.

Existen muchas variables para tener en cuenta al diseñar una red. Tenga en cuenta el ejemplo de la figura 2-1. El diagrama de topología de alto nivel para una red empresarial grande que consta de un campus principal que conecta sitios pequeños, medianos y grandes.

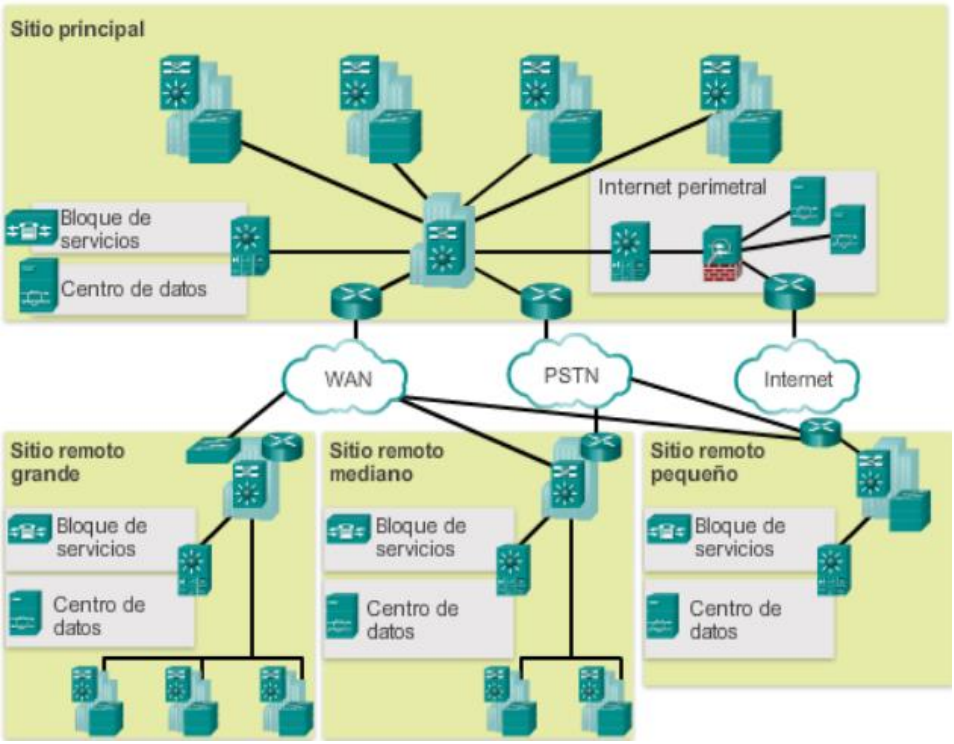


Figura 2-1: Diseño de una arquitectura para red empresarial.

Fuente: Manual de Cisco Certified Design Associate (CCDA)

2.2.2.2. Principios de Ingeniería estructurada.

Independientemente del tamaño o los requisitos de la red, un factor fundamental para la correcta implementación de cualquier diseño de red es seguir buenos principios de ingeniería estructurada. Estos principios incluyen lo siguiente:

- ***Jerarquía:*** un modelo de red jerárquico es una herramienta útil de alto nivel para diseñar una infraestructura de red confiable. Divide el problema complejo del diseño de red en áreas más pequeñas y más fáciles de administrar.
- ***Modularidad:*** al separar en módulos las diversas funciones que existen en una red, esta es más fácil diseñar. Cisco identificó varios módulos, incluido el campus empresarial, el bloque de servicios, el centro de datos e Internet perimetral.
- ***Resistencia:*** la red debe estar disponible para que se pueda utilizar tanto en condiciones normales como anormales. Entre las condiciones normales se incluyen los flujos y los patrones de tráfico normal o esperado, así como los eventos programados, como los períodos de mantenimiento. Entre las condiciones anormales se incluyen las fallas de hardware o de software, las cargas de tráfico extremas, los patrones de tráfico poco comunes, los eventos de denegación de servicio (DoS), ya sean intencionales o involuntarios, y otros eventos imprevistos.
- ***Flexibilidad***: la capacidad de modificar partes de la red, agregar nuevos servicios o aumentar la capacidad sin necesidad de realizar actualizaciones de gran importancia (es decir, reemplazar los principales dispositivos de hardware).

Para cumplir con estos objetivos fundamentales del diseño la red se debe armar sobre la base de una arquitectura de red jerárquica que permita la flexibilidad y el crecimiento.

2.2.3. Diseño Jerárquico de tres capas.

En la topología de redes, un diseño jerárquico implica dividir la red en capas independientes. Cada capa (o nivel) en la jerarquía proporciona funciones específicas que definen su función dentro de la red general. Esto ayuda al diseñador y al arquitecto de red a optimizar y seleccionar las características, el hardware y el software de red adecuada para llevar a cabo las funciones específicas de esa capa de red. Los modelos jerárquicos se aplican al diseño de LAN y WAN. Un diseño típico de red LAN jerárquica de campus incluye las siguientes tres capas:

- Capa de acceso: proporciona acceso a la red para los grupos de trabajo y los usuarios.
- Capa de distribución: proporciona una conectividad basada en políticas y controla el límite entre las capas de acceso y de núcleo.
- Capa de núcleo: proporciona un transporte rápido entre los switches de distribución dentro del campus empresarial.

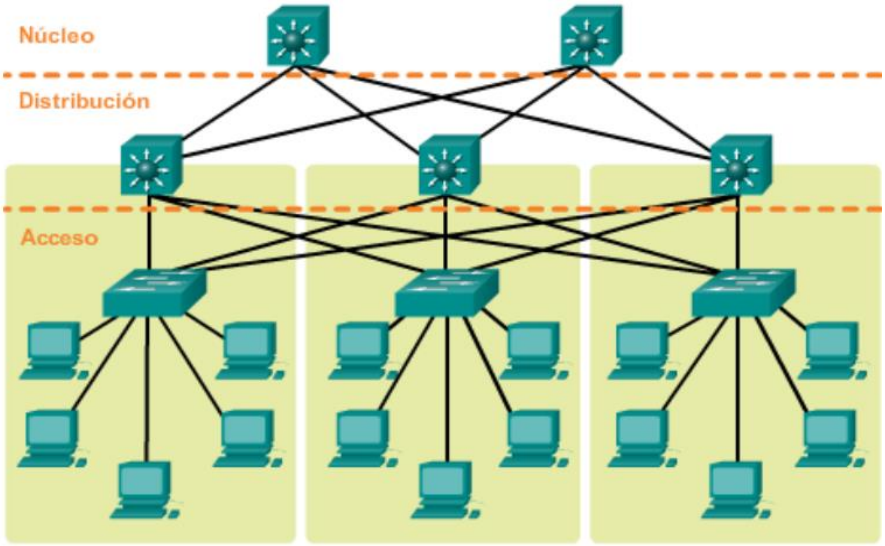


Figura 2-2: Diseño Jerárquico de Red.

Fuente: Manual de Cisco Certified Design Associate (CCDA).

El beneficio de dividir una red plana en bloques más pequeños y fáciles de administrar es que el tráfico local sigue siendo local. Sólo el tráfico destinado a otras redes se traslada a una capa superior.

Los dispositivos de Capa 2 en una red plana brindan pocas oportunidades de controlar broadcasts o filtrar tráfico no deseado. A medida que se agregan más dispositivos y aplicaciones a una red plana, los tiempos de respuesta se degradan hasta que la red queda inutilizable.

Cada capa ofrece una funcionalidad diferente y funcionalidad para la red. Según las características del sitio de implementación, es posible que necesite una, dos o las tres capas. Por ejemplo, un sitio que ocupa un solo edificio puede necesitar solamente las capas de acceso y distribución. Pero si la organización es lo suficientemente grande, es posible que su red necesite las capas de acceso, distribución y central, a pesar de encontrarse todo en un solo edificio.

Un campus de varios edificios probablemente necesitará las tres capas.

2.2.3.1. Capa de acceso.

La capa de acceso es por donde los dispositivos controlados por el usuario, dispositivos accesibles al usuario y otros dispositivos terminales se conectan a la red. La capa de acceso ofrece conectividad tanto inalámbrica como por cable y contiene características y servicios para garantizar seguridad y recuperabilidad para toda la red.

- ***Conectividad de dispositivos:*** la capa de acceso ofrece conectividad de dispositivos con ancho de banda de alta velocidad. A

fin de hacer de la red una pieza transparente del trabajo diario del usuario final, la capa de acceso debe poder admitir ráfagas de tráfico de ancho de banda de alta velocidad cuando los usuarios realizan tareas de rutina, como enviar correos electrónicos pesados o abrir un archivo desde una página web interna. Debido a que muchos tipos de dispositivos de los usuarios finales se conectan a la capa de acceso (equipos personales, teléfonos IP, puntos de acceso inalámbricos, y cámaras de video vigilancia mediante IP), la capa de acceso puede admitir muchas redes lógicas, con lo cual ofrece los beneficios de rendimiento, administración y seguridad.

- ***Servicios de seguridad y recuperabilidad:*** El diseño de la capa de acceso debe garantizar que la red esté disponible para todos los usuarios que la necesitan, cuando la necesitan. Como punto de conexión entre la red y los dispositivos clientes, la capa de acceso debe ayudar a proteger la red contra errores humanos y ataques maliciosos. Esta protección incluye garantizar que los usuarios tengan acceso solamente a servicios autorizados, con lo cual se evita que los dispositivos de usuario final se apoderen del rol de otros dispositivos en la red y, cuando es posible, se verifica que todos los dispositivos de usuario final están permitidos en la red.
- ***Funcionalidades de tecnología avanzada:*** La capa de acceso ofrece un conjunto de servicios de red que admiten tecnologías avanzadas, como voz y video. La capa de acceso debe ofrecer acceso especializado para los dispositivos mediante el uso de tecnologías avanzadas, para garantizar que el tráfico de estos dispositivos no se

vea afectado por el tráfico de otros dispositivos y, además, para garantizar la distribución eficiente del tráfico que necesitan muchos dispositivos en la red.

- ***Plataformas de capa de acceso.***

  La Guía de diseño para la tecnología LAN por cable en campus es compatible con los siguientes switches de Cisco como plataformas de capa de acceso:

  - Switches Cisco Catalyst de la serie 2960-S.
  - Switches Cisco Catalyst de la serie 2960-X.
  - Switches Cisco Catalyst de la serie 3560-X.
  - Switches Cisco Catalyst de la serie 3750-X.
  - Switches Cisco Catalyst de la serie 3650.
  - Switches Cisco Catalyst de la serie 3850.
  - Switches Cisco Catalyst de la serie 4500E.

2.2.3.2. Capa de distribución.

La capa de distribución admite muchos servicios importantes. En una red donde la conectividad debe atravesar la LAN completa, ya sea entre distintos dispositivos de la capa de acceso o desde un dispositivo de la capa de acceso a la WAN, la capa de distribución hace posible esta conectividad.

- ***Escalabilidad:*** en cualquier sitio con más de dos o tres dispositivos de capa de acceso, no resulta práctico interconectar todos los

switches de acceso. La capa de distribución sirve como un punto de agregación para múltiples switches de la capa de acceso.

La capa de distribución puede reducir los gastos operativos haciendo que la red sea más eficiente, exigiendo menos cantidad de memoria, creando dominios de falla que compartimenten las fallas o los cambios en la red y procesando los recursos para dispositivos en cualquier otro lado en la red. La capa de distribución también aumenta la disponibilidad de red gracias a que contiene las fallas en dominios más pequeños.

- ***Reducción de la complejidad y aumento de la recuperabilidad:*** La capa de distribución simplificada, en la cual un nodo de la capa de distribución se compone de una entidad lógica individual que puede implementarse usando un par de switches físicamente separados que funcionan como un dispositivo, o bien usando una pila física de switches que funcionan como un dispositivo. La recuperabilidad la aportan los componentes físicamente redundantes, como fuentes de alimentación, supervisores y módulos, así como también la conmutación activa para los planos de control lógico redundantes.
- ***Diseño de dos capas:*** La capa de distribución ofrece conectividad para los servicios basados en la red para la WAN y para el perímetro de Internet. Los servicios basados en la red pueden incluir y no se limitan a los Servicios de aplicaciones de área amplia (WAAS) y a los controladores LAN inalámbricos. Según las dimensiones de la LAN, estos servicios y la interconexión a WAN y al perímetro de Internet pueden residir en un switch de la capa de distribución que también

agrega la conectividad de la capa de acceso LAN. Esto también se conoce núcleo fusionado, porque la distribución sirve como la capa de agregación de capa 3 para todos los dispositivos.

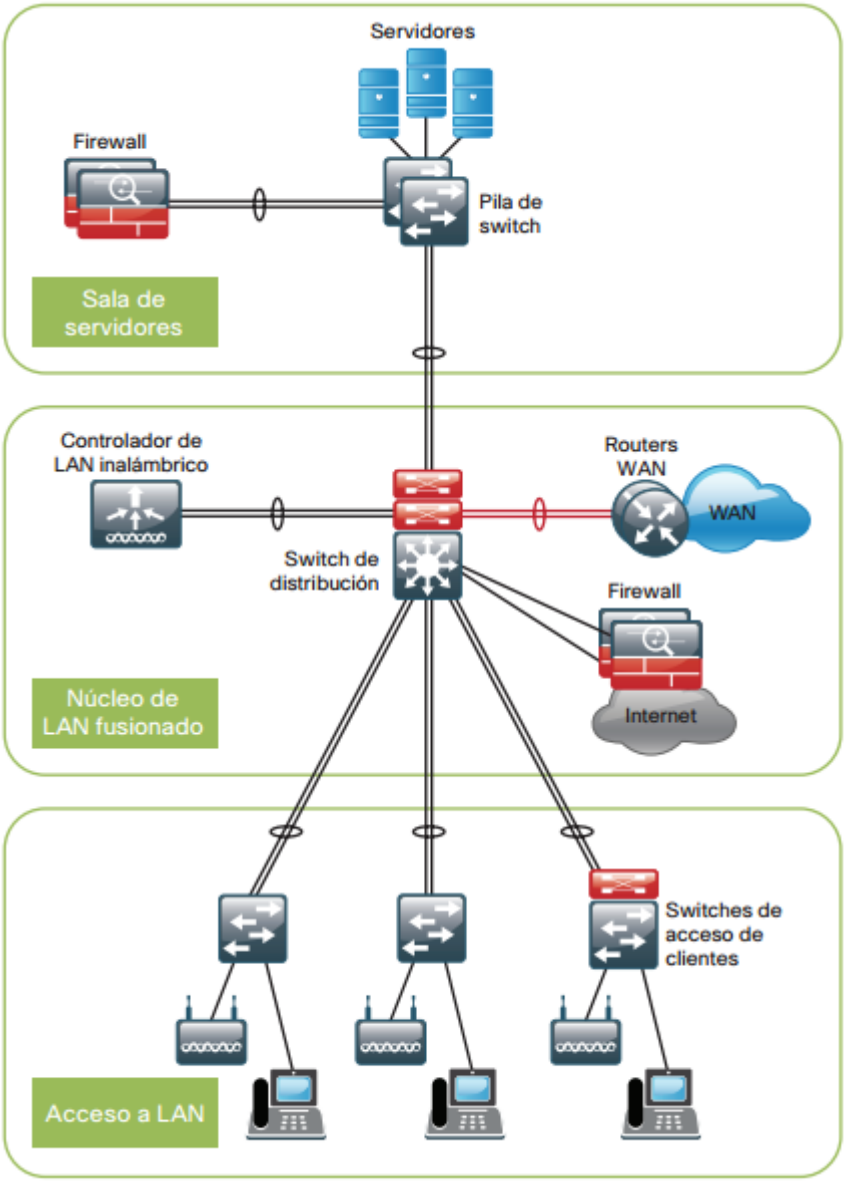


Figura 2-3: Diseño de dos capas, capa de distribución funciona como capa fusionado.

Fuente: Cisco Validated Desing (CVD).

- ***Diseño de tres capas,*** los diseños de LAN más grandes requieren una capa de distribución exclusiva para los servicios basados en la red frente a la necesidad de compartir la conectividad con los dispositivos de la capa de acceso. A medida que la densidad de los routers WAN, los controladores WAAS, los dispositivos del perímetro de Internet y los controladores LAN inalámbricos crece, la capacidad de conectarse a un solo switch de la capa de distribución se hace difícil de administrar. Existe una cantidad de factores que impulsan el diseño de red LAN con diversos módulos de capa de distribución:
    - La cantidad de puertos y ancho de banda del puerto que la plataforma de la capa de distribución puede proporcionar afecta el rendimiento y desempeño de la red.
    - La capacidad de recuperación de la red es un factor cuando todos los servicios LAN y basados en la red dependen de una única plataforma; independientemente del diseño de dicha plataforma, puede presentar un punto de falla único o un gran e inaceptable dominio de fallas.
    - La frecuencia y el control de cambios afectan a la capacidad de recuperación. Cuando todas las LAN, WAN y demás servicios de red se consolidan en una sola capa de distribución, los errores de configuración u operativos pueden afectar a todo el funcionamiento de la red.
    - La dispersión geográfica de los switches de acceso LAN entre distintos edificios en un campus más grande exigiría más interconexiones de fibra óptica a un núcleo fusionado único.

Al igual que la capa de acceso, la capa de distribución también ofrece calidad de servicio (QoS) para flujos de aplicaciones a fin de garantizar que las aplicaciones críticas y las aplicaciones multimedia se desempeñen tal como se diseñaron.

- Plataformas de capa de distribución, el diseño para la tecnología LAN por cable en campus es compatible con los siguientes switches de Cisco como plataformas de capa de distribución:
  - Switch Cisco Catalyst de la serie 6500 con Supervisor Engine 2T.
  - Switches Cisco Catalyst de la serie 6880-X.
  - Switches Cisco Catalyst de la serie 4500-X.
  - Switches Cisco Catalyst de la serie 4507R+E.
  - Switches Cisco Catalyst de la serie 3750-X.

2.2.3.3. Capa de núcleo central

En un entorno de LAN grande con frecuencia surge la necesidad de contar con varios switches de capa de distribución. Uno de los motivos es que cuando los switches de la capa de acceso se ubican en varios edificios geográficamente dispersos, puede ahorrarse la instalación de fibra óptica potencialmente costosa entre los edificios mediante la colocación de un switch de capa de distribución en cada uno de esos edificios. Dado que las redes crecen más allá de las tres capas de distribución en una sola ubicación, las organizaciones deberían usar una capa de núcleo central para optimizar el diseño.

Otro motivo para usar varios switches de capa de distribución es cuando la cantidad de switches de capa de acceso que se conectan a una sola capa de distribución excede los objetivos de rendimiento del diseñador de redes. En un diseño modular y escalable, puede colocar capas de distribución para el centro de datos, conectividad WAN o servicios periféricos de Internet.

En entornos en los que existen varios switches de capa de distribución próximos entre sí y en los que la fibra óptica ofrece capacidad de interconexión de ancho de banda de alta velocidad, la capa de núcleo central reduce la complejidad de la red, tal como se muestra en figura 2-4.

