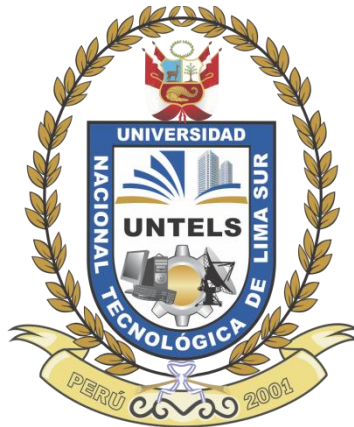


UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

**FACULTAD DE INGENIERÍA MECÁNICA, ELECTRÓNICA Y
AMBIENTAL**

**CARRERA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y
TELECOMUNICACIONES**



**“DISEÑO DE UNA RED LAN PARA MEJORAR LA SEGURIDAD,
DISPONIBILIDAD Y RENDIMIENTO DE LOS SERVICIOS UTILIZANDO
UN EQUIPAMIENTO HÍBRIDO CON TECNOLOGÍAS JUNIPER Y CISCO
PARA LA ENTIDAD FINANCIERA MI BANCO, SEDE SAN ISIDRO”**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

INCA TUEROCONZA, LILIANA

**Villa El Salvador
2016**

DEDICATORIA

“Agradecer a dios, a mis padres Eleuterio Inca y Eudosia Tuerconza quienes juntos y el esfuerzo constante han hecho posible realizarme como profesional, a mis hermanos Elvis y Edward por su apoyo y compañía durante toda mi vida, y a Diego Peralta por su apoyo incondicional”

AGRADECIMIENTO

Me gustaría agradecer en primer lugar a mi familia por haberme guiado a lo largo de estos años por el camino del bien.

Finalmente a todas aquellas personas, amigos de la vida y del trabajo, que han fomentado en mí el deseo de superación y anhelo de triunfo en la vida.

ÍNDICE

INTRODUCCIÓN.....	1
CAPITULO I	2
1. PLANTEAMIENTO DEL PROBLEMA.....	2
1.1. Descripción de la Realidad Problemática.....	2
1.2. Justificación del problema	3
1.3. Delimitación del proyecto.....	3
1.3.1. Delimitación teórica.....	3
1.3.2. Delimitación temporal	3
1.3.3. Delimitación espacial	4
1.4. Formulación del problema.....	4
1.4.1. Problema General	4
1.4.2. Problema Específico	4
1.5. Objetivos	4
1.5.1. Objetivo general.....	4
1.5.2. Objetivos específicos	5
CAPITULO II	6
2. MARCO TEÓRICO.....	6
2.1. Antecedentes de la investigación	6
2.2. Bases teóricas.....	7
2.2.1. Conceptos generales.....	7
2.2.2. Dispositivos de red.....	9
2.2.3. Ethernet.....	12
2.2.4. Dominios de colisión	13
2.2.5. Dominio de broadcast.....	13
2.2.6. Broadcast y Multicast.....	13
2.2.7. Modelo jerárquico CISCO	14
2.2.8. Red de área local virtual.....	18
2.2.9. Listas de control de acceso – ACL	28
2.2.10. LACP (Link Agreggation Control Protocol).....	29
2.3. Marco conceptual	30

CAPITULO III	36
3. DISEÑO, DESCRIPCIÓN DEL SISTEMA Y RESULTADOS	36
3.1. Metodología de recolección de datos.....	36
3.1.1. Métodos, técnicas e instrumentos de recolección de datos	36
3.1.2. Desarrollo del estudio de campo	36
3.1.3. Descripción Sede San isidro.....	38
3.1.4. Descripción Sede La Molina	53
3.1.5. Estado actual de los procesos de trabajo.....	55
3.2. Construcción, diseño de la herramienta/ sistema	64
3.2.1. Estudio y diseño	64
3.2.2. Materiales y equipos para el funcionamiento del sistema	71
3.2.3. Configuración de switches de Núcleo, Distribución y Accesos.....	74
3.3. Revisión y consolidación de resultados	85
3.3.1. Protocolo de pruebas.....	85
3.3.2. Estimación de resultados	90
CONCLUSIONES.....	93
RECOMENDACIONES	94
BIBLIOGRAFÍA.....	95
ANEXOS.....	96

LISTADO DE FIGURAS

Pág.

Figura N° 1: Comunicación Peer-to-Peer	9
Figura N° 2: Iconos de los dispositivos de red.....	10
Figura N° 3: Transmisiones simultáneas en un Switch.....	11
Figura N° 4: Capas de modelo jerárquico	15
Figura N° 5: Estructura de red definido por jerarquía.....	18
Figura N° 6: Vlan's y límites físicos.....	19
Figura N° 7: Vlan's en base a puertos.....	22
Figura N° 8: Vlan's en base a direcciones MAC	23
Figura N° 9: Filtrado de Tramas	27
Figura N° 10: Etiquetado de Tramas.....	28
Figura N° 11: Putty, opciones básicas de sesión.....	37
Figura N° 12: Software cliente; PuTTY	37
Figura N° 13: Diagrama de red actual de la Red de MI BANCO.....	39
Figura N° 14: Diagrama de red actual de Sede San Isidro.....	40
Figura N° 15: QSFP+ Direct Attach Copper Cables for EX Series Switches.....	41
Figura N° 16: Vista frontal del equipo EX4500.....	42
Figura N° 17: Vista frontal del equipo EX4200.....	43
Figura N° 18: Vista frontal del equipo EX2200-48P.....	46
Figura N° 19: Vista frontal del equipo EX2200-24P.....	46
Figura N° 20: Vista frontal del equipo WS-C2960S-48FPS-L de Cisco Systems.....	48
Figura N° 21: Vista frontal del equipo WS-C2960-48PST-S de Cisco Systems	48
Figura N° 22: Vista frontal del Switch EX3300-24T.....	50
Figura N° 23: Vista frontal del Controlador Wireless Juniper WLC800R	52
Figura N° 24: Vista frontal del Access Point Juniper, WLA321	53
Figura N° 25: Diagrama de sede La Molina	54
Figura N° 26: Conexión Core – Piso 1.....	56
Figura N° 27: Conexión Core – Gabinete 2.	57
Figura N° 28: Conexión Core –Surquillo, San Isidro y La Molina por fibra oscura.	57
Figura N° 29: Entorno Ringmaster de Mi Banco.....	58
Figura N° 30: licencia actual de los WLC 1- WLC 2	59
Figura N° 31: Entorno gráfico del Ringmaster.	61
Figura N° 32: Diagrama de red Inalámbrica de San Isidro.....	62
Figura N° 33: Distribución de los niveles de Jerarquía de la red en la Sede Surquillo.....	63
Figura N° 34: Mibanco Sede San Isidro ubicado en Av. Paseo de la Republica 3717	64
Figura N° 35: Jerarquía de la conexión.....	65
Figura N° 36: Mapa física de la ubicación de los Switches de Distribución y Acceso (pisos).....	67
Figura N° 37: Topología Física de la solución en la Sede San Isidro.....	68
Figura N° 38: Topología Lógica de la solución en la Sede San Isidro.	69

Figura N° 39: EX3300-48P Juniper.....	71
Figura N° 40: Cisco 3850-48P.....	72
Figura N° 41: Transceiver EX-SFP-10GE.....	72
Figura N° 42: Patch core de fibra óptica LC-LC MMF.....	72
Figura N° 43: Cable CAT 6 Panduit.....	73
Figura N° 44: Conectores RJ45 CAT 6.....	73
Figura N° 45: Cable SFP+direct attach copper.....	74
Figura N° 46: Estoboles + Pernos enjaulados.....	74
Figura N° 47: Conexión del Stackwise en los Switch Cisco 3850.....	78
Figura N° 48: Conexión de Virtual Chassis con cable DAC en anillos.....	79
Figura N° 49: Conexión de Switch Master y Switch Backup - (1).....	80
Figura N° 50: Conexión de Switch Master y Switch Backup - (2).....	81
Figura N° 51: Topología de red para BPDU Protection.....	82
Figura N° 52: Esquema de la descripción de interfaces del Port Security.....	83
Figura N° 53: Ruta del tráfico en la red LAN desde los puntos finales.....	91
Figura N° 54: Conmutación Switch Principal con Switch Backup.....	92

LISTADO DE TABLAS

Pág.

Tabla N° 1: Distribución de Switches Juniper en el Core de San Isidro.....	41
Tabla N° 2: Características técnicas del Switch EX4500 de Juniper Networks.	42
Tabla N° 3: Características técnicas del Switch EX4200 de Juniper Networks.	43
Tabla N° 4: Distribución de los Switches en el Sótano y los 9 Pisos de la sede San Isidro.	45
Tabla N° 5: Características técnicas del Switch EX2200-48P y Switch EX2200-24P de Juniper Networks.....	46
Tabla N° 6: Características técnicas del Switch WS-C2960S-48FPS-L de Cisco Systems.	48
Tabla N° 7: Características técnicas del Switch WS-C2960-48PST-S de Cisco Systems.	49
Tabla N° 8: Distribución de switches Juniper en los Gabinetes de San Isidro.	49
Tabla N° 9: Característica técnicas del Switch EX3300-24T de Juniper Networks	50
Tabla N° 10: Ringmaster, Software Cliente.....	51
Tabla N° 11: WLC (Wireless LAN Controller)	51
Tabla N° 12: Distribución de los Access Point.....	52
Tabla N° 13: Distribución de Switches Juniper en los Gabinetes de La Molina.	55
Tabla N° 14: Asignación de puertos para la interconexión entre Nivel de Core, Nivel de Distribución y Nivel de Acceso.....	70
Tabla N° 15: Servicios descritos por cada VLAN que pertenecen a gestión en producción actual en el cliente.	76
Tabla N° 16: Distribución de las direcciones IP de cada Switch de piso con la VLAN de teléfonos asociados.....	77

INTRODUCCIÓN

El presente trabajo de investigación lleva por título “Diseño de una red LAN para mejorar la seguridad, disponibilidad y rendimiento de los servicios utilizando un equipamiento híbrido con tecnologías Juniper y Cisco para la Entidad Financiera MI BANCO, sede San Isidro”, presentado por la bachiller LILIANA INCA TUEROCONZA para optar el título de Ingeniería Electrónica y Telecomunicaciones.

En Mi Banco sede de San Isidro actualmente se tienen instaladas equipos de red trabajando como Switch-Core, Switches de piso, Switches de gabinete, infraestructura de red, control de acceso y plataforma de gestión de red (Junos Space).

Se diseñara una topología de red utilizando equipamiento Juniper y Cisco de tal manera mejorar la red LAN brindando disponibilidad, rendimiento y seguridad; ya que actualmente presentan problemas en el servicio en datos, voz, vídeo, etc.

La estructura que hemos seguido en este proyecto se compone de 3 capítulos. El primer capítulo comprende el planteamiento del problema, el segundo capítulo el desarrollo del marco teórico y el tercer capítulo corresponde al desarrollo del proyecto.

El autor.

CAPITULO I

1. PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la Realidad Problemática

Mi Banco, es un banco peruano en el sistema financiero que centraliza sus operaciones en la micro y pequeña empresa, su mayor accionista es la empresa financiera Edyficar y ahora son el nuevo Mi Banco. Tiene más de 280 sucursales en todo el país, con más de 40 años de experiencia en el sector. Mi Banco sede San Isidro manifiesta problemática en cuanto a la comunicación y servicio de datos. La realidad problemática de la empresa son los siguientes:

- Switches en cascada, sin disponibilidad al 100% en el servicio de datos; es decir sin respaldo.
- Puertos de red de cada switch encendidos, libres, sin ninguna seguridad; libre maniobra de terceros en adicionar hardware que podrían afectar el servicio en general.
- No se aprovechan las características de los equipamientos que tienen o podrían utilizarse.

- Los equipos no están instalados en los ambientes adecuados; es decir están fuera de un gabinete sin la temperatura adecuada.

1.2. Justificación del problema

El diseño no requiere adquirir equipos dedicados excesivamente costosos, por lo que se puede ofrecer una mejor relación costo, beneficio y seguridad.

La propuesta de diseño y mejora va a permitir una comunicación óptima en la sede principal, para la transmisión y recepción de los servicios de datos dentro de los parámetros de red establecidos con seguridad y confiabilidad, de la cual se hará uso de una red ya existente de un proveedor de servicios.

1.3. Delimitación del proyecto

1.3.1. Delimitación teórica

La fuente de información teórica que se utilizó para el presente diseño proviene del levantamiento de información de la red de Mi Banco, datasheet de los equipos Juniper y Cisco, con la finalidad de proporcionar el cumplimiento de los objetivos en las siguientes categorías:

- a) Efectividad y eficiencia en las operaciones.
- b) Confiabilidad de la información de la red del cliente.
- c) Cumplimiento de los estándares aplicados en la red de comunicaciones.

1.3.2. Delimitación temporal

El diseño se elaboró en el periodo Mayo 2016-Agosto 2016

1.3.3. Delimitación espacial

La presente propuesta de diseño se llevará a cabo en la Entidad Financiera Mi Banco sede San Isidro.

1.4. Formulación del problema

1.4.1. Problema General

¿Es posible diseñar una red LAN para mejorar la seguridad, disponibilidad y rendimiento de los servicios de la entidad financiera Mi Banco?

1.4.2. Problema Específico

- a) ¿Cuáles serán los métodos de recolección de datos para el inicio del diseño de una red LAN?
- b) ¿Cómo diseñar una red LAN con alta disponibilidad y óptima velocidad de transmisión utilizando equipamiento híbrido Juniper y Cisco?
- c) ¿Cómo priorizar la seguridad de los servicios utilizados?
- d) ¿Cómo comprobar el funcionamiento del diseño de red?

1.5. Objetivos

1.5.1. Objetivo general

Con el diseño y simulación con los equipos que se utilizarán para la implementación se demostrará que podemos optimizar los servicios de la red LAN.

1.5.2. Objetivos específicos

- a)** Analizar y diagnosticar el estado de servicio y la topología de la red LAN existente.
- b)** Diseñar una red de datos con Switches de la marca Juniper y Cisco utilizando el protocolo LACP y haciendo uso de las características del Virtual Chassis (Junos) o Ethernet Channel (iOS).
- c)** Integrar métodos de seguridad para evitar caídas en el servicio haciendo uso de las características de seguridad que ofrece los equipos Juniper y Cisco.
- d)** Verificar el funcionamiento y operatividad de la red mediante la aplicación de un protocolo de pruebas.

CAPITULO II

2. MARCO TEÓRICO

2.1. Antecedentes de la investigación

En la tesis “Proyecto de Interconexión de Agencias Financieras Chiclayo-Tumán” realizada por la autora: Cotrina Orrego María Cecilia. Abordo, el análisis y diseño de 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. (Cotrina Orrego María Cecilia 2005).

En la tesis “Diseño de Red Estructurada de Datos con Vlan’s aplicado en la

Municipalidad Distrital de Puerto Eten”, realizada por la autor: Gonzales Vargas, Elmer. Abordo, el 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. (Gonzales Vargas, Elmer 2003).

2.2. Bases teóricas

2.2.1. Conceptos generales

Modelo OSI (Open Systems Interconnection)

OSI (1984): Es un modelo descriptivo de siete capas definido por ISO (International Organization for Standardization), que asegura compatibilidad e interoperabilidad entre diversas tecnologías de red producidas por diferentes compañías lo que permite trabajar de manera independiente sobre funciones de red separadas y por ende disminuir su complejidad y acelerar su evolución.

Este modelo está formado por siete capas cada una de las cuales realiza funciones diferentes que son:

- i. **Capa física:** Conectores, medio de transmisión, etc.
- ii. **Capa de enlace de datos:** Utiliza las direcciones MAC para acceder a las estaciones finales, notifica errores pero no los corrige, etc.

- iii. **Capa de red:** Determina el mejor camino, utilizando direccionamiento lógico (IP).
- iv. **Capa de transporte:** Provee una confiable o no confiable entrega de datos, re-ensambla los segmentos que llegan en desorden, etc.
- v. **Capa de sesión:** Establece, maneja y termina sesiones entre aplicaciones, asigna puertos lógicos, etc.
- vi. **Capa de presentación:** Traduce entre varios formatos de datos, encriptamiento, comprensión, etc.
- vii. **Capa de aplicación:** Provee protocolos y software al servicio del usuario (WEB, correo electrónico, etc.)

Para que los datos viajen desde un origen a su destino, cada capa del modelo OSI en el origen debe comunicarse con su respectiva capa en el destino. Esta comunicación es conocida como peer-to-peer. Durante este proceso, los protocolos de cada capa intercambian información denominada Protocol Data Unit (PDUs).

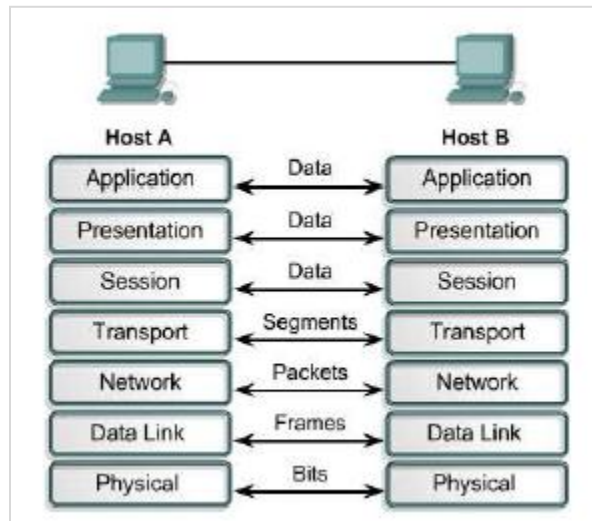


Figura N° 1: Comunicación Peer-to-Peer

Fuente: Slideplayer “TCP/IP vs OSI. Redes 2 Modelo OSI”.

2.2.2. Dispositivos de red

William Stallings (2000). Señala que existen dos clasificaciones, la primera clasificación son los dispositivos de usuario final, como por ejemplo computadoras, impresoras, scanners y otros dispositivos que provean servicios directamente al usuario.

Estos dispositivos son conectados físicamente a la red usando una Network Interface Card (NIC) que tiene su propio código o dirección MAC. La segunda clasificación son los dispositivos de red.

Los dispositivos de red proveen la comunicación entre dispositivos de usuario final, como por ejemplo:

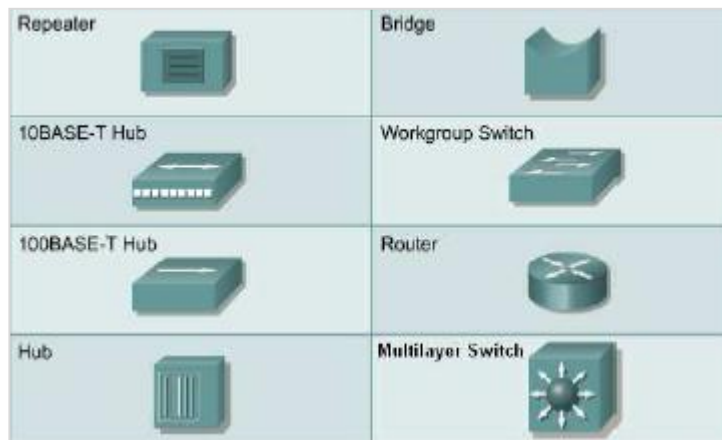


Figura N° 2: Iconos de los dispositivos de red

Fuente: Cisco Systems, learning Netacad.

2.2.2.1. Switch

Andrew S. Tanenbaum-4ta. Ed. (2003). Menciona que es un dispositivo de capa 2 y puede ser referido como un bridge multipuerto. Los switches toman las decisiones de envío basadas en las direcciones MAC origen que se encuentran en las tramas que ingresan al switch, luego esta información es ingresada dentro de la tabla de conmutación que es almacenada en la MAC. Los switches crean un circuito virtual entre dos dispositivos conectados que quieren comunicarse. Cuando este circuito virtual ha sido creado, un camino de comunicación dedicado es establecido entre los dos dispositivos. Esto crea un ambiente libre implica de colisiones entre el origen y el origen lo cual implica la máxima utilización del ancho de banda disponible.

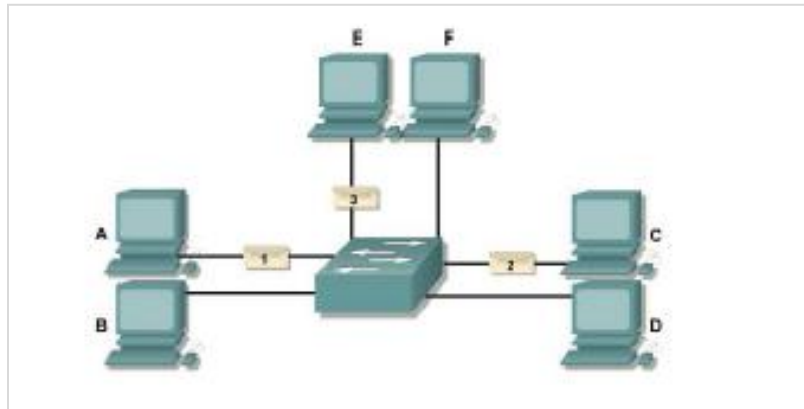


Figura N° 3: Transmisiones simultáneas en un Switch

Fuente: Cisco Systems, learning Netacad.

Cada puerto del switch representa un solo dominio de colisión lo cual se conoce como micro segmentación. La desventaja de todos los dispositivos de capa 2, es que ellos envían tramas broadcast a todos los dispositivos conectados a sus puertos.

2.2.2.2. Switch Multilayer

Un switch multilayer es la combinación de la conmutación tradicional de capa 2 con la operación de enrutamiento de capa 3 en un solo dispositivo, mediante acciones de hardware de alta velocidad. En tanto que un router el enrutamiento lo realiza mediante técnicas de software lentas. Este switch se fundamenta en circuitos del tipo ASIC.

Los switches multilayer son las rápidos y baratos que los routers. Aunque algunos switches multilayer carecen de modularidad y flexibilidad que usualmente tienen asociados los routers.

En la actualidad existen switches que pueden manejar información relacionada desde la capa 2 (enlace de datos) hasta capa 7 (aplicación) del modelo OSI.

2.2.3. Ethernet

Ethernet o su estándar equivalente IEEE 802.3, es básicamente una tecnología de transmisión broadcast, donde los dispositivos como computadoras, impresoras, servidores, etc.; se comunican sobre un medio de transmisión compartido, lo que quiere decir que ellos se encuentran en una continua competencia por el ancho de banda disponible. Por lo tanto, las colisiones son una natural ocurrencia en redes Ethernet y pueden llegar a ser un gran problema.

La entrega de tramas de datos Ethernet es de naturaleza broadcast. Ethernet usa el método CSMA/CD (acceso múltiple con censado de portadora y detección de colisión), que le permite a una sola estación transmitir, y puede soportar altas tasas de transmisión, como: Ethernet: 1000 Mbps y 10-Gigabit Ethernet: 10,000 Mbps.

El desempeño de un medio compartido Ethernet/802.3 puede ser negativamente afectado por factores como: las aplicaciones multimedia con alta demanda de ancho de banda tales como video e Internet, que junto con la naturaleza broadcast de Ethernet, pueden crear congestión en la red; y la latencia normal que adquieren las tramas por viajar a través de los medios de red, atravesar dispositivos de red y los propios retardos de las NICs.

2.2.4. Dominios de colisión

En un grupo de dispositivos conectados al mismo medio físico, es decir si dos dispositivos acceden al mismo tiempo al medio, entonces esto resulta en una colisión. Este es un dominio de capa 1.

2.2.5. Dominio de broadcast

Es un grupo de dispositivos sobre la red que reciben mensajes de broadcast. Este es un dominio de capa 2.

2.2.6. Broadcast y Multicast

Para comunicarse con todos los dominios de colisión, los protocolos usan tramas broadcast y multicast en la capa 2 del modelo OSI. Por lo tanto si un nodo necesita comunicarse con todos los host en la red, este envía una trama broadcast con una dirección MAC de destino 0xFFFFFFFFFFFF.

Esta es una dirección a la cual todas las tarjetas NIC deben responder. La acumulación de tráfico broadcast y multicast de cada dispositivo de la red es referido como: radiación de broadcast. Cuya circulación puede saturar la red, es decir que no hay ancho de banda disponible para aplicaciones de datos, resultando en la caída de estas conexiones, situación conocida como una tormenta de broadcast.

2.2.6.1. Causas de broadcast y multicast

Existen varias fuentes de broadcast y multicast en redes IP, estas pueden ser; las estaciones de trabajo, los routers, las aplicaciones multicast, el protocolo DHCP, etc., las estaciones de trabajo envían

broadcast de pedidos ARP (protocolo de resolución de direcciones), cada vez que ellos necesitan localizar una dirección MAC que no está en su tabla ARP. Las tormentas de broadcast pueden ser causadas por el pedido de información de un dispositivo dentro de una red que ha crecido mucho. Las aplicaciones multicast, particularmente las aplicaciones de paquetes de video pueden generar una cadena de siete megabytes de datos multicast, que en una red conmutada podría ser enviada a cada segmento, resultando en una severa congestión.

Otra fuente generadora de broadcast es el protocolo DHCP cuando un cliente DHCP usa un pedido de broadcast para localizar el servidor DHCP. Además estos clientes por lo general repiten este pedido después de un relativo corto "timeout", posiblemente debido a una respuesta lenta del servidor, lo que producen las conocidas tormentas de broadcast; que a su vez producen retardos anormales de otros tráficos cliente / servidor. Los cuales también pueden empezar a retransmitir.

2.2.7. Modelo jerárquico CISCO

Consta de tres capas:

- Capa Núcleo: Backbone
- Capa de Distribución: Routing
- Capa de Acceso: Switching

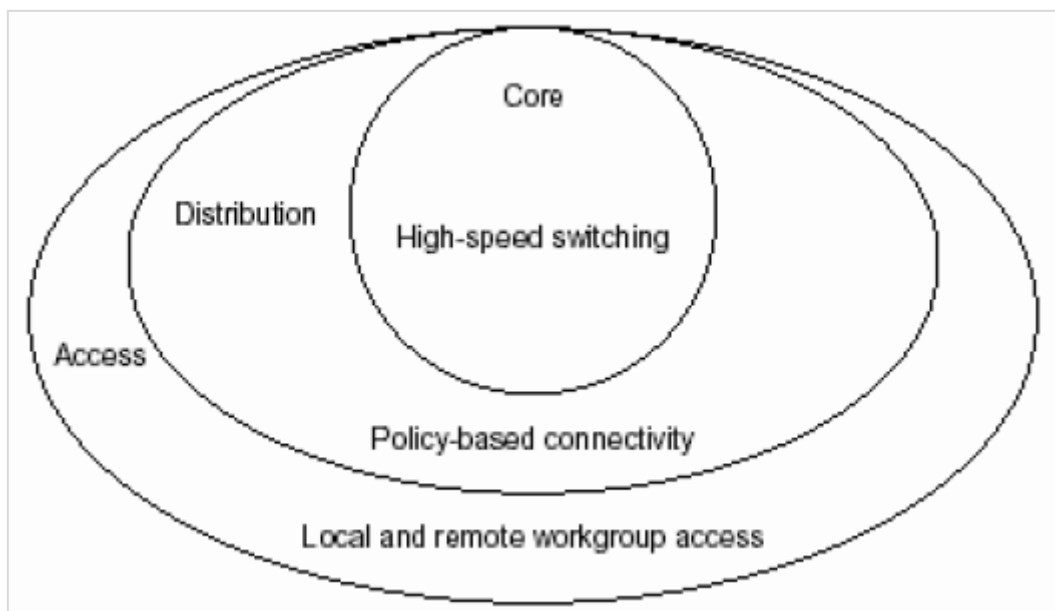


Figura N° 4: Capas de modelo jerárquico

Fuente: Nicanet Profesional “Diseño de Redes, Modelo Jerárquico”.

2.2.7.1. Capa Núcleo

Es el backbone de conmutación de alta velocidad que debe ser diseñado para conmutar paquetes lo mas rápido posible, es decir es responsable del transporte de grandes cantidades de tráfico en forma confiable y rápida, por lo tanto la preocupación de esta capa es la velocidad y latencia. Es importante considerar, lo que no debemos hacer en esta capa:

- No realizar ningún tipo de manipulación de paquetes, tal como usar listas de control de acceso, enrutamiento entre redes de área local virtuales (VLAN) o filtro de paquetes, lo cual reducirá el tráfico.
- No soporta accesos de grupos de trabajo.

- Evitar expandir el núcleo o Core usando la red crece. Si el desempeño es un problema en el Core, son preferibles las actualizaciones en lugar de las expansiones.

2.2.7.2. Capa de distribución

Es el punto de comunicación entre la capa de acceso y el Core. Las principales funciones de la capa de distribución son el proveer enrutamiento, filtros, accesos WAN y determinar como los paquetes pueden acceder al Core si es necesario.

La capa de distribución es donde se implementan las políticas para la red. Existen algunas acciones que generalmente deben hacerse en esta capa:

- Enrutamiento
- Implementación de listas de control de acceso o filtro de paquetes.
- Implementación de seguridad y políticas de red, incluyendo traslado de direcciones y firewalls.
- Calidad de servicio, en base a las políticas definidas.
- Redistribución entre protocolos de enrutamiento incluyendo rutas estáticas.
- Enrutamiento entre Vlan's y otras funciones que soportan los grupos de trabajo.
- Definición de dominios de broadcast y multicast.
- Posible punto para acceso remoto.

- Traslado de medios de comunicación.

2.2.7.3. Capa de acceso

La capa de acceso es el punto en el cual los usuarios finales son conectados a la red. Esta capa puede también usar listas de acceso o filtros para optimizar las necesidades de un grupo particular de usuarios deben estar disponibles localmente. Esta son algunas de las funciones que incluye esta capa:

- Continúa el control de acceso y políticas (desde capa de distribución)
- Creación de dominios de colisión separados (micro-segmentación)
- Conectividad de los grupos de trabajo dentro de la capa de distribución.
- Habilitar filtros de direcciones MAC.
- También es posible tener acceso a grupos de trabajo remotos.
- Presta servicios de asignación de Vlan's a nivel de capa 2 del modelo OSI.

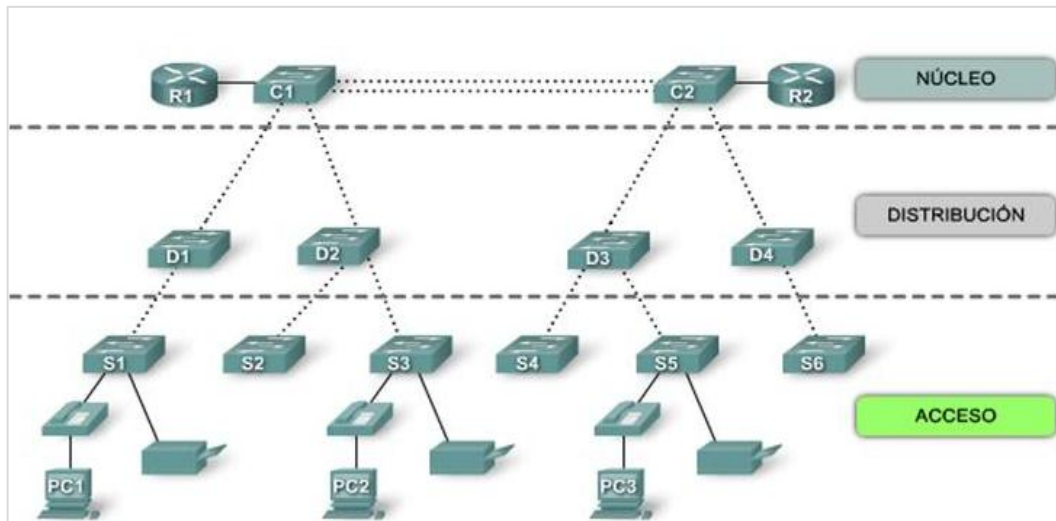


Figura N° 5: Estructura de red definido por jerarquía

Fuente: Emaze “Arquitectura de redes”.

2.2.8. Red de área local virtual

Una VLAN (red de área local virtual) es una agrupación lógica de dispositivos o servicios de red, en base a funciones, departamentos, equipos de trabajo o aplicaciones, sin considerar la localización física o conexiones de red.

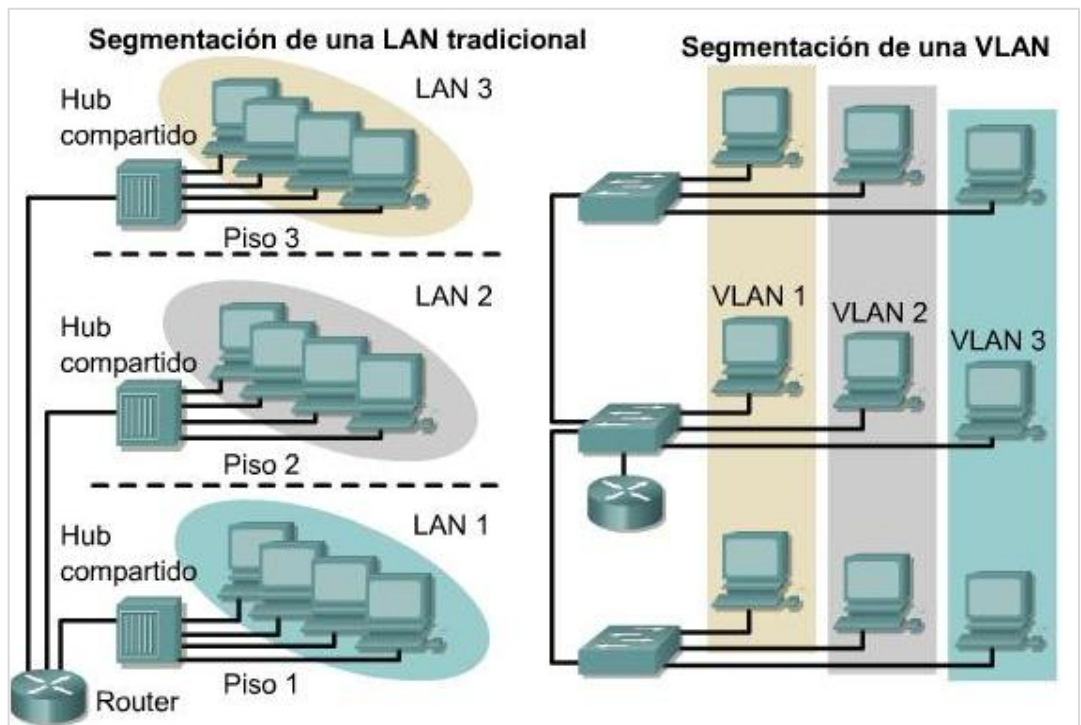


Figura N° 6: Vlan's y límites físicos

Fuente: Cisco Systems, "Introduccion a las VLANs".

La función de las Vlan's es una segmentación lógica de la red en diferentes dominios de broadcast, es decir que los paquetes son solamente conmutados entre puertos que han sido asignados a la misma VLAN.

Así como solo los routers proveen conectividad entre diferentes segmentos LAN, también solo los routers o equipos que operen en la capa 3 del modelo OSI, proveen conectividad entre diferentes segmentos VLAN. Los routers en topologías VLAN proveen filtrado de broadcast, seguridad y administración del flujo de tráfico.

2.2.8.1. Ventajas de las Vlan's

- **Incrementan el desempeño de la red** agrupando estaciones de trabajo, recursos y servidores según su función, sin importar si ellos se encuentran en el mismo segmento físico LAN. (Mejor desempeño, facilidad de administración).
- **Facilidad en la administración** de adición, movimiento y cambio de estaciones de trabajo en la red. (Flexibilidad).
- **Mejoran la seguridad de la red**, porque solamente las estaciones de trabajo que pertenezcan a la misma VLAN podrán comunicarse directamente (sin enrutamiento).
- **Incrementan el número de dominios de broadcast** mientras estos decrecen en su tamaño. (Mejor desempeño).
- **Facilitan el control de flujo de tráfico**, porque permiten controlar la cantidad y tamaño de los dominios de broadcast, debido a que estos por defecto son filtrados desde todos los puertos que no son miembros de la misma VLAN en un Switch. (Mejor desempeño).
- La configuración o reconfiguración de Vlan's se realiza a través de software, por lo tanto esto no requiere de movimientos o conexiones físicas de los equipos de red. (Facilidad de administración).

Las Vlan's proveen flexibilidad, escalabilidad, seguridad, facilidad de administración y mejor desempeño de la red.

2.2.8.2. Características de la Vlan's

a) VLAN de rango normal

- Para redes de pequeñas y medianas empresas.
- ID de VLAN entre 1 y 1005.
- ID de 1002 a 1005 se reservan para las VLAN Token Ring y FDDI, estas VLAN se crean automáticamente y no se pueden eliminar. Las configuraciones se almacenan en la vlan.dat, el cual se encuentra en la memoria flash del switch VTP, solo puede asimilar VLAN de rango normal.

b) VLAN de rango extendido

- Se diseñan para proveedores de servicios.
- 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.

2.2.8.3. Tipo de VLAN

a) VLAN de nivel 1, (también denominada VLAN basada en puerto) define una red virtual según los puertos de conexión del conmutador, cuyas ventajas son:

- Facilidad de movimientos y cambios.
- Micro segmentación y reducción de dominio de broadcast.

- Multiprotocolo: la definición de la VLAN es independiente del o los protocolos utilizados, no existen limitaciones en cuando a los protocolos utilizados, incluso permitiendo el uso de protocolos dinámicos.

