ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“OPTIMIZACIÓN Y MEJORA DE LA RED DE DATOS DEL HOSPITAL LEÓN BECERRA"

INFORME DE MATERIA INTEGRADORA

Previo a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

DIEGO MANUEL BELTRÁN TRIVIÑO

FLAVIO PAÚL GOYÓN CASTILLO

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTOS

Agradezco a Dios por darme la oportunidad de llegar hasta estas instancias de mi formación profesional, a mis padres Manuel y Carmen por sus valiosos consejos y apoyo incondicional, a mis hermanos que aportaron en varias circunstancias; agradezco también a Melissa por haber estado pendiente de mí, apoyándome y dándome ánimos cada día; y, por último, pero no menos importante a mis profesores de LICRED que fueron los que aportaron con sus conocimientos durante todos estos años de estudio.

Diego Manuel Beltrán Triviño

Agradezco a Dios por brindarme salud, sabiduría y fortaleza; y por haber permitido que culminase una de mis metas al completar este ciclo de mi formación profesional, a mis padres Flavio y Blanca, mis hermanos por su completo apoyo en cada fase de mi desarrollo, a la Facultad de Ingeniería Eléctrica y Computación, LICRED y maestros por brindar la oportunidad de desarrollar este proyecto y poder compartir los conocimientos brindados en clase con la comunidad ecuatoriana.

Flavio Paul Goyón Castillo

DEDICATORIA

Dedico este trabajo especialmente a Dios, el cual día y noche me ha permitido trabajar arduamente para cumplir todas mis responsabilidades, me brindó sabiduría, el responsable de mis éxitos. Quiero dedicar también este trabajo a mis padres, hermanos, novia Meli, amigos de carrera y profesores, que han estado presentes en cada situación que se presentaba durante esta etapa universitaria, ofreciéndome lo mejor de ellos para obtener mi título.

Diego Manuel Beltrán Triviño

Dedico este trabajo a Dios, por permitirme haber llegado a este importante momento llenándome de entusiasmo y optimismo cada día. Además, quiero dedicar este trabajo a mi madre por ser mi pilar más importante, demostrándome su cariño y apoyo a pesar de las diferencias en opiniones. A mi padre, a pesar de la separación repentina que se generó, siento que donde te encuentras te encontrarías orgulloso de lo que representa este momento para mí. A mis hermanos, amigos, compañeros y profesores que han dedicado un espacio para compartir conmigo brindándome apoyo para lograr esta meta.

Flavio Paul Goyón Castillo

TRIBUNAL DE EVALUACIÓN

Msg. Robert Andrade Troya	**Msc. Jorge Magallanes**
PROFESOR EVALUADOR	PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

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

Diego Manuel Beltrán Triviño

Flavio Paúl Goyón Castillo

RESUMEN

El Hospital León Becerra de Guayaquil cuenta con una red de datos, la cual presenta problemas de comunicación, tanto en la parte funcional como en la parte administrativa.

Este proyecto propone mitigar los problemas encontrados en la red de datos. Está basado en el diseño de mecanismos como: Un sistema de cableado estructurado con normas de implementación que nos permite tener un cableado ordenado importante al momento de resolver un problema en un punto específico de la red o a nivel general y máximo rendimiento en los enlaces. Otro mecanismo utilizado es la segmentación de la red con el objetivo de dividir el tráfico, balancear cargas y aplicar seguridad a cada segmento de red. En cuanto a la administración de la red se usará un sistema que nos permite aplicar políticas de seguridad y ofrecer servicios a todos los trabajadores del hospital.

En el primer capítulo, antecedentes y problemática, se incluye una pequeña introducción de cómo es la empresa y se expone la situación actual de la red de datos del Hospital. Además, se especifican los objetivos, alcance y limitaciones.

En el segundo capítulo, requerimientos, se detalla cada uno de los requerimientos y las necesidades que tienen los servicios que maneja el hospital.

En el tercer capítulo, diseño de la solución, se da una propuesta de solución a cada uno de los requerimientos analizados en el anterior capitulo y a las necesidades que tiene el hospital en su infraestructura de red. En éste se detallan los componentes de la solución para la parte pasiva y activa de la red LAN. Así mismo, se propone una administración de los recursos de la red entre ellos los usuarios y equipos.

En el cuarto capítulo, se muestra un presupuesto estimado incluyendo mano de obra para realizar la implementación del proyecto, así mismo se realiza una planificación del tiempo para implementar todo el proyecto.

Finalmente aparece la sección de conclusiones y recomendaciones, en la cual se muestra los resultados de nuestros objetivos planteados, así mismo se sugieren acciones y mejoras al momento de realizar la implementación del proyecto.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

1. ANTECEDENTES Y PROBLEMÁTICA.

El Hospital León Becerra, es una institución perteneciente al estado ecuatoriano, encargada de prestar servicios como son: Medicina general, operación, terapias físicas, farmacia y hospitalización.

Cuando el personal de IT (Information Technology) del Hospital León Becerra implementó la red de datos, no se tomaron ciertas consideraciones como la implementación de un sistema de cableado basado en normas internacionales, implementación de equipos administrables y de alto rendimiento. Esto quiere decir que la red presenta una gran debilidad hablando específicamente de la infraestructura tecnológica y no cumple con las diversas exigencias que las nuevas tecnologías requieren.

1.1. Estructura de la empresa.

Las instalaciones del hospital ocupan una manzana entera la cual tiene una superficie rectangular, de un lado mide aproximadamente 150 metros y del otro lado 80 metros. Para una mejor administración de las diversas zonas, departamentos y áreas se han dividido en 5 bloques las instalaciones del hospital; el hospital cuenta con un parqueadero de autos, el cual tiene salida a la entrada principal del hospital que es la calle Bolivia; la ubicación de las áreas será mostrada en la Figura 1.1.

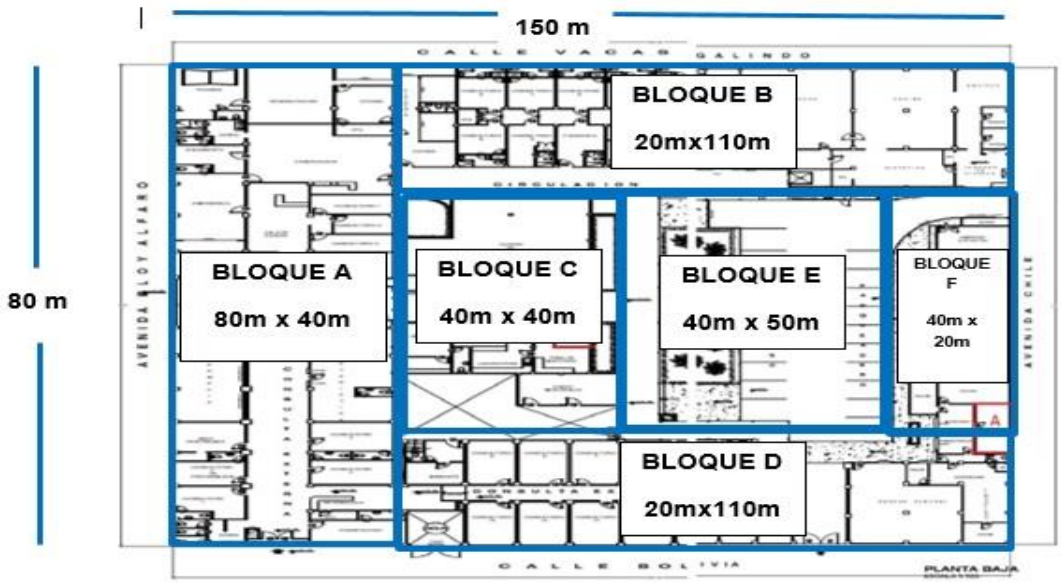


Figura 1.1: Plano general del Hospital León Becerra de Guayaquil.

El hospital es de dos plantas, constituido por los siguientes departamentos sistemas, gestión ambiental y procesos, contabilidad, financiera, pagaduría, auditoria médica, laboratorio, servidores (aquí encontraremos los servidores de imagen, base de datos, contabilidad, aplicaciones, hospitalización y marcación), biometría, proveeduría.

Los bloques son de diferentes medidas como se los puede observar en la Figura1.1, estos bloques están divididos en los diversos departamentos ya mencionados.

1.2. Investigación de campo.

El análisis general del entorno en que trabajamos permitió conocer la situación actual de la red de datos, así mismo se pudo conocer mejor el lugar, el personal que trabaja en cada departamento y ver los principales problemas que se están dando con respecto a la red de datos.

Se realizaron los siguientes pasos para identificar los problemas:

- Recopilación de información mediante una inspección del hospital.
- Se buscaron los planos del hospital para reconocer cada área y poder guiarnos dentro del mismo.

- Se realizaron recorridos por el hospital junto al personal de sistemas para revisar los diferentes dispositivos, sistemas y tecnologías usadas en cada departamento. Incluye el cableado estructurado del lugar.
- Adicional se solicitó información al departamento de sistemas para conocer como es la administración de los recursos informáticos en el hospital.

1.3. Situación actual de la red de datos del Hospital León Becerra.

1.3.1. Usuarios de la red de datos.

En este proyecto se han considerado todos los empleados del hospital. Se dio a conocer que en el hospital existen 300 empleados en total en todas las áreas de los cuales solo 120 empleados son usuarios de la red de datos. El resto de empleados no tiene acceso a la red de datos.

1.3.2. Análisis de los elementos de la red: Parte activa.

El hospital León Becerra posee una red de datos que tiene como fin proveer la comunicación entre los distintos departamentos del hospital.

La red del hospital posee un cuarto de telecomunicaciones donde están ubicados los equipos principales de la red, los cuales proveen conectividad a los equipos secundarios y estos a las estaciones de trabajo de cada departamento.

La topología de red de datos del Hospital León Becerra de Guayaquil es mostrada en la Figura 1.2. Se puede ver que los equipos de networking están conectados en cascada distribuyéndose a cada departamento. Se utiliza equipos no administrables los cuales complican la correcta administración de anchos de banda, servicios, aplicación de seguridad, entre otros factores.