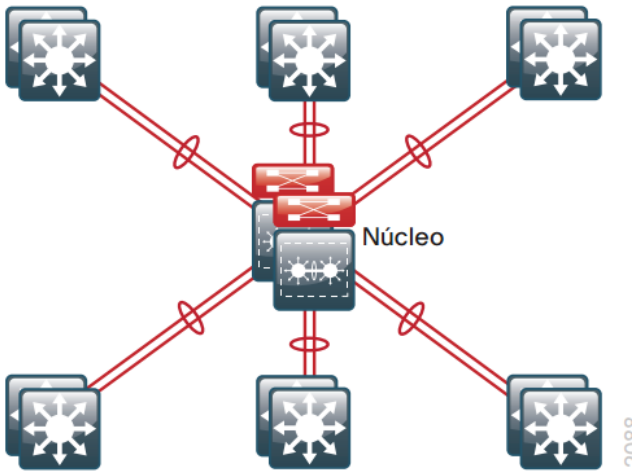


Figura 2-4: Topología LAN con una capa de núcleo principal.

Fuente: Cisco Validated Desing (CVD).

La capa de núcleo central de la LAN es una pieza fundamental de la red escalable y, aun así, es una de las más simples de diseñar. La capa de distribución aporta los dominios de control y fallas, y el núcleo central

representa la conectividad ininterrumpida, 24 horas al día, los 7 días de la semana todos los días del año, entre ellos; las organizaciones deben contar con esto en entornos comerciales modernos en los que la conectividad a los recursos para realizar negocios sea crucial.

Cuando se usan los switches Cisco Catalyst de la serie 6800 o de la serie 6500, la alternativa preferida es un diseño con núcleo central Catalyst VSS de Capa 3, que generalmente usa dos plataformas administradas y configuradas de forma independiente. La conectividad hacia y desde el núcleo es solo de Capa 3, lo que fomenta mejor estabilidad y recuperabilidad.

- Plataformas de capa de núcleo central, la Guía de diseño para la tecnología LAN por cable en campus es compatible con los siguientes switches de Cisco como plataformas para la capa de núcleo central:
    - Switches Cisco Catalyst de la serie 6807-XL con Cisco Catalyst 6500 Supervisor Engine 2T.
    - Switches Cisco Catalyst de la serie 6500 con Cisco Catalyst 6500 Supervisor Engine 2T.
    - Switches Cisco Catalyst de la serie 6807-XL con Cisco Catalyst 6500 Supervisor Engine 2T.
    - Switches Cisco Catalyst de la serie 6500 con Cisco Catalyst 6500 Supervisor Engine 2T.

2.2.4. Principios del modelo de la red jerárquica

2.2.4.1. Diámetro de la red

El diámetro de la red es el número de dispositivos que un paquete debe cruzar antes de alcanzar su destino. Mantener bajo el diámetro asegura una latencia baja y predecible entre los dispositivos. Entre menor sea el diámetro o número de dispositivos para llevar paquete a su destino más rápida es el tiempo de respuesta, es decir a menor dispositivos a recorrer mayor rapidez en la transmisión de los datos a su destino. El menor diámetro es seleccionado por el router con la mejor ruta para cumplir el objetivo. Véase en el anexo 4. Figura. A4-1.

2.2.4.2. Agregado del Ancho de Banda.

El agregado del ancho de banda, se implementa normalmente al combinar varios enlaces paralelos entre 2 switches en enlace lógico.

El agregado de ancho de banda se debe configurar en la capa de distribución y en la capa de núcleo combinando 2 enlaces, para ello se debe tomar en cuenta el ancho de banda requerido. Véase en el anexo 4. Figura. A4-2.

2.2.4.3. Redundancia

Una de las ventajas del modelo jerárquico es la redundancia entre las capas de redes a fin de asegurar la disponibilidad de la red. La redundancia de los equipos y conexiones garantiza que cuando se produce una falla en un segmento de red, esta siga funcionando con normalidad, tal es el caso de que si uno de los switches de la capa de distribución falla, el switch de la capa de acceso afectado tiene la

alternativa de conectarse a otro puerto del switch de distribución, lo mismo pasaría si el caso se diera a nivel de la capa de núcleo. La redundancia permite asegurar la disponibilidad de la red. Véase en el anexo 4. Figura. A4-3.

2.2.4.4. Convergencia.

La convergencia es el proceso en el cual se logra la combinación de las comunicaciones con voz y video en una red. Las aplicaciones colaborativas utilizadas para trabajos en grupo exigen la transmisión simultánea de datos, video y voz, ya que no es fácil trasladarse físicamente hasta otros lugares de forma inmediata o los recursos económicos no nos lo permiten. Las redes jerárquicas abren la posibilidad de convergencia. Véase en el anexo 4. Figura. A4-4.

2.2.5. Calidad de servicio (QoS)

Debido a que el tráfico de comunicación en tiempo real es muy sensible a las demoras y caídas, la red debe garantizar que este tipo de tráfico se administre con prioridad, de manera tal que el flujo de audio o video no se vea interrumpido. Calidad de servicio (QoS) es la tecnología que responde a esta necesidad.

QoS permite a una organización definir distintos tipos de tráfico y crear una gestión más determinista del tráfico en tiempo real. QoS es útil en particular para manejar congestiones, en donde un canal de comunicaciones completo puede impedir que flujos de voz o video sean inteligibles del lado receptor. La congestión es común cuando los enlaces tienen sobresuscripción por agregación de tráfico de una cantidad de

dispositivos y, también, cuando el tráfico en un enlace a un dispositivo proviene de enlaces de carga con mayor ancho de banda. En lugar de crear ancho de banda, QoS toma ancho de banda de una clase y lo asigna a otra clase.

El diseño para la tecnología de LAN cableada en campus, Cisco mantuvo los perfiles de QoS lo más simples posible y a la vez garantizó la compatibilidad para aplicaciones que necesitan una distribución especial.

Este enfoque establece un marco de trabajo modular, escalable y sólido para implementar QoS en toda la red.

Los objetivos principales de implementar QoS en la red son los siguientes:

- Servicio de distribución de comunicaciones acelerado para aplicaciones compatibles en tiempo real.
- Continuidad de los negocios para aplicaciones cruciales para el negocio.
- Equidad entre el resto de las aplicaciones cuando ocurren congestiones.
- Quitar prioridad a aplicaciones que se ejecutan en segundo plano y a aplicaciones no comerciales orientadas al entretenimiento, de manera tal que no retrasen las aplicaciones interactivas o cruciales para el negocio.
- Un perímetro de confianza alrededor de la red para garantizar que los usuarios no puedan inyectar sus propios valores arbitrarios y para permitir que la organización confíe en el tráfico marcado a través de la red.

A fin de alcanzar estos objetivos, el diseño implementa QoS en toda la red, de la siguiente manera:

- Establece una cantidad limitada de clases de tráfico (es decir, de una a ocho clases) dentro de la red que necesitan administración especial (por ejemplo, voz en tiempo real, video en tiempo real, datos de alta prioridad, tráfico interactivo, tráfico por lotes y clases predeterminadas).
- Clasifica las aplicaciones en las clases de tráfico.
- Aplica administración especial a las clases de tráfico para lograr el comportamiento de red pretendido.

2.2.6. VLAN.

Una VLAN es una subred IP separada de manera lógica. Las VLAN permiten que redes de IP y subredes múltiples existan en la misma red conmutada. Para que las computadoras se comuniquen en la misma VLAN, cada una debe tener una dirección IP y una máscara de subred consistente con esa VLAN. En el switch deben darse de alta las VLANs y cada puerto asignarse a la VLAN correspondiente. Un puerto de switch con una VLAN singular configurada en el mismo se denomina puerto de acceso. Recuerde que si dos computadoras están conectadas físicamente en el mismo switch no significa que se puedan comunicar. Los dispositivos en dos redes y subredes separadas se deben comunicar a través de un router (Capa 3), se utilicen o no las VLAN. No necesita las VLAN para tener redes y subredes múltiples en una red conmutada, pero existen ventajas reales para utilizar las VLAN.

2.2.6.1. Ventajas de las VLAN

La productividad del usuario y la adaptabilidad de la red son impulsores clave para el crecimiento y el éxito del negocio. La implementación de la tecnología de VLAN permite que una red admita de manera más flexible las metas comerciales. Los principales beneficios de utilizar las VLAN son los siguientes:

- Seguridad: los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial.
- Reducción de costo: el ahorro en el costo resulta de la poca necesidad de actualizaciones de red caras y más usos eficientes de enlaces y ancho de banda existente.
- Mejor rendimiento: la división de las redes planas de Capa 2 en múltiples grupos lógicos de trabajo (dominios de broadcast) reduce el tráfico innecesario en la red y potencia el rendimiento.
- Mitigación de la tormenta de broadcast: la división de una red en las VLAN reduce la cantidad de dispositivos que pueden participar en una tormenta de broadcast. La segmentación de LAN impide que una tormenta de broadcast se propague a toda la red.
- Mayor eficiencia del personal de TI: las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN. Cuando proporciona un switch nuevo, todas las políticas y procedimientos que ya se configuraron para la VLAN particular se implementan cuando se asignan los puertos.

También es fácil para el personal de TI identificar la función de una VLAN proporcionándole un nombre.

- Administración de aplicación o de proyectos más simples: las VLAN agregan dispositivos de red y usuarios para admitir los requerimientos geográficos o comerciales. Tener funciones separadas hace que gestionar un proyecto o trabajar con una aplicación especializada sea más fácil, por ejemplo una plataforma de desarrollo de e-learning para el cuerpo docente. También es fácil determinar el alcance de los efectos de la actualización de los servicios de red.

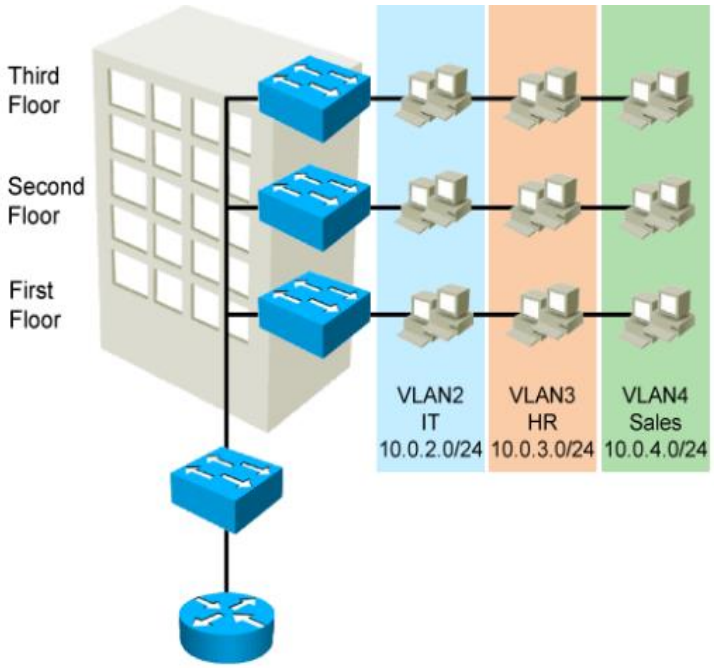


Figura 2-5: Esquema de las VLANs.

Fuente: Interconnecting Cisco Networking Devices (ICND1).

2.2.6.2. Rangos del ID de la VLAN

El acceso a las VLAN está dividido en un rango normal o un rango extendido.

- VLAN de rango normal
  - Se utiliza en redes de pequeños y medianos negocios y empresas.
  - Se identifica mediante un ID de VLAN entre 1 y 1005.
  - Los ID de 1002 a 1005 se reservan para las VLAN Token Ring FDDI.
  - Los ID 1 y 1002 a 1005 se crean automáticamente y no se pueden eliminar. Aprenderá más acerca de VLAN 1 más adelante en este capítulo.
  - Las configuraciones se almacenan dentro de un archivo de datos de la VLAN, denominado vlan.dat. El archivo vlan.dat se encuentra en la memoria flash del switch.
  - El protocolo de enlace troncal de la VLAN (VTP), que ayuda a gestionar las configuraciones de la VLAN entre los switches, sólo puede asimilar las VLAN de rango normal y las almacena en el archivo de base de datos de la VLAN.
- VLAN de rango extendido
  - Posibilita a los proveedores de servicios que amplíen sus infraestructuras a una cantidad de clientes mayor. Algunas empresas globales podrían ser lo suficientemente grandes como para necesitar los ID de las VLAN de rango extendido.
  - Se identifican mediante un ID de VLAN entre 1006 y 4094.

- Admiten menos características de VLAN que las VLAN de rango normal.
- Se guardan en el archivo de configuración en ejecución.
- VTP no aprende las VLAN de rango extendido.

- 255 VLAN configurables

  Un switch de Cisco Catalyst 2960 puede admitir hasta 255 VLAN de rango normal y extendido, a pesar de que el número configurado afecta el rendimiento del hardware del switch. Debido a que la red de una empresa puede necesitar un switch con muchos puertos, Cisco ha desarrollado switches a nivel de empresa que se pueden unir o apilar juntos para crear una sola unidad de conmutación que consiste en nueve switches separados. Cada switch por separado puede tener 48 puertos, lo que suma 432 puertos en una sola unidad de conmutación. En este caso, el límite de 255 VLAN por un solo switch podría ser una restricción para algunos clientes de empresas.

2.2.6.3. Tipo de VLAN

VLAN basada en puerto. Una VLAN basada en puerto se asocia con un puerto denominado acceso VLAN. A continuación, se describe la terminología común de VLAN:

VLAN de Datos, una VLAN de datos es una VLAN configurada para enviar sólo tráfico de datos generado por el usuario. Una VLAN podría enviar tráfico basado en voz o tráfico utilizado para administrar el switch, pero este tráfico no sería parte de una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos.

La importancia de separar los datos del usuario del tráfico de voz y del control de administración del switch se destaca mediante el uso de un término específico para identificar las VLAN que sólo pueden enviar datos del usuario: una "VLAN de datos". A veces, a una VLAN de datos se la denomina VLAN de usuario.

VLAN Predeterminada, todos los puertos de switch se convierten en un miembro de la VLAN predeterminada luego del arranque inicial del switch. Hacer participar a todos los puertos de switch en la VLAN predeterminada los hace a todos parte del mismo dominio de broadcast. Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch. La VLAN predeterminada para los switches de Cisco es la VLAN 1. La VLAN 1 tiene todas las características de cualquier VLAN, excepto que no la puede volver a denominar y no la puede eliminar. El tráfico de control de Capa 2, como CDP y el tráfico del protocolo Spanning Tree se asociará siempre con la VLAN 1: esto no se puede cambiar. Es una optimización de seguridad para cambiar la VLAN predeterminada a una VLAN que no sea la VLAN 1; esto implica configurar todos los puertos en el switch para que se asocien con una VLAN predeterminada que no sea la VLAN 1. Los enlaces troncales de la VLAN admiten la transmisión de tráfico desde más de una VLAN.

VLAN Nativa, Una VLAN nativa está asignada a un puerto troncal 802.1Q. Un puerto de enlace troncal 802.1 Q admite el tráfico que llega de muchas VLAN (tráfico etiquetado) como también el tráfico que no llega de una

VLAN (tráfico no etiquetado). El puerto de enlace troncal 802.1Q coloca el tráfico no etiquetado en la VLAN nativa. El tráfico no etiquetado lo genera una computadora conectada a un puerto de switch que se configura con la VLAN nativa. Las VLAN se establecen en la especificación IEEE 802.1Q para mantener la compatibilidad retrospectiva con el tráfico no etiquetado común para los ejemplos de LAN antigua. Para nuestro fin, una VLAN nativa sirve como un identificador común en extremos opuestos de un enlace troncal. Es una optimización usar una VLAN diferente de la VLAN 1 como la VLAN nativa.

VLAN de Administración, Una VLAN de administración es cualquier VLAN que usted configura para acceder a las capacidades de administración de un switch. La VLAN 1 serviría como VLAN de administración si no definió proactivamente una VLAN única para que sirva como VLAN de administración. Se asigna una dirección IP y una máscara de subred a la VLAN de administración. Se puede manejar un switch mediante HTTP, Telnet, SSH o SNMP.

VLAN de voz, Es fácil apreciar por qué se necesita una VLAN separada para admitir la Voz sobre IP (VoIP). Imagine que está recibiendo una llamada de urgencia y de repente la calidad de la transmisión se distorsiona tanto que no puede comprender lo que está diciendo la persona que llama. El tráfico de VoIP requiere:

- Ancho de banda garantizado para asegurar la calidad de la voz.
- Prioridad de la transmisión sobre los tipos de tráfico de la red.
- Capacidad para ser enrutado en áreas congestionadas de la red.

- Demora de menos de 150 milisegundos (ms) a través de la red.

Para cumplir estos requerimientos, se debe diseñar la red completa para que admita VoIP. Los detalles sobre cómo configurar una red para que admita VoIP están más allá del alcance del curso, pero es útil resumir cómo una VLAN de voz funciona entre un switch, un teléfono IP de Cisco y una computadora.

Un teléfono de Cisco es un switch, El teléfono IP de Cisco contiene un switch integrado de tres puertos 10/100. Los puertos proporcionan conexiones dedicadas para estos dispositivos:

- El puerto 1 se conecta al switch o a otro dispositivo de voz sobre IP (VoIP).
- El puerto 2 es una interfaz interna 10/100 que envía el tráfico del teléfono IP.
- El puerto 3 (puerto de acceso) se conecta a una PC u otro dispositivo.

La función de la VLAN de voz permite que los puertos de switch envíen el tráfico de voz IP desde un teléfono IP. Cuando se conecta el switch a un teléfono IP, el switch envía mensajes que indican al teléfono IP conectado que envíe el tráfico de voz etiquetado con el ID 150 de VLAN de voz. El tráfico de la PC conectada al teléfono IP pasa por el teléfono IP sin etiquetar. Cuando se configuró el puerto del switch con una VLAN de voz, el enlace entre el switch y el teléfono IP funciona como un enlace troncal para enviar tanto el tráfico de voz etiquetado como el tráfico de datos no etiquetado.

2.2.7. Tipos de tráfico de red

Debido a que una VLAN tiene todas las características de una LAN, una VLAN debe incorporar el mismo tráfico de red que una LAN.

2.2.7.1. Administración de red y tráfico de control

Muchos tipos diferentes de tráfico de administración de red y de control pueden estar presentes en la red, como las actualizaciones de Cisco Discovery Protocol (CDP), Simple Network Management Protocol (SNMP) y tráfico de Remote Monitoring (RMON).

2.2.7.2. Telefonía IP

Los tipos de tráfico de telefonía IP son el tráfico de señalización y el tráfico de voz. El tráfico de señalización es responsable de la configuración de la llamada, el progreso y la desconexión y atraviesa la red de extremo a extremo. El otro tipo de tráfico de telefonía consiste en paquetes de datos de la conversación de voz existente. Como acaba de ver, en una red configurada con VLAN, se recomienda con énfasis asignar una VLAN diferente a la VLAN 1 como VLAN de administración. El tráfico de datos debe asociarse con una VLAN de datos (diferente a la VLAN 1) y el tráfico de voz se asocia con una VLAN de voz.