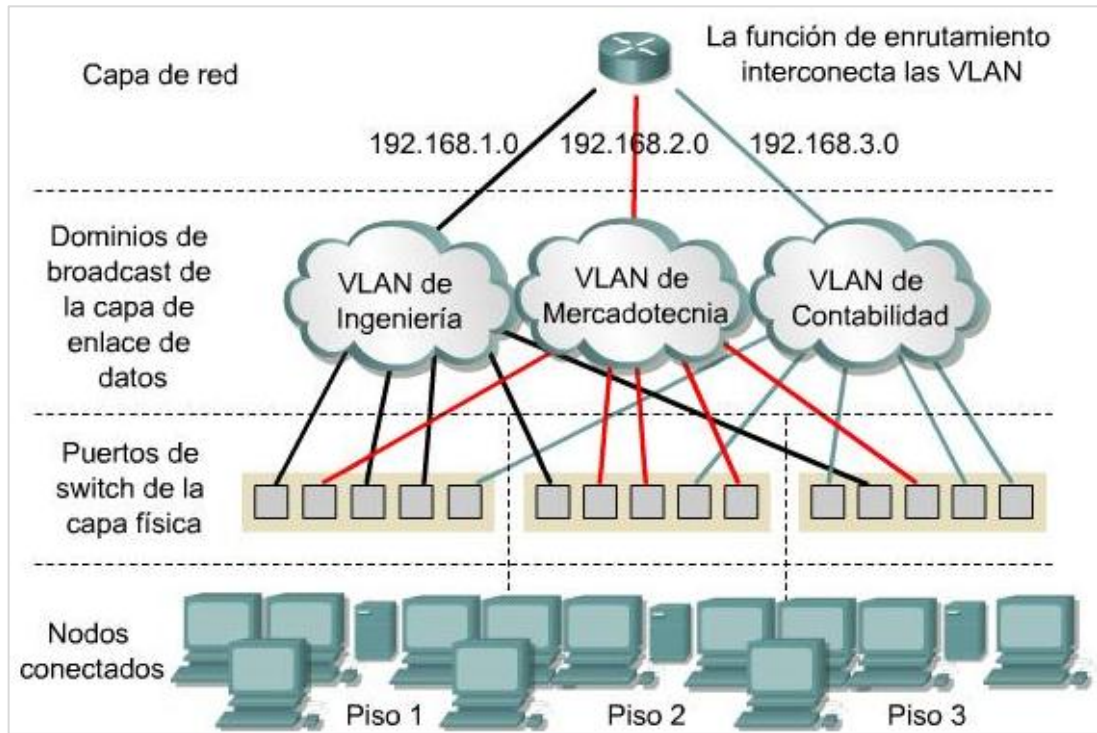


Figura N° 7: Vlan's en base a puertos.

Fuente: Cisco Systems, learning Netacad.

b) VLAN de nivel 2 (Denominada VLAN en base a direcciones MAC)

Operan agrupados estaciones finales a una VLAN en base a sus direcciones MAC. La forma como se realiza la asignación de usuarios a una VLAN es utilizando un servidor de políticas de administración de Vlan's (VMPS), para que maneje la base de datos de todas las direcciones MAC; de tal forma que cuando un usuario se conecte a

un puerto de un switch, este último, consulte al servidor a que VLAN corresponde este dispositivo, de acuerdo a su dirección MAC.

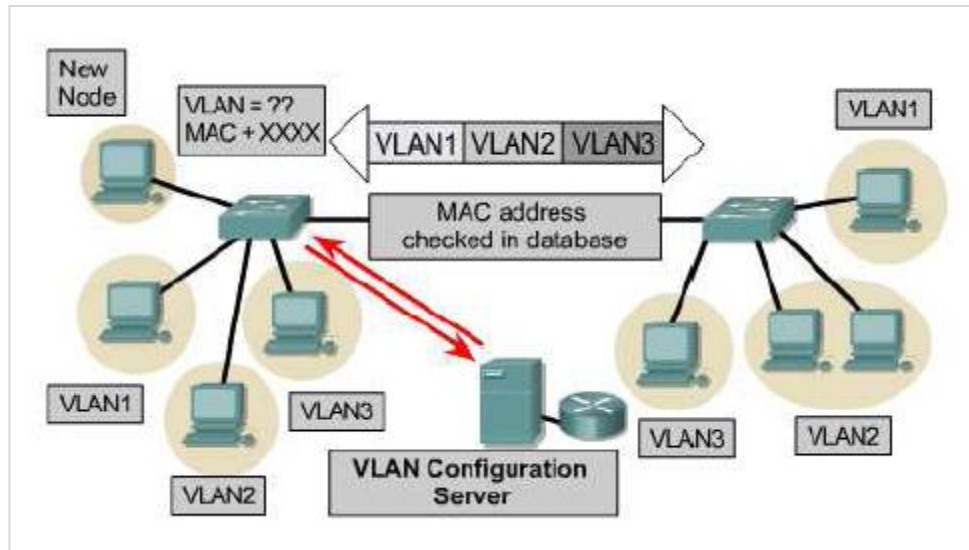


Figura N° 8: Vlan's en base a direcciones MAC

Fuente: Cisco Systems, learning Netacad.

También permite a los administradores de red mover una estación de trabajo a una localización física distinta en la red y mantener su pertenencia a la VLAN. Por lo tanto las Vlan's basadas en MAC prestan su mayor servicio de movilidad y seguridad a nivel de computadoras portátiles.

La principal desventaja, es que inicialmente se necesita recopilar la información de las direcciones MAC de todas las estaciones de trabajo de la red, para construir la base de datos que necesita el servidor de políticas.

2.2.8.4. Estándar

Las VLAN están definidas por el estándar:

802.1Q: El protocolo IEEE 802.1Q fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet.

2.2.8.5. Etiquetado de la trama 802.1Q

La norma IEEE 802.1Q identifica el mecanismo de etiquetado de trama de capa 2. El protocolo 802.Q interconecta switches, routers y servidores. Solo los puertos FasEthernet y GigabitEthernet soporta el enlace troncal con el etiquetado 802.1Q (también conocido como Dot1q). Gracias a este protocolo los switches reconocen la existencia de Vlan's a través del etiquetado de trama, reconociendo el número de VLAN independientemente del nombre que estas VLAN posean en cada switch.

- Los switch solo utilizan la información del encabezado de trama para enviar paquetes. El encabezado no contiene la información que indique a que VLAN pertenece la trama.
- Cuando las tramas de Ethernet se ubican en un enlace troncal, necesitan información adicional sobre las VLAN a las que pertenecen.
- Esto se logra por medio de la utilización del encabezado de encapsulación 802.1Q.

- Este encabezado agrega una etiqueta a la trama de Ethernet original y especifica la VLAN a la que pertenece la trama.

2.2.8.6. Estándares Integrados

- IEEE 802.1Q: Es un estándar que proporciona priorización de tráfico y filtrado multicast dinámico. Esencialmente, proporciona un mecanismo para implementar calidad de servicio (QoS) a nivel de MAC (Media Access Control). 802.1Q está integrado en los estándares IEEE 802.1D y 802.1Q.
- IEEE 802.10: El protocolo Inter-Switch de Cisco (ISL) para Vlan's en Ethernet y tecnologías similares del LAN fue basado en IEEE 802.10; en este uso 802.10 ha sido substituido en gran parte por IEEE 802.1Q.
- IEEE 802.1D; Las Vlan's (redes virtuales) no son parte de 802.1D, sino de IEEE 802.1Q.

2.2.8.7. Tipos de puertos

Las VLAN utilizan puertos no seriales, es decir únicamente Ethernet, FastEthernet, GigabitEthernet.

2.2.8.8. Enlaces troncales VLAN

Una troncal es una conexión física y lógica entre dos switches, entre un switch y un router, o entre un switch y un servidor (con una NIC especial que soporte trunking), a través del cual el tráfico de red viaja. Generalmente es un enlace punto a punto de 100 o 1000 Mbps. Es decir los puertos

FastEthernet de un switch son configurable porque pueden funcionar para enlaces de acceso o enlaces troncales.

El propósito de las troncales es evitar poner un enlace por cada VLAN. Esta es una simple forma de implementar la comunicación de Vlan's entre switches, pero esta no es escalable. Es importante entender que un enlace troncal no pertenece a ninguna VLAN específica. Simplemente es un conducto para Vlan's entre switches y routers.

Las troncales permiten convertir a un simple puerto, en parte de múltiples Vlan's al mismo tiempo. Lo cual es una verdadera ventaja, por ejemplo, actualmente se puede configurar para tener un servidor en varios dominios de broadcast simultáneamente, lo que quiere decir que usuarios de diferentes dominios de broadcast no necesitarán cruzar un dispositivo de capa 3 (router) para acceder al mismo servidor.

a) Trunking con filtrado de tramas

Las tablas de filtrado son creadas por cada switch, asociando cada dirección física con la VLAN a la que pertenece. Los switches comparten estas tablas a través del backbone. Por lo tanto, cuando llega una trama a un switch, las tablas de conmutación en los dos extremos de la troncal son usadas para realizar las decisiones de envío basadas en las direcciones MAC de destino de las tramas.

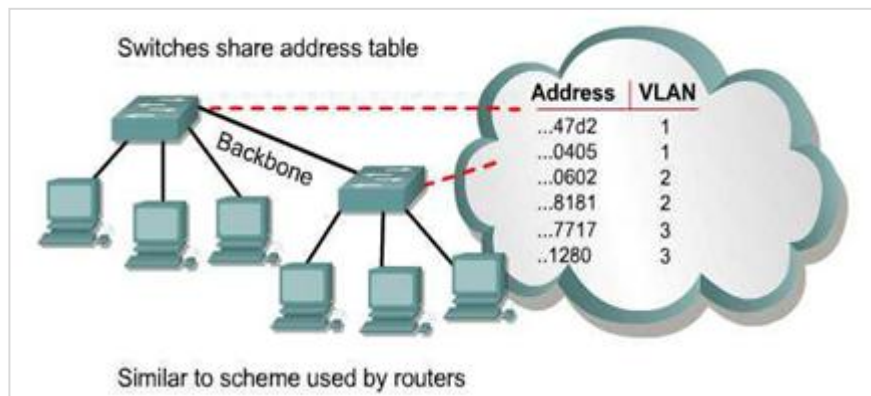


Figura N° 9: Filtrado de Tramas

Fuente: Cisco Systems, learning Netacad.

b) Trunking con etiquetado de tramas

Este método tiene asociado un identificador para cada VLAN, algunas personas se refieren a esto como el “VLAN ID” o “color”. Las tramas procedentes de los usuarios, antes de ser enviadas a través del enlace troncal o backbone, se etiquetan con el identificador correspondiente a la VLAN a la que pertenecen.

Este identificador es entendido y examinado por cada switch antes de cualquier broadcast o transmisión a otros switches, routers o estaciones de trabajo. Una vez que la trama va a abandonar el backbone, entonces el switch elimina el identificador antes de ser enviada a la estación final.

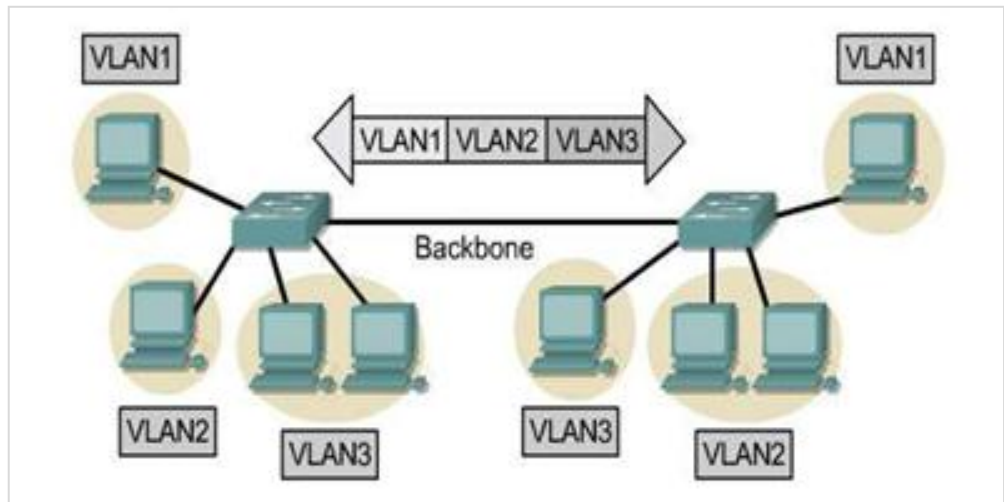


Figura N° 10: Etiquetado de Tramas

Fuente: Cisco Systems, learning Netacad.

Los protocolos de trunking que usan etiquetamiento, consiguen la entrega de tramas en forma más rápida y hacen su manejo más fácil.

2.2.9. Listas de control de acceso – ACL

Las listas de control de acceso (ACL / Access Control List) incluyen una descripción de los usuarios y grupos de usuarios con diferentes permisos sobre los archivos y carpetas de un volumen NTFS (New Technology File System).

Aparecer en la lista ACL significa tener derecho de acceso sobre el archivo o carpeta. El tipo de permiso definido en la entrada de un usuario o grupo de usuarios especifica el nivel de privilegio sobre el objeto (lectura, escritura, etc.).

Cada vez que un usuario accede a un archivo o carpeta se verifica si el usuario o el grupo de usuarios al que pertenece tienen al menos una entrada en la lista ACL del objeto. De no ser así, el sistema le niega el derecho sobre el objeto; en cambio, si posee uno o más entradas, el usuario podrá acceder al objeto con los privilegios especificados por los permisos asociados a las entradas.

2.2.10. LACP (Link Aggregation Control Protocol)

El Protocolo de Agregación de Enlaces de Control – LACP, es un protocolo definido en el estándar 802.1ad y que puede ser implementado en los switches. LACP permite agrupar puertos por su velocidad, modo dúplex, trocales, VLAN, sumando la velocidad nominal de cada puerto físico y así obtener un único enlace troncal de alta velocidad.

La ventaja principal de LACP es que posee el ancho de banda de red de todos sus adaptadores en una sola presencia en la red. Si un adaptador tiene una anomalía, el tráfico de la red se envía al siguiente adaptador disponible de forma automática, sin interrumpir las conexiones del usuario existentes. El adaptador se devuelve automáticamente al servicio de Agregación de enlaces cuando se recupera y esto nos proporciona:

Alta disponibilidad (si unimos 3 enlaces y cae uno de ellos, el enlace “lógico” seguirá siendo operativo)

Balanceo de carga (en base al algoritmo de balanceo elegido, los datos se repartirán entre los enlaces reales)

Mayor ancho de banda (matizable)

Tiempos de convergencia reducidos en caso de fallo de algún link (STP)

Las conexiones LACP pueden interconectar switches, routers, servidores y clientes, su implementación es recomendable en enlaces sobre puertos de acceso, uno por VLAN.

2.3. Marco conceptual

ACCESS POINT: Un punto de acceso inalámbrico, en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada

ACL: es un conjunto de reglas identificadas con un número o un nombre y cada regla especifica una acción y una condición, las acciones a aplicar son permitir o denegar todos los paquetes que cumplan la condición asociada a la regla. Una : se identifica con un número o un nombre y todas las reglas que tengan el mismo número/nombre hacen parte de la ACL, éstos identificadores suelen indicar también qué tanta expresividad tendrá la ACL, es decir, qué tan específicas pueden ser las reglas.

BPDU: significa Bridge Protocol Data Unit (Unidad de datos de protocolo puente), que es un paquete de datos, enviado en redes de área local o LAN, que trabaja para detectar bucles en una red. Los bucles pueden hacer que los paquetes de datos duplicados se envíen fuera, que puede utilizar el ancho de banda en una

red. Las guardas BPDU protegen los equipos de recepción de paquetes de datos no autorizados que pueden contener virus informáticos.

BROADCAST: es la difusión amplia, difusión ancha o broadcast, es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

CAT 6: es un estándar de cables para Gigabit Ethernet y otros protocolos de redes que es retro compatible con los estándares de categoría 5/5e y categoría 3. La categoría 6 posee características y especificaciones para evitar la diafonía (o crosstalk) y el ruido

CISCO: es una empresa de telecomunicaciones que se dedica a la venta y fabricación de equipo como routers, switches, productos de telefonía etc.

COLISIÓN: 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. A medida que aumenta el número de nodos que pueden transmitir en un segmento de red, aumentan las posibilidades de que dos de ellos transmitan a la vez. Esta transmisión simultánea ocasiona una interferencia entre las señales de ambos nodos, que se conoce como colisión. Conforme aumenta el número de colisiones disminuye el rendimiento de la red.

DAC: El control de acceso discrecional, es un tipo de control de acceso definido de acuerdo a los criterios. En seguridad informática, control de acceso discrecional (DAC) es una especie de control de acceso definidos por los Criterios de Trusted Computer System Evaluation (TCSEC) "como una forma de restringir el acceso a objetos basados en la identidad de los sujetos y / o grupos a los que pertenecen

ETHERCHANNEL: es una tecnología de CISCO que nos permite realizar una agrupación lógica de varios enlaces físicos Ethernet para que estos enlaces sean tratados como un único enlace, permitiendo sumar la velocidad de cada puerto y de esta forma lograr un enlace troncal de alta velocidad.

IP: Es un número que identifica un ordenador dentro de una red que utilice el protocolo IP. Dicho número no se ha de confundir con la dirección MAC, que es un número asignado a la tarjeta de red del propio ordenador (viene impuesta por el fabricante de la tarjeta), mientras que la dirección IP se puede cambiar.

Juniper Networks: es una multinacional dedicada a sistemas de redes y seguridad.

LACP: forma parte de una especificación IEEE (802.3ad) que permite agrupar varios puertos físicos para formar un único canal lógico. LACP permite que un switch negocie un grupo automático mediante el envío de paquetes LACP al peer.

Realiza una función similar a PAgP con EtherChannel de Cisco. Debido a que

LACP: es un estándar IEEE, se puede usar para facilitar los EtherChannels en entornos de varios proveedores. En los dispositivos de Cisco, se admiten ambos protocolos.

LAN: significa Red de área local. Es un grupo de equipos que pertenecen a la misma organización y están conectados dentro de un área geográfica pequeña a través de una red, generalmente con la misma tecnología (la más utilizada es Ethernet).

MAC: es el identificador único asignado por el fabricante a una pieza de hardware de red (como una tarjeta inalámbrica o una tarjeta Ethernet). «MAC» significa Media Access Control, y cada código tiene la intención de ser único para un dispositivo en particular.

MMF: Fibra óptica multimodo es un tipo de fibra óptica mayormente utilizada en el ámbito de la comunicación en distancias cortas, como por ejemplo un edificio o un campus. **MULTICAST:** (multidifusión) es el envío de información en una red a múltiples receptores de forma simultánea, un emisor envía un mensaje y son varios los receptores que reciben el mismo.

PANDUIT: es un fabricante global de soluciones de infraestructura física con soluciones para sectores de energía, comunicaciones, informática, control y sistemas de seguridad.

PuTTY: proviene de las siglas Pu: Port unique TTY: terminal type. Su traducción al castellano sería: Puerto único de tipo terminal. El almacenamiento de hosts y preferencias para uso posterior. Control sobre la clave de cifrado SSH y la versión de protocolo. Clientes de línea de comandos SCP y SFTP, llamados "pscp" y "psftp" respectivamente.

RJ-45: es una interfaz física comúnmente utilizada para conectar redes de computadoras con cableado estructurado (categorías 4, 5, 5e, 6 y 6a). Posee ocho pines o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado (UTP).

SSID: es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red.

STACKWISE: es una línea de interruptores de red creada por Cisco. Cada uno de ellos puede funcionar de forma independiente o actuar como un bloque de construcción para un interruptor con capacidades superiores. La capacidad de apilar interruptores permite que un usuario amplíe su infraestructura de red a medida que crecen sus necesidades, en lugar de tener que planificar para el peor de los casos o desechar equipos de red antiguos de poca potencia. Puedes configurar dos interruptores Stackwise para que funcionen juntos como una sola unidad.

STP: el protocolo STP (Spanning Tree Protocol, protocolo del árbol de expansión) es un protocolo de Capa 2 que se ejecuta en bridges y switches. La especificación para STP se denomina IEEE 802.1D. El principal objetivo de STP es garantizar que se impida la creación de bucles en trayectos redundantes en la red. Los bucles son fatales para una red.

SWITCH: es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y

embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto.

VLAN: acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

WLAN: (en inglés; *Wireless Local Area Network*) es un sistema de comunicación de datos inalámbrico, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas.

WLC: Una LAN controlador inalámbrico se utiliza para gestionar los puntos de acceso ligeros en grandes cantidades por el administrador de red o centro de operaciones de red.

CAPITULO III

3. DISEÑO, DESCRIPCIÓN DEL SISTEMA Y RESULTADOS

3.1. Metodología de recolección de datos

3.1.1. Métodos, técnicas e instrumentos de recolección de datos

a) Métodos

El método se ejecuta a partir de una situación problemática actual, observando los puntos deficientes o mejoras por ejecutar para la elaboración del diseño.

b) Técnicas e instrumentos

El software que se utilizó para la obtención de los datos sobre el rendimiento de la LAN es el PUTTY, que es un software libre para el acceso local y remoto de la cual nos permite analizar en tiempo real el tráfico de los usuarios, estado del hardware y conocer lógicamente la red del cliente.

3.1.2. Desarrollo del estudio de campo

La metodología utilizada para el levantamiento de la información o estudio de campo fue teniendo accesos locales a los equipos que conforman las sedes San Isidro y alrededores. Teniendo como herramienta el software cliente PuTTY.

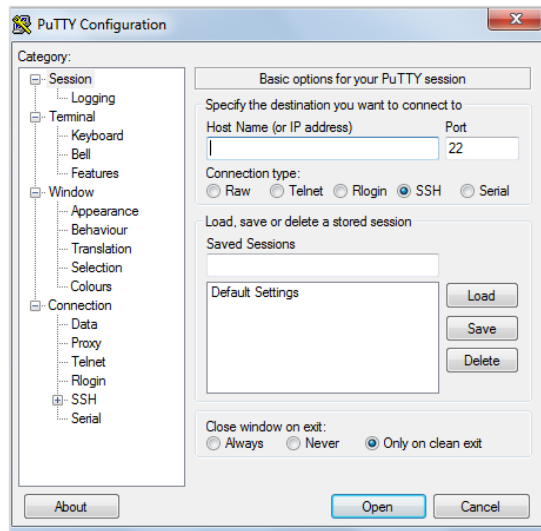


Figura N° 11: Putty, opciones básicas de sesión

Fuente: Putty, “Using SSH en Putty (Windows)”.

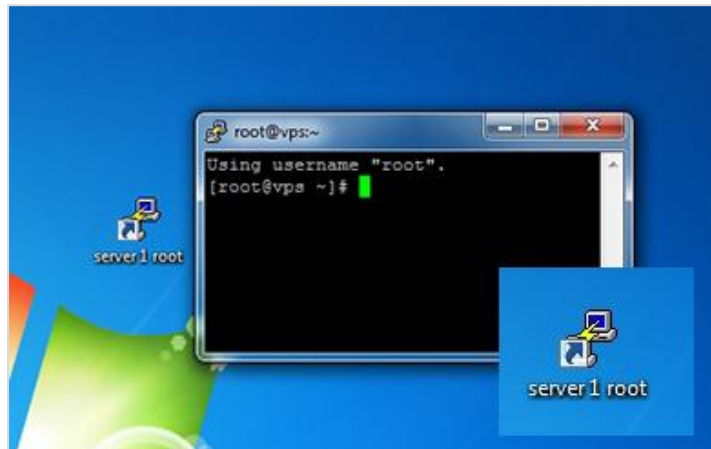


Figura N° 12: Software cliente; PuTTY

Fuente: Putty, “Using SSH en Putty (Windows)”.

3.1.3. Descripción Sede San isidro

En la sede de San Isidro actualmente se tienen instaladas equipos Juniper y Cisco, con una cantidad de un Switch-Core de 4 equipos en Virtual-Chassis, 21 Switches de piso, 14 Switches de gabinete con la infraestructura de red Wireless a nivel LAN.

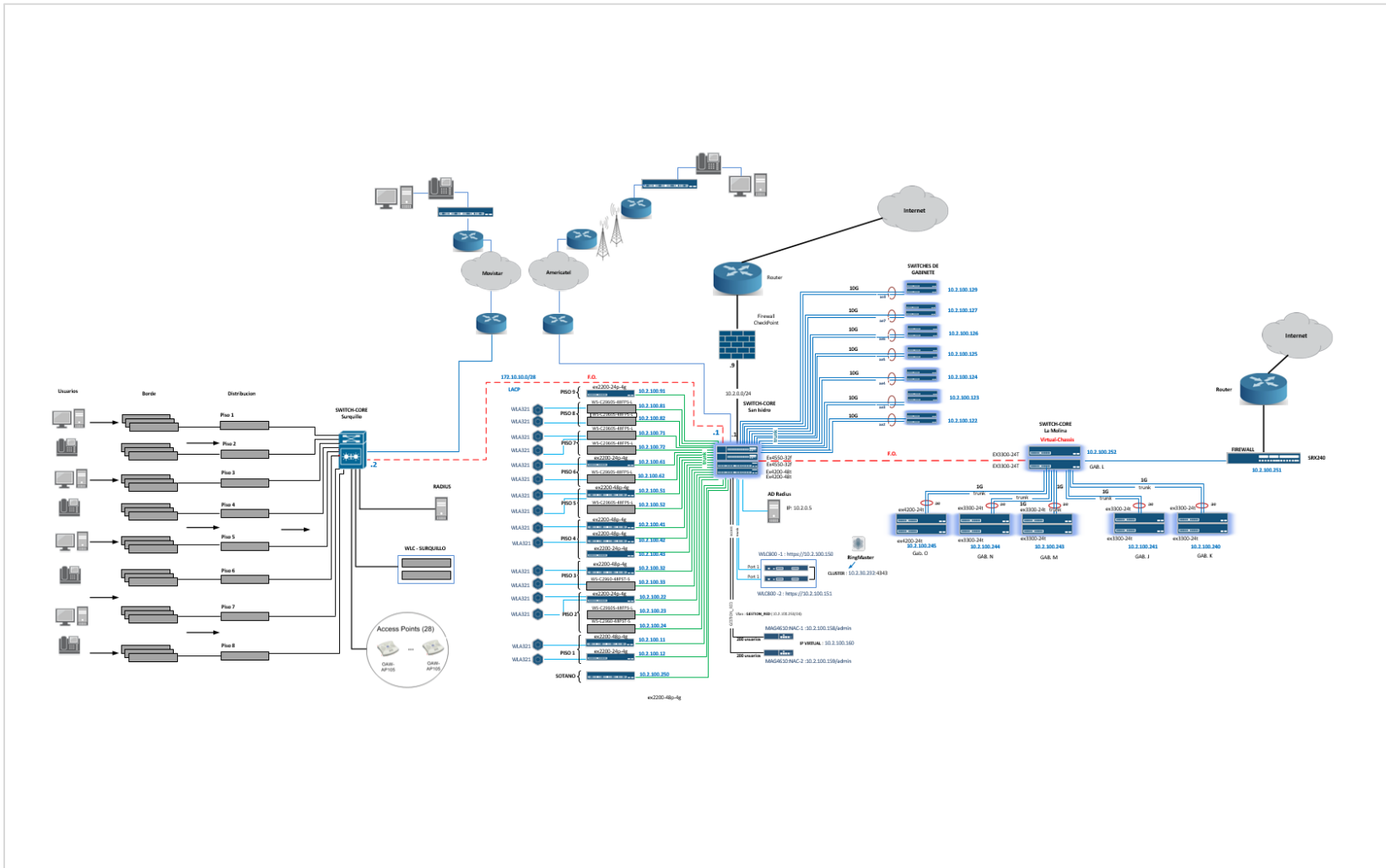


Figura N° 13: Diagrama de red actual de la Red de MI BANCO
Fuente: Elaboracion propia.

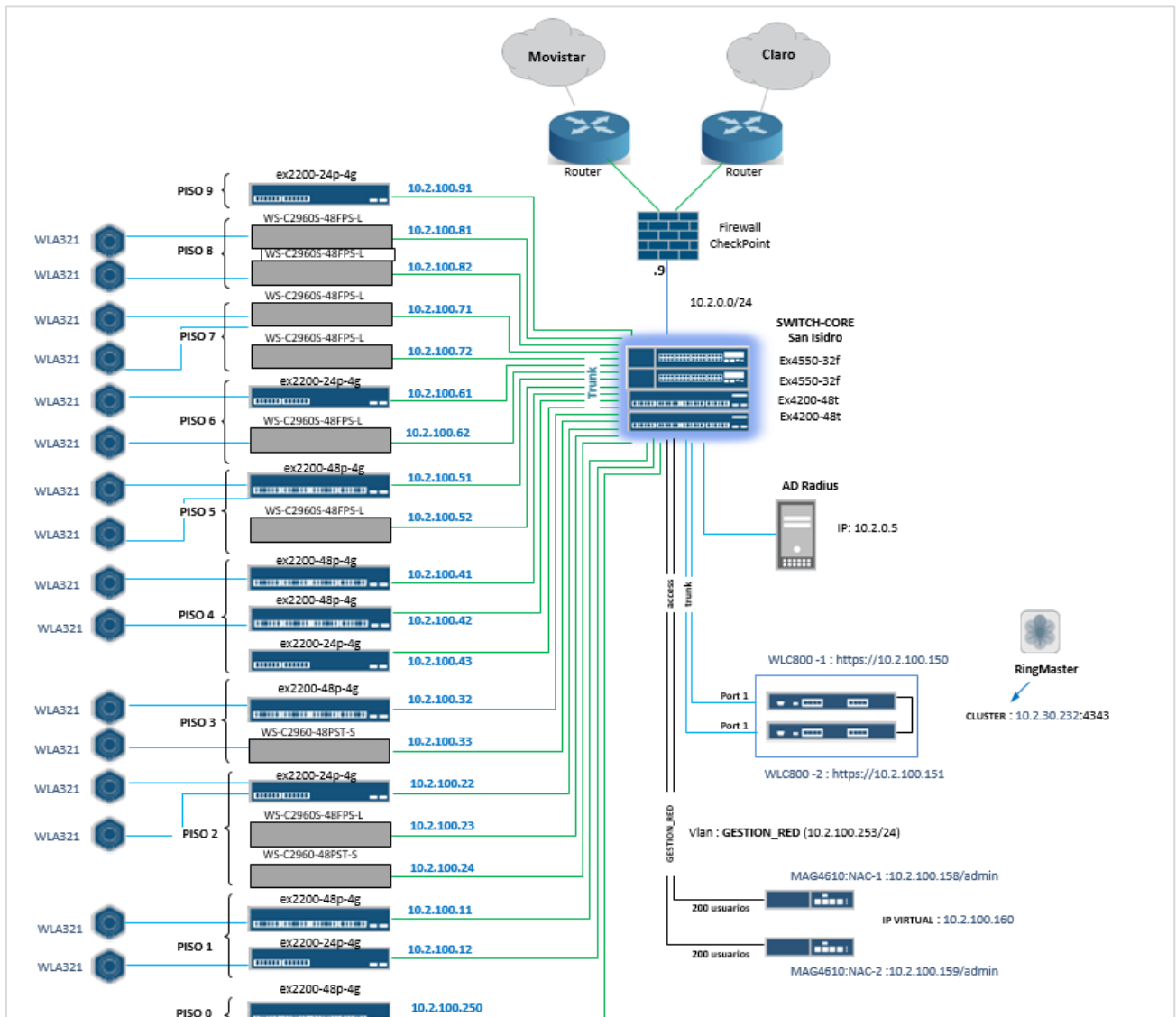


Figura N° 14: Diagrama de red actual de Sede San Isidro.

Fuente: Elaboracion propia, Mi Banco sede San Isidro.

a) Switch Core

Las especificaciones técnicas del equipo son las siguientes: Los 4 switches conforman un virtual-chassis (VC) haciendo uso de los cables DAC que son de fibra con Tranceiver acoplado.

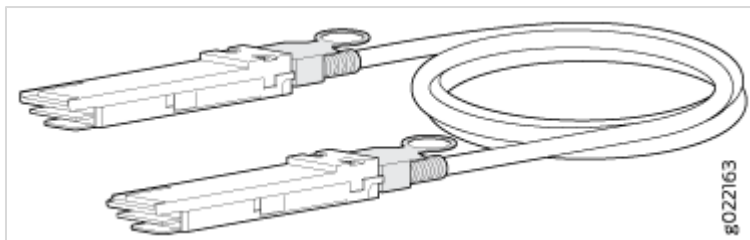


Figura N° 15: QSFP+ Direct Attach Copper Cables for EX Series Switches

Fuente: Juniper Networks, “ Cables EX Series Switches”.

Tabla N° 1: *Distribución de Switches Juniper en el Core de San Isidro.*

Fuente: Elaboracion propia, Mi Banco sede San Isidro.

HOSTNAME	PISO	MARCA	IP ADDRESS	MODELO	Numero de puertos
SW_CORE_JUNIP ER	4	Juniper	10.2.100.253	ex4550-32f	32 SFP(Fibra) + módulo de ampliación de hasta 48 puertos.
				ex4550-32f	
				ex4200-48t	48 + 4 puertos opcionales
				ex4200-48t	

El equipamiento del SWITCH-CORE, corresponde a los siguientes modelos en Virtual-Chassis de Juniper Networks EX4550-32F y EX420048T:



Figura N° 16: Vista frontal del equipo EX4500

Fuente: Juniper Networks, “EX Series Switches”.

Tabla N° 2: Características técnicas del Switch EX4500 de Juniper Networks.

Fuente: Juniper Networks, “EX Series Switches”.

Características	Métrica
Factor de forma	<ul style="list-style-type: none"> Plataforma fija Configuración de chasis virtual que consta de hasta 10 switches
Dimensiones	EX4500 : <ul style="list-style-type: none"> (W x H x D) 17.3 en x 3.5 en x 21,1 en (43.8 cm x 8.9 cm x 53.6 cm) 2 unidades de rack EX4550 : <ul style="list-style-type: none"> (W x H x D) 17.4 en x 1.7 en x 18,5 en (44,07 cm x 4.4 cm x 47.0 cm) 1 unidad de rack
Velocidad del backplane	EX4500 : Hasta 128 Gbps (Virtual chasis) EX4550 : Hasta 256 Gbps (Virtual chasis)
Velocidad de datos	960 Gbps (full dúplex)
Throughput	714 Mpps
10/100/1000BASE-T Densidades de puertos	EX4500 <ul style="list-style-type: none"> 40 puertos 1000BASE -T en la unidad base (48 en total con módulos uplink opcionales) a través de la óptica SFP de cobre Hasta 480 en la configuración de chasis virtual EX4550 : <ul style="list-style-type: none"> 32 1000BASE -X SFP / SFP + en la unidad base, 48 en total con los módulos de ampliación opcionales. Hasta 400 en la configuración de chasis virtual
40GBASE QSFP + Densidades de puertos	N / A
100GBASE PPC Densidades de puertos	N / A
Resiliency	Resiliency doble carga interna compartiendo CA y las fuentes de alimentación de CC (opcional); ventiladores de velocidad variable redundantes
Opciones de energía	EX4550 : <ul style="list-style-type: none"> 650 fuentes de alimentación W de CA y CC

Sistema operativo	Junos
Monitoreo de tráfico	sFlow
QoS Queues / Port	8
Direcciones MAC	32000
Jumbo Frames	9216 bytes
IPv4 Unicast / Multicast Routes	14,000*/ 4,000 *Uni-dimensional scale
IPv6 Unicast / Multicast Routes	3,400*/ 1,000 *Uni-dimensional scale
Number of VLANs	4096
Entradas ARP	8000
Garantía	La garantía estándar es de un año de duración



Figura N° 17: Vista frontal del equipo EX4200

Fuente: Juniper Networks, “EX Series Switches”.

Tabla N° 3: Características técnicas del Switch EX4200 de Juniper Networks.

Fuente: Juniper Networks, “EX Series Switches”.

Características	Métrica
Factor de forma	<ul style="list-style-type: none"> plataforma fija Configuración de chasis virtual que consta de 10 interruptores
Dimensiones	<ul style="list-style-type: none"> (W x H x D) 17.4 x 1.7 x 16.4 cm (44.2 x 4.3 x 41.7 cm) 1 unidad de rack
Velocidad del backplane	128 Gbps (Virtual Chassis)
Velocidad de datos	<ul style="list-style-type: none"> EX4200-24P/24T/24F : 88 Gbps EX4200-48P/48T : 136 Gbps

Rendimiento	<ul style="list-style-type: none"> EX4200-24P/24T/24F : 65 Mpps (velocidad de cable) EX4200-48P/48T : 101 Mpps (velocidad de cable)
10/100/1000BASE-T Densidades de puertos	<ul style="list-style-type: none"> De 24/48 por plataforma Hasta 480 en la configuración de chasis virtual
100BASE -FX / 1000BASE -X (SFP) Densidades de puertos	<ul style="list-style-type: none"> 24 por switch ; 28 con módulo de enlace ascendente GbE de cuatro puertos opcional Hasta 280 en la configuración de chasis virtual
10GBASE -X Densidades de puertos	<ul style="list-style-type: none"> 2 por interruptor (a través del módulo de enlace ascendente de 10 GbE de dos puertos opcional) Hasta 20 en la configuración de chasis virtual
40GBASE QSFP + Port Densidades	N / A
100GBASE PPC Port Densidades	N / A
Resiliency	Interna , hot- swappable de alimentación redundante ; bandeja de ventiladores reemplazables en campo con tres ventiladores; grácil transición Ruta Engine (GRES) en la configuración de chasis virtual
Opciones de energía	<ul style="list-style-type: none"> AC: 320W , 600W y 930W con detección automática , 100 -120V / 200 - 240V; fuentes de alimentación dobles que comparten la carga intercambiables en caliente internas redundantes DC: 190W : de entrada Rango de tensión de 36V - 72V ; alimentación de entrada doble , dos fuentes de alimentación comparten la carga intercambiables en caliente internas redundantes
sistema Operativo	Junos
Monitoreo de Tráfico	sFlow
QoS Colas / Puerto	8
direcciones MAC	32000
Jumbo Frames	9216 Bytes
Rutas IPv4 Unicast / Multicast	16000 / 8000
Rutas IPv6 Unicast / Multicast	4000 / 2000
Número de VLANs	4096
Entradas ARP	16000
Garantía	Garantía ilimitada de hardware de por vida

b) Switches de Pisos

Las especificaciones técnicas de los equipos son las siguientes:

Tabla N° 4: Distribución de los Switches en el Sótano y los 9 Pisos de la sede San Isidro.