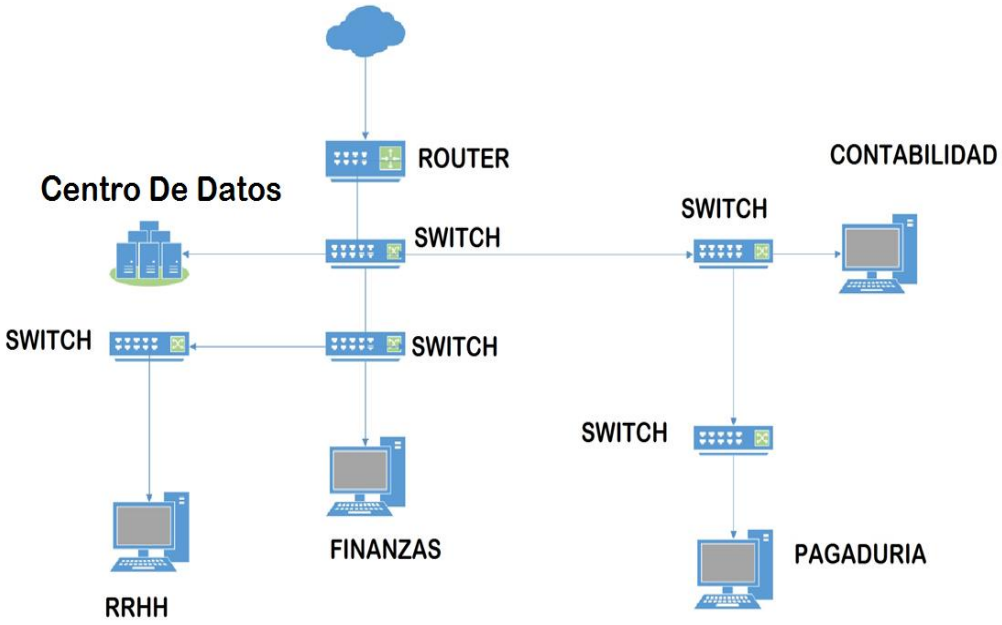


Figura 1.2: Ejemplo de un segmento de red del Hospital León Becerra.

Existen 120 estaciones de trabajo, de modo que los dispositivos están conectados a switch's no administrables, los mismos que se conectan al cuarto de telecomunicaciones mediante cable UTP Categoría 5 y en algunos casos cables UTP Categoría 6. [1]

La red del Hospital León Becerra cuenta con las características reflejadas en la siguiente tabla 1 que se presenta a continuación:

	DESCRIPCIÓN
Estaciones de trabajo	120 equipos / red cableada
Medio	Cable de cobre
Modelo Jerárquico	NO
Tipo de cable	UTP Categoría 5, UTP Categoría 6
Velocidad de transmisión	100 Mbps
Distancia Máxima de cable	100 metros
Ancho de banda para conexión a internet (proveedor Telconet)	7 Mbps

Tabla 1: Descripción actual de la red.

El rendimiento, velocidad, escalabilidad de la red dependerá de las características de los equipos y las configuraciones establecidas en cada uno de ellos. En la tabla 2 se puede ver la ubicación de estos equipos y descripción de los mismos, ya que al momento de analizar la red serán de gran importancia conocer su uso y características.

DISPOSITIVOS DE RED				
DEPARTAMENTO	**TIPO/ESTADO**	**MODELO**	**PUERTOS**	**PUERTOS OCUPADOS**
Auditoría	Switch-inactivo	Trendnet TEG-S24Dg	24	15
Administración	Router inalámbrico-activo	TP-Link	4	2
Contabilidad	Switch-activo	Trendnet TEG-S24Dg	24	3
Talento humano	Switch-inactivo	HP	24	10
Talento humano	Switch-activo	Trendnet TEG-S24Dg	24	
Talento humano	Router inalámbrico-activo	DLink	5	1
Proveeduría	Router-activo	Linksys DEFSR41	4	2
Proveeduría	Router inalámbrico-activo	D-Link DIR-610N+	4	1
Emergencia	Switch-activo	TL-SF1016	16	5
Emergencia	Switch-activo	TP-Link TL-SF1008D	8	6
Hospitalización	Switch-activo	TP-Link TL-SF1008D	8	
Pensionado Baquerizo	Switch-activo	TP-Link TL-SF1008D	8	5
Pensionado especial	Switch-inactivo	TP-Link TL-SF1008D	8	3
Farmacia	Switch-activo	Trendnet TEG-S24Dg	24	9
Presidencia	Router-activo	DLink	4	
Presidencia	Router-activo	DLink	4	
Sistemas	Switch-activo	HP	5	4
Sistemas	Switch-activo	HP	24	24
Sistemas	Switch-activo	HP	24	24
Sistemas	Router-activo	DLink	4	

Consulta interna	Switch-activo	3 com 3GBLUG16A	24	
Corredor	Switch-inactivo	TP-Link TL-SF1008D	8	
Cirugía	Switch-inactivo	TP-Link TL-SF1008D	8	
Total de equipos	**23 equipos**			

Tabla 2: Especificaciones de equipos por departamento, modelo, puertos.

Adicional a estos equipos existen 5 servidores conectados a un switch. A continuación, se detalla la función de los servidores en el hospital:

- Servidor de Imágenes (Linux).
- Servidor de Aplicaciones (Pruebas, páginas web, etc.).
- Servidor de Contabilidad y Base de Datos.
- Servidor de Sistema de Marcación.
- Servidor de Sistema de Hospitalización.
- Existen 2 equipos-servidores sin utilizar.

Las características de estos servidores se presentan en la siguiente tabla 3:

Nombre del Servidor	Memoria	Disco Duro	Procesador
S. Imágenes	1 GB	80 GB	Intel Xeon X5460
S. Aplicaciones	1 GB	60 GB	Intel Xeon E5450
S. Contabilidad y BD	2 GB	2 de 80 GB	Intel Xeon X5460
S. Marcación	1 GB	60 GB	Intel Xeon E5450
S. Hospitalización	2 GB	80 GB	Intel Xeon E5450

Tabla 3: Características de los servidores.

Existen 96 puntos de datos distribuidos en los diversos departamentos del hospital. En la tabla 4 se puede visualizar la información de la cantidad de puntos de red que tienen instalados.

DEPARTAMENTO/ÁREA	NÚMEROS DE PUNTO DE RED
Sistemas	15
Ambiental y procesos	1
Contabilidad financiera	31
Pagaduría	1
Contabilidad	31
Auditoria médica	1
Laboratorios	1
Biometría	1
Proveeduría	1
Servidores	10
Piso 1 sala izquierda	1
Piso 1 sala derecha	1
Piso 2 sala derecha	1
Total	96

Tabla 4: Puntos de red de acuerdo al departamento.

1.3.3. Direccionamiento IP.

La red de datos del Hospital León Becerra de Guayaquil actualmente trabaja con un bloque de direcciones IP privadas, la red que usa es la 192.168.1.0/24. Estas direcciones IP son asignadas de manera estática a los equipos de red.

Las direcciones IP son asignadas de acuerdo con el orden de implementación del equipo, no cuentan con un plan de direccionamiento o una guía de las IP´s a usar de forma ordenada. Actualmente, hay 141 direcciones ocupadas quedando 112.

Los usuarios del Hospital tienen acceso a Internet mediante el ISP (Proveedor de Servicios de Internet) TELCONET, se encarga de hacer la traducción de dirección es decir realiza el proceso de cambiar la dirección IP privada a una pública (NAT).

Cuentan con 4 IP públicas de las cuales quedan disponibles 2 de ellas, una fue asignada al servidor web y la otra a un servidor de pruebas.

En los ANEXOS se muestran las direcciones IP ocupadas y disponibles para próximos equipos de red.

1.3.4. Análisis de los elementos de la red: Parte pasiva.

El Hospital León Becerra de la ciudad de Guayaquil cuenta con un sistema de cableado, el cual no cumple con los estándares internacionales lo cual también complica al personal de soporte en el momento de querer resolver un problema. El cableado se lo ha instalado por partes o fases por lo que no presenta un backbone vertical. El hospital tiene en sus instalaciones cableado UTP categoría 5 y categoría 6, se conectan a los diversos equipos activos como switch con las computadoras.

Se encuentran cables sin etiquetar por lo que la localización de éstos es difícil y conlleva más tiempo encontrar su ubicación. El mantenimiento y búsqueda de averías también se ve afectado.

No todos los departamentos presentan canaletas para el cableado, como se muestra en las Figura 1.3 y Figura 1.4. Por lo que muchas veces el cable se encuentra en el piso o pasando por alguna pared a simple vista por los techos.

Figura 1.3: Cables de datos enviados por tubos de agua.

Figura 1.4: Cables de datos en los techos junto a cables eléctricos.

El Hospital León Becerra cuenta con un cuarto de telecomunicaciones. En este cuarto está el rack de los equipos, los patch-panels y la terminación del cableado tanto el horizontal como el vertical.

Para ingresar a este cuarto de equipos el acceso es muy fácil ya que no posee ningún mecanismo de seguridad o autenticación (tarjetas magnéticas, candados, biométricos, etc.), que permita el ingreso al mismo. Solo cuenta con una puerta de madera.

En la Figura 1.5 se ve que no hay ningún tipo de seguridad, cualquier persona puede tener acceso hacia los servidores, router, swicth, patch-panels sin ninguna restricción.

Figura 1.5: Falta de seguridad en la puerta de acceso a cuarto de telecomunicaciones.

Ciertos cables y equipos presentan etiquetado otros no cuentan con un etiquetado. Se puede observar que no cuentan con la documentación indispensable para realizar una correcta administración de equipos, cableado y sistemas por parte del departamento de Sistemas el cual es el encargado.

