UNIVERSIDAD NACIONAL DE SAN MARTÍN - T

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

SEGMENTACIÓN DE LA RED Y PRIORIZACIÓN DEL ANCHO DE BANDA PARA MEJORAR EL RENDIMIENTO Y SEGURIDAD LA UNIVERSIDAD NACIONAL DE SAN MARTÍN – TARAPOTO.

Para optar el Título de:

INGENIERO DE SISTEMAS E INFORMÁTICA

Presentado por el Bachiller

Mirko Ramírez Rodríguez.

Tarapoto -Perú

2015

UNIVERSIDAD NACIONAL DE SAN MARTÍN - T

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

SEGMENTACIÓN DE LA RED Y PRIORIZACIÓN DEL ANCHO DE BANDA PARA MEJORAR EL RENDIMIENTO Y SEGURIDAD DE LA UNIVERSIDAD NACIONAL DE SAN MARTÍN – TARAPOTO.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO DE SISTEMAS E INFORMÁTICA

Presentado por:

Bachiller : **MIRKO RAMÍREZ RODRÍGUEZ**

Asesor : **Ing. Mg. Miguel Ángel Valles Coral**

Firma

SUSTENTADO Y APROBADO ANTE EL HONORABLE JURADO:

Presidente : **Ing. M. Sc. Jorge Damián Valverde Iparraguirre**

Firma

Secretario : **Ing. Mg. Pedro Antonio Gonzales Sánchez**

Firma

Miembro : **Ing. Alberto Alva Arévalo**

Firma

DEDICATORIA

A mi adorada madre Luz Angélica Rodríguez Ruiz,
y a mi querido padre Emeterio Ramírez Villanueva,
por su apoyo incondicional día a día inculcándome
buenos valores para poder ser un profesional de calidad.

A Dios, por guiar mis pasos y poner en mi camino a personas de buenos sentimientos que contribuyeron en formarme como persona con sus buenos y sabios consejos.

AGRADECIMIENTO

Al ing. Miguel Ángel Valles Coral, quien estuvo asesorándome en el desarrollo del proyecto de tesis.

A mi familia Ramírez Rodríguez y también a mis amigos quienes me brindaron su apoyo moral en cada momento

RESUMEN

La presente investigación, pretende realizar la segmentación de la red y priorización del uso del ancho de banda, debido a que el diseño actual de la red de la Ciudad Universitaria de la Universidad Nacional de San Martín – Tarapoto es una red plana con la VLan por defecto, en consecuencia no existe una adecuada segmentación del dominio de colisión y dominio de broadcast, lo que repercute drásticamente en el rendimiento de la misma a nivel de transmisión de paquetes entre los edificios que son extremos de la estrella y el nodo concentrador.

Esto ocasiona la latencia de la red en fechas y horas pico, degradándose la velocidad de transferencia por el tráfico desmedido y no segmentado de los datos y perjudicando o retardando los procesos académicos y administrativos.

Por ello, como parte de la solución a las necesidades identificadas en la presente investigación, se plantea el rediseño de la red para el soporte de redes LAN Virtuales, y de esta manera segmentar las áreas en subredes para un mayor nivel de protección; brindar seguridad (Listas de control de acceso ACL's, tecnologías emergentes en seguridad de Windows).

Posteriormente a la segmentación de la red, se realiza la priorización del ancho de banda de acuerdo a los segmentos VLan creados, identificando qué edificios necesitan de un mayor ancho de banda discriminando adecuadamente su acceso en función a su prioridad, permitiendo esto mejorar el consumo de ancho de banda (Calidad de servicio QoS), implementando protocolos para improbar la administración de la red, permitiendo disminuir costos y elevar la productividad de la UNSM-T.

SUMMARY

This research aims to make the network segmentation and prioritization of bandwidth use, because the current design of the network of the University City of the National University of San Martin - Tarapoto is a flat network with VLAN default, therefore there is no adequate segmentation collision domain and broadcast domain, which drastically affects the performance of the same level of packet transmission between buildings that are ends of the star and the hub node.

This causes network latency on dates and times peak transfer rate degraded by excessive traffic and not segmented data and damaging or retarding the academic and administrative processes.

Therefore, as part of the solution to the needs identified in this research, redesigning the network to support Virtual LAN networks arises, and thus target areas subnets for a higher level of protection; provide security Control Lists (ACL's access, security of emerging technologies in Windows).

Following the segmentation of the network, prioritizing bandwidth according to VLAN segments created is done, identifying which buildings require a higher bandwidth adequately discriminate access according to its priority, allowing it to improve consumption bandwidth (QoS), implementing protocols to disapprove the network management, enabling lower costs and raise productivity UNSM-T.

ÍNDICE

NOMENCLATURAS

a) Lista de cuadros.

b) Lista de figuras.

c) Lista de siglas, abreviaturas y símbolos.

- DHCP : Protocolo Dinámico de la Configuración del Anfitrión.
- IP : Internet Protocol.
- LAN : Red de Área Local.
- Mbps : Megabytes por segundo.
- TCP/IP : Protocolo del Control/Internet de la Transmisión.
- WAN : Red de Área Amplia.
- WLAN : Red de Área Local de la Radio.
- QoS : Calidad de servicio.
- VPN : Red Privada Virtual.

I. Planteamiento del problema

1.1 Antecedentes del problema.

Es indudable el gran impacto social, económico, cultural y sobre todo académico que ha generado el desarrollo de la tecnología de información y comunicaciones en nuestros tiempos, y la forma de comunicación se ha modernizado y globalizado.

Bajo esta perspectiva, la universidad no ha sido ajena a su influencia y utilidad como herramienta de respaldo para las comunicaciones, investigación y desarrollo y eficiencia. Hoy en día las computadoras, los softwares, protocolos y equipos de comunicación, deben estar correctamente implementados y configurados, de tal manera que, todos ellos trabajen de manera armoniosa, maximizando así sus funciones de trabajo.

Esto se traduce en un gran sistema de redes, redes de datos que vienen siendo planificadas e instaladas de acuerdo a las necesidades de cada organización o empresa.

Y ante el crecimiento exponencial de las necesidades de comunicación, en la Universidad Nacional de San Martín, se ha hecho indispensable el aumento de la infraestructura tecnológica, la misma que está respaldada sobre una carretera de comunicación con altas capacidades de transferencia como lo es la fibra óptica.

Esto implica cambios y adaptación al crecimiento tecnológico, necesidad de crear nuevos mecanismos para potenciar la investigación y desarrollo, o mejorarlos, o potenciar la productividad estos con los mismos recursos. Cambios que vienen afectando el desarrollo, la investigación, los procesos, tareas y funciones y que, deben adaptarse rápidamente a los nuevos requerimientos de trabajo, todo ello bajo la plataforma tecnológica que posee: La red de datos con backbone de fibra óptica.

A finales del año 2004, considerando que los edificios de la Ciudad Universitaria de la Universidad Nacional de San Martín – Tarapoto, aún no estaban integrados a través de una Red de Datos, la Facultad de Ingeniería de Sistemas e Informática se motivó a presentar el perfil de proyecto titulado

“SISTEMA DE CABLEADO ESTRUCTURADO Y DE NETWORKING PARA EL CAMPUS UNIVERSITARIO DE LA UNIVERSIDAD NACIONAL DE SAN MARTÍN-T”, con backbone de fibra óptica.

En la primera fase del proyecto se procedió a realizar un estudio de los servicios de telecomunicaciones y levantamiento de información acerca del número de usuarios y tipo de servicio requerido; con la finalidad de determinar el número y la ubicación de los nodos y la configuración de red de datos de la universidad. Luego se formuló la topología de red que se adapte a la distribución geográfica, demanda y crecimiento de las facultades de la Universidad Nacional de San Martín - Tarapoto.

Culminado el estudio del proyecto y propuesto a las autoridades correspondientes, a mediados de 2005, decidieron ejecutarlo, concluyendo dicha ejecución aproximadamente en marzo de 2006.

Posteriormente como parte del proceso de integración de las redes de datos, se formularon proyectos para integrar las otras 3 sedes de la UNSM-T, que incluía un estudio para la adquisición, instalación y configuración de radio enlaces que permitan interconectar la ciudad universitaria con el local central, con el complejo universitario y con la sede de la Escuela Académica Profesional de Turismo en Lamas, el proyecto incluía la instalación de torres necesarias para garantizar línea de vista entre estos locales.

Cuadro 1. Incremento de la cantidad de equipos de cómputo- UNSM-T

Año	Nro de Equipos	% Crecimiento Anual
2008	120	0
2009	140	17%
2010	180	29%
2011	409	127%
2012	522	28%
2013	612	17%
2014	767	25%
2015	856	12%

Fuente: Información obtenida de la Oficina de Informática y Comunicaciones, memorias e informes.

El crecimiento de la cantidad de equipo se cómputo en estos 8 últimos años, ha provocado que la RED tuviera un elevado congestionamiento en el tráfico de la red (degradación de la tasa de transferencia), debido a envíos (flujo externo) y transferencias (flujo interno) de páginas web, imágenes, vídeos, música.

1.2 Definición del problema.

La Universidad Nacional de San Martín cuenta con una red de datos para el Campus Universitario cuyo backbone está constituido por fibra óptica, la misma es la única a nivel regional que cuenta con dicha infraestructura la que la convierte en pionera y a la vanguardia de los adelantos tecnológicos tanto en investigación como en aplicación, comparable con las universidades más prestigiosas de la costa peruana.

Gracias a ello, las oficinas académicas y administrativas cuentan con el soporte tecnológico necesario para llevar a cabo sus actividades operativas diarias, en los plazos establecidos y seguros de contar con los medios de comunicación necesarios.

Sin embargo toda esta infraestructura tecnológica, no funcionaría sin la correcta administración de la misma. Esto involucra tareas de gestión de dispositivos, seguridad de la red, priorización, categorización de perfiles de acceso, reducción de riesgos y principalmente conocimiento de toda la infraestructura existente, así como de la interconexión de las diferentes redes con las que se cuenta en la Universidad Nacional de San Martín.

Sin embargo es justamente la administración de la misma la que adolece de muchos de los principios de diseño de redes que la hace compleja, ya que a pesar de contar con varios edificios interconectados, estos edificios y sus dependencias orgánicas administrativamente son independientes unas de las otras, sin embargo la red que las interconecta es una red plana (es decir: un solo dominio de colisión, un solo dominio de broadcast, un solo segmento de red, una sola VLan), por tanto no segmenta los paquetes de cada edificio, así como también los paquetes de datos pertenecientes a los equipos cómputo de los estudiantes y docentes que hacen uso de la red inalámbrica para sus actividades académicas, presentando además

ausencia de estándares de calidad en gestión de tráfico LAN, así como políticas de seguridad que permitan garantizar la confidencialidad de los datos y entrega al destino sin ninguna interferencia o vulneración de la seguridad y confiabilidad del paquete.

1.3 Formulación del problema.

¿La segmentación con redes virtuales y priorización del ancho de banda con QoS permitirá mejorar el rendimiento y seguridad de la red Lan Universidad Nacional de San Martín – Tarapoto?

1.4 Justificación e importancia.

De La Conveniencia

La presente investigación busca generar un impacto positivo en la administración de la red, bajo ciertos estándares y parámetros de QoS, en aras de proporcionar mejores condiciones para la investigación y desarrollo.

De la Relevancia Social

Se busca generar un impacto positivo en el rendimiento de la red de datos a fin de que los servicios implementados en la misma sean rápidos, beneficiando a toda la comunidad universitaria entre alumnos, docentes y administrativos.

De Las Implicancias Prácticas

Se pretende mejorar el rendimiento de la red, haciendo uso de tecnología, métodos y protocolos disponibles en los dispositivos existentes en la red, como son el uso de técnicas de segmentación de la red para mejorar la organización, implementación de directivas de seguridad interna y externa, racionalización, todo ello sustentado en los análisis de acuerdo a metodologías establecidas para ello.

Del Valor Teórico

Como se menciona en la relevancia social, este estudio servirá para que gracias a la aplicación de teorías estadísticas, los resultados se podrán inferir a partir de la muestra a fin de que los mismos sean representativos de toda la red de datos de la UNSM-T.

De La Utilidad Metodológica

Gracias al uso de la metodología de investigación científica y los pasos relacionados a la operacionalización de las variables, se ha diseñado un instrumento que permite recolectar datos para su posterior análisis correlacionando la variable dependiente de la independiente, el mismo que forma parte de los anexos de este documento.

1.5 Alcance y limitaciones

La investigación abarca la red de datos de la Universidad Nacional de San Martín.

II. MARCO TEÓRICO

2.1 Antecedentes de la investigación.

Título: SOLUCIÓN PARA EL SISTEMA DE COMUNICACIONES DIGITALES DE LA EMPRESA AGROINDUSTRIAL POMALCA SAC.

Autor: Samamé Villegas, Roberto Frank, 2010.

Universidad: Universidad Católica Santo Toribio de Mogrovejo,

Resumen: La presente investigación fue realizada con el objetivo de diseñar e implementar una Red Inalámbrica de Área Local (WLAN) para la empresa Agroindustrial Pomalca a fin de mejorar la comunicación y el nivel de seguridad en la red de la empresa azucarera. Ello se logró contribuyendo a la existencia de una mayor cobertura de conexión para los trabajadores y permitió mayor dinámica dentro de los flujos de trabajo: apoyando a la cadena productiva y económica de la empresa. Todo ello sustentado en la investigación de optar por la mejor tecnología de acuerdo a la infraestructura y giro de negocio.

Título: DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE RED PARA MEJORAR EL SISTEMA DE COMUNICACIÓN EN EL PROYECTO ESPECIAL DE INFRAESTRUCTURA DE TRANSPORTE NACIONAL- PROVIAS NACIONAL-ZONAL II LAMBAYEQUE.

Autor: Cotrina Reaño, Oscar Alexander y Guevara Flores, Liliana Arlita.

Universidad: Universidad Católica Santo Toribio de Mogrovejo.

Resumen: La tesis trata del Diseño e implementación de un sistema de red para mejorar el sistema de comunicación en el Proyecto Especial de Infraestructura de Transporte Nacional – PROVIAS NACIONAL, considerando las oficinas de su dependencia la ZONAL II LAMBAYEQUE, ubicadas en la avenida Santa Victoria Nº719 – Chiclayo y las estaciones de peaje de Mocce y Mórrope, ubicadas en la Panamericana Norte, Ramal Nororiental y Ramal Norte, respectivamente. Se concluyó que el uso de VPN es un método de acceso seguro desde puntos externos a la red LAN, también se concluyó que la implementación de directivas de

seguridad a través de Active Directory de Windows permitió desplegar las restricciones que se plantearon para un nivel de seguridad óptimo a nivel de usuario.

Correlación. Está relacionada con el proyecto en desarrollo, en la medida en que ambas establecen propuestas de solución y mejora en la conectividad de los distintos componentes del sistema de comunicación; todo ello apoyado en un Sistema de Red (LAN/WAN) y tecnologías de seguridad, performance y aplicación de un conjunto de software para monitorear su rendimiento. Ello permite que la propuesta desarrollada, tome como referencias algunas estrategias de éxito aplicadas en el antecedente, como el uso de VPN's y directivas de seguridad internas como Active Directory como instrumento de seguridad

Título: "Implementación y Administración de una Intranet en la Red Asistencial Lambayeque de EsSalud"

Autor: Gonzalo Rojas, Luis

Universidad: Universidad Señor de Sipán

Resumen: Esta tesis se basó en el uso de la tecnología como factor óptimo en la implementación de la Intranet dentro del sector salud, el uso de tecnologías de información y de las telecomunicaciones desde una perspectiva de modernización, destacando su importancia dentro del plan estratégico de la institución, con los cual se buscó solucionar un conjunto de deficiencias en el flujo de la información, como prolongados tiempos de espera, trámite documentario innecesario, información incompleta, etc. Por todo ello, la propuesta pretendió minimizar el impacto que genera toda esta problemática, factor común en muchas instituciones. Por ello su aportación es importante desde el punto de vista de un modelo a seguir para otras entidades del mismo rubro.

Conclusiones: La implementación de esta propuesta tecnológica, se relaciona en la medida que busca solucionar el problema que presenta la Red Asistencial Lambayeque de EsSalud, mediante el análisis previo del conjunto de deficiencias, tomando valores, y obteniendo la mejor alternativa de solución dentro de la plataforma de las Redes informáticas con soporte web. Si bien aquí se propone el uso de herramientas de administración de la red, no se ha evaluado el impacto de esta herramienta a nivel del uso de ancho de banda, tecnología de protocolos que estas herramientas usan como SNMP. Del mismo modo el presente proyecto se propone mejorar la plataforma tecnológica de las comunicaciones con la utilización de herramientas o aplicativos, Pilas de Protocolos de Red, Estándares de calidad en Lan's, Directivas de Seguridad todo ello con la premisa de atacar deficiencias tecnológicas en la empresa, que si bien son distintas por el giro del negocio, convergen en la medida que obstaculizan los procesos de la institución.

Título: Proyecto de Interconexión de Agencias Financieras Chiclayo-Tumán

Autor: Cotrina Orrego María Cecilia

Universidad: Universidad Nacional Pedro Ruiz Gallo.

Resumen: El proyecto analizó y diseñó la interconexión de las agencias financieras Cooperativa de Ahorro y Crédito Tumán con la agencia sucursal ubicada en el centro de la ciudad de Chiclayo, donde se propuso implementar una tecnología que sea segura y eficiente sin incurrir para ello en altos costos. El autor recomendó que es necesario dimensionar el requerimiento en función a los criterios de distancia a cubrir y servicios disponibles. Se concluyó que la interconexión de las agencias respondía a las exigencias del mercado y la competitividad, usando para ello, la tecnología como herramienta indispensable para el apoyo del plan estratégico de la empresa.

Título: DISEÑO DE RED ESTRUCTURADA DE DATOS CON VLAN'S APLICADO EN LA MUNICIPALIDAD DISTRITAL DE PUERTO ETEN

Autor: Gonzales Vargas, Elmer.

Universidad: Universidad Nacional Pedro Ruiz Gallo, 2003

Resumen: Este estudio buscó incrementar la seguridad de datos y la información dentro de la red en la Municipalidad Distrital de Puerto Eten, proponiendo un mejor control en el Dominio Broadcast y la Gestión de la Red, sugiriendo la implementación de una Red Virtual Local para lograr este objetivo. Se demostró que la implementación de VLAN proporciona una serie de beneficios como: Segmentación de red, división y control del dominio broadcast, división lógica de una LAN basada en la estructura y nivel organizacional, seguridad a nivel de la capa de Red es decir a nivel IP.

Título: Rediseño de la Red LAN del Hospital Belén de Trujillo.

Autor: De la Torre Battifora, Miguel Ángel

Universidad: Universidad César Vallejo, 2011.

Resumen: El proyecto tuvo como finalidad rediseñar la red LAN del hospital, partiendo de un análisis de la problemática actual, cuyos hechos más evidentes denotan una lentitud o latencia de la red, además de un cableado estructurado no estandarizado sin considerar los patrones de diseño mínimo. Se concluyó que para la implementación de una solución con VLAN es necesario que se asegure primero que a nivel físico (cableado + equipos activos + pasivos) se tenga un diseño de acuerdo a los parámetros.

Título: Rediseño de la red Lan del Hospital Eugenio Espejo para soporte de videoconferencia y diseño de la red de interconexión con hospitales de la ciudad de Quito

Autor: Olipa Buendía, Yenny Cristina y Yupanqui Cushicondor, Isabel Cristina

Universidad: Escuela Politécnica Nacional de Quito

Resumen: Se planteó el rediseño de la red LAN del Hospital Eugenio Espejo para soporte de videoconferencia, por ello se presenta la situación actual de la red LAN, tanto en la parte pasiva como activa de la red; el análisis de tráfico de la red, las políticas de administración y seguridad con la que actualmente trabajan. Una de las conclusiones que se mencionaron hace referencia a que en el rediseño se priorizó el tipo de información crítica, que para este caso fue video y voz. El tipo de información tuvo que tener prioridad sobre el ancho de banda; para lograr esto se implementó QoS en todos los equipos activos.

Título: DISEÑO E IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL PARA LA EMPRESA ELÉCTRICA QUITO S.A., MATRIZ LAS CASAS, PARA LA TRANSMISIÓN DE DATOS Y VOZ SOBRE IP

Autor: PABLO ANDRÉS DÍAZ ALVEAR

Universidad: Escuela Politécnica Nacional – Quito.

Resumen: En esta investigación se concluyó que la implementación de VLAN es una solución para cubrir las necesidades más urgentes en el aspecto de comunicación-seguridad en la red de datos de la Empresa Eléctrica Quito S.A. (E.E.Q.S.A.); además esta solución se encuentra en el dominio del modelo de referencia TCP/IP. Además de solucionar las necesidades o requerimientos, se determinó que las VLan's también son una solución para lo planificado y proyectado de tener soluciones a las futuras necesidades y aplicaciones que ingresen y sean parte de la red de datos, como por ejemplo las aplicaciones multimedia (VoIP, Telefonía IP, Videoconferencia, etc.).

Título: Análisis de Tráfico de una Red Local Universitaria

Autor: Carina Vaca.

Universidad: Escuela Politécnica Nacional – Quito, 2010.

Resumen: El propósito del trabajo fue analizar el tráfico de una red

local universitaria (DICC), mediante un software comercial, Tracer Plus Ethernet, se estudió el flujo de información generado por los sistemas administrativos y académicos de la universidad. El tráfico fue monitoreado a nivel de las capas 2 y 3 del modelo OSI. El desempeño de la red se caracterizó mediante los parámetros Cantidad de Tráfico, Tasa de Transferencia y el Porcentaje de Utilización. Se determinó que la red universitaria, bajo la estructura actual, tiene un comportamiento dentro de los estándares recomendados.

Conclusiones: Este estudio nos da pautas para cuantificar la realidad problemática así como la obtención de resultados. Dentro de las recomendaciones, sugiere realizar un rediseño para mejorar la eficiencia del tráfico LAN, considerando la implementación de nuevos servicios. Esto hace posible que el tráfico generado circule de manera óptima aun con las nuevas aplicaciones implementadas. Paralelamente, la aplicación de políticas de calidad de servicio o de clasificación del tráfico, permitirán dar prioridad a la data sensible.

2.2 Definición de términos.

Globalizado:

La globalización es un proceso histórico de integración mundial en los ámbitos político, económico, social, cultural y tecnológico.

Software:

Se conoce como software al equipo lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Protocolos:

En informática y telecomunicación, un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información.

Redes de datos:

Se denomina red de datos a aquellas infraestructuras o redes de comunicación que se ha diseñado específicamente a la transmisión de información mediante el intercambio de datos.

Carretera de comunicación:

"Carrtera de la comunicacion" fue un término popularizado durante la década de 1990 para referirse a la red de los sistemas de comunicaciones digitales y telecomunicaciones asociadas y orientadas al transporte global de información y conocimiento

Fibra óptica:

La fibra óptica es un medio de transmisión, empleado habitualmente en redes de datos y telecomunicaciones, consistente 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.

Backbone de fibra óptica:

La palabra backbone se refiere a las principales conexiones troncales de Internet. Están compuestas de un gran número de routers interconectados comerciales, gubernamentales, universitarios y otros de gran capacidad que llevan los datos a través de países, continentes y océanos del mundo mediante cables de fibra óptica.

Networking:

Es acudir a actividades y eventos con el fin de incrementar su red de contactos profesionales y buscar oportunidades de negocio.

Nodos:

En informática y en telecomunicación, de forma muy general, un nodo es un punto de intersección, conexión o unión de varios elementos que confluyen en el mismo lugar

Topología de red:

La topología de red se define como el mapa físico o lógico de una red para intercambiar datos.

Radio enlaces:

Se denomina radio enlace a cualquier interconexión entre los terminales de telecomunicaciones efectuados por ondas electromagnéticas.

Línea de vista:

La propagación de la línea de visión se refiere a la radiación electromagnética o a la propagación de ondas acústicas.

Tasa de transferencia:

En informática y telecomunicaciones, el término tasa de bits (en inglés: bit rate), a menudo tasa de transferencia, define el número de bits que se transmiten por unidad de tiempo a través de un sistema de transmisión digital o entre dos dispositivos digitales.

Dominio de colisión:

Un dominio de colisión es un segmento físico de una red de computadores donde es posible que las tramas puedan "colisionar" (interferir) con otros. Estas colisiones se dan particularmente en el protocolo de red Ethernet.

Dominio de broadcast:

Un dominio de difusión o broadcast es una red lógica de dispositivos que comparten básicamente la misma subred y la misma puerta de enlace.

Segmento de red:

Segmento de red es un sinónimo de LAN: es un conjunto de equipos (computadoras y periféricos) conectados en red.

VLan:

Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

Paquetes de datos:

Paquete de red o paquete de datos es cada uno de los bloques en que se divide la información para enviar, en el nivel de red

QoS:

QoS o Calidad de Servicio (Quality of Service, en inglés) es el rendimiento promedio de una red de telefonía o de computadoras, particularmente el rendimiento visto por los usuarios de la red. Cuantitativamente mide la calidad de los servicios que son considerados varios aspectos del servicio de red, tales como tasas de errores, ancho de banda, rendimiento, retraso en la transmisión, disponibilidad, jitter, etc.

WLAN:

Una red de área local inalámbrica, también conocida como WLAN (del inglés wireless local area network), es un sistema de comunicación inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de éstas.

Active Directory:

Active Directory (AD) es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos (principalmente LDAP, DNS, DHCP, Kerberos...).

Intranet:

Una intranet es una red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización.

TCP/IP:

El modelo TCP/IP describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red.

VoIP:

Es un grupo de recursos que hacen posible que la señal de voz viaje a través de internet empleando un protocolo IP (protocolo de internet). Esto significa que se envía la señal de voz en forma digital.

2.3 Bases teóricas

Para pequeñas y medianas empresas, la comunicación digital de datos, voz y video es esencial para la supervivencia de la empresa. En consecuencia, una LAN con un diseño apropiado es un requisito fundamental para hacer negocios en el presente. El usuario debe ser capaz de reconocer una LAN bien diseñada y seleccionar los dispositivos apropiados para admitir las especificaciones de las redes de una empresa pequeña o mediana.

En este capítulo, el lector comenzará a explorar la arquitectura de la LAN conmutada y algunos de los principios que se utilizan para diseñar una red jerárquica.

2.3.1 Modelo de redes jerárquicas.

La construcción de una LAN que satisfaga las necesidades de empresas pequeñas o medianas tiene más probabilidades de ser exitosa si se utiliza un modelo de diseño jerárquico. 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.

El diseño de 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 en una red hace que el diseño de la red se vuelva modular y esto facilita la escalabilidad y el rendimiento. El modelo de diseño jerárquico típico se separa en tres capas: capa de acceso, capa de distribución y capa núcleo. Un ejemplo de diseño de red jerárquico de tres capas se observa en la figura.

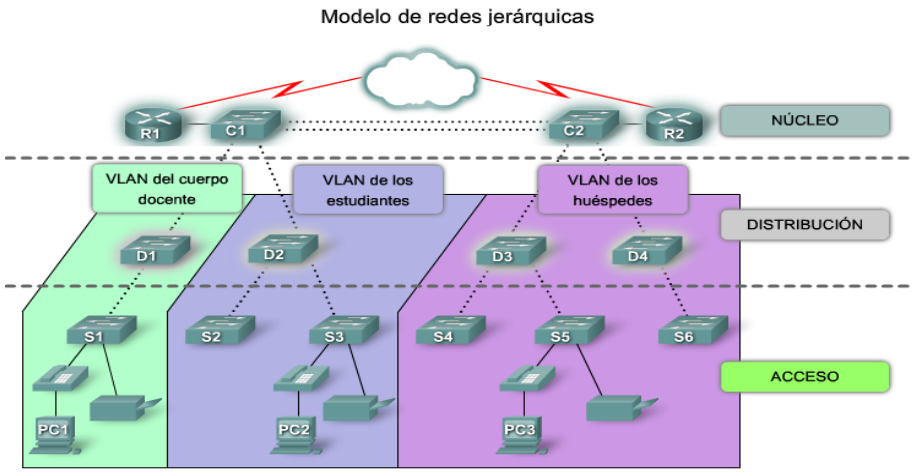


Figura 1. Modelo de redes jerárquicas

Capa de acceso

La capa de acceso hace interfaz con dispositivos finales como las PC, impresoras y teléfonos IP, para proveer acceso al resto de la red. Esta capa de acceso puede incluir routers, switches, puentes, hubs y puntos de acceso inalámbricos. El propósito principal de la capa de acceso es aportar un medio de conexión de los dispositivos a la red y controlar qué dispositivos pueden comunicarse en la red.