Fuente: Elaboracion propia, Mi Banco sede San Isidro.

HOSTNAME	PISO	MARCA	IP ADDRESS	MODELO	Numero de puertos
SW12JS1.1	sótano	Juniper	10.2.100.250	EX2200-48P-4G	48 + 4 SFP(fibra)
SW12JP1.1	1	Juniper	10.2.100.11	EX2200-48P-4G	48 + 4 SFP(fibra)
SW12JP1.2		Juniper	10.2.100.12	EX2200-24P-4G	24 + 4 SFP(fibra)
SW12JP2.2	2	Juniper	10.2.100.22	EX2200-24P-4G	24 + 4 SFP(fibra)
SW12CP2_3		Cisco	10.2.100.23	WS-C2960S-48FPS-L	48 + 4 SFP(fibra)
SW12CP2_4		Cisco	10.2.100.24	WS-C2960-48PST-S	48 + 2 SFP(fibra)
SW12JP3.1	3	Cisco	10.2.100.31	WS-C2960S-48FPS-L	48 + 4 SFP(fibra)
SW12JP3.2		Juniper	10.2.100.32	EX2200-48P-4Gb	48 + 4 SFP(fibra)
SW12CP3.3		Cisco	10.2.100.33	WS-C2960-48PST-S	48 + 2 SFP(fibra)
SW12JP4.1	4	Juniper	10.2.100.41	EX2200-48P-4G	48 + 4 SFP(fibra)
SW12JP4.2		Juniper	10.2.100.42	EX2200-48P-4G	
SW12JP4.3		Juniper	10.2.100.43	EX2200-24P-4G	24 + 4 SFP(fibra)
SW12CP4_4		Cisco	10.2.100.44	WS-C2960S-48FPS-L	48 + 4 SFP(fibra)
SW12JP5.1	5	Juniper	10.2.100.51	EX2200-48P-4G	48 + 4 SFP(fibra)
SW12CP5_2		Cisco	10.2.100.52	WS-C2960S-48FPS-L	48 + 4 SFP(fibra)
SW12JP6.1	6	Juniper	10.2.100.61	EX2200-24P-4G	24 + 4 SFP(fibra)
SW12CP6.2		Cisco	10.2.100.62	WS-C2960S-48FPS-L	48 + 4 SFP(fibra)
SW12CP7_1	7	Cisco	10.2.100.71	WS-C2960S-48FPS-L	
SW12CP7_2		Cisco	10.2.100.72	WS-C2960S-48FPS-L	
SW12CP8_1	8	Cisco	10.2.100.81	WS-C2960S-48FPS-L	
SW12CP8_2		Cisco	10.2.100.82	WS-C2960S-48FPS-L	
SW12JP9.2	9	Juniper	10.2.100.92	EX2200-24P-4G	24 + 4 SFP(fibra)



Figura N° 18: Vista frontal del equipo EX2200-48P

Fuente: Juniper Networks, “EX Series Switches”.



Figura N° 19: Vista frontal del equipo EX2200-24P

Fuente: Juniper Networks, “EX Series Switches”.

Tabla N° 5: Características técnicas del Switch EX2200-48P y Switch EX2200-24P de Juniper Networks.

Fuente: Juniper Networks, “EX Series Switches”.

Características	Se Brinda
Form Factor	<ul style="list-style-type: none"> • Fixed platform • Virtual Chassis configuration consisting of up to four switches
Dimensions	EX2200: <ul style="list-style-type: none"> • (W x H x D) 17.4 x 1.7 x 10 in (44.1 x 4.4 x 25.4 cm) • 1 rack unit EX2200-C: <ul style="list-style-type: none"> • (W x H x D) 10.6 x 1.7 x 9 in (26.9 x 4.4 x 22.8 cm) • 1 rack unit
Backplane Speed	N/A

Data Rate	<ul style="list-style-type: none"> EX2200-24P/24T: 56 Gbps EX2200-48P/48T: 104 Gbps EX2200-C-12T/12P-2G: 28 Gbps
Throughput	<ul style="list-style-type: none"> EX2200-24P/24T: 42 Mpps (wire speed) EX2200-48P/48T: 77 Mpps (wire speed) EX2200-C-12T/12P-2G: 21 Mpps
10/100/1000BASE-T Port Densities	EX2200: <ul style="list-style-type: none"> 24 / 48 per platform Up to 96 / 192 in Virtual Chassis configuration EX2200-C: <ul style="list-style-type: none"> 14 per platform Up to 56 in Virtual Chassis configuration
100BASE-FX / 1000BASE-X (SFP) Port Densities	EX2200: <ul style="list-style-type: none"> 4 per switch (fixed ports, SFP required) Up to 16 in Virtual Chassis configuration EX2200-C: <ul style="list-style-type: none"> 2 per switch (fixed ports, SFP required) Up to eight in Virtual Chassis configuration
10GBASE-X Port Densities	N/A
40GBASE QSFP+ Port Densities	N/A
100GBASE CFP Port Densities	N/A
Resiliency	<ul style="list-style-type: none"> EX2200: Integral power supply and fans; external power supply option EX2200-C: Fanless design improves MTBF by eliminating moving parts that can fail
Power Options	<ul style="list-style-type: none"> EX2200-24T (non-PoE): Autosensing; 100-120 V / 200-240 V / 200-240 V; AC 50 W EX2200-48T (non-PoE): Autosensing; 100-120 V / 200-240 V / 200-240 V; AC 470 W EX2200-24P (PoE/PoE+): Autosensing; 100-120 V / 200-240 V / 200-240 V; AC 470 W EX2200-48P (PoE/PoE+): Autosensing; 100-120 V / 200-240 V / 200-240 V; AC 496 W EX2200-C-12T-2G (non-PoE): 100-120 V / 200-240 V; AC 30 W EX2200-C-12P-2G (PoE/PoE+): 100-120 V / 200-240 V; AC 180 W
Operating System	Junos
Traffic Monitoring	sFlow
QoS Queues / Port	8
MAC Addresses	16000
Jumbo Frames	9216 Bytes
IPv4 Unicast / Multicast Routes	65000 / 1000
IPv6 Unicast / Multicast Routes	N/A
Number of VLANs	1024

ARP Entries	2000
Warranty	<ul style="list-style-type: none"> EX2200: Enhanced limited lifetime hardware warranty EX2200-C: Enhanced limited lifetime hardware warranty



Figura N° 20: Vista frontal del equipo WS-C2960S-48FPS-L de Cisco Systems.

Fuente: Cisco Systems, “Switches Cisco, para la pequeña empresa”.

Tabla N° 6: Características técnicas del Switch WS-C2960S-48FPS-L de Cisco Systems.

Fuente: Juniper Networks, “EX Series Switches”.

Características	Métrica
Interfaces	48 x 10Base-T/100Base-TX/1000Base-T - RJ-45 - PoE 1 x USB - Type A 1 x consola - mini USB tipo B - gestión 1 x consola - RJ-45 - gestión 1 x 10Base-T/100Base-TX - RJ-45 - gestión 4 x SFP (mini-GBIC)



Figura N° 21: Vista frontal del equipo WS-C2960-48PST-S de Cisco Systems

Fuente: Cisco Systems, “Switches Cisco, para la pequeña empresa”.

Tabla N° 7: Características técnicas del Switch WS-C2960-48PST-S de Cisco Systems.

Fuente: Cisco Systems, “ Switches Cisco, para la pequeña empresa”.

Características	Métrica
Interfaces	48 x 100Base-TX - RJ-45 - PoE 2 x 1000Base-T - RJ-45 1 x consola - RJ-45 - gestión 2 x SFP (mini-GBIC)

c) Switches de gabinete

Las especificaciones técnicas de los equipos son las siguientes: En la cual el VC(virtual chasis) de 2 Switches está armado con cables DAC.

Tabla N° 8: Distribución de switches Juniper en los Gabinetes de San Isidro.

Fuente: Elaboracion propia, Mi Banco sede San Isidro.

HOSTNAME	PISO	MARCA	IP ADDRESS	MODELO	Numero de puertos
SW_GABINETE2	4	Juniper	10.2.100.122	ex3300-24t	24 + 4 SFP(fibra)
				ex3300-24t	
SW_GABINETE3	4	Juniper	10.2.100.123	ex3300-24t	
				ex3300-24t	
SW_GABINETE4	4	Juniper	10.2.100.124	ex3300-24t	
				ex3300-24t	
SW_GABINETE5	4	Juniper	10.2.100.125	ex3300-24t	
				ex3300-24t	
SW_GABINETE6	4	Juniper	10.2.100.126	ex3300-24t	
				ex3300-24t	
SW_GABINETE7	4	Juniper	10.2.100.127	ex3300-24t	
				ex3300-24t	
SW_GABINETE9	4	Juniper	10.2.100.129	ex3300-24t	
				ex3300-24t	



Figura N° 22: Vista frontal del Switch EX3300-24T

Fuente: Juniper Networks, “EX Series Switches”.

Tabla N° 9: Característica técnicas del Switch EX3300-24T de Juniper Networks

Fuente: Juniper Networks, “EX Series Switches”.

Características	Se Brinda
Form Factor	<ul style="list-style-type: none"> Fixed platform Virtual Chassis configuration consisting of up to 10 switches
Dimensions	<ul style="list-style-type: none"> (W x H x D) 17.4 x 1.7 x 12 in (44.1 x 4.3 x 31 cm) 1 rack unit
Backplane Speed	<ul style="list-style-type: none"> 40-80 Gbps
Data Rate	<ul style="list-style-type: none"> EX3300-24P/24T/24T-DC: 128 Gbps EX3300-48P/48T/48T-BF: 176 Gbps
10/100/1000BASE-T Port Densities	EX3300-24P/24T/24T: <ul style="list-style-type: none"> 28 per platform (24 access ports + four uplink ports) Up to 280 in Virtual Chassis configuration EX3300-48P/48T/48T: <ul style="list-style-type: none"> 52 per platform (48 access ports + four uplink ports) Up to 520 in Virtual Chassis configuration
100BASE-FX / 1000BASE-X (SFP) Port Densities	<ul style="list-style-type: none"> 4 per switch (fixed ports, SFP/SFP+ required) Up to 40 in Virtual Chassis configuration
10GBASE-X Port Densities	<ul style="list-style-type: none"> 4 per Switch Up to 40 in Virtual Chassis configuration
40GBASE QSFP+ Port Densities	N/A
100GBASE CFP Port Densities	N/A
Resiliency	Si
Power Options	<ul style="list-style-type: none"> EX3300-24T/-48T/-48T-BF (non-PoE): Autosensing; 100-120 V / 200-240 V; AC 100 W EX3300-24P (PoE/PoE+): Autosensing; 100-120 V / 200-240 V; AC 550 EX3300-48P (PoE/PoE+): Autosensing; 100-120 V / 200-240 V; AC 900 EX3300-24T-DC: Autosensing; 100-120 V / 200-240 V; DC 100 W
Operating System	Junos
Traffic Monitoring	N/A

QoS Queues / Port	8
MAC Addresses	16000
Jumbo Frames	9,216 Bytes
IPv4 Unicast / Multicast Routes	8,000 / 0
IPv6 Unicast / Multicast Routes	N/A
Number of VLANs	4096
ARP Entries	4000
Warranty	Enhanced limited lifetime hardware warranty

d) Infraestructura de red

Las especificaciones técnicas de los equipos son las siguientes: El Ringmaster como software administrativo y los WLC800R como equipos físicos.

Tabla N° 10: Ringmaster, Software Cliente

Fuente: Elaboracion propia, Mi Banco sede San Isidro.

RingMaster (Administrador de Clúster WLC)	MARCA	Tipo	IP ADDRESS
	Juniper	software	10.2.30.232:4343

Los 2 WLCs están configurados en clúster.

Tabla N° 11: WLC (Wireless LAN Controller)

Fuente: Elaboracion propia, Mi Banco sede San Isidro.

MODELO	HOSTNAME	CANTIDAD	MARCA	IP ADDRESS
WLC800R	WLC-1	2	Juniper	https://10.2.100.150
	WLC-2		Juniper	https://10.2.100.151



Figura N° 23: Vista frontal del Controlador Wireless Juniper WLC800R

Fuente: Juniper Networks, “WLAN Series Hardware Dates & Milestones”.

Características técnicas del WLC800R:

- Configuración en alta disponibilidad y centralizada.
- Soporta hasta una escalabilidad de 128 AP.
- Licencia base para 16 AP.
- 4 puertos GbE SFP y 4 puertos 10/100/1000 BaseT.

Tabla N° 12: *Distribución de los Access Point*

Fuente: Elaboracion propia, Mi Banco sede San Isidro.

MODELO	HOSTNAME	CANTIDAD	MARCA
WLA321-WW	AP1-1	15	Juniper
	AP1-2		
	AP2-1		
	AP2-2		
	AP3-1		
	AP3-2		
	AP4-1		
	AP4-2		
	AP5-1		
	AP5-2		

	AP6-1		
	AP7-1		
	AP7-2		
	AP8-1		
	AP8-2		



Figura N° 24: Vista frontal del Access Point Juniper, WLA321

Fuente: Juniper Networks, “WLA321 Access Point Hardware Documentation”.

Características técnicas del WLC800R:

- Single Radio (2.4 GHz o 5 GHz).
- Tasa de transferencia hasta de 300 Mbps.
- 01 puerto 10/100/1000 BASET
- 802.3af PoE power

3.1.4. Descripción Sede La Molina

En la sede de La Molina actualmente se tienen instaladas equipos Juniper trabajando como Switch-Core de contingencia.

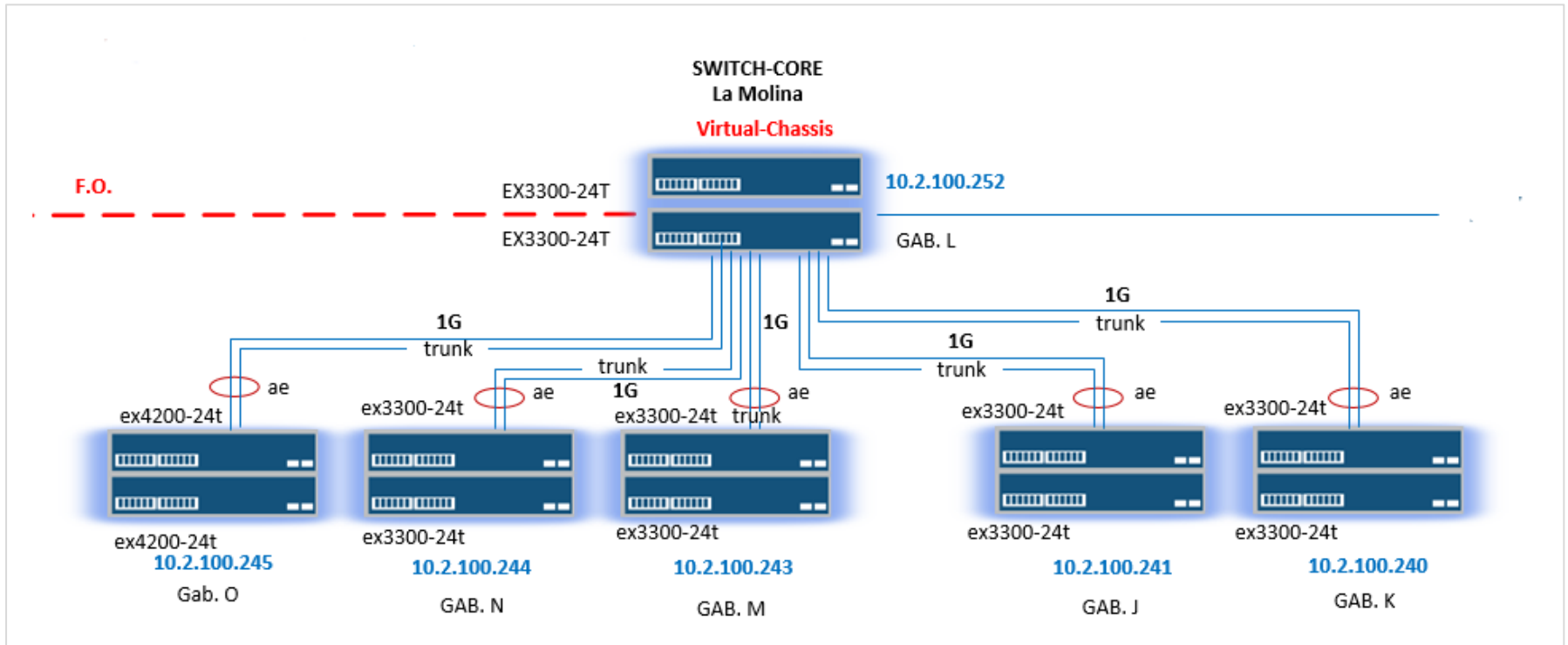


Figura N° 25: Diagrama de sede La Molina

Fuente: Elaboracion propia, Mi Banco Sede La Molina.

a) Switches de gabinete

En la Sede La Molina se tiene actualmente instalados switches-Core, switches de acceso en virtual-chassis y un srx240.

Tabla N° 13: *Distribución de Switches Juniper en los Gabinetes de La Molina.*

Fuente: Elaboracion propia, Mi Banco sede San La Molina.

SWITCH	GABINETE	MARCA	IP	MODELO
SW_GAB-O	O	juniper	10.2.100.245	ex4200-24t
				ex4200-24t
SW_GAB-N	N	juniper	10.2.100.244	ex3300-24t
				ex4200-24t
SW_GAB_M	M	juniper	10.2.100.243	ex3300-24t
				ex4200-24t
SW_SITE_CONTINGENCIA1	L	juniper	10.2.100.252	ex3300-24t
				ex3300-24t
SW_GAB_K	K	juniper	10.2.100.241	ex3300-24t
				ex4200-24t
SW_GAB_J	J	juniper	10.2.100.240	ex3300-24t
				ex4200-24t

3.1.5. Estado actual de los procesos de trabajo

Posterior al levantamiento de información o estudio de campo.

a) Comportamiento de los Switch-Core con los Switches de piso:

Los switches de piso están conectados con cable Ethernet hacia el switch-Core en modo trunk con todas las vlans asociadas en capa 2 y muchas de los pisos

Por ejemplo: Una conexión similar es como se muestra en la figura n° 28

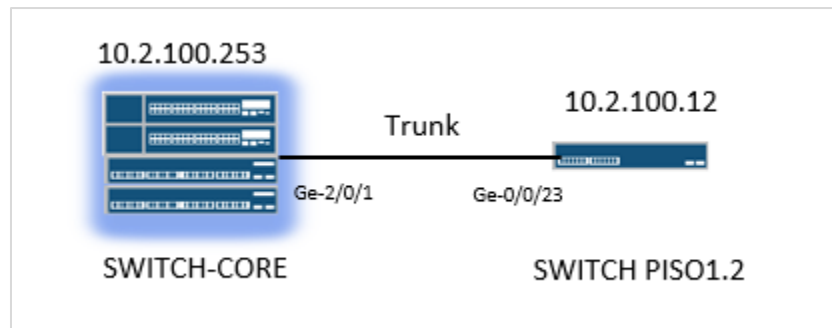


Figura N° 26: Conexión Core – Piso 1.

Fuente: Elaboracion propia, Mi Banco sede San Isidro

Los switches de piso tienen como default gateway al switch-Core. El switch-Core está en el Layer 3 y realizan procesos de enrutamiento.

b) Comportamiento de los switch-Core con los switches de gabinete:

El switch-Core está conectado con los switches de gabinete utilizando el protocolo LACP para una mejor disponibilidad, mejor velocidad en el proceso de transmisión de datos.

Los LACP están asociados a una VLAN, en la cual están trabajando las interfaces virtuales (ae) y constan de dos interfaces físicas a una velocidad de 10GB cada interface y en full dúplex.

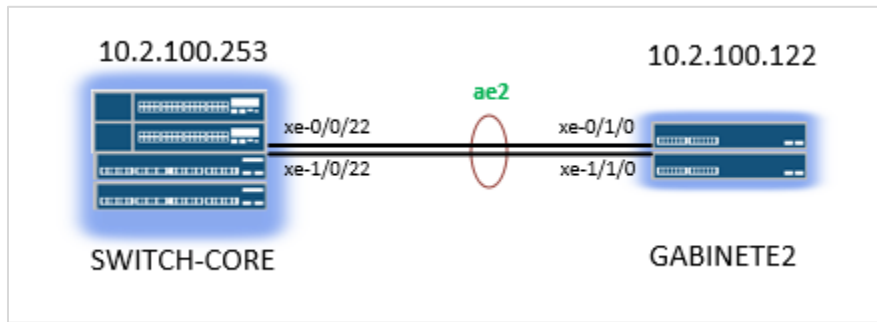


Figura N° 27: Conexión Core – Gabinete 2.

Fuente: Elaboracion propia, Mi Banco sede San Isidro

c) Comportamiento de los Switch-Core Surquillo, Switch-Core San Isidro con los Switch-Core La Molina:

Los switch-Core de las sedes están interconectadas mediante una fibra oscura. La interconexión de las sedes Surquillo y San isidro están utilizando el protocolo de LACP para 2 interfaces físicas en Layer 2 con 2G de velocidad en total. La interconexión de las sedes San isidro y La Molina conectadas con fibra oscura en modo trunk en Layer 2. Los Switch-Core de San Isidro y La Molina trabajan en Layer 3 en términos en enrutamiento.

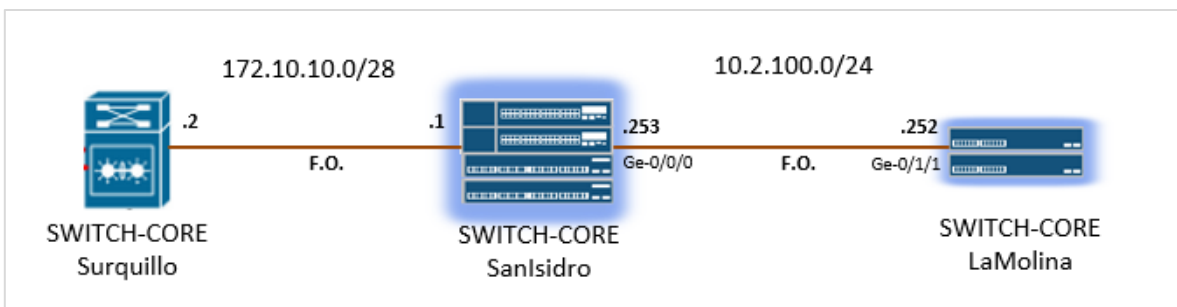


Figura N° 28: Conexión Core –Surquillo, San Isidro y La Molina por fibra oscura.

Fuente: Elaboracion propia, Mi Banco.

d) Comportamiento de la plataforma Wireless:

En el switch-Core de San Isidro tiene configurado un servicio de DHCP que recibirán los APS con un pool 10.2.62.0/24 desde la dirección ip 10.2.62.5 hasta la ip 10.2.62.250.

El sistema inalámbrico consta de 2 Wireless LAN Controller (WLC) en Clúster en modo activo. En la cual es administrada mediante el software cliente RingMaster.

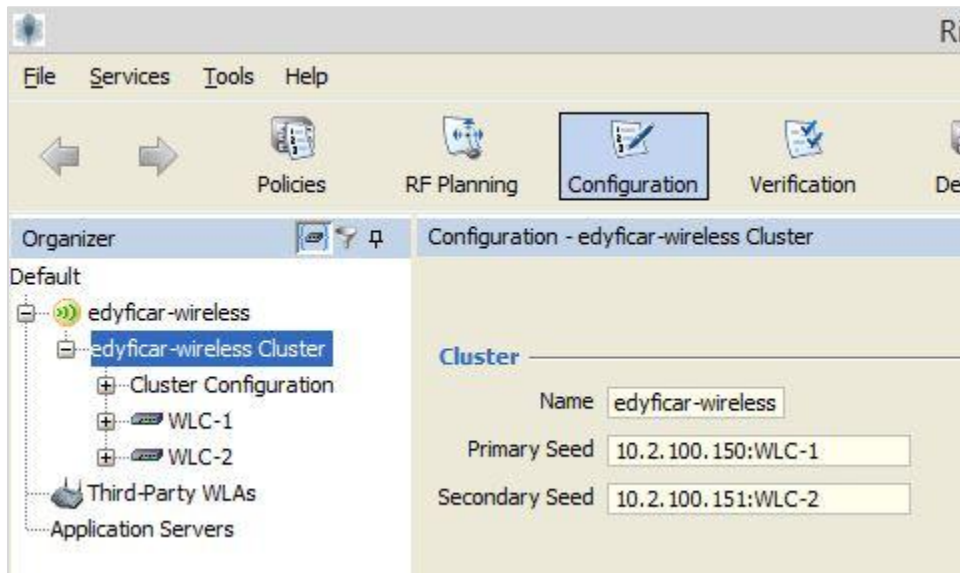


Figura N° 29: Entorno Ringmaster de Mi Banco.

Fuente: Base de datos de equipo WLC por Ringmaster, Mi Banco sede San Isidro.

Cada WLC tiene la licencia para el uso de 16 AP; es decir el clúster tiene licencia para 32 AP. Actualmente se tiene 15 APs en el clúster así que si un WLC pierde gestión o presente un desperfecto este sistema seguirá en su funcionamiento normal porque aún tiene la licencia para 16 APs del otro WLC.

A continuación se muestra la verificación en entorno CLI de las licencias activas en cada WLC. En la cual cada captura corrobora licencia para 16 APs en cada equipo y clúster levantado.

```
WLC-1> show license
Serial Number      : KF0212380610

Platform AP Count : 16 access points are supported
Redundant AP Count : 16 access points are supported

32 access points are supported

|
Additional Features:

      Feature Description              Installed
-----
High-Availability                      Yes
```

```
WLC-2> show license
Serial Number      : KF0212380512

Platform AP Count : 16 access points are supported
Redundant AP Count : 16 access points are supported

32 access points are supported

Additional Features:

      Feature Description              Installed
-----
High-Availability                      Yes
```

Figura N° 30: licencia actual de los WLC 1- WLC 2

Fuente: Base de datos de equipo WLC por Consola Putty, Mi Banco sede San Isidro.

Se tienen configurados 2 SSID:

- AIR_INT
- AIR_INV

Al conectarse al SSID: AIR_INT el usuario recibirá por DHCP una dirección en el segmento 10.2.61.0/24. La autenticación de los usuarios es a través de las MAC de las PCs o laptops y por dominio.

Al conectarse al SSID: AIR_INV el usuario recibirá por DHCP una dirección en el segmento 192.168.1.0/24. La autenticación de los usuarios es a través de un User y un Password configurador en el Radius y el tipo de autenticación es por un portal web.

Trabajando en conjunto con el Servidor Radius que es el Active Directory (AD) de la Sede San Isidro y es quien tiene configurado a todos los usuarios en su dominio y permite el acceso al Internet inalámbrico local.

A continuación se muestra en la siguiente captura la configuración de quien es el servidor Radius para el clúster.

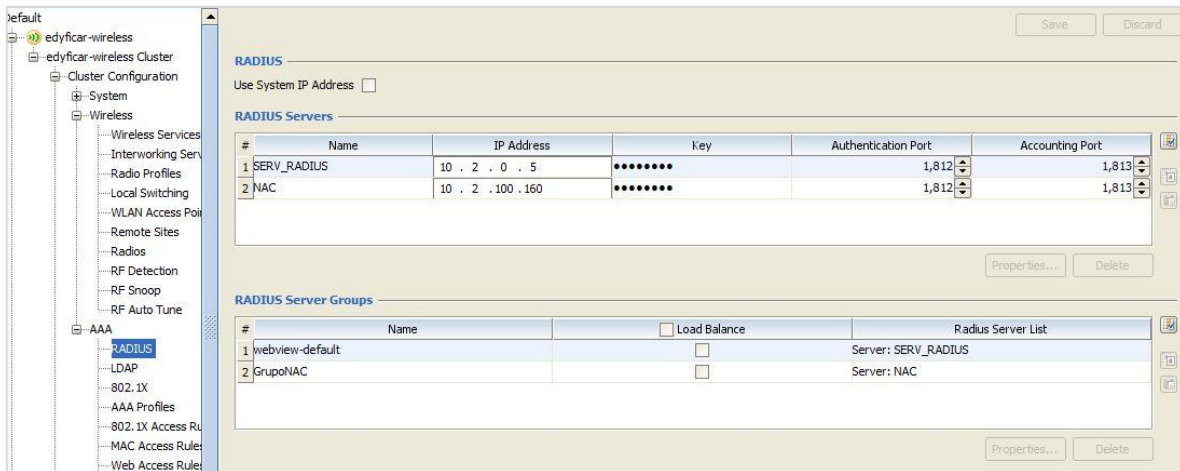


Figura N° 31: Entorno gráfico del Ringmaster.

Fuente: Base de datos de equipo WLC por Ringmaster, Mi Banco sede San Isidro.

Los pasos de funcionamiento cuando un usuario se conecta a un SSID, son las siguientes:

- I. El usuario selecciona el SSID a conectarse, ingresando las credenciales correspondientes.
- II. El SSID configurado en el clúster de los WLCs disponen del SSID solicitado.
- III. El clúster de los WLCs consultan al Servidor Radius (AD) para la autenticación del dominio del usuario. Y le da el permiso para el acceso.
- IV. Con el OK del Servidor Radius entonces el clúster permite la conexión del usuario.

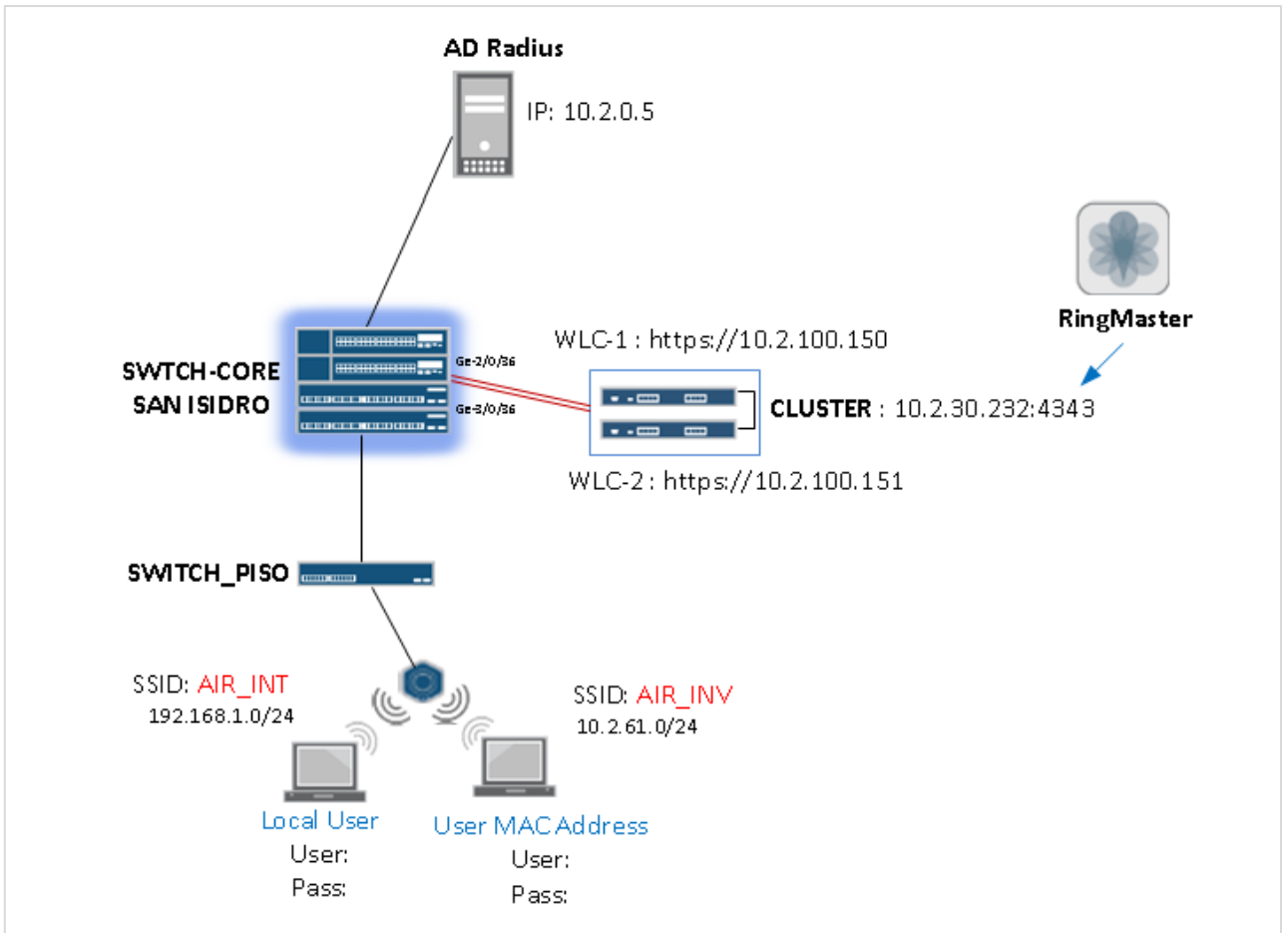


Figura N° 32: Diagrama de red Inalámbrica de San Isidro.

Fuente: Elaboracion propia, Mi Banco Sede San Isidro.

e) Esquema actual en sede SURQUILLO

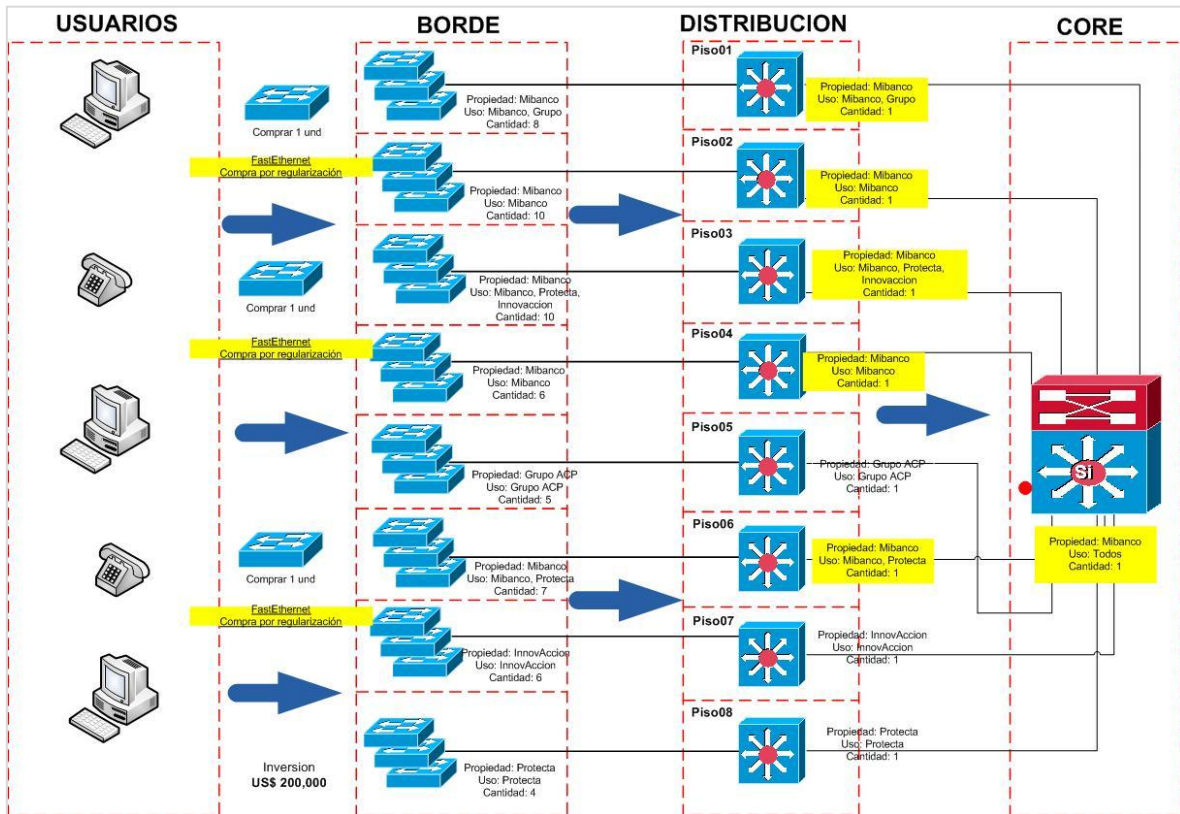


Figura N° 33: Distribución de los niveles de Jerarquía de la red en la Sede Surquillo.

Fuente: Elaboracion del cliente Mi Banco, "Red LAN", Mi Banco sede Surquillo.

3.2. Construcción, diseño de la herramienta/ sistema

3.2.1. Estudio y diseño

Para el presente diseño se llevó a cabo el estudio de campo o levantamiento de información en la cual se encontró debilidades de la red en la sede San Isidro en referencia a los Switches ubicados en todos los 10 pisos del Edificio.