Al no contar con una correcta documentación al momento de que suceden problemas como desconexión de algún cable, recalentamiento de equipos, entre otros problemas, no se puede actuar inmediatamente ya que es difícil poder identificar de donde viene el problema lo cual afecta directamente a que se pierda información y tiempo

En el cuarto de equipos solo se deben guardar equipos que estén relacionados con el sistema de telecomunicaciones del hospital en este caso se han encontrado otras cosas como modulares, repisas, cartones, maquinas dañadas y equipos arrimados reciclados.

Se destaca que el cuarto de equipos posee un sistema de aire acondicionado.

Con respecto al sistema de energía eléctrica, existe un sistema puesto a tierra, adicional cuenta con UPS y estabilizadores de energía para los equipos de comunicación, estos brindan corriente estabilizada lo que evita que aumente o baje la energía. En la figura 1.6 se observa que los equipos y cables de datos están cercanos a cables de energía eléctrica los cuales son fuentes de interferencias electromagnéticas, además no cumplen con normas de seguridad.

Figura 1.6: Alimentación eléctrica.

En la figura 1.7 se puede observar que los cables en el rack se encuentran desordenados, no existe una organización completa de los cables por lo que se hace muy difícil identificar cual punto le corresponde a un determinado cable.

Figura 1.7: Rack y equipos principales de la red.

1.4. Objetivos generales y específicos.

1.4.1. Objetivo General.

Rediseñar la red de datos del Hospital León Becerra de Guayaquil aplicando normas, estándares de cableado estructurado, medidas de administración y seguridad de la red.

1.4.2. Objetivos Específicos.

- Describir especificaciones técnicas junto a características de los equipos de redes necesarios para hacer funcionar correctamente la red de datos.
- Diseñar una topología para brindar alta disponibilidad de equipos y confiabilidad de servicios.
- Definir la segmentación de la red permitiendo una mejor administración de los recursos e información.
- Diseñar una infraestructura basada en Active Directory para administrar de manera centralizada los recursos de la red, además de servicios necesarios para el uso del hospital y brindar mecanismos de seguridad.
- Definir medidas de seguridad de manera física y lógica que permita asegurar la información que maneja el hospital.

1.5. Justificación del Problema.

Una de las necesidades más importantes de un Hospital es brindar atención médica y servicios de calidad para sus pacientes. Un hospital maneja mucha información privada tanto de sus pacientes como de la misma institución.

Una de las características primordiales que debe tener esta red es la disponibilidad debido que los doctores necesitan acceder a la información de los pacientes tanto de manera local como a información que posee el IESS de los afiliados de una manera rápida y a su vez segura que implica la integridad de sus datos, por lo que en este proyecto se plantea cubrir con la parte de disponibilidad, rapidez y seguridad.

1.6. Alcance y Limitaciones.

1.6.1. Alcances

- El proyecto está destinado para el Hospital León Becerra de la ciudad de Guayaquil, el cual podrá ser analizado por el departamento de sistemas para su ejecución e implementación.
- En la propuesta de la nueva red de datos para el hospital, se plantea un diseño más eficiente y acorde a la realidad, que permitirá reducir los problemas y mejorar la administración de la red de datos.
- Al realizar el diseño lógico de la red de datos se pretende que la red de datos tenga la capacidad de ser escalable, eficiente y óptima parar poder ser usada sin problemas.

1.6.2. Limitaciones

- El proyecto únicamente se enfoca en el rediseño de la red del hospital, no se analizará a fondo el tema de instalaciones eléctricas.
- El tiempo de implementación es también una de las limitantes, ya que el hospital no puede cerrar sus puertas, ni apagar toda la red de datos para poder realizar el trabajo de implementación.
- El área donde se desea realizar las instalaciones e implementación de equipos será una de las limitaciones, ya que hay que determinar si lo que se propone en el proyecto con respecto a los cuartos de equipos y el cableado, se lo puede implementar en esa determinada zona.
- Se deberá recolectar información actual de los equipos de red que estén en funcionamiento, ya sean antiguos o nuevos.
- En este proyecto no se podrá realizar la implementación del rediseño de la red y las pruebas correspondientes ya que la ejecución de nuestro proyecto dependerá de la autorización del jefe de Sistemas del Hospital y su grupo de trabajo.

CAPÍTULO 2

2. REQUERIMIENTOS.

Basándose en los requerimientos del hospital, además de los servicios y aplicaciones de importancia para la red del hospital se establecieron los siguientes requerimientos:

- Contar con acceso a los recursos de la red (Servidores, Aplicaciones, ancho de banda).
- Tener un cableado estructurado con un estándar acorde a las exigencias para redes de hospitales.
- Disponibilidad en el acceso a los servidores y a internet.
- Direccionamiento IP distribuidos por departamentos.
- Administración de los recursos de acuerdo a la jerarquía.

2.1. Disponibilidad en el acceso a los servidores y a internet.

El hospital al trabajar con información de afiliados necesita conectarse mediante internet a la base de datos del IESS, por lo que se necesita un ancho de banda óptimo para la consulta y posterior almacenamiento de la información, para lo cual se ha hecho el estudio mediante fórmulas para definir el ancho de banda apropiado para el uso de los doctores que usan este servicio. Adicionalmente, existe personal que también necesita el uso de internet, alrededor de 53 usuarios en total son los que utilizaran este recurso, por lo que se ha procedido a realizar el cálculo respectivo que se detalla más adelante.

2.2. Análisis de los requerimientos de ancho de banda.

De acuerdo a un estudio realizado en conjunto con el personal del departamento de sistemas, se pudo establecer las prioridades para así tener segmentado el tráfico de la red de acuerdo a los de mayor importancia para así poder administrar de mejor forma el ancho de banda y asignar prioridad a los datos más importantes que necesitan ser transmitidos. Se desea que la

red del hospital pueda soportar diferentes servicios sin que presenten problemas constantemente. Los servicios, aplicaciones y sistemas que funcionarán en esta red serán:

- Acceso a internet.
  - Conectividad alámbrica.
  - Conectividad con los servidores del IESS.
  - Acceso a correo electrónico.
  - Páginas web.
  - Subida y descarga de archivos.
- Acceso a bases de datos.

En este capítulo se presentan los requerimientos para la nueva red de datos con el objetivo de obtener una óptima comunicación tanto dentro de la LAN, como para la conexión hacia internet.

2.2.1. Cálculos de tráfico de red.

Para la selección de un adecuado ancho de banda se procedió a realizar cálculos matemáticos que permiten conocer cuál es el ancho de banda mínimo para el óptimo desempeño de cada aplicación.

Sabiendo que a partir del 2015 las páginas web promedios tienen una estructura y un peso de 2262 KB [2] definido en la siguiente figura 2.1:

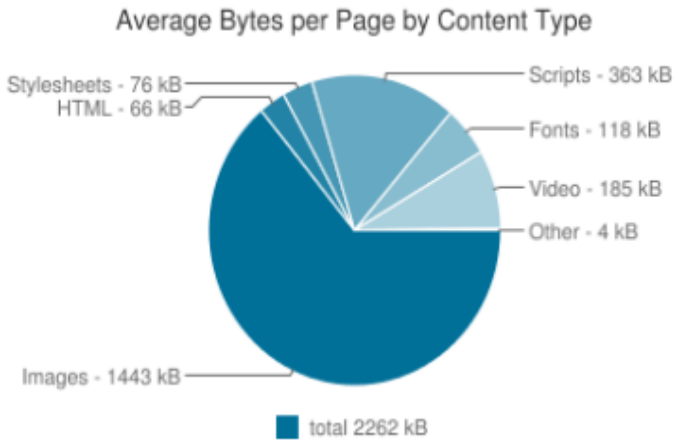


Figura 2.1: Peso de un archivo, dividido por tipo de sistema o aplicación.

Con estos datos se realiza el cálculo en función de los requerimientos que tiene cada usuario con permisos de acceder a páginas web para así conocer la capacidad del ancho de banda necesario para el correcto funcionamiento acorde a las expectativas de los usuarios. El tamaño de referencia utilizado es 2262 KBytes y con un tiempo de 10 segundos de carga máxima.

Donde:

Cpw = Es la capacidad necesaria para un rendimiento aceptable para tener acceso a una página web.

Tpw = Es el tamaño de referencia de una página web.

tpw = Es el tiempo promedio que toma una página web en cargar.

$$C_{PW} = T_{PW} * t_{PW} \qquad (2.1)$$

Cpw = 2262 KB * 10 seg

Cpw = 22620 KB/s ó 180960 kbps

Así mismo dará a conocer la cantidad de ancho de banda que usaremos para él envió de correos electrónicos aplicamos la siguiente formula, donde: 128KBytes es el valor máximo de ancho de banda que consume un correo electrónico y 10 segundos que es el tiempo aceptable de descarga del mismo.

Donde:

CCE = Es la velocidad adecuada para un correo electrónico.

TCE = Es el tamaño aproximado de un correo electrónico.

tCE = Es el periodo de tiempo que le toma a un correo electrónico en cargar.

$$C_{CE} = T_{CE} * t_{CE} \qquad (2.2)$$

CCE = 128 KB * 10 seg

CCE= 1280 KB/s ó 10240 kbps

Por último, se muestra el cálculo del ancho de banda necesario para la descarga de datos se emplea la siguiente formula [3]:

Donde:

N= número de usuarios de la red.

G= el ancho de banda asignado a cada usuario.

C= número de personas estimados que estarán descargando datos simultáneamente.

$$AB = G * C \qquad (2.3)$$

$$AB = 256\ Kbps * 25 = 6400\ Kbps$$

Una vez obtenido el consumo de ancho de banda de cada servicio podemos definir que, para un rendimiento estable, la red debería soportar un mínimo de 8.312 kbps.

2.3. Requerimiento del sistema de cableado estructurado.

El Hospital León Becerra con el fin de mejorar los procedimientos y servicios que se ofrecen en la institución desean que, al momento de rediseñar la red de datos, esta sea capaz de soportar diversas aplicaciones cumpliendo con características como alta velocidad, efectividad, disponibilidad y una red de calidad. Por lo tanto, se ha elegido entre una de las mejoras la tecnología

Gigabit Ethernet la cual ofrece más efectividad, velocidad y mejora el rendimiento de la red.