Capa de distribución

La capa de distribución agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final. La capa de distribución controla el flujo de tráfico de la red con el uso de políticas y traza los dominios de broadcast al realizar el enrutamiento de las funciones entre las LAN virtuales (VLAN) definidas en la capa de acceso. Las VLAN permiten al usuario segmentar el tráfico sobre un switch en subredes separadas. Por ejemplo, en una universidad el usuario podría separar el tráfico según se trate de profesores, estudiantes y huéspedes. Normalmente, los switches de la capa de distribución son dispositivos que presentan disponibilidad y redundancia altas para asegurar la fiabilidad. Aprenderá más acerca de las VLAN, los dominios de broadcast y el enrutamiento entre las VLAN, posteriormente en este curso.

Capa núcleo

La capa núcleo del diseño jerárquico es la backbone de alta velocidad de la internetwork. La capa núcleo es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante. El área del núcleo también puede conectarse a los recursos de Internet. El núcleo agrega el tráfico de todos los dispositivos de la capa de distribución, por lo tanto debe poder reenviar grandes cantidades de datos rápidamente.

Nota: En redes más pequeñas, no es inusual que se implemente un modelo de núcleo colapsado, en el que se combinan la capa de distribución y la capa núcleo en una capa.

Red jerárquica en una empresa mediana

Examinemos un modelo de red jerárquica aplicada a una empresa. En la figura, las capas de acceso, de distribución y núcleo se encuentran separadas en jerarquías bien definidas. Esta representación lógica contribuye a que resulte fácil ver qué switches desempeñan qué función. Es mucho más difícil ver estas capas

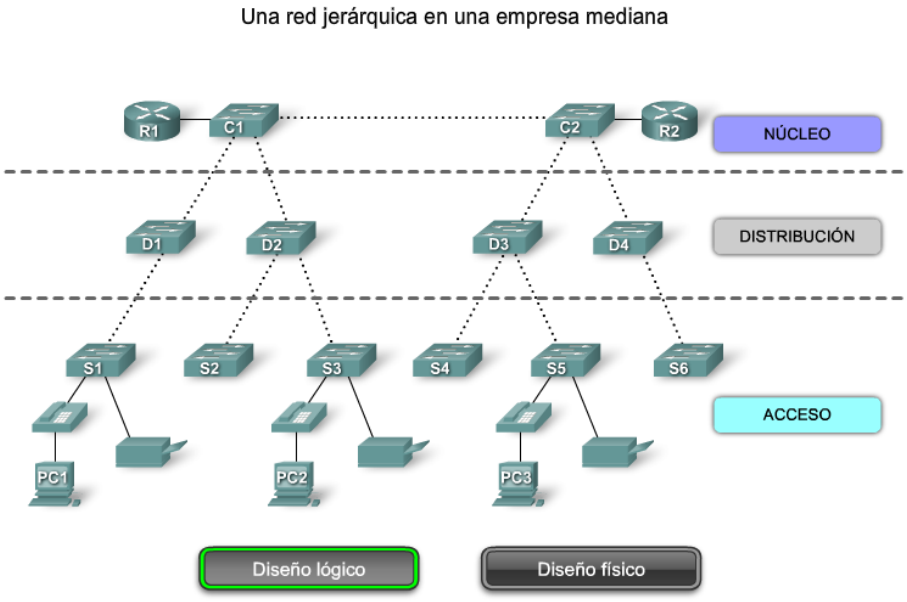


Figura 2. Redes jerárquicas en la empresa

La figura muestra dos pisos de un edificio. Las computadoras del usuario y los dispositivos de la red que necesitan acceso a la red se encuentran en un piso. Los recursos, como servidores de correo electrónico y servidores de bases de datos, se ubican en otro piso. Para asegurar que cada piso tenga acceso a la red, se instalan la capa de acceso y los switches de distribución en los armarios de cableado de cada piso y se conectan a todos los dispositivos que necesitan acceso a la red. La figura muestra un pequeño bastidor de switches. El switch de la capa de acceso y el switch de la capa de distribución se encuentran apilados uno sobre el otro en el armario de cableado.

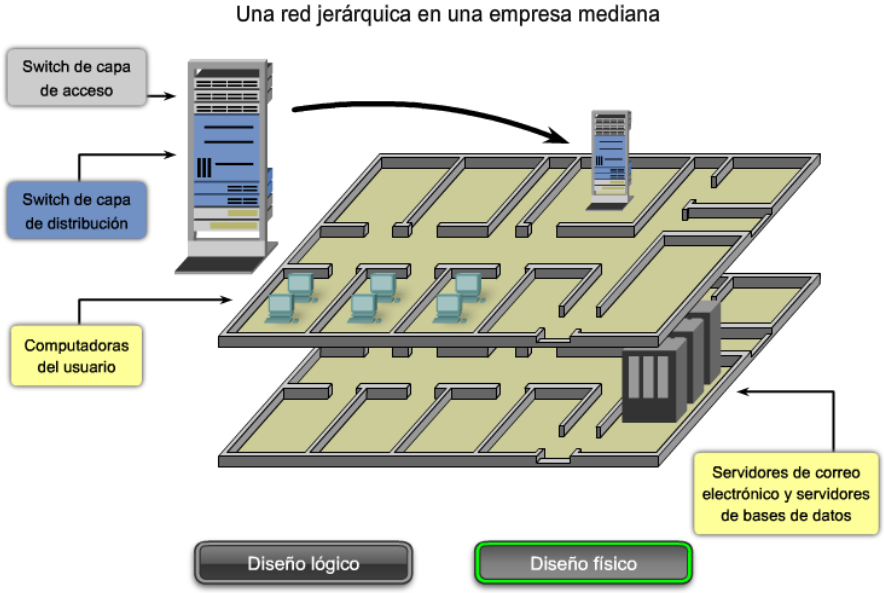


Figura 3. Red jerárquica en una empresa pequeña

Aunque no se muestran los switches de la capa núcleo y otros switches de la capa de distribución, es posible observar cómo la distribución física de una red difiere de la distribución lógica de una red.

Beneficios de una red jerárquica. Existen muchos beneficios asociados con los diseños de la red jerárquica.

Escalabilidad

Las redes jerárquicas escalan muy bien. La modularidad del diseño le permite reproducir exactamente los elementos del diseño a medida que la red crece. Debido a que cada instancia del módulo es consistente, resulta fácil planificar e implementar la expansión. Por ejemplo, si el modelo del diseño consiste en dos switches de la capa de distribución por cada 10 switches de la capa de acceso, puede continuar agregando switches de la capa de acceso hasta tener 10 switches de la capa de acceso interconectados con los dos switches de la capa de distribución antes de que necesite agregar switches adicionales de la capa de distribución a la topología de la red. Además, a medida que se agregan más switches de la capa de distribución para adaptar la carga de los switches de la capa de acceso, se pueden agregar switches adicionales de la capa núcleo para manejar la carga adicional en el núcleo.

Redundancia

A medida que crece una red, la disponibilidad se torna más importante. Puede aumentar radicalmente la disponibilidad a través de implementaciones redundantes fáciles con redes jerárquicas. Los switches de la capa de acceso se conectan con dos switches diferentes de la capa de distribución para asegurar la redundancia de la ruta. Si falla uno de los switches de la capa de distribución, el switch de la capa de acceso puede conmutar al otro switch de la capa de distribución. Adicionalmente, los switches de la capa de distribución se conectan con dos o más switches de la capa núcleo para asegurar la disponibilidad de la ruta si falla un switch del núcleo. La única capa en donde se limita la redundancia es la capa de acceso. Habitualmente, los dispositivos de nodo final, como PC, impresoras y teléfonos IP, no tienen la capacidad de conectarse con switches múltiples de la capa de acceso para redundancia. Si falla un switch de la capa de acceso, sólo se verían afectados por la interrupción los dispositivos conectados a ese switch en particular. El.

Rendimiento

El rendimiento de la comunicación mejora al evitar la transmisión de datos a través de switches intermediarios de bajo rendimiento. Los datos se envían a través de enlaces del puerto del switch agregado desde la capa de acceso a la capa de distribución casi a la velocidad de cable en la mayoría de los casos. Luego, la capa de distribución utiliza sus capacidades de conmutar el alto rendimiento para reenviar el tráfico hasta el núcleo, donde se enruta hacia su destino final. Debido a que las capas núcleo y de distribución realizan sus operaciones a velocidades muy altas, no existe contención para el ancho de banda de la red. Como resultado, las redes jerárquicas con un diseño apropiado pueden lograr casi la velocidad de cable entre todos los dispositivos.

Seguridad

La seguridad mejora y es más fácil de administrar. Es posible configurar los switches de la capa de acceso con varias opciones de seguridad del puerto que proveen control sobre qué dispositivos se permite conectar a la red. Además, se cuenta con la flexibilidad de utilizar políticas de seguridad más avanzadas en la capa de distribución. Puede aplicar las políticas de control de acceso que definen qué protocolos de comunicación se implementan en su red y dónde se les permite dirigirse. Por ejemplo, si desea limitar el uso de HTTP a una comunidad de usuarios específica conectada a la capa de acceso, podría aplicar una política que bloquee el tráfico de HTTP en la capa de distribución. La restricción del tráfico en base a protocolos de capas más elevadas, como IP y HTTP, requiere que sus switches puedan procesar las políticas en esa capa. Algunos switches de la capa de acceso admiten la funcionalidad de la Capa 3, pero en general es responsabilidad de los switches de la capa de distribución procesar los datos de la Capa 3, porque pueden procesarlos con mucha más eficacia.

Facilidad de administración

La facilidad de administración es relativamente simple en una red jerárquica. Cada capa del diseño jerárquico cumple funciones específicas que son consistentes en toda esa capa. Por consiguiente, si necesita cambiar la funcionalidad de un switch de la capa de acceso, podría repetir ese cambio en todos los switches de la capa de acceso en la red porque presumiblemente cumplen las mismas funciones en su capa. La implementación de switches nuevos también se simplifica porque se pueden copiar las configuraciones del switch entre los dispositivos con muy pocas modificaciones. La consistencia entre los switches en cada capa permite una recuperación rápida y la simplificación de la resolución de problemas. En algunas situaciones especiales, podrían observarse inconsistencias de configuración entre los dispositivos, por eso debe asegurarse de que las configuraciones se encuentren bien documentadas, de manera que pueda compararlas antes de la implementación.

Capacidad de mantenimiento

Debido a que las redes jerárquicas son modulares en naturaleza y escalan con mucha facilidad, son fáciles de mantener. Con otros diseños de la topología de la red, la administración se torna altamente complicada a medida que la red crece. También, en algunos modelos de diseños de red, existe un límite en cuanto a la extensión del crecimiento de la red antes de que se torne demasiado complicada y costosa de mantener. En el modelo del diseño jerárquico se definen las funciones de los switches en cada capa haciendo que la selección del switch correcto resulte más fácil. La adición de switches a una capa no necesariamente significa que se evitará un cuello de botella u otra limitación en otra capa. Para que una topología de red de malla completa alcance el rendimiento máximo, es necesario que todos los switches sean de alto rendimiento porque es fundamental que cada switch pueda cumplir todas las funciones en la red. En el modelo

jerárquico, las funciones de los switches son diferentes en cada capa. Se puede ahorrar dinero con el uso de switches de la capa de acceso menos costosos en la capa inferior y gastar más en los switches de la capa de distribución y la capa núcleo para lograr un rendimiento alto en la red.

Principios de diseño de redes jerárquicas

Sólo porque aparentemente una red presenta un diseño jerárquico, no significa que la red esté bien diseñada. Estas guías simples le ayudan a diferenciar entre redes jerárquicas con un buen diseño y las que presentan un diseño deficiente. La intención de esta sección no es proporcionarle todas las destrezas y el conocimiento que necesita para diseñar una red jerárquica sino ofrecerle una oportunidad de comenzar a practicar sus destrezas a través de la transformación de una topología de red plana en una topología de red jerárquica.

Diámetro de la red

Al diseñar una topología de red jerárquica, lo primero que debe considerarse es el diámetro de la red. Con frecuencia, el diámetro es una medida de distancia pero en este caso se utiliza el término para medir el número de dispositivos. El diámetro de la red es el número de dispositivos que un paquete debe cruzar antes de alcanzar su destino. Mantener bajo el diámetro de la red asegura una latencia baja y predecible entre los dispositivos.

El diámetro de la red es el número de switches en la ruta del tráfico entre dos puntos finales.

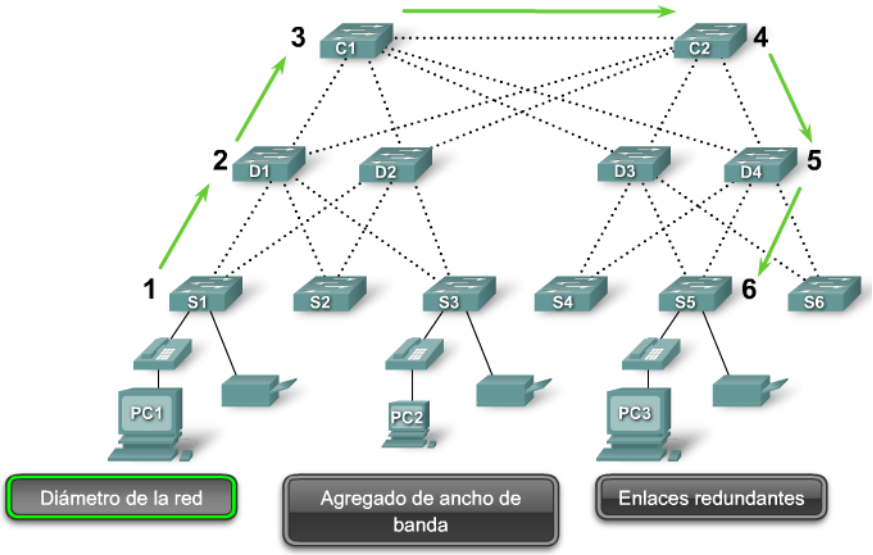


Figura 4. Diámetro de una red

En la figura, la PC1 se comunica con la PC3. Es posible que existan hasta seis switches interconectados entre la PC1 y la PC3. En este caso, el diámetro de la red es 6. Cada switch en la ruta introduce cierto grado de latencia. La latencia del dispositivo de red es el tiempo que transcurre mientras un dispositivo procesa un paquete o una trama. Cada switch debe determinar la dirección MAC de destino de la trama, verificar la tabla de la dirección MAC y enviar la trama al puerto apropiado. Aunque el proceso completo se produce en una fracción de segundo, el tiempo se acrecienta cuando la trama debe cruzar varios switches.

En el modelo jerárquico de tres capas, la segmentación de la Capa 2 en la capa de distribución prácticamente elimina el diámetro de la red como consecuencia. En una red jerárquica, el diámetro de la red siempre va a ser un número predecible de saltos entre el dispositivo origen y el dispositivo destino.

Agregado de ancho de banda

Cada capa en el modelo de redes jerárquicas es una candidata posible para el agregado de ancho de banda. El agregado de ancho de banda es la práctica de considerar los requisitos de ancho de banda específicos de cada parte de la jerarquía. Después de que se conocen los requisitos de ancho de banda de la red, se pueden agregar enlaces entre switches específicos, lo que recibe el nombre de agregado de enlaces. El agregado de enlaces permite que se combinen los enlaces de puerto de los switches múltiples a fin de lograr un rendimiento superior entre los switches. Cisco cuenta con una tecnología de agregado de enlaces específica llamada EtherChannel, que permite la consolidación de múltiples enlaces de Ethernet. Un análisis de EtherChannel excede el alcance de este curso. Para obtener más información, visite: http://www.cisco.com/en/US/tech/tk389/tk213/tsd_technology_support_protocol_home.html.

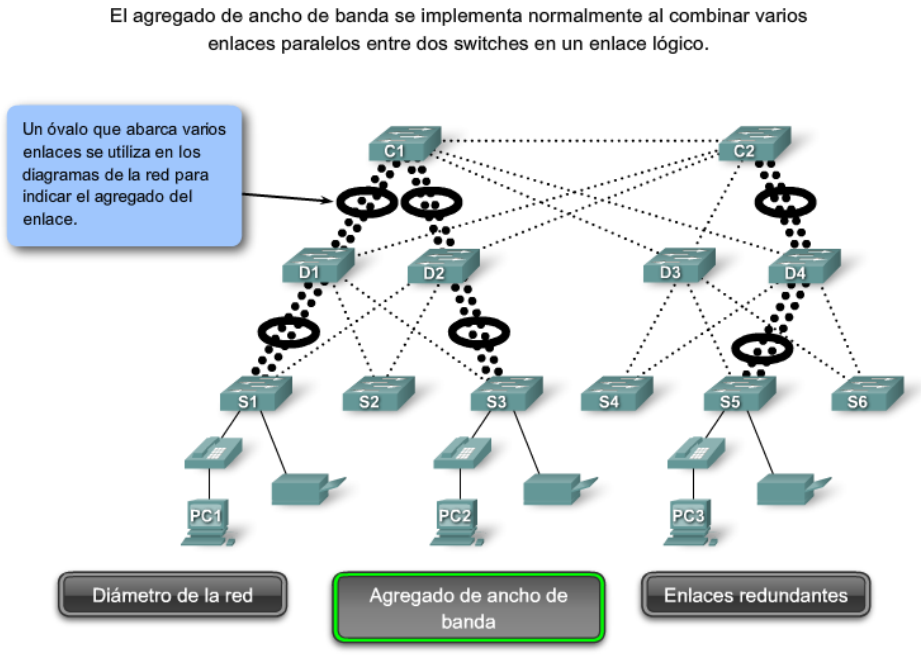


Figura 5. Diámetro de una red

Agregado de ancho de banda

En la figura, las computadoras PC1 y PC3 requieren una cantidad significativa de ancho de banda porque se utilizan para desarrollar simulaciones de condiciones climáticas. El administrador de la red ha determinado que los switches S1, S3 y S5 de la capa de acceso requieren un aumento del ancho de banda. Estos switches de la capa de acceso respetan la jerarquía y se conectan con los switches de distribución D1, D2 y D4. Los switches de distribución se conectan con los switches C1 y C2 de la capa núcleo. Observe cómo los enlaces específicos en puertos específicos se agregan en cada switch. De esta manera, se suministra un aumento del ancho de banda para una parte específica, seleccionada de la red. Observe que en esta figura se indican los enlaces agregados por medio de dos líneas de puntos con un óvalo que las relaciona. En otras figuras, los enlaces agregados están representados por una línea de puntos única con un óvalo.

Redundancia

La redundancia es una parte de la creación de una red altamente disponible. Se puede proveer redundancia de varias maneras. Por ejemplo, se pueden duplicar las conexiones de red entre los dispositivos o se pueden duplicar los propios dispositivos. Este capítulo explora cómo emplear rutas de redes redundantes entre los switches. Un análisis de la duplicación de los dispositivos de red y del empleo de protocolos especiales de red para asegurar una alta disponibilidad excede el alcance de este curso. Para acceder a un análisis interesante acerca de la alta disponibilidad, visite: http://www.cisco.com/en/US/products/ps6550/products_ios_technology_home.html.

La implementación de los enlaces redundantes puede ser costosa. Imagine que cada switch en cada capa de la jerarquía de la red tiene una conexión con cada switch de la capa siguiente. Es improbable que sea capaz de implementar la redundancia en la capa de acceso

debido al costo y a las características limitadas en los dispositivos finales pero puede crear redundancia en las capas de distribución y núcleo de la red.

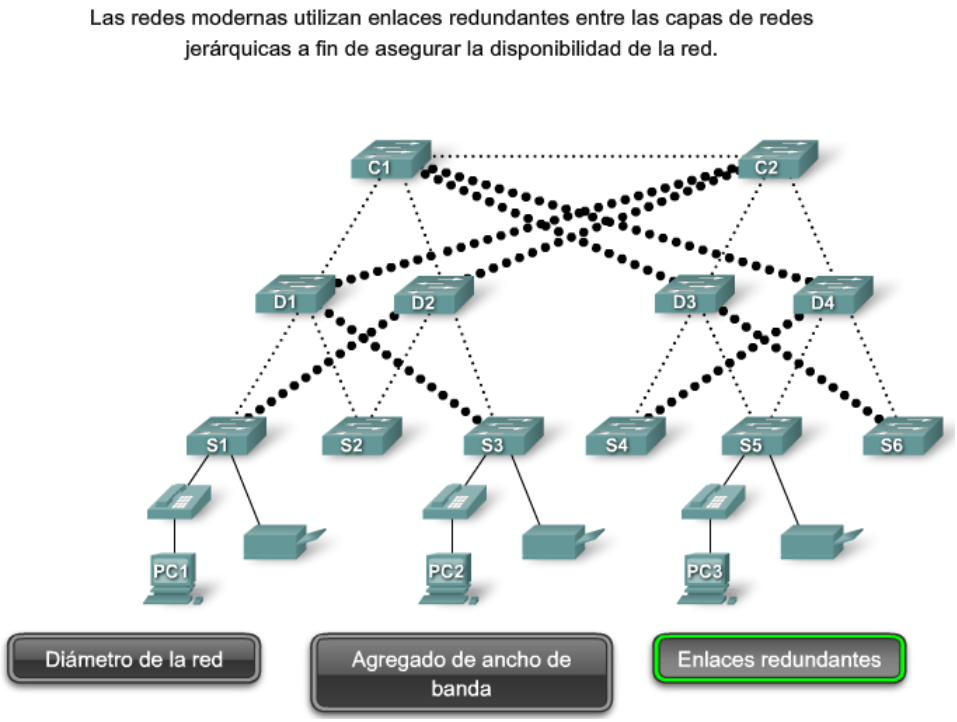


Figura 6. Redes modernas

En la figura 6, los enlaces redundantes se observan en la capa de distribución y en la capa núcleo. En la capa de distribución existen dos switches de capa de distribución, el mínimo requerido para admitir redundancia en esta capa. Los switches de la capa de acceso, S1, S3, S4 y S6, se encuentran interconectados con los switches de la capa de distribución. Esto protege su red si falla uno de los switches de distribución. En caso de falla, el switch de la capa de acceso ajusta su ruta de transmisión y reenvía el tráfico a través del otro switch de distribución.

Ciertas situaciones de falla de la red nunca pueden impedirse, por ejemplo si la energía eléctrica se interrumpe en la ciudad entera o el edifico completo se derrumba debido a un terremoto. La redundancia no intenta abordar estos tipos de desastres. Para obtener más información acerca de cómo una empresa puede continuar

funcionando y recuperarse de un desastre, visite: http://www.cisco.com/en/US/netsol/ns516/networking_solutions_package.html.

Comience en la capa de acceso

Imagine que se requiere un diseño nuevo de redes. Los requisitos de diseño, como el nivel de rendimiento o la redundancia necesaria, están determinados por las metas comerciales de la organización. Una vez que se documentan los requisitos de diseño, el diseñador puede comenzar a seleccionar el equipo y la infraestructura para implementar el diseño.

Cuando se inicia la selección del equipo en la capa de acceso, puede asegurarse de que se adapta a todos los dispositivos de la red que necesitan acceso a la red. Después de tener en cuenta todos los dispositivos finales se tiene una mejor idea de cuántos switches de la capa de acceso se necesitan. El número de switches de la capa de acceso y el tráfico estimado que cada uno genera ayuda a determinar cuántos switches de la capa de distribución se necesitan para lograr el rendimiento y la redundancia necesarios para la red. Después de determinar el número de switches de la capa de distribución, se puede identificar cuántos switches de núcleo se necesitan para mantener el rendimiento de la red.

Un análisis exhaustivo acerca de cómo determinar qué switch seleccionar en base al análisis del flujo de tráfico y cuántos switches de núcleo se requieren para mantener el rendimiento queda fuera del alcance de este curso. Para una buena introducción al diseño de red, lea este libro que se encuentra disponible en Ciscopress.com: Top-Down Network Design, de Priscilla Oppenheimer (2004).

2.3.2 ¿Qué es una red convergente?

Las empresas pequeñas y medianas adoptan la idea de ejecutar servicios de voz y video en sus redes de datos. Observemos cómo la voz y el video sobre IP (VoIP) afectan una red jerárquica.

Figura 7. Convergencia

Equipos heredados

La convergencia es el proceso de combinación de las comunicaciones con voz y video en una red de datos. Las redes convergentes han existido durante algún tiempo pero sólo fueron factibles en grandes organizaciones empresariales debido a los requisitos de infraestructura de la red y a la compleja administración necesaria para hacer que dichas redes funcionen en forma continua. Los costos de red asociados con la convergencia eran altos porque se necesitaba un hardware de switches más costoso para admitir los requisitos adicionales de ancho de banda. Las redes convergentes también necesitaban una administración extensiva en relación con la Calidad de Servicio (QoS), porque era necesario que el tráfico de datos con voz y video se clasificara y priorizara en la red. Pocas personas contaban con la experiencia profesional en cuanto a redes de datos, voz y video para hacer que la convergencia fuese factible y funcional. Además, el equipo antiguo obstaculiza el proceso. La figura

muestra un switch antiguo de una empresa telefónica. En la actualidad, la mayoría de las empresas telefónicas ha cambiado a switches digitales. Sin embargo, existen muchas oficinas que aún utilizan teléfonos análogos por lo que todavía tienen armarios de cableado de teléfonos análogos. Debido a que aún no se han reemplazado los teléfonos análogos, también observará que debe admitir tanto el sistema telefónico PBX antiguo como los teléfonos IP. Con lentitud se reemplazará esta clase de equipamiento por switches modernos de teléfonos IP.

Figura 8. Convergencia 2

Tecnología avanzada

La convergencia de redes de voz, video y datos se ha vuelto muy popular recientemente en el mercado empresarial pequeño y mediano debido a los avances en la tecnología. En el presente resulta más fácil implementar y administrar la convergencia y su adquisición es menos costosa. La figura muestra una combinación de switch y de teléfono VoIP de alta tecnología apropiada para una empresa mediana de entre 250 y 400 empleados. La figura también muestra

un switch Cisco Catalyst Express 500 y un teléfono Cisco 7906G adecuados para empresas pequeñas y medianas. Esta tecnología VoIP solía presentar un precio razonable para empresas y entidades gubernamentales.

La transferencia a una red convergente puede ser una decisión difícil si la empresa ya realizó una inversión en redes de voz, video y datos separadas. El abandono de una inversión que aún funciona resulta arduo pero la convergencia de voz, video y datos en una infraestructura de red única presenta varias ventajas.

Un beneficio de una red convergente es la existencia de sólo una red para administrar. Con las redes de voz, video y datos separadas, los cambios realizados en la red deben coordinarse a través de redes. Además, existen costos adicionales que resultan del uso de tres conjuntos de cableado de redes. El uso de una red única significa que el usuario sólo debe administrar una infraestructura conectada por cables.

Otro beneficio es el menor costo de implementación y administración. Es menos costoso implementar una infraestructura de red única que tres infraestructuras de redes distintas. La administración de una red única es también menos costosa. Tradicionalmente, si una empresa cuenta con una red separada de voz y datos, necesita a un grupo de personas que administren la red de voz y otro grupo que administre la red de datos. Con una red convergente, se necesita a un grupo que administra tanto la red de voz como la de datos.

Figura 9. Convergencia 3

Opciones nuevas

Las redes convergentes ofrecen opciones que no existían con anterioridad. Ahora se pueden unir las comunicaciones de voz y video directamente en el sistema de la computadora personal de un empleado, según se observa en la figura. No es necesario contar con un aparato telefónico o un equipo para videoconferencias caros. Se puede lograr la misma función con el uso de un software especial integrado con una computadora personal. Las herramientas de telesoftware, como Cisco IP Communicator, ofrecen mucha flexibilidad a las empresas. La persona que se encuentra en la parte superior izquierda de la figura utiliza una herramienta de telesoftware en la computadora. Cuando se utiliza el software en lugar de un teléfono físico, una empresa puede realizar la conversión a redes convergentes con rapidez porque no hay gastos de capital en la adquisición de teléfonos IP y de los switches necesarios para accionar los teléfonos. Con la incorporación de cámaras Web económicas, se pueden agregar videoconferencias al telesoftware. Éstos son sólo algunos ejemplos proporcionados por una cartera más

amplia de soluciones de comunicación que redefinen el proceso comercial en la actualidad.