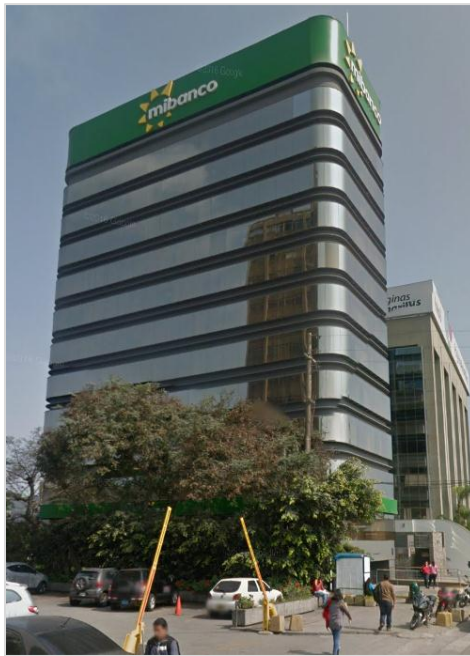


Figura N° 34: Mibanco Sede San Isidro ubicado en Av. Paseo de la Republica 3717

Fuente: Google Maps, Mi Banco Sede San Isidro.

Se encontró distribución de los Switches de piso:

- Conexión escalonada y clandestina.
- Puertos libres sin ningún tipo de seguridad sensibles a presentar corte en el servicio o bucles, si un usuario llevaba conexión en cualquiera de los puertos de red.

- Conexión lineal, no hay funcionalidades específicas por equipo de red (Switches).
- Problemas del servicio y gestión de las operaciones.

El diseño consiste en trabajar con el siguiente nivel de jerarquía:

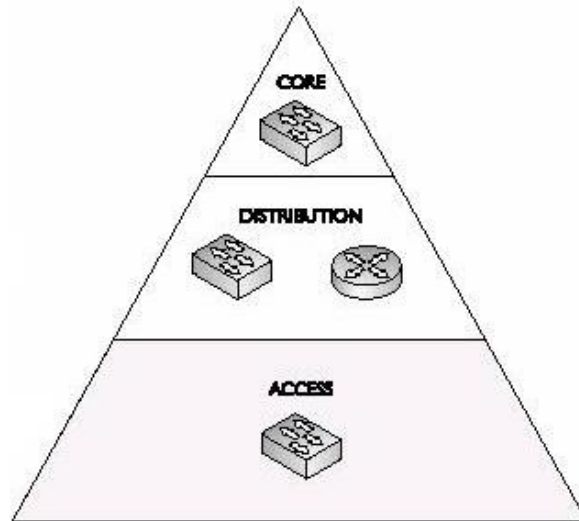


Figura N° 35: Jerarquía de la conexión.

Fuente: Consultas CCNA, “Modelo de Red Jerarquico”.

CORE o NÚCLEO es el backbone de la red. Este proveerá un acceso rápido entre los diferentes dispositivos de la red, para ejecutar una tarea rápida se usan switches de alta velocidad. El tráfico que atraviesa esta zona es un acceso a recursos internos como servidores de correo, aplicaciones corporativas del cliente.

DISTRIBUTION, este nivel usaran switches que realizara las más grandes funciones de distribución de tráfico y se empleara el direccionamiento del nivel 3 (nivel IP). Sus funciones serán:

- Limitar el tráfico de broadcast.
- Asegurar tráfico entre las capas.
- Proveer una jerarquía en el direccionamiento del nivel 3 y el enrutamiento.
- Intercambio entre los diferentes tipos de medio.

ACCESS LAYER, este nivel se encarga principalmente de proveer una primera conexión a los usuarios de la red.

Entonces se propone para este caso la ubicación que tendría la propuesta de diseño en todo el Edificio de Mi Banco.

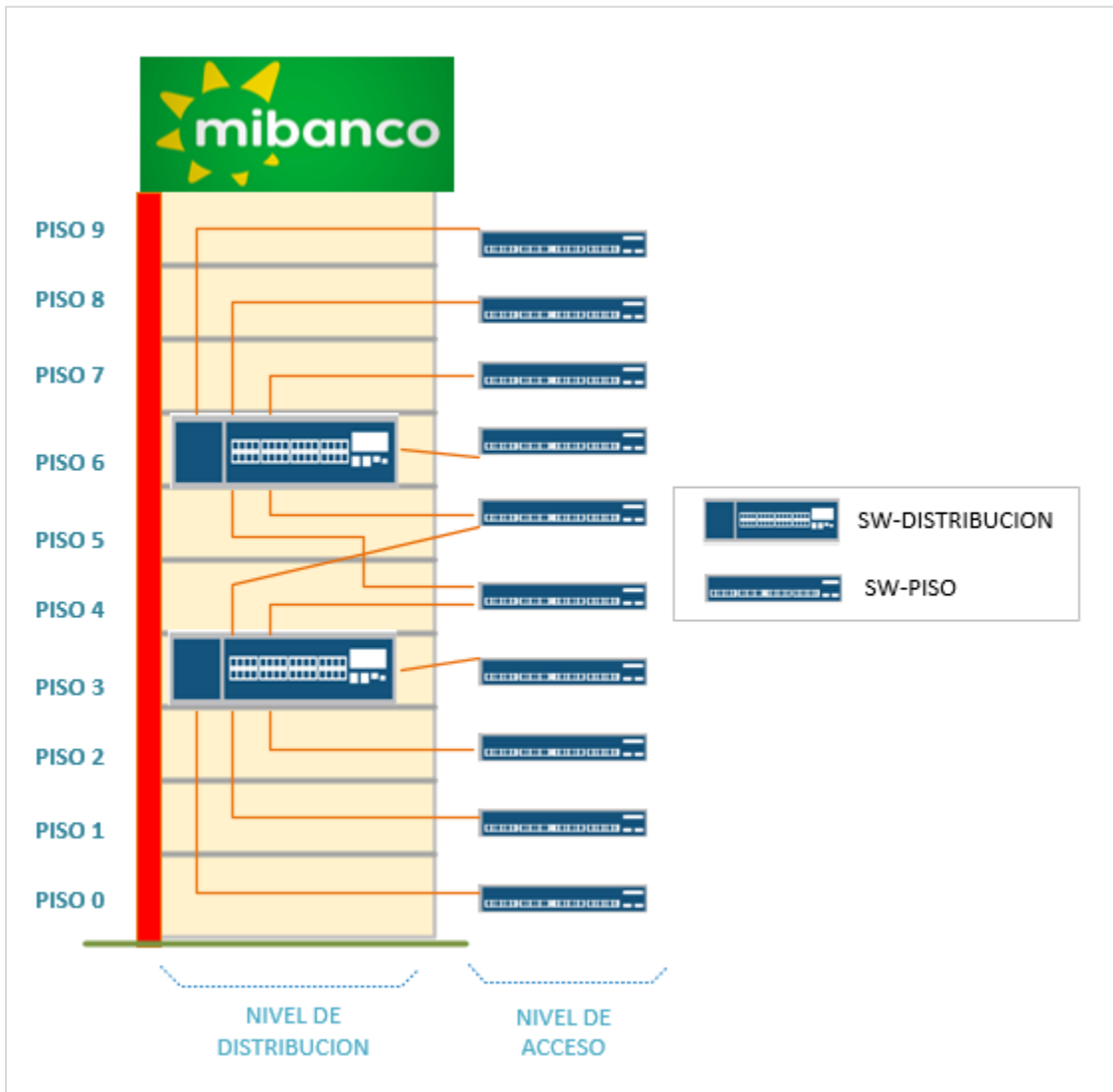


Figura N° 36: Mapa física de la ubicación de los Switches de Distribución y Acceso (pisos).

Fuente: Elaboracion propia, Mi Banco Sede San Isidro.

El diseño consiste en adicionar el nivel de Distribución e integrar alta disponibilidad con el protocolo LACP (Link Aggregation Control Protocol), virtualizando los switches de acceso.

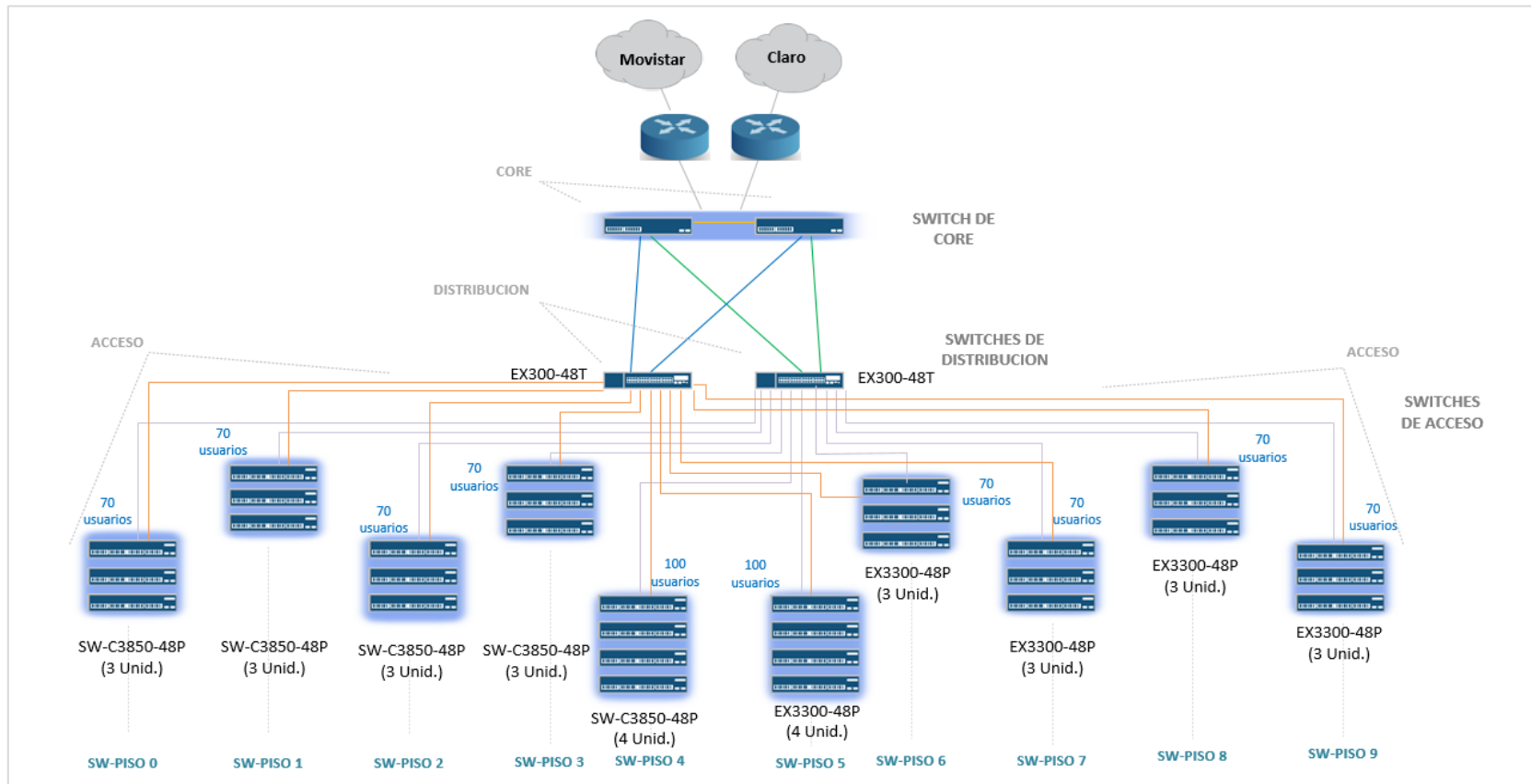


Figura N° 37: Topología Física de la solución en la Sede San Isidro.
Fuente: Elaboración propia, “Red LAN” Sede San Isidro.

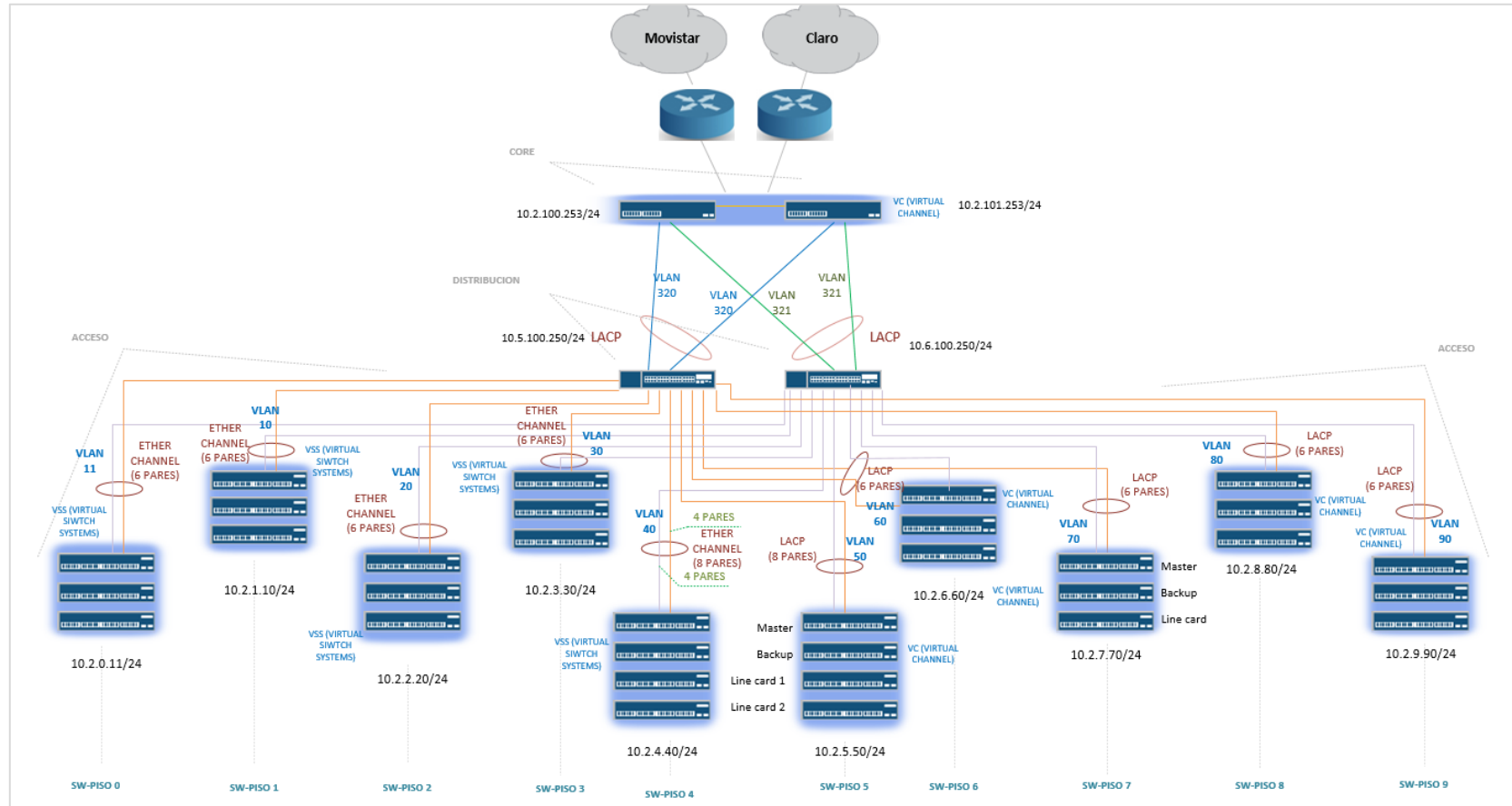


Figura N° 38: Topología Lógica de la solución en la Sede San Isidro.

Fuente: Elaboración propia, “Red LAN” Sede San Isidro.

Se tiene en cuenta la siguiente tabla N°14 para ejecutar la nueva configuración en base al diseño según a figura N°38.

Tabla N° 14: Asignación de puertos para la interconexión entre Nivel de Core, Nivel de Distribución y Nivel de Acceso.

Fuente: Elaboracion Propia, Mi Banco Sede San Isidro.

SWITCH	Cantidad de puertos	MARCA	PISO	Interface ACCESO	Interface CORE_1	Interface CORE_2	Interface DIST_1	Interface DIST_2
CORE	48	JUNIPER	04	--	--	VC	xe-0/0/46 xe-0/0/46	xe-0/0/47 xe-0/0/47
	48	JUNIPER	04	--	VC	--	xe-1/0/47 xe-0/0/47	xe-1/0/46 xe-0/0/46
DIST_1	48	JUNIPER	04	--	LACP(ae0)	LACP(ae0)	--	--
DIST_2	48	JUNIPER	07	--	LACP(ae1)	LACP(ae1)	--	--
PISO_0	48	CISCO	00	VSS	--	--	ge-1/46 ge-0/0/0	ge-1/47 ge-0/0/0
	48	CISCO	00	VSS	--	--	ge-2/46 ge-0/0/1	ge-2/47 ge-0/0/1
	48	CISCO	00	VSS	--	--	ge-3/46 ge-0/0/2	ge-3/47 ge-0/0/2
PISO_1	48	CISCO	01	VSS	--	--	ge-1/46 ge-0/0/3	ge-1/47 ge-0/0/3
	48	CISCO	01	VSS	--	--	ge-2/46 ge-0/0/4	ge-2/47 ge-0/0/4
	48	CISCO	01	VSS	--	--	ge-3/46 ge-0/0/5	ge-3/47 ge-0/0/5
PISO_2	48	CISCO	02	VSS	--	--	ge-1/46 ge-0/0/6	ge-1/47 ge-0/0/6
	48	CISCO	02	VSS	--	--	ge-2/46 ge-0/0/7	ge-2/47 ge-0/0/7
PISO_3	48	CISCO	03	VSS	--	--	ge-3/46 ge-0/0/8	ge-3/47 ge-0/0/8
	48	CISCO	03	VSS	--	--	ge-1/46 ge-0/0/9	ge-1/47 ge-0/0/9
PISO_4	48	CISCO	04	VSS	--	--	ge-2/46 ge-0/0/10	ge-2/47 ge-0/0/10
	48	CISCO	04	VSS	--	--	ge-3/46 ge-0/0/11	ge-3/47 ge-0/0/11
	48	CISCO	04	VSS	--	--	ge-1/46 ge-0/0/12	ge-1/47 ge-0/0/12
PISO_5	48	CISCO	04	VSS	--	--	ge-2/46 ge-0/0/13	ge-2/47 ge-0/0/13
	48	CISCO	04	VSS	--	--	ge-3/46 ge-0/0/14	ge-3/47 ge-0/0/14
	48	CISCO	04	VSS	--	--	ge-4/46 ge-0/0/15	ge-4/47 ge-0/0/15
PISO_6	48	JUNIPER	05	VC	--	--	ge-0/0/46 ge-0/0/16	ge-0/0/47 ge-0/0/16
	48	JUNIPER	05	VC	--	--	ge-1/0/46 ge-0/0/17	ge-1/0/47 ge-0/0/17
	48	JUNIPER	05	VC	--	--	ge-2/0/46 ge-0/0/18	ge-2/0/47 ge-0/0/18
	48	JUNIPER	05	VC	--	--	ge-3/0/46 ge-0/0/19	ge-3/0/47 ge-0/0/19
PISO_7	48	JUNIPER	06	VC	--	--	ge-0/0/46 ge-0/0/20	ge-0/0/47 ge-0/0/20
	48	JUNIPER	06	VC	--	--	ge-1/0/46 ge-0/0/21	ge-1/0/47 ge-0/0/21
	48	JUNIPER	06	VC	--	--	ge-2/0/46 ge-0/0/22	ge-2/0/47 ge-0/0/22
PISO_8	48	JUNIPER	07	VC	--	--	ge-0/0/46 ge-0/0/23	ge-0/0/47 ge-0/0/23
	48	JUNIPER	07	VC	--	--	ge-1/0/46 ge-0/0/24	ge-1/0/47 ge-0/0/24
PISO_9	48	JUNIPER	07	VC	--	--	ge-2/0/46 ge-0/0/25	ge-2/0/47 ge-0/0/25
	48	JUNIPER	08	VC	--	--	ge-0/0/46 ge-0/0/26	ge-0/0/47 ge-0/0/26
	48	JUNIPER	08	VC	--	--	ge-1/0/46 ge-0/0/27	ge-1/0/47 ge-0/0/27
PISO_10	48	JUNIPER	08	VC	--	--	ge-2/0/46 ge-0/0/28	ge-2/0/47 ge-0/0/28
	48	JUNIPER	09	VC	--	--	ge-0/0/46 ge-0/0/29	ge-0/0/47 ge-0/0/29
	48	JUNIPER	09	VC	--	--	ge-1/0/46 ge-0/0/31	ge-1/0/47 ge-0/0/31
PISO_11	48	JUNIPER	09	VC	--	--	ge-2/0/46 ge-0/0/32	ge-2/0/47 ge-0/0/32

3.2.2. Materiales y equipos para el funcionamiento del sistema

Para el diseño se necesitan:

DISTRIBUCION

- 2 Unidades de switch EX3300-48T Juniper
- 2 Módulos ópticos EX-SFP-10GE-USR para EX3300 Juniper
- 4 patch core de fibra LC MMF 10-20 metros

ACCESOS

- 16 Unidades de switch Cisco 3850-48P
- 16 Unidades de StackWise-480
- 16 Unidades de switch EX3300-48P Juniper
- 16 Unidades de EX-SFP-10GE-DAC-1M

ACCESORIOS

- Cable CAT 6 Panduit
- Conectores RJ45 CAT 6
- Unidades de pernos enjaulados
- Pernos y estoboles



Figura N° 39: EX3300-48P Juniper.

Fuente: Juniper Networks, “EX Series Switches”.



Figura N° 40: Cisco 3850-48P.

Fuente: Cisco Systems, “Switches Cisco, para la pequeña empresa”.



Figura N° 41: Transceiver EX-SFP-10GE.

Fuente: Juniper Networks, “Pluggable Transceivers Supported on EX Switches”.

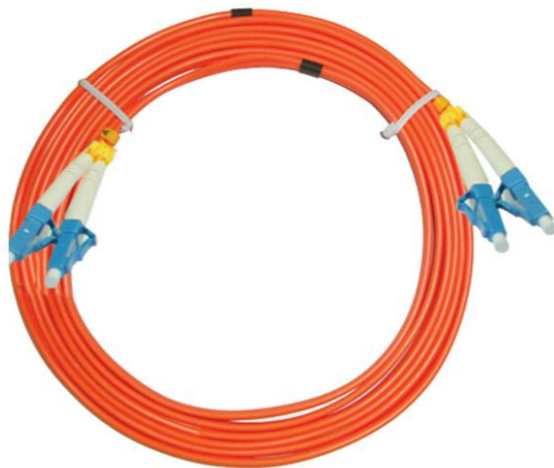


Figura N° 42: Patch core de fibra óptica LC-LC MMF.

Fuente: Cablematic, “Cable de fibra optica”.



Figura N° 43: Cable CAT 6 Panduit.

Fuente: Panduit, "Categoría 6 Shielded".



Figura N° 44: Conectores RJ45 CAT 6.

Fuente: Openetics, "Conector Cat. 6 UTP RJ45 para cable flexible".



Figura N° 45: Cable SFP+direct attach copper.

Fuente: Juniper Networks, "Cable SFP+direct attach copper. Cables for EX Series".



Figura N° 46: Estoboles + Pernos enjaulados.

Fuente: Satranet, "pernos enjaulados".

3.2.3. Configuración de switches de Núcleo, Distribución y Accesos

3.2.3.1. Configuración en el Switch-Core(Nodo/Núcleo)

- I. Configuración para establecer alta disponibilidad entre CORE y DISTRIBUCIÓN.

```
ge-0/0/46 {  
  ether-options {  
    802.3ad ae2;  
  }  
  
  ae2 {  
    mtu 1500;  
    aggregated-ether-options {
```



```
lACP {
  passive;
}
}
unit 0 {
  family inet {
    address 192.168.98.1/30;
  }
}
```

3.2.3.2. Configuración en el Switch de Distribución

I. Configuración para establecer alta disponibilidad entre switch de DISTRIBUCIÓN y switch CORE

```
interface Port-channel98
description TO-JUNIPER-L3-SWITCH-DIS-1
ip address 192.168.98.2 255.255.255.252
logging event spanning-tree status
logging event bundle-status
logging event trunk-status
load-interval 30

interface GigabitEthernet1/35
description TO-JUNIPER-L3-SWITCH -DIS-1
no ip address
logging event link-status
logging event spanning-tree status
logging event bundle-status
logging event trunk-status
load-interval 30
carrier-delay msec 0
channel-group 98 mode active
```

II. Configuración de LACP en los EX3300-48T

```
[edit chassis]
user@switch# show
aggregated-devices {
  ethernet {
    device-count 1;
  }
}
.....

[edit interfaces ae0]
```

```

user@switch# show
aggregated-ether-options {
  lACP {
    passive;
  }
}
unit 0 {
  family ethernet-switching {
    port-mode trunk;
    vlan {
      members [ GESTION DATOS ];
    }
  }
}
.....

[edit interfaces]
user@switch# show
...
xe-0/0/46 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/47 {
  ether-options {
    802.3ad ae0;
  }
}

```

III. La siguiente tabla forma parte de las antiguas distribuciones de los servicios:

Tabla N° 15: *Servicios descritos por cada VLAN que pertenecen a gestión en producción actual en el cliente.*

Fuente: Elaboracion propia, Mi Banco Sede Isidro.

ROUTED VLAN INTERFACE (RVI) – L3		
SW DISTRIBUCION		
VLAN 4	ENLACE_AGENCIAS	10.4.0.2/24
VLAN 7	AMERICATEL	10.7.0.250/24
VLAN 8	VLAN8	10.8.0.250/24
VLAN 11	PISO0	10.2.0.250/24
VLAN 10	PISO1	10.2.1.250/24
VLAN 20	PISO2	10.2.2.250/24

VLAN 30	PISO3	10.2.3.250/24
VLAN 40	PISO4	10.2.4.250/24
VLAN 50	PISO5	10.2.5.250/24
VLAN 60	PISO6	10.2.6.250/24
VLAN 70	PISO7	10.2.7.250/24
VLAN 71	TELAN	10.2.71.250/24
VLAN 74	PISO7	10.2.70.250/24
VLAN 80	PISO8	10.2.8.250/24
VLAN 90	PISO9	10.2.9.250/24
VLAN 100	SERVIDORES	10.2.0.250/24
VLAN 110	REPLICA_FO	10.100.0.250/24
VLAN 170	HEARTBEAT	192.168.0.250/24
VLAN 191	VMOTION	192.168.191.250/24
VLAN 200	SERV.EDYCOL	20.2.0.250/24
VLAN 231	CONT.EDYCOL	20.2.31.250/24
VLAN 240	DESA.EDYCOL	20.2.40.250/24
VLAN 280	QA.EDYCOL	20.2.80.250/24
VLAN 300	GESTION	10.2.31.250/24
VLAN 310	SOPORTE	10.2.31.250/24
VLAN 320	GESTION_RED	10.2.100.250/24
VLAN 400	DESARROLLO	10.2.40.250/24
VLAN 500	INVITADOS	10.2.50.250/24
VLAN 600	INVITADOS-WIRELESS	10.2.60.250/24
VLAN 610	INTERNOS-WIRELESS	10.2.61.250/24
VLAN 620	APS	10.0.62.250/24
VLAN 630	EXTERNOS_WIRELESS	10.2.63.250/24
VLAN 800	QA	10.2.80.250/24

Tabla N° 16: *Distribución de las direcciones IP de cada Switch de piso con la VLAN de teléfonos asociados.*

Fuente: Elaboracion propia, Mi Banco Sede Isidro.

PISOS	SERVICIO	VLAN	DIRECCIÓN IP
0	DATOS	10	10.2.0.11/24
	VOZ	71	10.2.71.11/24
1	DATOS	10	10.2.1.10/24
	VOZ	71	10.2.71.10/24

2	DATOS	20	10.2.2.20/24
	VOZ	71	10.2.71.20/24
3	DATOS	30	10.2.3.30/24
	VOZ	71	10.2.71.30/24
4	DATOS	40	10.2.4.40/24
	VOZ	71	10.2.71.40/24
5	DATOS	50	10.2.5.50/24
	VOZ	71	10.2.71.50/24
6	DATOS	60	10.2.6.60/24
	VOZ	71	10.2.71.60/24
7	DATOS	70	10.2.7.70/24
	VOZ	71	10.2.71.70/24
8	DATOS	80	10.2.8.80/24
	VOZ	71	10.2.71.80/24
9	DATOS	90	10.2.9.90/24
	VOZ	71	10.2.71.90/24

3.2.3.3. Configuración en el Switch de Acceso (Pisos)

- I. VSS (Virtual Switching Systems): Configuración y conexión de en los Switches 3850 para la activación de cada StackWise-480

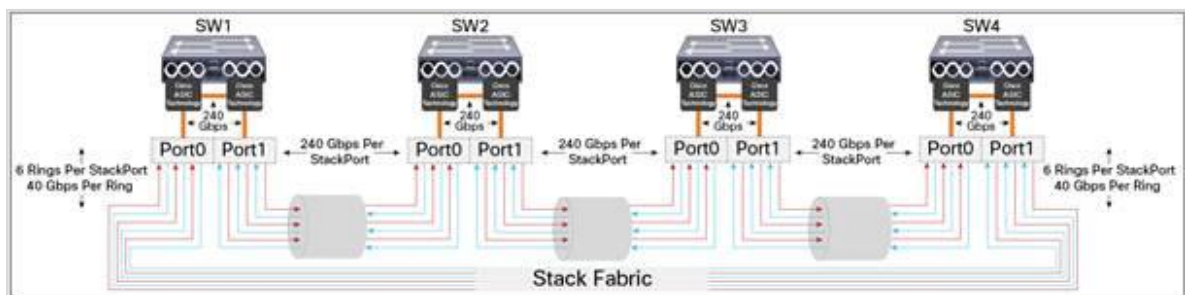


Figura N° 47: Conexión del Stackwise en los Switch Cisco 3850..

Fuente: Cisco Systems, “Stack Manager and High Availability, Cisco IOS EX (Catalyst 3850 Switches)”.

```
switch(config)# switch 1 priority 15
```

II. VC (Virtual chassis): Configuración y conexión de los cables DAC en cada Switch Juniper EX300-48P en cada Switch Juniper EX300-48P

Haciendo uso de los DAC(figura 42) se realizan las siguientes conexiones de las cuales se deben respetar cada conexión de dichos cables.

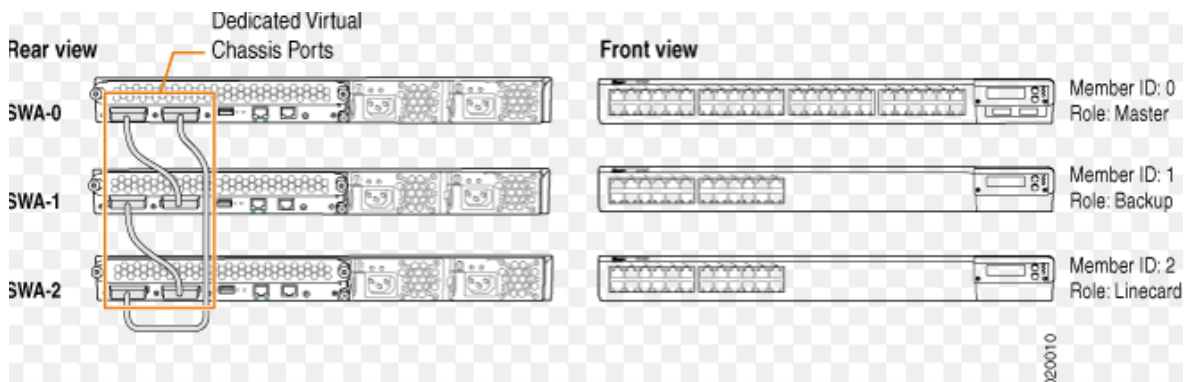


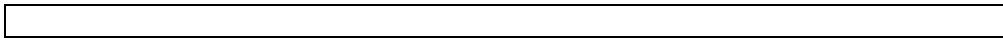
Figura N° 48: Conexión de Virtual Chassis con cable DAC en anillos.

Fuente: Juniper Networks, “Understanding EX Series Virtual Chassis Components”.

Proceso recomendado:

- i. Instalar el Switch Master deseada
- ii. Encienda Switch Master de conmutación se convierte en maestro y obtiene miembro-id 0
- iii. Asignar prioridad maestría (255)

```
[edit virtual-chassis]
user@switch# show
member 0 {
    mastership-priority 255;
}
```



- iv. Añadir Switch de Backup deseada
- v. Conectarse al Master haciendo uso de cable DAC
- vi. Encienda Switch de Backup deseada asignando el miembro id-1
- vii. Asignar mastership priority (254)

```
[edit virtual-chassis]
user@switch# show
member 0 {
  mastership-priority 255;
}
member 1 {
  mastership-priority 254;
}
```

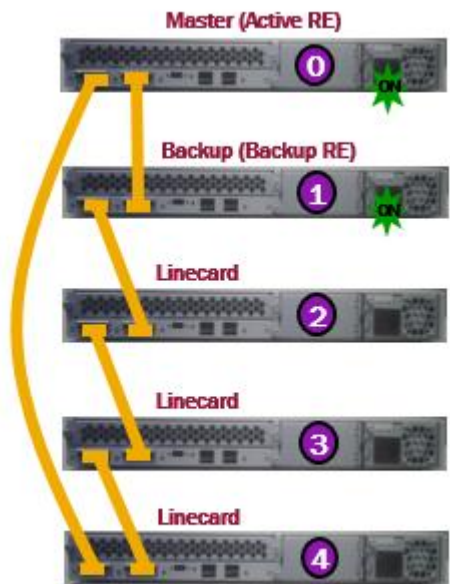


Figura N° 49: Conexión de Switch Master y Switch Backup - (1).

Fuente: Juniper Networks, “Understanding EX Series Virtual Chassis Components”.

- viii. Añadir Switch line card

- ix. Conectar al Switch de encima con el cable DAC
- x. Encender Switch - Switch que convierte line card y es asignado con miembro-id 2
- xi. Asignar prioridad deseada al Master
- xii. Repetir el paso iii para agregar un siguiente Switch line card
- xiii. Switch Line card complete el anillo de conexión con el Master

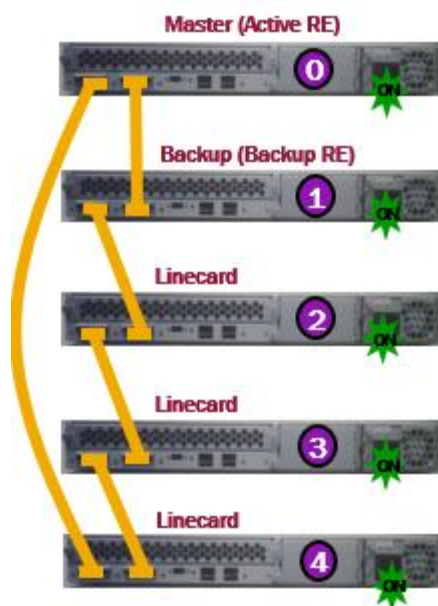


Figura N° 50: Conexión de Switch Master y Switch Backup - (2).

Fuente: Juniper Networks, “Understanding EX Series Virtual Chassis Components”.

- III. Configuración de BPDU protection en cada Switch de acceso Cisco y Juniper

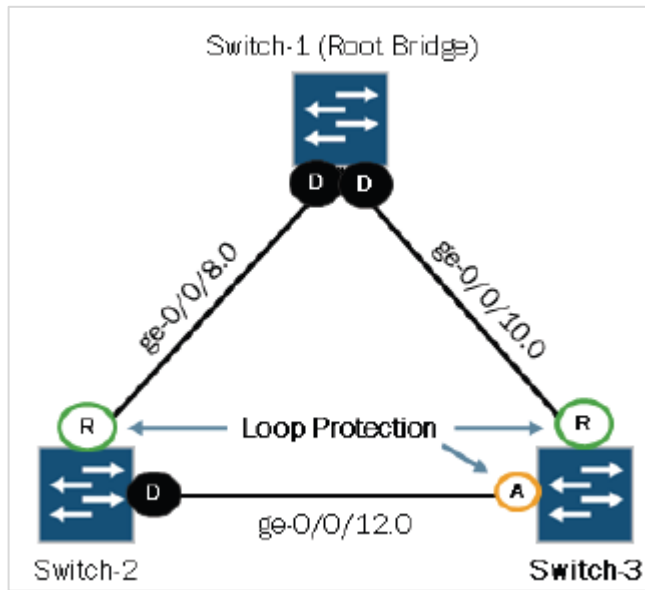


Figura N° 51: Topología de red para BPDU Protection.

Fuente: Juniper Networks, “Configuring BPDU Protection on an Interface”.

```
switch(config)# show running-config interface Ge1/36
..
Spanning-tree portfast
Spanning-tree bpduguard enable
...
```

```
[edit protocol rstp]
Switch# show
Interface ge-0/0/45.0 {
  bpdu-timeout-action {
    Block;
  }
}
Interface ge-0/0/46.0 {
  bpdu-timeout-action {
    Block;
  }
}
```


IV. Configuración de port security

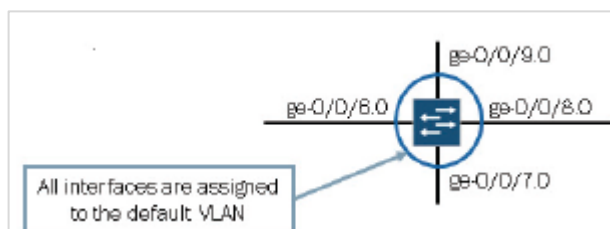


Figura N° 52: Esquema de la descripción de interfaces del Port Security.