2.2.7.3. IP Multicast

El tráfico IP multicast se envía desde una dirección de origen particular a un grupo multicast que se identifica mediante un único IP y un par de direcciones MAC de grupo de destino. Broadcasts Cisco IP/TV son ejemplos de aplicaciones que genera este tipo de tráfico. El tráfico multicast puede producir una gran cantidad de datos que se transmiten a

través de la red. Cuando la red debe admitir tráfico multicast, las VLAN deben configurarse para asegurarse de que el tráfico multicast se dirija sólo a aquellos dispositivos de usuario que utilizan el servicio proporcionado, como aplicaciones de audio o video remoto. Los routers se deben configurar para asegurar que el tráfico multicast se envíe a las áreas de red cuando se le solicita.

2.2.7.4. Datos normales

El tráfico de datos normales se relaciona con el almacenamiento y creación de archivos, servicios de impresión, acceso a la base de datos del correo electrónico y otras aplicaciones de red compartidas que son comunes para usos comerciales. Las VLAN son una solución natural para este tipo de tráfico, ya que pueden segmentar a los usuarios por sus funciones o área geográfica para administrar de manera más fácil las necesidades específicas.

2.2.7.5. Clase Scavenger

Se pretende que la clase Scavenger proporcione servicios less-than-best-effort a ciertas aplicaciones. Las aplicaciones que se asignan a esta clase contribuyen poco o nada a los objetivos organizativos de la empresa y están generalmente orientadas, por su naturaleza, al entretenimiento. Esto incluye aplicaciones compartidas de medios entre pares (KaZaa, Morpheus, Groekster, Napster, iMesh, y demás), aplicaciones de juegos (Doom, Quake, Unreal Tournament, y demás) y cualquier aplicación de video de entretenimiento.

2.2.8. Seguridad en la red.

La seguridad de la red está básicamente en los procesos que se llevan a cabo para controlar los accesos a la red de datos. Con la finalidad de proteger la información que es el recurso más valioso para la universidad, se debe diseñar una arquitectura de red segura y confiable que garantice las tres características básicas de la información. Para lograrlo se requiere implementar el estándar de seguridad de la Norma Técnica Peruana NTP-ISO / IEC 27001:2014. Que es el sistema de gestión de la seguridad de la información que preserva la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de la gestión de riesgos y proporciona confianza a las partes interesadas en el sentido en que los riesgos se manejan adecuadamente. A través de los controles que se detallaran a continuación:

A.5 Políticas de seguridad de la información.

A.5.1 Dirección de la gerencia para la seguridad de la información.

A.5.1.1 Políticas para la seguridad de la información.

A.5.1.2 Revisión de las políticas para la seguridad de la información.

A.9.2.2 Aprovisionamiento de acceso al usuario.

A.9.2.3 Gestión de derechos de acceso privilegiados.

A.9.2.4 Gestión de información de autentificación secreta de usuarios.

A.11.1.1 Perímetro de seguridad física

A.11.1.2 Controles de ingreso físico.

A.11.1.4 Protección contra amenazas externas y ambientales.

A.11.2.1 Emplazamiento y protección de los equipos.

A.11.2.2 Servicios de suministro.

A.11.2.3 Seguridad de cableado.

A.11.2.4. Mantenimiento de equipos.

A.13.1.1 Controles de red.

A.13.1.2 Seguridad de servicios de red.

A.13.1.3 Segregación en redes.

A.13.2 Transferencia de información.

2.2.8.1 Seguridad en el modelo Jerárquico de tres capas

La seguridad en una red jerárquica se implementa en la capa acceso y en la capa de distribución, con la finalidad de mantener la seguridad e integridad de la información, evitando que esta pudiera ser hurtado o distorsionada.

- ***Seguridad en la capa de acceso***

  Es posible incrementar la seguridad en esta capa a través de los siguientes mecanismos:

  - Se pueden controlar el acceso a estas zonas utilizando métodos de autentificación y reglas definidas, implementadas en los firewalls, routers u otros equipos de seguridad tales como:
  - Router Perímetro, “la primera línea de defensa contra ataques externos”. Con las configuraciones realizadas en los routers

perímetro, solamente el tráfico permitido puede entrar en la red, creando una barrera ante los ataque externos.

- Routers internos, se colocan detrás de los routers en la topología de la red perimetral de una organización.
- Routers Firewall, proporciona una frontera segura que filtra el tráfico de red entre redes de confianza. Se utilizan para filtrar el tráfico en función de las políticas de acceso entre subredes. Estas políticas pueden ser estatales y permitir o denegar el acceso a la zona desmilitarizada (DMZ) a nivel local.
    - Zona desmilitarizada (DMZ), se encuentra entre el interior y exterior de la red, ofrece servicios externos para el acceso exterior a través de uno o más servidores de seguridad. La DMZ es menos seguro que la red interna pero más seguro que la red externa.

- ***Seguridad en la capa distribución.***

  La seguridad a nivel de capa de distribución, se realiza a través de listas de control de acceso (ACL), para permitir o denegar el acceso a la red de datos al usuario final, de acuerdo a los privilegios o restricciones configuradas por el administrador de la red.

  - Listas de control de acceso (ACL), “Las ACL son listas de condiciones que se aplican al tráfico que viaja a través de la interfaz del router”. Con el uso de las ACL se pueden restringir o permitir el tipo de tráfico que debe llegar o no a la red de datos, de acuerdo a las normal de seguridad establecidas por la Universidad.

Las ACL deben ser creadas en la routers, utilizando los comandos correspondientes.

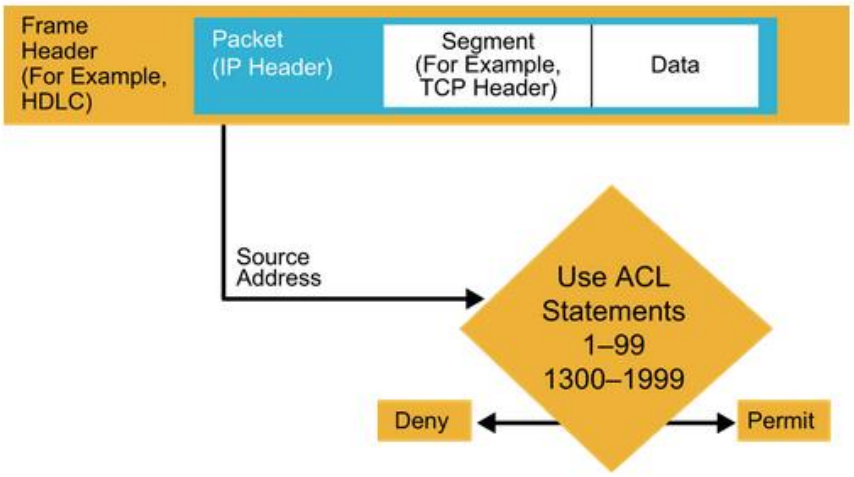


Figura 2-6: Estructura de una ACL.

Fuente: Interconnecting Cisco Networking Devices (ICND1).

2.3. MARCO CONCEPTUAL

- **Arquitectura de red**

  La arquitectura de red es el medio más efectivo en cuanto a costos para desarrollar e implementar un conjunto coordinado de productos que se puedan interconectar. La arquitectura es el “plan” con el que se conectan los protocolos y otros programas de software. Estos son benéfico tanto para los usuarios de la red como para los proveedores de hardware y software.

- **Router**

  Son dispositivos que proporciona internetworking y puesto de interfaz de acceso WAN que se usan para conectarse a la rede del proveedor de servicios. Estas conexiones pueden ser seriales, Ethernet u otras interfaces WAN.

- **Switch**

  Son dispositivos que toman decisiones de envió basadas en la direcciones MAC contenidas dentro de la trama de datos transmitidos. Las switches aprenden las direcciones MAC de los dispositivos conectados a cada puesto, a través de la lectura de las direcciones MAC origen que se encuentran en las tramas que ingresan al switch, luego esta información es almacenada dentro de la tabla de conmutación que almacenada en la CAM.

- **Cable UTP**

  Cable UTP, acrónimo de unshielded twisted pair o par trenzado sin apantallar. Son cables de pares trenzados sin apantallar que se utilizan para diferentes tecnologías de red local. Son de bajo costo y de fácil uso, pero producen más errores que otros tipos de cable y tienen limitaciones para trabajar a grandes distancias sin regeneración de la señal.

- **SecureCRT**

  SecureCRT es un emulador de terminal de software que soporta la emulación VT100, Telnet, SSH, Kerberos y conexiones de puerto serie. Viene con un lenguaje de script y se puede utilizar a través de redes Ethernet o conexiones de acceso telefónico.

- **Dirección IP**

  Una dirección IP es un número que identifica de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, Tablet, Laptop, Smartphone) que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo OSI. La dirección IP no debe confundirse con la dirección MAC, que es un identificador de 48 bits para reconocer de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red.

- **Máscara**

  La máscara de subred es una máscara de bits que determina la parte de sistema principal y la parte de red de una dirección IP (Protocolo Internet). La máscara de subred es un entero de 32 bits exclusivo que define la parte de la red donde se conecta una interfaz. La máscara debe especificarse siempre conjuntamente con una dirección de red (IP).

- **Máscara Wildcard**

  Un mascara Wildcard no es una máscara de red. Esto es algo muy importante a tener en cuenta. Esta tiene 32 bits de longitud, como se aprecia en la Tabla 2-1.

Tabla 2-1: Valor Bit que se usa en la Wildcard.

VALOR	MASCARA DE SUBRED	MASCARA WILDCARD
0	Componente de host	Se usa
1	Componente de red	Se ignora.

Fuente: Interconnecting Cisco Networking Devices (ICND1).

Cuando una Wildcard encuentra un 0 significa que si debe de mirar el bit de la ip del paquete en cuestión. Pero cuando encuentra un 1 significa que

no debe de mirar el bit de la dirección ip del paquete en cuestión. Por lo que la máscara Wildcard y la ip del paquete se usan conjuntamente indicando al router la porción de dirección ip y que bits que se usa de usar.

- **Fibra Óptica**

  La fibra óptica es un medio de transmisión, consiste en un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. El haz de luz queda completamente confinado y se propaga por el interior de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, en función de la ley de Snell. La fuente de luz puede provenir de un láser o un diodo led.

- **PMBOK**

  Project Management Body of Knowledge (PMBOK). Describe un conjunto de conocimientos y de prácticas aplicables a cualquier situación que requiera formular, las cuales han sido concebidas luego de evaluación y consenso entre profesionales pares sobre su valor y utilidad. El PMBOK no es una metodología, sino como una guía de estándares internacionales para que los profesionales puedan adaptar a cada caso y contexto particular los procesos, reconocidos como buenas practicas por el PMI que se pueden aplicar a la mayoría de los proyectos en la mayoría de los casos. El PMBOK documenta la información necesaria para iniciar, planificar, ejecutar, supervisar y controlar, y cerrar un proyecto individual, e identifica los procesos de la dirección de proyectos que han sido reconocidos como buenas prácticas para la mayoría de los proyectos, la mayor parte del tiempo.

CAPÍTULO III:

DESARROLLO DE LA METODOLOGÍA

3.1. ANÁLISIS DEL MODELO.

La presente propuesta está enteramente basado en el modelo jerárquico de tres capas de cisco, por lo que a continuación se analizarán cada uno de las capas, protocolos y equipos que se usaran, para dicha propuesta.

3.1.1. Modelo de redes Jerárquicas.

La construcción de una red LAN que satisfaga las necesidades de una institución universitaria tiene más probabilidades de ser exitosa si se utiliza el modelo de diseño jerárquico de tres capas. En comparación con otros diseños de redes, una red jerárquica se administra y expande con más facilidad y los problemas se resuelven con mayor rapidez. Además una red jerárquica nos proporciona los siguientes beneficios.

- Escalabilidad, ya que toda red jerárquica se expande con facilidad.
- Redundancia, a nivel de núcleo y distribución asegura de disponibilidad de la ruta.
- Rendimiento, el agregado del enlace entre el núcleo de alto rendimiento y switches de distribución permiten la velocidad del cable en toda la red.

- La seguridad por puerto en el nivel de acceso y las políticas en el nivel de distribución hacen que la red sea más segura.
- Facilidad de administración, la consistencia entre los switches de cada nivel hace que la administración sea mucho más fácil.
- Facilidad de mantenimiento, la modularidad del diseño jerárquico permite que la red escale sin volverse demasiado complicado.

3.1.1.1. Redes jerárquicas de tres capas

El diseño basado en las redes jerárquicas implica la división de la red en capas independientes. Cada capa cumple funciones específicas que definen su rol dentro de la red general.

La separación de las diferentes funciones existentes hace que una arquitectura de red se vuelva modular que esto permite la escalabilidad y el rendimiento. Es así que este diseño jerárquico se separa en tres capas: acceso, distribución y núcleo, como se muestra en la figura 2-2.

- **Capa de acceso.**

  La capa de acceso de la red es la que controla a los usuarios y el acceso de grupos de trabajo o los recursos de la red. En esta capa se lleva la conmutación Ethernet, DDR (Dial-On-Demand Routing) y ruteo estático, es importante considerar que no tienen que ser routers separados lo que se efectúan estas funciones de diferentes capas, podrían ser incluso varios dispositivos por capa o un dispositivos haciendo funciones de varias capas. Entre sus características tenemos:

  - Hace interfaz con los dispositivos finales, tales como PCs, impresoras y teléfonos IP para proveer acceso al resto de la red.

- Puede incluir routers, switches, bridges y Wireless Access points.
- Su propósito principal, es proveer un medio de conexión de dispositivos a la red y controlar a los dispositivos que pueden comunicarse en la red.
- Opera el protocolo STP para evitar loops o bucles y por consiguiente disminuye tormentas de broadcast.
- Debe contar con conectividad a 10/100/1000 Ethernet.
- PoE, Vlan y QoS.

- **Capa de distribución**

  Esta capa representa el punto medio entre la capa de acceso y los servicios principales de la red, la función primordial de esta capa es realizar funciones tales como:

  - Realizar filtrados, enrutamientos con el cual determina si el tráfico debe llegar hasta la capa de Núcleo. Además en esta capa se deben configurar la lista de acceso, los route-map, protocolos de enrutamiento tales como EIGRP OSPF.
  - Agrega los datos recibidos de los switches de la capa de acceso antes que sean transmitidos a la capa del núcleo para el enrutamiento a su destino final.
  - Controla el flujo de tráfico en la red con el uso de políticas y delinea dominios de Broadcast para realizar funciones de enrutamiento entre VLANs definidas en la capa de acceso.

- Las VLANs permiten segmentar el tráfico de un switch en subredes separadas, por ejemplo en la arquitectura propuesta contaremos con 30 VLANs.
- Los switches son normalmente dispositivos de alto rendimiento que tienen alta disponibilidad y redundancia que aseguran su confiabilidad.

- **Capa de Núcleo**

  Esta capa se encarga de desviar el tráfico de datos lo más rápido posible hacia los servicios apropiados, estos se conocen como servicios globales o corporativos, algunos de tales servicios pueden ser, email, acceso a internet o la Telepresencia.

  - La capa de núcleo es crítica para la interconectividad entre los dispositivos de la capa de distribución, por consiguiente es importante para el núcleo ser altamente disponible y redundante.
  - Esta área puede conectarse a los recursos de internet.
  - Agrega el tráfico de todos los dispositivos de la capa de distribución, por consiguiente debe ser capaza de enviar grandes cantidades de datos rápidamente.
  - Debe enviar los paquetes hacia redes externas los más rápido posible, es por esta razón no se debe configurar los filtrados, listas de acceso, políticas, etc. Para no agregar los retardo a los paquetes.

- Deben configurarse con los protocolos de enrutamiento tales como EIGRP u OSPF, además para las redes externas se le publicará rutas sumariadas para no cargar rutas aprendidas por los equipos.

3.1.1.2. Principios de la red jerárquica de tres capas.

- **Diámetro de red.**
  - Al diseñar una topología de red jerárquica, lo primero que se debe considerar es el diámetro de la red. Este es el número de dispositivos que el paquete debe cruzar antes de llegar a su destino.
  - Cada switch debe determinar la dirección MAC destino de la trama, verificar la tabla de dirección MAC y enviar la trama al puerto apropiado.
  - Aunque el proceso dure milésimas de segundo, el tiempo se acrecienta cuando la trama tenga que cruzar mucho switches.
  - Al implementar el modelo jerárquico de tres capas, en el nivel de distribución prácticamente elimina el diámetro de la red. Ya que el diámetro de la red, siempre va ser un número predecible de saltos entre el dispositivo origen y el destino.
- **Agregado de ancho de banda.**
  - El agregado de enlaces permite que se combinen los enlaces de puerto de múltiples switches, con el fin de lograr un rendimiento máximo.
  - Se hace uso de la tecnología de agregado de enlaces EtherChannel, que permite la interconexión de múltiples enlaces Ethernet.

- Conectar enlaces específicos en puertos específicos de cada switch, para que se suministre un incremento de ancho de banda a una parte específica de la red, para el EtherChannel.

- **Redundancia.**
  - Propiedad que indica que se debe crear una arquitectura de red de alta disponibilidad.
  - La redundancia puede ser proveída en varias formas: doblar la conexión entre dispositivos o se puede doblar los dispositivos.
  - La implementación de enlaces redundantes puede ser costosa.
  - Para la implementación de los enlaces redundantes, se debe contar como mínimo con dos switches, esto generalmente se implemente en la capa de distribución y núcleo, a través de conexiones cruzadas, esto protege a la red si un switch de distribución falla.

- **Convergencia de red.**
  - La convergencia es el proceso de combinación de las comunicaciones con voz y video en una red de datos.
  - La convergencia de redes también necesita una administración extensiva en relación con la calidad de servicios, ya que es importante que se debe dar prioridad en ocasiones voz sobre datos.
  - La convergencia de red tiene como beneficio: Existencia de solo una red para administrar y menor costo de administración e implementación.
  - Actualmente todos los modelos de switches soportar la convergencia de red.

3.1.1.3. Características de los Switches.

Para seleccionar un switch se necesita decidir entre una configuración fija o una configuración modular, apilables o no apilables. Otra consideración es el grosor del switch expresado en cantidad de bastidores.

- **Switch de configuración fija.**
  - Como son fijos en su configuración no es posible agregar características más allá de su licencia obtenida.
  - El modelo en particular de compra determina las características y opciones disponibles.
  - Habitualmente existen diferentes opciones de configuración que varían en cuanto al número y al tipo de puertos.

- **Switches modulares.**
  - Vienen usualmente con chasis de diferentes tamaños.
  - La tarjeta de línea son las que contienen los puertos.
  - La tarjeta de línea se ajusta al chasis del switch de igual manera que las tarjetas de expansión se ajustan a la PC. Además estos pueden ser de 24 puertos y agregables tarjetas de hasta 48 puertos.