Figura 10. Redes separadas de voz, video y datos

Como se puede ver en la figura, una red de voz contiene líneas telefónicas aisladas que ejecutan un switch PBX para permitir la conectividad telefónica a la Red pública de telefonía conmutada (PSTN). Cuando se agrega un teléfono nuevo, se debe ejecutar una línea nueva de regreso al PBX. El switch del PBX se ubica habitualmente en el armario de cableado de Telco, separado de los armarios de cableado de datos y video. Los armarios de cableado con frecuencia se separan porque el personal de apoyo necesita acceso a cada sistema. Sin embargo, mediante el uso de una red jerárquica apropiadamente diseñada y la implementación de políticas de QoS que dan prioridad a los datos de audio, los datos de voz se pueden converger en una red de datos existente con muy poco o ningún impacto en la calidad del audio.

Figura 11. Redes separadas de voz

En esta figura, el equipo para videoconferencias está conectado por cable en forma separada de las redes de voz y de datos. Los datos de videoconferencias pueden consumir un ancho de banda significativo en una red. Como resultado, se mantuvieron las redes de videos por separado para permitir que los equipos de videoconferencias funcionen a toda velocidad sin competir por el ancho de banda con los flujos de voz y de datos. Mediante el uso de una red jerárquica apropiadamente diseñada y la implementación de políticas de QoS que dan prioridad a los datos de video, puede hacerse que dichos datos converjan en una red de datos existente con muy poco o ningún impacto en la calidad del video.

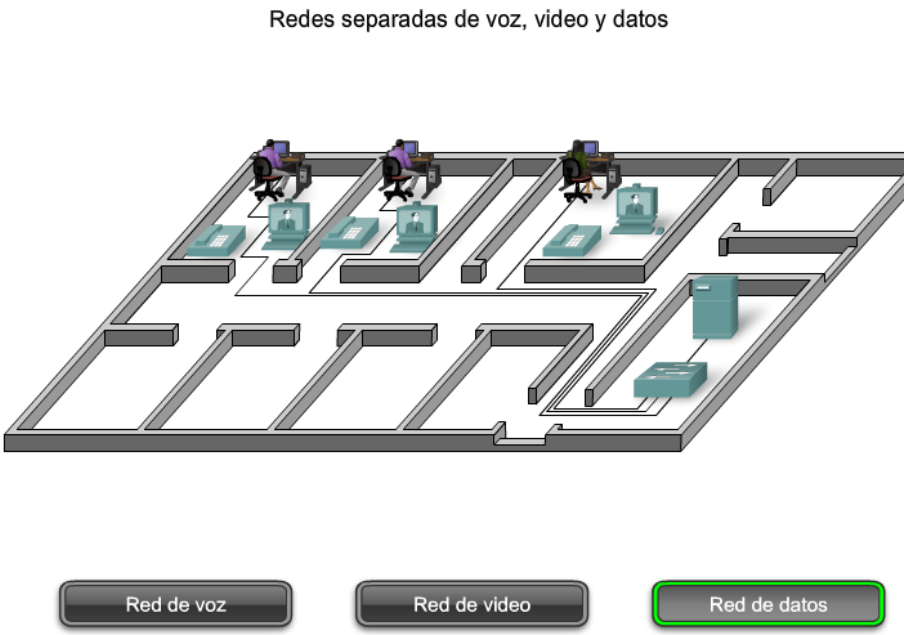


Figura 12. Redes separadas de voz y video

La red de datos interconecta las estaciones de trabajo y los servidores en una red para facilitar el uso compartido de recursos. Las redes de datos pueden consumir un ancho de banda de datos significativo y éste es el motivo por el cual las redes de voz, video y datos se mantuvieron separadas por tan largo tiempo. Ahora que las redes jerárquicas con el diseño apropiado pueden incluir los requerimientos de ancho de banda de las comunicaciones por voz, video y datos al mismo tiempo; tiene sentido hacer que converjan en una única red jerárquica.

2.3.3 Relación entre los switches y las funciones específicas de la LAN.

2.3.3.1 Consideraciones para los switches de redes jerárquicas.

Para seleccionar el switch apropiado para una capa en una red jerárquica, es necesario contar con especificaciones que detallen los flujos de tráfico objetivo, las comunidades de usuario, los servidores de datos y los servidores de almacenamiento de datos.

Las empresas necesitan una red que pueda satisfacer los requerimientos del desarrollo. Una empresa puede comenzar con algunas PC interconectadas de manera que puedan compartir datos. A medida que la empresa contrata más empleados, los dispositivos, como PC, impresoras y servidores, se agregan a la red. La incorporación de los nuevos dispositivos implica un aumento en el tráfico de la red. Algunas compañías reemplazan sus sistemas telefónicos existentes por sistemas telefónicos VoIP convergentes, lo que agrega un tráfico adicional.

Cuando se selecciona el hardware de switch, se determina qué switches se necesitan en las capas núcleo, distribución y acceso para adaptarse a los requerimientos del ancho de banda de red. Su plan debe considerar los requerimientos de ancho de banda en el futuro. Adquiera el hardware del switch Cisco apropiado para incorporar tanto las necesidades actuales como las futuras. Para contribuir con la elección más precisa de los switches apropiados, realice y registre los análisis de flujo de tráfico de forma regular.

Análisis del flujo de tráfico

El análisis del flujo de tráfico es el proceso de medición del uso del ancho de banda en una red y el análisis de datos con el fin de lograr ajustes del rendimiento, planificación de la capacidad y toma de decisiones con respecto a las mejoras del hardware. El análisis del flujo de tráfico se realiza con el uso de software para análisis de flujo de tráfico. Aunque no existe una definición exacta de flujo de tráfico de la red, a efectos del análisis del flujo de tráfico, es posible decir que el tráfico de la red es la cantidad de datos enviados durante un cierto período de tiempo. Todos los datos de la red contribuyen con el tráfico, independientemente de su

propósito u origen. El análisis de los diferentes orígenes del tráfico y su influencia en la red, permite realizar ajustes más exactos y actualizar la red para lograr el mejor rendimiento posible.

Los datos del flujo de tráfico pueden utilizarse para ayudar a determinar exactamente cuánto tiempo puede continuar utilizando el hardware de la red existente antes de que tenga sentido actualizarlo para adaptarse según los requerimientos adicionales de ancho de banda. Al tomar las decisiones con respecto a qué hardware adquirir, se deben tener en cuenta las densidades de puerto y las tasas de reenvío del switch para asegurarse de lograr una capacidad de crecimiento adecuada. La densidad de puerto y las tasas de reenvío se explican más adelante en este capítulo.

Existen muchas formas de controlar el flujo de tráfico en una red. Se pueden controlar manualmente los puertos individuales de switch para obtener la utilización del ancho de banda con el tiempo. Al analizar los datos de flujo de tráfico se deben determinar los requerimientos de flujo de tráfico futuro en base a la capacidad en ciertos momentos del día y a dónde se genera y se envía la mayor cantidad de datos. Sin embargo, para obtener resultados exactos es necesario registrar datos suficientes. El registro manual de los datos del tráfico es un proceso tedioso que requiere mucho tiempo y diligencia. Afortunadamente existen algunas soluciones automatizadas.

Herramientas de análisis

Figura 13. Herramienta de análisis

Se encuentran disponibles muchas herramientas de análisis de flujo de tráfico que registran automáticamente los datos de flujo de tráfico en una base de datos y realizan un análisis de tendencias. En redes mayores, las soluciones del conjunto del software constituyen el único método eficaz para realizar el análisis de flujo de tráfico. La figura exhibe un resultado de muestra obtenido del Solarwinds Orion 8.1 NetFlow Analysis, que controla el flujo de tráfico en una red. Al recopilar datos mediante el software, se puede observar exactamente cómo se desempeña cada interfaz en un punto de tiempo dado en la red. Con el uso de los cuadros incluidos, se pueden identificar los problemas de flujo de tráfico visualmente. Este proceso es mucho más sencillo que tener que interpretar los números en una columna de datos de flujo de tráfico.

Para obtener una lista de algunas herramientas comerciales de recopilación y de análisis de flujo de tráfico, visite http://www.cisco.com/warp/public/732/Tech/nmp/netflow/partners/commercial/index.shtml.

Para obtener una lista de algunas herramientas freeware de recopilación y de análisis de flujo de tráfico, visite http://www.cisco.com/warp/public/732/Tech/nmp/netflow/partners/freeware/index.shtml.

Análisis de las comunidades de usuarios

El análisis de las comunidades de usuarios es el proceso de identificación de varios grupos de usuarios y su influencia en el rendimiento de la red. La forma en que se agrupan los usuarios afecta los aspectos relacionados con la densidad de puerto y con el flujo de tráfico, que a su vez influye en la selección de los switches de la red. La densidad de puerto se explica con posterioridad en este capítulo.

En un edificio típico de oficinas, los usuarios finales se agrupan de acuerdo con la función que cumplen en su trabajo porque necesitan un acceso similar a los recursos y aplicaciones. Es posible que el Departamento de Recursos Humanos (HR) se encuentre en un piso de un edificio de oficinas mientras que el Departamento de Finanzas está en otro. Cada departamento tiene un número diferente de usuarios y de necesidades de aplicación y requiere de acceso a los diferentes recursos de datos disponibles a través de la red. Por ejemplo, cuando se seleccionan switches para los armarios de cableado de los departamentos de Recursos Humanos y de Finanzas, se debería elegir un switch que tuviese los puertos suficientes para satisfacer las necesidades del departamento y que fuese lo suficientemente poderoso para adaptarse a los requerimientos de tráfico para todos los dispositivos en ese piso. Además, un buen plan de diseño de redes considera el crecimiento de cada departamento para asegurar que existen puertos de switch lo suficientemente

abiertos que se pueden utilizar antes de la próxima actualización planificada de la red.

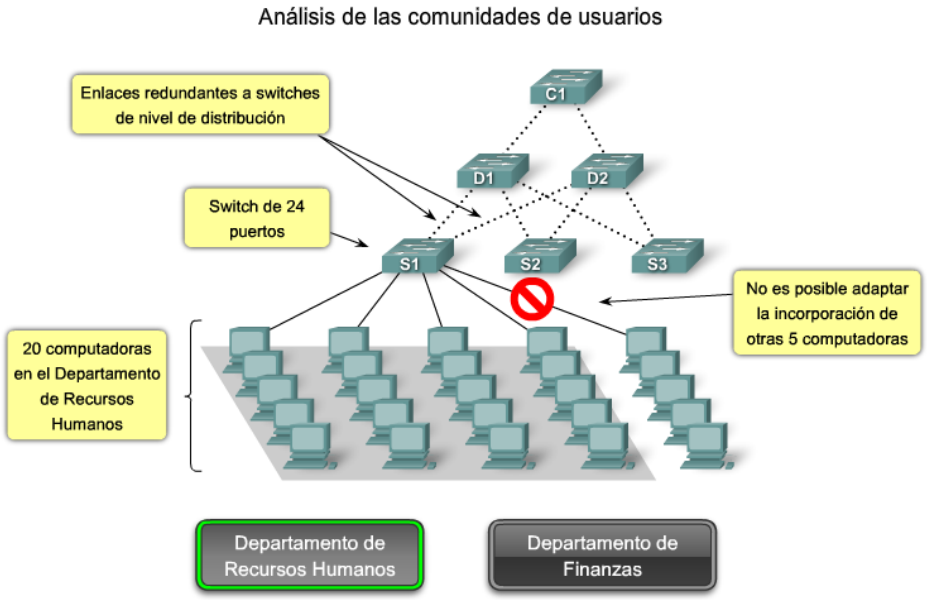


Figura 14. Análisis de las comunicaciones de usuarios

Como se muestra en la figura, el Departamento de Recursos Humanos requiere 20 estaciones de trabajo para sus 20 usuarios. Eso se traduce en 20 puertos de switch necesarios para conectar las estaciones de trabajo a la red. Si se seleccionase un switch apropiado de la capa de acceso para adaptarse al Departamento de Recursos Humanos, probablemente se elegiría un switch de 24 puertos, que cuenta con los puertos suficientes para incluir las 20 estaciones de trabajo y los enlaces a los switches de la capa de distribución.

Crecimiento Futuro

Pero este plan no informa acerca del crecimiento futuro. Considere qué sucederá si se agregan cinco empleados al Departamento de Recursos Humanos. Un plan de redes sólido incluye la tasa de crecimiento de personal en los pasados cinco años para poder anticipar el crecimiento futuro. Con ese concepto en mente, se debe adquirir un switch que

pueda incluir más de 24 puertos, como es el caso de los switches apilables o modulares que pueden escalar.

Además de observar el número de dispositivos en un cierto switch en una red, se debe investigar el tráfico de red generado por las aplicaciones de los usuarios finales. Algunas comunidades de usuarios utilizan aplicaciones que generan mucho tráfico de red mientras que otras comunidades de usuarios no lo hacen. Mediante la medición del tráfico de red generado para todas las aplicaciones en uso por las diferentes comunidades de usuarios y la determinación de la ubicación del origen de los datos, se puede identificar el efecto de sumar más usuarios a esa comunidad.

Una comunidad de usuarios que pertenece a un grupo de trabajo en una empresa pequeña queda admitida por un par de switches y en general se conecta al mismo switch que el servidor. En empresas o compañías medianas, las comunidades de usuarios son admitidas por muchos switches. Los recursos que las comunidades de usuarios de empresas o compañías medianas necesitan podrían ubicarse en áreas geográficamente separadas. En consecuencia, la ubicación de las comunidades de usuarios influye en el lugar donde se localizan los almacenamientos de datos y los servidores centrales.

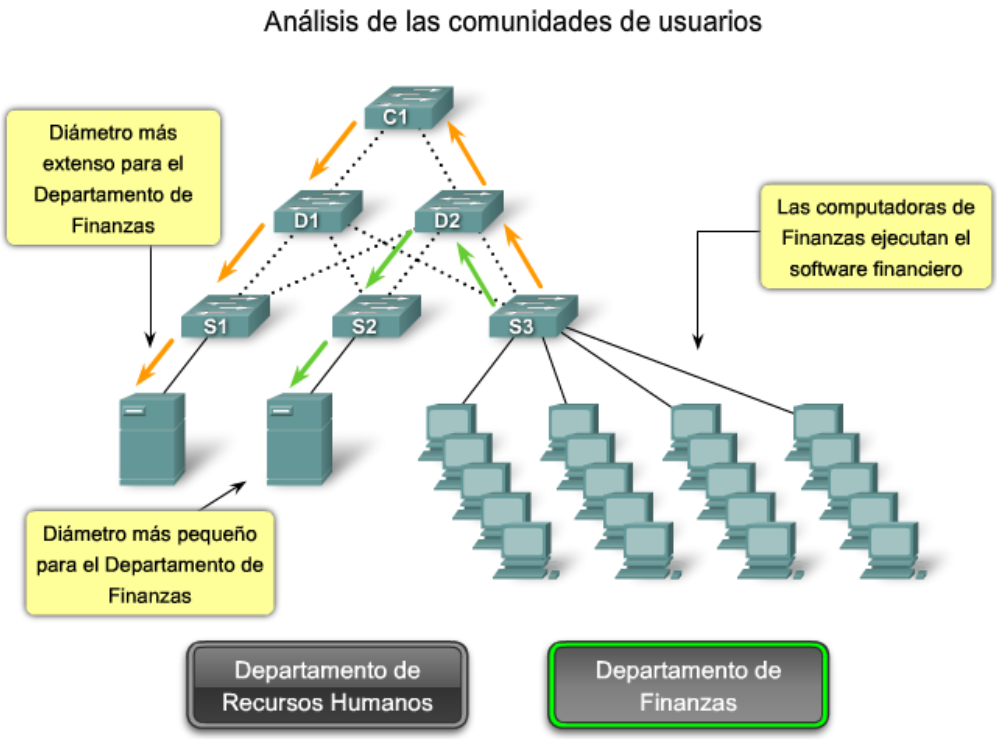


Figura 15. Análisis de las comunicaciones de usuarios

Si los usuarios de Finanzas están utilizando una aplicación intensiva de red y que intercambia datos con un servidor específico en la red, es posible que resulte útil ubicar a la comunidad de usuarios de Finanzas cerca de ese servidor. Al ubicar a los usuarios cerca de sus servidores y de sus medios de almacenamiento de datos, se puede reducir el diámetro de la red para sus comunicaciones y, por consiguiente, reducir el impacto de su tráfico a través del resto de la red.

Una complicación del análisis del uso de la aplicación según las comunidades de usuarios es que el uso no siempre está unido por departamentos o ubicación física. Es posible que se deba analizar el impacto de la aplicación a través de muchos switches de la red para determinar su impacto general.

Análisis de los medios de almacenamiento de datos y de los servidores de datos

Al analizar el tráfico en una red, se debe considerar dónde se ubican los medios de almacenamiento y los servidores de datos de manera que se pueda determinar el impacto del tráfico en la red. Los medios de almacenamiento de datos pueden ser servidores, redes de almacenamiento de datos (SAN), almacenamiento adjunto a redes (NAS), unidades de copia de respaldo en cinta o cualquier otro dispositivo o componente en los que se almacenan grandes cantidades de datos.

Al considerar el tráfico para los medios de almacenamiento y los servidores de datos, se debe considerar tanto el tráfico según el modelo cliente-servidor como el tráfico entre servidor y servidor.

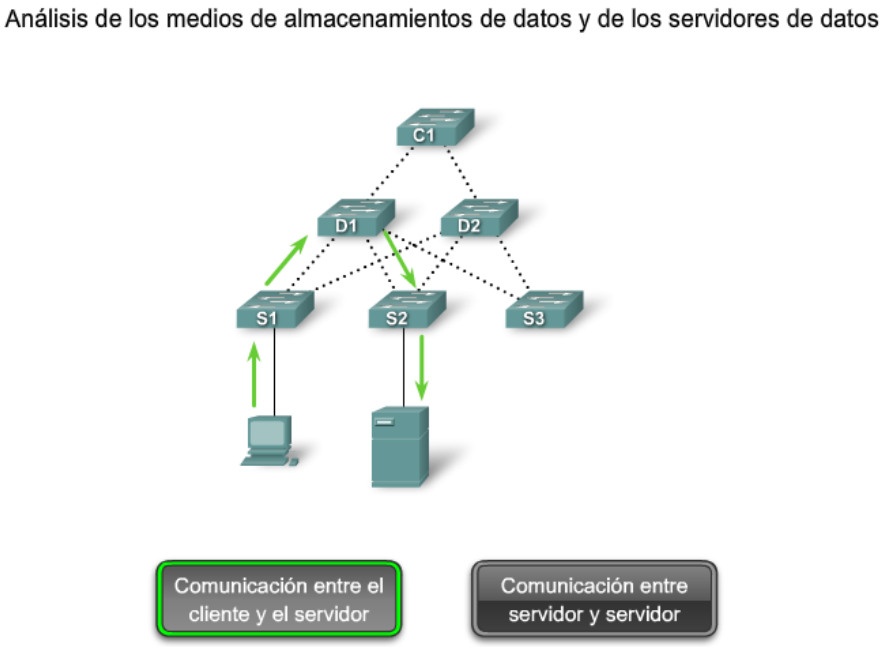


Figura 16. Análisis de los medios de almacenamiento

Según se observa en la figura, el tráfico entre el cliente y el servidor es el tráfico generado cuando el dispositivo de un cliente accede a los datos de los medios de almacenamiento o de los servidores de datos. El tráfico entre el cliente y el servidor habitualmente atraviesa múltiples switches para alcanzar su destino. El agregado de ancho de banda y las

tasas de reenvío del switch son factores importantes que se deben considerar cuando se intenta eliminar cuellos de botella para este tipo de tráfico.

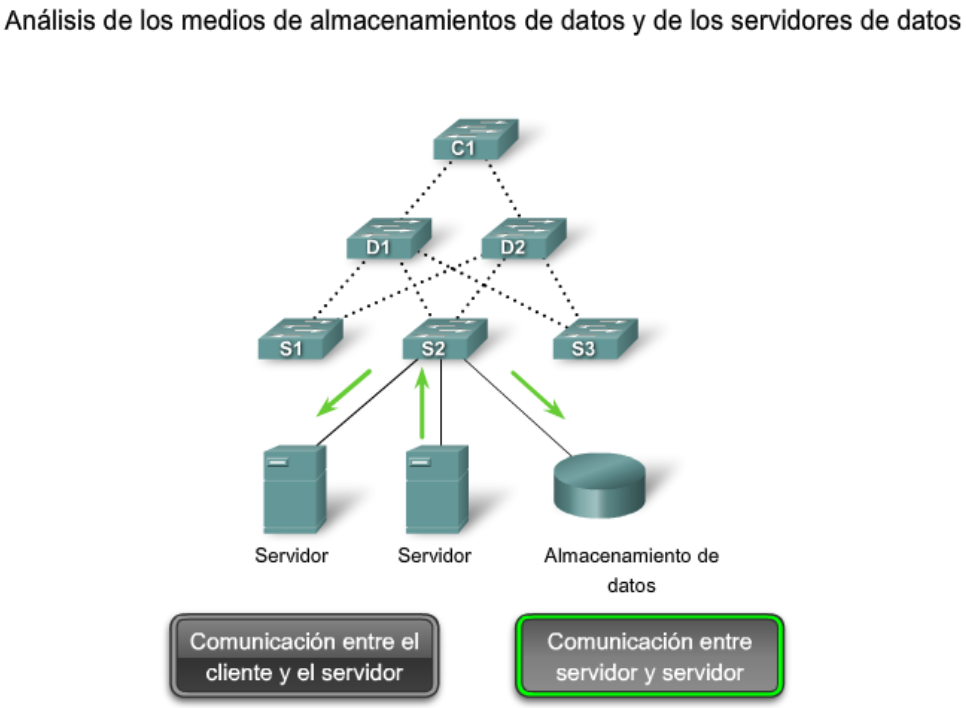


Figura 17. Análisis de los medios de almacenamiento

El tráfico entre servidor y servidor es el tráfico generado entre los dispositivos de almacenamiento de datos en la red. Algunas aplicaciones del servidor generan volúmenes muy altos de tráfico entre los almacenamientos de datos y otros servidores. Para optimizar el tráfico entre servidor y servidor, los servidores que necesitan acceso frecuente a ciertos recursos se deben ubicar a muy corta distancia uno del otro, para que el tráfico que generan no afecte el rendimiento del resto de la red. Los medios de almacenamiento y los servidores de datos habitualmente se ubican en los centros de datos dentro de una empresa. Un centro de datos es un área segura del edificio donde se ubican los servidores, los medios de almacenamiento de datos y otros equipos de la red. Un dispositivo puede ubicarse físicamente en el centro de datos pero puede representarse en una ubicación totalmente diferente en la topología lógica. El tráfico a través de los

switches del centro de datos con frecuencia es muy alto debido al tráfico entre servidor y servidor y entre el servidor y el cliente que atraviesa los switches. Como resultado, los switches seleccionados para los centros de datos deben ser switches de más alto rendimiento que los switches que se hallan en los armarios de cableado en la capa de acceso.

Al examinar las rutas de los datos para varias aplicaciones utilizadas por diferentes comunidades de usuarios, se pueden identificar los cuellos de botella potenciales cuando el rendimiento de la aplicación puede verse afectado por el ancho de banda inadecuado. Para mejorar el rendimiento, se podrían agregar enlaces para adaptarse al ancho de banda o reemplazar los switches más lentos por switches más rápidos que puedan manejar la carga del tráfico.

Diagramas de topología

Un diagrama de topología es una representación gráfica de la infraestructura de una red. Un diagrama de topología muestra cómo se interconectan todos los switches e incluye detalles de qué puerto del switch interconecta los dispositivos. Un diagrama de topología muestra de forma gráfica toda ruta redundante o todos los puertos agregados entre los switches que aportan resiliencia y rendimiento. Demuestra dónde y cuántos switches están en uso en su red, así como también identifica su configuración. Los diagramas de topología también pueden contener información acerca de las densidades de los dispositivos y de las comunidades de usuarios. Al tener un diagrama de topología, se pueden identificar visualmente los potenciales cuellos de botella en un tráfico de red de manera que se pueda centrar la recopilación de datos del análisis de tráfico en áreas en las que las mejoras pueden ejercer el impacto más significativo en el rendimiento.

Es posible que resulte difícil componer una topología de red a

posteriori si no se ha participado en el proceso de diseño. Los cables de la red en los armarios de cableado desaparecen en los pisos y techos y este hecho dificulta el trazado de sus destinos. Y debido a que los dispositivos están dispersos en todo el edificio, resulta difícil saber cómo se conectan todas las piezas. Con paciencia, se puede determinar exactamente cómo se interconecta todo y luego documentar la infraestructura de la red en un diagrama de topología.

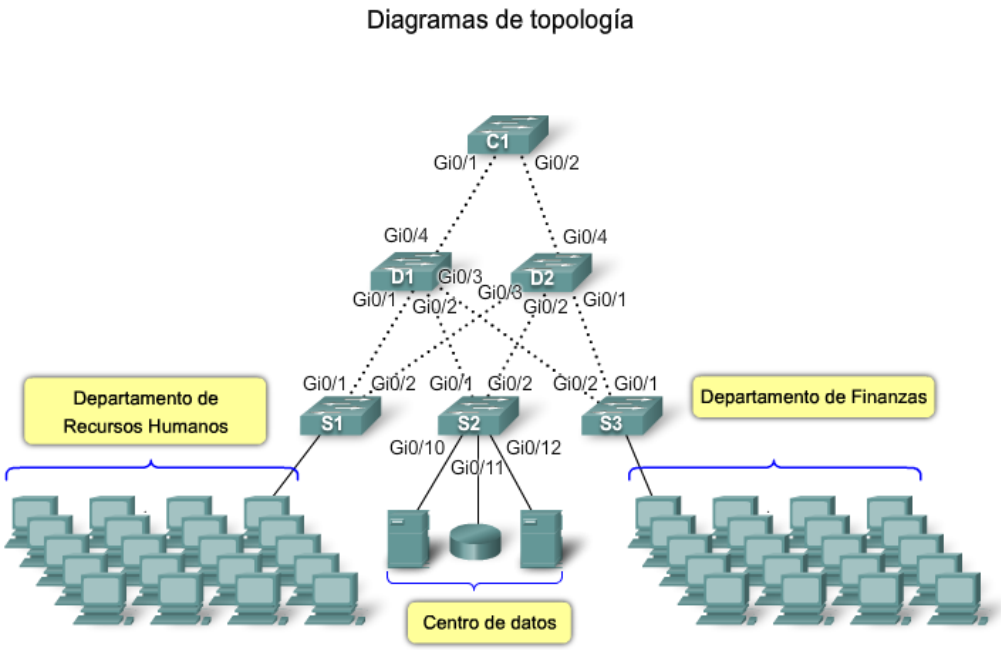


Figura 18. Diagrama de topología

La figura muestra un diagrama simple de topología de red. Nótese cuántos switches se encuentran presentes en la red, así como también la forma en que cada switch se interconecta. El diagrama de topología identifica cada puerto del switch utilizado para las comunicaciones inter switches y rutas redundantes entre switches de capa de acceso y switches de capa de distribución. El diagrama de topología también muestra dónde se ubican las diferentes comunidades de usuarios en la red y la ubicación de los servidores y de los medios de almacenamiento de datos.

2.3.4 Características de los switches.

¿Cuáles son las características clave de los switches que se utilizan en las redes jerárquicas? Al buscar las especificaciones para un switch, ¿Qué significan todos los acrónimos y las frases? ¿Qué significa "PoE" y qué es "tasa de reenvío"? En este tema aprenderá sobre estas características.

Figura 19. Factores de forma de los switches

Al seleccionar un switch se necesita decidir entre una configuración fija o una configuración modular y entre apilable y no apilable. Otra consideración es el grosor del switch expresado en cantidad de bastidores. Por ejemplo, los Switches de configuración fija que se muestran en la figura son todos de 1 bastidor (1U). Con frecuencia estas opciones se denominan factores de forma del switch.