Fuente: Juniper Networks, "Configuring Basic Port Security Features".

```
Switch-piso# config terminal
Switch-piso(config)# interface GigabitEthernet 1/24
Switch-piso(config-if)# switchport mode access
Switch-piso(config-if)#switchport port-security
Switch-piso(config-if)#switchport port-security maximum 1
Switch-piso(config-if)# switchport port-security violation shutdown
Switch-piso(config-if)# switchport port-security mac-address 0a04.aaf8.13ad
Switch-piso(config-if)# end
```

```
[edit Ethernet-switching-options]
Switch# show
Secure access-port{
  Interface ge-0/0/24.0{
    Allowed-mac [00:26:88:02:74:85 00:26:88:02:74:86];
  }
  Interface ge-0/0/25.0{
    Mac-limit 2 action drop;
  }
  Interface all {
    Mac-limit 1 action shutdown;
  }
  Vlan default {
    Mac-move-limit 1 action shutdown;
  }
}
```

V. Configuración de vlans

```
Switch-piso#configure terminal
Switch-piso(config)#interface Vlan2
Switch-piso(config-if)#ip address 10.1.2.1 255.255.255.0
Switch-piso(config-if)#no shutdown
.....
Switch-piso(config)#interface Ge1/21
Switch-piso(config-if)#no switchport
Switch-piso(config-if)#ip address 200.1.1.1 255.255.255.0
Switch-piso(config-if)#no shutdown
```

```
vlans {
  GESTION {
    vlan-id 300;
  }
  GESTION_RED {
    vlan-id 320;
    I3-interface vlan.320;
  }
}
.....
interfaces {
  vlan {
    unit 320 {
      description "IP DE GESTION";
      family inet {
        address 10.2.100.22/24;
      }
    }
  }
}
```

Los puntos importantes del diseño son:

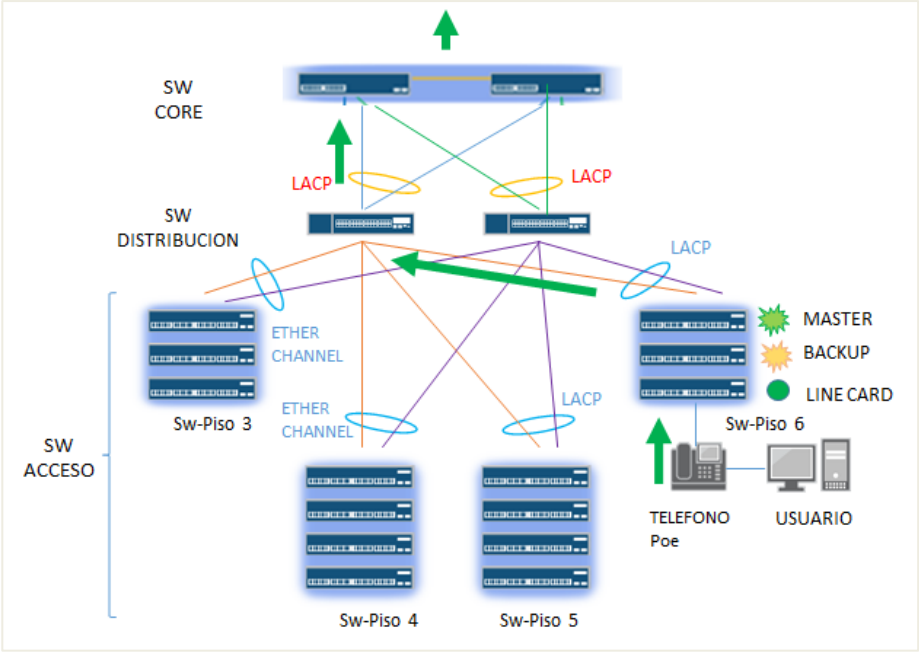
- Llevar todo a capa 3 para evitar bucles de tráfico ante una avería.
- LACP , características de alta disponibilidad
- Port Security
- BPDU protection
- Device Security

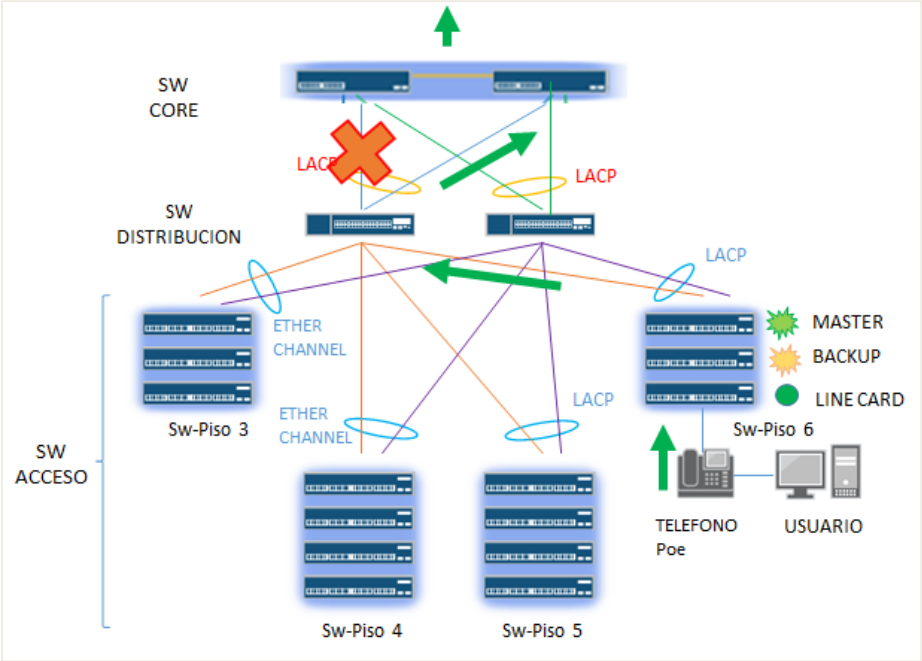
3.3. Revisión y consolidación de resultados

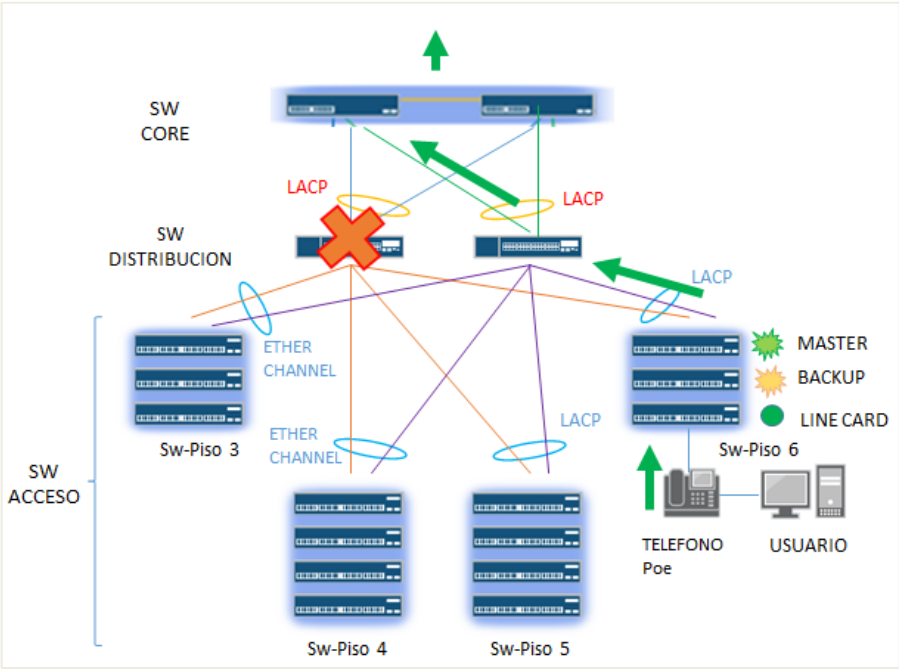
A continuación se muestra el protocolo de pruebas del funcionamiento de alta disponibilidad del diseño.

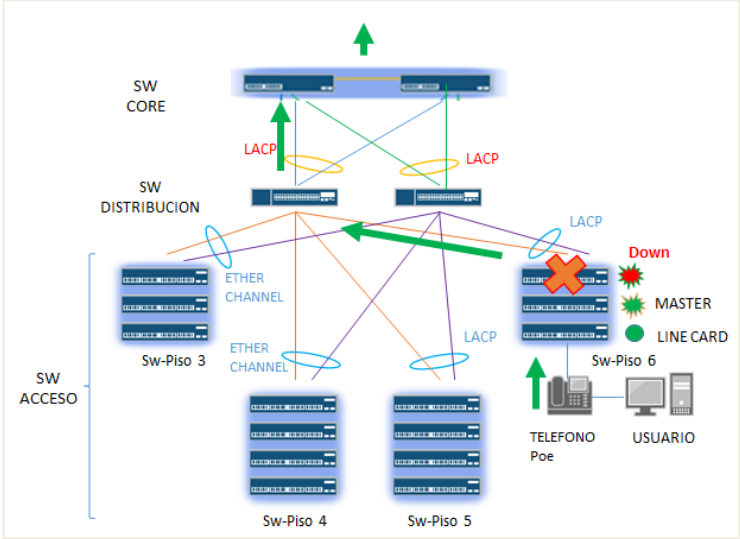
3.3.1. Protocolo de pruebas

A continuación se muestra los resultados de los distintos escenarios que se presentarán ante una avería en los equipos de red:

Escenario	Descripción:	Flujo de Tráfico	Resultado	Observaciones
Escenario 0	<p>Se tiene un bosquejo de la topología final con el equipos de la solución.</p>  <p>The diagram illustrates a three-tier network architecture. At the top is the SW CORE. Below it is the SW DISTRIBUCION layer, which consists of two switches connected to the core via LACP. The bottom layer is SW ACCESO, which includes Sw-Piso 3, Sw-Piso 4, Sw-Piso 5, and Sw-Piso 6. Sw-Piso 3 and Sw-Piso 4 are connected to the distribution switches via Ether Channels. Sw-Piso 5 and Sw-Piso 6 are also connected via LACP. Sw-Piso 6 is further connected to a TELEFONO Poe and a USUARIO. A legend indicates that Sw-Piso 6 has a MASTER BACKUP role and a LINE CARD. A large green arrow points from the core towards the distribution and access layers, indicating the direction of traffic flow.</p>	CORE >> DISTRI>> ACCESO	ok	Tráfico adecuado para la transmisión y recepción de los servicios.

Escenario	Descripción:	Flujo de Tráfico	Resultado	Observaciones
Escenario 1	<p>Para validar los servicios y aplicativos, se procederá a cortar el enlace mediante el retiro de la conexión de uno de los cables en LACP, se procederá a verificar que no se pierda la navegación.</p>  <p>Luego de validado el punto anterior, se volverá a conectar el cable retirado y se probará nuevamente el servicio.</p>	CORE >> DISTRI > > ACCESO	ok	Tráfico adecuado para la transmisión y recepción de los servicios.

Escenario	Descripción:	Flujo de Tráfico	Resultado	Observaciones
Escenario 2	<p>Para validar los servicios y aplicativos, se procederá a cortar el enlace mediante el retiro de la conexión del equipo, se procederá a verificar que no se pierda la navegación</p>  <p>Luego de validado el punto anterior, se volverá a conectar el switch y se probará nuevamente el servicio.</p>	CORE >> DISTRI>> ACCESO	ok	Tráfico adecuado para la transmisión y recepción de los servicios.

Escenario	Descripción:	Flujo de Tráfico	Resultado	Observaciones
Escenario 3	<p>Parta validar la funcionalidad del Master y Backup de los switches, se procederá a cortar el servicio del Switch Master, se procederá a verificar que no se pierda la navegación</p>  <p>Luego de validado el punto anterior, se volverá a encender el Switch Master y se probará nuevamente el servicio.</p>	CORE >> DISTRI>> ACCESO	ok	Tráfico adecuado para la transmisión y recepción de los servicios.

3.3.2. Estimación de resultados

Se estima que durante los cambios y pruebas de alta disponibilidad del diseño esta no presente un mayor impacto sobre los servicios que están en uso por los usuarios.

3.3.3. Factor de disponibilidad actual del Sistema

Los niveles de la red LAN de Mi Banco actual son el nivel de Core y nivel de acceso; de las cuales solo el Nivel de Core tiene contingencia ó respaldo pero el Nivel de Acceso no tiene respaldo ante un corte por averia en el servicio.

Ante una Falla fisica en el nivel de acceso, Mi Banco no tendra servicio para los usuarios afectados.

3.3.3.1. Puntos de Falla

- SWICTHES DE PISO, los accesos de cada piso no tienen equipo de respaldo por ello ante una incidencia no contarán con servicio.

3.3.4. Tiempo promedio de recuperacion despues de una falla

Como propuesta de diseño se ofrecera disponibilidad al 100% (ver figura n° 53).

Ante una falla en su enlaces principales del diseño elaborado.

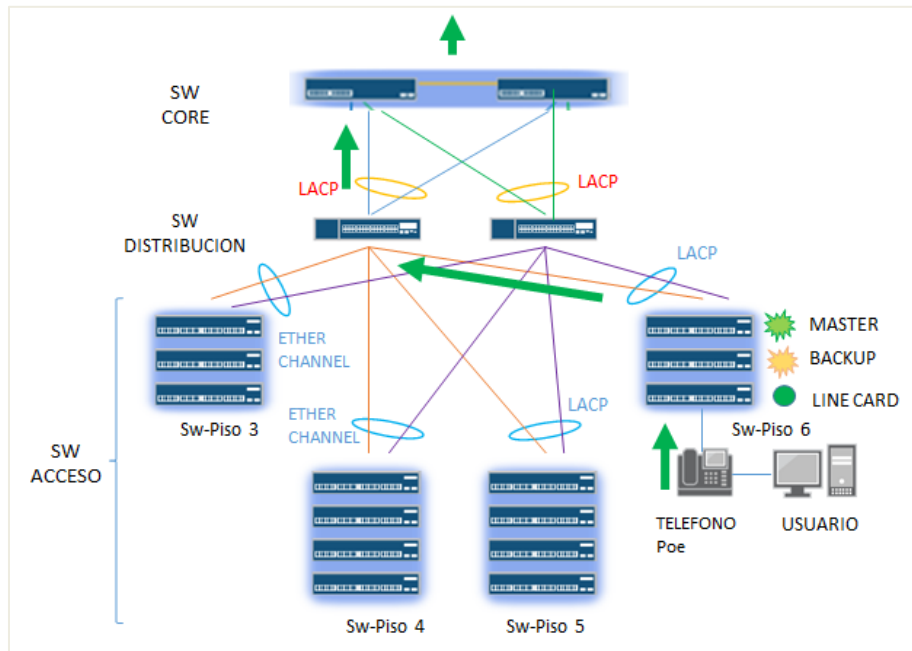


Figura N° 53: Ruta del trafico en la red LAN desde los puntos finales.

Fuente: Elaboracion propia, proyecto de Diseño con alta disponibilidad.

3.3.4.1. Tiempo de Recuperacion por Niveles

- Nivel de distribucion: Los switches estan en activo-activo asi que el tiempo de recuperacion sera al 100%, inmediato.
- Nivel de acceso: Los switches de piso tienen los swicches de respaldo en Standby, asi que ante un evento o averia la conmutacion luego de tener problemas con el switch principal y que el switch en stanby trabaje como principal sera al 99.9%, es decir solo se tenga 4 paquetes perdidos en a conmutacion (ver Figura n°54).

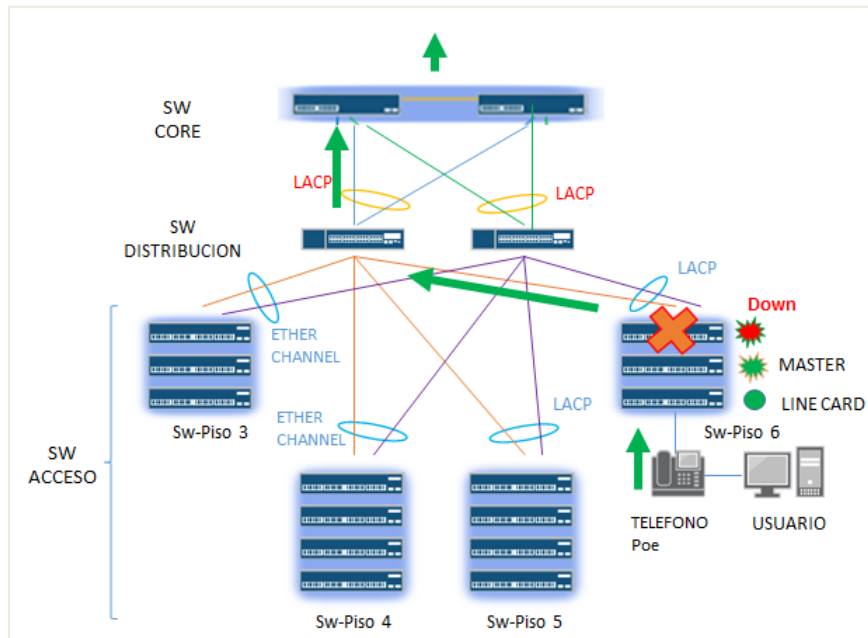


Figura N° 54: Conmutacion Swieth Principal con Switch Backup.

Fuente: Elaboracion propia, proyecto de Diseño con alta disponibilidad

3.3.4.2. Tiempo de Recuperacion del Switch principal averiado

Esta asociado al tiempo de inicio de reporte de averia por parte del cliente Mi Banco. Según manejo del tiempo de reparacion de averia:

- Inicio de averia: cliente reporta a soporte del servicio.
- Reparacion de equipo averiado: consiste en reparar temas de actualizacion software del equio, equipo de reemplazo,cable de alimentacion, tarjeta de red,etc.
- Fin de averia: servicio estable.

El tiempo sera según el tiempo de reparacion bajo contrato.

CONCLUSIONES

- a) Se realizó el análisis y diagnóstico de la red existente en Mi Banco Sede San Isidro y que permitió identificar los requerimientos de cambio y optimización de la red LAN tanto en infraestructura como servicios de datos, voz, etc.
- b) Se realizó el diseño y se planteó las especificaciones de la nueva red LAN, topología, equipamiento, configuración, en base al diagnóstico previo y los nuevos requerimientos que necesita el cliente y que se detallan en las secciones del 3.2.1 del capítulo 3.
- c) Se integró en la red diseñada los métodos de seguridad que consisten en las características del BPDU Protection y Port Security para los equipos Cisco y Juniper y que brindara una protección al 100% en los servicios de datos.
- d) Se verificó mediante la aplicación del protocolos de pruebas descrito en la sección 3.3 del capítulo 3, que la red LAN funciona adecuadamente en los distintos escenarios que podrían presentarse, según muestra los resultados de la sección 3.3.1 del protocolo de pruebas.

RECOMENDACIONES

- a) Se estima un alto costo en la adquisición de los nuevos equipos que tendrán para la implementación respecto al diseño realizado. Se recomienda que el cliente tenga un cuadro de costos de determinados periodos para su adquisición y solicitar las cotizaciones en detalle y la aplicación de descuentos.
- b) Establecer los puntos indicados como problemas específicos del capítulo 1 para mejorar el servicio de comunicación de Mi Banco.
- c) Para efectos de simplificar los bucles que se están presentado en la red en determinadas situación ante una saturación en el ancho de banda, para lo cual se recomienda el uso de los protocolos de seguridad en todos los puertos libres de cada equipo de red.
- d) Para posibles escenarios de las incidencias que puedan presentar los equipos Master en determinados niveles de jerarquía de la red, se recomienda el reporte hacia su soporte de servicios para la habilitación y recuperación de la alta disponibilidad brindada.

BIBLIOGRAFÍA

- Cisco Systems. (2015). Cisco Catalys 3850 Series Switches StackWise-480 Architecture. Recuperado de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3850-series-switches/white-paper-c11-734429.html#_Toc417362562
- Juniper Networks. (2016). Pluggable Transceivers Supported on EX3300 Switches. Recuperado de http://www.juniper.net/techpubs/en_US/release-independent/junos/topics/reference/specifications/optical-interface-ex3300-support.html
- Juniper Networks. (2016). SFP+ Direct Attach Copper Cables for EX Series Switches. Recuperado de http://www.juniper.net/documentation/en_US/release-independent/junos/topics/reference/general/cable-ex-series-sfp-plus-direct-attach.html
- Molina Ruiz, J. (2012). Propuesta de Segmentación con Redes Virtuales y Priorización del Ancho de Banda con QoS para la mejora del Rendimiento y Seguridad de la Red Lan en la Empresa Editora El Comercio Planta Norte. (Trabajo de Tesis). Recuperada de http://tesis.usat.edu.pe/jspui/bitstream/123456789/77/1/TL_Molina_Ruiz_Julio.pdf

ANEXOS

- Switch_EX300 JUNIPER_DATASHEET
- Switch_3850_CISCO_DATASHEET

EX3300 Ethernet Switch

Entry-Level Access Switch with Virtual Chassis Technology



Product Overview

Juniper Networks EX3300 switch delivers a high-performance, flexible and cost-effective solution for today's most demanding converged data, voice, and video enterprise access environments. It supports Juniper Networks Virtual Chassis technology, allowing up to 10 switches to be interconnected over uplink ports and managed as a single logical device to deliver a scalable, pay-as-you-grow solution for expanding network environments.

Product Description

The Juniper Networks® EX3300 Ethernet Switch with Virtual Chassis technology provides enterprises with the flexibility and ease of management that previously was only available with higher end access switches. The fixed configuration EX3300 supports a number of key features:

- 24-port and 48-port models with and without Power over Ethernet (PoE) for campus wiring closet deployments
- Data center-optimized cooling options, which offer both front-to-back and back-to-front airflows, and make the EX3300 suitable for GbE data center access deployments
- 24-port data center models for metro deployments
- Four dual-mode (GbE/10GbE) small form-factor pluggable transceiver (SFP/SFP+) uplink ports
- Uplink ports that can be configured as Virtual Chassis interfaces and connected via standard GbE/10GbE optics interfaces (the last two uplink ports are preconfigured by default as Virtual Chassis ports)
- Comprehensive Layer 2 functionality with RIP and static routing
- Compact, 12-inch deep 1 U form factor to enable flexible deployment options
- Easy-to-manage solution with centralized software upgrades and a single management interface, along with an LCD for managing Virtual Chassis configurations
- Same consistent modular Juniper Networks Junos® operating system control plane feature implementation as other fixed configuration switches in the Juniper Networks EX Series Ethernet Switch product family
- Layer 3 (OSPF v2, IGMP v1/v2/v3, PIM, VRRP, Q-in-Q, BFD, Virtual Router) supported via enhanced feature license
- BGP and MBGP supported via advanced feature license
- IPv6 management support, including neighbor discovery, stateless auto configuration, telnet, SSH, DNS, syslog, NTP, ping, traceroute, ACL, CoS static routing and RIPng
- IPv6 routing features (OSPFv3, virtual router support for unicast, VRRPv6, PIM, MLDv1/v2) supported via enhanced feature license
- Additional IPv6 routing features (BGP and MBGP) supported via advanced feature license

Your ideas. Connected.™

* Input power without PoE

Table 1: EX3300 Models

SKU	Total 10/100/1000 Ports	Uplinks	Airflow	Power Supply Type	PoE+ Power Budget (W)	Max. System Power Consumption (W)*
EX3300-24T	24	4 dual-mode 10GbE/GbE SFP+/SFP ports	Front-to-back	AC	0	51
EX3300-48T	48		Front-to-back	AC	0	73
EX3300-48T-BF	48		Back-to-front	AC	0	73
EX3300-24P	24 PoE+		Front-to-back	AC	405	65
EX3300-48P	48 PoE+		Front-to-back	AC	740	81
EX3300-24T-DC	24		Front-to-back	DC	0	49

Virtual Chassis Technology

The EX3300 supports Juniper Networks Virtual Chassis technology, allowing up to 10 switches to be interconnected over uplink ports and be managed as a single logical device, delivering a scalable, pay-as-you-grow solution for expanding network environments.

When deployed in a Virtual Chassis configuration, the EX3300 switches elect a master and backup switch based on a set of criteria or preconfigured policies. The master switch automatically creates and updates the switching and optional routing tables on all switches in the Virtual Chassis configuration. Virtual Chassis technology allows switches to be added or removed without service disruption. An EX3300 Virtual Chassis configuration operates as a highly resilient unified system, providing simplified management using a single IP address, single telnet session, single command-line interface (CLI), automatic version checking, and automatic configuration. The EX3300 switches are also capable of local switching, so that packets coming into a port destined for another port on the same switch do not have to traverse the Virtual Chassis, increasing the forwarding capacity of the switch.

The EX3300 implements the same slot/module/port numbering schema as other Juniper Networks chassis-based products when numbering Virtual Chassis ports, providing true chassis-like operations. By using a consistent operating system and a single configuration file, all switches in a Virtual Chassis configuration are treated as a single device, simplifying overall system maintenance and management.

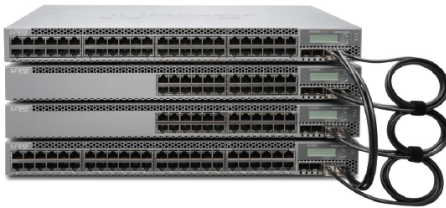


Figure 1: EX3300 Virtual Chassis connections

The last two uplink ports on the EX3300 front panel are configured by default as Virtual Chassis ports, automating Virtual Chassis deployments when these ports are connected using

standard 10GbE SFP+ or GbE SFP transceivers (sold separately). These two ports can also be configured as GbE or 10GbE uplinks to aggregation devices by disabling Virtual Chassis technology.

Converged LAN Environments

The EX3300 switches provide a flexible solution for demanding converged data, voice, and video environments. The EX3300-24P and EX3300-48P support the IEEE 802.3at Power over Ethernet (PoE) standard, also known as PoE+, delivering up to 30 watts of power per port to support networked devices such as telephones, video cameras, IEEE 802.11n wireless LAN (WLAN) access points, and video phones. The PoE+ standard provides nearly double the 15.4 watts per port available with the IEEE 802.3af PoE standard.

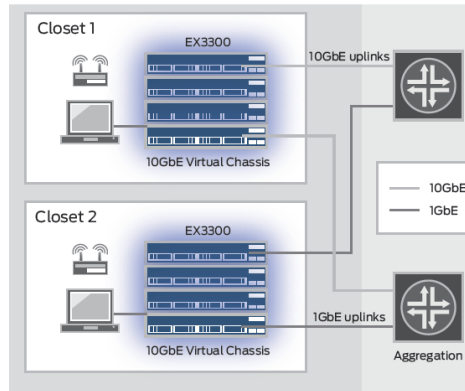


Figure 2: EX3300 campus wiring closet deployments

The EX3300-48P includes a total PoE power budget of 740 watts, enabling the switch to provide the full 15.4 watts of 802.3af Class 3 PoE to all 48 ports, or the full 30 watts of PoE+ to 24 ports. The switch can support any combination of PoE and PoE+ ports until the maximum PoE power budget of 740 watts is exhausted.

The EX3300-24P includes a total power budget of 405 watts, enabling the switch to provide the full 15.4 watts of PoE power to all 24 ports, or the full 30 watts of PoE+ to 13 attached devices. The switch can support any combination of PoE and PoE+ ports until the maximum PoE power budget of 405 watts is exhausted.

Table 2: EX3300 PoE Power Budgets

SKU	Total 10/100/1000 Ports	Total 30 W PoE+ Ports That Can Be Enabled	Total 15.4 W PoE Ports That Can Be Enabled	Power Supply Type	PoE+ Power Budget (W)
EX3300-24T	None	0	0	AC	0
EX3300-48T	None	0	0	AC	0
EX3300-48T-BF	None	0	0	AC	0
EX3300-24P	24	13 ports up to 30 W	24 ports up to 15.4 W	AC	405
EX3300-48P	48	24 ports up to 30 W	48 ports up to 15.4 W	AC	740
EX3300-24T-DC	None	0	0	DC	0

There are two PoE power mode settings on the EX3300 switches:

- **Static mode**, which allows customers to specify the maximum PoE power setting on an individual port
- **Class mode**, which allows end devices to specify PoE class and negotiate whether the switch can provide PoE power to the device

The EX3300 also supports the industry-standard Link Layer Discovery Protocol (LLDP) and LLDP-Media Endpoint Discovery (LLDP-MED), which enable the switches to automatically discover Ethernet-enabled devices, determine their power requirements, and assign virtual LAN (VLAN) parameters. LLDP-MED-based granular PoE management allows the EX3300 to negotiate PoE usage down to a fraction of a watt on powered devices, enabling more efficient PoE utilization across the switch.

The EX3300 supports the Institute of Electrical and Electronics Engineers (IEEE) 802.3az standard for Energy Efficient Ethernet (EEE) functionality, reducing power consumption of copper physical layers (PHY) during periods of low link utilization.

In addition, the EX3300 supports rich quality-of-service (QoS) functionality for prioritizing data, voice, and video traffic. The switches support eight QoS queues on every port, enabling them to maintain multilevel, end-to-end traffic prioritization. The EX3300 also supports a wide range of scheduling options, such as priority and shaped deficit weighted round-robin (SDWRR) scheduling.

An optional enhanced license for supporting additional L3 protocols such as OSPF, Internet Group Management Protocol (IGMP v1/v2/v3), and Protocol Independent Multicast (PIM) will be supported in future. An external redundant power system (RPS) delivering additional power resiliency is also available.

Data Center Gigabit Ethernet Server Access

The EX3300 switches are optimized for GbE server access deployments in the data center, with front-to-back and back-to-front cooling. The four SFP+ uplink ports on the EX3300 can operate at 10 Gbps simultaneously, offering up to 20GbE of uplink connectivity to each of the dual aggregation switches.

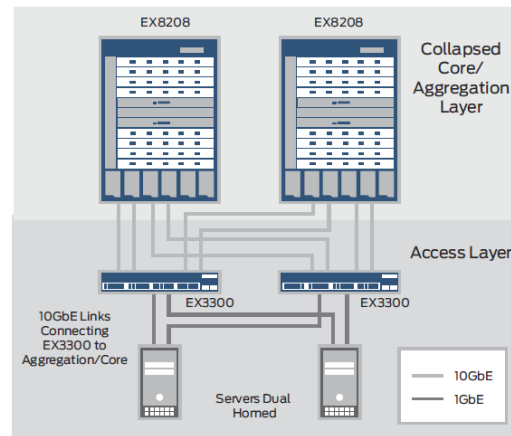


Figure 3: Data center top-of-rack deployments

Security

The EX3300 switches fully interoperate with Juniper Networks Unified Access Control, which consolidates all aspects of a user's identity, device, and location, enabling administrators to enforce access control and security down to the individual port or user levels. Working as an enforcement point within the UAC, the EX3300 provides both standards-based 802.1X port-level access control and Layer 2-4 policy enforcement based on user identity, location, and/or device. A user's identity, device type, machine posture check, and location can be used to not only grant or deny access but also to determine the duration of access. If access is granted, the switch assigns the user to a specific VLAN based on authorization levels. The switch can also apply QoS policies or mirror user traffic to a central location for logging, monitoring, or threat detection by intrusion prevention systems (IPS).

The EX3300 also provides a full complement of port security features, including Dynamic Host Configuration Protocol (DHCP) snooping, dynamic ARP inspection (DAI), and media access control (MAC) limiting to defend against internal and external spoofing, man-in-the-middle, and denial-of-service (DoS) attacks.

Junos Operating System

The EX3300 switches run the same Junos OS used by other EX Series Ethernet Switches, as well as Juniper routers and Juniper Networks SRX Series Services Gateways. By utilizing a common operating system, Juniper delivers a consistent implementation and operation of control plane features across all products. To maintain that consistency, Junos OS adheres to a highly disciplined development process that uses a single source code, follows a single quarterly release train, and employs a highly available modular architecture that prevents isolated failures from bringing an entire system down.

These attributes are fundamental to the core value of the software, enabling all Junos OS-powered products to be updated simultaneously with the same software release. All features are fully regression tested, making each new release a true superset of the previous version; customers can deploy the software with complete confidence that all existing capabilities will be maintained and operate in the same way.

High Availability

The EX3300 line of Ethernet switches is designed to support many of the same failover capabilities and high availability (HA) functionality as the Juniper Networks EX4200 line of Ethernet switches with Virtual Chassis technology.

Each EX3300 switch is capable of functioning as a Routing Engine when deployed in a Virtual Chassis configuration. When two or more EX3300 switches are interconnected in a Virtual Chassis configuration, all member switches share a single control plane. Junos OS automatically initiates an election process to assign a master (active) and backup (hot-standby) Routing Engine. An integrated Layer 2 and Layer 3 graceful Routing Engine switchover (GRES) feature maintains uninterrupted access to applications, services, and IP communications in the unlikely event of a master Routing Engine failure.

When more than two switches are interconnected in a Virtual Chassis configuration, the remaining switch elements act as line cards and are available to assume the backup Routing Engine position should the designated master fail. Master, backup and line card priority status can be assigned by the network operations team to dictate the order of ascension. This N+1 Routing Engine redundancy, coupled with GRES, the nonstop routing (NSR) and, in the future, the nonstop bridging (NSB) capabilities of Junos OS, ensures a smooth transfer of control plane functions following unexpected failures.

The EX3300 also supports the following HA features:

- Redundant trunk group: To avoid the complexities of Spanning Tree Protocol (STP) without sacrificing network resiliency, the EX3300 employs redundant trunk groups to provide the necessary port redundancy and simplify switch configuration.
- Cross-member link aggregation: Cross-member link aggregation allows redundant link aggregation connections

between devices in a single Virtual Chassis configuration, providing an additional level of reliability and availability.

- Non-Stop Bridging (NSB) and Non-stop Routing (NSR): NSB and NSR on the EX3300 switch ensure control plane protocols, states and tables are synchronized between master and backup REs to prevent protocol flaps or convergence issues following a Routing Engine failover.
- Non-Stop Software Upgrade (NSSU): With NSSU, all members of an EX3300 Virtual Chassis configuration can be upgraded with a single command. Mission-critical traffic can be configured as a link aggregate across multiple Virtual Chassis switch members, ensuring minimal disruption during the upgrade process.

Simplified Management and Operations

When deployed in a Virtual Chassis configuration, the EX3300 dramatically simplifies network management. Up to 10 interconnected EX3300 switches can be managed as a single device utilizing a single Junos OS image file and a single configuration file, reducing the overall number of units to monitor and manage. When the Junos OS is upgraded on the master switch in an EX3300 Virtual Chassis configuration, the software is automatically upgraded on all other member switches at the same time.

The EX3300 includes port profiles that allow network administrators to automatically configure ports with security, QoS, and other parameters based on the type of device connected to the port. Six preconfigured profiles are available, including default, desktop, desktop plus IP phone, WLAN access point, routed uplink, and Layer 2 uplink. Users can select from the existing profiles or create their own and apply them through the command-line interface (CLI), J-Web Software interface, or Junos Space network management system.

In addition, a feature called System Snapshot makes a copy of all software files used to run the switch, including the Junos operating system, the active configuration and the rescue configuration, that can be used to reboot the switch at the next power-up or as a backup boot option. The Junos OS software can also be preinstalled on a flash drive and used to boot the EX3300 at any time.

Another feature, called automatic software download, enables network administrators to easily upgrade the EX3300 using the DHCP message exchange process to download and install software packages. Users simply configure the automatic software download feature on EX3300 switches acting as DHCP clients and establish a path to the server where the software package file is installed. The server then communicates the path to the software package file through DHCP server messages.

An EZ touchless provisioning feature allows a DHCP server to push configuration details and software images to multiple switches at bootup.

Three system management options are available for the EX3300 line. The standard Junos OS CLI management interface offers the same granular capabilities and scripting parameters found in any router powered by the Junos operating system. The EX3300 also includes the integrated J-Web interface, an embedded web-based device manager that allows users to configure, monitor, troubleshoot, and perform system maintenance on individual switches via a browser-based graphical interface.

Finally, EX3300 fault, configuration and performance data can be exported to leading third-party management systems such as HP OpenView, IBM Tivoli, and Computer Associates Unicenter software, providing a complete, consolidated view of network operations.

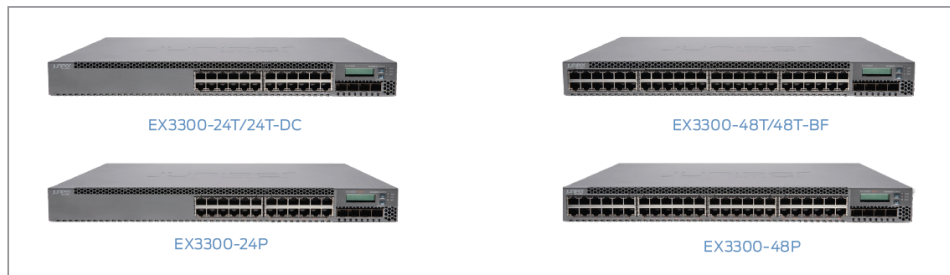
Warranty

For warranty information, please visit www.juniper.net/support/warranty/.

Product Options

Table 3: EX3300 Product Options

SKU	Access Ports	PoE+ Ports	Airflow	Power Supply Type	PoE+ Power Budget (W)	Power Supply Rating (W)
EX3300-24T	24-port 10/100/1000BASE-T	None	Front-to-back	AC	0	100
EX3300-48T	48-port 10/100/1000BASE-T	None	Front-to-back	AC	0	100
EX3300-48T-BF	48-port 10/100/1000BASE-T	None	Back-to-front	AC	0	100
EX3300-24P	24-port 10/100/1000BASE-T	24	Front-to-back	AC	405	550
EX3300-48P	48-port 10/100/1000BASE-T	48	Front-to-back	AC	740	900
EX3300-24T-DC	24-port 10/100/1000BASE-T	None	Front-to-back	DC	0	100



Specifications

Uplink

- Fixed 4-port uplinks which can be individually configured as GbE (SFP) or 10GbE (SFP+) ports.