- **Rendimiento.**

  Cuando se selecciona un switch para las capas de acceso, se debe considerar la capacidad del switch para admitir los requerimientos de: Densidad de puerto, Tasas de envió, Agregado de ancho de banda.
  - *Densidad de puerto*. Es el número de puertos disponibles en un switch, además las altas densidades de puertos permiten un mejor uso de

espacio y de energía cuando la fuente de ambos es limitada. Por ejemplo el switch Catalyst 6500 puede admitir un exceso de 1000 puerto de switch en un único dispositivo.

- *Tasas de Envió*. Las velocidades de reenvió definen las capacidades de procesamiento de un switch mediana la estimación de la cantidad de datos que puede procesar por segundo el switch. Por ejemplo un switch de gigabit de 48 puertos que opera a una velocidad de cable completa genera 48Gb/s de tráfico, si el switch solo admite una tasa de reenvió de 32Gb/s, no puede ejecutar la velocidad de cable completa a través de todos los puertos de forma simultánea.

- **Power Over Ethernet y la capa 3**
  - Power Over Ethernet (PoE), permite que el switch suministre energía aun dispositivo por el cableado de Ethernet existente. Por ejemplo a los teléfonos IP.
  - Los switches de capa 3 ofrecen funcionalidad avanzada para enrutar tráfico con direcciones IP en la capa 3. También son conocidos como switches multicapa.

- **Características del switch de la capa de acceso.**
  - Seguridad de puerto, permite que el switch decida cuantos y que dispositivos específicos se permiten conectar al switch.
  - VLANs, permiten establecer las VLAN para los dispositivos de nodo final. El tráfico de voz habitualmente recibe una VLAN separada, de esta manera el tráfico de voz pueda admitirse con más ancho de banda, conexiones redundantes y seguridad mejorada.

- Velocidad de puerto, FastEthernet permite hasta 100Mb/s de tráfico por puerto de switch. Gigabit Ethernet permite hasta 1000Mb/s de tráfico por puerto de switch.
- PoE, solo debe considerarse cuando se necesita convergencia de voz o están implementados puntos de acceso inalámbricos.
- Agregado de enlaces, permite que el switch utilice enlaces múltiples simultáneamente. Los switches de capa de acceso se benefician con el agregado de enlaces cuando se agrega ancho de banda hasta los switches de capa de distribución.
- QoS, en una red convergente que admite tráfico de red datos voz y video, los switches de capa de acceso necesitan admitir QoS para mantener prioridades.

- **Características del switch de la capa de distribución.**
  - Los switches de capa de distribución proporcionan funciones de enrutamiento entre VLAN, para que una Vlan pueda comunicarse con otra red.
  - Se utilizan listas de acceso para controlar como fluye el tráfico a través de la red. Además necesitan admitir QoS para mantener la prioridad del tráfico que provienen de los switches de la capa de acceso.
  - Es importante que los switches admitan redundancia para la disponibilidad adecuada.
  - Agregación de enlace, debido a que los switches de capa de distribución aceptan el tráfico entrante de los múltiples switches de

capa acceso, necesitan enviar todo ese tráfico tan rápido como sea posible a la capa de núcleo.

- **Características del switch de la capa de núcleo.**
  - Necesita admitir el agregado de enlaces para asegurar el ancho de banda adecuado que ingresa al núcleo.
  - Se busca los switches de capa de núcleo que admiten las características de redundancia del hardware adicional como fuentes de energía redundante que pueden intercambiarse mientras el switch continúa funcionando.
  - En el núcleo y el extremo de la red deben recibir garantías superiores de QoS para obtener mejores tiempos en las transferencias de archivos o el correo electrónico.

3.1.2. Análisis de la Arquitectura de red Actual.

En este capítulo detallaremos la situación actual de la arquitectura de red de la Universidad Nacional Tecnológica de Lima Sur, sus elementos y como ésta se encuentra administrada, dicha información fue recolectada a través de la observación, entrevistas y consulta de documentos disponibles, cuyos resultados se muestran más adelante.

La red de la Universidad Nacional Tecnológica de Lima Sur, tiene las siguientes características:

- La red actualmente presenta una topología en estrella, su diseño lógica es plana por lo que representa varias desventajas, tales como un único dominio de broadcast de capa 2, ya que una petición arp, viaja a cada

host y dispositivo de la red LAN. Debido a esto se consume una gran cantidad de ancho de banda disponible en la red.

- La asignación de IPs se da a través del protocolo DHCP, que han sido configuradas con un rango limitado para cada VLAN creada. (Véase en el anexo la tabla de IPs.).
- Los equipos de enrutamiento usados actualmente son de alto nivel, que soportan las exigencias que una red requiere, pero no existe una administración especializada para dicho efecto. Dichos equipos son:
    - Firewall Fortigate modelo 200d.
    - Balanceado ancho de Banda, Exinda 4010series.
    - RouterBoard 1100 AHXZ.
    - Switches Juniper NETWORKS EX 4200 series.
- Actualmente la distribución de la red no cuenta con un cableado estructurado, los host son conectados directamente desde switch de acceso a través de cables UTP. Además los tendidos de cables no están recubiertos con canaletas como la norma lo indica.
- Las interconexiones desde Switch Core, a los otros Switch principales que se encuentran en los distintos pabellones se dan con cables UTP que superan los límites establecidos y el tendido no está recubierto con ningún tipo de material.
- No se cuenta con un cableado vertical o Backbone que tiene como función principal la interconexión entre los armarios de distribución primarios, intermediarios y las infraestructuras de entrada de unos sistemas de cableado estructurado.

- Se cuenta con servidores que están directamente conectadas al switch Core: servidor abastecimiento, servidor admisión, servidor académico, servidor del portal web, servidor SIGA, servidor SIAF, servidor de repositorios, servidor asterisk y servidor DHCP.
- No cuenta con unas políticas de seguridad implementada como lo recomienda la Norma Técnica Peruana – NTP/IEC ISO 27001.

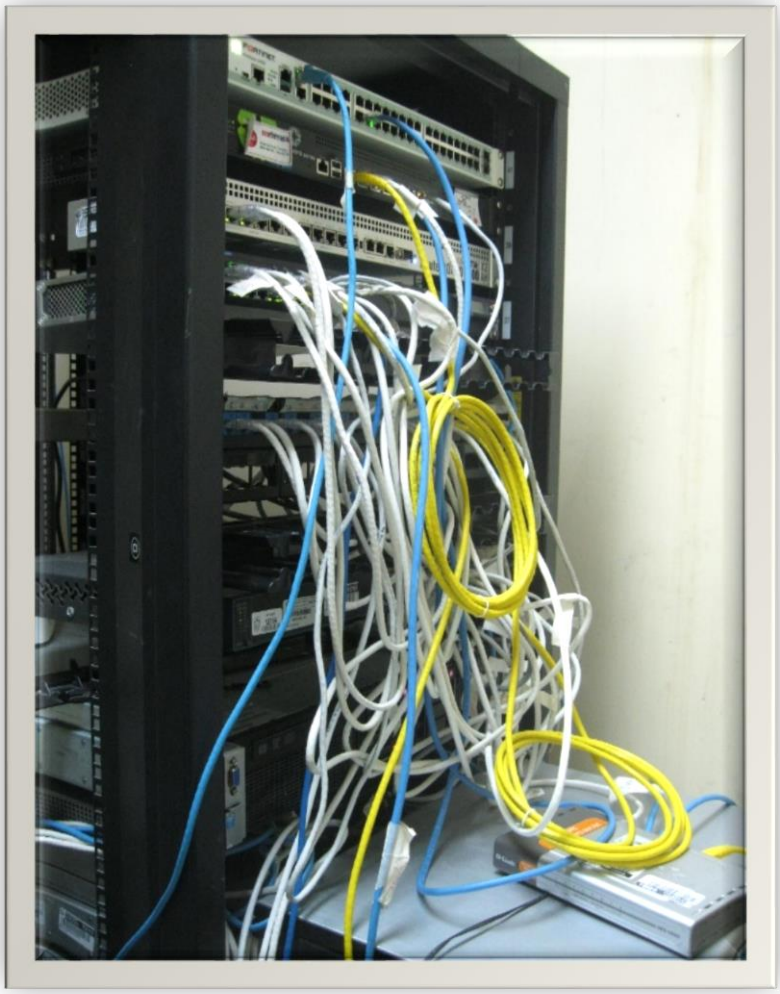


Figura 3-1: Gabinete de equipos en le ODTIC

Fuente: Proporcionado por el área de la ODTIC. Conjunto de equipos que soportan la red actual de la UNTELS, ubicada en el pabellón B.

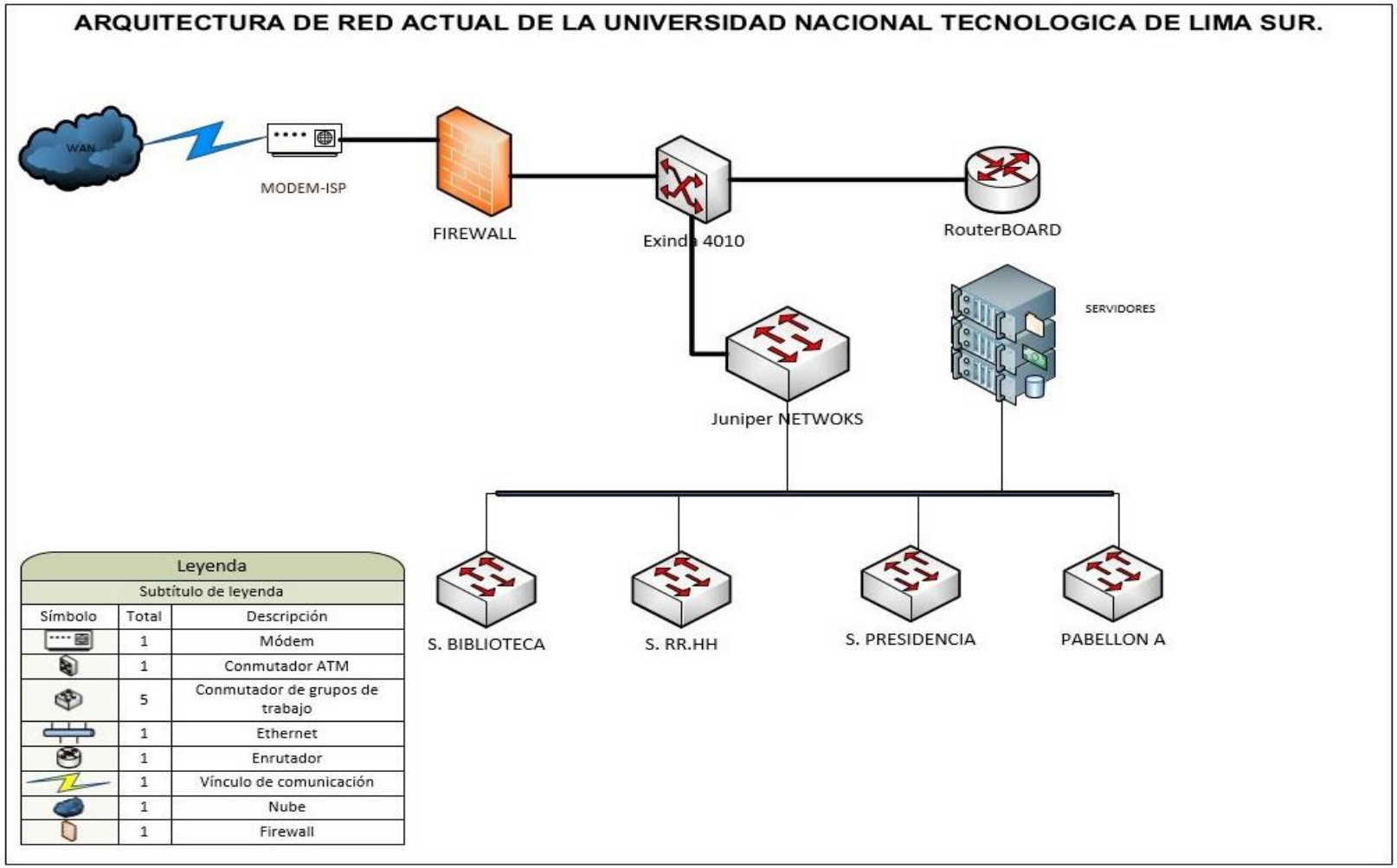


Figura 3-2: Arquitectura actual de la Universidad Nacional Tecnológica de Lima Sur.

Fuente: Elaboración propio.

3.1.3. Análisis del tráfico de datos.

El tráfico de datos es la cantidad de información que fluye a través de la red, es decir toda la información que se envía y se recepciona. Al identificar el tipo de tráfico que circula por toda la red, nos permitirá conocer su estado, congestión y rendimiento. Con esta información podemos incrementar su productividad evitando su congestionamiento. Además permite establecer el número de VLANs que se requieren para implementarse.

Para el análisis del tráfico de datos se procedió a utilizar uno de los programas más conocidos que sirve para analizar los protocolos y paquetes que circulan por la red, este es el software Wireshark. Entre sus características tenemos:

- Análisis de protocolos.
- Captura en vivo y análisis de fuera de línea de paquetes.
- Sistema multiplataforma.
- Análisis de paquetes de voz.
- Captura de paquetes en la interfaces Ethernet, IEE802.11, PPP/HDLC, ATM, Frame Relay y otros.

La metodología consistió, mediante el software Wireshark, un computador portátil y pc instalada en el pabellón A, se procedió la captura durante los días de semana, en turno de la mañana, ya que en este horario hay un consumo masivo de ancho de banda. Y los periodos de captura fueron durante 30 min, cada uno, almacenando todos los archivos en un formato *pcapng para su posterior análisis.

Al analizar todos los datos capturados, en un promedio de 150000 paquetes, diarios, se realizó un filtro de los nueve protocolos más frecuentes que circulan por la red, como se observa en la Tabla 3-1.

Tabla 3-1: Captura de Tráfico de datos desde 25 al 30 junio 2016.

PROTOCOLOS	OCURRENCIAS	PORCENTAJE
ARP	75289	48.12%
NBNS	32978	21.08%
SSDP	12082	7.72%
STP	1764	1.13%
ISMP	16113	10.30%
UDP	4394	2.81%
BROWSER	3538	2.26%
IPSX SAP	7206	4.61%
MS NLB	3094	1.98%
TOTAL	156458	100.00%

Nota: Fuente: Elaboración propio. Los datos mostrados son en un promedio de la captura de 5 días.

Como se aprecia en la Tabla 3-1, hay un alto índice del protocolo ARP, que un promedio representa el 48%, básicamente este protocolo se genera por la acumulación de trafico de broadcast y multicast de cada uno de los dispositivos que están conectadas a la red, también se denomina radiación de broadcast. En ocasiones la radiación de broadcast puede saturar la red, dando como resultado que no exista ancho de banda en toda la red. La tormenta de broadcast aumenta a medida que crece la red y aún más si no se cuenta con una arquitectura bien definida y no escalable.

3.1.4. Análisis de Seguridad de la red.

Toda institución ya sea pública, privada o de cualquier índole cuenta con el activo más importante que es la información, es por ello que se debe tener mayor interés en la parte de la seguridad, para poder asegurar toda la data que se encuentra en los servidores de la universidad.

Al investigar toda la infraestructura de la universidad, se pudo observar algunas deficiencias en la parte de la seguridad de la red, tales como:

- Falta de políticas de seguridad para los cableados o interconexión entre las pabellones.
- Ausencia de ACL's (lista de control de accesos) para le filtrado de paquetes de datos en forma externa o interna.
- Acceso de extremo a extremo no controlado.
- Falta de políticas de seguridad de equipos, como lo recomienda la NTP –ISO/IEC 270001.
- No todos los equipos están en el servidor de autentificación para control de acceso y administración de los dispositivos intermediarios de la red.

3.1.5. Direcciones Ip y las VLANs

La red de la universidad comprende una red de clase C (192.168.10.0) con máscara (255.255.255.0). Se ha creado subredes, con el propósito de proporcionar una sub red a cada área de trabajo dentro de la universidad, (Véase en el anexo la tabla A2-2) que detalla las IPs y los VLANs para cada sub red. Cabe mencionar que algunas de VLANs creadas tienen un rango de IPs que no se están haciendo uso, por ejemplo a la VLAN GYM se ha proporcionado un sub red 192.168.19.0 /24 que cuenta con 253 IPs

disponibles, sin embargo dicho área solo se cuenta con 4 computadoras, por lo que se ve innecesario contar con tal rango de IPs.

Los VLANs están creadas para cada área o jefatura que cuenta la universidad, dicho protocolo está configurado en el switch Core de la ODTIC, también se cuenta con switch que tiene la misma capacidad que se encuentra en biblioteca , que también en ella están configuradas todas las demás VLANs de acceso.

3.1.6. Requerimientos Funcionales.

En base al análisis desarrollado de la red actual de la universidad, se requiere implementar una arquitectura de red que garantice el máximo rendimiento y disponibilidad de la red de datos, en esto debe incluir la característica principal que es la escalabilidad de la red. A continuación se detallan los requerimientos funcionales básicos.

Tabla 3-2: Requerimiento funcionales de la red de la UNTELS.

N°	Código	Nombre	Descripción
1	RF-001	Diseñar una arquitectura de red eficiente.	El diseño eficiente de una arquitectura de red que nos garantice el máximo rendimiento, además que dicha arquitectura cuente con: escalabilidad, tolerante a fallos, QoS y seguridad.
2	RF-002	Solución basada en el modelo Jerárquico de Tres capas de Cisco.	Este modelo implementado por cisco permite adaptarse a los cambios de red, ya que consiste en un diseño de tres

			capas, permitiendo tener escalabilidad en la infraestructura de la red.
3	RF-003	Mejorar el tráfico de datos y seguridad de la red.	A través de protocolos de comunicación y priorización de ancho de banda (QoS), además con la arquitectura bien definida se resolverán y mejoraran el tráfico de datos de la red, también se implementará seguridad sofisticada en toda la infraestructura.
4	RF-004	Monitorear la red de datos.	Se debe conocer estado de la red actual, para ello se debe monitorear la red, durante las horas lectivas dentro de la universidad.

Fuente: Elaboración propio.

3.1.7. Identificación de equipos para la arquitectura de red.

Actualmente en el mercado existen muchas empresas que son proveedores de equipos para redes de computadoras, tales como:

- Huawei
- Hp
- Dell
- Cisco y otros

La UNTELS, actualmente cuenta con equipos de alta gama que le proporciona el proveedor de servicios de internet como se muestra en la figura 3-2. Además la institución cuenta con equipos propios tales como el firewall y los switches cisco de acceso que son modelo 2960.

Para la implementación de la arquitectura es necesario contar con equipos de alta gama, a continuación se describen de acuerdo a las capas los equipos necesarios.