Switches de configuración fija

Los switches de configuración fija son sólo lo que podría esperarse: fijos en su configuración. Esto significa que no se pueden agregar características u opciones al switch más allá de las que originalmente

vienen con el switch. El modelo en particular que se compra determina las características y opciones disponibles. Por ejemplo, si se adquiere un switch fijo gigabit de 24 puertos, no se pueden agregar puertos cuando se les necesite. Habitualmente, existen diferentes opciones de configuración que varían en cuanto al número y al tipo de puertos incluidos.

Switches modulares

Los switches modulares ofrecen más flexibilidad en su configuración. Habitualmente, los switches modulares vienen con chasis de diferentes tamaños que permiten la instalación de diferentes números de tarjetas de línea modulares. Las tarjetas 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 en la PC. Cuanto más grande es el chasis, más módulos puede admitir. Como se observa en la figura, es posible elegir entre muchos tamaños de chasis diferentes. Si se compró un switch modular con una tarjeta de línea de 24 puertos, con facilidad se podría agregar una tarjeta de línea de 24 puertos para hacer que el número de puertos ascienda a 48.

Switches apilables

Los switches apilables pueden interconectarse con el uso de un cable especial del backplane que otorga rendimiento de ancho de banda entre los switches. Cisco introdujo la tecnología StackWise en una de sus líneas de productos con switches. StackWise permite interconectar hasta nueve switches con el uso de conexiones backplane totalmente redundantes. Como se observa en la figura, los switches están apilados uno sobre el otro y los cables conectan los switches en forma de cadena margarita. Los switches apilados operan con efectividad como un único switch más grande. Los

switches apilables son convenientes cuando la tolerancia a fallas y la disponibilidad de ancho de banda son críticas y resulta costoso implementar un switch modular. El uso de conexiones cruzadas hace que la red pueda recuperarse rápidamente si falla un único switch. Los switches apilables utilizan un puerto especial para las interconexiones y no utilizan puertos de línea para las conexiones inter switches. Asimismo, las velocidades son habitualmente más rápidas que cuando se utilizan puertos de línea para la conexión de switches.

Rendimiento

Cuando se selecciona un switch para las capas de acceso, de distribución y núcleo, se debe considerar la capacidad del switch para admitir los requerimientos de densidad de puerto, tasas de reenvío y agregado de ancho de banda de la red.

Densidad de puerto

La densidad de puerto es el número de puertos disponibles en un switch único. Los switches de configuración fija habitualmente admiten hasta 48 puertos en un único dispositivo, con opciones de cuatro puertos adicionales para dispositivos de factor de forma pequeños enchufables (SFP), según muestra la figura. Las altas densidades de puerto permiten un mejor uso del espacio y de la energía cuando la fuente de ambos es limitada. Si tiene dos switches y cada uno contiene 24 puertos, se podrían admitir hasta 46 dispositivos porque se pierde al menos un puerto por switch para conectar cada switch al resto de la red. Además, se requieren dos tomas de alimentación eléctrica. Por otro lado, si tiene un único switch con 48 puertos, se pueden admitir 47 dispositivos con un sólo puerto utilizado para conectar el switch con el resto de la red y sólo una toma de alimentación eléctrica es necesaria para incluir el único switch.

Figura 20. Densidad del puerto

Los switches modulares pueden admitir densidades de puerto muy altas mediante el agregado de tarjetas de línea de puerto de switch múltiples, como muestra la figura. Por ejemplo, el switch Catalyst 6500 puede admitir un exceso de 1000 puertos de switch en un único dispositivo.

Las grandes redes empresariales que admiten muchos miles de dispositivos de red requieren switches modulares de alta densidad para lograr el mejor uso del espacio y de la energía. Sin el uso de un switch modular de alta densidad, la red necesitaría muchos switches de configuración fija para incluir el número de dispositivos que necesitan acceso a la red. Este enfoque puede consumir muchas tomas de alimentación eléctrica y mucho espacio en el armario.

El usuario también debe abordar el tema de los cuellos de botella del enlace. Una serie de switches de configuración fija pueden consumir muchos puertos adicionales para el agregado de ancho de banda entre los switches con el fin de lograr el rendimiento previsto. Con un único switch modular, el agregado del ancho de banda no constituye

un problema porque el backplane del chasis puede proporcionar el ancho de banda necesario para incluir los dispositivos conectados a las tarjetas de línea de puerto del switch.

Velocidades de envío

Figura 21. Velocidad de envío

Las tasas de reenvío definen las capacidades de procesamiento de un switch mediante la estimación de la cantidad de datos que puede procesar por segundo el switch. Las líneas de productos con switch se clasifican según las tasas de reenvío. Los switches de la capa de entrada presentan tasas de reenvío inferiores que los switches de la capa empresarial. Es importante considerar las tasas de reenvío cuando se selecciona un switch. Si la tasa de reenvío del switch es demasiado baja, no puede incluir una comunicación a velocidad de cable completa a través de todos sus puertos de switch. La velocidad de cable es la tasa de datos que cada puerto en el switch puede lograr, 100 Mb/s Fast Ethernet o 1000 Mb/s Gigabit Ethernet. Por ejemplo, un switch gigabit con 48 puertos que opera a una velocidad de cable completa genera 48 Gb/s de tráfico. Si el switch sólo admite

una tasa de reenvío de 32 Gb/s, no puede ejecutar la velocidad de cable completa a través de todos los puertos de forma simultánea. Afortunadamente, es habitual que los switches de la capa de acceso no necesiten operar a velocidad de cable completa porque se encuentran físicamente limitados por sus enlaces en la capa de distribución. Esto permite utilizar switches menos costosos, de rendimiento inferior en la capa de acceso y switches más caros pero con un rendimiento superior en la capa de distribución y en la capa núcleo, en las que la tasa de reenvío es más importante.

Agregado de enlaces

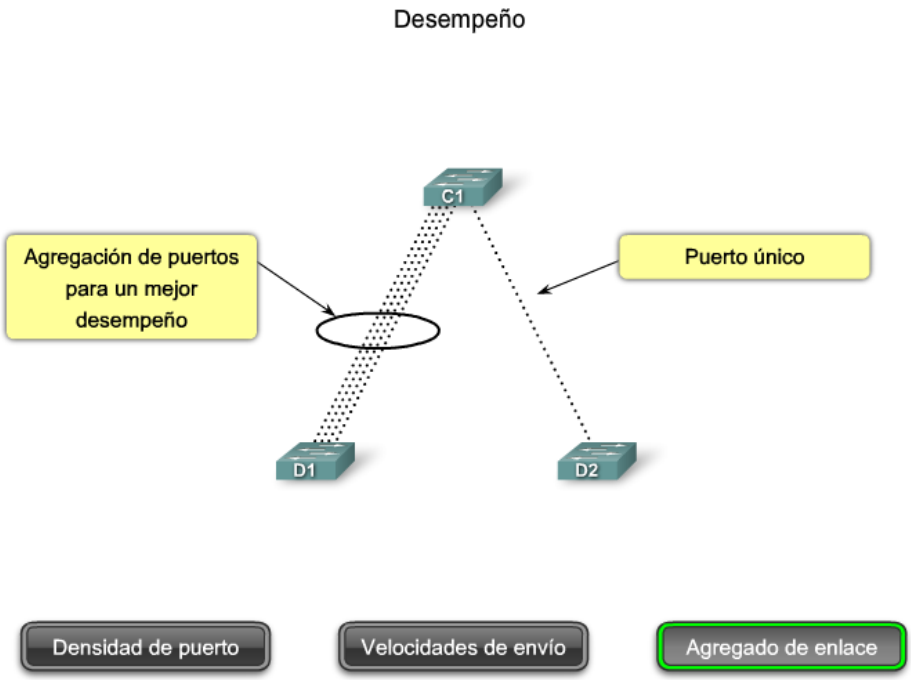


Figura 22. Agregado de enlaces

Como parte del agregado de ancho de banda, se debe determinar si existen puertos suficientes en un switch para agregar y así admitir el ancho de banda requerido. Por ejemplo, considere un puerto Gigabit Ethernet, que transporta hasta 1 Gb/s de tráfico. Si tiene un switch con 24 puertos, con todos los puertos capaces de ejecutar a velocidades de gigabit, podría generar hasta 24 Gb/s de tráfico de red. Si el switch está conectado con el resto de la red a través de un

único cable de red, puede sólo enviar 1 Gb/s de datos al resto de la red. Debido a la contención para el ancho de banda, los datos se enviarían con más lentitud. El resultado es una velocidad de cable de 1/24º disponible para cada uno de los 24 dispositivos conectados al switch. La velocidad de cable describe la tasa máxima y teórica de transmisión de datos de una conexión. Por ejemplo, la velocidad de cable de una conexión Ethernet depende de las propiedades físicas y eléctricas del cable, combinadas con la capa más baja de los protocolos de conexión.

El agregado de enlace ayuda a reducir estos cuellos de botella del tráfico al permitir la unión de hasta ocho puertos de switch para las comunicaciones de datos y al suministrar hasta 8 Gb/s de rendimiento de datos cuando se utilizan los puertos Gigabit Ethernet. Con el agregado de enlaces múltiples de 10 Gigabit Ethernet (10GbE) en algunos switches de la capa empresarial, es posible lograr tasas de rendimiento muy altas. Cisco utiliza el término EtherChannel cuando describe los puertos de switch agregados.

Como se observa en la figura, se utilizan cuatro puertos separados en los switches C1 y D1 para crear un EtherChannel de 4 puertos. La tecnología EtherChannel permite que un grupo de enlaces físicos de Ethernet cree un enlace lógico de Ethernet con el fin de proporcionar tolerancia a fallas y enlaces de alta velocidad entre switches, routers y servidores. En este ejemplo hay un rendimiento equivalente a cuatro veces el de la conexión de único puerto entre los switches C1 y D2.

Funcionalidad de la PoE y de la Capa 3

Otras dos características que se necesita considerar cuando se selecciona un switch son la funcionalidad de Power over Ethernet (PoE) y de la Capa 3.

Power over Ethernet

Power over Ethernet (PoE) permite que el switch suministre energía a un dispositivo por el cableado de Ethernet existente. Como se puede observar en la figura, esta característica puede utilizarse por medio de los teléfonos IP y algunos puntos de acceso inalámbricos. PoE permite mayor flexibilidad al instalar los puntos de acceso inalámbricos y los teléfonos IP porque se los puede instalar en cualquier lugar donde se puede tender un cable de Ethernet. No es necesario considerar cómo suministrar energía eléctrica normal al dispositivo. Sólo se debe elegir un switch que admita PoE si realmente se va a aprovechar esa función, porque suma un costo considerable al switch.

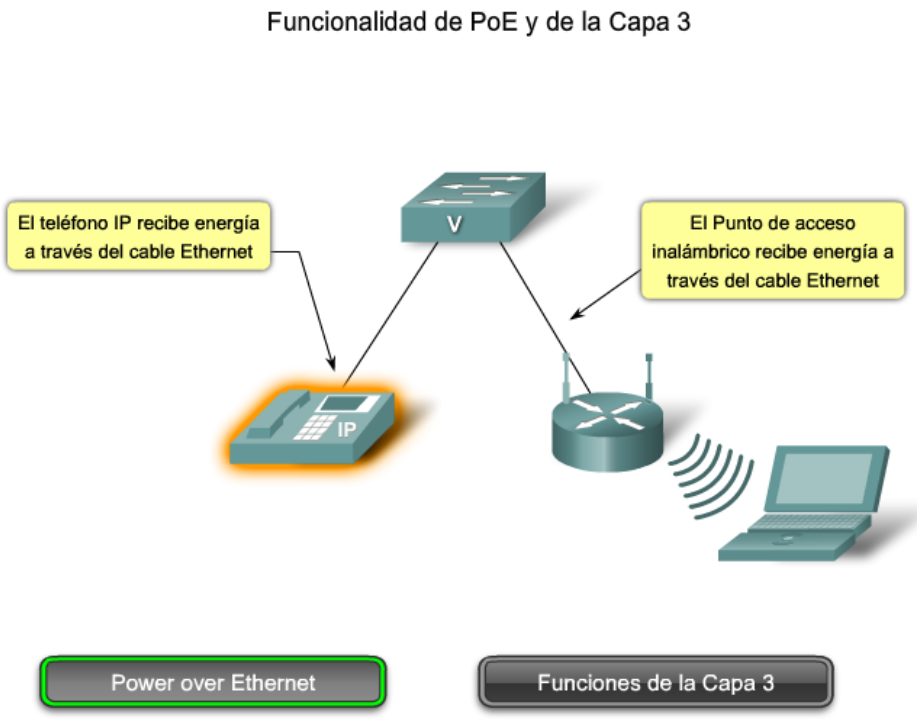


Figura 23. Funciones de la Capa 3

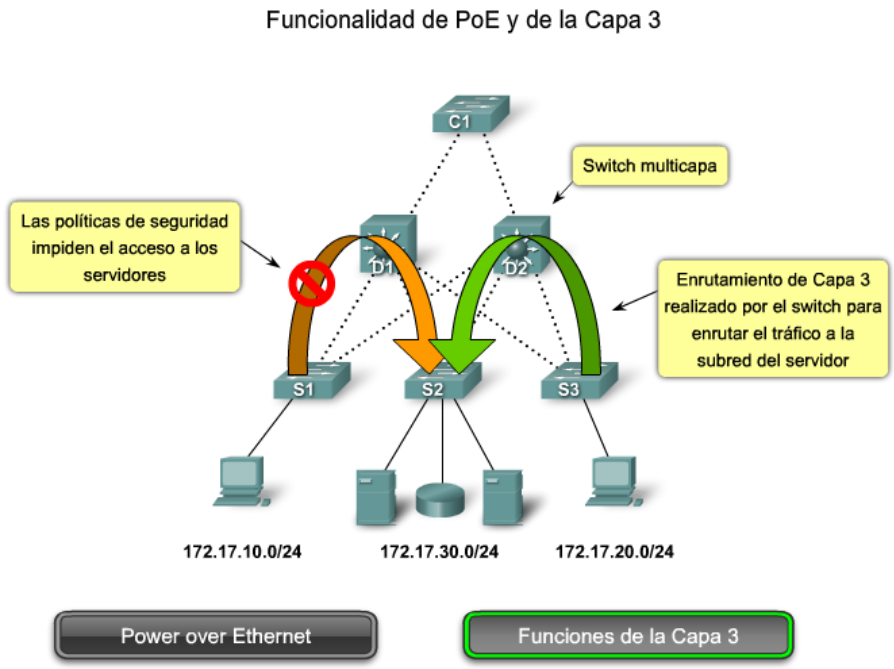


Figura 24. Funcionalidad del PoE

Normalmente, los switches operan en la Capa 2 del modelo de referencia OSI, donde pueden ocuparse principalmente de las direcciones MAC de los dispositivos conectados con los puertos del switch. Los switches de la Capa 3 ofrecen una funcionalidad avanzada que se analiza en más detalle en los capítulos posteriores de este curso. Los switches de la Capa 3 también reciben el nombre de switches multicapas.

2.3.5 Características de los switch en una red jerárquica. Características del switch de la capa de acceso

Ahora que conoce qué factores debe considerar al elegir un switch, examinemos qué características se necesitan en cada capa en una red jerárquica. Luego, podrá relacionar la especificación del switch con su capacidad para funcionar como switch de las capas de acceso, de distribución o núcleo.

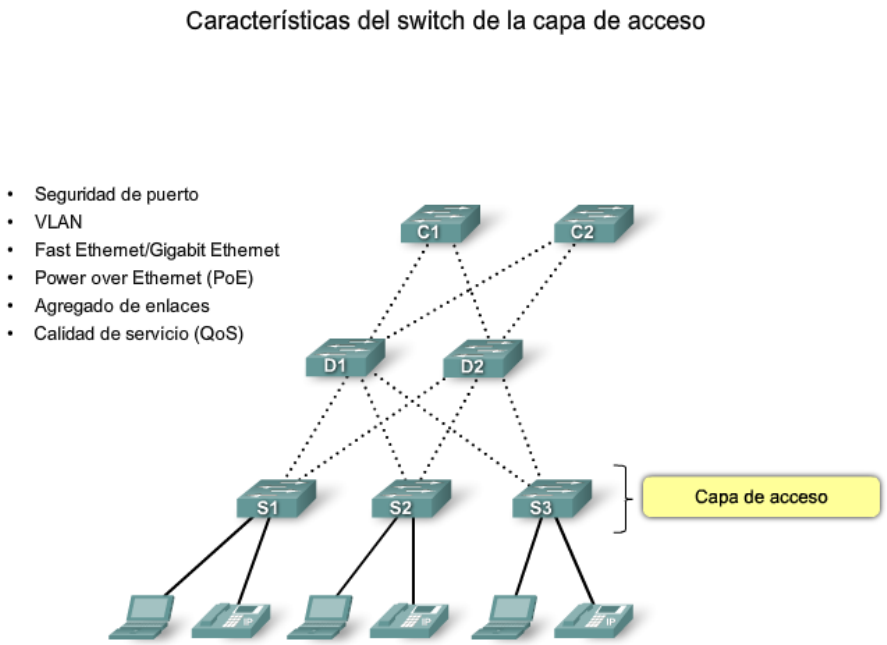


Figura 25. Características del switch

Los switches de la capa de acceso facilitan la conexión de los dispositivos de nodo final a la red. Por esta razón, necesitan admitir características como seguridad de puerto, VLAN, Fast Ethernet/Gigabit Ethernet, PoE y agregado de enlaces.

La seguridad de puerto permite que el switch decida cuántos y qué dispositivos específicos se permiten conectar al switch. Todos los switches Cisco admiten seguridad de capa de puerto. La seguridad de puerto se aplica en el acceso. En consecuencia, es una importante primera línea de defensa para una red. Aprenderá acerca de seguridad de puerto en el capítulo 2.

Las VLAN son un componente importante de una red convergente. El tráfico de voz habitualmente recibe una VLAN separada. De esta manera, el tráfico de voz puede admitirse con más ancho de banda, conexiones más redundantes y seguridad mejorada. Los switches de la capa de acceso permiten establecer las VLAN para los dispositivos de nodo final en su red.

La velocidad de puerto es también una característica que se necesita considerar para los switches de la capa de acceso. Según los requerimientos de rendimiento para su red, debe elegir entre los puertos de switch Fast Ethernet Fast y Gigabit Ethernet. Fast Ethernet permite hasta 100 Mb/s de tráfico por puerto de switch. Fast Ethernet es adecuada para telefonía IP y tráfico de datos en la mayoría de las redes comerciales. Sin embargo, el rendimiento es más lento que el de los puertos Gigabit Ethernet. Gigabit Ethernet permite hasta 1000 Mb/s de tráfico por puerto de switch. La mayoría de los dispositivos modernos, como las estaciones de trabajo, computadoras portátiles y teléfonos IP, admite Gigabit Ethernet. Esto permite transferencias de datos más eficaces y permite a los usuarios ser más productivos. Gigabit Ethernet presenta una desventaja: los switches que admiten Gigabit Ethernet son más costosos.

Otro requerimiento de la característica de algunos switches de capa de acceso es PoE. PoE aumenta drásticamente el precio general del switch en todas las líneas de productos de switches Cisco Catalyst, por lo que sólo debe considerarse cuando se necesita convergencia de voz o se están implementando puntos de acceso inalámbricos y es difícil o costoso ponerlos en funcionamiento en la ubicación deseada.

El agregado de enlaces es otra característica común a la mayoría de los switches de capa de acceso. El 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.

Debido a que la conexión de enlace entre el switch de capa de acceso y el switch de capa de distribución es en general el cuello de botella en la comunicación, la tasa interna de reenvío de los switches de capa de acceso no necesita ser tan alta como el enlace entre los switches de capa de distribución y los de capa de acceso. Las

características como la tasa interna de envío no ofrecen problemas para los switches de capa de acceso porque sólo manejan el tráfico desde los dispositivos finales y lo reenvían a los switches de capa de distribución.

En una red convergente que admite tráfico de red de datos, voz y video, los switches de capa de acceso necesitan admitir QoS para mantener la prioridad del tráfico. Los teléfonos IP Cisco son tipos de equipos que se hallan en la capa de acceso. Cuando se conecta un teléfono IP Cisco a un puerto del switch de capa de acceso configurado para admitir tráfico de voz, ese puerto del switch indica al teléfono IP cómo enviar su tráfico de voz. Es necesario permitir QoS en los switches de capa de acceso para que el tráfico de voz del teléfono IP tenga prioridad, por ejemplo, sobre el tráfico de datos.

Características del switch de la capa de distribución

Los switches de la capa de distribución desempeñan una función muy importante en la red. Recopilan los datos de todos los switches de capa de acceso y los envían a los switches de capa núcleo. Aprenderá más adelante en este curso que el tráfico generado en la Capa 2 en una red conmutada necesita ser administrado o segmentado en las VLAN para no consumir ancho de banda de forma innecesaria a través de la red. Los switches de capa de distribución proporcionan funciones de enrutamiento entre las VLAN, para que una VLAN pueda comunicarse con otra en la red. Habitualmente, este enrutamiento se produce en la capa de distribución porque los switches de capa de distribución presentan capacidades de procesamiento más altas que los switches de capa de acceso. Los switches de capa de distribución reducen la necesidad de que los switches núcleo realicen la tarea, debido a que el núcleo está ocupado con el manejo del reenvío de volúmenes muy altos de tráfico. Debido a que el enrutamiento entre las VLAN se realiza en la capa de distribución, los switches en esta capa necesitan admitir las

funciones de la Capa 3.

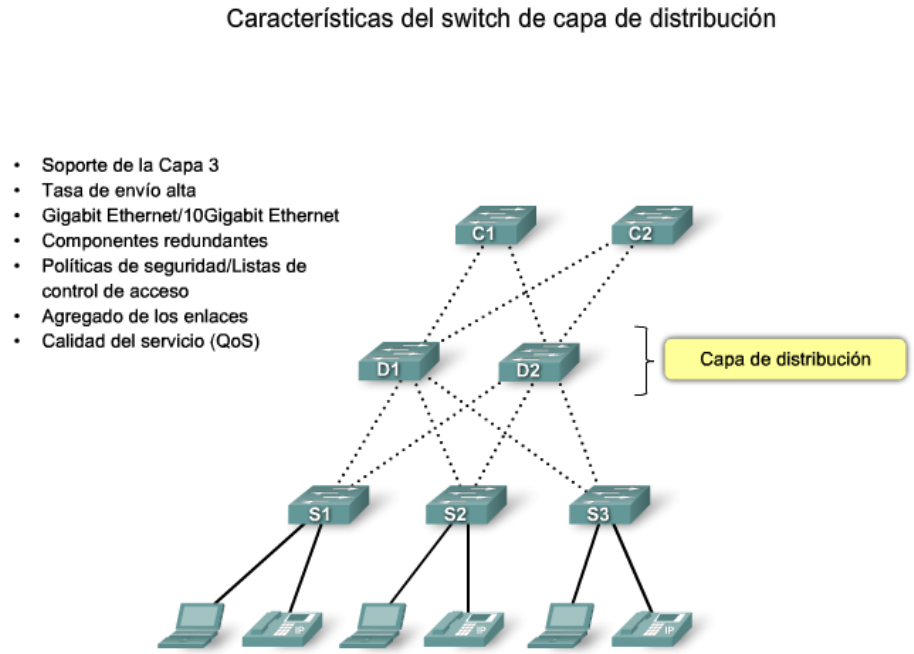


Figura 26. Características del switich de la capa de distribución

Políticas de seguridad

Otro motivo por el que se necesita la funcionalidad de la Capa 3 para los switches de capa de distribución obedece a las políticas de seguridad avanzada que pueden aplicarse al tráfico de red. Se utilizan listas de acceso para controlar cómo fluye el tráfico a través de la red. Una Lista de control de acceso (ACL) permite que el switch impida ciertos tipos de tráfico y autorice otros. Las ACL también permiten controlar qué dispositivos de red pueden comunicarse en la red. El uso de las ACL es un procesamiento intensivo porque el switch necesita inspeccionar cada paquete y observar si coincide con una de las reglas de la ACL definida en el switch. Se realiza la inspección en la capa de distribución porque los switches en esta capa habitualmente tienen capacidad de procesamiento como para manejar la carga adicional y también dicha capa simplifica el uso de las ACL. En vez de utilizar las ACL para cada switch de capa de acceso en la red, las mismas se definen en los switches de capa de distribución, que son menos y hacen que la administración de las ACL sea más fácil.

Calidad de servicio

Los switches de capa de distribución también necesitan admitir QoS para mantener la prioridad del tráfico que proviene de los switches de capa de acceso que implementaron QoS. Las políticas de prioridad aseguran que se garantice el ancho de banda adecuado para las comunicaciones de audio y video a fin de mantener una calidad aceptable del servicio. Para mantener la prioridad de los datos de voz a través de la red, todos los switches que envían datos de voz deben admitir QoS; si la totalidad de los dispositivos de la red no admite QoS, sus beneficios se reducen. Esto produce rendimiento y calidad deficientes en las comunicaciones de video.

Los switches de capa de distribución tienen alta demanda en la red debido a las funciones que desempeñan. Es importante que los switches de distribución admitan redundancia para una disponibilidad adecuada. La pérdida de un switch de capa de distribución podría afectar en gran medida al resto de la red porque todo el tráfico de capa de acceso pasa a través de los switches de capa de distribución. Normalmente, los switches de capa de distribución se implementan en pares para asegurar la disponibilidad. Además, se recomienda que los switches de capa de distribución admitan fuentes de energía múltiples, intercambiables en caliente. La disposición de más de una fuente de energía permite que el switch continúe operando incluso si una de las fuentes de energía falló durante el funcionamiento. Si posee fuentes de energía intercambiables en caliente, puede cambiar una fuente de energía que falla mientras el switch se está ejecutando. Esto permite reparar el componente con fallas sin afectar la funcionalidad de la red.

Finalmente, los switches de capa de distribución necesitan admitir el agregado de enlaces. Habitualmente, los switches de capa de acceso utilizan enlaces múltiples para conectarse a un switch de capa de distribución para asegurar el adecuado ancho de banda y así adaptar el tráfico generado en la capa de acceso y aportar tolerancia ante

fallas en caso de que se pierda un enlace. Debido a que los switches de capa de distribución aceptan el tráfico entrante de múltiples switches de capa de acceso, necesitan enviar todo ese tráfico tan rápido como sea posible a los switches de capa núcleo. Como resultado, los switches de capa de distribución también necesitan enlaces agregados de un alto ancho de banda de regreso a los switches de capa núcleo. Los switches más nuevos de capa de distribución admiten enlaces agregados de 10 Gigabit Ethernet (10GbE) en los switches de capa núcleo.

Características del switch de capa núcleo

La capa núcleo de una topología jerárquica es una backbone de alta velocidad de la red y requiere switches que pueden manejar tasas muy altas de reenvío. La tasa de reenvío requerida depende en gran medida del número de dispositivos que participan en la red. Determine su tasa de reenvío necesaria mediante la realización y el examen de varios informes de flujo de tráfico y análisis de las comunidades de usuarios. En base a sus resultados, puede identificar un switch apropiado para admitir la red. Tome la precaución de evaluar sus necesidades para el presente y el futuro cercano. Si opta por un switch inadecuado para ejecutar el núcleo de la red, enfrentará los problemas potenciale con cuellos de botella en el núcleo y contribuirá a que todas las comunicaciones en la red se vuelvan más lentas.