Dimensions (W x H x D)

- 17.4 x 1.7 x 12 in (43.7 x 4.4 x 31 cm)

Weight Lbs (Kg)

- EX3300-48P: 12.8 lb (5.8 kg)
- EX3300-24P: 11.6 lb (5.3 kg)
- EX3300-48T: 10.8 lb (4.9 kg)
- EX3300-48T-BF: 10.8 lb (4.9 kg)
- EX3300-24T: 10.0 lb (4.6 kg)
- EX3300-24T-DC: 9.8 lb (4.5 kg)

Environmental Ranges

- Operating temperature: 32° to 113° F (0° to 45° C)
- Storage temperature: -40° to 158° F (-40° to 70° C)
- Operating altitude: Up to 10,000 ft (3,049 m)
- Non-operating altitude: Up to 16,000 ft (4,877 m)
- Relative humidity operating: 10% to 85% (noncondensing)
- Relative humidity non-operating: 0% to 95% (noncondensing)

Hardware Specifications

- Switching Engine Model: Store and forward
- DRAM: 1 GB with ECC
- Flash: 1 GB
- CPU: 1 GHz

GbE Port Density per System

- EX3300-24T/EX3300-24P/EX3300-24T-DC: 28 (24 host ports + four 10 GbE/GbE uplink ports)
- EX3300-48T/EX3300-48T-BF/EX3300-48P: 52 (48 host ports + four 10 GbE/GbE uplink ports)

Virtual Chassis Capabilities

- Maximum number of members: 10
- Number of Virtual Chassis ports: 4
- Maximum Virtual Chassis interconnect capacity: 80 Gbps

Physical Layer

- Time Domain Reflectometry (TDR) for detecting cable breaks and shorts
- Auto medium-dependent interface/medium dependent interface crossover (MDI/MDIX) support
- Port speed downshift/setting maximum advertised speed on 10/100/1000BASE-T ports
- Digital optical monitoring for optical ports

Packet Switching Capacities (Maximum with 64 Byte Packets)

- EX3300-24T, EX3300-24P, EX3300-24T-DC: 128 Gbps
- EX3300-48T, EX3300-48T-BF, EX3300-48P: 176 Gbps
- Layer 2/Layer 3 Throughput (Mpps):
- 24P/24T/24T-DC: 95 Mpps
- 48P/48T/48T-BF: 130 Mpps

Layer 2 Switching

- Maximum MAC addresses per system: 16,000
- Jumbo frames: 9,216 Bytes
- Number of VLANs: 4,096
- Range of possible VLAN IDs: 1-4,095
- Port-based VLAN
- MAC-based VLAN
- Voice VLAN
- Compatible with Per-VLAN Spanning Tree Plus (PVST+)
- RVI (Routed VLAN Interface)
- IEEE 802.1AB: Link Layer Discovery Protocol (LLDP)
- LLDP-MED with VoIP integration
- IEEE 802.1D: Spanning Tree Protocol
- IEEE 802.1p: CoS prioritization
- IEEE 802.1Q: VLAN tagging
- IEEE 802.1Q-in-Q: VLAN stacking
- IEEE 802.1s: Multiple Spanning Tree Protocol (MSTP)
- IEEE 802.1ak Multiple VLAN Registration Protocol (MVRP)
- Persistent MAC (sticky MAC)
- Number of MST instances supported: 64
- Number of VSTP instances supported: 253
- IEEE 802.1w: Rapid Spanning Tree Protocol (RSTP)
- RSTP and VSTP running concurrently
- IEEE 802.1X: Port access control
- IEEE 802.3: 10BASE-T

- IEEE 802.3u: 100BASE-T
- IEEE 802.3ab: 1000BASE-T
- IEEE 802.3z: 1000BASE-X
- IEEE 802.3af: PoE
- IEEE 802.3at: PoE+
- IEEE 802.3x: Pause frames/flow control
- IEEE 802.3ad: Link Aggregation Control Protocol (LACP)
- Layer 3 VLAN-tagged sub-interface
- NetBios snooping
- Metro
 - PVL Domain support
 - IEEE 802.1ag connectivity fault management
 - ITU-T G.8032 Ethernet Ring Protection Switching
 - IEEE 802.1ad Q-in-Q tunneling
 - Multicast VLAN routing
 - Layer 2 Tunneling Protocol (L2TP)
 - Adding/removing single tag
- Filter-based SVLAN tagging
- Flexible CoS (outer IP marking)

Layer 3 Features: IPv4

- Maximum number of Address Resolution Protocol (ARP) entries: 4,000
- Maximum number of IPv4 unicast routes in hardware: 8,000
- Layer 3 redundancy: VRRP
- Routing protocols:
 - RIP v1/v2
 - Static routing
 - OSPF v2
 - BGP v4
- IP directed broadcast – traffic forwarding
- Virtual router (VRF-Lite) supporting RIP, OSPF, BGP
- Routing policy
- Filter-based Forwarding (FBF)
- Unicast Reverse Path Forwarding (uRPF)
- Multiprotocol BGP (MBGP)

Layer 3 Features: IPv6 Management Functionality

- Neighbor discovery, system logging, Telnet, SSH, Junos Web, SNMP, Network Time Protocol (NTP), Domain Name System (DNS)
- Static routing
- IPv6 ACL (PACL, VAACL, RAACL)
- IPv6 CoS (BA, MF classification and rewrite, scheduling based on TC)
- MLDv1/v2 snooping
- MLDv1/v2
- IPv6 ping, traceroute
- IPv6 stateless auto-configuration
- IPv6 Layer 3 forwarding in hardware

Layer 3 Features: IPv6 Routing

- RIPng
- OSPF v3
- BGP v6
- IPv6 Layer 3 redundancy: VRRP v6
- Virtual Router support for IPv6 unicast
- PIM for IPv6 multicast
- MBGP

Supported RFCs

- RFC 2925 MIB for remote ping, trace
- RFC 1122 Host requirements
- RFC 768 UDP
- RFC 791 IP
- RFC 783 Trivial File Transfer Protocol (TFTP)
- RFC 792 Internet Control Message Protocol (ICMP)
- RFC 793 TCP
- RFC 826 Address Resolution Protocol (ARP)
- RFC 894 IP over Ethernet
- RFC 903 Reverse ARP (RARP)
- RFC 906 TFTP bootstrap
- RFC 1027 Proxy ARP
- RFC 2068 HTTP server
- RFC 1812 Requirements for IP Version 4 routers
- RFC 1519 Classless Interdomain Routing (CIDR)
- RFC 1256 IPv4 ICMP Router Discovery (IRDP)
- RFC 1058 RIP v1
- RFC 2453 RIP v2
- RFC 1492 TACACS+
- RFC 2138 RADIUS authentication
- RFC 2139 RADIUS accounting
- RFC 3579 RADIUS Extensible Authentication Protocol (EAP) support for 802.1X
- RFC 5176 Dynamic Authorization Extensions to RADIUS
- RFC 2267 Network ingress filtering
- RFC 2030 SNTTP
- RFC 854 Telnet client and server
- RFC 951, 1542 BootP
- RFC 2131 BootP/DHCP relay agent and DHCP server
- RFC 1591 Domain Name System (DNS)
- RFC 2474 DiffServ Precedence, including 8 queues/port
- RFC 2598 DiffServ Expedited Forwarding (EF)
- RFC 2597 DiffServ Assured Forwarding (AF)
- LLDP-MED, ANSI/TIA-1057, draft 08
- RFC 2328 OSPF v2
- RFC 3768 VRRP
- RFC 4271 BGP4
- RFC 4601 PIM-SM
- RFC 3973 PIM-DM
- RFC 3569 PIM-SSM
- RFC 3618 Multicast Source Discovery Protocol (MSDP)

Security

- MAC limiting
- Allowed MAC addresses, configurable per port
- Dynamic ARP inspection (DAI)
- Proxy ARP
- Static ARP support
- DHCP snooping
- IP source guard
- 802.1X port-based
- 802.1X multiple supplicants
- 802.1X with VLAN assignment
- 802.1X with authentication bypass access (based on host MAC address)
- 802.1X with VoIP VLAN support
- 802.1X dynamic access control list (ACL) based on RADIUS attributes
- 802.1X supported EAP types: Message Digest 5 (MD5), Transport Layer Security (TLS), Tunneled Transport Layer Security (TTLS), Protected Extensible Authentication Protocol (PEAP)
- Access control lists, (Junos OS firewall filters)
- Port-based ACL (PACL)—ingress and egress
- VLAN-based ACL (VAACL)—ingress and egress
- Router-based ACL (RAACL)—ingress and egress
- ACL entries (ACE) in hardware per system: 1,500
- ACL counter for denied packets
- ACL counter for permitted packets
- Ability to add/remove/change ACL entries in middle of list (ACL editing)
- L2-L4 ACL
- Trusted Network Connect (TNC) certified
- Static MAC authentication
- MAC-RADIUS
- Control plane denial-of-service (DoS) protection
- Firewall filter on me0 interface (control plane protection)
- Captive Portal – Layer 2 interfaces
- Fallback authentication

High Availability

- External redundant power system option
- Link aggregation:
 - 802.3ad (LACP) support
 - Number of link aggregation groups (LAGs) supported: 32
 - Maximum number of ports per LAG: 8
 - LAG load sharing algorithm—bridged unicast traffic
 - IP: S/D MAC, S/D IP
 - TCP/UDP: S/D MAC, S/D IP, S/D port
 - Non-IP: S/D MAC
- LAG sharing algorithm—routed unicast traffic
 - IP: S/D IP
 - TCP/UDP: S/D IP, S/D port

High Availability (continued)

- LAG load sharing algorithm—bridged multicast traffic
- IP: S/D MAC, S/D IP
 - TCP/UDP: S/D MAC, S/D IP, S/D port
 - Non-IP: S/D MAC
- LAG sharing algorithm—routed multicast traffic
 - IP: S/D IP
 - TCP/UDP: S/D IP, S/D port
- Tagged ports support in LAG
- Graceful Route Engine Switchover (GRES) for IGMP v1/v2/v3 snooping
- Non-stop Routing (OSPF v1/v2/v3, RIP/RIPng, BGP, BGP v6, ISIS, PIM)
- Non-Stop Software Upgrade (NSSU)

Quality of Service (QoS)

- Layer 2 QoS
- Layer 3 QoS
- Ingress policing: 1 rate 2 color
- Hardware queues per port: 8
- Scheduling methods (egress): Strict Priority (SP), SDWRR
- 802.1p, DiffServ code point (DSCP/IP) precedence trust and marking
- L2-L4 classification criteria, including Interface, MAC address, EtherType, 802.1p, VLAN, IP address, DSCP/IP precedence, and TCP/UDP port numbers
- Congestion avoidance capabilities: Tail drop

Multicast

- IGMP snooping entries: 3,000
- IGMP snooping
- IGMP v1/v2/v3
- PIM-SM, PIM-SSM, PIM-DM
- VRF-Lite support for PIM and IBMP
- IPv6 multicast snooping MLD v1/v2
- MLD v1/v2 snooping
- IGMP filter
- Multicast Source Discovery Protocol (MSDP)
- PIM for IPv6 multicast
- MBGP

Services and Manageability

- Junos OS CLI
- Web interface Junos Web support
- Out-of-band management: Serial, 10/100BASE-T Ethernet
- ASCII configuration
- Rescue configuration
- Configuration rollback
- Image rollback
- Element management tools: Junos Space Network Management Platform
- Real-Time Performance Monitoring (RPM)
- SNMP: v1, v2c, v3

- Remote monitoring (RMON) (RFC 2819) Groups 1, 2, 3, 9
- Network Time Protocol (NTP)
- DHCP server
- DHCP client and DHCP proxy
- DHCP relay and helper
- VR-aware DHCP
- RADIUS authentication
- TACACS+ authentication
- SSHv2
- Secure copy
- HTTP/HTTPS
- DNS resolver
- System logging
- Temperature sensor
- Configuration backup via FTP/secure copy
- sFlow
- Interface range
- Port profile associations
- Ethernet OAM link fault management (LFM)
- Uplink Failure Detection (UFD)
- EZ Touchless Provisioning using DHCP

Supported MIBs¹

- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 4862 IPv6 Stateless Address Autoconfiguration
- RFC 4443 ICMPv6 for the IPv6 Specification
- RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers
- RFC 1155 Structure of Management Information (SMI)
- RFC 1157 SNMPv1
- RFC 1905 RFC 1907 SNMP v2c, SMIv2, and revised MIB-II
- RFC 2570-2575 SNMPv3, user-based security, encryption, and authentication
- RFC 2576 Coexistence between SNMP Version 1, Version 2, and Version 3
- RFC 1212, RFC 1213, RFC 1215 MIB-II, Ethernet-like MIB, and traps
- RFC 2578 SNMP Structure of Management Information MIB
- RFC 2579 SNMP textual conventions for SMIv2
- RFC 2925 Ping/traceroute MIB
- RFC 2665 Ethernet-like interface MIB
- RFC 1643 Ethernet MIB
- RFC 1493 Bridge MIB
- RFC 2096 IPv4 forwarding table MIB
- RFC 2011 SNMPv2 for IP using SMIv2
- RFC 2012 SNMPv2 for transmission control protocol using SMIv2
- RFC 2013 SNMPv2 for user datagram protocol using SMIv2
- RFC 2863 Interface MIB
- RFC 3413 SNMP application MIB
- RFC 3414 User-based security model for SNMPv3
- RFC 3415 View-based access control model for SNMP
- RFC 3621 PoE-MIB (PoE switches only)

- RFC 1724 RIPv2 MIB
- RFC 2863 Interface group MIB
- RFC 2819 RMON MIB
- RFC 2287 System application packages MIB
- RFC 4188 STP and extensions MIB
- RFC 4363 Definitions of managed objects for bridges with traffic classes, multicast filtering, and VLAN extensions
- RFC 2922 LLDP MIB
- RFC 2328 OSPF v2
- RFC 5643 OSPF v3 MIB support
- RFC 1981 Path MTU discovery for IPv6
- RFC 2460 IPv6 specification
- RFC 3484 Default address selection for IPv6
- RFC 4291 IPv6 addressing architecture
- RFC 4861 Neighbor discovery for IPv6
- IEEE 802.1ad Q-in-Q
- Draft – blumenthal – aes – usm - 08
- Draft – reeder - snmpv3 – usm - 3desede -00

Troubleshooting

- Debugging: CLI via console, telnet, or SSH
- Diagnostics: Show and debug command statistics
- Traffic mirroring (port)
- Traffic mirroring (VLAN)
- Filter-based mirroring
- Mirroring destination ports per system: 1
- LAG port monitoring
- Multiple destination ports monitored to 1 mirror (N:1)
- Maximum number of mirroring sessions: 1
- Mirroring to remote destination (over L2): 1 destination VLAN
- IP tools: Extended ping and trace
- Juniper Networks commit and rollback

Safety Certifications

- UL-UL60950-1 (First Edition)
- C-UL to CAN/CSA 22.2 No.60950-1 (First Edition)
- TUV/GS to EN 60950-1, Amendment A1-A4, A11
- CB-IEC60950-1, all country deviations

Electromagnetic Compatibility Certifications

- FCC 47CFR Part 15 Class A
- EN 55022 Class A
- ICES-003 Class A
- VCCI Class A
- AS/NZS CISPR 22 Class A
- CISPR 22 Class A
- EN 55024
- EN 300386
- CE

Telecom Quality Management

- TL9000

Environmental

- Reduction of Hazardous Substances (ROHS) 6

Telco

- CLEI code

FIPS

- FIPS 140-2 Level 1

Noise Specifications

- Noise measurements based on operational tests taken from bystander position (front) and performed at 23° C in compliance with ISO 7779.

Table 4: Noise Test Results

Model	Acoustics Noise (DBA)
EX3300-24T	45.2
EX3300-48T	41.2
EX3300-24P	45.4
EX3300-48P	42.8

Juniper Networks Service and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit www.juniper.net/us/en/products-services.

Ordering Information

Model Number	Description
Switches	
EX3300-48P	EX3300 48-port 10/100/1000BASE-T (48 PoE+ ports) with 4 SFP+ uplink ports (optics not included)
EX3300-24P	EX3300 24-port 10/100/1000BASE-T (24 PoE+ ports) with 4 SFP+ uplink ports (optics not included)
EX3300-48T	EX3300 48-port 10/100/1000BASE-T with 4 SFP+ uplink ports (optics not included)
EX3300-48T-BF	EX3300 48-port 10/100/1000BASE-T with 4 SFP+ uplink ports (optics not included), back-to-front cooling
EX3300-24T	EX3300 24-port 10/100/1000BASE-T with 4 SFP+ uplink ports (optics not included)
EX3300-24T-DC	EX3300 24-port 10/100/1000BASE-T with 4 SFP+ uplink ports (optics not included) and internal DC power supply

Accessories

EX-RPS-PWR-930-AC	External redundant power system (RPS) for power supply and power feed redundancy; includes one RPS cable and one 930 W AC power supply (shipped separately)
EX-4PST-RMK	Adjustable 4-post rack-mount kit for EX2200, EX3200, EX3300, and EX4200
EX-RMK	Rack-mount kit for EX2200, EX3200, EX3300, and EX4200
EX-WMK-BFL	EX4200, EX3200, EX3300, and EX2200 wall-mount kit with baffle
RE-USB-1G-S	USB media upgrade/spare for Routing Engine
RE-USB-2G-S	2 GB USB media upgrade/spare for Routing Engine
RE-USB-4G-S	4 GB USB media upgrade/spare for Routing Engine
CBL-EX-PWR-C13-AU	AC power cable, Australia (10 A/250 V, 2.5 m)
CBL-EX-PWR-C13-C14	AC power cable, patch cord (10 A/250 V, 2.5 m) for EU only
CBL-EX-PWR-C13-CH	AC power cable, China (10 A/250 V, 2.5 m)
CBL-EX-PWR-C13-EU	AC power cable, Europe (10 A/250 V, 2.5 m)
CBL-EX-PWR-C13-IT	AC power cable, Italy (10 A/250 V, 2.5 m)
CBL-EX-PWR-C13-JP	AC power cable, Japan (12 A/125 V, 2.5 m)
CBL-EX-PWR-C13-KR	AC power cable, Korea (10 A/250 V, 2.5 m)
CBL-EX-PWR-C13-SZ	AC power cable, Switzerland (10 A/250 V, 2.5 m)
CBL-EX-PWR-C13-UK	AC power cable, UK (10 A/250 V, 2.5 m)
CBL-EX-PWR-C13-US	AC power cable, US (13 A/125 V, 2.5 m)

Model Number	Description
Feature Licenses	
EX-24-EFL	Enhanced Feature License for EX3300-24P, EX3300-24T and EX3300-24T-DC switches includes licenses for IPv4 routing (OSPF v1/v2, IGMP v1/v2/v3, PIM, VRRP, BFD, IPv4 Virtual Router support and Q-in-Q) and IPv6 routing (OSPF v3, VRRP v6, VR support for unicast and filter based forwarding—FBF, MLD v1/v2 routing and PIM).
EX-48-EFL	Enhanced Feature License for EX3300-48P, EX3300-48T and EX3300-48T-BF switches includes licenses for IPv4 routing (OSPF v1/v2, IGMP v1/v2/v3, PIM, VRRP, BFD, IPv4 Virtual Router support and Q-in-Q) and IPv6 routing (OSPF v3, VRRP v6, VR support for unicast and filter based forwarding—FBF, MLD v1/v2 routing and PIM).
EX-24-AFL	Advanced Feature License for EX3300-24P, EX3300-24T and EX3300-24T-DC switches includes license for BGP/MBGP, Virtual Router running BGP, and IPv6 routing protocols (BGP v6, MBGP). Requires purchase of EFL.
EX-48-AFL	Advanced Feature License for EX3300-48P, EX3300-48T and EX3300-48T-BF switches includes license for BGP/MBGP, Virtual Router running BGP, and IPv6 routing protocols (BGP v6, MBGP). Requires purchase of EFL.
Optics	
EX-SFP-10GE-DAC-1M	SFP+ 10-Gigabit Ethernet Direct Attach Copper (twinax copper cable), 1 m
EX-SFP-10GE-DAC-3M	SFP+ 10-Gigabit Ethernet Direct Attach Copper (twinax copper cable), 3 m
EX-SFP-10GE-DAC-5M	SFP+ 10-Gigabit Ethernet Direct Attach Copper (twinax copper cable), 5 m
EX-SFP-10GE-DAC-7M	SFP+ 10-Gigabit Ethernet Direct Attach Copper (twinax copper cable), 7 m
EX-SFP-10GE-ER	SFP+ 10GBASE-ER 10-Gigabit Ethernet Optics, 1,550 nm for 40 km transmission on SMF
EX-SFP-10GE-LR	SFP+ 10GBASE-LR 10-Gigabit Ethernet Optics, 1,310 nm for 10 km transmission on single-mode fiber-optic (SMF)
EX-SFP-10GE-LRM	SFP+ 10-Gigabit Ethernet LRM Optics, 1,310 nm for 220 m transmission on multimode fiber-optic (MMF)
EX-SFP-10GE-SR	SFP+ 10GBASE-SR 10-Gigabit Ethernet Optics, 850 nm for up to 300 m transmission on MMF
EX-SFP-10GE-USR	SFP+ 10-Gigabit Ethernet Ultra Short Reach Optics, 850 nm for 10 m on OM1, 20 m on OM2, 100 m on OM3 multimode fiber
EX-SFP-1GE-LX	SFP 1000BASE-LX Gigabit Ethernet Optics, 1,310 nm for 10 km transmission on SMF
EX-SFP-1GE-LX40K	SFP 1000BASE-LX Gigabit Ethernet Optics, 1,310 nm for 40 km transmission on SMF
EX-SFP-1GE-SX	SFP 1000BASE-SX Gigabit Ethernet Optics, 850 nm for up to 550 m transmission on MMF

Model Number	Description
EX-SFP-IGE-LH	SFP 1000BASE-LH Gigabit Ethernet Optics, 1,550 nm for 70 km transmission on SMF
EX-SFP-IGE-T	SFP 10/100/1000BASE-T Copper Transceiver Module for up to 100 m transmission on Category 5
EX-SFP-GE10KT13R14	SFP 1000BASE-BX Gigabit Ethernet Optics, Tx 1,310 nm/Rx 1,490 nm for 10 km transmission on single strand of SMF
EX-SFP-GE10KT13R15	SFP 1000BASE-BX Gigabit Ethernet Optics, Tx 1,310 nm/Rx 1,550 nm for 10 km transmission on single strand of SMF
EX-SFP-GE10KT14R13	SFP 1000BASE-BX Gigabit Ethernet Optics, Tx 1,490 nm/Rx 1,310 nm for 10 km transmission on single strand of SM
EX-SFP-GE10KT15R13	SFP 1000BASE-BX Gigabit Ethernet Optics, Tx 1,550 nm/Rx 1,310 nm for 10 km transmission on single strand of SMF
EX-SFP-GE40KT13R15	SFP 1000BASE-BX Gigabit Ethernet Optics, Tx 1,310 nm/Rx 1,550 nm for 40 km transmission on single strand of SMF
EX-SFP-GE40KT15R13	SFP 1000BASE-BX Gigabit Ethernet Optics, Tx 1,550 nm/Rx 1,310 nm for 40 km transmission on single strand of SMF

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters
 Juniper Networks, Inc.
 1133 Innovation Way
 Sunnyvale, CA 94089 USA
 Phone: 888.JUNIPER (888.586.4737)
 or +1.408.745.2000
 Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
 Juniper Networks International B.V.
 Boeing Avenue 240
 1119 PZ Schiphol-Rijk
 Amsterdam, The Netherlands
 Phone: +31.0.207125.700
 Fax: +31.0.207125.701

Copyright 2015 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos and QFabric are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

1000389-013-EN Dec 2015

JUNIPER
 NETWORKS

Cisco Catalyst 3850 Series Switches

The Cisco® Catalyst® 3850 Series is the next generation of enterprise-class stackable Ethernet and Multigigabit Ethernet access and aggregation layer switches that provide full convergence between wired and wireless on a single platform. Cisco's new Unified Access Data Plane (UADP) application-specific integrated circuit (ASIC) powers the switch and enables uniform wired-wireless policy enforcement, application visibility, flexibility and application optimization. This convergence is built on the resilience of the new and improved Cisco StackWise-480 technology. The Cisco Catalyst 3850 Series Switches support full IEEE 802.3 at Power over Ethernet Plus (PoE+), Cisco Universal Power over Ethernet (Cisco UPOE), modular and field-replaceable network modules, RJ45 and fiber-based downlink interfaces, and redundant fans and power supplies. With speeds that reach 10Gbps, the Cisco Catalyst 3850 Multigigabit Ethernet Switches support current and next-generation wireless speeds and standards (including 802.11ac Wave 2) on existing cabling infrastructure.

Product Overview

- Integrated wireless controller capability with:
 - Up to 40G of wireless capacity per switch (48-port RJ45 models)
 - Support for up to 100 access points and 2000 wireless clients on each switching entity (switch or stack)
- 24 and 48 10/100/1000Mbps data PoE+ and Cisco UPOE models with energy-efficient Ethernet (EEE)
- 24 and 48 100Mbps/1/2.5/5/10 Gbps Cisco UPOE models with energy-efficient Ethernet (EEE)
- 12- and 24-port 1 Gigabit Ethernet SFP-based models
- 12- and 24-port 1/10 Gigabit Ethernet SFP+-based models
- 48-port 1/10 Gigabit Ethernet SFP+ model with 4 fixed 40 Gigabit Ethernet QSFP+ uplinks
- Cisco StackWise-480 technology provides scalability and resiliency with 480 Gbps of stack throughput¹
- Cisco StackPower™ technology provides power stacking among stack members for power redundancy¹
- Five optional uplink modules² with 4 x Gigabit Ethernet, 2 x 10 Gigabit Ethernet, 4 x 10 Gigabit Ethernet³, 8 x 10 Gigabit Ethernet⁴, or 2 x 40 Gigabit Ethernet QSFP+⁴ ports
- Dual redundant, modular power supplies and three modular fans providing redundancy
- Full IEEE 802.3at (PoE+) with 30W power on all copper ports in 1 rack unit (RU) form factor
- Cisco UPOE with 60W power per port in 1 rack unit (RU) form factor

¹ StackWise and StackPower technologies are not supported on the 48-port SFP+ switch model.

² Optional uplink modules are not supported on the 48-port 10G SFP+ switch model.

³ Compatible only with the 48-port RJ45 models and with the 12-port (or higher) 10 Gigabit capable models.

⁴ Compatible only with Cisco Catalyst 3850 Multigigabit and 24-port SFP+ switch models.

- Software support for IPv4 and IPv6 routing, multicast routing, modular quality of service (QoS), Flexible NetFlow (FNF), and enhanced security features
- Single universal Cisco IOS® Software image across all license levels, providing an easy upgrade path for software features
- Enhanced limited lifetime warranty (E-LLW) with next business day (NBD) advance hardware replacement and 90-day access to Cisco Technical Assistance Center (TAC) support

Switch Configurations

All switches ship with one of the five power supplies (350WAC, 715WAC, 750WAC, 1100WAC, or 440WDC)⁵. Figures 1 through 3 show the Cisco Catalyst 3850 Series Switches.

Figure 1. Cisco Catalyst 3850 Series Switches



Figure 2. Cisco Catalyst 3850 Switches with 12 and 24 1/10 Gigabit Ethernet SFP+ Ports



Figure 3. Cisco Catalyst 3850 Switches with 12 and 24 1 Gigabit Ethernet SFP Ports



⁵ The 48-port 10G SFP+ switch model will only support dedicated power supplies with front-to-back and back-to-front configurations.

Table 1 shows the Cisco Catalyst 3850 Series configurations.

Table 1. Cisco Catalyst 3850 Series Configurations

Models	Total 10/100/1000 or SFP or SFP+ Ports	Default AC Power Supply	Available PoE Power	StackWise-480	StackPower
WS-C3850-24T	24	350WAC	-	Yes	Yes
WS-C3850-48T	48				
WS-C3850-24P	24 PoE+	715WAC	435W		
WS-C3850-48P	48 PoE+				
WS-C3850-48F	48 PoE+	1100WAC	800W		
WS-C3850-24U	24 UPOE	1100WAC	800W		
WS-C3850-48U	48 UPOE	1100WAC	800W		
WS-C3850-24XU	24 UPOE (100Mbps/1/2.5/5/10 Gbps)	1100WAC	580W		
WS-C3850-12X48U	48 UPOE (with 12 100Mbps/1/2.5/5/10 Gbps Ports)	1100WAC	630W		
WS-C3850-12S	12 SFP	350WAC			
WS-C3850-24S	24 SFP				
WS-C3850-12XS	12 1/10G SFP+	350WAC	-		
WS-C3850-24XS	24 1/10G SFP+	715 WAC	-		
WS-C3850-48XS	48 1/10G SFP+	750WAC (front to back)	-	No	No

Network Modules

The Cisco Catalyst 3850 Series Switches support five optional network modules for uplink ports. The default switch configuration does not include the network module⁶. At the time of switch purchase the customer has the flexibility to choose from the network modules described in Table 2.

Figure 4 shows the following network modules:

- 4 x Gigabit Ethernet with Small Form-Factor Pluggable (SFP) receptacles
- 2 x 10 Gigabit Ethernet with SFP+ or 4 x Gigabit Ethernet with SFP receptacles
- 4 x 10 Gigabit Ethernet with SFP+ receptacles (supported only on the 48-port Gigabit Ethernet models or on the 12-port or higher 10 Gigabit Ethernet models)

Figure 4. Network Modules with Four Gigabit Ethernet, Two 10 Gigabit Ethernet SFP+, or Four 10 Gigabit Ethernet SFP+ Interfaces



⁶ Network modules are not supported on the 48-port 10G SFP+ switch model, which comes with four fixed 40 Gigabit Ethernet QSFP+ uplinks.

Figure 5 shows the following network modules:

- 8 x 10 Gigabit Ethernet with Small Form-Factor Pluggable+ (SFP+) receptacles
- 2 x 40 Gigabit Ethernet with Quad Small Form-Factor Pluggable+ (QSFP+) receptacles

Figure 5. Network Modules with Two 40 Gigabit Ethernet QSFP+ or Eight 10 Gigabit Ethernet SFP+ Interfaces



Table 2. Network Module Numbers and Descriptions

Product Number	Product Description	WS-C3850-24XU	WS-C3850-12XS
		WS-C3850-12X48U	WS-C3850-24XS
C3850-NM-4-1G	4 x Gigabit Ethernet network modules	Supported	Not supported
C3850-NM-2-10G	4 x Gigabit Ethernet/2 x 10 Gigabit Ethernet network modules	Supported	Not supported
C3850-NM-4-10G	4 x Gigabit Ethernet/4 x 10 Gigabit Ethernet network modules	Supported	Supported
C3850-NM-8-10G	8 x Gigabit Ethernet/8 x 10 Gigabit Ethernet network modules	Supported	See note
C3850-NM-2-40G	2 x 40 Gigabit Ethernet network modules	Supported	See note

Note: The C3850-NM-4-10G module is supported only on the 48-port Gigabit Ethernet models or on the 12-port or higher 10 Gigabit Ethernet models. The C3850-NM-8x10G and C3850-NM-2x40G modules are supported on the 24-port and 48-port multigigabit switches and also on the 24-port 10G SFP+ switch model. The C3850-NM-4-1G and C3850-NM-2-10G modules are not supported on the 12-port and 24-port SFP+ models.

Table 3. Network Module Compatibility Matrix

Models	Network Modules
WS-C3850-24T	C3850-NM-4-1G, C3850-NM-2-10G
WS-C3850-48T	C3850-NM-4-1G, C3850-NM-2-10G, C3850-NM-4-10G
WS-C3850-24P	C3850-NM-4-1G, C3850-NM-2-10G
WS-C3850-48P	C3850-NM-4-1G, C3850-NM-2-10G, C3850-NM-4-10G
WS-C3850-48F	C3850-NM-4-1G, C3850-NM-2-10G, C3850-NM-4-10G
WS-C3850-24U	C3850-NM-4-1G, C3850-NM-2-10G
WS-C3850-48U	C3850-NM-4-1G, C3850-NM-2-10G, C3850-NM-4-10G
WS-C3850-24XU	C3850-NM-4-1G, C3850-NM-2-10G, C3850-NM-4-10G, C3850-NM-8-10G, C3850-NM-2-40G
WS-C3850-12X48U	C3850-NM-4-1G, C3850-NM-2-10G, C3850-NM-4-10G, C3850-NM-8-10G, C3850-NM-2-40G
WS-C3850-12S	C3850-NM-4-1G, C3850-NM-2-10G
WS-C3850-24S	C3850-NM-4-1G, C3850-NM-2-10G
WS-C3850-12XS	C3850-NM-4-10G
WS-C3850-24XS	C3850-NM-4-10G, C3850-NM-8-10G, C3850-NM-2-40G
WS-C3850-48XS	None

An SFP+ receptacle supports both 10 Gigabit Ethernet and Gigabit Ethernet modules, allowing customers to use their investment in Gigabit Ethernet SFP modules and upgrade to 10 Gigabit Ethernet when business demands change without having to do a comprehensive upgrade of the access switch. In contrast, SFP receptacles can be used only as Gigabit Ethernet ports, as shown in the examples in Table 4.

Table 4. Network Module Configuration Examples

Network Module	Interface Options	
	10 Gigabit Ethernet SFP+ Ports	Gigabit Ethernet SFP Ports
4 x Gigabit Ethernet	0	4
4 x Gigabit Ethernet/2 x10 Gigabit Ethernet network modules	2	0
	1	3
	2	2
	0	4
4 x Gigabit Ethernet/4 x10 Gigabit Ethernet network modules	4	0
	0	4
	2	2
	3	1
	1	3

Dual Redundant Modular Power Supplies

The Cisco Catalyst 3850 Series Switches support dual redundant power supplies⁷. The switch ships with one power supply by default, and the second power supply can be purchased at the time of ordering the switch or at a later time. If only one power supply is installed, it should always be in power supply bay 1. The switch also ships with three field-replaceable fans. (See Figure 6.)

Figure 6. Dual Redundant Power Supplies



Table 5 shows the different power supplies available in these switches and available PoE power.

Table 5. Power Supply Models

Models	Default Power Supply	Available PoE Power
24-port data switch	PWR-C1-350WAC	-
48-port data switch		
24-port PoE switch	PWR-C1-715WAC	435W
48-port PoE switch		
48-port full PoE switch	PWR-C1-1100WAC	800W

⁷ The 48-port 10G SFP+ switch model will only support dedicated power supplies with front-to-back and back-to-front configurations.

Models	Default Power Supply	Available PoE Power
24-port UPOE switch	PWR-C1-1100WAC	800W
48-port UPOE switch		
24-port Multigigabit UPOE switch	PWR-C1-1100WAC	580W
48-port Multigigabit UPOE switch	PWR-C1-1100WAC	630W
12-port SFP switch	PWR-C1-350WAC	-
24-port SFP switch		
12-port SFP+ switch	PWR-C1-350WAC	-
24-port SFP+ switch	PWR-C1-715WAC	-
48-port SFP+ switch (WS-C3850-48XS-S and WS-C3850-48XS-E)	PWR-C3-750WAC-R	-
48-port SFP+ switch (WS-C3850-48XS-F-S and WS-C3850-48XS-F-E)	PWR-C3-750WAC-F	-

In addition to the power supplies listed in Table 5, a 440WDC power supply is available as a configuration option and also as a spare (that is, it can be ordered separately) on all switch models. The DC power supply also delivers PoE capabilities for maximum flexibility (refer to Table 6 for available PoE budget with DC power supplies). Customers can mix and match the AC and DC power supplies in the two available power supply slots. Any of these power supplies can be installed in any of the switches.

Table 6. Available PoE with DC Power Supply

Model	Number of 440WDC Power Supplies	Total Available PoE Budget
24-port PoE switch	1	220W
	2	660W
48-port PoE switch	1	185W
	2	625W
24-port MgiG UPoE switch	2	360W
48-port MgiG UPoE switch	2	410W

Power over Ethernet Plus (PoE+)

In addition to PoE (IEEE 802.3af), the Cisco Catalyst 3850 Series Switches support PoE+ (IEEE 802.3at standard), which provides up to 30W of power per port. The Cisco Catalyst 3850 Series Switches can provide a lower total cost of ownership (TCO) for deployments that incorporate Cisco IP phones, Cisco Aironet® wireless LAN (WLAN) access points, or any IEEE 802.3at-compliant end device. PoE removes the need for wall power to each PoE-enabled device and eliminates the cost for additional electrical cabling and circuits that would otherwise be necessary in IP phone and WLAN deployments. Table 7 shows the power supply combinations required for different PoE needs.

Table 7. Power Supply Requirements for PoE and PoE+

	24-Port PoE Switch	48-Port PoE Switch
PoE on all ports (15.4W per port)	One PWR-C1-715WAC	One PWR-C1-1100WAC or two PWR-C1-715WAC
PoE+ on all ports (30W per port)	One PWR-C1-1100WAC or two PWR-C1-715WAC	Two PWR-C1-1100WAC or one PWR-C1-1100WAC and one PWR-C1-715WAC

Cisco Universal Power over Ethernet (UPOE)

Cisco Universal Power over Ethernet (Table 8) is a breakthrough technology, offering the following services and benefits.