- *Para la capa de acceso*: se cuenta con equipos de la serie 2960-X, que permitirán la conexión de dispositivos finales con ancho de banda de alta velocidad. Además estos admiten redes lógicas, con lo cual se ofrece los beneficios de rendimiento, administración y seguridad.
- *Capa de distribución*, esta capa sirve como un punto de agregación para múltiples switches de la capa de acceso, por lo que se debe contar con switches de capa 3 (3750-X). Además esta capa debe reducir los gastos operativos haciendo que la red sea más eficiente, exigiendo menos cantidad de memoria, creando dominios de falla y procesando los recursos para dispositivos en cualquier otro lado de la red, también debe aumentar disponibilidad de la red debido a que contiene las fallas en dominios más pequeños. La serie C3750-48T-L nos proporcionará: disponibilidad, escalabilidad, además nos permitirá, implementar seguridad en el control de accesos (MACsec), enrutamientos IPv4 e IPv6 y configuración de QoS.
- *Capa Núcleo*, representa la conectividad ininterrumpida, las 24 horas del día y los 7 días de la semana y todos los días del año, por ello debe contar con equipos de la serie 4500-X, ya que este nos proporcionará:
  - Una alta capacidad bi-direccional hasta 800 Gbps.
  - Envío de hasta 250 Mpps en IPv4 o 125 Mpps en IPv6.
  - Tiene una replicación de multicast en el hardware hasta 250 Mpps

- Tiene una capacidad de lectura de hasta 20000 MAC por segundo.
- Permite las configuraciones de ACL y la priorización de calidad de servicio (QoS).
- Soporta hasta 4096 VLANs, además cuenta con 3k instancias para el protocolo Spanning Tree.

3.1.8. Selección de la herramienta para la implementación de la propuesta en un ambiente simulado.

Existen muchas herramientas de simulación, por ello se propone realizar un estudio de las herramientas gratuitas que se usara para dicho propósito, entre ellas tenemos el GNS3 y Packet Tracer que nos ofrecen robustez, disponibilidad, eficiencia, flexibilidad, etc.

GNS3

Es una herramienta especializada en la simulación tanto lógico y físico para las redes de datos, porque permite implementar diferentes topologías, debido a que soporta IOS de los routers ATM/Frame Relay, switches y firewall. GNS3 está basado en Dynamips, PEMU (incluyendo el encapsulador) y Dinagen, desarrollado en Phyton, utiliza la tecnología SVG (gráficos vectoriales escalables), que lo provee de símbolos para el diseño de las topologías de redes.

Packet Tracer.

Es un simulador de redes diseñando por Cisco System, para modelar y probar diseños de redes de datos, esta permite crear grandes redes sin la necesidad

de tener 2 o más computadoras o demás dispositivos de red, interfaces y cables.

Luego de conocer los simuladores de softwares, se establece como la mejor alternativa el software Packet Tracer, por las características que ofrece, sobre todo porque nos permite comprobar el funcionamiento y la configuración de la arquitectura que se propone, además contiene los IOS de los propios equipos ya establecido.

Tabla 3-3: comparación entre GNS3 y Packet Tracer.

GNS3	Packet Tracer
Es simulador de redes	Es simulador de redes
Facilidad de uso	Facilidad de uso
Fácil de instalar	Fácil de instalar
Es un software libre	Es un software libre
Trabaja con IOS reales, y estos no es gratuito.	Trabaja con IOS propio de cisco.
Permite simular grandes arquitecturas de redes, debido a las interconexiones con máquinas virtuales y equipos reales.	Solo simula con equipos propios, dados por el simulador. Solo permite conocer el comportamiento físico y real de la red.
Requiere computadoras con altos recursos, debido que consume mucha memoria RAM del equipo al simular con más tres routers.	Permite la ejecución en cualquier tipo de computador, ya que se puede simular grandes redes con poca cantidad de recursos.

Fuente: www.gns3.com y www.netacad.com.

3.2. CONSTRUCCIÓN, DISEÑO O SIMULACIÓN DE LA HERRAMIENTA / MODELO / SISTEMA.

3.2.1. Plan del Proyecto.

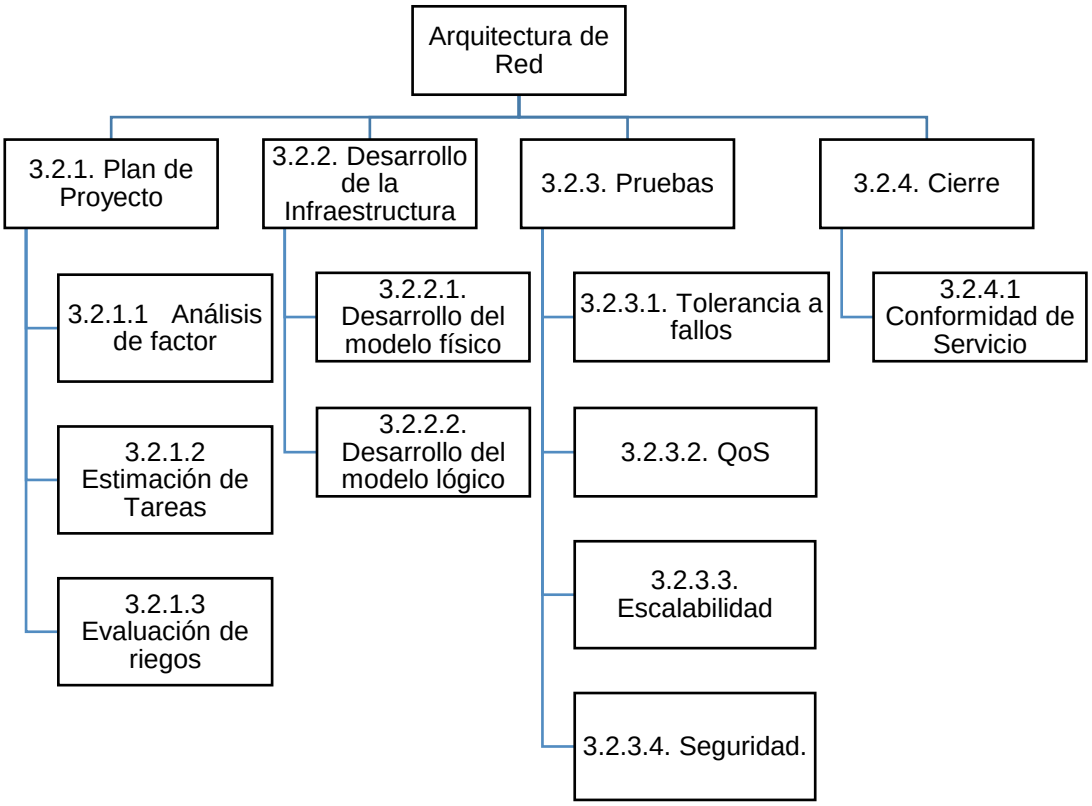


Figura 3-3: EDT del Proyecto.

Fuente: Elaboración propio, basado en PMBOK Versión 5.

Tabla 3-4: Recursos y Costos de la EDT.

N° Entr.	ENTREGABLES	RECURSOS	TIEMPO	COSTO
3.2.1	**Plan del Proyecto**	**PMI, Ing. de Redes**	**14**	**S/. 9,000.00**
3.2.1.1	Análisis de factor	Ing. De Redes	8	**S/. 5,143.00**
3.2.1.2	Estimación de Tareas	PMI	6	**S/. 2,571.00**
3.2.1.3	Evaluación de riesgos	Ing. De Redes y PMI	4	**S/. 1,286.00**
3.2.2	**Desarrollo de la Infraestructura**	**Ing. de Redes 2 Técnicos en Redes**	**96**	**S/. 32,000.00**
3.2.2.1	Desarrollo del modelo físico	Ing. Redes y Técnico	72	S/. 18,000.00
3.2.2.2	Desarrollo del modelo lógico	Ing. Redes y Técnico	42	S/. 14,000.00
3.2.3	**Pruebas**	**Ing. de Redes 1 Técnico en Redes**	**15**	**S/. 5,000.00**
3.2.3.1	Tolerancia a fallos	Ing. De Redes	15	S/. 1,500.00
3.2.3.2	QoS	Ing. De Redes	15	S/. 1,000.00
3.2.3.3	Escalabilidad	Ing. Redes y Técnico	3	S/. 1,500.00
3.2.3.4	Seguridad	Ing. De Redes	15	S/. 1,000.00
3.2.4	**Cierre**	**Ing. de Redes.**	**1**	**S/. 500.00**
3.2.4.1	Conformidad de Servicio	Ing. De Redes	1	S/. 500.00
	Total de Días		**126**	**S/. 46,500.00**

Fuente: Elaboración propio según la EDT propuesto. Leyenda: Entregables (Entr.), Tiempo en días y Costo en soles.

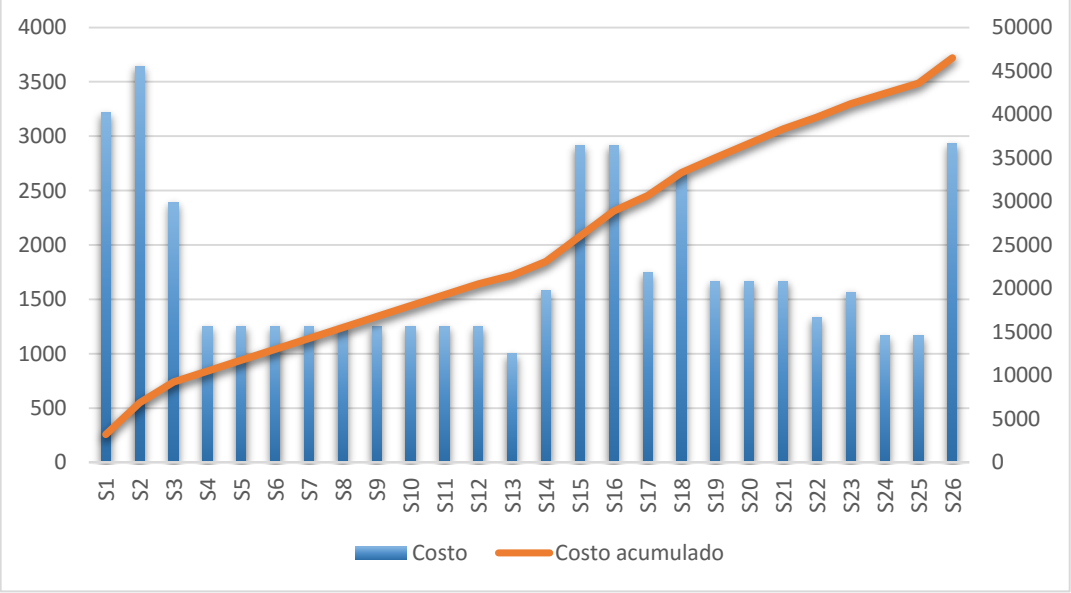


Figura 3-4: Acumulación semanal del costo Total.

Fuente: Elaboración propio, basado en flujo de costos. (Véase Anexo 3.)

Tabla 3-5: Costo Total del Proyecto.

Costo del Proyecto	S/. 46,500.00
Gastos administrativos	S/. 3,000.00
IGV	S/. 8,910.00
Total	S/. 58,410.00

Fuente: Elaboración Propio.

3.2.2. Desarrollo de la Infraestructura.

El diseño de la arquitectura o diseño físico de la red LAN, se crea basado en el modelo Jerárquico de tres capas implementada por cisco, que se adapte a las necesidades de la institución universitaria, además se debe implementar el NOC(centro de operaciones de red), que permita el monitoreo del estado de la red datos de la universidad constantemente.

3.2.2.1. Propuesta del Modelo Jerárquico de Tres Capas.

Las Redes de datos basada en el modelo jerárquico de tres capas de cisco para campus es adaptable a los requerimientos funcionales propuestos para la universidad, la arquitectura de red propuesta se muestra en la figura 3-5, que está basada a los principios de diseño de la red jerárquica detallados en el capítulo 2.2.4.

La arquitectura de red propuesta, para la UNTELS, esta creado bajo el modelo jerárquico de tres capas, para asegurar el rendimiento, disponibilidad, seguridad, escalabilidad y administración para utilizar lo mejor de los recursos. En el modelo propuesto claramente se identifican las capas de acceso, distribución y núcleo, cada uno de ellos está constituido de la siguiente manera.

- *Capa de Acceso*, para la implementación de esta capa física , se usaran 20 switches de modelo 2960 – T, de 24 y 48 puertos, administrable, ya que estos estarán asociados a VLANs previamente establecidas , debido a que estos son los encargados de conmutar paquetes hacia la capa de distribución , además proporciona acceso a la red, a todos los usuarios que pertenecen a las oficinas administrativas, jefaturas, etc.
- *Capa de Distribución*, en la arquitectura propuesta esta capa está compuesta por 3 Switches de capa 3, modelo 3750 – X, de 24 puertos cada una, debido a que la función de estos equipos es conmutar paquetes a gran velocidad, en esta capa se segmenta la red de datos en varios dominios de broadcast de acuerdo a las configuraciones que se establecerán. Además los equipos estarán configuradas como VTP (protocolo de enlace troncal de las VLANs), que permitirá tener un dominio administrativo unificado a la red. Estos equipos estarán instaladas de la siguiente manera:
    - Switch 1, en el pabellón que se propondrá para NOC, permitiendo así abastecer a los switches de acceso del edificio de presidencia, pabellón A y la parte administrativa del centro PRE.
    - Switch 2, estará ubicada en el pabellón B, para conectar los switches de acceso para los laboratorios, parte administrativa y el gimnasio.
    - Switch 3, este equipo estará ubicada en la biblioteca, para abarcar con las jefaturas de carreras, RR.HH y demás áreas administrativas.

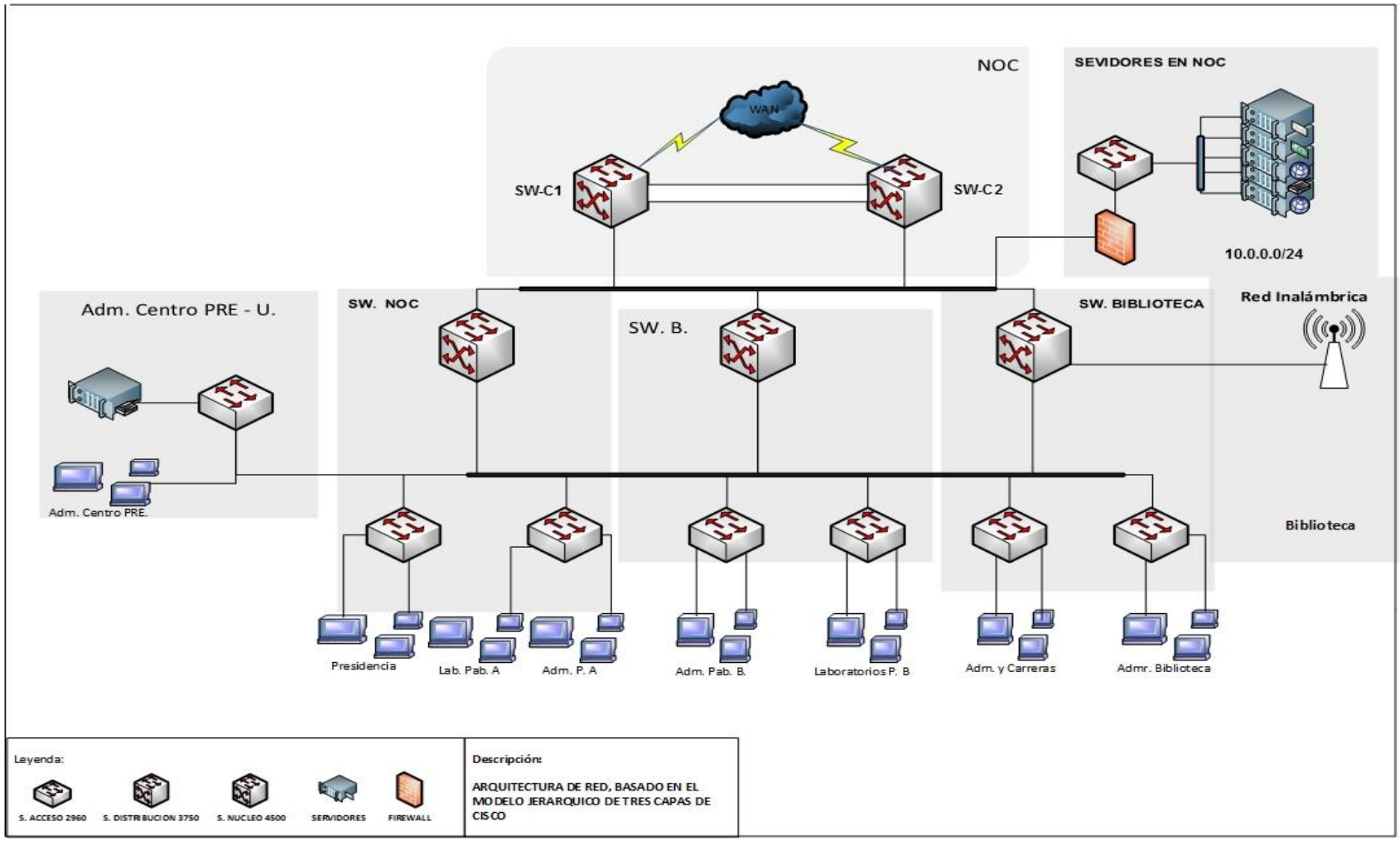


Figura 3-5: Arquitectura de red propuesta para la UNTELS.

Fuente: Diseño propio, basado en el modelo jerárquico de tres capas

- *Capa de Núcleo*, esta capa conocida también como capa principal o Core está compuesta por 2 switches de capa 3 modelo 4500 – X, ya que la función principal de esta es tener un enrutamiento avanzado para tener mayor velocidad de transmisión de datos. Este equipo se ubicara en el NOC propuesto junto a servidores, véase en el anexo el plano referencial de la ubicación.

La red Inalámbrica que se instalará en la biblioteca para el acceso libre de los estudiantes y docentes, estará creado bajo el estándar IEEE 802.11 cuyo punto de acceso se conectará directamente al switch de distribución que estará ubicada en el mismo lugar, a través del Access point que se usa actualmente, dando prioridad a la red, cuando se haga uso de teleconferencias o Telepresencia.

Tabla 3-6: Distribución de Switches.

Switch	Detalle
SW-NOC	Switch de capa 3 Modelo 3750 – X Series de 24 puertos, ubicada en la capa de distribución, la cual permitirá la conexión a los switches de acceso para los pabellones de presidencia, “A, C” y Centro PRE.
SW-B	Switch de capa 3, Modelo 3750-x Series de 24 puertos, equipo de capa de distribución, que permitirá conectar los switches de acceso a las oficinas de administrativas ubicada en el pabellón B y el gimnasio.

SW-BIBLIOTECA	Switch de capa 3, que interconectará a las áreas administrativas tales como: jefatura de carreras, RR-HH, producción y el servidor de la biblioteca.
SW-C1 y 2	Switches de capa 3 modelo 4500 – X series, que estarán ubicadas en el NOC propuesto, que permitirán la conexión de los equipos de la capa de distribución.
SW-ACCESO	Equipos de modelo 2960 –T, que estarán ubicados en los pabellones descritos anteriormente para el acceso de los usuarios, estas están directamente conectados a los switches de distribución.