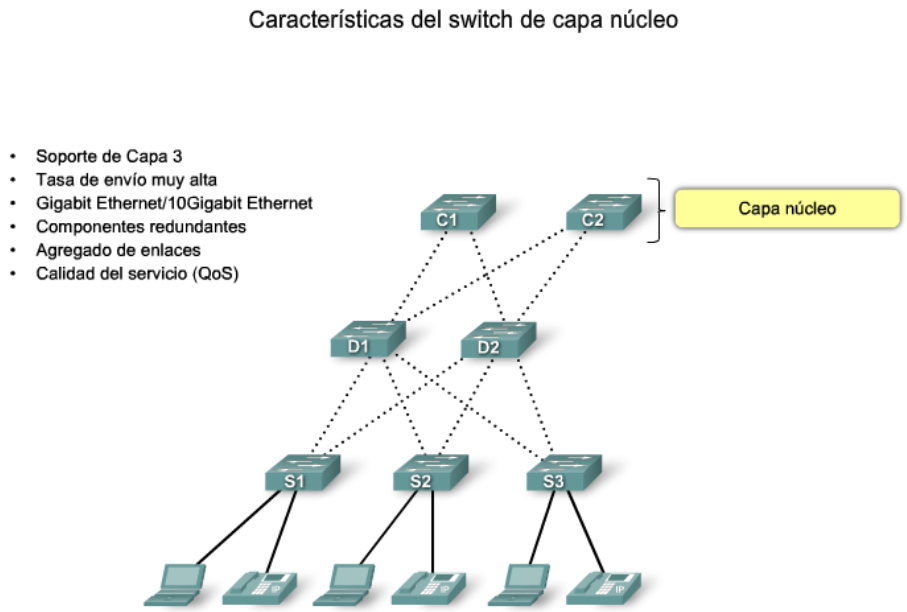


Figura 27. Características del swicht

Agregado de enlaces

La capa núcleo también necesita admitir el agregado de enlaces para asegurar el ancho de banda adecuado que ingresa al núcleo proveniente de los switches de capa de distribución. Los switches de capa de distribución deben tener soporte para conexiones agregadas de 10GbE, que en la actualidad es la opción de conectividad Ethernet disponible de mayor velocidad. Esto permite que los correspondientes switches de capa de distribución distribuyan el tráfico con la mayor eficiencia posible al núcleo.

Redundancia

La disponibilidad de la capa núcleo es también esencial para crear tanta redundancia como se pueda. Normalmente, la redundancia de la Capa 3 presenta una convergencia más veloz que la redundancia de la Capa 2 en caso de falla del hardware. La convergencia en este contexto hace referencia al tiempo que le consume a la red la adaptación a un cambio y no debe confundirse con una red convergente que admite comunicaciones de datos, audio y video. Con ese concepto en mente, necesita asegurarse de que sus switches de capa núcleo admiten las funciones de la Capa 3. Un análisis completo

sobre las implicaciones de la redundancia de la Capa 3 excede el alcance de este curso. La necesidad de redundancia de la Capa 2 en este contexto continúa siendo una cuestión pendiente. La redundancia de la Capa 2 se examina en el capítulo 5, donde se trata el protocolo spanning tree (STP). Además, busque los switches de capa núcleo que admiten las características de redundancia del hardware adicional como fuentes de energía redundante que pueden intercambiarse mientras el switch continúa funcionando. Debido a la alta carga de trabajo que transportan los switches de capa núcleo, tienden a funcionar con más temperatura que los switches de capa de acceso o de distribución, y entonces deben contar con opciones de refrigeración más sofisticadas. Muchos switches verdaderos con capacidad de capa núcleo presentan la habilidad de intercambiar ventiladores de refrigeración sin necesidad de apagar el switch.

Por ejemplo, sería perjudicial apagar un switch de capa núcleo para cambiar una fuente de energía o un ventilador en la mitad del día cuando el uso de la red está en su máximo punto. Para realizar un reemplazo de hardware se podría considerar una interrupción de la red de al menos 5 minutos si se es muy veloz para realizar el mantenimiento. En una situación más realista, el switch podría estar desconectado durante 30 minutos o más y es probable que esta situación no sea aceptable. Con hardware intercambiable en caliente no se realizan interrupciones durante el mantenimiento de los switches.

QoS es una parte importante de los servicios prestados por los switches de capa núcleo. Por ejemplo, los prestadores de servicios (que suministran IP, almacenamiento de datos, correo electrónico y otros servicios) y las Redes de área extensa (WAN) de las empresas, están adicionando mayor tráfico de voz y video a una cantidad de tráfico de datos en crecimiento. En el núcleo y el extremo de la red, el tráfico fundamental y sensible a los tiempos como la voz debe recibir

garantías superiores de QoS que el tráfico de menor sensibilidad a los tiempos como las transferencias de archivos o el correo electrónico. Debido a que el acceso a la WAN de alta velocidad es con frecuencia extremadamente costoso, la suma de ancho de banda en la capa núcleo no es una opción. Ya que QoS proporciona una solución basada en software para priorizar el tráfico, los switches de capa núcleo pueden suministrar una manera rentable de admitir uso óptimo y diferenciado del ancho de banda existente.

2.3.6 Presentación de las VLAN.

El rendimiento de la red puede ser un factor en la productividad de una organización y su reputación para realizar sus transmisiones en la forma prevista. Una de las tecnologías que contribuyen al excelente rendimiento de la red es la división de los grandes dominios de broadcast en dominios más pequeños con las VLAN. Los dominios de broadcast más pequeños limitan el número de dispositivos que participan en los broadcasts y permiten que los dispositivos se separen en agrupaciones funcionales, como servicios de base de datos para un departamento contable y transferencia de datos a alta velocidad para un departamento de ingeniería. En este capítulo, aprenderá a configurar, manejar y solucionar problemas de las VLAN y los enlaces troncales.

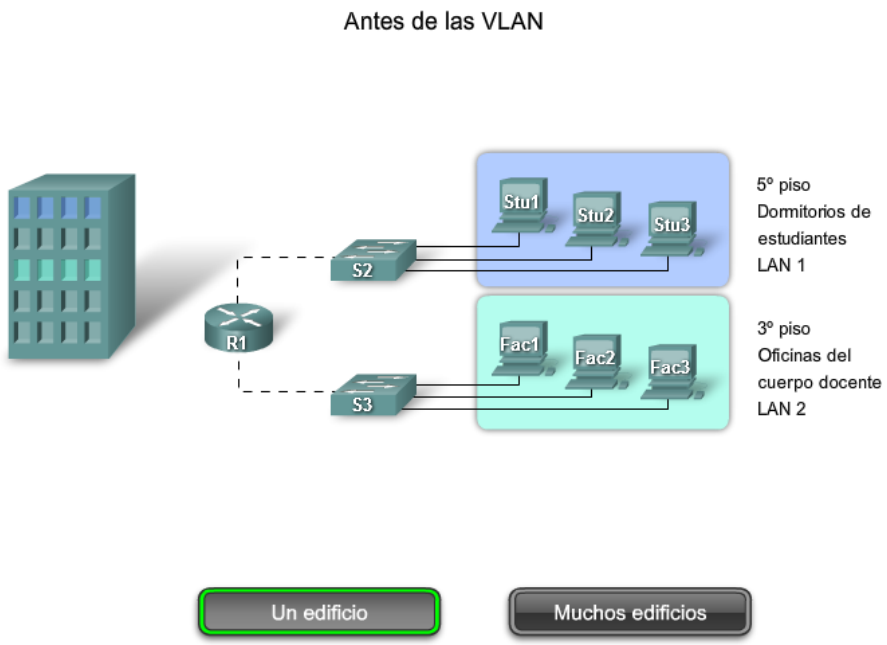


Figura 28. Antes de la VLAN

Antes de las VLAN

Para poder apreciar por qué las VLAN se utilizan tanto hoy en día, considere una pequeña comunidad con dormitorios de estudiantes y oficinas del cuerpo docente, todo en un solo edificio. La figura muestra las computadoras de los estudiantes en una LAN y las computadoras del cuerpo docente en otra LAN. Esto funciona bien debido a que todos los departamentos están juntos físicamente, por lo tanto, es fácil proporcionarles los recursos de la red.

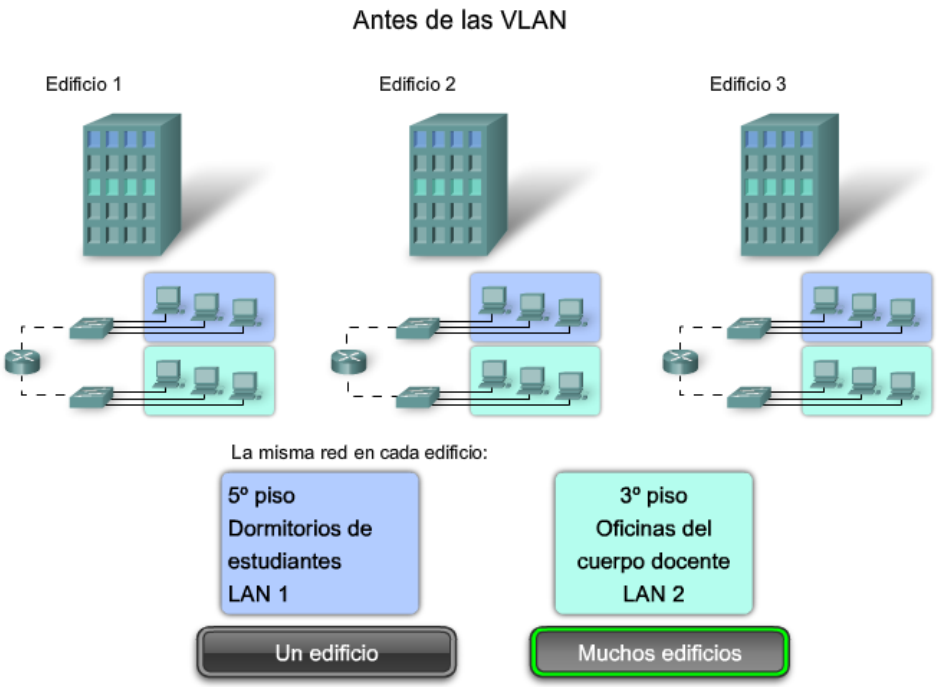


Figura 29. Antes de la VLAN

Un año después, la universidad creció y, ahora, tiene tres edificios. En la figura, la red original es la misma pero las computadoras de los estudiantes y del cuerpo docente están distribuidas en los tres edificios. Los dormitorios de los estudiantes permanecen en el quinto piso y las oficinas del cuerpo docente en el tercer piso. Sin embargo, el departamento de TI ahora quiere asegurarse de que todas las computadoras de los estudiantes compartan las mismas características de seguridad y controles de ancho de banda. ¿Cómo puede la red acomodar las necesidades compartidas de los departamentos separados geográficamente? ¿Crea una LAN grande y conecta por cable a todos los departamentos juntos? ¿Cuán fácil sería realizar cambios a esa red? Sería muy bueno agrupar a las personas con los recursos que utilizan sin tener en cuenta su ubicación geográfica, y sería más fácil administrar la seguridad específica y las necesidades de ancho de banda.

Antes de las VLAN

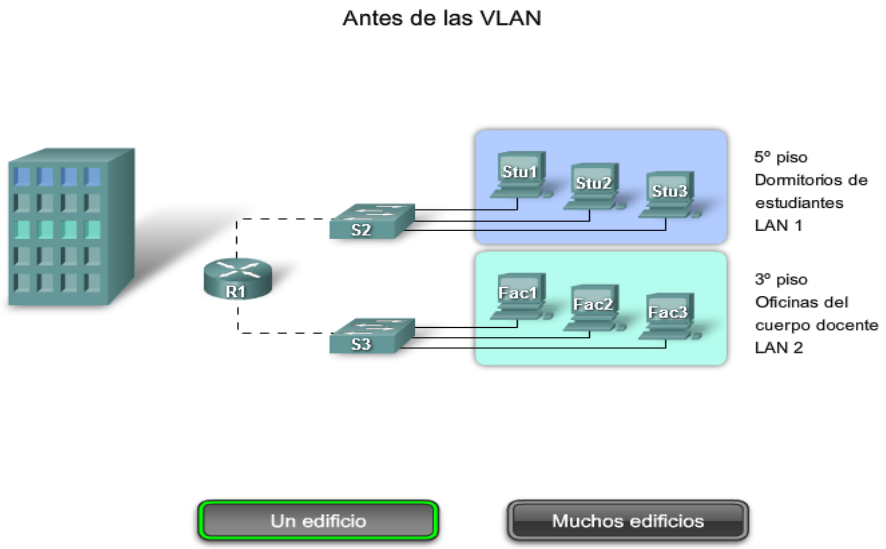


Figura 30. Antes de la VLAN

Para poder apreciar por qué las VLAN se utilizan tanto hoy en día, considere una pequeña comunidad con dormitorios de estudiantes y oficinas del cuerpo docente, todo en un solo edificio. La figura muestra las computadoras de los estudiantes en una LAN y las computadoras del cuerpo docente en otra LAN. Esto funciona bien debido a que todos los departamentos están juntos físicamente, por lo tanto, es fácil proporcionarles los recursos de la red.

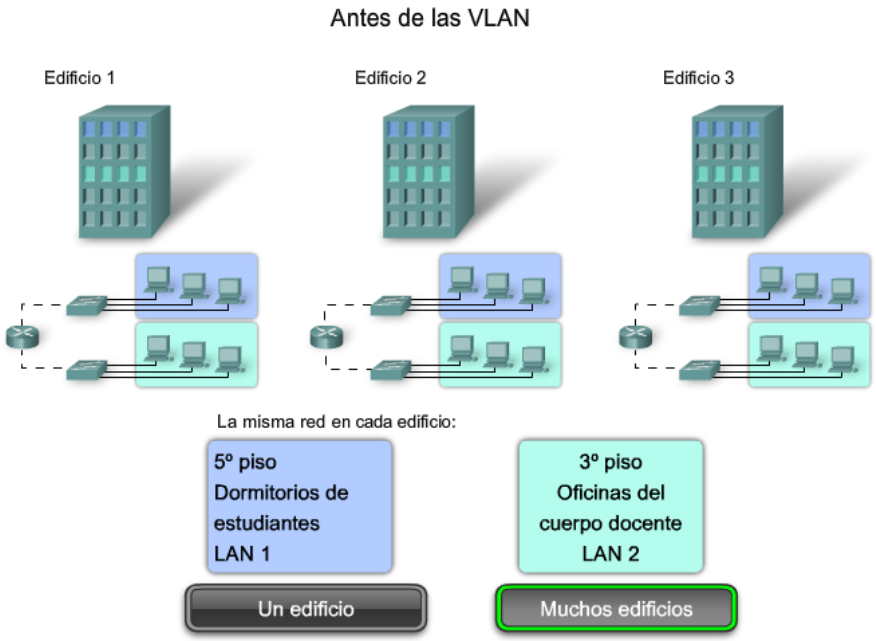


Figura 31. Antes de la VLAN

Un año después, la universidad creció y, ahora, tiene tres edificios. En la figura, la red original es la misma pero las computadoras de los estudiantes y del cuerpo docente están distribuidas en los tres edificios. Los dormitorios de los estudiantes permanecen en el quinto piso y las oficinas del cuerpo docente en el tercer piso. Sin embargo, el departamento de TI ahora quiere asegurarse de que todas las computadoras de los estudiantes compartan las mismas características de seguridad y controles de ancho de banda. ¿Cómo puede la red acomodar las necesidades compartidas de los departamentos separados geográficamente? ¿Crea una LAN grande y conecta por cable a todos los departamentos juntos? ¿Cuán fácil sería realizar cambios a esa red? Sería muy bueno agrupar a las personas con los recursos que utilizan sin tener en cuenta su ubicación geográfica, y sería más fácil administrar la seguridad específica y las necesidades de ancho de banda.

Visión general de VLAN

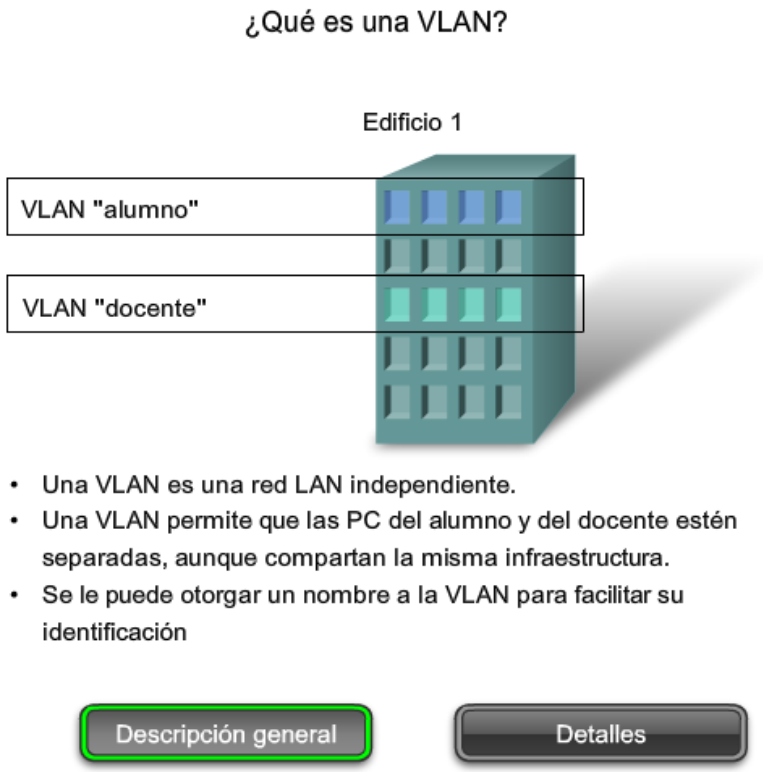


Figura 32. Visión general de VLAN

La solución para la comunidad de la universidad es utilizar una tecnología de red denominada LAN (VLAN) virtual. Una VLAN permite que un administrador de red cree grupos de dispositivos conectados a la red de manera lógica que actúan como si estuvieran en su propia red independiente, incluso si comparten una infraestructura común con otras VLAN. Cuando configura una VLAN, puede ponerle un nombre para describir la función principal de los usuarios de esa VLAN. Como otro ejemplo, todas las computadoras de los estudiantes se pueden configurar en la VLAN "Estudiante". Mediante las VLAN, puede segmentar de manera lógica las redes conmutadas basadas en equipos de proyectos, funciones o departamentos. También puede utilizar una VLAN para estructurar geográficamente su red para respaldar la confianza en aumento de las empresas sobre trabajadores domésticos. En la figura, se crea una VLAN para los estudiantes y otra para el cuerpo docente. Estas VLAN permiten que el administrador de la red implemente las políticas de acceso y

seguridad para grupos particulares de usuarios. Por ejemplo: se puede permitir que el cuerpo docente, pero no los estudiantes, obtenga acceso a los servidores de administración de e-learning para desarrollar materiales de cursos en línea.

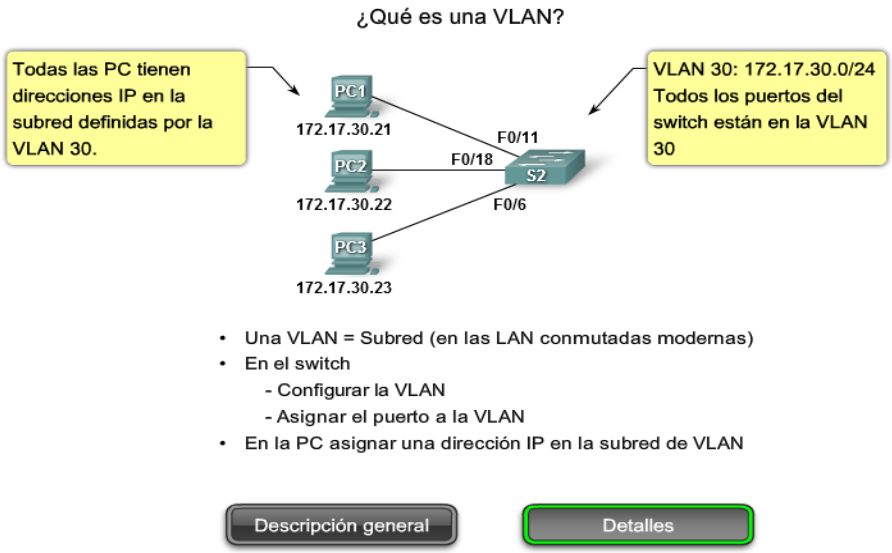


Figura 33. VLAN

Detalles de la 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. La figura muestra una red con tres computadoras. 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.

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.

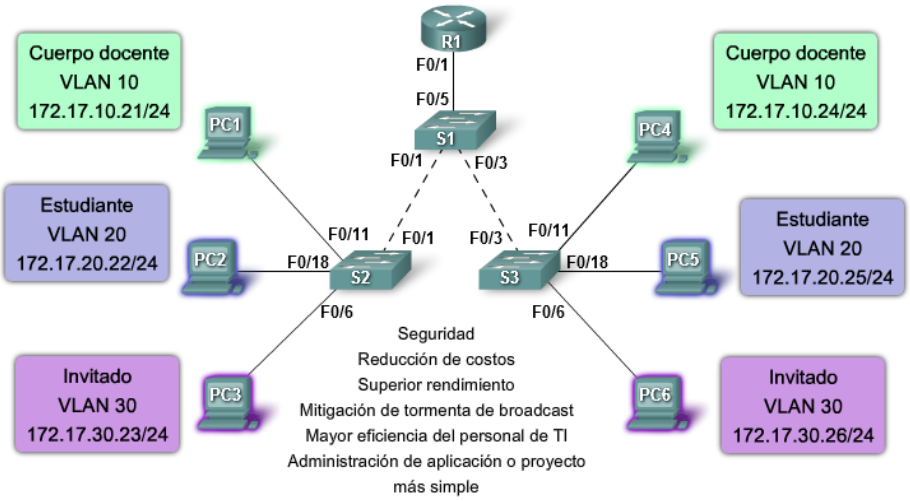


Figura 34. Ventajas de la VLAN

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. Las computadoras del cuerpo docente se encuentran en la VLAN 10 y están completamente separadas del tráfico de datos del Invitado y de los estudiantes.

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. Como se analizó en el capítulo "Configure un switch", la segmentación de LAN impide que una tormenta de broadcast se propague a toda la red. En la figura puede observar que, a pesar de que hay seis computadoras en esta red, hay sólo tres dominios de broadcast: Cuerpo docente, Estudiante y Invitado .

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. En la figura, para una identificación más fácil se nombró "Estudiante" a la VLAN 20, la VLAN 10 se podría nombrar "Cuerpo docente" y la VLAN 30 "Invitado ".

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.

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 y 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.

2.3.7 Tipos de VLAN.

Hoy en día, existe fundamentalmente una manera de implementar las VLAN: VLAN basada en puerto. Una VLAN basada en puerto se asocia con un puerto denominado acceso VLAN.

Sin embargo, en las redes existe una cantidad de términos para las VLAN. Algunos términos definen el tipo de tráfico de red que envían y otros definen una función específica que desempeña una VLAN. A continuación, se describe la terminología común de VLAN:

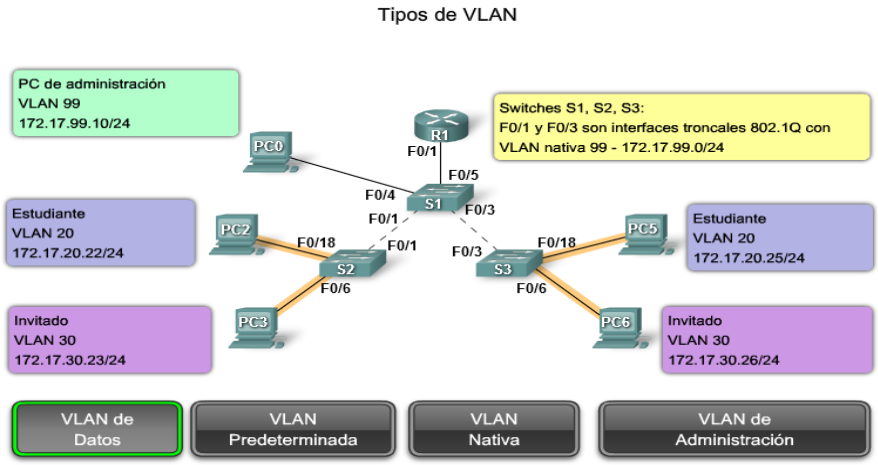


Figura 35. Tipos de VLAN

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.

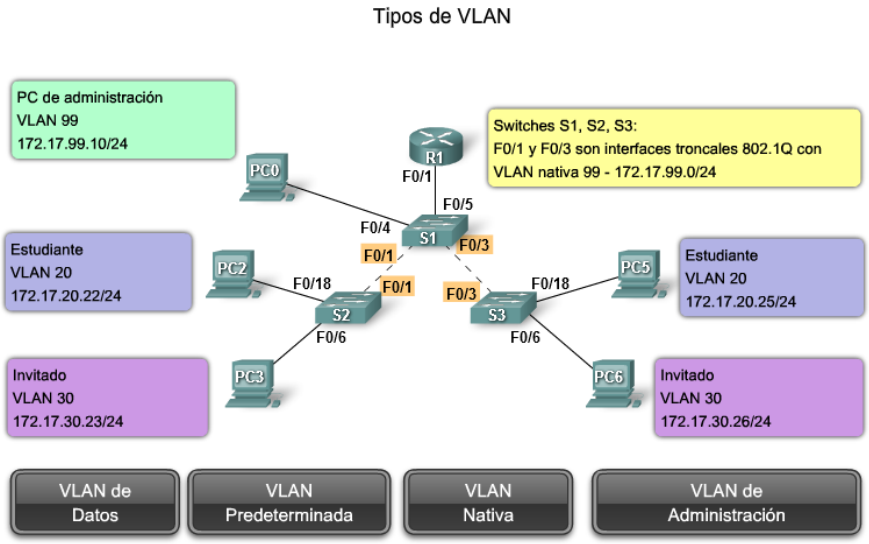


Figura 36. Tipos de VLAN

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. En la figura, el tráfico de la VLAN1 se envía sobre los enlaces troncales de la VLAN conectando los switches S1, S2 y S3. 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. A pesar de que los enlaces troncales de la VLAN se mencionan a lo largo de esta sección, se explican a detalle en la próxima sección.

Nota: Algunos administradores de red utilizan el término "VLAN predeterminada" para referirse a una VLAN que no sea la VLAN 1 que el administrador de red definió como la VLAN a la que se asignan todos los puertos cuando no están en uso. En este caso, la única función que cumple la VLAN 1 es la de manejar el tráfico de control de Capa 2 para la red.

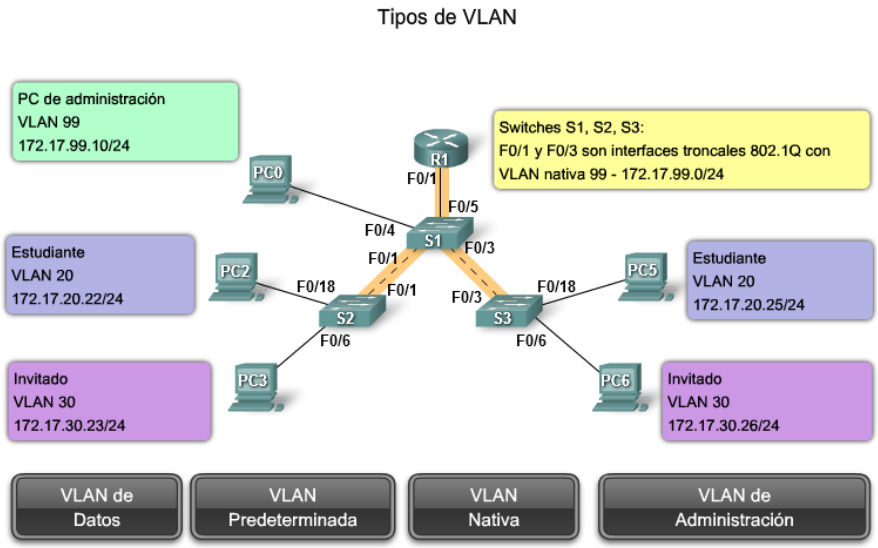


Figura 37. Tipos de Vlan

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. En la figura, la VLAN nativa es la VLAN 99. 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.