- 60W per port to enable a variety of end devices such as Samsung VDI client, BT IP turret systems in trading floors, Cisco Catalyst compact switches in retail/hospitality environments, personal Cisco TelePresence® systems, and physical access control devices
- High availability for power and guaranteed uninterrupted services, a requirement for critical applications (e911)
- Lowering OpEx by providing network resiliency at lower cost by consolidating backup power into the wiring closet
- Faster deployment of new campus access networking infrastructures by eliminating the need for a power outlet for every endpoint

Table 8. Power Supply Requirements for UPOE

	24-Port UPOE Switch	48-Port UPOE Switch	24-Port Multigigabit UPOE Switch	48-Port Multigigabit UPOE Switch
UPOE (60W per port) on all (24 port switch) or max. 30 ports (48 port switch)	One PWR-C1-1100WAC and one PWR-C1-715WAC	Two PWR-C1-1100WAC	Two PWR-C1-1100WAC	Two PWR-C1-1100WAC

Cisco Catalyst Multigigabit Ethernet Technology

Cisco Multigigabit Ethernet is a unique Cisco innovation to the new Cisco Catalyst Ethernet Access Switches. With the enormous growth of 802.11ac and new wireless applications, wireless devices are promoting the demand for more network bandwidth. This creates a need for a technology that supports speeds higher than 1 Gbps on all cabling infrastructure. Cisco Multigigabit technology allows you to achieve bandwidth speeds from 1 Gbps through 10 Gbps over traditional Cat 5e cabling or above. In addition, the Multigigabit ports on select Cisco Catalyst switches support UPOE, which is increasingly important for next-generation workspaces and Internet of Things (IoT) ecosystems.

Cisco Multigigabit technology offers significant benefits for a diverse range of speeds, cable types, and PoE power. The benefits can be grouped into three different areas:

- **Multiple speeds:** Cisco Multigigabit technology supports autonegotiation of multiple speeds on switch ports. The supported speeds are 100 Mbps, 1 Gbps, 2.5 Gbps, and 5 Gbps on Cat 5e cable and up to 10 Gbps over Cat 6a cabling.
- **Cable type:** The technology supports a wide range of cable types, including Cat 5e, Cat 6, and Cat 6a or above.
- **PoE power:** The technology supports PoE, PoE+, and UPOE for all the supported speeds and cable types.

For more information, visit <http://www.cisco.com/c/en/us/solutions/enterprise-networks/catalyst-multigigabit-switching/index.html>.

Benefits

Converged Wired plus Wireless Access

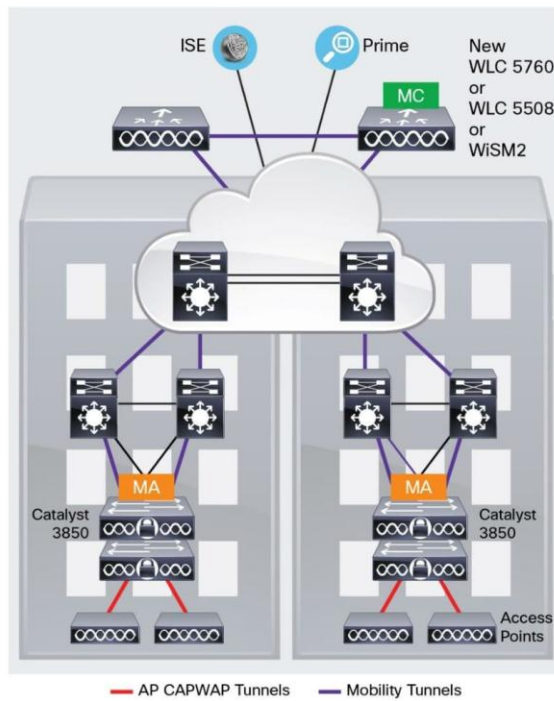
The Cisco Catalyst 3850 is the first stackable access switching platform that enables wired plus wireless services on a single Cisco IOS XE Software-based platform. With this, Cisco has pioneered a host of rich capabilities such as high availability based on stateful switchover (SSO) on stacking, granular QoS, security, and Flexible Netflow (FNF) across wired and wireless in a seamless fashion. Also, the wired plus wireless features are bundled into a single Cisco IOS Software image, which reduces the number of software images that users have to qualify/certify before enabling them in their network. The single console port for command-line interface (CLI) management reduces the number of touch points to manage for wired plus wireless services, thereby reducing network complexity, simplifying network operations, and lowering the TCO to manage the infrastructure.

Converged wired plus wireless not only improves wireless bandwidth across the network but also the scale of wireless deployment. Each 48-port Cisco Catalyst 3850 provides 40 Gbps of wireless throughput (20 Gbps on the 24-port/12-port models). This wireless capacity increases with the number of members in the stack. This makes sure that the network can scale with current wireless bandwidth requirements, as dictated by IEEE 802.11n-based access points and with future wireless standards such as IEEE 802.11ac. Additionally, the Cisco Catalyst 3850 distributes the wireless controller functions to achieve better scalability. Each Cisco Catalyst 3850 switch/stack can operate as the wireless controller in two modes (Figure 7):

- **Mobility agent (MA):** This is the default mode in which a Cisco Catalyst 3850 switch ships. In this mode the switch is capable of terminating the CAPWAP tunnels from the access points and providing wireless connectivity to wireless clients. Maintaining wireless client databases and configuring and enforcing security and QoS policies for wireless clients and access points can be enforced in this mode. No additional license on top of IP Base is required to operate in the mobility agent mode.
- **Mobility controller (MC):** In this mode, the Cisco Catalyst 3850 switch can perform all the mobility agent tasks in addition to mobility coordination, radio resource management (RRM), and Cisco CleanAir[®] coordination within a mobility subdomain. The mobility controller mode can be enabled on the switch CLI. IP Base license level is required when the Cisco Catalyst 3850 switch is acting as the mobility controller. A centrally located Cisco 5508 Wireless LAN Controller (WLC 5508), Cisco Wireless Services Module 2 (WiSM2) (when running AireOS Version 7.3), and Wireless LAN Controller 5760 can also perform this role for larger deployments.

With mobility agents located in the wiring closets providing 40 Gbps of wireless per 48-port Gigabit Ethernet RJ45 switch ($n \times 40$ Gbps for a stack of n switches) and mobility controllers managing some of the central wireless functions, the converged access-based wireless deployment provides best-in-class scalability for wireless and significantly improved wireless throughput.

Figure 7. Mobility Controller (MC) and Mobility Agent (MA)



For more information about Converged Wired plus Wireless Access, refer to the Q&A document here: <http://www.cisco.com/c/dam/en/us/products/collateral/switches/catalyst-3850-series-switches/cisco-catalyst-3850-series-switches-faq.pdf>.

Distributed Intelligent Services

Flexible NetFlow (FNF)

Full visibility into the wired plus wireless traffic is achieved because of the access point Control and Provisioning of Wireless Access Points (CAPWAP) tunnel termination on the switch. This helps identify users and user traffic flows in order to identify potential attackers and take corrective action at the access layer before the attack penetrates further into the network. This is achieved using FNF, which monitors every single flow entering and exiting the switch stack for wired and wireless users. It also helps identify the top wired/wireless talkers and enforce appropriate bandwidth provisioning policies.

QoS

The Cisco Catalyst 3850 switch has advanced wired plus wireless QoS capabilities. It uses the Cisco modular QoS command line interface (MQC). The switch manages wireless bandwidth using unprecedented hierarchical bandwidth management starting at the per-access-point level and drilling further down to per-radio, per-service set identification (SSID), and per-user levels. This helps manage and prioritize available bandwidth between various radios and various SSIDs (enterprise, guest, and so on) within each radio on a percentage basis. The switch is also capable of automatically allocating equal bandwidth among the connected users within a given SSID. This makes sure that all users within a given SSID get a fair share of the available bandwidth while being connected to the network. The UADP ASIC enables the hierarchical bandwidth management and fair sharing of bandwidth, thereby providing hardware-based QoS for optimized performance at line-rate traffic.

In addition to these capabilities, the switch is able to do class of service (CoS) or differentiated services code point (DSCP) based queuing, policing, shaping, and marking of wired plus wireless traffic. This enables users to create common policies that can be used across wired plus wireless traffic. The Cisco Catalyst 3850 also supports downloadable policy names from the Cisco Identity Services Engine (ISE) when a user successfully authenticates to the network using the ISE.

Security

The Cisco Catalyst 3850 provides a rich set of security features for wired plus wireless users. Features such as IEEE 802.1x, port security, Dynamic Host Configuration Protocol (DHCP) Snooping and Guard, Dynamic ARP Inspection, RA Guard, IP Source Guard, control plane protection (CoPP), wireless intrusion prevention systems (WIPSs), and so on enable protection against unauthorized users and attackers. With a variety of wired plus wireless users connecting to the network, the switch supports session-aware networking, in which each device connected to the network is identified as one session, and unique access control lists (ACLs) and/or QoS policies can be defined and applied using the ISE for each of these sessions, providing better control on the devices connecting to the network.

Resiliency

Cisco StackWise-480 Technology

Cisco StackWise-480 technology is built on the highly successful industry-leading StackWise® technology, which is a premium stacking architecture⁸. StackWise-480 has a stack bandwidth of 480 Gbps. StackWise - 480 uses Cisco IOS Software SSO for providing resiliency within the stack. The stack behaves as a single switching unit that is managed by an "active" switch elected by the member switches.

The active switch automatically elects a standby switch within the stack. The active switch creates and updates all the switching/routing/wireless information and constantly synchronizes that information with the standby switch. If the active switch fails, the standby switch assumes the role of the active switch and continues to keep the stack operational. Access points continue to remain connected during an active-to-standby switchover.

A working stack can accept new members or delete old ones without service interruption. StackWise-480 creates a highly resilient single unified system of up to nine switches, providing simplified management using a single IP address, single Telnet session, single CLI, autoversion checking, autoupgrading, autoconfiguration, and more. StackWise-480 also enables local switching in Cisco Catalyst 3850 Series Switches.

⁸ StackWise and StackPower technologies are not supported on the 48-port SFP+ switch model.

Cisco StackPower Technology

The Cisco Catalyst 3850 Series uses the Cisco StackPower⁹ technology present on the Cisco Catalyst 3850 Series. StackPower is an innovative power interconnect system that allows the power supplies in a stack to be shared as a common resource among all the switches. Cisco StackPower unifies the individual power supplies installed in the switches and creates a pool of power, directing that power where it is needed. Up to four switches¹⁰ can be configured in a StackPower stack with the special connector at the back of the switch using the StackPower cable, which is different than the StackWise-480 cables. (See Figure 8.)

Figure 8. StackWise-480 and StackPower Connectors



StackPower can be deployed in either power-sharing mode or redundancy mode. In power-sharing mode, the power of all the power supplies in the stack is aggregated and distributed among the switches in the stack. In redundant mode, when the total power budget of the stack is calculated, the wattage of the largest power supply is not included. That power is held in reserve and used to maintain power to switches and attached devices when one power supply fails, enabling the network to operate without interruption. Following the failure of one power supply, the StackPower mode becomes power sharing.

StackPower allows customers to simply add one extra power supply in any switch of the stack and either provide power redundancy for any of the stack members or simply add more power to the shared pool. StackPower eliminates the need for an external redundant power system or installation of dual power supplies in all the stack members. StackPower is available in LAN Base license level (or higher). For LAN Base, cables need to be purchased separately.

Foundation for Open Network Environment

The heart of the Cisco Catalyst 3850 is the UADP ASIC with programmability for future features and intelligence with investment protection. The new ASIC provides the foundation for converged APIs across wired and wireless, Cisco Open Network Environment, software-defined networking (SDN) readiness and OnePK SDK through software updates over the product lifetime.

⁹ Stackpower is not supported on the 48-port 10G SFP+ switch model

¹⁰ Up to nine switches are supported in a star configuration with XPS-2200.

Software Features and Services on Cisco Catalyst 3850 Series Switches

Software services supported on the Cisco Catalyst 3850 Series Switches can be classified into five broad categories:

- Ease of operations
- Advanced security features
- Resiliency
- Application visibility and control

Ease of Operations

The Cisco Catalyst 3850 helps reduce the operating costs through:

- Cisco Catalyst Smart Operations
- Easy-to-use deployment and control features
- Efficient switch operations
- Network management tools

Cisco Catalyst Smart Operations

Cisco Catalyst Smart Operations are a comprehensive set of capabilities that simplify LAN deployment, configuration, and troubleshooting. In addition to adaptive, always-on technologies such as StackWise-480 and StackPower, Cisco Catalyst Smart Operations enable zero-touch installation and replacement of switches, fast upgrade, and ease of troubleshooting with reduced operational cost. Cisco Catalyst Smart Operations are a set of features that includes Smart Install, Auto Smartports, Smart Configuration and Smart Troubleshooting to enhance operational excellence:

- Cisco Smart Install is a transparent plug-and-play technology to configure the Cisco IOS Software image and switch configuration without user intervention. Smart Install utilizes dynamic IP address allocation and the assistance of other switches to facilitate installation, providing transparent network plug and play.
- Cisco Auto Smartports provide automatic configuration as devices connect to the switch port, allowing autodetection and plug and play of the device onto the network.
- Cisco Smart Troubleshooting is an extensive array of debug diagnostic commands and system health checks within the switch, including Generic Online Diagnostics (GOLD) and Onboard Failure Logging (OBFL).
- Embedded Event Manager (EEM) is a powerful and flexible feature that provides real-time network event detection and onboard automation. Using EEM, customers can adapt the behavior of their network devices to align with their business needs. This feature requires the IP Base feature set.

Easy-to-Use Deployment and Control Features

- User experience:
 - IP service-level agreements (SLAs) enable customers to assure new business-critical IP applications, as well as IP services that utilize data, voice, and video, in an IP network. This feature requires the IP Services feature set.
 - DHCP autoconfiguration of multiple switches through a boot server eases switch deployment.

-
- Automatic QoS (AutoQoS) simplifies QoS configuration in voice over IP (VoIP) networks by issuing interface and global switch commands to detect Cisco IP phones, classify traffic, and help enable egress queue configuration.
 - Autonegotiation on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth.
 - Automatic media-dependent interface crossover (MDIX) automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight through) is installed.
 - Simplified configuration and connectivity:
 - Dynamic Trunking Protocol (DTP) facilitates dynamic trunk configuration across all switch ports.
 - Port Aggregation Protocol (PAgP) automates the creation of Cisco Fast EtherChannel groups or Gigabit EtherChannel groups to link to another switch, router, or server.
 - Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad. This feature is similar to Cisco EtherChannel technology and PAgP.
 - Unidirectional Link Detection Protocol (UDLD) and aggressive UDLD allow unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.
 - Cisco VLAN Trunking Protocol (VTP) Version 3 supports dynamic VLANs and dynamic trunk configuration across all switches.
 - Efficient switch operation:
 - Switching database manager (SDM) templates, VLAN template (specific to LAN Base license level), and advanced template allow the administrator to automatically optimize the ternary content-addressable memory (TCAM) allocation to the desired features based on deployment-specific requirements.
 - Local proxy Address Resolution Protocol (ARP) works in conjunction with private VLAN edge to minimize broadcasts and maximize available bandwidth.
 - Stacking master configuration management with Cisco StackWise-480 technology helps make sure that all switches are automatically upgraded when the master switch receives a new software version. Automatic software version checking and updating help ensure that all stack members have the same software version.
 - Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location.
 - Network Timing Protocol (NTP) provides an accurate and consistent timestamp to all intranet switches.
 - Multicast:
 - Optimized multicast for wired plus wireless: Cisco Catalyst 3850 offers greater multicast efficiency by receiving only one multicast stream and replicating it for all connected wired plus wireless devices connected to that switch.
 - Internet Group Management Protocol (IGMP) v1, v2, v3 snooping for IPv4: multicast listener discovery (MLD) v1 and v2 snooping provides fast client joins and leaves of multicast streams and limits bandwidth-intensive video traffic to only the requestors.

-
- **Monitoring:**
 - Remote Switch Port Analyzer (RSPAN) allows administrators to remotely monitor ports in a Layer 2 switch network from any other switch in the same network.
 - For enhanced traffic management, monitoring, and analysis, the Embedded Remote Monitoring (RMON) software agent supports four RMON groups (history, statistics, alarms, and events).
 - Layer 2 traceroute eases troubleshooting by identifying the physical path that a packet takes from source to destination.
 - Wireless RF management provides both real-time and historical information about RF interference affecting network performance across controllers using systemwide Cisco CleanAir technology integration.

Efficient Switch Operation

Cisco Catalyst 3850 Series Switches, designed and engineered by Cisco, provide optimum power-saving, EEE (on RJ45 ports), low-power operations for industry best-in-class power management and power consumption capabilities. The Cisco Catalyst 3850 ports are capable of reduced power modes so that ports not in use can move into a lower power utilization state. Other efficient switch operation features are:

- Cisco Discovery Protocol Version 2 allows the Cisco Catalyst 3850 Series Switches to negotiate a more granular power setting when connecting to a Cisco powered device such as IP phones or access points than what is provided by IEEE classification.
- Per-port power consumption command allows customers to specify maximum power setting on an individual port. Per-port PoE power sensing measures actual power being drawn, enabling more intelligent control of powered devices.
- The PoE MIB provides proactive visibility into power usage and allows customers to set different power-level thresholds.

Environmental Responsibility

Organizations may choose to turn off access point radios to reduce power consumption during off-peak hours. The integrated wireless LAN controller avoids the deployment of additional devices in the network.

Network Management Tools

The Cisco Catalyst 3850 Series Switches offer both a superior CLI for detailed configuration and Cisco Prime™ infrastructure for unified wired plus wireless management. Prime infrastructure provides day 0 and ongoing provisioning, ongoing monitoring and maintenance, configuration templates, and device and user 360-degree views and serves as the FNF collector for user traffic views using the Prime Assurance Manager module.

For detailed information about Cisco Prime infrastructure, go to <http://www.cisco.com/en/US/products/ps12239/index.html>.

Advanced Security Features

Cisco Catalyst 3850 Series Switches support advanced security features including but not limited to:

- Protection against attackers:
 - Port security secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding.

-
- DHCP snooping prevents malicious users from spoofing a DHCP server and sending out bogus addresses. This feature is used by other primary security features to prevent a number of other attacks such as ARP poisoning.
 - Dynamic ARP inspection (DAI) helps ensure user integrity by preventing malicious users from exploiting the insecure nature of ARP.
 - IP source guard prevents a malicious user from spoofing (that is, taking over) another user's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN, and by using it to selectively block bogus packets.
 - The Unicast Reverse Path Forwarding (uRPF) feature helps mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address.
 - Bidirectional data support on a SPAN port allows the Cisco intrusion detection system (IDS) to take action when an intruder is detected.
 - User authentication:
 - Flexible authentication that supports multiple authentication mechanisms, including 802.1X, MAC authentication bypass, and web authentication using a single, consistent configuration.
 - RADIUS change of authorization and downloadable calls for comprehensive policy management capabilities.
 - Private VLAN edge restricts traffic between hosts in a switch by segregating traffic at Layer 2, turning a broadcast segment into a nonbroadcast multiaccess like segment. Private VLAN edge provides security and isolation between switch ports, which helps ensure that users cannot snoop on other users' traffic.
 - Multidomain authentication allows an IP phone and a PC to authenticate on the same switch port while placing them on appropriate voice and data VLAN.
 - MAC address notification allows administrators to be notified of users added to or removed from the network.
 - Mobility and security for secure, reliable wireless connectivity and consistent end-user experience. Increased network availability through proactive blocking of known threats.
 - IGMP filtering provides multicast authentication by filtering out nonsubscribers and limits the number of concurrent multicast streams available per port.
 - ACLs:
 - Cisco security VLAN ACLs on all VLANs prevent unauthorized data flows from being bridged within VLANs.
 - Cisco standard and extended IP security router ACLs define security policies on routed interfaces for control-plane and data-plane traffic. IPv6 ACLs can be applied to filter IPv6 traffic.
 - Port-based ACLs for Layer 2 interfaces allow security policies to be applied on individual switch ports.
 - Device access:
 - Secure Shell (SSH) Protocol, Kerberos, and Simple Network Management Protocol Version 3 (SNMPv3) provide network security by encrypting administrator traffic during Telnet and SNMP sessions. SSH Protocol, Kerberos, and the cryptographic version of SNMPv3 require a special cryptographic software image because of U.S. export restrictions.

-
- TACACS+ and RADIUS authentication facilitates centralized control of the switch and restricts unauthorized users from altering the configuration.
 - Multilevel security on console access prevents unauthorized users from altering the switch configuration.
 - Bridge protocol data unit (BPDU) Guard shuts down Spanning Tree PortFast-enabled interfaces when BPDUs are received to avoid accidental topology loops.
 - Spanning Tree Root Guard (STRG) prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.
 - Wireless end-to-end security offers CAPWAP-compliant DTLS encryption to make sure of encryption between access points and controllers across remote WAN/LAN links.

Resiliency

Borderless networks enable enterprise mobility and business-grade video services. Industry's first unified network (wired plus wireless) location services enable tracking of mobile assets and the users of those assets for both wired plus wireless devices. The true borderless experience is enabled by the following feature sets in the Cisco Catalyst 3850 Series Switches:

- High availability
- High-performance IP routing
- Superior QoS

High Availability

In addition to StackWise-480 and StackPower¹¹, the Cisco Catalyst 3850 Series supports high-availability features including but not limited to the following:

- Cross-Stack EtherChannel provides the ability to configure Cisco EtherChannel technology across different members of the stack for high resiliency.
- Flexlink provides link redundancy with convergence time less than 100ms.
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) provides rapid spanning-tree convergence independent of spanning-tree timers and also offers the benefit of Layer 2 load balancing and distributed processing.
- Per-VLAN Rapid Spanning Tree (PVRST+) allows rapid spanning-tree (IEEE 802.1w) reconvergence on a per-VLAN spanning-tree basis, providing simpler configuration than MSTP. In both MSTP and PVRST+ modes, stacked units behave as a single spanning-tree node.
- Switch-port autorecovery ("err-disable" recovery) automatically attempts to reactivate a link that is disabled because of a network error.

¹¹ Stackpower is not supported on the 48-port 10G SFP+ switch model

¹¹ Stackpower is not supported on the 48-port 10G SFP+ switch model

High-Performance IP Routing

The Cisco Express Forwarding hardware routing architecture delivers extremely high-performance IP routing in the Cisco Catalyst 3850 Series Switches:

- IP unicast routing protocols (static, Routing Information Protocol Version 1 [RIPv1], and RIPv2, RIPv2, Enhanced Interior Gateway Routing Protocol [EIGRP] stub) are supported for small-network routing applications with the IP Base feature set. Limited static routing with the LAN Base feature set. Equal-cost routing facilitates Layer 3 load balancing and redundancy across the stack.
- Advanced IP unicast routing protocols (Open Shortest Path First [OSPF], EIGRP, Border Gateway Protocol Version 4 [BGPv4], and Intermediate System-to-Intermediate System Version 4 [IS-ISv4]) are supported for load balancing and constructing scalable LANs. IPv6 routing (OSPFv3, EIGRPv6) is supported in hardware for maximum performance. OSPF for routed access is included in the IP Base image. The IP Services feature set is required for full OSPF, EIGRP, BGPv4, and IS-ISv4.
- Policy-based routing (PBR) allows superior control by facilitating flow redirection regardless of the routing protocol configured. The IP Base feature set is required for PBR. Virtual routing and forwarding (VRF)-Lite enables a service provider to support two or more VPNs, with overlapping IP addresses. The IP Services feature set is required for VRF-Lite.
- Protocol-independent multicast (PIM) for IP multicast routing is supported, including PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), PIM sparse-dense mode, and source-specific multicast (SSM). The IP Services feature set is required.
- IPv6 addressing is supported on interfaces with appropriate show commands for monitoring and troubleshooting.

Superior QoS

The Cisco Catalyst 3850 Series offers Gigabit Ethernet speed with intelligent services that keep traffic flowing smoothly, even at 10 times the normal network speed. Industry-leading mechanisms for cross-stack marking, classification, and scheduling deliver superior performance for data, voice, and video traffic, all at wire speed.

The following are some of the QoS features supported in the Cisco Catalyst 3850 Series Switches:

- Granular wireless bandwidth management and fair sharing use Cisco's proven Cisco IOS Software and UADP ASIC technology to provide hierarchical bandwidth management at line rate (per access point, per radio, per SSID, per client-based policies). Fair sharing across the users within an SSID makes sure that no single user is starved because of other heavy-hitting users. Fair sharing is automatically enabled for wireless at user level as well as SSID level.
- 802.1p CoS and DSCP field classification is provided, using marking and reclassification on a per-packet basis by source and destination IP address, MAC address, or Layer 4 Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port number.
- Shaped round robin (SRR) scheduling helps ensure differential prioritization of packet flows by intelligently servicing the ingress queues and egress queues. Weighted tail drop (WTD) provides congestion avoidance at the ingress and egress queues before a disruption occurs. Strict priority queuing helps ensure that the highest priority packets are serviced ahead of all other traffic.
- The Cisco committed information rate (CIR) function provides bandwidth in increments as low as 8 Kbps.

-
- Rate limiting is provided based on source and destination IP address, source and destination MAC address, Layer 4 TCP/UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps.
 - Eight egress queues per port for wired traffic and four egress queues for wireless help enable differentiated management of different traffic types across the stack for wired traffic. Up to 2000 aggregate policers are available per switch.

Application Visibility and Control Using Flexible NetFlow

Cisco IOS Software FNF is the next generation in flow visibility technology, allowing optimization of the network infrastructure, reducing operation costs, and improving capacity planning and security incident detection with increased flexibility and scalability. The Cisco Catalyst 3850 provides optimized application visibility with FNF across wired plus wireless. The switch is capable of up to 48,000 flow entries on 48-port models and up to 24,000 flow entries on 12-port and 24-port models across wired plus wireless. With UADP ASIC, Cisco Catalyst 3850 delivers next-generation flow technology with unprecedented flexibility and comprehensive visibility extending from Layer 2 (MAC and VLAN) to Layer 4 (TCP/UDP) flags and so on across wired plus wireless traffic. The Cisco Catalyst 3850 switch is Medianet capable to provide visibility and troubleshooting capabilities across wired plus wireless video traffic. Specific Medianet features will be enabled in future software updates.

The flow data collected by FNF can be exported to an external collector for analysis and reporting or tracked by the EEM. The Cisco Catalyst 3850 enables powerful on-box and customizable event correlation and policy actions with EEM, allowing the switches to trigger customized event alarms or policy actions when the predefined condition is met. With no external appliance required, customers are able to use existing infrastructure to perform traffic monitoring, making traffic analysis economical even on a large IP network.

Details about Cisco FNF are available at

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/ps6965/product_data_sheet0900aecd804b590b.html.

High-performance video over wireless integrates Cisco VideoStream technology to optimize the delivery of video applications across the WLAN.

Wired plus wireless IP telephony supports [unified communications](#) for improved collaboration through messaging, presence, and conferencing and supports all Cisco Unified Communications wireless IP phones for cost-effective, real-time voice service.

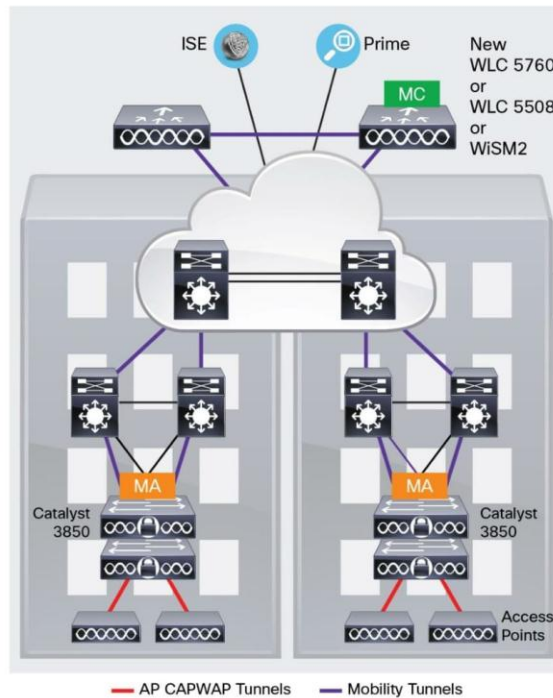
Deployment Options

Campus

In a campus-type deployment, operating the Cisco Catalyst 3850 in the mobility agent mode and centralizing the mobility controller functionality in a WLC 5760, WLC 5508, or WiSM2 helps achieve better scalability and performance. The Cisco Catalyst 3850 provides CAPWAP termination for access points, uniform policy enforcement for wireless clients, better wireless bandwidth, and uniform Cisco IOS Software-based configuration and monitoring for wired plus wireless features. The mobility controller provides central mobility, RRM, and CleanAir coordination.

Backward compatibility with traditional centralized wireless deployment mode on the WLC 5508, WiSM2, and WLC 5760 helps ensure that customers can migrate to the Cisco Catalyst 3850-based converged access approach in phases, providing a continued controller for existing access points. This migration also provides investment protection on the existing wireless controller infrastructure. A phased adoption of the new Cisco Catalyst 3850 helps ensure that migration to the converged access mode of wireless is seamless. Figure 9 shows a Cisco Catalyst 3850 in the campus type deployment.

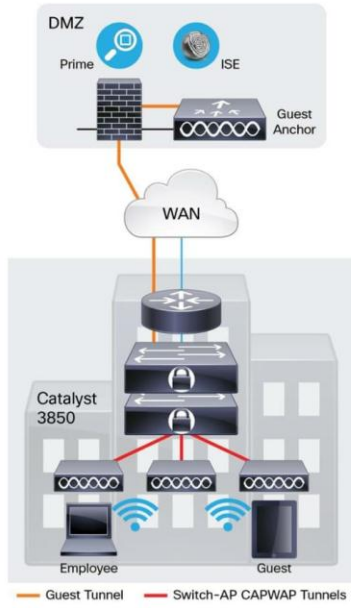
Figure 9. Mobility Controller (MC) and Mobility Agent (MA)



Branch

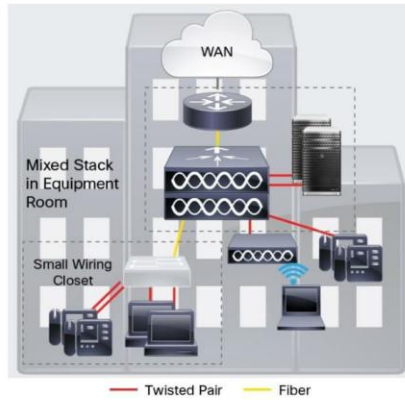
The Cisco Catalyst 3850 is optimized for branch deployments when it operates in mobility controller mode. In this mode, not only can the switch terminate CAPWAP tunnels from the access points and provide client connectivity, it can also manage mobility within the branch. This eliminates the need for a local controller in every branch in addition to the access-layer switches. Also, complete visibility into the wired plus wireless traffic means that the WAN router can prioritize the right wired plus wireless traffic in and out of the branch. Figure 10 shows a Cisco Catalyst 3850 in a branch access type deployment.

Figure 10. Deploying the Cisco Catalyst 3850 in the Branch Access



The new 12-port and 24-port SFP+ or SFP-based Cisco Catalyst 3850 models as well as the nonstackable 48-port SFP+ model can also be used in the branch to aggregate traffic from smaller access switches through fiber links for more secure and EMI-sensitive deployments (Figure 11).

Figure 11. Deploying Mixed Copper and Fiber Connections with a Cisco Catalyst 3850 Stack in the Branch



Cisco Catalyst 3850 Series Specifications

Switch Performance

Table 9 shows Cisco Catalyst 3850 Series Switches performance specifications.

Table 9. Cisco Catalyst 3850 Performance Specifications

Performance Numbers for All Switch Models	
Switching capacity	176 Gbps on 48-port Gigabit Ethernet model 92 Gbps on 24-port Gigabit Ethernet model 68 Gbps on 12-port Gigabit Ethernet model 640 Gbps on 24-port Multigigabit Ethernet model [†] 472 Gbps on 48-port Multigigabit Ethernet model 1280 Gbps on 48-port 10 Gigabit Ethernet SFP+ model [†] 640 Gbps (packet size >= 80 bytes) on 24-port 10 Gigabit Ethernet SFP+ model [†] 320 Gbps on 12-port 10 Gigabit Ethernet SFP+ model [†] [†] Packet size >= 80 bytes
Stacking bandwidth	480 Gbps
Total number of MAC addresses	32,000
Total number of IPv4 routes (ARP plus learned routes)	24,000
FNF entries	48,000 flow on 48-port Gigabit Ethernet models 24,000 flows on 12-port and 24-port Gigabit Ethernet models 96,000 flows on 48-port 10 Gigabit Ethernet SFP+ model 48,000 flows on 24-port 10 Gigabit Ethernet SFP+ model 24,000 flows on 12-port 10 Gigabit Ethernet SFP+ model
DRAM	4 GB (8 GB on 48-port SFP+ model)
Flash	2 GB (4 GB on 12-port and 24-port SFP+ models, 8 GB on 48-port SFP+ model)
VLAN IDs	4,000
Total switched virtual interfaces (SVIs)	1,000
Jumbo frame	9198 bytes
Total routed ports per 3850 stack	208
Wireless	
Number of access points per switch/stack	100
Number of wireless clients per switch/stack	2000
Total number of WLANs per switch	64
Wireless bandwidth per switch	Up to 40 Gbps on 48-port Gigabit Ethernet model Up to 20 Gbps on 24-port Gigabit Ethernet model
Supported Aronet access point series	3600, 3500, 2600, 1600, 1260, 1140, 1040
Forwarding Rate of Switch Models (with 2 x 10 Gigabit + 2 x 1 Gigabit Ethernet uplinks for 12-Port and 24-Port Models and 4 x 10 Gigabit Ethernet Uplinks for 48-Port Models)	
Model	Forwarding Rate
WS-C3850-12S	50.5 Mpps
WS-C3850-24T	68.4 Mpps
WS-C3850-24P	
WS-C3850-24S	
WS-C3850-48T	130.95 Mpps
WS-C3850-48P	
WS-C3850-48F	
WS-C3850-24XU	500 Mpps (80B packets)
WS-C3850-12X48U	460 Mpps (64B packets)
WS-C3850-12XS	227.28 Mpps

Performance Numbers for All Switch Models	
WS-C3850-24XS	454.55 Mpps
WS-C3850-48XS	909 Mpps

Dimensions, Weight, Acoustic, Mean Time between Failure, and Environmental Range Specifications for Cisco Catalyst 3850 Series Switches

Table 10 shows dimensions, weight, acoustic, mean time between failure (MTBF), and environmental range. Weight does not include an uplink FRU. Weight includes the chassis assembly as it is shipped (with fans), one power supply and, and one power supply slot blank.

Table 10. Dimensions, Weight, Acoustic, MTBF, and Environmental Range¹²

Dimensions (H x W x D)	Inches	Centimeters
WS-C3850-12S	1.75 x 17.5 x 17.7	4.45 x 44.5 x 45.0
WS-C3850-24S		
WS-C3850-24T		
WS-C3850-24P		
WS-C3850-48T		
WS-C3850-48P	1.75 x 17.5 x 19.2	4.45 x 44.5 x 48.8
WS-C3850-48F		
WS-C3850-48U		
WS-C3850-24U		
WS-C3850-24XU		
WS-C3850-12X48U	1.75 x 17.5 x 17.7	4.45 X 44.5 x 45.0
WS-C3850-12XS		
WS-C3850-24XS		
WS-C3850-48XS	1.75 x 17.5 x 20.1	4.45 X 44.5 x 51.1
Weight	Pounds	Kilograms
WS-C3850-12S	15.48	7.02
WS-C3850-24S	15.5	7.03
WS-C3850-24T	15.9	7.2
WS-C3850-24P	16.3	7.4
WS-C3850-24U	16.5	7.5
WS-C3850-48T	17.0	7.7
WS-C3850-48P	17.4	7.9
WS-C3850-48F	17.6	8.0
WS-C3850-48U	17.6	8.0
WS-C3850-24XU	17.6	8.0
WS-C3850-12X48U	17.6	8.0
WS-C3850-12XS	12.9	5.8
WS-C3850-24XS	13.5	6.1
WS-C3850-48XS	16.42	7.45
C3850-NM-4-1G	0.66	0.30
C3850-NM-2-10G	0.71	0.32
C3850-NM-4-10G	0.75	0.34
C3850-NM-8-10G	0.74	0.34
C3850-NM-2-40G	0.62	0.28

¹² Additional information about the 48-port SFP+ model will be provided at time of shipment.

MTBF Hours	
WS-C3850-12S	315,840
WS-C3850-24S	300,760
WS-C3850-24T	303,230
WS-C3850-24P	269,450
WS-C3850-24U	237,310
WS-C3850-48T	303,660
WS-C3850-48P	241,050
WS-C3850-48F	241,050
WS-C3850-48U	205,110
WS-C3850-24XU	203,150
WS-C3850-12X48U	202,030
WS-C3850-12XS	371,440
WS-C3850-24XS	307,990
WS-C3850-32XS	307,990
WS-C3850-48XS	286,900
PWR-C1-350WAC	580,710
PWR-C1-715WAC	664,055
PWR-C1-1100WAC	392,174
PWR-C1-440WDC	469,350
C3850-NM-4-1G	7,052,100
C3850-NM-2-10G	4,315,970
C3850-NM-4-10G	3,835,330
C3850-NM-8-10G	6,544,410
C3850-NM-2-40G	9,303,100
Environmental Ranges	
With AC power supply Operating environment and altitude	Normal operating temperature* and altitudes: <ul style="list-style-type: none"> • -5°C to +45°C, up to 5000 feet (1500m) • -5°C to +40°C, up to 10,000 feet (3000m) * Minimum ambient temperature for cold start is 32°F (0°C) Short-term† exceptional conditions: <ul style="list-style-type: none"> • -5°C to +50°C, up to 5000 feet (1500m) • -5°C to +45°C, up to 10,000 feet (3000m) • -5°C to +45°C, at sealevel with single fan failure † Not more than following in one-year period: 96 consecutive hours, or 360 hours total, or 15 occurrences.
With DC power supply Operating environment and altitude (NEBS)	Normal operating temperature and altitudes: <ul style="list-style-type: none"> • -5°C to +45°C, up to 6000 feet (1800m) • -5°C to +40°C, up to 10,000 feet (3000m) • -5°C to +35°C, up to 13,000 feet (4000m) Short-term† exceptional conditions: <ul style="list-style-type: none"> • -5°C to +55°C, up to 6000 feet (1800m) • -5°C to +50°C, up to 10,000 feet (3000m) • -5°C to +45°C, up to 13,000 feet (4000m) • -5°C to +45°C, at sealevel with single fan failure † Not more than following in one-year period: 96 consecutive hours, or 360 hours total, or 15 occurrences.
Relative humidity	10% to 95%, noncondensing
Acoustic noise Measured per ISO 7779 and declared per ISO	With AC or DC power supply (with 24 PoE+ ports loaded): <ul style="list-style-type: none"> • LpA: 43dB typical, 45dB maximum

9296	<ul style="list-style-type: none"> LWA: 5.2B typical, 5.5B maximum
Bystander positions operating to an ambient temperature of 25°C	Typical: Noise emission for a typical configuration Maximum: Statistical maximum to account for variation in production
Storage environment	Temperature: -40°C to 70°C Altitude: 15,000 ft
Vibration	Operating: 0.41Grms from 3 to 500Hz with spectral break points of 0.0005 G2/Hz at 10Hz and 200Hz 5dB/octave roll off at each end. Nonoperating: 1.12Grms from 3 to 500Hz with spectral break points of 0.0065 G2/Hz at 10Hz and 100Hz 5dB/octave roll off at each end.
Shock	Operating: 30G, 2ms half sine Nonoperating: 55G, 10ms trapezoid

Connectors for Cisco Catalyst 3850 Series

Table 11 shows the supported connectors.