Fuente: Elaboración propio, basado en el modelo jerárquico de tres capas.

Todos los switches que conforman la arquitectura de red propuesta deben poseer un número mayor de puertos que la cantidad de host disponibles, para que posteriormente se adapte al crecimiento de la red, permitiendo así cumplir con la característica básica que es la escalabilidad de la red,

3.2.2.2. Diseño del modelo lógica de la red.

Consideraciones para la arquitectura lógica.

Para un correcto diseño lógico de la red, debemos basarnos en los 4 criterios fundamentales de una arquitectura red: Tolerante a fallas, escalabilidad, calidad de servicios y seguridad.

El objetivo principal es implementar una arquitectura de red para mejorar el tráfico de datos, basado en el modelo jerárquico de tres capas, en la plataforma LAN para la universidad.

- *Tolerante a fallas*, la arquitectura estará diseñada teniendo en cuenta las grandes tecnologías o protocolos actuales, que nos permitirán limitar cualquier impacto de una falla del software o hardware, a través de sus enlaces o rutas redundantes entre el origen y el destino para cada host, es así que la infraestructura física como los procesos lógicos estarán diseñadas para adaptarse a unos enlaces redundantes. Dicho esquema estará implementado a través del protocolo STP (Spanning Tree Protocol), bajo el estándar IEEE 802.1.
- *Escalabilidad*, esta arquitectura estará diseñada para aumentar su tamaño, sin que ello produzca cambios importantes en el diseño general por lo que se proveerá de un número considerable de puntos de red o puerto en los switches. Además los switches de la capa de distribución son escalables para así permitir aumentar la cantidad de puertos para soportar crecimientos futuros.
- *Calidad de Servicios (QoS),* la arquitectura propuesta proporcionara conectividad a todos usuarios a través de la red, proporcionando políticas o dando prioridades a ciertos tipos de datos, dependiendo de la necesidad de uso para cada cual, además de esto, de debe implementar VLANs bajo el estándar 802.1Q, mediante segmentación de la LAN en subredes, que nos permitir crear fronteras lógicas para distintos departamentos o áreas, aumentando seguridad y prioridad en la red.
- *Seguridad,* la seguridad de la red, se implementará a través de:
    - ACL, la red mantendrá seguridad a nivel lógico con la creación de reglas de acceso, que permitirá generar restricciones a los

terminales de diferentes áreas disminuyendo la vulnerabilidad de los datos que fluyen.

- Se hará uso del equipo firewall Fortigate 200d, para filtrado de paquetes entrantes y salientes, reforzando de esta manera la protección completa para la LAN.

Direcciones IP.

Actualmente la Universidad Nacional Tecnológica de Lima Sur, tiene en promedio 500 computadoras, 20 impresoras, 100 teléfonos IP conectados a red en todas la áreas administrativas del campus.

- ***VLSM y subredes*** Las máscaras de subred de tamaño variable (variable length subnet mask, VLSM), representa una de las soluciones que se presentaron por el agotamiento de las direcciones IP y como la división en subredes. El concepto básico es simple, se toma una red y se divide en subredes fijas, luego se toma una de esas subredes y se vuelve a dividir tomando bits prestados de la porción de host, ajustándose a la cantidad de los hosts requeridos por cada segmento de la red.

  Para calcular el direccionamiento se ha agrupado algunos de las áreas administrativas con fin de maximizar la cantidad de IPs, además se ha tomado en cuenta el crecimiento de éstas en un futuro. Véase en el anexo tabla A2-4.

  Para esta propuesta se mantendrá la notación de las dirección IP 192.168.10.0, debido a que realizar los cambios en cada equipo sería muy complejo, además como la mayoría de los equipos obtiene direcciones IP a través del protocolo DHCP, será más sencillo quedarse

con las mismas direcciones. Por lo tanto lo más recomendable en este direccionamiento será cambiar las máscaras. Para dicho efecto se aplicará la formula básica para subneteo.

$$Número\ de\ Host\ \leq\ 2^n - 2$$

Véase en el anexo la tabla A2-5. Rango de IPs, calculado con la metodología VLMS.

- ***Protocolos,*** en esta propuesta se harán uso del protocolo TCP/IP y para realizar los enrutamiento entre los switches se procederá a través de los protocolos EIGRP y OSPF, siendo la primera el protocolo autónomo de cisco y la segunda protocolo estándar.

3.2.2.3. Redes Virtuales (VLANs)

Se implementarán VLANs de puertos, en la capa de distribución en los switches, para nuestro caso en switch 3750 - X.

- **Ventaja**
  - Facilidad de movimiento y cambios
  - Micro segmentación y dominio de Broadcast
  - Las VLANs son autónomos respecto a demás protocolos
  - No existen limitaciones en cuanto a los protocolos utilizados
- **Desventaja**
  - Un movimiento de una estación de trabajo requiere la configuración del switch al que se va a conectar.

Véase en el anexo la tabla A2-6, VLANs propuesta.

3.2.2.4. Implementación del Modelo Jerárquico de Tres capas en un ambiente simulado.

De acuerdo a la sección 3.1.8 se establece que la mejor alternativa para la simulación de la arquitectura de la red de la universidad es el Packet Tracer. Esta simulación evita que ocurran imprevistos durante la implementación y como consecuencia la falta de productividad y pérdida económica. La arquitectura simulada en Packet Tracer se muestra en la figura 3-6.

- **Configuración de los Switches de la capa de núcleo.**

  La capa de núcleo de la red jerárquica está conformado por 2 Switches de capa 3, modelo 4500. Para la conexión entre switches a través del EtherChannel, se usaran los puertos Gigabit Ethernet, configurados con el protocolo LACP de IEEE 802.3ad. Además en estos switches se configuraran los enrutamiento dinámicos a través de los protocolos OSPF.

- **Configuración de los switches de la capa de distribución.**

  Los switches de distribución serán configurados como servidores de los switches de la capa acceso, además en estos switches serán configurados los VLANs establecidas en la tabla A2-6.

  Para tener conexión con el resto de los equipos, se crean enlaces troncales (una troncal es una conexión entre dos equipos de red) para conducción de las VLANs. Se ha establecido que los puertos FastEthernet 0/1-10, serán los puertos troncales, Para dicha configuración se usaron los siguientes comandos:

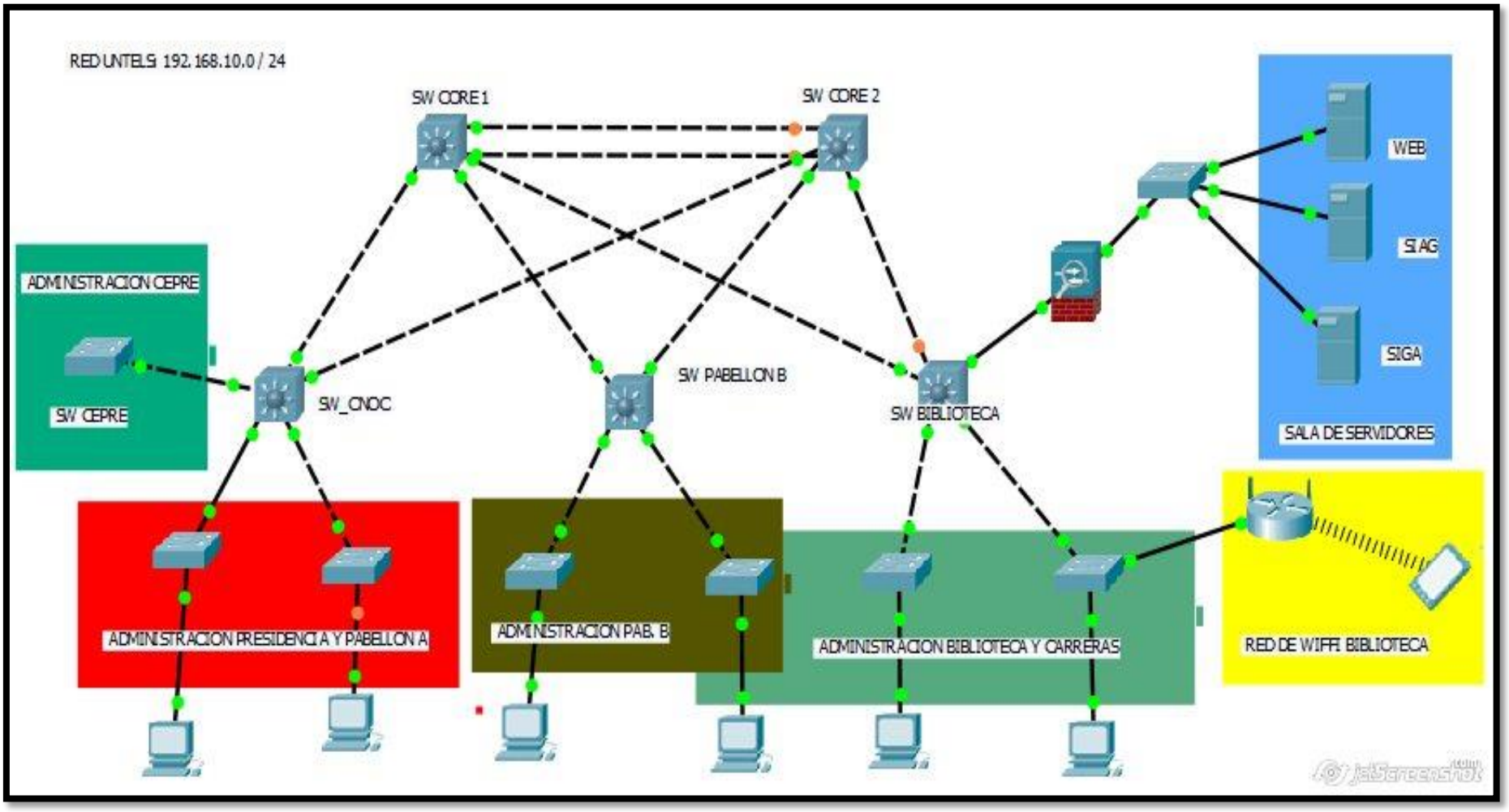


Figura 3-6: Arquitectura lógica de la universidad simulada en Packet Tracer.

Fuente: Diseño propio, basado en el modelo jerárquico de tres capas.

```
configure  terminal
interface range FastEthernet 0/1-10
switchport trunk allowed vlan 100,101,102,103,104,105,106
switchport mode trunk
switchport nonegotiate
channel-group 1 mode active
```

Figura 3-7: Comandos para configuración de puertos Troncales.

Fuente: Configuración propio, referencia ICND1.

- **Configuración de los switches de capa de acceso.**

  Cada uno de los switches que conforman la capa de acceso, serán configurados en modo cliente de acuerdo a las jefaturas que existen en cada pabellón. También se configuraran los enlaces trocales en estos equipos para tal proceso se ha establecido los puertos FastEthernet 0/24 para dicha configuración.

```
configure  terminal
interface range FastEthernet 0/24
switchport trunk allowed vlan 100,101,102,103,104,105,106
switchport mode trunk
switchport nonegotiate
channel-group 1 mode active

interface FastEthernet0/1
switchport access vlan 100
switchport mode access
spanning-tree portfast
```

Figura 3-8: Configuración de puertos troncales y acceso.

Fuente: Configuración propia, referente a ICND1.

3.2.2.5. Seguridad en los puertos

Para la mantener la seguridad en la red, se ha establecido ACL's y configuración de puertos a través de MAC ADRESS de equipo de acceso. Las listas de acceso, están implementadas en la capa de distribución, dichas definiciones se establecerán mediante la ip o el segmento de red, para tal

configuración contamos con tres tipos, ACL estándar, ACL extendida estas pueden ser Nombras o numeras.

```
10 permit 192.168.19.0 0.0.0.31
```

Para seguridad por puertos se configuraran mediante las mac address de cada computador conectada. Para dicho efecto se usa el siguiente comando.

```
interface FastEthernet0/1
 switchport trunk allowed vlan 100,200,300,400,500,600
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
```

Figura 3-9: Configuración de puertos a través del mac address.

Fuente: Configuración propia, referencia ICND1.

3.2.2.6 Costo estimado de los equipos.

La implementación de una red jerárquica conlleva costos que se deben ser tomados en cuenta, estos costos servirán para tener una idea más completa de esta propuesta.

Tabla 3-7: Costos de los Switches Cisco.

Ítem	Descripción	Cantidad	P. U	P.T
1	Switch Capa 3, modelo 4500, 24 puertos, Power Over Ethernet	2	$5900	$11800
2	Switch Capa 3, modelo 3750, 24 puertos, Power Over Ethernet	3	$ 4500	$ 13500
			TOTAL DE COSTOS DE HARDWARE	$ 25300

Fuente: partners de cisco. Costos referenciales hasta el 15 de julio 2016.

3.2.3. Pruebas

3.2.3.1. Tolerancia a fallos

La red esta implementada para superar esta prueba, debido que los equipos están conectadas redundantemente. Como se aprecia en la figura 3-10, se ha simulado que el SW CORE 1 está en avería, sin embargo la arquitectura lógica sigue operativo ya que tenemos conectividad con los switches de distribución y los equipos de acceso.

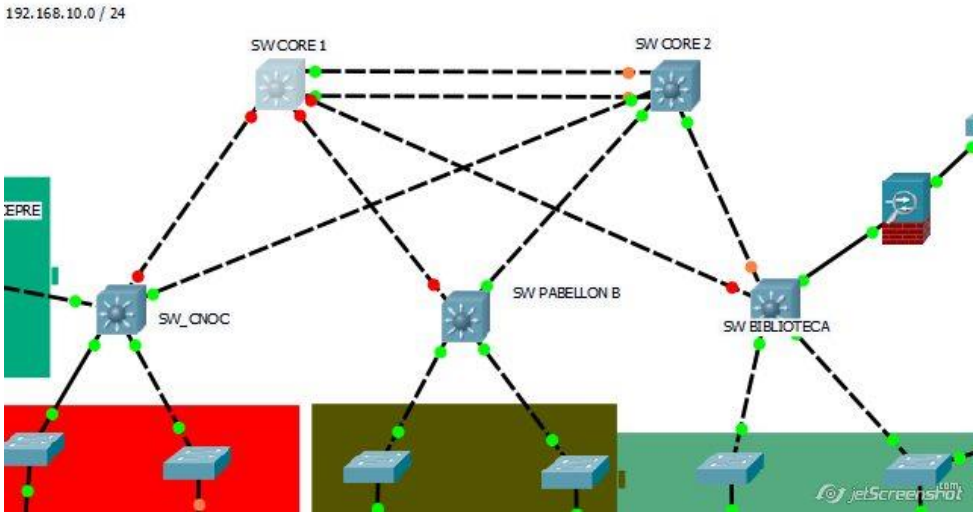


Figura 3-10: Prueba de tolerancia a fallos.

3.2.3.2. Calidad de Servicio.

La arquitectura lógica esta implementada para dar prioridades cuando el usuario requiera, es así que los Switches de núcleo están configuradas para realizar Telepresencia al momento que se requiera.

3.2.3.3. Escalabilidad

La red está completamente diseñada para ser escalable ya que nos permite expandir la capa de acceso, según los requerimientos solicitados (Por ejemplo en la figura 3-11, se conectó un switch para acceso al switch de distribución

de la biblioteca), además los equipos están configuras con el protocolo VTP, para tener la facilidad de configurar un nuevo de acceso a la red.

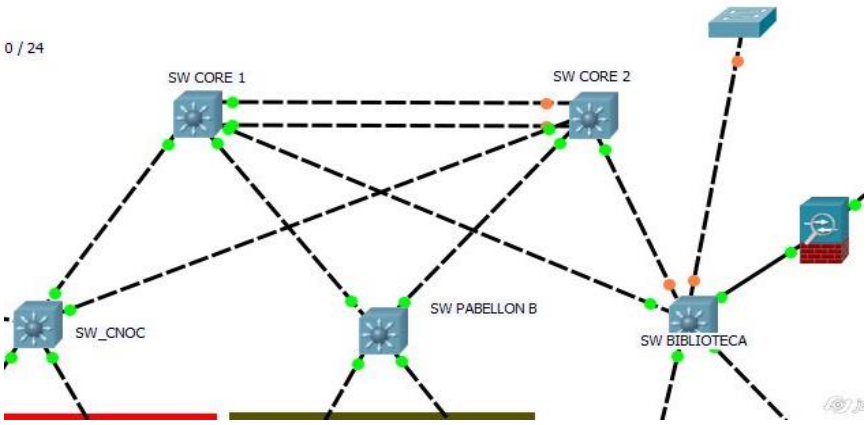


Figura 3-11: Escalabilidad de la arquitectura.

3.2.3.4. Seguridad

La arquitectura está diseñada para tener seguridad en tres modos:

- Están configurado las listas de acceso de acuerdo a los requerimientos del área de la OTIC.
- Los switches de acceso están configuradas con seguridad por puerto a través de la mac address.
- Por último se cuenta con un firewall para tener el control de los servidores.

Figura 3-12: Seguridad de la red.

3.3. REVISION Y CONSOLIDACION DE RESULTADOS

Además de los beneficios que una red jerárquica de tres capas nos brinda: tal como la escalabilidad, redundancia, seguridad, facilidad de administración y mantenimiento, se realizaron prueba de broadcast con el software Packet Tracer.

Uno de los parámetros que se debe evaluar en una red de datos es su rendimiento, esto garantiza que la infraestructura y funcionamiento de la red sea óptima. Las pruebas se realizaron con el simulador, saturando de paquetes, a toda la arquitectura de red, como se muestra en la figura 3-13.

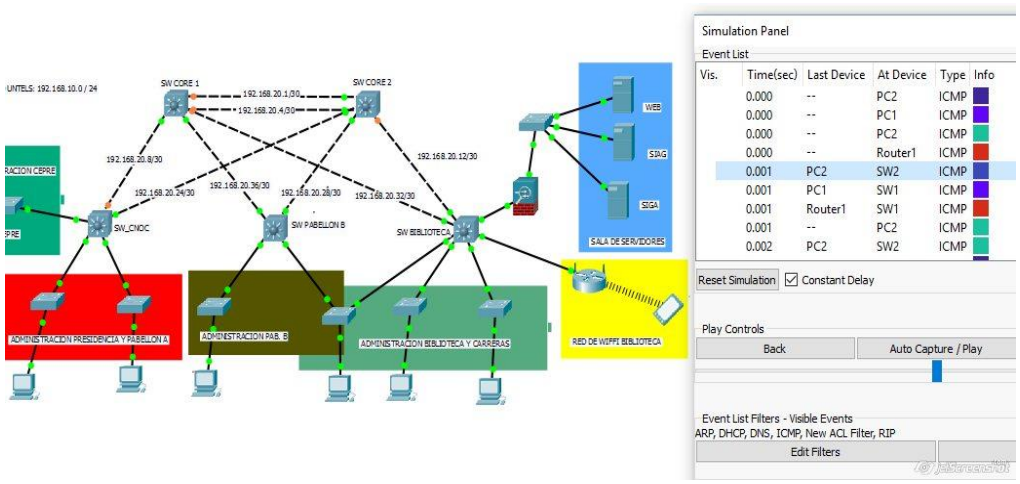


Figura 3-13: Captura de protocolos Broadcast.