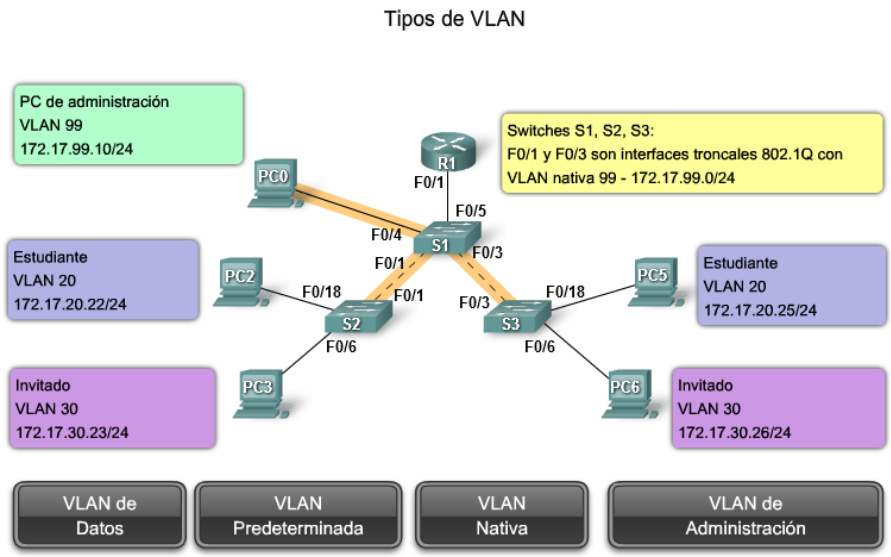


Figura 38. Tipos de VLAN

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 1serviría 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. Debido a que la configuración lista para usar de un switch de Cisco tiene a VLAN 1 como la VLAN predeterminada, puede notar que la VLAN 1 sería una mala opción como VLAN de administración; no querría que un usuario arbitrario se conectara a un switch para que se configurara de manera predeterminada la VLAN de administración. Recuerde que configuró la VLAN de administración como VLAN 99 en el capítulo Configuración y conceptos básicos de switch.

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

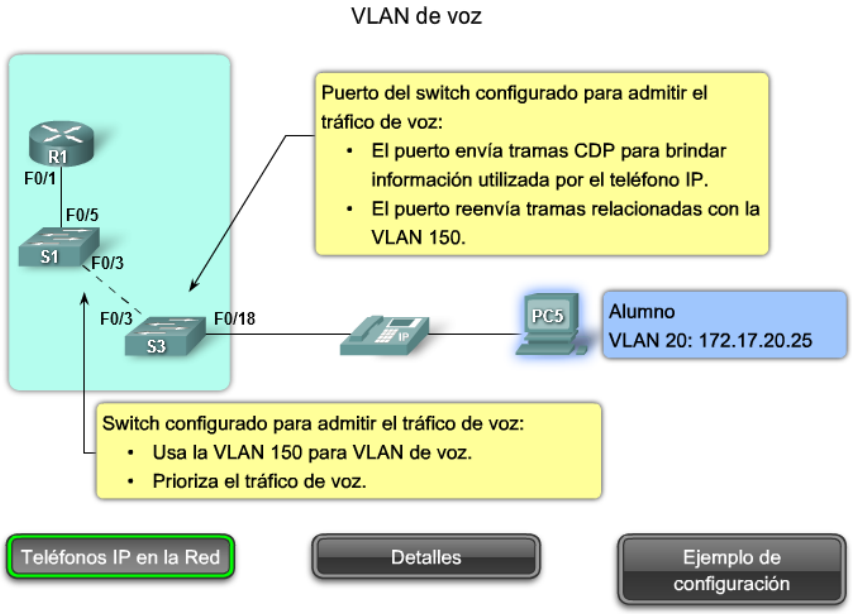


Figura 39. VLAN de voz

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.

En la figura, la VLAN 150 se diseña para enviar tráfico de voz. La computadora del estudiante PC5 está conectada al teléfono IP de Cisco y el teléfono está conectado al switch S3. La PC5 está en la VLAN 20 que se utiliza para los datos de los estudiantes. El puerto F0/18 en S3 se configura para que esté en modo de voz a fin de que diga al teléfono que etiquete las tramas de voz con VLAN 150. Las tramas de datos que vienen a través del teléfono IP de Cisco desde la

PC5 no se marcan. Los datos que se destinan a la PC5 que llegan del puerto F0/18 se etiquetan con la VLAN 20 en el camino al teléfono, que elimina la etiqueta de la VLAN antes de que los datos se envíen a la PC5. Etiquetar se refiere a la adición de bytes a un campo en la trama de datos que utiliza el switch para identificar a qué VLAN se debe enviar la trama de datos. Más adelante, aprenderá cómo se etiquetan las tramas de datos.

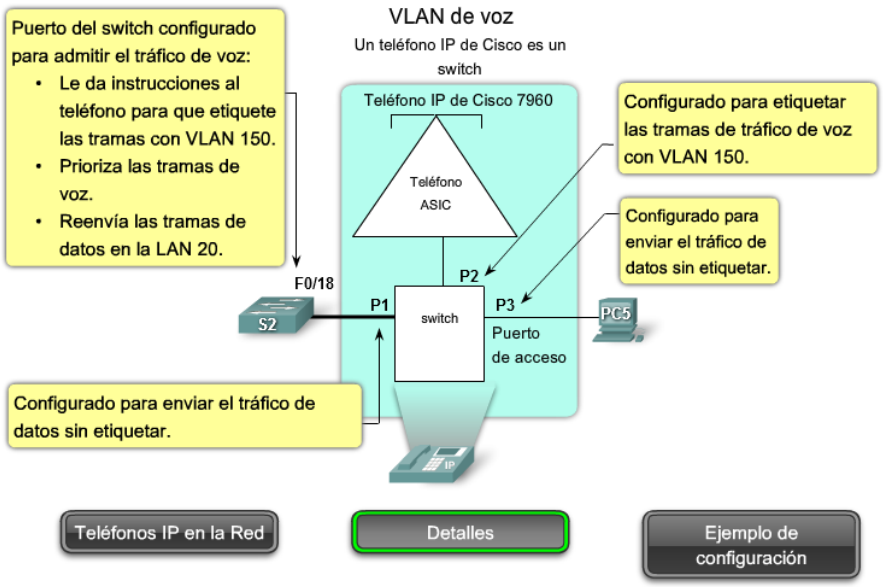


Figura 40. VLAN de voz

Un teléfono de Cisco es un switch

El teléfono IP de Cisco contiene un switch integrado de tres puertos 10/100, como se muestra en la figura. 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 figura muestra una manera de conectar un teléfono IP.

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.

Nota: La comunicación entre el switch y el teléfono IP la facilita el protocolo CDP. Este protocolo se analizará en detalle en CCNA Exploration: Curso sobre Conceptos y protocolos de enrutamiento.

Figura 41. VLAN de voz

Ejemplo de configuración

La figura muestra el resultado del ejemplo. Un análisis de los comandos IOS de Cisco está más allá del alcance de este curso pero

puede observar que las áreas destacadas en el resultado del ejemplo muestran la interfaz F0/18 configurada con una VLAN configurada para datos (VLAN 20) y una VLAN configurada para voz (VLAN 150).

2.3.8 METODOLOGÍAS PARA REDES

Metodología Cormac Long, ("IP Network Design").

Diseño Físico:

- Se estructura la red WAN jerárquicamente.
- Se estructura de cada una de las redes LAN
- Grafo enfatizando los servicios
- Grafo enfatizando los routers, switches, etc.
- Descripción de asignaciones de números IP
- Descripción de los mecanismos de enrutamiento
- Detalles de configuración de los algoritmos de enrutamiento dinámico

Metodología James McCabe ("Practical Computer Network Analysis and Design").

Fase de análisis:

Mapas de aplicaciones.

Normalmente en esta fase se detallan las redes a nivel de campus y a nivel de computadoras, asi también se detalla a nivel de LAN's dentro de un campus.

Flujos de datos simples y compuestos.

Un flujo simple y compuesto tiene las siguientes especificaciones:

- Origen y destino
- Capacidad
- Retardo
- Confiabilidad

Fase de diseño:

· Diseño lógico.

· Se establecen las metas del diseño

· Realizan la evaluación de tecnologías (costo, rapidez, confiabilidad).

· Selección de la tecnología.

· Mecanismos de interconexión.

· Integrar los aspectos de administración.

· Analizar los riesgos.

Diseño físico.

· Evaluar el diseño de cableado.

· Seleccionar la ubicación de los equipos

· Desarrollo del diagrama físico de la red.

· Incorporar las estrategias de enrutamiento de flujos

· Optimizar los flujos.

· Asignar las direcciones.

· Desarrollar una estrategia de enrutamiento.

Metodología Cisco

Fase de diseño top-down

Fase 1: Analizar Requerimientos: Fase donde se analizan las metas de negocio, técnicas, las ventajas y desventajas, también se caracterizan el tráfico de las redes existentes.

Fase 2: Diseño Lógico de la Red:Fase donde se diseña la topología de la red, la selección de los protocolos (Swiching, Routing).Desarrollar las estrategias de matenimiento y seguridad de la red.

Fase 3: Diseño Físico de la Red: Esta fase se emplea para seleccionar las tecnologías y dispositivos para las redes de cada sector o redes coperativas.

Fase 4: Probar, Optimizar y Documentar el diseño de la red:Fase

donde se probar, optimizar y documentar los diseños de la Red.

Diseño de Redes PDIOO

Describe las diferentes fases por las que un red atraviesa utilizando el ciclo de vida PDIOO (Planificación, diseño, implementación, operación, optimización).

Fase 1: Planificación (Plan): En esta fase se identifican todos los requerimientos detallados que son identificadas, así también realizar el estudio del estado actual de la red.

Fase 2: Diseño: Se diseña de acuerdo con los requisitos y el estado de red consultando con el usuario o propietario.

Fase 3: Implementación: En esta fase se procede a la creación de acuerdo con los diseños establecidos

Fase 4: Operación: En esta fase se realiza la operación y monitorización de la red y como también la respectiva comprobación final del diseño.

Fase 5: Optimización: Fase donde se realiza las detecciones y correcciones de los problemas.

2.4 Hipótesis

La segmentación de la red y priorización del ancho de banda permitirá mejorar el rendimiento y la seguridad de la red de la Universidad Nacional de San Martín – Tarapoto.

2.4.1 Hipótesis alterna

La segmentación de la red y priorización del ancho de banda SÍ permitirá mejorar el rendimiento y la seguridad de la red de la Universidad Nacional de San Martín – Tarapoto.

2.4.2 Hipótesis nula

La segmentación de la red y priorización del ancho de banda NO permitirá mejorar el rendimiento y la seguridad de la red de la Universidad Nacional de San Martín – Tarapoto.

2.5 Sistema de variables

2.5.1 Variable independiente.

La segmentación de la red y priorización del ancho de banda

2.5.2 Variable dependiente.

Rendimiento y la seguridad de la red de la Universidad Nacional de San Martín – Tarapoto.

2.6 Escala de medición

Tipo de Variable	Variable	Indicador	Escala de medición	Instrumento Evaluación.
Dependientes	Rendimiento y la seguridad de la red de la Universidad Nacional de San Martín – Tarapoto.	Nro de Ataques de Denegación de Servicios.	Unidades	Reporte de seguridad del Firewall.
Independientes	La segmentación de la red y priorización del ancho de banda	Nro de Segmentos de Red	Unidades	Documen-tación de la red.

2.7 Objetivos

2.7.1 General

- Mejorar el rendimiento de los servicios de la Red de Datos de la Universidad Nacional de San Martín - Tarapoto.

2.7.2 Objetivo Especifico

- Segmentar la red y priorizar el ancho de banda
- Incrementar el rendimiento y la seguridad de la red de datos.
- Rediseñar la red de datos aplicando criterios de segmentación y priorización de ancho de banda para incrementar el rendimiento y la seguridad de la red de datos.

III. MATERIALES Y MÉTODOS

3.1 Universo y muestra

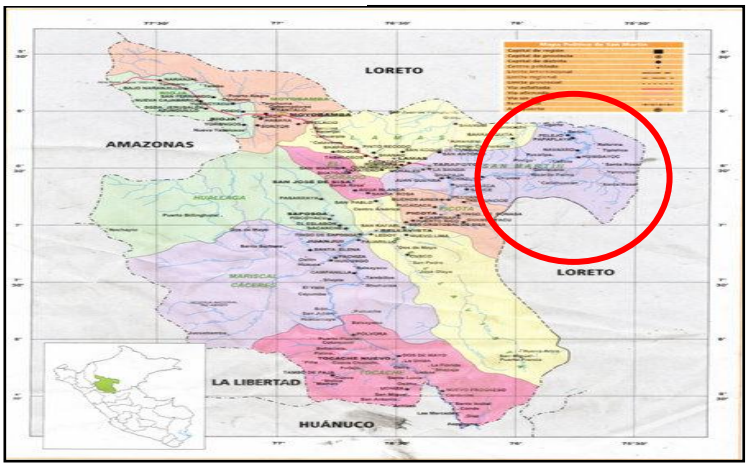
La investigación es de caso único, por lo que el universo, así como la muestra está determinado por la Red de Datos de la Universidad Nacional de San Martín - Tarapoto.

3.2 Ámbito geográfico

El proyecto ***SEGMENTACIÓN DE LA RED Y PRIORIZACIÓN DEL ANCHO DE BANDA PARA MEJORAR EL RENDIMIENTO Y SEGURIDAD LA UNIVERSIDAD NACIONAL DE SAN MARTÍN – TARAPOTO.*** se realizará en la Ciudad Universitaria de la Universidad Nacional de San Martín, en el distrito de Morales, provincia y departamento de San Martín.

Ubicación del Perú en Sudamérica Ubicación de San Martín en el Perú

Figura 42. Distribución geográfica



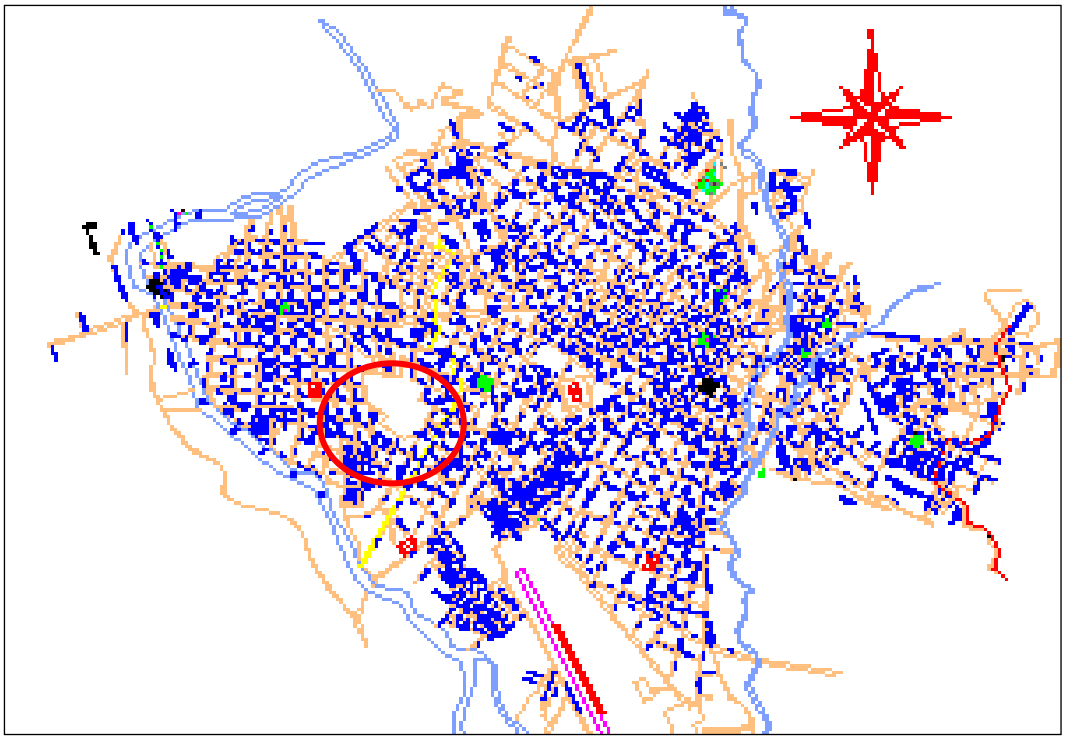


Figura 44. Ubicación de la ciudad universitaria en San Martin

3.3 Diseño de la investigación

3.3.1 Tipo de investigación

Por las características de la presente investigación, que espera poder caracterizar al fenómeno a estudiar, esta investigación es de tipo Descriptiva.

3.3.2 Nivel de investigación

La investigación desarrollada en este estudio es de nivel correlacional, fundamentado en el hecho de que se comprobará cómo la variable independiente, segmentación de la red y priorización del ancho de banda, influye positivamente en la variable dependiente que se rendimiento y seguridad de la red de la UNSM-T.

3.3.3 Diseño de investigación

Esta investigación, por sus características es de un Diseño Cuasi experimental, Transversal.

3.4 Procedimientos y técnicas

3.4.1 Procedimientos

Los parámetros para la obtención de la información estadística, serán obtenidos mediante herramientas de medición, como NTOP, IPTRAF, Fortianalyzer, considerando que su puesta en marcha debe realizarse en horarios de altas tasas de transferencias de información, archivos que pesan en promedio de 9 a 30 mbps, cuyos resultados se utilizan para su posterior análisis.

Este procedimiento se utiliza para agrupar datos por medio de la computadora, para tabular, ponderar e interpretar usando una hoja de cálculo en Excel. La información se presenta mediante histogramas.

3.4.2 Técnicas

Las técnicas para la recolección de datos que se utilizan en el estudio son: la observación, reportes de la solución implementada, la encuesta, así como softwares de simulación y medición de indicadores de red. La encuesta se define como un procedimiento que consiste en hacer las mismas preguntas, a una parte de la población, que previamente fue definida y determinada.

El software que se utiliza para la obtención de valores de indicadores de rendimiento de la red lan es NTOP, IPTRAF, así como el Fortianalyzer, que son software de análisis de tráfico de red y permiten monitorizar en tiempo real, mediante la utilización del protocolo SNMP, los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto.

Lo que hacen estos softwares es monitorizar toda la red en busca de datos para generar estadísticas. Los protocolos que son capaces de monitorizar son: TCP/UDP/ICMP/ARP.

3.5 Instrumentos

3.5.1 Instrumentos de recolección de datos

Se emplearán fuentes bibliográficas como artículos científicos obtenidos en revistas electrónicas y textos especializados sobre el tema. El método de investigación utilizado será el de la Observación, porque se trata de una investigación en la cual se recolectan datos a partir de la observación en campo del cambio de los indicadores luego de la aplicación del experimento.

Por el procesamiento de los datos, se plantea un enfoque cuantitativo toda vez que se trata de medición numérica continua de los valores de los indicadores.

3.5.2 Instrumentos de procesamiento de datos

El proceso de análisis de datos se hará siguiendo las pautas establecidas por el tipo de investigación propuesta para el presente proyecto.

Los datos obtenidos serán presentados en cuadros y gráficos, con el objeto de facilitar su análisis.

Los parámetros para la obtención de la información estadística, serán obtenidos mediante herramientas de medición como NTOP, donde se consideró su puesta en marcha en horarios de altas tasas de transferencias de información, archivos que “pesan” en promedio de 9 MB a 30 MB, cuyos resultados se utilizaran para su posterior análisis.

Este procedimiento se utilizará para agrupar los datos por medio de computadoras, a tabular, ponderar e interpretar los datos usando una hoja de cálculo en Excel, serán presentados la información recopilada por medio de encuestas que serán transcritas a su posterior análisis, en este caso el indicador estadístico serán presentados como información en forma de cuadros y gráficos.

3.6 Prueba de hipótesis

El desarrollo presentado nos permite verificar la hipótesis planteada sobre la mejora del rendimiento y seguridad de la RED

Tabla 1. Revisión de los datos Antes y Después de la segmentación de la Red

Indicador	**Item**	**Pretest**	**Postest**	**Difern**	**Broadcast**
Velocidad o tasa de transferencia de datos	Ancho de Banda disponible en Horas pico	25 kbps	5.5 Mbps	5.95 Mbps	
	Porcentaje de buen rendimiento de la Red	8 %	90 %	82%	
Disponibilidad de Servicios	Disponibilidad continua 24 horas x 7 días	No	Si		
	Frecuencia de interrupciones	3/Día	0		
Latencia de la Red	Tipos de paquetes identificados para priorización del Ancho de Banda	0	3 (datos, voz, video)		
	Tiempo en la ejecución de procesos de alta prioridad	5 horas	3.5 horas	1.5 horas	
	Tiempo para transferencia de	50 min	8 min	42 min	

	videos e imágenes				
Accesos a Recursos compartidos	Segmentos de Red de acuerdo a afinidad de usuarios o áreas	1	15		
Control o Filtros de paquetes externos e internos	Listas Control de Acceso implementadas	0	3		
Autenticación de los accesos a servicios y recursos de red a través de roles y perfiles de usuario.	Mecanismos de autenticación implementados	1	2 (Active directory y ACL's)		
Cantidad de Dominio Broadcast.	Mecanismo de segmentación reducción de la propagación de Dominios de Broadcast	1	16	15	Mitigación de tormentas de broadcast al impedir que se propague por la red deliberadamente

Fuente: Elaboración Propia.

IV. RESULTADOS

Para la presentación de resultados, se procederá a mostrar el desarrollo de la Metodología de Cysco Systems, referenciada en la bibliografía, la misma que propone varios pasos a fin de mejorar el rendimiento de una red de datos.

1. **Desarrollo de la metodología Cisco Systems**

A. Situación de la UNSM-T

El diseño de la red LAN se basará en la actual estructura topológica de la red de fibra óptica, cuyo Nodo Concentrador se encuentra en el Pabellón de Video Conferencia, a partir del cual se extienden 8 cables de fibra óptica que conectan los 23 edificios disponibles en la red de la siguiente manera:

Nodo concentrador: Pabellón de video conferencia, luego con Cable UTP →, pabellón de aulas de idiomas y laboratorio de Ciencias Básicas, luego con Radio Enlace → Pabellón Decanatura FCA, Pabellón Biblioteca Central FCA, Pabellón Decanatura FIAI, Pabellón Biblioteca Central FIAI

Cable nro 1: Pabellón FISI, luego con Cable UTP → Pabellón FMH, FIAI administrativo, FCS administrativo.

Cable nro 2: FCS administrativo, luego con Cable UTP → Pabellón FCS aulas,

Cable nro 3: Pabellón del IIMI.

Cable nro 4: Pabellón FIAI aulas.

Cable nro 5: Pabellón FCA aulas y laboratorios

Cable nro 6: Pabellón FICA aulas, luego con Cable UTP → Laboratorios y Oficinas Administrativas

Cable nro 7: Pabellón FCE aulas.

Cable nro 8: Pabellón Infraestructura, luego mediante radio enlace →, Local Central, Complejo Universitario y Escuela Académico Profesional de Turismo – Lamas.

En esta etapa iniciamos el proceso de recopilación de información en la Universidad Nacional de San Martín - Tarapoto, para así identificar los problemas de la red actual, apoyados también en parámetros como el crecimiento anual y proyecciones de crecimiento, procedimientos de administración, académicos, sistemas, y el resto de las áreas anteriormente mencionadas. Para ello, se planteó los siguientes puntos al reunir la información:

a. Personas que utilizan la red.

b. Operaciones que han sido declaradas críticas por la organización.

c. Equipos.

d. Hosts instalados

e. Calidad de Servicio.

f. Recursos para brindar seguridad LAN.

En conjunto, la población universitaria, requiere para sus procesos individuales o grupales un Ancho de Banda en horas críticas (Entre 45 MB/s y 99 MB/s) y mejoras en los parámetros de seguridad de la red (Resultados de encuesta interna y análisis de vulnerabilidades LAN).

Para ello, la propuesta de ***implementar redes virtuales para segmentar la red y configurar nuevos estándares de seguridad en equipos de comunicación***, parte de la premisa de elevar la eficiencia y efectividad de la red. Estas mejoras se plasman en la reducción de tiempos de procesos de alta prioridad, mejorar la flexibilidad, mediante tolerancia a fallas y mayor escalabilidad, brindar mayores controles de seguridad para asegurar la integridad de la información; todo ello apoyado en una plataforma estratégicamente configurada.

B. Operaciones que han sido declaradas críticas por la organización.

Mediante un análisis de los distintos procesos académicos y administrativos que se llevan a cabo en la empresa, se clasificaron y puntualizaron de

acuerdo al grado de impacto que poseen dentro de los procesos core de la institución.

C. Data:

Debido a que el “tamaño” y demanda de datos aumentó de manera exponencial, la red de datos actual se degrada en horas pico en índices por debajo de lo aceptable (10 Mb/s a 8 Mb/s), generando un impacto en el tráfico de la red actual y afectando la operatividad de la organización.

D. Equipos:

Si los equipos que permiten enlaces fallasen permanentemente, originaría un retraso en los procesos académicos y administrativos diarios y retraso en la generación de información para la toma de decisiones y procesos a seguir.

Los switch 3COM 8800 y 3COM 4400 Series, están configurados con funciones predeterminadas, donde no se está explotando al máximo el potencial de los equipos.

E. Seguridad:

Este segmento conforma la columna vertebral de la plataforma Lan, donde si se ve vulnerada, el impacto podría afectar seriamente procesos, tareas, actividades, etc. Un ejemplo de ello es el compartir recursos en la red y su disponibilidad para cualquier usuario del recurso, acceso a internet sin restricciones y filtros, ejecución de comandos de acceso remoto desde cualquier terminal, etc

F. Equipos de comunicación

Switch CORE.

La Universidad Nacional de San Martín, cuenta en la actualidad con un switch 3COM 8800, el mismo que sirve como CORE o centro de la estrella de toda la red de datos y soporta la interconexión directa de todos los host’s

y servidores principales, sin embargo solo está instalado con la configuración por defecto.

G. Hosts soportados

Representa la distribución de las computadoras entre todos los edificios de la Ciudad Universitaria.

Tabla 2. Distribución de las PCs Universidad Nacional de San Martín - Tarapoto

Edificios	Hosts Soportados según Máscara
FISI – FMH	254
FICA	254
FCA	254
FIAI	254
INFRA – Complejo – Local Central	510
IIMI	254
IDIOMAS – OTRAS	510
FCE	254
Total	**2544**

Fuente: Elaboración Propia.

H. Calidad de Servicio

Se ha determinado que los equipos de comunicación instalados tienen la capacidad de soportar la implementación de tecnologías que mejorarán el rendimiento y seguridad en la red como por ejemplo: VLAN, ACL, QoS, etc.

Análisis de Factibilidad.

A. Factibilidad Operativa

Para poner en marcha este proyecto en la Universidad Nacional de San Martín - Tarapoto, no es necesario contratar personal adicional al existente, considerando que si se llegase a implementar la propuesta, ésta sólo afectaría los controles internos o niveles lógicos, cambios en los parámetros de configuración, implementación de nuevos protocolos, etc.

El personal operativo, llevará a cabo sus tareas o actividades de la misma manera en la que ha venido haciéndolo, considerando que es personal calificado y adaptable a cambios tecnológicos (uno de los requisitos de la propuesta). Por ello, la factibilidad operativa es dable en este contexto.

B. Factibilidad Técnica

La plataforma tecnológica si bien está trabajando y soportando múltiples procesos, está aún no ha llegado al tope de su capacidad operativa, debido a que las características técnicas que presentan (Switch 3COM, Router 2800 Series, Procesadores Core 2 Dúo, Core i3, Intel Xeon, Cableado estructurado con certificación de calidad 5E, etc.) aún no han sido dispuestas desde un enfoque estratégicamente acorde a la nueva realidad problemática.

C. Factibilidad Financiera

La UNSM-T, cuenta con disponibilidad económica para sustentar el desarrollo e implementación de este proyecto de investigación, sin embargo, el uso de los mismos no será necesario toda vez que para la ejecución de este proyecto no se considera la necesidad de realizar gastos para la ejecución del mismo toda vez que serán íntegramente financiados por el tesista.

Nº	Descripción	Cant	U/M	Modalidad
1	Computadora Corel i3 (incluye accesorios)	01	Unid.	Préstamo
2	Impresora	01	Unid.	Préstamo
4	Servicio de Internet	01	Unid.	Préstamo
5	Switch 3com 8800	01	Unid	Préstamo-UNSM
6	Firewall Fotigate 600C	01	Unid	Préstamo-UNSM
Total S/.				**0.00**

Fase II: Análisis de Datos y Requisitos

Análisis de la Red actual de la Universidad Nacional de San Martín - Tarapoto.

La red cuenta con las siguientes características:

- La red presenta una topología estrella pero es plana en su diseño lógico lo cual representa varias desventajas, incluyendo un único dominio de broadcast de Capa 2 como, por ejemplo, una petición ARP, viaja hacia cada host y dispositivo en la LAN, estos y otros broadcasts de capa 2 consumen una gran cantidad del ancho de banda disponible de la LAN, ello aunado al vertiginoso volumen de información que se da entre host durante horas pico que logran generar “cuellos de botella”.