Es importante definir que en este proyecto se debe usar cable de cobre UTP categoría 6A, ya que este es capaz de soportar hasta 10 GPS en velocidad de transmisión hasta 100 metros. Este tipo de cable soporta aplicaciones actuales y así mismo aplicaciones futuras, lo que permitirá que si se desean cambiar los equipos actuales la red sea capaz de ser escalable y adaptable sin sufrir bajas de rendimiento.

Con un cable de estas características junto a equipos de gran rendimiento se podrá manejar mejor la transmisión de datos, el consumo de ancho de banda y los servicios del hospital. Adicional hay que recalcar que esta categoría de cable puede ser compatible con otras categorías de cables como la 5, 5e, 6g.

Hay que tener en cuenta que al momento de implementar esta categoría de cableado se deberá realizar una actualización o mejora de los elementos del cableado como jacks, patch cords, patch panel ya que deben ser de la misma categoría para mejorar el rendimiento de la red.

El nuevo diseño de cableado se ajusta a las necesidades actuales de la institución y a futuras necesidades así mismo se ajusta a las nuevas tecnologías y funcionalidades de la red, sin dejar a un lado el costo que se ahorrara en el futuro realizando una correcta implementación.

En el hospital actualmente existe un único cuarto de equipos de telecomunicaciones el cual se encuentra mal ubicado dentro de la institución por lo cual se desea que se realice un estudio para poder tener una mejor ubicación y realizar la creación del cuarto de equipos de telecomunicaciones o ver si es preferible tener más cuartos destinados para alojar los equipos principales del hospital. También, se debe tomar en cuenta la creación de un cuarto de entrada de servicios el cual servirá para conectar el hospital a los servicios del proveedor de internet u otros servicios externos necesarios. Este cuarto separara los equipos que puede manejar o administrar el hospital y lo que pertenece a proveedores externos, esto es lo que se conoce como el

punto de demarcación. En este cuarto se encuentran los equipos de conexión y protección de la red.

Luego de analizar distintas necesidades se ha determinado diseñar nuevos puntos de red en las diversas áreas o departamentos las cuales deben tener dos salidas, se ha hecho esta propuesta con la visión de que en un futuro se necesite colocar más equipos en una determinada área.

2.4. Direccionamiento IP distribuidos por departamentos.

El Hospital cuenta con un plan de direccionamiento IP desordenado, por lo que, al momento de existir un error, en algún punto de la red se tiene inconvenientes para identificar de manera rápida y precisa cual fue el punto de falla. Por lo que uno de los requerimientos además del orden, es que sea de una manera dinámica y por servicios para así no tener que preocuparse por la asignación manual si no que sea un dispositivo el que se encargue de realizar este trabajo facilitando la resolución de errores.

2.5. Administración de los recursos.

Para el hospital es muy importante la administración de los recursos y seguridad de la información por lo que se requiere que solo su personal pueda acceder al uso de los recursos y de la información.

Además, que se desea conceder diferentes permisos y restricciones a los usuarios de la red dependiendo del departamento y puesto que tenga estos permisos se necesita que sean por jerarquía.

La seguridad es un punto clave puesto que al trabajar con información de pacientes como de datos de pacientes afiliados que provee el IESS, lo que se requiere es un nivel de seguridad acorde a la importancia de los datos que se transitan por la red del hospital.

2.6. Requerimiento de una red Inalámbrica

Se estima que los doctores podrían usar tecnologías inalámbricas como celulares, laptops, tablets, etc, para sus consultas con los pacientes por lo que se desea darles todas las facilidades para que puedan cumplir con su trabajo

de una manera más eficaz y eficiente por lo que se requiere que en el área de consulta externa exista una red que permita conectarse a internet de conexión inalámbrica, con un nivel de seguridad adecuado al igual que el ancho de banda.

CAPÍTULO 3

3. DISEÑO DE LA SOLUCIÓN.

3.1. Propuesta de diseño del Sistema de cableado estructurado.

La propuesta de rediseño del sistema tiene como fin cumplir con los estándares que se mencionara luego los cuales permitirán lograr las mejores condiciones de implementación.

Se desea realizar una instalación de cableado estructurado que soporte las tecnologías actuales, pero a la vez tecnologías futuras. Además, debe permitir una fácil administración y mantenimiento para el personal encargado.

Actualmente, el cableado del hospital León Becerra no cumple con las normas internacionales y es por eso que se realiza la propuesta de un cableado estructurado basado en las normas ANSI/TIA/EIA.

3.1.1. Especificaciones de los Estándares.

Para la correcta implementación del sistema de cableado se aplicarán las normas establecidas por organismos internaciones las cuales permiten proponer un buen diseño del sistema de cableado y sus elementos.

Se utiliza la norma ANSI/TIA-1179, la cual indica parámetros exclusivos para el sector de la salud [4] [5], sin embargo, se utilizarán otras normas importantes para el desarrollo del proyecto. A continuación, se muestra las normas/estándares a usar y una breve descripción del uso que le daremos [8][9]:

Estándar ANSI/TIA-568-C.1: Especifica las normas para edificios comerciales.

Estándar ANSI/TIA/EIA-568-B y 568 D-1: Especifica como instalar el cableado en los edificios comerciales.

Estándar ANSI/TIA/EIA-569: Especifica las rutas y espacios para el sistema de cableado.

Estándar ANSI/TIA/EIA-606: Especifica la manera de administrar la infraestructura.

Estándar ANSI/TIA/EIA-607: Esta norma específica los requerimientos para el correcto funcionamiento de equipos utilizando la energía eléctrica adecuada dentro de un edificio comercial.

Para implementar un sistema completo de cableado estructurado se lo ha dividido en subsistemas los cuales se los analizará uno a uno y se especificará las características necesarias según las normas. Entre los subsistemas de cableado tenemos:

- Cableado Vertical.
- Cableado horizontal.
- El cuarto de telecomunicaciones.
- Cuarto de equipos.
- Estaciones de trabajo.
- Sistema de puesta a tierra.
- Cuarto de entrada de los servicios.

3.1.2. Especificaciones para el cableado vertical.

En el hospital se implementará una topología del cableado vertical en forma de estrella, el rack ubicado en el ER será el centro de la estrella de donde partirán cables de fibra óptica hacia los rack’s en los TR de cada zona. Se usará cable de fibra óptica multimodo om3, ya que la distancia que existe entre los cuartos de telecomunicaciones no es larga, menos de 1km. En la siguiente figura 3.1 se puede ver la distribución del cableado vertical entre los dos pisos del hospital.

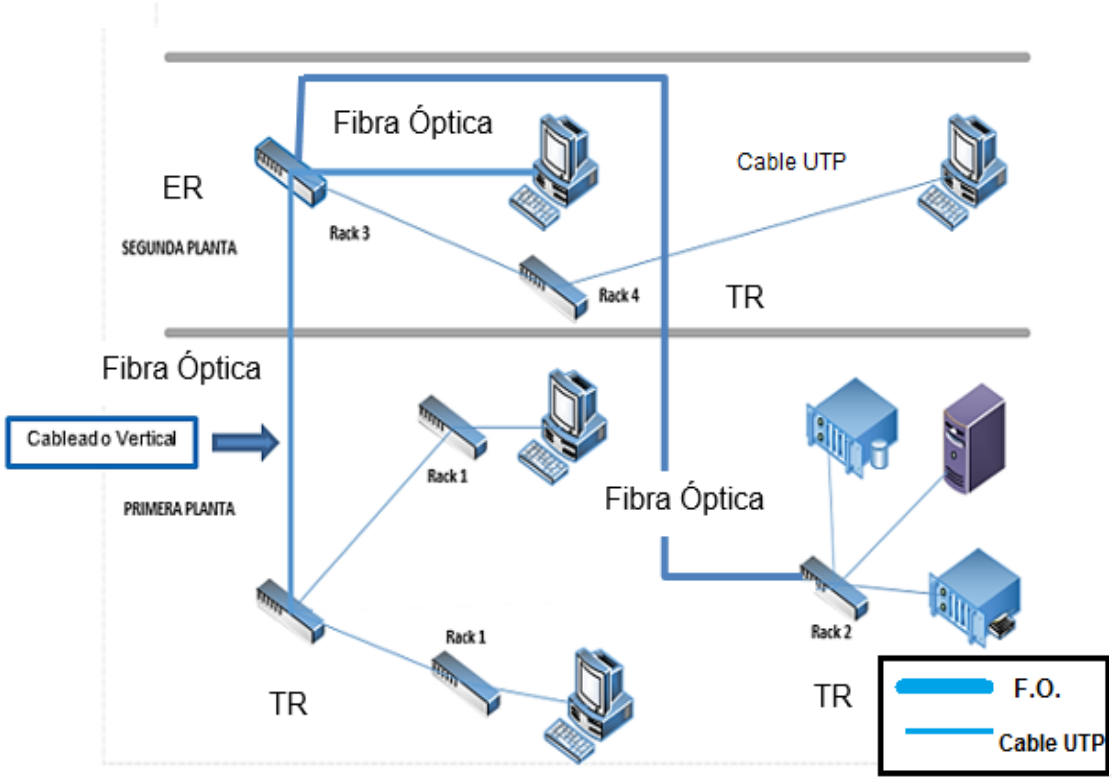


Figura 3.1: Diagrama del cableado vertical.

3.1.3. Especificaciones para el cableado horizontal.

En el hospital el sistema de cableado horizontal se regirá bajo la norma ANSI/TIA/EIA 568-B [10]. Este cableado es el que se va a extender desde las estaciones de trabajo al cuarto de telecomunicaciones ubicado en las diferentes zonas del hospital y de este a las estaciones de trabajo.

Según la norma 568-B al momento de implementar el cableado horizontal en el hospital León Becerra se deben cumplir los siguientes requerimientos:

- Debe facilitar el mantenimiento, ser capaz de crecer en un futuro y aunque se cambie de ubicación las estaciones de trabajo el cableado pueda ser usado.