Table 11. Connectors

Connectors and cabling	<ul style="list-style-type: none"> 1000BASE-T ports: RJ-45 connectors, 4-pair Cat-5E UTP cabling Multigig-T ports: RJ-45 connectors, 4-pair Cat-5E, Cat-6, Cat6A UTP cabling 1000BASE-T SFP-based ports: RJ-45 connectors, 4-pair Cat-5E UTP cabling 100BASE-FX, 1000BASE-SX, -LX/LH, -ZX, -BX10, DWDM and CWDM SFP transceivers: LC fiber connectors (single-mode or multimode fiber) 10GBASE-SR, LR, LRM, ER, ZR, DWDM SFP+ transceivers: LC fiber connectors (single-mode or multimode fiber) CX1 cable assemblies: SFP+ connector Cisco StackWise-480 stacking ports: copper-based Cisco StackWise cabling Cisco StackPower: Cisco proprietary power stacking cables Ethernet management port: RJ-45 connectors, 4-pair Cat-5 UTP cabling Management console port: RJ-45-to-DB9 cable for PC connections
Power connectors	<ul style="list-style-type: none"> Customers can provide power to a switch by using either the internal power or StackPower from another member in the power stack. The connectors are located at the back of the switch. Internal power supply connector: The internal power supply is an autoranging unit. The internal power supply supports input voltages between 100 and 240VAC. Use the supplied AC power cord to connect the AC power connector to an AC power outlet.

For the latest Cisco transceiver module compatibility information, refer to

<http://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html>.

Management and Standards Support for Cisco Catalyst 3850 Series Switches

Table 12 shows management and standards support for the Cisco Catalyst 3850 Series.

Table 12. Management and Standards Support for the Cisco Catalyst 3850 Series

Description	Specification
Management	BRIDGE-MIB CISCO-AUTH-FRAMEWORK-MIB CISCO-BGP4-MIB, BGP4-MIB CISCO-BRIDGE-EXT-MIB CISCO-BULK-FILE-MIB CISCO-CABLE-DIAG-MIB CISCO-CALLHOME-MIB CISCO-CEF-MIB CISCO-CIRCUIT-INTERFACE-MIB CISCO-ENTITY-VENDORTYPE-OID-MIB CISCO-CONTEXT-MAPPING-MIB CISCO-SNMP-TARGET-EXT-MIB CISCO-STACKMAKER-MIB CISCO-MEMORY-POOL-MIB CISCO-STP-EXTENSIONS-MIB CISCO-SYSLOG-MIB CISCO-TCP-MIB CISCO-UDLD-MIB CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB CISCO-VLAN-MEMBERSHIP-MIB CISCO-VTP-MIB EtherLike-MIB

Description	Specification
	CISCO-DEVICE-LOCATION-MIB
	CISCO-DHCP-SNOOPING-MIB
	CISCO-EIGRP-MIB
	CISCO-EMBEDDED-EVENT-MGR-MIB
	CISCO-ENTITY-FRU-CONTROL-MIB
	CISCO-ENTITY-SENSOR-MIB
	ENTITY-MIB
	CISCO-ERR-DISABLE-MIB
	CISCO-CONFIG-COPY-MIB
	CISCO-FLOW-MONITOR-MIB
	CISCO-FTP-CLIENT-MIB
	CISCO-HSRP-EXT-MIB
	CISCO-HSRP-MIB
	CISCO-IETF-ISIS-MIB
	CISCO-IF-EXTENSION-MIB
	CISCO-IGMP-FILTER-MIB
	CISCO-CONFIG-MAN-MIB
	CISCO-IP-CBR-METRICS-MIB
	CISCO-IPMROUTE-MIB
	CISCO-IP-STAT-MIB
	CISCO-IP-URPF-MIB
	CISCO-L2L3-INTERFACE-CONFIG-MIB
	CISCO-LAG-MIB
	CISCO-LICENSE-MGMT-MIB
	CISCO-MAC-AUTH-BYPASS-MIB
	CISCO-MAC-NOTIFICATION-MIB
	CISCO-MDI-METRICS-MIB
	CISCO-FLASH-MIB
	CISCO-OSPF-MIB
	CISCO-OSPF-TRAP-MIB
	CISCO-PAE-MIB
	CISCO-PAGP-MIB
	CISCO-PIM-MIB
	CISCO-PING-MIB
	CISCO-PORT-QOS-MIB
	CISCO-PORT-SECURITY-MIB
	CISCO-PORT-STORM-CONTROL-MIB
	CISCO-POWER-ETHERNET-EXT-MIB
	CISCO-PRIVATE-VLAN-MIB
	CISCO-PROCESS-MIB
	CISCO-PRODUCTS-MIB
	CISCO-RF-MIB
	CISCO-RTP-METRICS-MIB
	CISCO-RTTMON-MIB
	CISCO-SMART-INSTALL-MIB
	HC-RMON-MIB
	IEEE8021-PAE-MIB
	IEEE8023-LAG-MIB
	IF-MIB
	IGMP-MIB
	IGMP-STD-MIB
	IP-FORWARD-MIB
	IP-MIB
	IPMROUTE-STD-MIB
	LLDP-EXT-MED-MIB
	LLDP-MIB
	NOTIFICATION-LOG-MIB
	OLD-CISCO-MEMORY-MIB
	CISCO-CDP-MIB
	POWER-ETHERNET-MIB
	RMON2-MIB
	RMON-MIB
	SNMP-COMMUNITY-MIB
	SNMP-FRAMEWORK-MIB
	SNMP-MPD-MIB
	SNMP-NOTIFICATION-MIB
	SNMP-PROXY-MIB
	SNMP-TARGET-MIB
	SNMP-USM-MIB
	SNMPv2-MIB
	SNMP-VIEW-BASED-ACM-MIB
	TCP-MIB
	UDP-MIB
	CISCO-IMAGE-MIB
	CISCO-STACKWISE-MIB
	AIRESPACE-WIRELESS-MIB
	CISCO-LWAPP-IDS-MIB
	CISCO-LWAPP-AP-MIB
	CISCO-LWAPP-CCX-RM-MIB
	CISCO-LWAPP-CLIENT-ROAMING-MIB
	CISCO-LWAPP-DOT11-CCX-CLIENT-DIAG-MIB
	CISCO-LWAPP-DOT11-CCX-CLIENT-MIB
	CISCO-LWAPP-DOT11-CLIENT-CCX-REPORTS-MIB
	CISCO-LWAPP-DOT11-CLIENT-MIB
	CISCO-LWAPP-DOT11-MIB
	CISCO-LWAPP-DOWNLOAD-MIB
	CISCO-LWAPP-LINKTEST-MIB
	CISCO-LWAPP-MFP-MIB
	CISCO-LWAPP-MOBILITY-EXT-MIB
	CISCO-LWAPP-QOS-MIB
	CISCO-LWAPP-REAP-MIB
	CISCO-LWAPP-ROGUE-MIB
	CISCO-LWAPP-RRM-MIB
	CISCO-LWAPP-SI-MIB
	CISCO-LWAPP-TSM-MIB
	CISCO-LWAPP-WLAN-MIB
	CISCO-LWAPP-WLAN-SECURITY-MIB

Description	Specification
Standards	IEEE 802.1s IEEE 802.1w IEEE 802.11 IEEE 802.1x IEEE 802.1x-Rev IEEE 802.3ad IEEE 802.3af IEEE 802.3at IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports IEEE 802.1D Spanning Tree Protocol IEEE 802.1p CoS prioritization IEEE 802.1Q VLAN IEEE 802.3 10BASE-T specification IEEE 802.3u 100BASE-TX specification IEEE 802.3ab 1000BASE-T specification IEEE 802.3z 1000BASE-X specification
	RMON I and II standards SNMPv1, SNMPv2c, and SNMPv3

Power Supply Specifications

Table 13 lists the power specifications for the Cisco Catalyst 3850 Series based on the kind of power supply used.

Table 13. Power Specifications for Cisco Catalyst 3850 Series

Description	Specification			
	PWR-C1-1100WAC	PWR-C1-715WAC	PWR-C1-350WAC	PWR-C1-440WDC
Power supply rated maximum	1100W	715W	350W	440W
Total output BTU (Note: 1000 BTU/hr = 293W)	3793 BTU/hr, 1100W	2465 BTU/hr, 715W	1207BTU/hr, 350W	1517BTU/hr, 440W
Input-voltage range and frequency	115-240VAC, 50-60 Hz	100-240VAC, 50-60 Hz	100-240VAC, 50-60 Hz	-36VDC to -72VDC
Input current	12-6A	10-5A	4-2A	<8A at -72VDC <16A at -36VDC
Output ratings	-56V at 19.64A	-56V at 12.8A	-56V at 6.25A	-56V at 7.86A
Output holdup time	10 ms minimum at 102.5VAC	16.7 ms minimum at 100VAC	16.7 ms minimum at 100VAC	> 2ms at -48VDC
Power-supply input receptacles	IEC 320-C16 (IEC60320-C16)	IEC 320-C16 (IEC60320-C16)	IEC 320-C16 (IEC60320-C16)	Terminal strip
Power cord rating	13A	13A	10A	20A at 100VDC
Physical specifications	(H x W x D): 1.58 X 3.25 X 13.7 in Weight: 3 lb (1.4 kg)	(H x W x D): 1.58 X 3.25 X 12.20 in Weight: 2.8 lb (1.3 kg)	(H x W x D): 1.58 X 3.25 X 12.20 in Weight: 2.6 lb (1.2 kg)	(H x W x D): 1.58 X 3.25 X 12.20 in Weight: 2.6 lb (1.2 kg)
Operating temperature	23 to 113°F (-5 to 45°C)			
Storage temperature	-40 to 158°F (-40 to 70°C)			
Relative humidity operating and nonoperating noncondensing	5 to 90% noncondensing			
Altitude	10,000 ft. (3000 meters), up to 45°C			
MTBF	Calculated MTBF must be greater than 300,000 using Telcordia SR-332, Method 1, Case 3. Demonstrated MTBF is 500,000 hr (with 90% confidence level).			

Description	Specification
EMI and EMC compliance	FCC Part 15 (CFR 47) Class A ICES-003 Class A EN 55022 Class A CISPR 22 Class A AS/NZS 3548 Class A BSMI Class A (AC input models only) VCCI Class A EN 55024, EN300386, EN 50082-1, EN 61000-3-2, EN 61000-3-3 EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN 61000-6-1
Safety compliance	UL 60950-1, CAN/CSA-C22.2 No. 60950-1, EN 60950-1, IEC 60950-1, CCC, CE Marking
LED indicators	*AC OK*: Input power to the power supply is OK *PS OK*: Output power from the power supply is OK

Power Consumption of Standalone Cisco Catalyst 3850 Series Switches

Table 14 shows power consumption of standalone Cisco Catalyst 3850 Series Switches based on Alliance for Telecommunications Industry Solutions (ATIS) testing using IMIX distribution stream traffic, with input voltage of 115VAC at 60 Hz and no PoE loading. The values given are the maximum possible power consumption numbers under the respective test scenarios.

Table 14. Power Consumptions (in Watts) of Standalone Cisco Catalyst 3850 Series

Models	Uplink Module	Power Consumption (W) (No More Than)				
		0% Traffic	10% Traffic	100% Traffic	Weighted Average	
WS-C3850-12S	C3850-NM-4-1G	85.84	85.89	86.75	86.0	
WS-C3850-24S		104.48	104.25	105.12	104.4	
WS-C3850-12S	C3850-NM-2-10G	87.95	88.30	90.04	88.4	
WS-C3850-24S		106.24	106.58	109.75	106.9	
WS-C3850-24T	C3850-NM-4-1G	83.47	82.86	83.76	83.04	
WS-C3850-24P		86.81	86.22	87.11	86.40	
WS-C3850-24U		81.5	81.4	82.1	81.5	
WS-C3850-48T		117.74	116.62	117.59	116.89	
WS-C3850-48P		125.35	124.15	125.15	124.43	
WS-C3850-48F		130.10	128.91	129.85	129.18	
WS-C3850-48U		114.8	114.7	115.6	114.8	
WS-C3850-24T		C3850-NM-2-10G	81.97	81.83	84.97	82.16
WS-C3850-24P			85.22	85.04	88.32	85.39
WS-C3850-24U			82.8	82.6	84.8	82.9
WS-C3850-48T	117.56		116.74	120.40	117.23	
WS-C3850-48P	123.78		122.90	126.75	123.42	
WS-C3850-48F	129.89	129.06	132.36	129.18		
WS-C3850-48U	116.8	116.9	119.9	117.2		
WS-C3850-48T	C3850-NM-4-10G	120.56	120.28	127.24	121.02	
WS-C3850-48P		129.59	129.64	135.96	130.27	
WS-C3850-48F		137.57	137.06	143.77	137.81	
WS-C3850-48U		119.9	121.2	127.7	121.5	
WS-C3850-12XS		109.0	109.5	112.7	109.7	

Models	Uplink Module	Power Consumption (W) (No More Than)			
		0% Traffic	10% Traffic	100% Traffic	Weighted Average
WS-C3850-24XU	C3850-NM-8-10G	229.7	231.2	248.1	232.7
WS-C3850-12X48U		191.3	193.6	208.1	194.8
WS-C3850-24XS		183.6	185.3	205.5	187.2
WS-C3850-24XS	C3850-NM-2-40G	159.2	161.1	177.0	162.5
WS-C3850-48XS	None	267.0	268.3	288.1	270.1

Safety and Compliance

Table 15 lists the safety and compliance information for the Cisco Catalyst 3850 Series.

Table 15. Safety and Compliance Information for Cisco Catalyst 3850 Series

Description	Specification
Safety certifications	UL 60950-1 Second Edition CAN/CSA-C22.2 No. 60950-1 Second Edition EN 60950-1 Second Edition IEC 60950-1 Second Edition NOM (obtained by partners and distributors)
Electromagnetic emissions certifications	47CFR Part 15 (CFR 47) Class A (FCC Part 15 Class A) AS/NZS CISPR22 Class A CISPR22 Class A EN55022 Class A ICES003 Class A VCCI Class A EN61000-3-2 EN61000-3-3 KN22 Class A KCC CNS13438 Class A EN55024 CISPR24 KN24
Environmental	Reduction of Hazardous Substances (ROHS) 5
Noise specifications	Office Product Spec: 48dBA at 30°C (refer to ISO 7779)
Telco	CLEI code

Cisco Enhanced Limited Lifetime Hardware Warranty

The Cisco Catalyst 3850 Series Switches come with an E-LLW that includes NBD delivery of replacement hardware where available and 90 days of 8x5 Cisco TAC support.

Your formal warranty statement, including the warranty applicable to Cisco software, appears in the Cisco information packet that accompanies your Cisco product. We encourage you to review carefully the warranty statement shipped with your specific product before use.

Cisco reserves the right to refund the purchase price as its exclusive warranty remedy.

For further information about warranty terms, visit <http://www.cisco.com/go/warranty>. Table 16 provides information about the E-LLW.

Table 16. E-LLW Details

	Cisco E-LLW
Device covered	Applies to Cisco Catalyst 3850 Series Switches.
Warranty duration	As long as the original customer owns the product.
EoL policy	In the event of discontinuance of product manufacture, Cisco warranty support is limited to 5 years from the announcement of discontinuance.
Hardware replacement	Cisco or its service center will use commercially reasonable efforts to ship a replacement for NBD delivery, where available. Otherwise, a replacement will be shipped within 10 working days after receipt of the RMA request. Actual delivery times might vary depending on customer location.
Effective date	Hardware warranty commences from the date of shipment to customer (and in case of resale by a Cisco reseller, not more than 90 days after original shipment by Cisco).
TAC support	Cisco will provide during business hours, 8 hours per day, 5 days per week basic configuration, diagnosis, and troubleshooting of device-level problems for up to a 90-day period from the date of shipment of the originally purchased Cisco Catalyst 3850 product. This support does not include solution or network-level support beyond the specific device under consideration.
Cisco.com access	Warranty allows guest access only to Cisco.com.

Licensing for Cisco Catalyst 3850 Series Switches

The three feature sets available with all Cisco Catalyst 3850 Series Switches are:

- LAN Base: Enterprise access layer 2 switching features
- IP Base: Enterprise access layer 3 switching features
- IP Services: Advanced enterprise layer 3 switching (IPv4 and IPv6) features

The LAN Base feature set offers enhanced intelligent services that include comprehensive Layer 2 features, with up to 255 VLANs. The IP Base feature set provides entry-level enterprise services in addition to all LAN Base features, with 1K VLANs. IP Base also includes the support for wireless controller functionality (mobility agent and mobility controller role; additional access point license required for mobility controller role), routed access, smart operations, FNF, and so on. The IP Services feature set provides full enterprise services that include advanced Layer 3 features such as EIGRP, OSPF, BGP, PIM, and IPv6 routing such as OSPFv3 and EIGRPv6. All software feature sets support advanced security and MQC-based QoS.

The Cisco Catalyst 3850 Series Switches with LAN Base feature set can only stack with other Cisco Catalyst 3850 Series LAN Base switches. The same applies to IP Base and IP Services as well. A mixed stack of LAN Base switch with IP Base or IP Services feature set is not supported.

The 12-port and 24-port SFP+- and SFP-based models as well as the 48-port SFP+ model can only be ordered with IP Base or IP Services licenses. Therefore, in order to stack with LAN Base models, they need to be configured in LAN Base mode from the CLI.

Customers can transparently upgrade the software feature set in the Cisco Catalyst 3850 Series Switches through Cisco IOS Software CLI using the right to use (RTU)-based software upgrade process. Software activation enables the Cisco IOS Software feature sets. Based on the license's type, Cisco IOS Software activates the appropriate feature set. License types can be changed, or upgraded, to activate a different feature set.

Access Point License for Cisco Catalyst 3850

An access point license is required for Cisco Catalyst 3850 operating in mobility controller mode. No access point license is required for 3850 operating in mobility agent mode. This functionality is included in the IP Base feature set. Other devices that can act as mobility controller are the WLC 5760, WLC 5508, and WiSM2 wireless controllers. Access point licenses can be transferred only between two 3850 switches or between 3850 and 5760 controller and vice versa.

Software Policy for Cisco Catalyst 3850 Series Switches

Customers with Cisco Catalyst LAN Base and IP Base software feature sets will be provided with maintenance updates and bug fixes designed to maintain the compliance of the software with published specifications, release notes, and industry standards compliance as long as the original end user continues to own or use the product or up to one year from the end-of-sale date for this product, whichever occurs earlier. Customers with licenses for our IP Services software images require a service support contract such as Cisco SMARTnet™ Service to download updates. This policy supersedes any previous warranty or software statement and is subject to change without notice.

Cisco ONE Software

[Cisco ONE Software for Access Switching](#) is available for the Cisco Catalyst 3850 Series Switches.

Cisco ONE Software is a new way for customers to purchase and use our infrastructure software. It offers a simplified consumption model, centered on common customer scenarios in the data center, WANs, and LANs.

Cisco ONE Software and services provide customers with four primary benefits:

- Software suites that address typical customer use scenarios at an attractive price
- Investment protection of their software purchase through software services-enabled license portability
- Access to ongoing innovation and new technology with Cisco Software Support Service (SWSS)
- Flexible licensing models to smoothly distribute customer's software spend over time

For ordering information for Cisco ONE Software for the Cisco Catalyst 3850 Series Switches, go to <http://www.cisco.com/c/en/us/products/software/one-access/switching-part-numbers.html>.

Cisco and Partner Services for Next-Generation Cisco Catalyst Fixed Switches

Enable the innovative, secure, intelligent edge in the Borderless Network Architecture using personalized services from Cisco and our partners. Through a discovery process that begins with understanding your business objectives, we help you integrate the next-generation Cisco Catalyst fixed switches into your architecture and incorporate network services onto that platform. Sharing knowledge and leading practices, we support your success every step of the way as you deploy, absorb, manage, and scale new technology. Choose from a flexible suite of support services designed to meet your business needs and help you maintain high-quality network performance while controlling operational costs. (See Table 17.)

Table 17. Technical Services Available for Cisco Catalyst 3850 Switches

Technical Services
<p>Cisco SMARTnet Service</p> <ul style="list-style-type: none"> • Around-the-clock, global access to the Cisco TAC • Unrestricted access to the extensive Cisco.com knowledge base and tools • Next-business-day, 8x5x4, 24x7x4, and 24x7x2 advance hardware replacement and onsite parts replacement and installation available • Ongoing operating system software updates within the licensed feature set • Proactive diagnostics and real-time alerts on Smart Call Home-enabled devices
<p>Cisco Smart Foundation Service</p> <ul style="list-style-type: none"> • NBD advance hardware replacement as available • Business hours access to SMB TAC (access levels vary by region) • Access to Cisco.com SMB knowledge base • Online technical resources through Smart Foundation Portal • Operating system software bug fixes and patches
<p>Cisco SP Base Service</p> <ul style="list-style-type: none"> • Around-the-clock, global access to the Cisco TAC • Registered access to Cisco.com • NBD, 8x5x4, 24x7x4, and 24x7x2 advance hardware replacement; return to factory option available² • Ongoing operating system software updates¹
<p>Cisco Focused Technical Support Services</p> <ul style="list-style-type: none"> • Three levels of premium, high-touch services are available: <ul style="list-style-type: none"> ◦ Cisco High-Touch Operations Management Service ◦ Cisco High-Touch Technical Support Service ◦ Cisco High-Touch Engineering Service • Valid Cisco SMARTnet or SP Base contracts on all network equipment are required

Notes:

¹ Cisco operating system updates include the following: maintenance releases, minor updates, and major updates within the licensed feature set.

² Advance hardware replacement is available in various service-level combinations. For example, 8x5xNBD indicates that shipment will be initiated during the standard 8-hour business day, 5 days a week (the generally accepted business days within the relevant region), with NBD delivery. Where NBD is not available, same day ship is provided. Restrictions apply; for details, review the appropriate service descriptions.

Ordering Information

Table 18 lists ordering information for the Cisco Catalyst 3850 Series. To place an order, visit the Cisco Ordering homepage at http://www.cisco.com/en/US/ordering/or13/or8/order_customer_help_how_to_order_listing.html.

Table 18. Cisco Catalyst 3850 Series Ordering Information

Product Number	Product Description
Cisco Catalyst 3850 Series	
WS-C3850-24T-L	Stackable 24 10/100/1000 Ethernet ports, with 350WAC power supply 1 RU, LAN Base feature set (StackPower cables need to be purchased separately)
WS-C3850-48T-L	Stackable 48 10/100/1000 Ethernet ports, with 350WAC power supply 1 RU, LAN Base feature set (StackPower cables need to be purchased separately)
WS-C3850-24P-L	Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715WAC power supply 1 RU, LAN Base feature set (StackPower cables need to be purchased separately)
WS-C3850-24U-L	Stackable 24 10/100/1000 Ethernet UPOE ports, with 1100WAC power supply 1 RU, LAN Base feature set (StackPower cables need to be purchased separately)
WS-C3850-48P-L	Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715WAC power supply 1 RU, LAN Base feature set (StackPower cables need to be purchased separately)

Product Number	Product Description
WS-C3850-48F-L	Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100WAC power supply 1 RU, LAN Base feature set (StackPower cables need to be purchased separately)
WS-C3850-48U-L	Stackable 48 10/100/1000 Ethernet UPOE ports, with 1100WAC power supply 1 RU, LAN Base feature set (StackPower cables need to be purchased separately)
WS-C3850-24T-S	Stackable 24 10/100/1000 Ethernet ports, with 350WAC power supply 1 RU, IP Base feature set
WS-C3850-48T-S	Stackable 48 10/100/1000 Ethernet ports, with 350WAC power supply 1 RU, IP Base feature set
WS-C3850-24P-S	Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715WAC power supply 1 RU, IP Base feature set
WS-C3850-24U-S	Stackable 24 10/100/1000 Ethernet UPOE ports, with 1100WAC power supply 1 RU, IP Base feature set
WS-C3850-48P-S	Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715WAC power supply 1 RU, IP Base feature set
WS-C3850-48F-S	Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100WAC power supply 1 RU, IP Base feature set
WS-C3850-48U-S	Stackable 48 10/100/1000 Ethernet UPOE ports, with 1100WAC power supply 1 RU, IP Base feature set
WS-C3850-24T-E	Stackable 24 10/100/1000 Ethernet ports, with 350WAC power supply 1 RU, IP Services feature set
WS-C3850-48T-E	Stackable 48 10/100/1000 Ethernet ports, with 350WAC power supply 1 RU, IP Services feature set
WS-C3850-24P-E	Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715WAC power supply 1 RU, IP Services feature set
WS-C3850-24U-E	Stackable 24 10/100/1000 Ethernet UPOE ports, with 1100WAC power supply 1 RU, IP Services feature set
WS-C3850-48P-E	Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715WAC power supply 1 RU, IP Services feature set
WS-C3850-48F-E	Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100WAC power supply 1 RU, IP Services feature set
WS-C3850-48U-E	Stackable 48 10/100/1000 Ethernet UPOE ports, with 1100WAC power supply 1 RU, IP Services feature set
WS-C3850-12X48U-L	Stackable 48 10/100/1000 with 12 100Mbps/1/2.5/5/10 Gbps UPOE Ethernet ports, with 1100W AC power supply 1RU, LAN Base feature set
WS-C3850-12X48U-S	Stackable 48 10/100/1000 with 12 100Mbps/1/2.5/5/10 Gbps UPOE Ethernet ports, with 1100W AC power supply 1RU, IP Base feature set
WS-C3850-12X48U-E	Stackable 48 10/100/1000 with 12 100Mbps/1/2.5/5/10 Gbps UPOE Ethernet ports, with 1100W AC power supply 1RU, IP Services feature set
WS-C3850-24XU-L	Stackable 24 100Mbps/1/2.5/5/10 Gbps UPOE Ethernet ports, with 1100W AC power supply 1RU, LAN Base feature set
WS-C3850-24XU-S	Stackable 24 100Mbps/1/2.5/5/10 Gbps UPOE Ethernet ports, with 1100W AC power supply 1RU, IP Base feature set
WS-C3850-24XU-E	Stackable 24 100Mbps/1/2.5/5/10 Gbps UPOE Ethernet ports, with 1100W AC power supply 1RU, IP Services feature set
WS-C3850-12S-S	Stackable 12 SFP Ethernet ports, with 350WAC power supply 1 RU, IP Base feature set
WS-C3850-12S-E	Stackable 12 SFP Ethernet ports, with 350WAC power supply 1 RU, IP Services feature set
WS-C3850-24S-S	Stackable 24 SFP Ethernet ports, with 350WAC power supply 1 RU, IP Base feature set

Product Number	Product Description
WS-C3850-24S-E	Stackable 24 SFP Ethernet ports, with 350WAC power supply 1 RU, IP Services feature set
WS-C3850-12XS-S	Stackable 12 SFP+ Ethernet ports, with 350WAC power supply 1 RU, IP Base feature set
WS-C3850-12XS-E	Stackable 12 SFP+ Ethernet ports, with 350WAC power supply 1 RU, IP Services feature set
WS-C3850-24XS-S	Stackable 24 SFP+ Ethernet ports, with 715WAC power supply 1 RU, IP Base feature set
WS-C3850-24XS-E	Stackable 24 SFP+ Ethernet ports, with 715WAC power supply 1 RU, IP Services feature set
WS-C3850-48XS-S	Standalone, 48 SFP+ and 4 QSFP+ Ethernet ports, with 750WAC front-to-back power supply 1 RU, IP Base feature set
WS-C3850-48XS-E	Standalone, 48 SFP+ and 4 QSFP+ Ethernet ports, with 750WAC front-to-back power supply 1 RU, IP Services feature set
WS-C3850-48XS-F-S	Standalone, 48 SFP+ and 4 QSFP+ Ethernet ports, with 750WAC back-to-front power supply 1 RU, IP Base feature set
WS-C3850-48XS-F-E	Standalone, 48 SFP+ and 4 QSFP+ Ethernet ports, with 750WAC back-to-front power supply 1 RU, IP Services feature set
Cisco Catalyst 3850 Bundles	
WS-C3850-24PW-S	Cisco Catalyst 3850 24-port PoE IP Base with 5 access point license
WS-C3850-48PW-S	Cisco Catalyst 3850 48-port PoE IP Base with 5 access point license
WS-C3850-24UW-S	Cisco Catalyst 3850 24 Port UPOE with 5 access point licenses IP Base
WS-C3850-48W-S	Cisco Catalyst 3850 48 Port PoE with 5 access point licenses IP Base
WS-C3850-48UW-S	Cisco Catalyst 3850 48 Port UPOE with 5 access point licenses IP Base
WS-C3850-24XUW-S	Cisco Catalyst 3850 24 Port UPOE with 24 100Mbps/1/2.5/5/10 Gbps and 5 access point licenses IP Base
WS-C3850-12X48UW-S	Cisco Catalyst 3850 48 Port UPOE with 12 100Mbps/1/2.5/5/10 Gbps and 5 access point licenses IP Base
WS-C3850-16XS-S	Cisco Catalyst 3850 12 SFP+ port stackable model, with C3850-NM-4-10G module and 350WAC power supply. 1 RU, IP Base feature set
WS-C3850-16XS-E	Cisco Catalyst 3850 12 SFP+ port stackable model, with C3850-NM-4-10G module and 350WAC power supply. 1 RU, IP Services feature set
WS-C3850-32XS-S	Cisco Catalyst 3850 24 SFP+ port stackable model, with C3850-NM-8-10G module and 715WAC power supply. 1 RU, IP Base feature set
WS-C3850-32XS-E	Cisco Catalyst 3850 24 SFP+ port stackable model, with C3850-NM-8-10G module and 715WAC power supply. 1 RU, IP Services feature set
Network Modules for the Cisco Catalyst 3850 Series	
C3850-NM-4-1G=	4 x Gigabit Ethernet network module spare
C3850-NM-2-10G=	4 x Gigabit Ethernet/2 x 10 Gigabit Ethernet network module spare
C3850-NM-BLANK=	Network module blank spare
C3850-NM-4-10G=	4 x Gigabit Ethernet/4 x 10 Gigabit Ethernet network module spare
C3850-NM-8-10G=	8 x Gigabit Ethernet/8 x 10 Gigabit Ethernet network module spare
C3850-NM-2-40G=	2 x 40 Gigabit Ethernet network module spare
Software Licenses	
C3850-12-S-E	Cisco Catalyst 3850 12-port IP Base to IP Services RTU paper license
C3850-24-L-S	Cisco Catalyst 3850 24-port Switch LAN Base to IP Base RTU paper license
C3850-48-L-S	Cisco Catalyst 3850 48-port Switch LAN Base to IP Base RTU paper license
C3850-24-L-E	Cisco Catalyst 3850 24-port LAN Base to IP Services RTU paper license
C3850-48-L-E	Cisco Catalyst 3850 48-port LAN Base to IP Services RTU paper license
C3850-24-S-E	Cisco Catalyst 3850 24-port IP Base to IP Services RTU paper license

Product Number	Product Description
C3850-48-S-E	Cisco Catalyst 3850 48-port IP Base to IP Services RTU paper license
L-C3850-24-L-S	Cisco Catalyst 3850 24-port LAN Base to IP Base RTU electronic license
L-C3850-48-L-S	Cisco Catalyst 3850 48-port LAN Base to IP Base RTU electronic license
L-C3850-24-L-E	Cisco Catalyst 3850 24-port LAN Base to IP Services RTU electronic license
L-C3850-48-L-E	Cisco Catalyst 3850 48-port LAN Base to IP Services RTU electronic license
L-C3850-24-S-E	Cisco Catalyst 3850 24-port IP Base to IP Services RTU electronic license
L-C3850-48-S-E	Cisco Catalyst 3850 48-port IP Base to IP Services RTU electronic license
L-C3850-12-S-E	Cisco Catalyst 3850 12-port IP Base to IP Services RTU electronic license
Access Point Licenses	
L-LIC-CT3850-UPG	Primary upgrade license SKU for Cisco 3850 wireless controller (e-delivery)
L-LIC-CTIOS-1A	1 access point adder license for Cisco IOS Software based wireless controller (e-delivery)
LIC-CT3850-UPG	Primary upgrade license SKU for Cisco 3850 wireless controller (paper license)
LIC-CTIOS-1A	1 access point adder license for the Cisco IOS Software based wireless controller (paper license)
Power Supplies and Fan for the Cisco Catalyst 3850 Series	
PWR-C1-350WAC=	350WAC power supply spare
PWR-C1-715WAC=	715WAC power supply spare
PWR-C1-1100WAC=	1100WAC power supply spare
PWR-C1-440WDC=	440WDC power supply spare
PWR-C1-BLANK=	Power supply blank spare
PWR-C3-750WAC-R=	750WAC power supply spare front-to-back airflow for 48XS
PWR-C3-750WAC-F=	750WAC power supply spare back-to-front airflow for 48XS
PWR-C3-750WDC-R=	750WDC power supply spare front-to-back airflow for 48XS
PWR-C3-750WDC-F=	750WDC power supply spare back-to-front airflow for 48XS
FAN-T3-R=	Fan module spare front-to-back airflow for 48XS
FAN-T3-F=	Fan module spare back-to-front airflow for 48XS
C3850-FAN-T1=	Cisco Catalyst 3850 and WLC 5760 Type 1 Fan Module
StackWise-480 and StackPower Cables for the Cisco Catalyst 3850 Series	
STACK-T1-50CM=	Cisco StackWise-480 50cm stacking cable spare
STACK-T1-1M=	Cisco StackWise-480 1m stacking cable spare
STACK-T1-3M=	Cisco StackWise-480 3m stacking cable spare
CAB-SPWR-30CM=	Cisco Catalyst 3850 StackPower cable 30cm spare
CAB-SPWR-150CM=	Cisco Catalyst 3850 StackPower cable 150cm spare
Spare Power Cords for the Cisco Catalyst 3850 Series	
CAB-TA-NA=	AC power cord for Cisco Catalyst 3850 (North America)
CAB-TA-AP=	AC power cord for Cisco Catalyst 3850 (Australia)
CAB-TA-AR=	AC power cord for Cisco Catalyst 3850 (Argentina)
CAB-TA-SW=	AC power cord for Cisco Catalyst 3850 (Switzerland)
CAB-TA-UK=	AC power cord for Cisco Catalyst 3850 (United Kingdom)
CAB-TA-JP=	AC power cord for Cisco Catalyst 3850 (Japan)
CAB-TA-250VAC-JP=	Japan 250VAC power cord for Cisco Catalyst 3850 (Japan)
CAB-TA-EU=	AC power cord for Cisco Catalyst 3850 (Europe)
CAB-TA-IT=	AC power cord for Cisco Catalyst 3850 (Italy)
CAB-TA-IN=	AC power cord for Cisco Catalyst 3850 (India)
CAB-TA-CN=	AC power cord for Cisco Catalyst 3850 (China)

Product Number	Product Description
CAB-TA-DN=	AC power cord for Cisco Catalyst 3850 (Denmark)
CAB-TA-IS=	AC power cord for Cisco Catalyst 3850 (Israel)
CAB-ACBZ-12A=	AC power cord for Cisco Catalyst 3850 (Brazil), 12A/125V BR-3-20 plug up to 12A
CAB-ACBZ-10A=	AC power cord for Cisco Catalyst 3850 (Brazil), 10A/250V BR-3-10 plug up to 10A
CAB-C15-CBN	Cabinet jumper power cord, 250 VAC 13A, C14-C15 connectors
Spare Accessory and Rack Mount Kits for the Cisco Catalyst 3850 Series	
C3850-ACC-KIT=	Accessory kit for Cisco Catalyst 3850 Series
C3850-RAC-KIT=	Rack mount kit for Cisco Catalyst 3850 Series
C3850-4PT-KIT=	Extension rails and brackets for four-point mounting for Cisco Catalyst 3850 Series

Optics Compatibility Information

The Cisco Catalyst 3850 Series supports a wide range of optics. Because the list of supported optics is updated on a regular basis, consult the tables available here for the latest QSFP+, SFP+, and SFP compatibility information: http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. [Learn more.](#)



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA

C78-720918-19 03/16

© 2016 Cisco and/or its affiliates. This document is Cisco Public Information.

Page 35 of 35