- La asignación de IP’s privados en cada Pc es manual, seguidos por un orden consecutivo (192.168.0.1/20, 192.168.0.2/20, 192.168.0.45/20, …192.168.15.254/20)

- Debido a su diseño lógico brinda menor flexibilidad en el tráfico de red y la seguridad. No existe ningún control sobre la ruta de las tramas. La fiabilidad es baja, debido a que no se tiene disponibilidad de la red al 100% durante las 24 horas.

- Las características técnicas de los dispositivos de conectividad son de un alto nivel, como es el caso de los switches 3COM modelo 4400, Router modelo 2800 Series, que poseen la capacidad suficiente para soportar las altas exigencias que hoy en día soporta la red. Sin embargo no existe una administración más rigurosa de estos equipos.

- El cableado estructurado esta implementado de acuerdo a las normas de calidad, respetando así espacios entre distintos enlaces, canaletas correctamente ubicadas, etc., presentando para ello un certificado de garantía.

- No existen políticas de seguridad rigurosa y acorde a los procesos académicos y administrativos de trabajo.

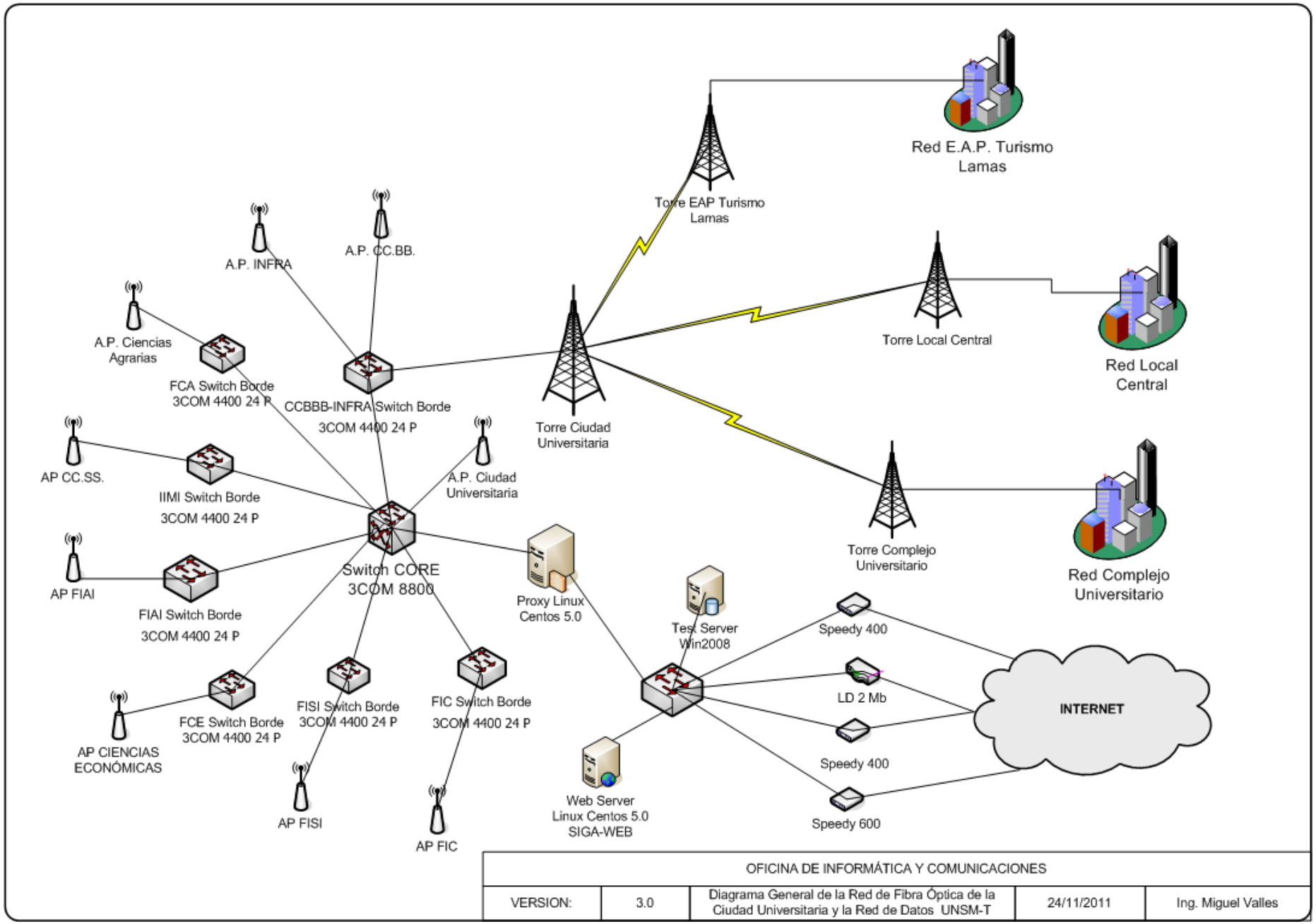


Figura 45.Red Actual de la Universidad Nacional de San Martín – Tarapoto

2. **Análisis Rendimiento de la Lan.**

Se realizó el análisis del tráfico de red de la Universidad Nacional de San Martín, la cual gracias a las herramientas de análisis de rendimiento LAN, permitieron obtener resultados que grafican el estado actual de la red. El promedio ideal o esperado del tráfico fluctúa entre los 45 MB/s a 90 MB/s, siendo el objetivo primordial medir el rendimiento, observar cuan congestionada esta nuestra red, y emplear mecanismos para evitar el mal rendimiento.

Una de las causas de congestión que se determinó son las siguientes: ·

- Velocidad insuficiente de las líneas.
- Ausencia de estrategias QoS.
- Interfaces de baja velocidad en los enlaces troncales.
- Protocolos IPX presentes en Pc's de manera innecesaria por tema de usabilidad.
- Para poder obtener el rendimiento real de la red; se ha utilizado el software PTRG NETWORK MONITOR.

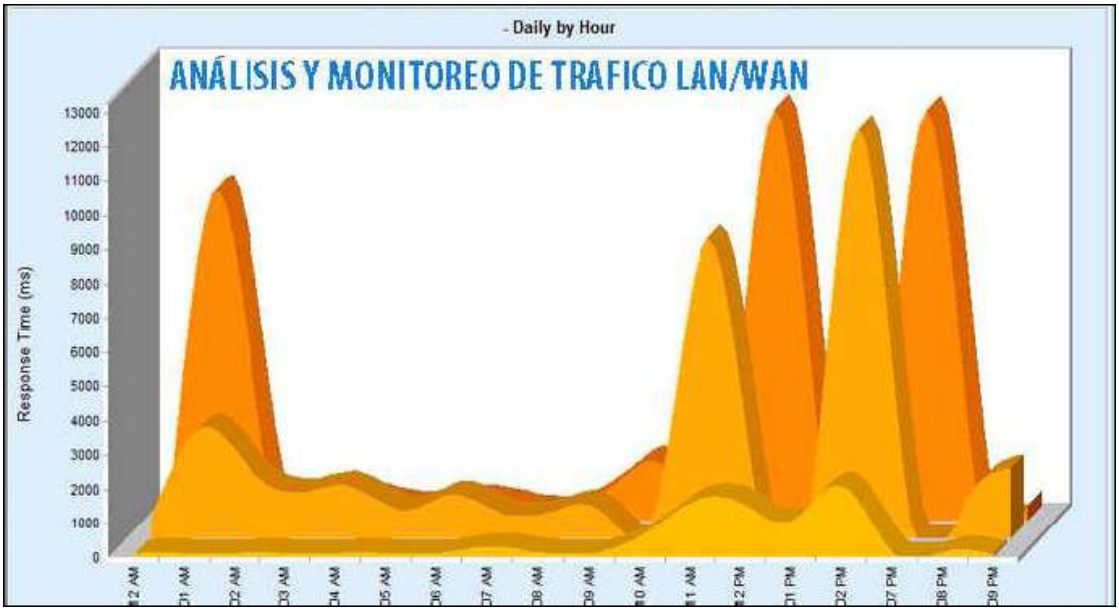


Figura 46. Análisis y monitoreo de trafico LAN/WAN

Descripción. En la figura Nº 03 observamos que durante las horas 12 am y 1 am existe una mayor saturación en nuestra red local, originando un tiempo de retardo mayor en las transacciones que están fluyendo, esto se debe a que los enlaces no pueden administrar una gran cantidad de información.

También se observa que entre las horas 7:00 am a 10:00 am existe un tráfico de red menor, lo que permite que la red trabaje de manera fluida sin percances o saturación.

Del mismo modo se detalla que entre las 11 am y 9 pm el tráfico aumentó de manera exponencial, ocasionando un bajo rendimiento de la Lan, todo ello muestra que la infraestructura tecnología de comunicación no cumple con el estándar adecuado de velocidad.

3. **Análisis de Seguridad de la Red.**

El activo más importante en las organizaciones públicas, privadas y de cualquier índole, es la información que tienen. Entre más grande es la organización más grande es el interés de mantener la seguridad en la red, por lo tanto, es de suma importancia brindar todas las garantías necesarias a la información o Data.

Dentro del entorno de la red de la Universidad Nacional de San Martín - Tarapoto, se detectaron los posibles puntos vulnerables:

- Falta de políticas de seguridad en la red interna, como permisos y restricciones hacia los dispositivos intermediarios de red.
- Falta de parametrización en el acceso a los recursos compartidos.
- Ausencia de ACL’s (Lista de control de acceso) para el filtrado de paquetes de forma externa e interna.
- No existe un servidor de autenticación para el acceso, control y administración de los dispositivos intermediarios de red.

- Acceso de “extremo a extremo” no controlado.
- Acceso no controlado a los servicios de internet.
- Falta de mecanismos de aislamiento y protección a los dispositivos finales.
- Ausencia de mecanismos de control y administración en el almacenamiento de archivos.

4. **Análisis de los Requerimientos.**

4.1 Firewall Fotigate 600C

Dispositivo que funcionara como cortafuegos entre redes, permitiendo o denegando las trasmisiones de una red a la otra. Sera situado entre la red local y la red Internet como dispositivo de seguridad para evitar que los intrusos puedan acceder a la red interna.

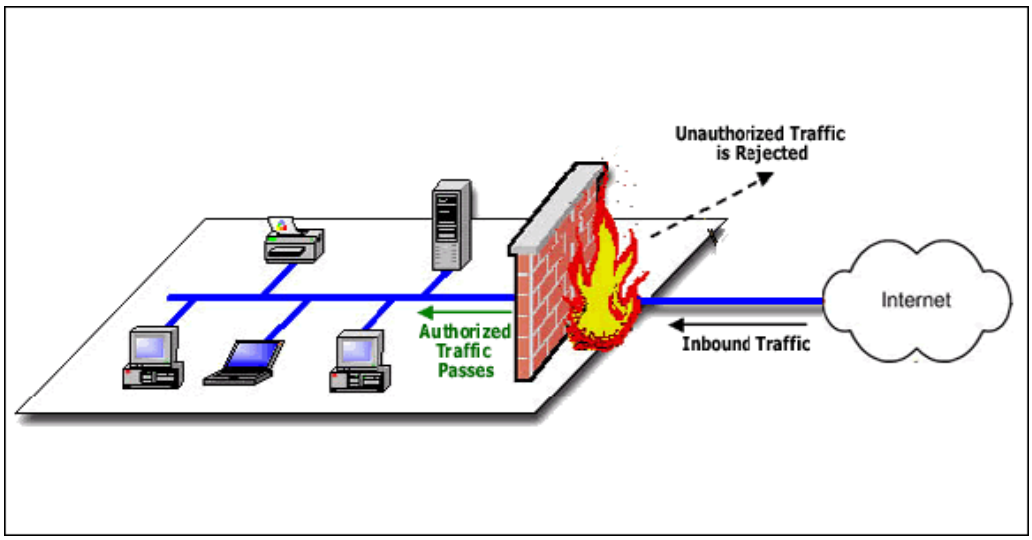


Figura 47. Firewall

Cumplirá las siguientes funciones:

0 Filtrado de Paquetes.

1 Implementación de ACL.

2 Permisos y restricciones en determinados puertos, etc.

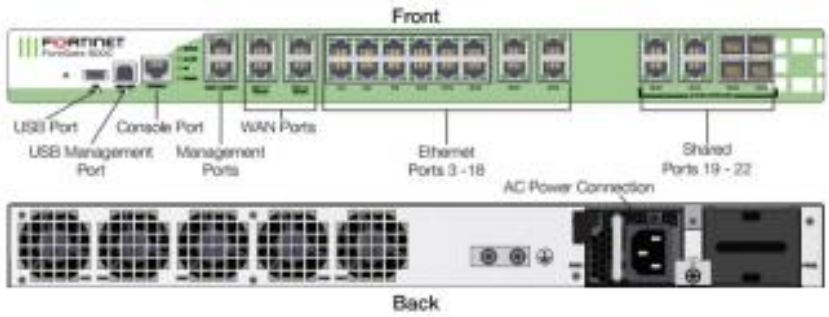


Figura 48. Firewall ASA 5520 – Dispositivo seleccionado

Tabla 3. Características del Firewall seleccionado

Descripción del producto Fortigate 600C - aparato de seguridad	
Tipo de dispositivo	Aparato de seguridad
Tipo incluido	Montable en bastidor - 1U
Dimensiones	44.5 cm x 33.5 cm x 4.4 cm
Peso	9.1 kg
RAM instalada (máx.)	2 GB
Memoria flash instalada	256 MB Flash
Protocolo de interconexión de datos	Fast Ethernet, Gigabit Ethernet
Red /Protocolo de transporte	IPSec
Rendimiento	Capacidad del cortafuegos : 450 Mbps Capacidad de la VPN : 225 Mbps Tasa de conexiones : 9000 sesiones x s
Sesiones concurrentes :	280000
Peers VPN IPSec :	750
Peers VPN SSL :	2
Interfaces virtuales (VLAN):	100
Capacidad	
Características	Protección firewall, asistencia técnica VPN, equilibrio de carga, soporte VLAN
Alimentación	CA 120/230 V (50/60 Hz)

Fuente: Elaboración propia.

Observación:

Si bien un firewall lógico constituye una alternativa más económica en relación con los firewall basados en hardware, sin embargo presentan mayores desafíos en su implementación.

- Debe seleccionarse adecuadamente la plataforma de hardware y endurecer el sistema operativo, para realizar reenvío de paquetes.
- Corren por defecto servicios que no son requeridos si la máquina funciona como firewall exclusivamente.
- Su arquitectura es menos robusta y especializada para operar como analizador de paquetes.
- Consume recursos del computador que lo aloja.

Por ello la elección de un firewall Físico como parte de la propuesta de implementación obedece a que estos dispositivos fueron concebidos íntegramente para mitigar ataques, puesto que su arquitectura fue diseñada para ello.

- También muestran un mejor desempeño en comparación con los firewalls basados en software.
- Menor tiempo de implementación que los firewalls basados en software.
- Reducen necesidad de decidir entre hardware, sistema operativo y software de filtrado, ya que todo viene configurado, simplificado y optimizado en un solo paquete.

5. **Redes Virtuales (VLAN)**

Nuestra red pretende presentar configuración e implementación de redes de área local virtuales, para mejorar el rendimiento de la red, proveer seguridad, segmentación, mejor administración de red, reducción de costos, uso adecuado y jerárquico cumpliendo con todas los estándares

de red. La infraestructura tecnológica con que se cuenta, permite soportar Redes Virtuales, permitiendo así implementar toda la gama de configuraciones para mejorar el desempeño de la LAN.

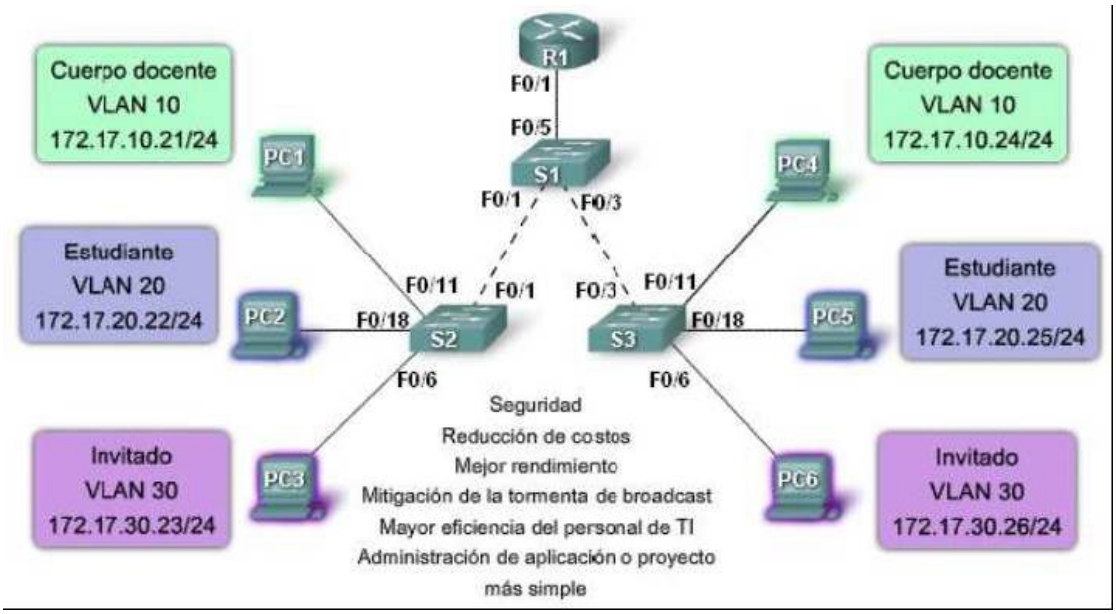


Figura 49. Diseño VLAN

Si bien los equipos que soportan las comunicaciones de la Universidad Nacional de San Martín - Tarapoto; son de la Familia 3COM, también existen otras marcas líderes en el mercado, como: 3COM (HP), AVAYA, D-Link, ENCORE

La Universidad nacional de San Martín cuenta con un diseño estructurado utilizando tecnología 3COM, y por ello no es pretensión cambiar los equipos por otras marcas o modelos de las mismas, sino todo lo contrario; la idea es utilizar los dispositivos con que contamos y elevar su nivel de trabajo mediante estrategias e implementaciones lógicas y físicas, para de esta manera obtener mejores resultados que los actuales.

Los equipos de Red son los siguientes:

- Router Cisco 2800 series – Cantidad : 1
- Switch 3COM 8800 – Cantidad : 1
- Switch 3COM 4400 – Cantidad : 7

6. **Diseño de la Solución**

IV.6.1.1. Diseño de la Estructura Lógica

Criterios

De acuerdo a los lineamientos de desarrollo que queremos alcanzar para un correcto rediseño lógico, nos basamos en 4 criterios fundamentales:

- Seguridad
- Funcionalidad
- Escalabilidad
- Adaptabilidad

El objetivo principal es mejorar el Rendimiento y Seguridad de la plataforma LAN que soporta los procesos de la Universidad Nacional de San Martín - Tarapoto, para ello los 4 criterios serán los pilares para esta propuesta.

a) Seguridad.

- ACL, la red mantendrá la 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.
- Tecnologías Seguridad Emergentes: NetWork Access Protection, que establece Redes de cuarentena ante cualquier infección o ataque interno y File Screening

Management que bloquea el almacenamiento en el servidor de archivo no autorizados como música, videos, etc.

- Se aplicara la configuración un Firewall Físico instalado, modelo Fortinet 600C para el filtrado de paquetes entrantes y salientes, reforzando de esta manera la protección en la Lan.

b) Funcionalidad.

La red proporcionará conectividad de usuario a usuario a través de la red, y de usuario a aplicación con una velocidad y confiabilidad muy razonable.

- VLAN, mediante la segmentación de la LAN en subredes, permitirá crear fronteras lógicas para los distintos edificios y sedes, aumentando los niveles de seguridad.

- La red será sensible a QoS para así efectuar la priorización del tráfico para permitir que flujos importantes se gestionen antes que flujos con menor prioridad, y una mayor fiabilidad de la red, ya que se controla la cantidad de ancho de banda que puede utilizar cada aplicación.

- La red actual cuenta con la asignación de IP de manera manual, donde el control es consecutivo: 192.168.0.1/20 – 192.168.15.254/20.... Ante este panorama se implementara un Servidor DHCP para la asignación automática de IP en todos los dispositivos finales de la LAN, bajo los parámetros de rango de cada Vlan.

c) Escalabilidad.

La red podrá 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.

Los Switches son escalables para permitir aumentar la cantidad de puertos para soportar crecimientos futuros.

d) Adaptabilidad.

La red estará rediseñada teniendo en cuenta las diferentes tecnologías y sus diferentes aplicaciones normativas lo que garantizará una amplia adaptabilidad muy independiente de la tecnología que se llegase a implementar.

7. **Estructura Modelo Jerárquico de 3 Capas – Metodología Cisco**

7.1 Capa de acceso

La implementación de esta capa (Física) cuenta con certificación de calidad, lo que involucra que el cableado estructurado se encuentra en condiciones, brindando la seguridad de no anomalías bajo esta naturaleza.

7.2 Capa de distribución

Aquí se establece el punto medio entre la capa de acceso y los servicios principales de la red. La función primordial de esta capa es realizar las siguientes funciones:

Servir como punto de concentración para acceder a los dispositivos de capa de acceso.

- Enrutar el tráfico para proporcionar acceso a los departamentos o grupos de trabajo.
- Segmentar la red en múltiples dominios de difusión / multidifusión.
- Proporcionar servicios de seguridad y filtrado.

- Proporcionará conectividad basada en una determinada política.

Asimismo este nivel se encargara del direccionamiento hacia los nuevos Servidores propuestos como: FTP (Alojado en Servidor de Datos SVICTORIA1), Radius (Alojado en Servidor Arkitex), DHCP (Alojado en el Router Cisco 2800 Series)

7.3 Capa de Núcleo

La capa del núcleo, principal o Core se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados. Normalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios. Estos servicios se conocen como servicios globales o corporativos.

Algunos de tales servicios pueden ser e-mail, el acceso a Internet o la videoconferencia. Cuando un usuario necesita acceder a un servicio corporativo, la petición se procesa al nivel de la capa de distribución.

El dispositivo de la capa de distribución envía la petición del usuario al núcleo. Este se limita a proporcionar un transporte rápido hasta el servicio corporativo solicitado. El dispositivo de la capa de distribución se encarga de proporcionar un acceso controlado a la capa de núcleo.

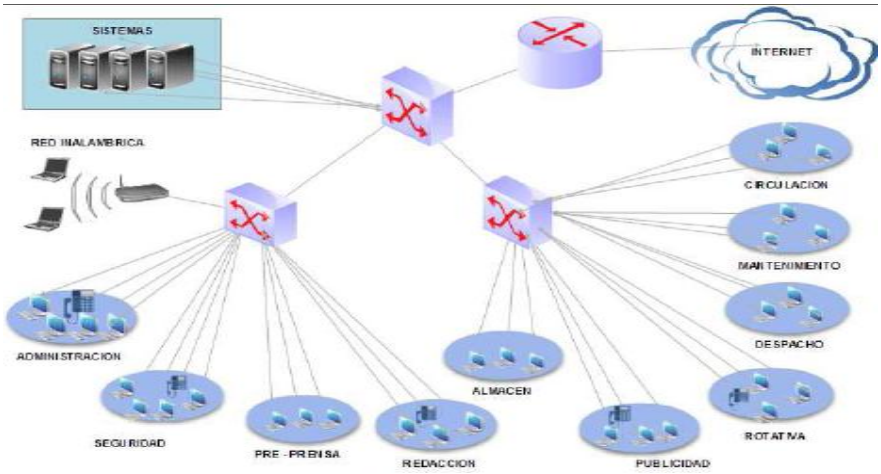


Figura 50. Capa núcleo

a. Diseño de la Estructura de Seguridad

8.1 Acceso a Páginas de Internet.

La seguridad se desplegará a través del uso de ACL (Access Control List).

En la Universidad Nacional de San Martín - Tarapoto, se han tomado en cuenta estrictas políticas de seguridad, y para ello se implementan Listas de Control de Acceso configuradas en nuestro Firewall.

8.2 Implementación de listas de control de acceso (ACL)

A continuación se presenta la tabla que muestra un resumen de las ACLs que aplican para discriminar el acceso al servicio de internet en toda la red corporativa.

Tabla 4. Listas de control de acceso para mejorar la seguridad perimetral.