- Se debe considerar que el cableado no se encuentre tan cerca al cableado eléctrico ya que este generara niveles de interferencia lo cual provocaría daños al cable de cobre.
- Los elementos necesarios en el sistema de cableado como paneles, patch cord y los conectores que van en la pared deben ser de igual categoría que el cable es decir 6A para aprovechar mejor las características del cable.
- Al momento de conectar los equipos que se encuentran en el cuarto de telecomunicaciones con el patch panel se deberá tomar en cuenta que el cable debe medir 5 metros y 3 metros desde los equipos de cada usuario al punto de pared como se lo muestra en la figura 3.2.
- Los cables categoría 6A serán enviados por canaletas para una mejor organización de los mismos.

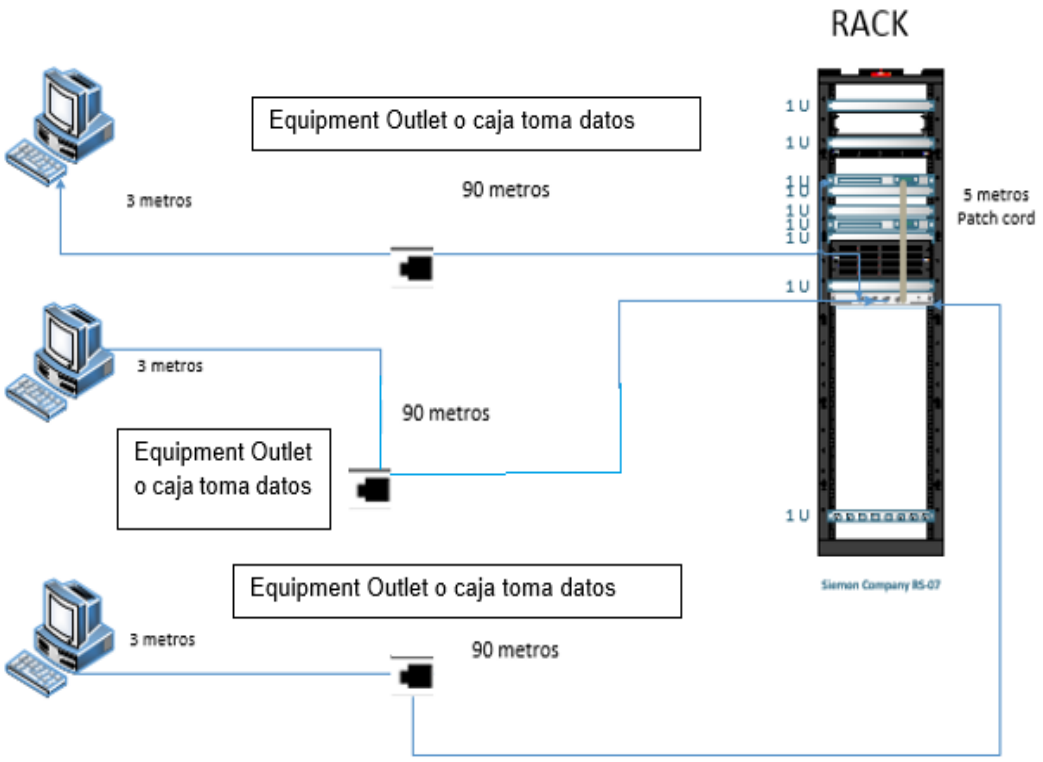


Figura 3.2: Diagrama de cableado horizontal.

3.1.4. Cálculo estimado de la cantidad de cable UTP CAT 6A.

Para conocer la cantidad de cable aproximada que se necesita para la red se reúne la siguiente información:

- Conocer la ubicación de los puntos de datos.
- Utilizar el plano para conocer la distancia máxima y mínima donde estarán los puntos de datos y la altura del edificio.
- Considerar la holgura promedio que debe tener.

Una vez que se conoce estos datos, se utiliza la siguiente formula que ayuda a obtener un cálculo estimado del cable que usaremos en el proyecto:

$$C = (Dmc + dml + 2 (altura) * NumE) \qquad (3.2)$$

C = (3m + 90m +2(7m)) * 120

C = 11160 metros (Para toda la red aproximadamente)

Donde:
C= Cantidad de cableado aproximado
Dmc=Distancia más cercana
dml= Distancia más lejana
NumE= Número de estaciones
Altura= Es la que se da desde el piso hasta el techo.

3.1.5. Rutas y espacios para transportar el cableado.

Al existir cielo raso se utilizará canaletas metálicas por donde se va a transportar todo el cableado horizontal y contra la losa de hormigón se deberá colocar las canaletas a 30 cm. Se utilizará una tubería de ¾ pulgadas especial para cables de datos como se ve en la Figura 3.3, por esta tubería pasaran 2 cables UTP en cada una. Habrá curvaturas mínimas en ciertos sectores.

Figura 3.3: Conduit metálico - Tuberías para cables.

A continuación, en las siguientes figuras se muestra la distribución de las canaletas por todo el edificio del hospital tanto para la planta baja que se muestra en la figura 3.4 como la planta alta que se muestra en la figura 3.5.

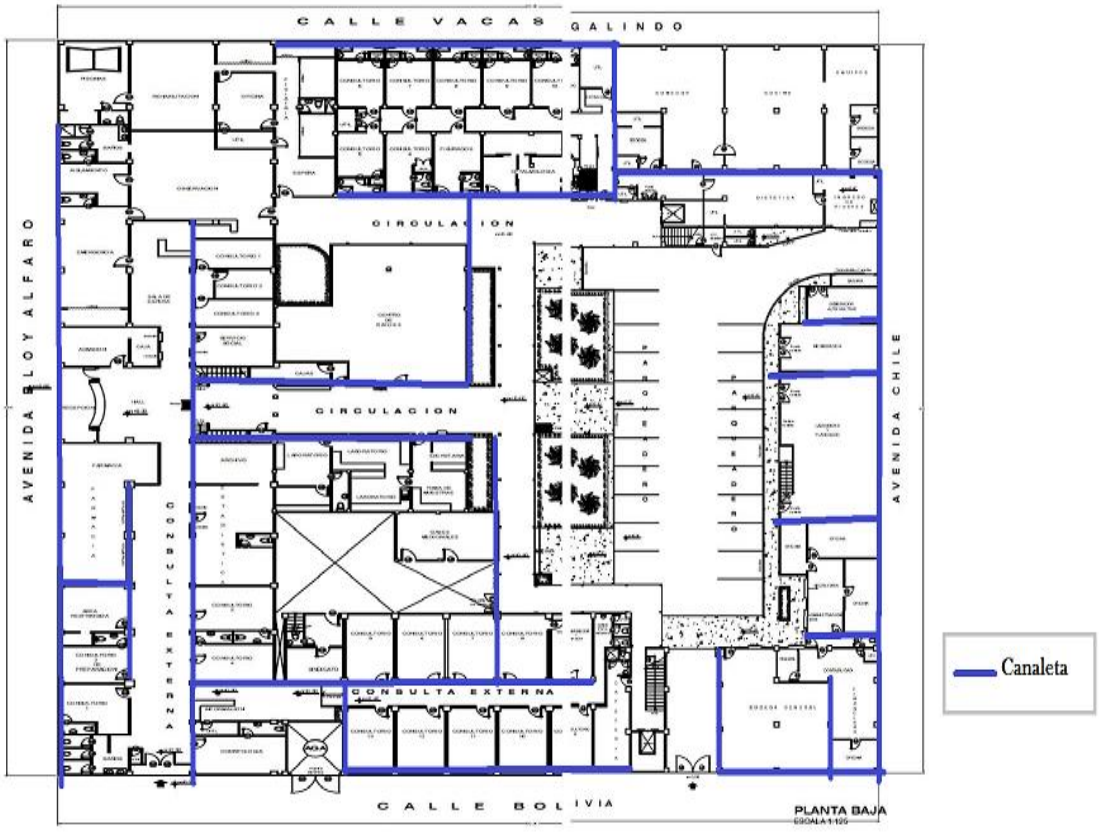


Figura 3.4: Distribución de canaletas Planta Baja.

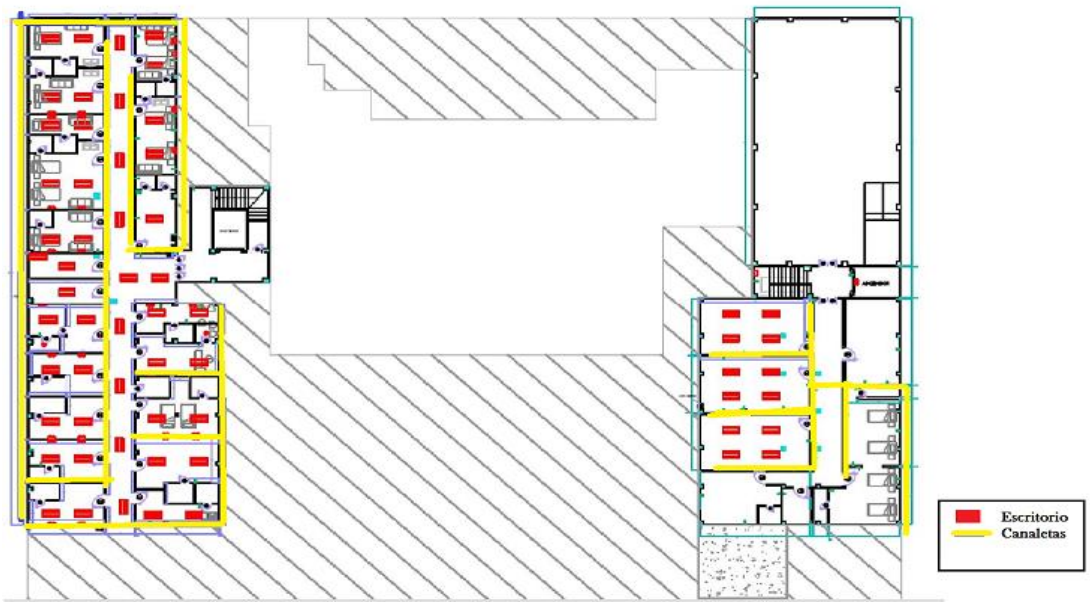


Figura 3.5: Distribución de canaletas Planta Alta.