Fuente: Propio, Captura de los protocolos ARP.

Para comprobar la disminución del congestionamiento de la red, se ha utilizado los datos capturados al simular la red como se muestra en la figura 3-13. Para ello se toma el porcentaje de los tres protocolos que causan más tráfico en la red, los cuales son ARP (Protocolo de resoluciones de direcciones), NBSN (Protocolo de Nombres de BIOS) y SSDP (Protocolo de descubrimiento de servicio simple), los cuales provocan la difusión masiva de Broadcast entre los equipos instalados, con todo estos datos se aplica la siguiente Tabla 3-8.

Además de esto se debe mencionar el direccionamiento de IPs se ha dado de acuerdo a los equipos instalados en todas las áreas, calculados como se muestra en el capítulo 3.2.2.2 y en la tabla A2-4.

Tabla 3-8: Comparación de difusión de broadcast.

Red	Dispositivos	Porcentajes causados		
		ARP	NBNS	SSDP
Red Actual de la universidad	256	48.12%	21.08%	7.72%
Modelo Propuesto				
Edificio de la presidencia	60	1.10%	0%	0.02%
Pabellón A	200	1.03%	1%	0.03%
Pabellón B	140	1.01%	0.80%	0.01%
Biblioteca	32	0.10%	0%	0%
Promedio del porcentaje de difusión		0.81%	0.50%	0.02%
Porcentaje de disminución en relación con la arquitectura actual (0.81%/48.12%)		98.29%		

Fuente: propio, comparación de los protocolos ARP.

Como se muestra en la Tabla 3-8, el porcentaje de disminución es el 98.29% de difusión del protocolo ARP, esto nos permite tener mayor ancho de banda ya que no tendremos acumulación de broadcast y multicast en la red de datos. Además podemos concluir que la red no es plana, ya que la difusión de broadcast no supera el 35% establecido por cisco.

Esto es debido que en la red jerárquica los paquete enviados no viajan a través de la toda la red de datos, sino viajan solo a la VLAN específica, la segmentación de la red en varias VLANs hace que por cada una haya un dominio de broadcast, ya que el tráfico es direccionado a la VLAN especifica. La

asignación de IPs, seguirá proporcionándose a través del protocolo DHCP, para tener la facilidad de asignación cuando la red se implemente, para tener la seguridad y no permitir la conexión de equipos (Access Point) externos, para ello se configura cada puerto de acceso con el Mac Address de la PC, como se muestra en la figura 3-9.

En base a la propuesta diseñada y las pruebas realizadas con el simulador, se encontró varios beneficios en la red de datos propuesta. Como se muestra en la siguiente tabla.

Tabla 3-9: Comparación de la arquitectura actual con la arquitectura propuesta basado en el modelo jerárquico de tres capas.

Red actual de datos	Red Jerárquica de tres capas
La red actual muestra que la capa de núcleo y de distribución se combinan lo que hace que la comunicación colapse y por consecuencia muy lenta.	La red jerárquica propuesta, al tener funciones específicas hace posible que la productividad y velocidad se incrementen.
La red actual cuenta con cierto nivel de seguridad, pero sin embargo puede darse el caso de que la información que fluye por la red pueda ser interceptada o también se puede ingresar a otras pc para hurtar la información. También puede darse el caso de conectar una maquina	Al implementar el modelo jerárquico, incrementa la seguridad, ya que cada área estará dentro de una VLAN independiente, sin necesidad que se encuentren en otras redes. En caso que se conecte una maquina infectada con virus a un segmento afectara a ese segmento, evitando de

infectada con virus la cual puede afectar toda la red.	esta manera que el virus se propague por toda la red.
Al producirse una falla en la red, se ve afectada toda la red de datos, quedándose así incomunicada. Para identificar la falla podría tardarse varios minutos u horas.	Con el modelo jerárquico propuesto, se identifican con mayor facilidad cual es el segmento de la red afectada, por ende aislarlo y darle solución en menor tiempo debido que esta arquitectura está conectada redundante mente.
Algunos equipos tales como Switches de acceso no son programables, debido a esto no se puede implementar la seguridad por puerto.	Con el modelo jerárquico se utilizara switches programables para garantizar la seguridad por puertos, además nos permitirá la fácil administración.
El crecimiento de la red puede implicar el rediseño de toda la red de datos, para agregar nuevos dispositivos.	Permite el crecimiento de la red con mucha facilidad, generalmente este crecimiento se da en la capa de acceso, ya que si se quiere interconectar más equipos simplemente se agrega uno más y la configuración de los equipos se puede reproducir de un equipo ya configurado.

CONCLUSIONES

- Al implementar el modelo jerárquico de tres capas, permite tener una red organizada, ofreciendo disponibilidad de crecimiento, agregando dispositivos de red desde la capa de acceso hasta la capa de distribución, también hace posible la reutilización de la misma configuración para los nuevos dispositivos. Por lo que ya no es necesario rediseñar toda la red para adaptarla al nuevo requerimiento de la institución.
- Al implementarse la red jerárquica, nos permite tener una mejora considerable en su rendimiento. Debido a que el protocolo ARP disminuye en un 98%, esto nos permite tener mayor ancho de banda ya que no tendremos acumulación de broadcast y multicast en la red de datos.
- El fraccionamiento de la red en redes más pequeñas, usando las soluciones VLSM y redes virtuales, nos evita el tráfico innecesario de red, permitiendo así un uso eficiente del ancho de banda a las áreas administrativas, además poder disponer de una infraestructura eficiente, escalable y segura.
- Cuando se crean VLANs en una red de datos, todos los equipos pertenecen a una, y estas se interconectan si necesidad de estar ubicados dentro de un mismo espacio específico, lo que permite a la institución adaptarse a los cambios de ubicación física del personal dentro del campus.
- Cuando existe un daño en la red jerárquica, se analiza desde la capa de acceso hasta la capa de núcleo, identificando con exactitud el segmento de la red donde se encuentra la falla, permitiendo aislar el problema sin afectar el resto de la red y solucionarlo de manera eficiente.

RECOMENDACIONES

- Implementar un centro de monitoreo de red (NOC) para controlar permanentemente la red e identificar fallos en la estructura, de esta manera podrán analizar y establecer soluciones óptimas al problema suscitado.
- Implementar un servidor FTP, para respaldar la configuración de los dispositivos de red, con la finalidad de restaurarlos en el momento que se requiera.
- Reorganizar la estructura de red utilizando cable UTP categoría 6.5, para incrementar la velocidad de transmisión. Este cable al no ser afectado por diafonía asegura su desempeño ya que cuenta con un separador de polietileno.
- Elaborar plan de contingencia, para los procesos más relevantes de la institución. Además se recomienda poner énfasis en la creación de políticas de seguridad, para restringir el acceso físico al NOC, así como también crear mayor seguridad para la infraestructura lógica.

BIBLIOGRAFÍA

- David Terán. (2011). Redes Convergentes: Diseño e implementación. Barcelona: Marcombo S.A.
- Jeremy Cloara, David Minutella, Heather Stevenson. (2008). CCNA Second Edition. United States of America: Pearson Education.
- Diane Tiare, Catherine Paquet. (2005). Campus Network Design Fundamentals. México: Cisco Press.
- Cisco. (2014). Campus: Resumen de Diseño. México: Cisco System, Inc.
- Cisco. (2013). Interconnecting Cisco Network Devices (ICND1). San Jose CA: Cisco System, Inc.
- Cisco. (2013). Interconnecting Cisco Network Devices (ICND2). San Jose CA: Cisco System, Inc.
- Cisco. (2014). Campus ClearAir, Technology Design Guide. San Jose CA: Cisco System Inc.
- Cisco. (2016). Campus LAN and Wireless LAN Design Summary. 1 agosto 2016, de Cisco Sitio web:
- http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2016/Campus_LAN_Wireless_LAN_Design_Aug2016.pdf
- Javier Moreno Balderrama. (2012). Normas y Estándares para un Sistema de Cableado Estructurado (SCE). 10 julio 2016, de SlideShare Sitio web: http://www.slideshare.net/riftbol/normas-y-estndares-para-un-sistema-de-cableado-estructurado-sce.

- Laura Ximena. (2009). CISCO PRIMER CAPITULO. 12 de Junio 2015, de Blog Sitio web: http://laurapita.blogspot.pe/2009/03/arquitectura-de-red.html.
- Alex Rguez. (2011). Switches - Modulo VLAN. 6 de Junio 2016, de Blog Sitio web: https://sites.google.com/site/modulovlan/3-1-presentacion-de-las-vlan/3-1-2-tipos-de-vlan.
- Flavio Nireo Gomero, Anderson Calderón Alva. (2008). Parámetros de Calidad de Servicio en Redes IP. 6 Julio 2016, de Facultad de Ingeniería Electrónica y Eléctrica de la Universidad Nacional Mayor de San Marcos Sitio web: http://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/electronica/2008_n22/pdf/a06.pdf
- CISCO VALIDATED PROFILE. (2016). Access Switching Education Vertical. 20 julio de 2016, de Cisco Sitio web: http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVP/Apr2016/CVP-Campus_Wired-Education-Apr2016.pdf.

ANEXOS

Anexo 1: Encuesta

1. ¿Cómo calificaría el rendimiento de la red actualmente?

   ☐ Pésimo ☐ Regular ☐ Bueno ☐ Muy bueno ☐ Excelente

2. ¿Cómo calificaría el acceso a internet?

   ☐ Lento ☐ Moderado ☐ Rápido ☐ Otros

3. ¿Con cuál de los problemas de la red tiene que lidiar regularmente?

   ☐ Acceso a internet

   ☐ Acceso a carpetas compartidas

   ☐ Lentitud de la red

   ☐ Otros……

4. ¿Alguna vez ha podido ingresar a equipos de otros usuarios y tomado la información?

   SI ☐ NO ☐

5. ¿Alguna vez ha tenido el problema de perder la información de su equipo?

   SI ☐ NO ☐

6. ¿Regularmente usas internet en más de dos equipos?

   SI ☐ NO ☐

7. ¿Tomas señal WiFi del área de trabajo?

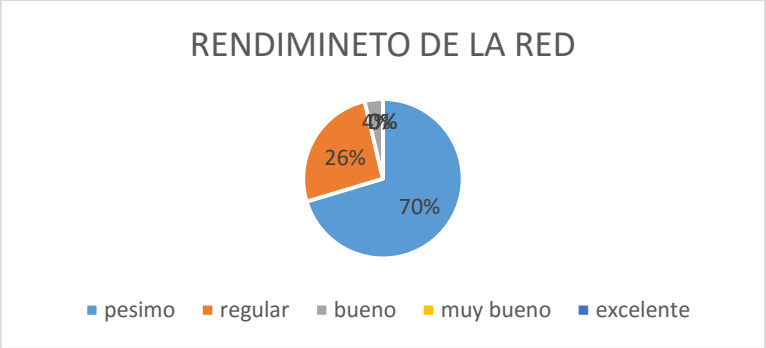
   SI ☐ NO ☐

8. ¿Alguna vez ha usado router Inalámbrico para aumentar la cantidad de equipos a usar en tu área?

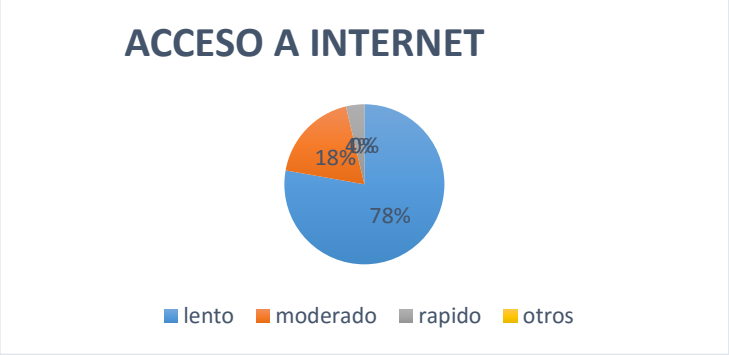
   SI ☐ NO ☐

Resultados.

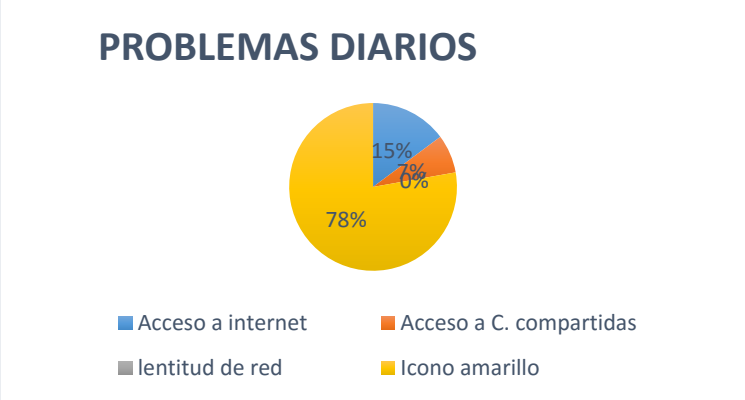
1.- ¿Cómo calificaría el rendimiento de la red actualmente?



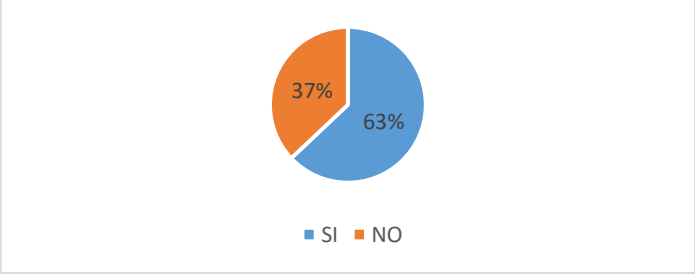
2.- ¿Cómo calificaría el acceso a internet?



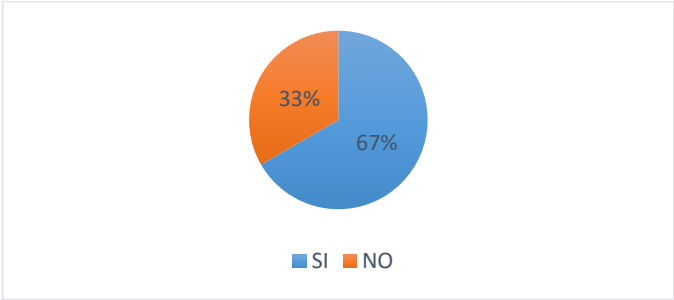
3.- ¿Con cuál de los problemas de la red tiene que lidiar regularmente?



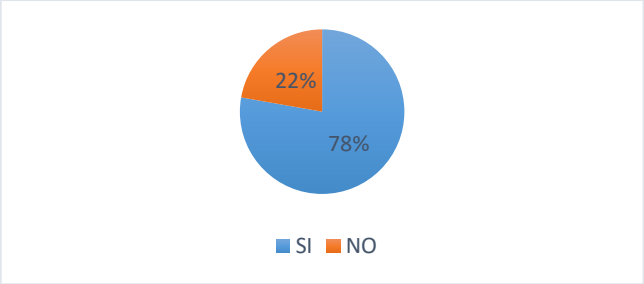
4.- ¿Alguna vez ha podido ingresar a equipos de otros usuarios y tomado la información?



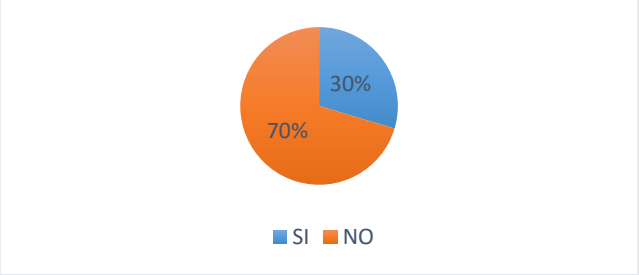
5.- ¿Alguna vez ha tenido el problema de perder la información de su equipo?



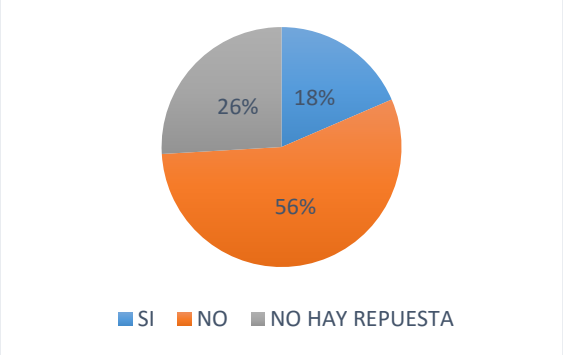
6.- ¿Regularmente usas internet en más de dos equipos?



7.- ¿Tomas señal WiFi del área de trabajo?



8.- ¿Alguna vez ha usado router Inalámbrico para aumentar la cantidad de equipos a usar en tu área?



Anexo 2: Tablas.

Tabla A2-1: Resultado del monitoreo de la red Untels.

PROTOCOLO	23-Jun	23-Jun	25-Jun	25-Jun	30-Jun	30-Jun	11-Jul	11-Jul	20-Jul	20-Jul	21-Jul	21-Jul
ARP	92134	50.30%	187813	51.85%	92026	44.66%	968	34.41%	43892	35.26%	34901	58.17%
NBNS	30538	16.67%	83012	22.92%	48149	23.37%	241	8.57%	23889	19.19%	12041	20.07%
SSDP	15421	8.42%	16143	4.46%	16548	8.03%	91	3.23%	15241	12.24%	9047	15.08%
STP	901	0.49%	1643	0.45%	1743	0.85%	254	9.03%	5454	4.38%	590	0.98%
ISMP	25987	14.19%	35441	9.78%	21794	10.58%	460	16.35%	11742	9.43%	1252	2.09%
UDP	2874	1.57%	3583	0.99%	13667	6.63%	48	1.71%	5482	4.40%	712	1.19%
BROWSER	348	0.19%	15841	4.37%	657	0.32%	157	5.58%	3940	3.17%	282	0.47%
IPSX SAP	6481	3.54%	12915	3.57%	9719	4.72%	451	16.03%	12941	10.40%	727	1.21%
MS NLB	8492	4.64%	5841	1.61%	1741	0.84%	143	5.08%	1897	1.52%	451	0.75%
TOTAL	183176	100.00%	362232	100.00%	206044	100.00%	2813	100.00%	124478	100.00%	60003	100.00%

Fuente: Propio. Monitoreo realizado en 5 días, entre el 23 junio y 21 de julio 2016. Se muestra los principales protocolos de un aproximado de 150000 datos.

Tabla A2-2: VLANs e IP actuales de la UNTELS.