FILTRADO WEB							
Categoría		Básico		Intermedio		Avanzado	
		P	B	P	B	P	B
Potentially Liable							
Sitios web que informan actividades ilegales de drogas, tráfico y distribución.	Drug Abuse		x		x		x
Sitios web que representan actividades ilícitas, no autorizada acceso a programas, computadoras, equipos, sitios web.	Hacking		x		x		x
Sitios web que informan las características, métodos o instrucciones sobre acciones fraudulentas, estafas, falsificación	Illegal or Unethical		x		x		x
Los sitios que promueven la identificación de grupos raciales, la denigración o el sometimiento de los grupos, o la superioridad de cualquier grupo.	Discrimination		x		x		x
Sitios web que muestran material ofensivo en la brutalidad, la muerte, crueldad, actos de abuso, mutilaciones.	Explicit Violence		x		x		x
Sitios web que contiene información de grupos radicales, milicias con acciones agresivas contra el gobierno, creencias.	Extremist Groups		x		x		x
Sitios web que proporcionan información, herramientas sobre cómo evitar los controles de acceso a Internet y navegar por la web anónimamente, incluye servidores proxy anónimos	Proxy Avoidance		x		x		x
Sitios web que ofrecen, distribuir o vender ensayos , proyectos o diplomas catalogados como plagio.	Plagiarism		x		x		x
Sitios web que contienen o puedan distribuir imágenes de niños que se representan en un estado de abuso.	Child Abuse		x		x		x
Adult/Mature Content							
Los sitios web que proporcionan información sobre las promociones de las religiones o no especificadas en las religiones tradicionales u otras creencias y prácticas no convencionales, culto, o folclóricos. Los sitios que promueven u ofrecen métodos, medios de instrucción y otros recursos para afectar o influir en acontecimientos reales a través del uso de hechizos, maldiciones, poderes mágicos, satánicos o seres sobrenaturales.	Alternat Beliefs	x		x		x	
Sitios web relacionados con datos sobre el aborto, la información, las cuestiones jurídicas y organizaciones.	Abortion	x		x		x	
Sitios web de contenido para adultos (18 + años y más),sexualidad, clubes de striptease, sex-shops.	Other Adult Materials		x		x		x
Esta categoría está dirigido a organizaciones que realizan campaña o buscan apoyo de la consciencia pública, influenciando en la política pública.	Advocacy Organizations	x		x		x	
Sitios web que se adaptan a las actividades de juego como las apuestas, loterías, casinos de juego.	Gambling		x		x		x
Sitios web de contenido para adultos que representan el cuerpo humano en la desnudez total o parcial, sin la intención de excitar sexualmente.	Nudity and Risque		x		x		x
Sitios web de contenido que presentan actos sexuales con la intención de excitar sexualmente y emocionar.	Pornography		x		x		x
Sitios web dedicados al uso de redes sociales ,anuncios personales, servicios de citas, clubes.	Dating		x		x		x
Sitios web que cuentan con la promoción o venta legal de armas como pistolas, cuchillos, rifles, explosivos.	Weapons		x		x		x
Sitios que proporcionan información o promover el cultivo, la preparación o el uso de la marihuana.	Marijuana		x		x		x
Sitios web educativos que proporcionan información sobre hablar de sexo y la sexualidad, sin la utilización de materiales pornográficos.	Sex Education	x		x		x	
Sitios web que promueven o vender legalmente productos de alcohol y accesorios.	Alcohol	x		x		x	
Sitios web que promueven legalmente o venta de productos de tabaco y accesorios.	Tobacco	x		x		x	
Sitios web que utiliza imágenes de semidesnudos modelos de lencería, ropa interior y trajes de baño para el propósito de vender o promover esos artículos.	Lingerie and Swimsuit	x		x		x	
Sitios web de contenido deportes de caza, juegos de guerra, las instalaciones de paintball, organizaciones y grupos.	Sports Hunting and War Games		x		x		x
Bandwidth Consuming	**Bandwidth Consuming**						
Sitios cuya principal función es la de proporcionar descargas	Freeware and		x		x	x	

FILTRADO WEB							
Categoría		Básico		Intermedio		Avanzado	
		P	B	P	B	P	B
freeware y software.	Software Downloads						
Sitios web que permiten a los usuarios utilizar los servidores de Internet para almacenar archivos personales o para compartir fotos.	File Sharing and Storage	x		x		x	
Los sitios web que permiten la descarga de archivos multimedia MP3 u otros.	Streaming Media and Download		x		x	x	
Los sitios web que permiten a los usuarios compartir archivos y almacenamiento de datos entre ellos.	Peer-to-peer File Sharing		x		x	x	
Los sitios web con programas de radio y televisión a través de Internet.	Internet Radio and TV		x		x		x
Los sitios web que permiten las comunicaciones telefónicas a través de Internet.	Internet Telephony		x	x		x	
Security Risk	**Security Risk**						
Sitios web catalogados como malware	Malware		x		x		x
Los sitios que software host que está secretamente descargado en el equipo del usuario para recoger la información y la actividad de los usuarios del monitor, y los sitios que están infectados con software destructivo o dañino, especialmente diseñado para dañar, alterar, atacar o manipular los sistemas informáticos sin el consentimiento del usuario, como virus o troyano.	Malicius Websites		x		x		x
Páginas web falsificados que duplican legítimos páginas web de negocios para el propósito de la obtención de información privada financiera, personal u otro de los usuarios.	Phishing		x		x		x
Sitios web o páginas web cuya URL se encuentran en los mensajes de spam. Estas páginas suelen anunciar sitios de sexo, artículos fraudulentos y otros materiales potencialmente ofensivos.	Spam URLs		x		x		x
General Interest – Personal							
Sitios que ofrecen gráficos publicitarios u otros archivos de contenido de anuncios, incluidos los servidores de anuncios.	Advertising		x	x		x	
Los sitios que apoyan la negociación activa de valores y gestión de inversiones.	Brokerage and Trading	x		x		x	
Sitios que proporcionan información o promoción de los juegos electrónicos, juegos de video, juegos de ordenador, juegos de rol, juegos o juegos en línea.	Games		x		x	x	
Los sitios que permiten a los usuarios utilizar los servicios de correo electrónico.	Web-based Email	x		x		x	
Sitios que proporcionan información o promueven el cine, la radio y la televisión no-noticias, música y guías de programación, libros, humor, tebeos, cines, galerías, artistas o revisiones en el entretenimiento y revistas. Incluye sitios de libros que tienen sabor personal o extra-material de los autores de promover los libros.	Entertainment		x	x		x	
Sitios web donde se informan temas de cultura	Arts and Culture	x		x		x	
Instituciones Educativas: sitios patrocinados por las escuelas, otras instituciones educativas. Sitios que se relacionan con eventos educativos y actividades.	Education	x		x		x	
Sitios que proporcionan información o consejos sobre la salud personal o los servicios médicos, procedimientos. Esta categoría incluye a los proveedores de cirugía estética, hospitales infantiles.	Health and Wellness	x		x		x	
Los sitios que ofrecen información o apoyo a la búsqueda de empleo o empleados. Incluye agentes de carrera y servicios de consultoría que ofrecen ofertas de trabajo.	Job Search	x		x		x	
Los sitios que ofrecen información sobre los medicamentos aprobados y su uso médico.	Medicine	x		x		x	
Los sitios que ofrecen noticias de actualidad y de opinión, periódicos, revistas de circulación, radio y televisión.	News and Media		x	x		x	
Sitios web dedicados al uso de redes sociales, anuncios personales, servicios de citas, clubes.	Social Networking		x		x	x	
Los sitios que son patrocinadas o proporcionar información sobre los partidos políticos y grupos de interés.	Political Organizations		x	x		x	
Los sitios web que proporcionan datos generales de referencia en forma de bibliotecas, diccionarios, enciclopedias, mapas, directorios, normas, etc.	Reference	x		x		x	
Los sitios que ofrecen información sobre religiones, creencias.	Global Religion	x		x		x	

FILTRADO WEB							
Categoría		Básico		Intermedio		Avanzado	
		P	B	P	B	P	B
Sitios web que ofrecen en línea promoción o venta de bienes y servicios generales, tales como la electrónica, flores, joyas, música.	Shopping and Action		x	x		x	
Esta categoría incluye sitios que se ocupan de temas de la vida cotidiana y las preferencias como aficiones (jardinería, filatelia, mascotas), revistas, blogs.	Society and Lifestyles		x	x		x	
Sitios web de actividades deportivas.	Sports		x		x	x	
Sitios web con los recursos para viajes, alojamiento, transporte (ferrocarril, líneas aéreas, cruceros), las agencias, los lugares turísticos, las atracciones turísticas, avisos.	Travel		x		x	x	
Sitios web que contienen información sobre la venta de autos, barcos, aviones, motocicletas, etc., incluidas las partes y accesorios.	Personal Vehicles		x		x	x	
URLs generadas dinámicamente por un servidor Web.	Dynamic Content		x		x		x
Esta categoría contiene URLs que no puede ser categorizada debido a la falta o a la ambigüedad del contenido	Meaningless Content		x		x	x	
Sitios web de contenido de adivinación, horóscopos, la quiromancia, lectura de tarot, historias.	Folklore		x		x	x	
Sitios que alojan los servicios de Web chat o que o proporcionan información sobre el chat a través de HTTP o IRC.	Web Chat		x		x	x	
Los sitios que permiten a los usuarios comunicarse en tiempo real a través de Internet.	Instant Messaging		x		x	x	
Sitios web grupos de discusión, tablones de anuncios y servidores de listas, incluye 'blogs' y 'revistas correo.	Newsgroups and Message Boards		x	x		x	
Sitios para enviar / ver tarjetas postales digitales.	Digital Postcards		x		x		
Sitios web desarrollado para niños de 12 años o menores. Incluye juegos educativos, herramientas, organizaciones y escuelas.	Child Education	x		x		x	
Los sitios web que promocionen la venta o alquiler de inmuebles.	Real Estate		x		x	x	
Sitios web relacionados con restaurantes y comedores, como los lugares de comida, comentarios, recetas, servicios de catering.	Restaurant and Dining		x		x	x	
Páginas web privadas que albergan información personal, opiniones e ideas de los propietarios.	Personal Websites and Blogs	x		x		x	
Los sitios que distribuyen contenidos para sitios web suscritos. Incluye servidores de imágenes y Web.	Content Servers		x		x	x	
Los sitios que simplemente son lugar los titulares de dominios sin contenido significativo.	Domain Parking		x		x	x	
Webs que ofrecen banca en línea, el comercio, la salud, y otros que contienen la información personal privada.	Personal Privacy		x		x	x	
General Interest – Business							
Los sitios que ofrecen noticias y cotizaciones de acciones, bonos ,datos Financieros y Servicios. Incluye bancos, uniones de crédito, tarjetas de crédito y seguros.	Finance and Banking	x		x		x	
Los sitios que apoyan la búsqueda de la Web, grupos de noticias, o índices / directorios. Los sitios de motores de búsqueda que proporcionan información exclusivamente para ir de compras o comparar precios, sin embargo, caen en Compras y Subastas.	Search Engines and Portals	x		x		x	
Los sitios que atienden a grupos, clubes u organizaciones de personas con intereses similares, ya sea profesional, social, humanitaria o de ocio en la naturaleza. Organizaciones Sociales y Afiliación: Sitios patrocinados por o que apoyan o ofrecen información sobre organizaciones que se dedican principalmente a socializar o intereses en común aparte de la filantropía o advancement. Not profesional que confundir con grupos de apoyo y grupos políticos.	General Organizations	x		x		x	
Sitios patrocinados por o dedicado a las empresas comerciales, asociaciones empresariales, grupos industriales o empresariales en general. Empresas de tecnología de la información están excluidos de esta categoría.	Business	x		x		x	
Periféricos de tecnología de la información y servicios, servicios de telefonía celular, televisión por cable / Internet proveedores.	Information and Computer Security	x		x		x	
Sitios de gobierno , oficinas o agencias de cualquier nivel de gobierno, con excepción de las fuerzas armadas.	Government and Legal Organizations	x		x		x	

FILTRADO WEB							
Categoría		Básico		Intermedio		Avanzado	
		P	B	P	B	P	B
Periféricos de tecnología de la información y servicios, servicios de telefonía celular, televisión por cable / Internet proveedores.	Information Technology	x		x		x	
Sitios web relacionados con fuerzas militares y armados, con exclusión de las organizaciones civiles.	Armed Forces	x		x		x	
Sitios de organizaciones que ofrecen servicios de alojamiento Web.	Web Hosting	x		x		x	
Sitios web en instituir medidas de seguridad como la autenticación, contraseñas, registro.	Secure Websites	x		x		x	
Los sitios que imitan a las aplicaciones de escritorio, tales como procesamiento de textos, hojas de cálculo y presentaciones de diapositivas.	Web-based Applications	x		x		x	

Fuente: Elaboración propia.

b. Diseño de VLAN

Nuestra propuesta implementa Vlans (Redes virtuales de área local), lo que permitirá segmentar y/o dividir lógicamente nuestra red.

Las Vlans nos ofrecerán lo siguiente.

- Mejor Administración de la Red
- Mejor rendimiento de la red, reduciendo los dominios de Broadcast
- Seguridad a la red
- Administración de los dispositivos conmutadores (Switches) de forma remota.
- Permite implementar estrategias QoS, etc.
- Nuestro switch de capa 3, será el servidor VTP donde se crea, administra o elimina las VLan's, y estas mismas se replican hacia los switches 4400 que serán nuestros clientes VTP donde ellos nopodrán crear, ni eliminar VLANS, solo accederán a las VLANS.

  A continuación se presenta el inventario de las VLan's creadas en la UNSM-T.

Tabla 5. Inventario de VLAN creadas en la UNSM-T

VLAN	Nombre VLAN	Dirección de Red/Mascara	Puerta de Enlace
0	Default	192.168.0.1/24	192.168.0.112
100	**Turismo-Lamas**	192.168.1.1/24	192.168.1.254
200	**FIAI**	192.168.2.1/24	192.168.2.254
300	**Administrativos**	192.168.3.1/24	192.168.3.254
400	**FISI**	192.168.4.1/24	192.168.4.254
500	**FMH**	192.168.5.1/24	192.168.5.254
600	**FICA**	192.168.6.1/24	192.168.6.254
666	**UTM**	172.16.100.1/24	172.16.1.2
700	**FCA**	192.168.7.1/24	192.168.7.254
800	**FCS**	192.168.8.1/24	192.168.8.254
900	**FCE**	192.168.9.1/24	192.168.9.254
999	**Servidores**	192.168.15.1/24	192.168.15.254
1000	**Idiomas**	192.168.10.1/24	192.168.10.254
1100	**FEH**	192.168.11.1/24	192.168.11.254
1200	**Infraestructura**	192.168.12.1/23	192.168.12.254

Fuente: Elaboración propia.

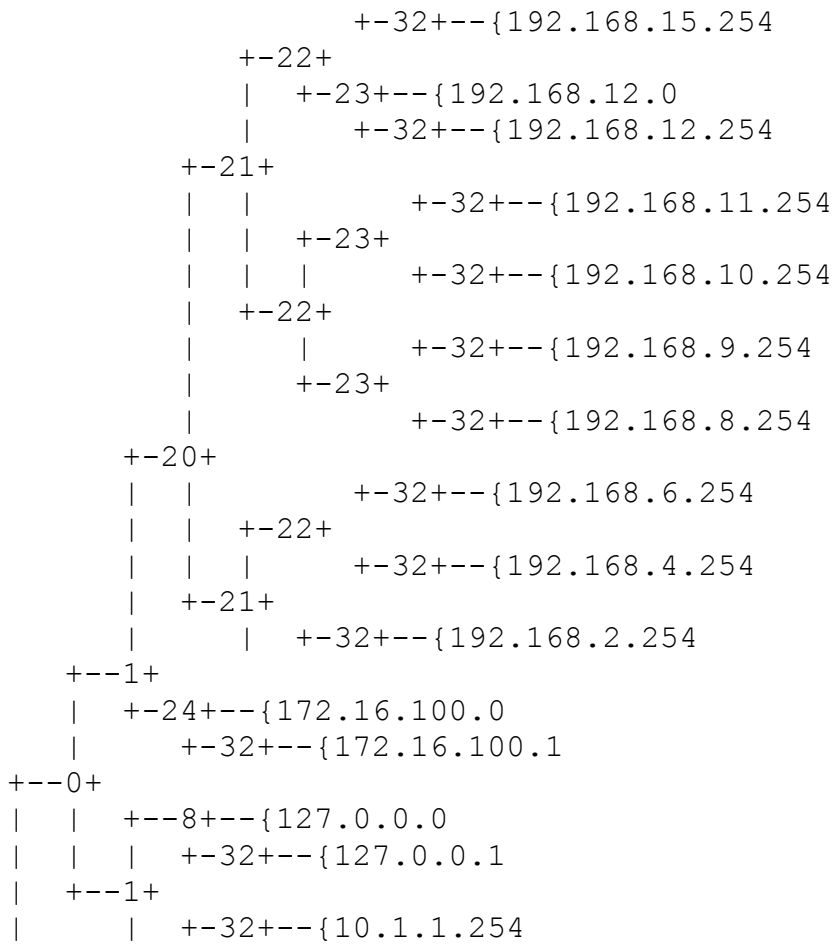
La creación de estas VLAN's implica la necesidad de crear rutas estáticas para el enrutamiento de paquetes, a fin de que el equipo pueda dirigir adecuadamente el tráfico, esas rutas estáticas, así como las VLANs son creadas en el 3COM 8800 y se muestran a continuación:

Tabla 6. VLANs creadas para segmentar la Red de Datos

Destination/Mask	Protocol	Pre	Cost	Nexthop	Interface
0.0.0.0/0	STATIC	60	0	172.16.100.2	Vlan-interface666
10.1.1.0/24	DIRECT	0	0	10.1.1.254	Vlan-interface1
10.1.1.254/32	DIRECT	0	0	127.0.0.1	InLoopBack0
127.0.0.0/8	DIRECT	0	0	127.0.0.1	InLoopBack0
127.0.0.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
172.16.100.0/24	DIRECT	0	0	172.16.100.1	Vlan-interface666
172.16.100.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
192.168.2.0/24	DIRECT	0	0	192.168.2.254	Vlan-interface200
192.168.2.254/32	DIRECT	0	0	127.0.0.1	InLoopBack0
192.168.4.0/24	DIRECT	0	0	192.168.4.254	Vlan-interface400
192.168.4.254/32	DIRECT	0	0	127.0.0.1	InLoopBack0
192.168.6.0/24	DIRECT	0	0	192.168.6.254	Vlan-interface600
192.168.6.254/32	DIRECT	0	0	127.0.0.1	InLoopBack0
192.168.8.0/24	DIRECT	0	0	192.168.8.254	Vlan-interface800
192.168.8.254/32	DIRECT	0	0	127.0.0.1	InLoopBack0
192.168.9.0/24	DIRECT	0	0	192.168.9.254	Vlan-interface900
192.168.9.254/32	DIRECT	0	0	127.0.0.1	InLoopBack0
192.168.10.0/24	DIRECT	0	0	192.168.10.254	Vlan-interface1000
192.168.10.254/32	DIRECT	0	0	127.0.0.1	InLoopBack0
192.168.11.0/24	DIRECT	0	0	192.168.11.254	Vlan-interface1100
192.168.11.254/32	DIRECT	0	0	127.0.0.1	InLoopBack0
192.168.12.0/23	DIRECT	0	0	192.168.12.254	Vlan-interface1200
192.168.12.254/32	DIRECT	0	0	127.0.0.1	InLoopBack0
192.168.15.0/24	DIRECT	0	0	192.168.15.254	Vlan-interface999
192.168.15.254/32	DIRECT	0	0	127.0.0.1	InLoopBack0

Fuente: Inventario de VLan’s del Switch Core.

A continuación se muestra la tabla de enrutamiento en formato de árbol de búsqueda, para su mejor entendimiento.



c. DHCP – Funcionalidad en Router Cisco 2800 Series.

DHCP o Dynamic Host Configuration Protocol, un protocolo que será instalado en el Router Cisco 2800 Series y que permitirá la configuración automática del protocolo TCP/IP de todos los clientes de dicha red. También nos permitirá obviar el tedioso trabajo de tener que configurar el protocolo TCP/IP cada vez que agregamos una nueva máquina a la red, por ejemplo, dirección IP, servidores DNS, gateway, WINS, etc.

Se podrá modificar la configuración de todos los equipos de la red con sólo modificar los datos del servidor.

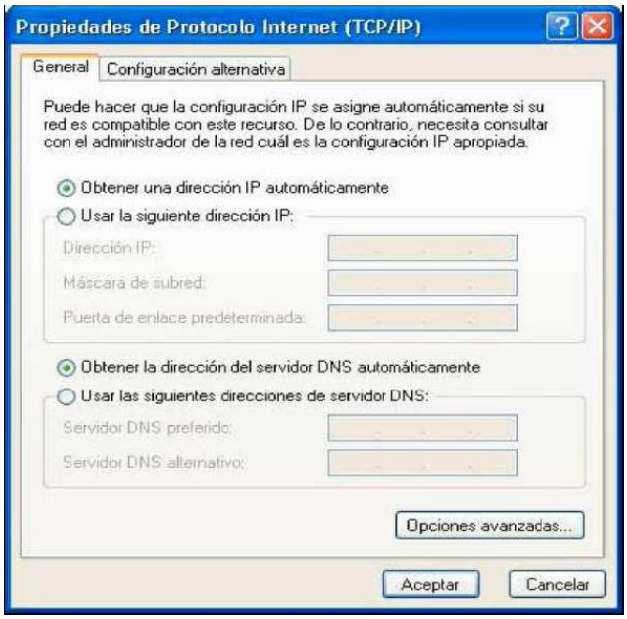


Figura 51. Propiedades TCP/IP

Después de configurar cambios en el Router Cisco 2800 Series, será necesario aplicar cambios en las propiedades de las tarjetas de red de cada dispositivo.

74. DISCUSIÓN DE LOS RESULTADOS

Tenemos lo siguiente:

- La velocidad o tasa de transferencia de datos en horas pico denotaba 25 Mbps frente a 5.5 Mbps como indicador actual de la red. Es decir que el ancho de banda disponible en horas críticas no era suficiente para soportar el flujo masivo de información en tiempo real (400 Mbps) por lo que la implementación de estrategias QoS ha permitido la mejora sustancial de la velocidad en la red LAN.

  Esto en parte se debe a la aplicada de Listas de Control de Acceso de la tabla 4, que aplica rigurosas políticas que impiden el uso inadecuado del ancho de banda disponible.

- Que las interrupciones o cortes de conexión fueron mermadas en un 82% gracias a los mecanismos balanceo de tráfico, identificación de paquetes, y por ende, su categorización en el uso de ancho de banda; estrategia que logró reducir el tiempo de los procesos Core en 90 minutos.

- El acceso a los servicios y recursos compartidos de la red se han visto reforzados como consecuencia de la configuración de tecnologías de seguridad emergentes, propias de la versión de los controladores de dominio actual (Windows Server 2008), detalles que no aplican tesis anteriores como propuesta de solución para aplicar controles ante los riesgos de seguridad. Estos nuevos mecanismos han permitido elevar el nivel de seguridad en un 95% mejoras que satisfacen las exigencias y lineamientos estratégicos de la empresa.

  Asimismo estas mejoras se ven reforzadas por el uso de un Firewall FORTINET 600C, logrando un nivel de seguridad superior.

- La nueva estructura lógica de la Red, predispone una estructura física más robusta permitiendo la escalabilidad de la LAN la cual permite soportar un crecimiento tecnológico.

75. CONCLUSIONES

a. El protocolo VTP (Virtual Trunking Protocol) es de gran ayuda para no tener que configurar las VLANs en todos los switches, simplemente se debe configurar las VLANs en el switch que esté en modo servidor, y el resto de switches debe estar en modo cliente.

   La proyección de crecimiento de la red de la UNSM-T es de 16% anual, donde actualmente se cuenta con aproximadamente entre 750 a 1500 terminales (dependiendo del periodo de clases). Se implementó y configuró la red para soportar este promedio de crecimiento sin afectar el rendimiento de la Lan, gracias a los lineamientos de la metodología adoptada. Con lo que es posible conectar otros switch de 48 puertos hacia el swicth Core y responder a la tasa de crecimiento, con una velocidad de 100/1000 Gbps en cada troncal.

   El uso de VLAN a nivel del switch core y la priorización del ancho de banda a nivel del dispositivo UTM utilizado ha permitido segmentar la red plana en varias redes lógicas separadas unas de otras, y además priorizar de acuerdo a la demanda el ancho de banda disponible para cada VLAN.

   Con ello concluimos que el objetivo de la segmentación y priorización del ancho de banda ha sido posible de ejcutar.

b. La velocidad o tasa de transferencia de datos está operando dentro de los rangos esperados, gracias a la implementación de técnicas de balanceo y priorización de tráfico con QoS, el cual se configuró en los dispositivos que consumen mayor ancho de banda (Pc's administrativos y alumnos),identificándose tipos de paquetes (Voz, Datos y Video) para reservar un ancho de banda de origen a destino donde los equipos detectan el tráfico de datos relevantes y lo gestionan con mayor prioridad (Video y Voz).

   Cabe anotar también que la configuración de un Firewall - físico, VLAN's, ACL's, DHCP, el uso de aplicativos emergentes propios del Windows

Server 2008 (File Screening Management, NetWork-Access Protection) ha propiciado la solución a la problemática de la perdida de información compartida en red, ofreciendo una administración de recursos más controlada y eficiente, mejorando al mismo tiempo la seguridad de la Red.

c. El resideño de la red, ha permitido mejorar el rendimiento de las misma, puesto que ha pasado de ser una red plana (es decir una sola red lógica y física para todos los equipos de cómputo disponibles en la universidad), con muchos problemas respecto del rendimiento de la misma y una difícil administración de los nodos disponibles, a ser una red segmentada (es decir una red física con varias redes lógicas segmentadas de acuerdo a la distribución física de los edificios de la universidad), permitiendo ello mejorar el rendimiento al segmentar no sólo físicamente la red, sino segmentar el dominio de colisión y dominio de broadcast, haciendo que sea una red más silenciosa y de mejor rendimiento.

   Se ha Implementado a nivel de piloto, mecanismos para autenticación de los accesos a servicios y recursos de red a través de roles y perfiles de usuario, como Active Directory, lográndose un mejor nivel de seguridad, dado que los filtros son más rigurosos gracias a las capas de seguridad que brinda. Asimismo se modificaron privilegios de usuarios en el Active Directory, para estar alineados al nuevo esquema de trabajo en red y uso de recursos.

76. RECOMENDACIONES

a. Establecer como política de administración, que solo las personas que administran y dan mantenimiento a la red tengan acceso a los equipos de interconexión de red, especialmente para la tarea más cotidiana que es el ingreso, salida o cambio de hosts, para que éste personal con el conocimiento claro de la distribución de VLANs, configure adecuadamente los puertos de los switches.

b. Configurar e implementar tecnología LACP (Agregados de Enlace) a nivel de Servidores – Switch, para mantener un esquema similar entre dispositivos intermedios. Logrando así ofrecer una mayor eficiencia en el balanceo y tráfico de carga de datos.

c. Implementar acciones de revisión física de la red, descartando equipos conectados sin autorización. Asimismo implementar políticas de conexión para equipos invitados o externos.

77. REFERENCIAS BIBLIOGRAFICAS

Andrew L. Russell (2013). *OSI: The Internet That Wasn't. How TCP/IP eclipsed the Open Systems Interconnection standards to become the global protocol for computer networking*. IEEE Spectrum. Recuperado de: http://spectrum.ieee.org/computing/networks/osi-the-internet-that-wasnt

Camposano, D y Zambrano, G. (2013). *Estudio del Ancho de Banda para el tráfico de Redes WAN de los ISP, con estudiantes de la Universidad Politécnica Salesiana Sede Guayaquil carrera Ingeniería de Sistemas, mediante la implementación de una página web.* (Ingeniería de Sistemas GYE - Tesis de Pregrado). Universidad Politécnica Salesiana. Guayaquil – Ecuador.

Cieza, D. (2007). *Efectos del Incremento del Ancho de Banda en las Pymes*. (Tesis para optar el grado de Magister en Administración con Mención en Marketing). Universidad Nacional Mayor de San Marcos. Lima – Perú.

Cisco. (2014, 15 de octubre). CCNA Exploration. Aspectos Básicos de Networkiing. Recuperado de www.netacad.com

Contreras, O y Contreras. N. (2010). *Modelo Matemático para la Predicción de Ancho de Banda. Primera Aproximación*. Artículo científico. Subgerencia de Administración y Operación de Redes – Ingeniería. Chile.

De Luz, S. (2014). *Análisis de la conexión Wi-Fi eduroam en la Universidad de Alcalá (UAH). (*Tesis para optar la Licenciatura en Ingeniería de Sistemas Computacionales). Universidad Alcalá de Henares. Alcalá de Henares – España.

Frez, J. (2011). *Estudio para el establecimiento de indicadores de calidad para el servicio de acceso a internet*. (Tesis para optar al grado de magister en ciencias mención computación). Universidad de Chile. Santiago de Chile – Chile.

Hernandez, J y otros. (2005). *Cálculo de ancho de banda necesario para una empresa.* Universidad Juárez Autónoma de Tabasco. Tabasco – México. 4(2), 1-10. Recuperado de

http://www.publicaciones.ujat.mx/publicaciones/revista_dacb/Acervo/v4n2OL/v4n2a1-ol/index.html

Morales, S. (2006). *Administración del ancho de banda de una WLAN.* (Tesis para optar la Licenciatura en Ingeniería de Sistemas Computacionales). Universidad de las Américas Puebla. Puebla – México.

Muñoz, C. (2013). *Diseño de una red de telecomunicaciones de banda ancha para la región tumbes.* (Tesis para optar el Título de Ingeniero de las Telecomunicaciones). Pontificia Universidad Católica del Perú. Lima – Perú.

Muñoz, J. (2003). *Desarrollo de métodos de medición para evaluar la calidad de servicio en el acceso a internet.* (Tesis para optar el título profesional de Ingeniero Electrónico). Universidad Nacional Mayor de San Marcos. Lima – Perú.

Serrano A. y Martinez E. (2003). *La brecha digital. Mitos y Realidades.* (1era Edición). Nueva Mexicali, Baja California, Mexico. Departamento Editorial Universitaria de la Universidad Autónoma de Baja California.

Villadangos, J. y Magaña E. (2009). *Garantía de calidad de servicio basada en la predicción del ancho de banda.* Artículo Científico. Universidad Pública de Navarra. Pamplona – España.

78. ANEXOS

Anexo I. Incremento de la cantidad de equipos de cómputo- UNSM-T

Año	Nro de Equipos	% Crecimiento Anual
2008	120	0
2009	140	17%
2010	180	29%
2011	409	127%
2012	522	28%
2013	612	17%
2014	767	25%
2015	856	12%

Anexo II. Encuesta

Medición de percepción de la seguridad de la red en el Universidad Nacional de San Martin- Tarapoto

Encuesta.

1.- ¿Alguna vez ha podido, de manera no intencional revisar archivos de usuarios de otras PCs?

si	No
81%	19%

2.- ¿Alguna vez han entrado en tu computador personal y han robado alguna información?

si	No
62%	38%

3. ¿Alguna vez se te ha perdido algún archivo cuando **lo has compartido a través de lared?**

si	No
74%	26%

4. ¿Estarías deacuerdo que se implementara políticas de seguridad para mejorar la seguridad de la red?

si	No
95%	5%

5. ¿Cómo considera usted que es la velocidad de transferencias de archivos y navegación por internet en horas punta?

Muy Malo	Malo	Regular	Buena	Excelente
		✓		

6. El contenido de restricciones y nivel de seguridad la red informática actual de la UNSM - T, lo considera.

Muy malo	**Malo**	**Regular**	**Bueno**	**Excelente**
		✓		