3.1.6. El cuarto de telecomunicaciones.

En el cuarto de telecomunicaciones se encuentran los equipos principales o centrales de la red de datos, en el operaran los servidores, equipos de internet, equipos núcleo y distribución. Además, se encuentra el rack principal, este se encontrará ubicado cerca al departamento de sistema, al cual llegan los cables desde los equipos de acceso. En este lugar está la conexión de equipos mediante cableado vertical y la llegada de cableado horizontal. Se recomienda que en cada piso deba existir un cuarto de telecomunicaciones en el hospital.

Este cuarto tiene 6 metros. Este cuarto contará con un sistema de acondicionamiento de aire que tiene que ajustarse a una temperatura de 18 a 24 grados centígrados y de humedad de 30 - 55 por ciento. Contar con sistema de aire acondicionado para lograr que los equipos conserven una temperatura óptima. Colocar temperatura entre 18 a 24 grados centígrados y mantener una humedad entre 30 y 55 porciento.

La iluminación de este cuarto tendrá 500 Lux y deberá estar el foco a 1 metro del piso. Es recomendable usar luces de emergencia. Para la alimentación eléctrica de los equipos se contará con un sistema de energía eléctrica con 2 tomas de corriente AC como mínimo con circuitos separados o independientes de 110V y Un amperaje de 15A.

En caso de emergencia como un posible incendio, el cuarto de equipos contará con extintores de incendio.

3.1.7. Puertas del cuarto de telecomunicaciones.

Para los cuartos de telecomunicaciones se tomaron en cuenta las siguientes recomendaciones:

- Las puertas tendrán un tamaño mínimo de 0.86 x 1.9 m abriéndola hacia fuera
- Las puertas pueden ser de dos formas las que abren solo hacia afuera o puertas que abran 180 grados.
- El tamaño de las puertas debe ser de 0.91m de ancho por 1.9m de alto.
- Para mejorar la seguridad deben colocarse dispositivos encargados de controlar el acceso a los cuartos.

3.1.8. Cuarto de telecomunicaciones protegido del fuego.

La protección del cuarto debe tener materiales retardantes de fuego.

Es importante no almacenar en este cuarto materiales, líquidos, objetos inflamables.

3.1.9. Aterrizaje de equipos de Telecomunicaciones.

El aterrizaje de equipos de telecomunicaciones es un proyecto que el hospital ya ha implementado cumpliendo con la norma EIA/TIA 607. Lo que si consideramos en nuestra propuesta de proyecto es aumentar la

cantidad de UPS, tendrá 2 UPS por rack ya que solo existía un solo UPS para un rack.

3.1.10. Distribución de equipos en los Racks.

Para la distribución de los equipos en los racks se tomaron en cuenta las siguientes consideraciones:

- En el diseño de la red, se utilizarán racks tanto de piso como de pared el cual permitirá alojar los equipos de telecomunicaciones.
- Debido al tamaño del hospital, se colocará los racks en puntos estratégicos de los bloques del edificio. Como se ve en la figura 3.6, en el piso 1 estarán 2 TR (Cuarto de telecomunicaciones) y en la parte superior o piso 2 se encontrarán 1 TR y un ER (Cuarto de equipos)

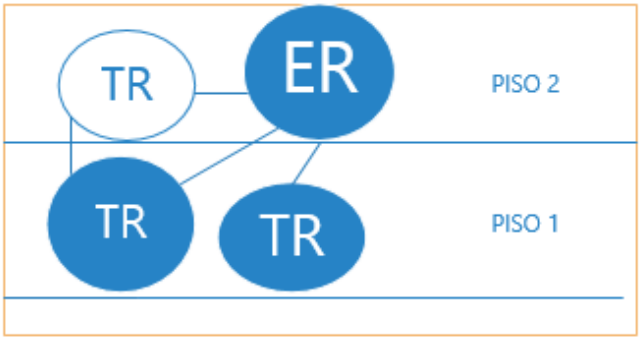


Figura 3.6: Distribución de cuartos donde irán los racks.

- Cuando se habla de los racks a usar existen dos tipos: de piso y de pared.
- Se utilizará 1 rack de piso principal y 3 racks de piso que serán los secundarios [14], con los respectivos organizadores verticales y horizontales.

3.1.11. Ubicación de los racks.

El primer rack secundario de piso se lo encontrará en la planta baja en el bloque C definidos en la figura 1.1 del Capítulo 1. En el área de secretaria se ubicará un rack en donde estarán los switch's que permiten conectar a los nodos de este sector. En la figura 3.7 se muestra detalladamente.

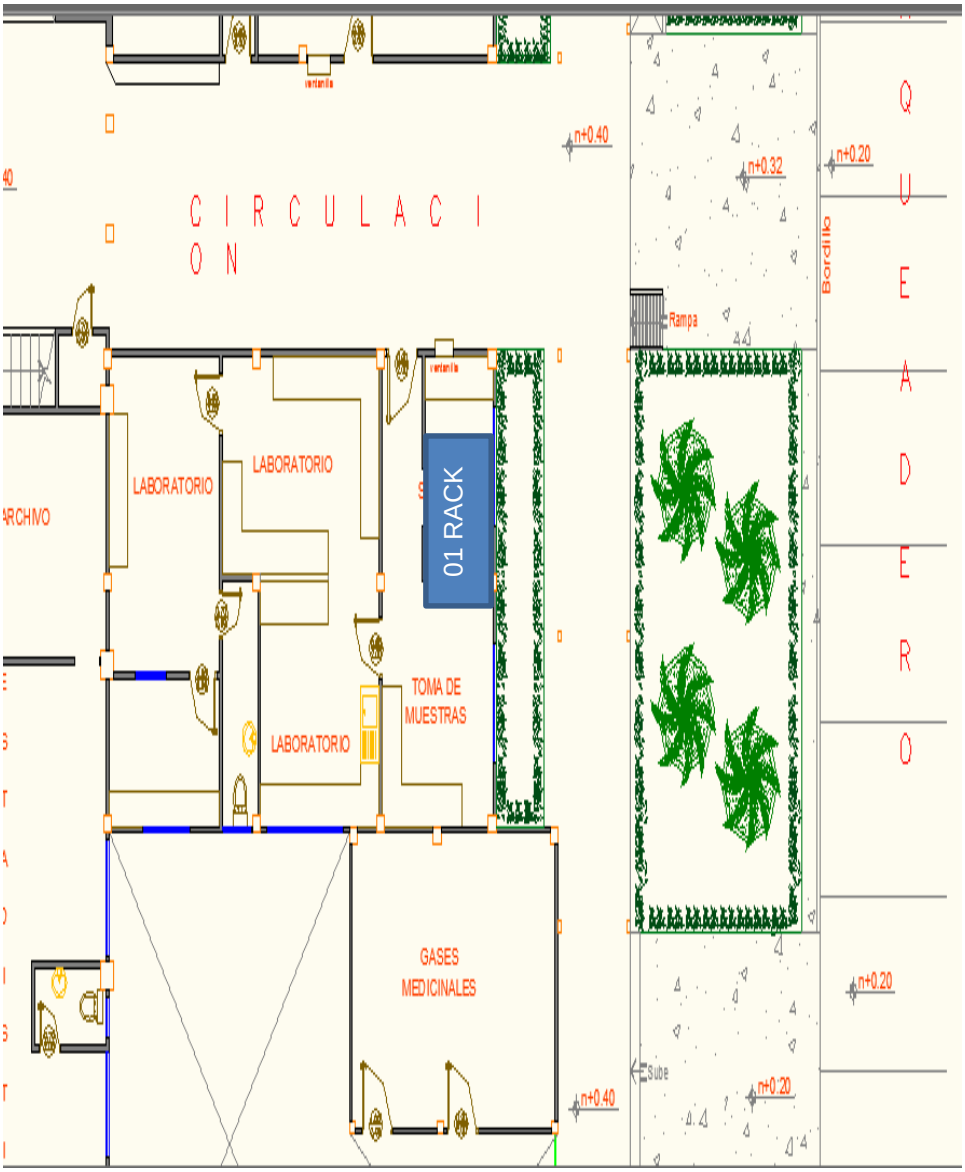


Figura 3.7: Ubicación de Rack en el bloque C planta baja.

El segundo rack secundario de piso se lo encontrará en la planta baja en el bloque F definido en la figura 1.1 del Capítulo 1. Cerca de una oficina es donde se ubicará un rack secundario en donde estarán los switch's que me permiten conectar a los nodos de este sector como se ve en la figura 3.8.

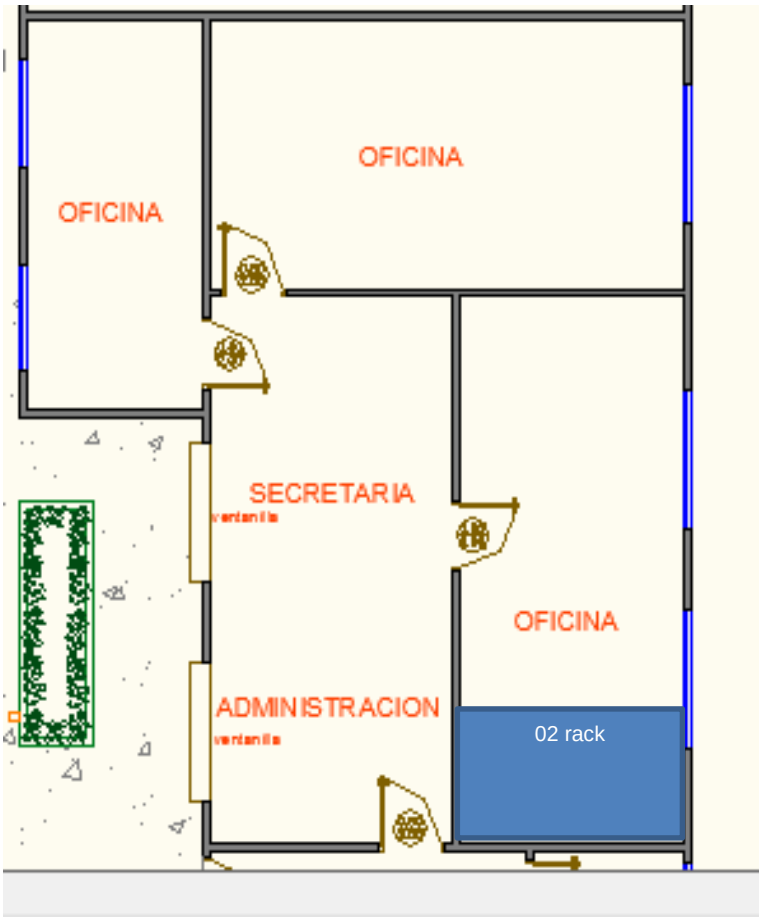


Figura 3.8: Ubicación de Rack en el bloque F planta baja.