VLAN	AREAS	IP
DATA CENTER	DATA CENTER	10.0.0.0
ADMISION	OFICINA DE ADMISION	192.168.11.0
ALMACEN	ALMACEN	192.168.12.0
BIBLIOTECA	BIBLIOTECA	192.168.13.0
CAJA	CAJA	192.168.14.0
COOP TEC	COOPERACION TECNICA	192.168.15.0
COORDLAB	COORD. DE LABORATORIOS	192.168.16.0
ECONOMIA	OFICINA DE ECONOMIA	192.168.17.0
EXTENSIONU	EXTENSION UNIVERSITARIA	192.168.18.0
GYM	GIMNASIO	192.168.19.0
IDIOMAS	CENTRO DE IDIOMAS	192.168.20.0
IMAGEN	IMAGEN INSTITUCIONAL	192.168.21.0
INFORMATICA	OFICINA DE INFORMATICA	192.168.22.0
INFRAESTRUCTURA	OFICINA DE INFRAESTRUCTURA	192.168.23.0
INVESTIGACION	AREA DE INVESTIGACION	192.168.24.0
OBU	OFICINA DE BIENESTAR UNIVERS.	192.168.25.0
OCI	OFICINA DE COOPERACION I.	192.168.26.0
OGBSG	OFICINA GENERAL B. S. G.	192.168.27.0
RRHH	RECURSOS HUMANOS	192.168.28.0
PLANEAMIENTO	OFICINA DE PLANEAMIENTO	192.168.29.0
PLANIFICACION	OFICINA DE PLANIFICACION	192.168.30.0
PRESIDENCIA	OFICINA DE PRESIDENCIA	192.168.31.0
PRODUCCION	AREA DE PRODUCCION	192.168.32.0
SALAPROF	SALA DE PROFESORES	192.168.33.0
VIGILANCIA	OFICINA DE VIGILANCIA	192.168.34.0
CARRERAS	OFICINAS DE CARREAS	192.168.35.0
INALAMBRICO	RED INALAMBRICA	192.168.50.0
LABMECANICA	LABORATORIO DE MECANICA	192.168.100.0
LAB1	LABORATORIO 1	192.168.101.0
LAB2	LABORATORIO 2	192.168.102.0
LAB3	LABORATORIO 3	192.168.103.0
LAB4	LABORATORIO 4	192.168.104.0
LABAUTOMA	LABORATORIO DE AUTOMATIZACION	192.168.105.0
LABELECTRONICA	LABORATORIO DE ELECTRONICA	192.168.106.0
LABFISICA	LABORATORIO DE FISICA	192.168.107.0
LABNEGOCIOS	LABORATORIO DE NEGOCIOS	192.168.108.0
LABPROYECCION	LABORATORIO DE PROYECCION	192.168.109.0
LABSOFTWARE	LABORATORIO DE SOFTWARE	192.168.110.0
LABTELECO	LABORATORIO DE COMUNICACIONES	192.168.111.0
LABAMBIENTAL	LABORATORIO DE AMBIENTAL	192.168.112.0

LABMECANICA	LABORATORIO DE MECANICA	192.168.113.0
PABELLONA	PABELLON A	192.168.220.0
PABELLONB	PABELLON B	192.168.221.0
PABELLONC	PABELLON C	192.168.222.0

Fuente: Oficina de Tecnologías de Información y Comunicación (ODTIC)

Tabla A2-3: Servidores de la UNTELS.

SERVIDORES	
1	ADMINISION
2	AVASTECIMIENTO
3	SERVICIO ACADEMICO
4	PORTAL WEB
5	SIGA
6	SIAF
7	SERVIDOR DE REPOSITORIO
8	SERVIDOR TELEFONICO(ASTERISK)
9	SERVIDOR DHCP

Fuente: Oficina de Tecnología de Información y Comunicación (OTIC).

Tabla A2-4: Número de dispositivos para cálculo de la máscara de la red.

AREAS	HOST
RED INALAMBRICA	255
LABORATORIO DE ING. DE SISTEMAS	255
LABORATORIO DE ELECTRONICA Y TELECOMUNICACIONES	255
LABORATORIO DE AMBIENTAL	255
LABORATORIO DE MECANICA	255
OFICINA DE ADMISION	50
OFICINA DE PRESIDENCIA	50
SALA DE PROFESORES y OFICINA DE VIGILANCIA	50
OFICINAS DE CARREAS	50
DATA CENTER	20
ALMACEN	20
BIBLIOTECA	20
CAJA	20
COOPERACION TECNICA	20
OFICINA DE ECONOMIA	20

EXTENSION UNIVERSITARIA y O. DE BIENESTAR UNIVERS.	20
GIMNASIO	20
C.DE IDIOMAS, I.INSTITUCIONAL y O. DE COOPERACION INT.	20
OFICINA DE INFORMATICA	20
OFICINA DE INFRAESTRUCTURA	20
AREA DE INVESTIGACION	20
OFICINA GENERAL B. S. G.	20
RECURSOS HUMANOS	20
OFICINA DE PLANEAMIENTO	20
OFICINA DE PLANIFICACION	20
AREA DE PRODUCCION	20
LABORATORIO DE FISICA	20
COORD. DE LABORATORIOS	10

Fuente: Oficina de Tecnología de Información y Comunicación (OTIC)

Tabla A2-5: Rango de Direcciones IP.

N°	**HOST**	n	MASCARA	RANGO DE IP
1	255	8	255.255.255.0	192.168.10.1 - 192.168.10.255
2	255	8	255.255.255.0	192.168.11.1 - 192.168.11.255
3	255	8	255.255.255.0	192.168.12.1 - 192.168.12.255
4	255	8	255.255.255.0	192.168.13.1 - 192.168.13.255
5	255	8	255.255.255.0	192.168.14.1 - 192.168.14.255
6	255	8	255.255.255.0	192.168.15.1 - 192.168.15.255
7	50	6	255.255.255.192	192.168.16.1 - 192.168.16.63
8	50	6	255.255.255.192	1925.168.16.64 - 192.168.16.127
9	50	6	255.255.255.192	192.168.16.128 - 192.168.16.191
10	50	6	255.255.255.192	192.168.16.192 - 192.168.16.255
11	20	5	255.255.255.224	192.168.17.0 - 192.168.17.31
12	20	5	255.255.255.224	192.168.17.32 - 192.168.17.63
13	20	5	255.255.255.224	192.168.17.64 - 192.168.17.95
14	20	5	255.255.255.224	192.168.17.96 - 192.168.17.127
15	20	5	255.255.255.224	192.168.17.128 - 192.168.17.159
16	20	5	255.255.255.224	192.168.17.160 - 192.168.17.191

17	20	5	255.255.255.224	192.168.17.192 - 192.168.17.223
18	20	5	255.255.255.224	192.168.17.224 - 192.168.17.255
19	20	5	255.255.255.224	192.168.18.0 - 192.168.18.31
20	20	5	255.255.255.224	192.168.18.32 - 192.168.18.63
21	20	5	255.255.255.224	192.168.18.64 - 192.168.18.95
22	20	5	255.255.255.224	192.168.18.96 - 192.168.18.127
23	20	5	255.255.255.224	192.168.18.128 - 192.168.18.159
24	20	5	255.255.255.224	192.168.18.160 - 192.168.18.191
25	20	5	255.255.255.224	192.168.18.192 - 192.168.18.223
26	20	5	255.255.255.224	192.168.18.224 - 192.168.18.255
27	20	5	255.255.255.224	192.168.19.0 - 192.168.19.31
28	20	5	255.255.255.224	192.168.17.32 - 192.168.19.63
29	20	5	255.255.255.224	192.168.19.64 - 192.168.19.95
30	20	5	255.255.255.224	192.168.19.96 - 192.168.19.127

Fuente: propuesta propia.

Tabla A2-6: VLANs propuestos.

AREAS	NOMBRE DE VLANS	IP ASIGNADOS
RED INALAMBRICA	INALAMBRICA_B	192.168.10.1 - 192.168.10.255
LABORATORIO DE ING. DE SISTEMAS	LAB_SISTEMAS	192.168.11.1 - 192.168.11.255
LABORATORIO DE ELECTRONICA Y TELECOMUNICACIONES	LAB_TELECOMUNICACIONES	192.168.12.1 - 192.168.12.255
LABORATORIO DE AMBIENTAL	LAB_AMBIENTAL	192.168.13.1 - 192.168.13.255
LABORATORIO DE MECANICA	LAB_MECANICA	192.168.14.1 - 192.168.14.255
TELEFONOS IP	TELEFONOS_IP	192.168.15.1 - 192.168.15.255
OFICINA DE ADMISION	O_ADMISION	192.168.16.1 - 192.168.16.63
OFICINA DE PRESIDENCIA	O_PRESIDENCIA	1925.168.16.64 - 192.168.16.127
SALA DE PROFESORESO FICINA DE VIGILANCIA	PROF_O_VIGILANCIA	192.168.16.128 - 192.168.16.191
OFICINAS DE CARREAS	O_CARREAS	192.168.16.192 - 192.168.16.255

DATA CENTER	DATA_CENTER	192.168.17.0 - 192.168.17.31
ALMACEN	ALMACEN	192.168.17.32 - 192.168.17.63
BIBLIOTECA	BIBLIOTECA	192.168.17.64 - 192.168.17.95
CAJA	CAJA	192.168.17.96 - 192.168.17.127
COOPERACION TECNICA	COOP_TECNICA	192.168.17.128 - 192.168.17.159
OFICINA DE ECONOMIA	O_ECONOMIA	192.168.17.160 - 192.168.17.191
EXTENSION UNIVERSITARIA O. DE BIENESTAR UNIVERS.	EXT_UNI_O_BIENESTAR	192.168.17.192 - 192.168.17.223
GIMNASIO	GIMNASIO	192.168.17.224 - 192.168.17.255
C.DE IDIOMAS I.INSTITUCIONAL O. DE COOPERACION INT.	IDIO_INSTITUCIONAL_COOP_INT.	192.168.18.0 - 192.168.18.31
OFICINA DE INFORMATICA	O_INFORMATICA	192.168.18.32 - 192.168.18.63
OFICINA DE INFRAESTRUCTURA	O_INFRAESTRUCTURA	192.168.18.64 - 192.168.18.95
AREA DE INVESTIGACION	A_INVESTIGACION	192.168.18.96 - 192.168.18.127
OFICINA GENERAL B. S. G.	O_GENERAL_B_ S_G	192.168.18.128 - 192.168.18.159
RECURSOS HUMANOS	RR_HH	192.168.18.160 - 192.168.18.191
OFICINA DE PLANEAMIENTO	O_PLANEAMIENTO	192.168.18.192 - 192.168.18.223
OFICINA DE PLANIFICACION	O_PLANIFICACION	192.168.18.224 - 192.168.18.255
AREA DE PRODUCCION	A_PRODUCCION	192.168.19.0 - 192.168.19.31
LABORATORIO DE FISICA	LAB_FISICA	192.168.17.32 - 192.168.19.63
SERVIDORES	SERVIDORES	192.168.19.64 - 192.168.19.95
COORD. DE LABORATORIOS	COORD_LABORATORIOS	192.168.19.96 - 192.168.19.127

Fuente: propuesta propia.

Anexo 3: Flujo de Costos.

Tabla A3-1: Flujo de Costos.

ITEM	DESCRIPCION	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	TOTAL
1	**ARQUITECTURA DE RED BASADO EN EL MODELO JERARQUICO DE TRES CAPAS PARA MEJORAR TRAFICO DE DATOS EN LA UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR.**	**S/. 10,500.00**	**S/. 5,500.00**	**S/. 5,250.00**	**S/. 9,416.67**	**S/. 8,333.33**	**S/. 7,500.00**	**S/. 46,500.00**
1.1	**Plan del Proyecto**	**S/. 9,000.00**						**S/. 9,000.00**
1.1.1	Análisis de factor	S/. 5,143.00						
1.1.2	Estimación de Tareas	S/. 2,571.00						
1.1.3	Evaluación de Riesgos	S/. 1,286.00						
1.2	**Desarrollo de la Infraestructura**	**S/. 1,500.00**	**S/. 5,500.00**	**S/. 5,250.00**	**S/. 9,416.67**	**S/. 8,333.33**	**S/. 2,000.00**	**S/. 32,000.00**
1.2.1	Desarrollo del modelo físico	S/. 1,500.00	S/. 5,500.00	S/. 5,250.00	S/. 4,750.00	S/. 1,000.00		
1.2.2	Desarrollo del modelo lógico				S/. 4,666.67	S/. 7,333.33	S/. 2,000.00	
1.3	**Pruebas**						**S/. 5,000.00**	**S/. 5,000.00**
1.3.1	Tolerancia de fallos						S/. 1,500.00	
1.3.2	QoS						S/. 1,000.00	
1.3.3	Escalabilidad						S/. 1,500.00	
1.3.4	Seguridad						S/. 1,000.00	
1.4	**Cierre**						**S/. 500.00**	**S/. 500.00**
1.4.1	Conformidad de Servicio						S/. 500.00	

Fuente: Propio, elaborado en software Project.

Anexo 4: Figuras.

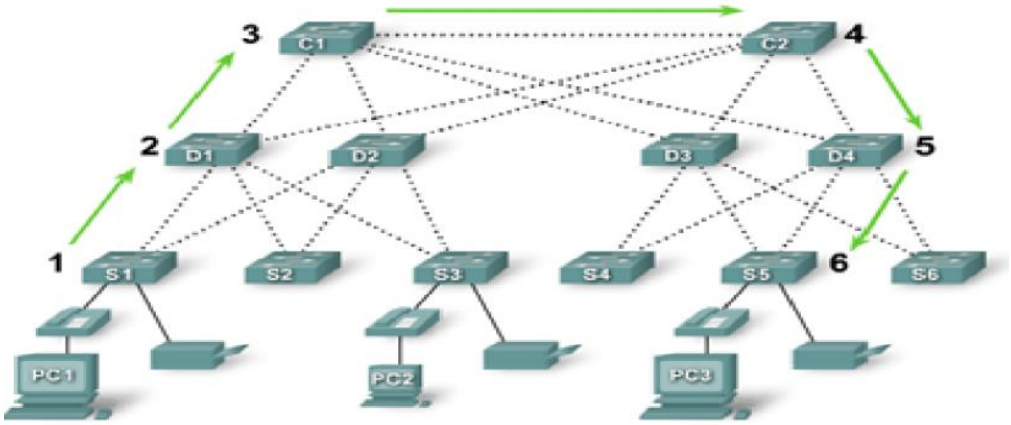


Figura A4-1: Diámetro de red en el modelo jerárquico de tres capas.

Fuente: CISCO VALIDATED DESING.

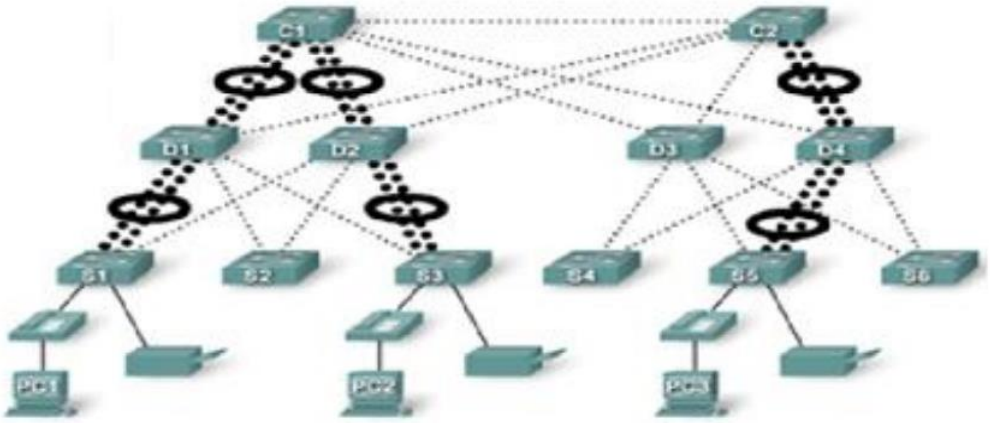


Figura A4-2: Agregado del ancho de banda en modelo jerárquico de tres capas.

Fuente: CISCO VALIDATED DESING.

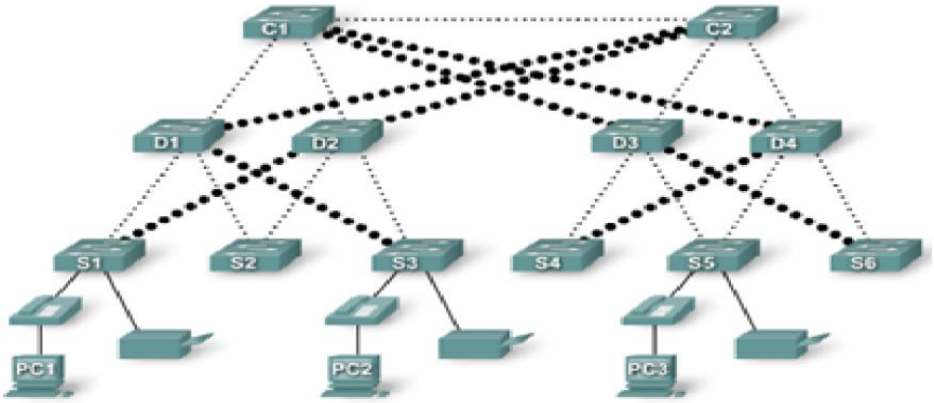


Figura A4-3: Redundancia en el modelo jerárquico de tres capas.

Fuente: CISCO VALIDATED DESING.

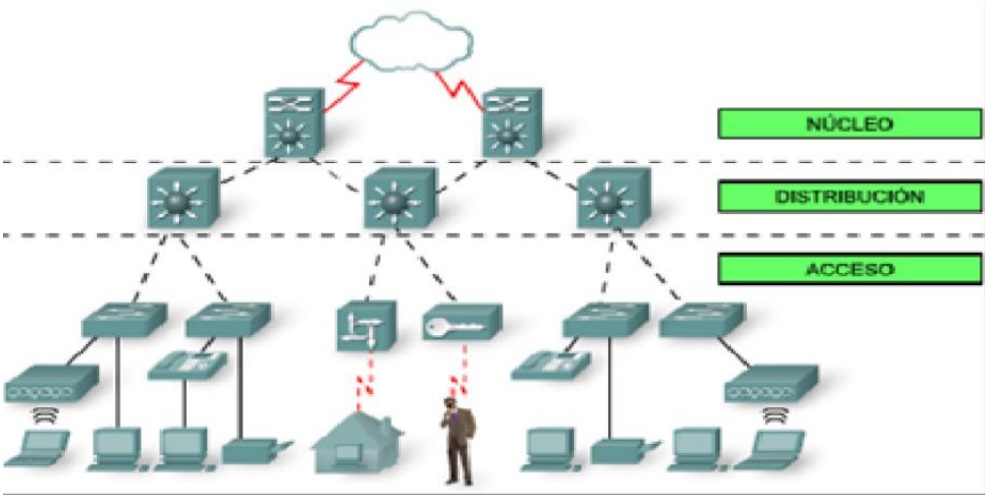


Figura A4-4: Convergencia en el modelo jerárquico de tres capas.

Fuente: CISCO VALIDATED DESING.