El tercer rack secundario de piso se encontrará en la planta alta en el bloque A y el rack principal de piso se encontrará en el bloque F definido en la figura 1.1 del Capítulo 1. En el bloque F se encuentra el departamento de sistemas en donde estará el área del cuarto de telecomunicaciones principal ahí se ubicará el router, los servidores, el

switch principal y de ahí saldrán las conexiones hacia los demás departamentos como se lo puede apreciar en la figura 3.9.

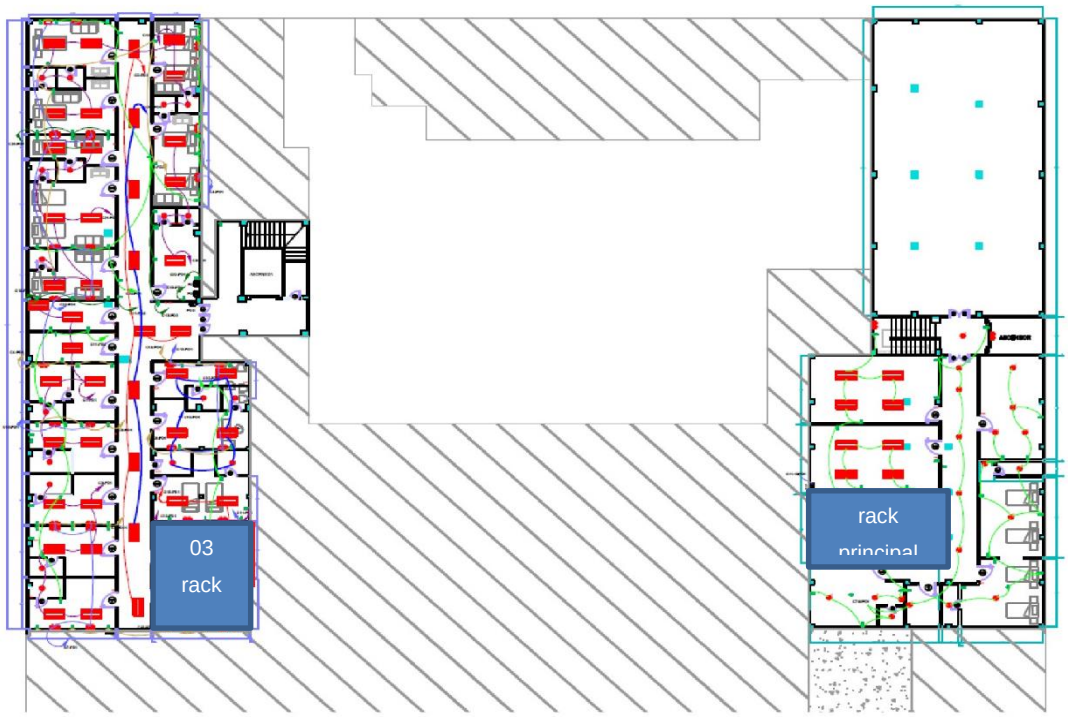


Figura 3.9: Ubicación de Rack en el bloque F planta baja.

3.1.12. Especificaciones del cuarto de equipos.

El cuarto de equipos está ubicado en el bloque F en el departamento de sistemas, el cual tiene una altura de 3 metros y un área de 12 m^2. Este cuarto contará con un sistema de acondicionamiento de aire que tiene que ajustarse a una temperatura de 18 a 27 grados centígrados y de humedad de 30 - 55 por ciento.

Para la alimentación eléctrica de los equipos se contará con un sistema de energía eléctrica, adicional los equipos deben usar un UPS para evitar problemas eléctricos.

En caso de emergencia como un posible incendio, el cuarto de equipos contará con extintores de incendio.

3.1.13. Especificaciones para las áreas de trabajo.

El área de trabajo lo conforman: equipos o dispositivos de los doctores, personal administrativo, personal de soporte técnico que le permitirán realizar la conexión con los diferentes servicios que provee el hospital.

El cable que va desde el equipment outlet o caja de toma de datos hasta el dispositivo del usuario tendrá una longitud de 3 metros.

3.1.14. Especificaciones del cuarto de entrada de servicios.

Dentro del cuarto de equipos ubicado en el bloque F en el departamento de sistemas, como lo muestra la figura 3.9 hay un pequeño espacio al que le llamaremos el cuarto de entrada de servicios el cual servirá para conectar el hospital a los servicios del proveedor de internet u otros servicios externos necesarios. Este cuarto separara los equipos que puede manejar o administrar el hospital y lo que pertenece a proveedores externos.

3.1.15. Cálculo y propuesta de los nuevos puntos de datos.

El edificio de dos pisos cuenta con las siguientes necesidades de punto de red:

En el piso 1 (planta baja), existirán 70 puestos de trabajo, 8 cámaras de video IP y 1 punto de acceso

En el piso 2, existirán 50 puestos de trabajo, 8 cámaras de video IP y 2 puntos de acceso.

En cada puesto de trabajo se habrá una toma doble de puntos de datos.

Los equipos principales estarán en el departamento de sistemas, entre estos equipos encontraremos los servidores.

Se ha solicitado cuartos para cada piso, lo cual depende también del apoyo del propietario del hospital.

En la tabla 5 se observa la cantidad de puntos de red necesarios para el funcionamiento de los distintos servicios y los puntos de red.

EDIFICIO	PUESTO DE TRABAJO	CAMARAS VIDEO IP	PUNTOS DE RED	TOTALES POR PISO
Piso 2	50	8	2	60
Piso 1	70	8	2	79
Totales	***120***	***16***	***4***	**140**

Tabla 5: Cálculo de puntos de datos.

3.1.16. Diseño del cuarto de telecomunicaciones-TR del piso 1 (planta baja) bloque C.

Necesidades:

- 39 puntos de red cable de cobre categoría 6A.
- Organizadores horizontales.
- Ventilación para el rack.
- 1 rack de pared.
- 2 switch de 24 puertos cada uno, Cisco Catalyst 3850.
- 1 patch panel de 48 puertos.

Para determinar el espacio de ampliación se ha seguido la técnica de que lo ocupado es el 60% y el 40%. Si se colocan todos los equipos organizados se necesitaría 9 RU en donde el espacio de ampliación en un futuro será de 6 RU = 40%, el gabinete debe ser de 15 RU como se lo ve en la figura 3.10. Se usarán switch POE, la anchura del gabinete será de 90cm frontal y la longitud lateral será de 1 metro. La ubicación del bloque C se muestra en la figura 1.1 del Capítulo 1.

Ecuación aplicada para el cálculo de espacio y tamaño de rack:

$$ED = \frac{UO*40\%}{60\%} \qquad (3.1)$$

R = UO + ED

ED = Espacio disponible

UO= Unidades ocupadas

R= Unidades de Rack necesarias en total

40% = Espacio de ampliación en unidades de rack para un futuro.

60%= Espacio de Unidades de Rack ocupadas.

Calculo:

$$ED = \frac{9 * 40\%}{60\%}$$

R = 9 + 6

R = 15 Unidades de Rack

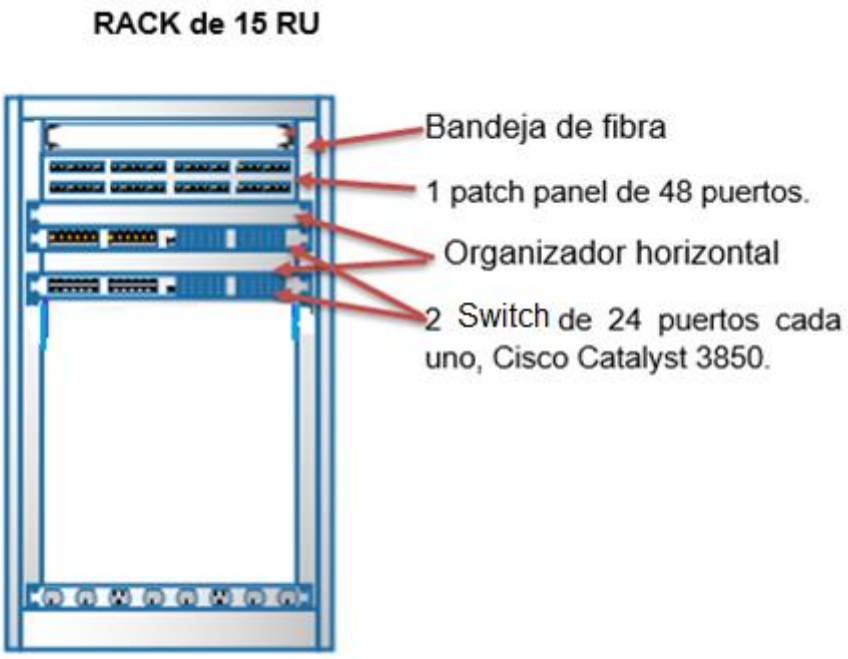


Figura 3.10: Rack para el Bloque C.

3.1.17. Diseño del cuarto de telecomunicaciones-TR del piso 1 (planta baja) bloque F.

Necesidades:

- 40 puntos de red cable categoría 6A.
- Organizadores horizontales.

- Ventilación para el rack.
- 1 rack de pared.
- 2 switch de 24 puertos cada uno, Cisco Catalyst 3850
- 1 patch panel de 48 puertos.

Para colocar todos los equipos organizados se necesita 9 RU, en donde el espacio de ampliación en un futuro será de 6 RU = 40%, el gabinete deber ser de 15 RU como se lo ve en la figura 3.11, se usarán switch POE, la anchura del gabinete será de 90cm frontal y la longitud lateral será de 1 metro. La ubicación del bloque F se muestra en la figura 1.1 del Capítulo 1.

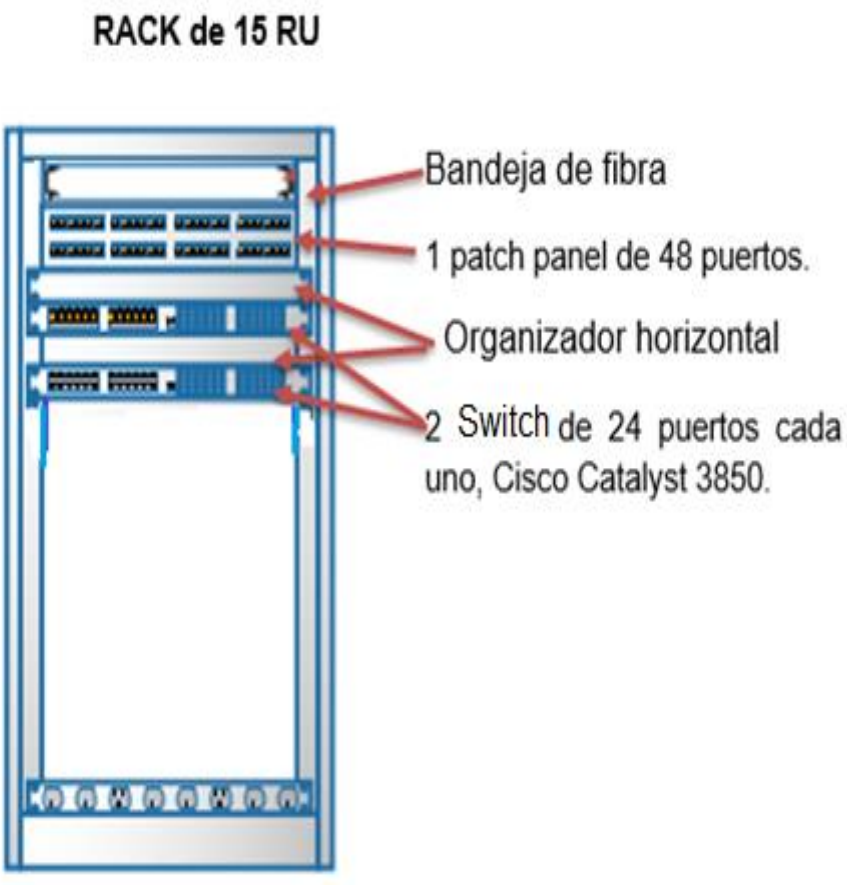


Figura 3.11: Rack para el Bloque F.

3.1.18. Diseño del cuarto de telecomunicaciones-TR del piso 2 (planta alta) bloque A.

Necesidades:

- 60 puntos de red cable categoría 6A.
- Organizadores horizontales.
- Ventilación para el rack.
- 1 rack de pared.
- 2 switch de 24 puertos cada uno, Cisco Catalyst 3850
- 1 switch de 16 puertos (switch disponible en el hospital).
- 1 patch panel de 48 puertos.

Para colocar todos los equipos organizados se necesita 11 RU en donde el espacio de ampliación en un futuro será de 8 RU, el gabinete deber ser de 19 RU como se lo ve en la figura 3.12. La anchura del gabinete será de 90cm frontal y la longitud lateral será de 1 metro. La ubicación del bloque A se muestra en la figura 1.1 del Capítulo 1.

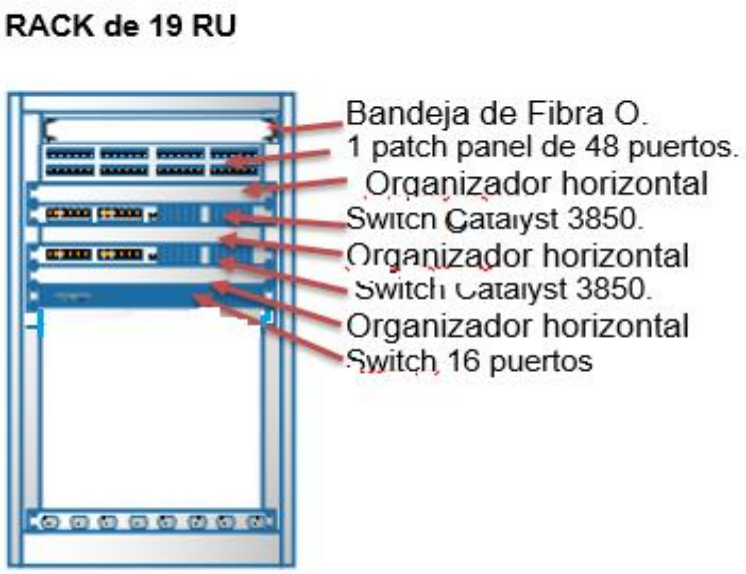


Figura 3.12: Rack para el Bloque A.

3.1.19. Diseño del cuarto de equipos-ER del piso 2 (plata alta) bloque F.

Necesitan:

- Organizadores horizontales.
- Ventilación para el rack.
- 1 rack de piso.
- Patch panel de 24 puertos.
- Puntos de red para conectar servidores.
- 1 router Cisco 1900.
- 1 switch de capa 3 Cisco Catalyst 6513-E
- 2 switch de capa 2 Cisco Catalyst 3850
- Bandeja de fibra óptica, hilos de cable F.O.

Para colocar todos los equipos/servidores organizados se necesita 19 RU en donde el espacio de ampliación en un futuro será de 13 RU, el gabinete deber ser de 32 RU como se lo ve en la figura 3.13. La anchura del gabinete será de 90cm frontal y la longitud lateral será de 1 metro. La ubicación del bloque F se muestra en la figura 1.1 del Capítulo 1.

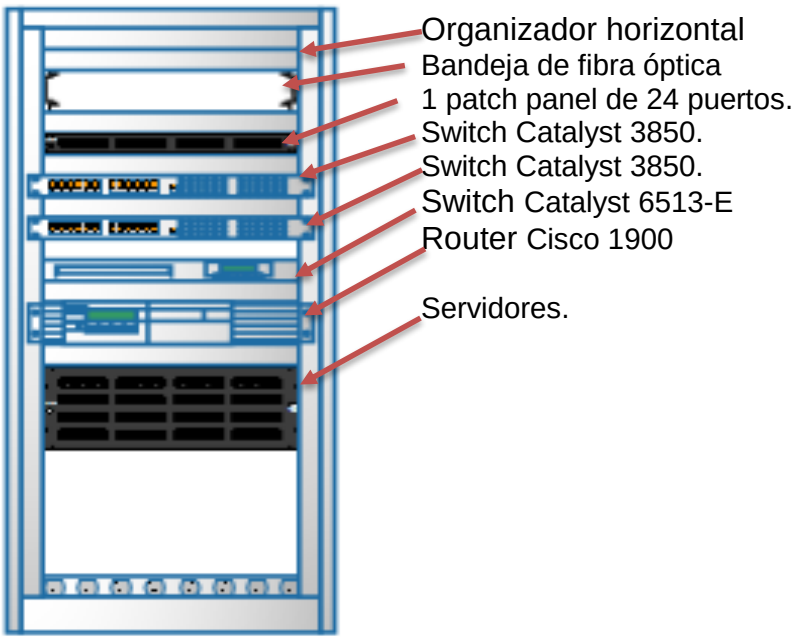


Figura 3.13: Rack para el Bloque F.

3.1.20. Plan de Administración e identificación de elementos parte activa y pasiva de la red.

El siguiente plan de administración permitirá realizar un mejor mantenimiento, control de la red y solucionar problemas de manera eficiente y rápida.

Se utilizará nomenclaturas que permitirán identificar a los equipos en nuestra red, como se lo ve en la Tabla 6, con respecto a los departamentos tendrán las siguientes nomenclaturas:

DEPARTAMENTOS/ÁREA	ABREVIATURA
Sistemas	SIS
Gestión Ambiental y Procesos	GAP
Contabilidad Financiera	CTF

Pagaduría	PGD
Auditoria Medica	ADM
Laboratorio	LAB
Servidores	SRV
Biometría	BMT
Proveeduría	PRV

Tabla 6: Identificación de los equipos de acuerdo al departamento.

A los switch principales de la red se les dará una nomenclatura que indique el número del equipo y el nombre de la institución como se lo puede ver en la Tabla 7.

SWITCH	ABREVIATURA
Switch 1	S1HLB
Switch 2	S2HLB
Switch 3	S3HLB

Tabla 7: Identificación de equipos switch's.

Se pueden tomar estos ejemplos para nombrar futuros equipos similares.

Así mismo, se procederá a etiquetar el cableado y sus elementos para lo cual se consideran los siguientes puntos:

- Es necesario que los elementos del cableado estén numerados correctamente por lo cual se propone la siguiente solución de identificación de componentes:
- Las salidas de datos serán identificadas con la letra D.
- Cada bloque del edificio deberá ser identificado por ejemplo BAxx-nn. Donde las xx representara los pisos y las "nn" indicaran el número de regleta o panel.

- Para los patch panels se les dará la identificación siguiente Dx-nn-mm, en donde la xx es la identificación del piso, las nn el número de patch-panel y las mm el puerto utilizado.

3.2. Plan de distribución lógico.

3.2.1. Diagrama lógico de la red de datos.

De acuerdo con los análisis realizados se desea conseguir un correcto rediseño de la red, de manera lógica el grafico se lo ve en la Figura 3.14 y la simbología del gráfico en la Figura 3.15.

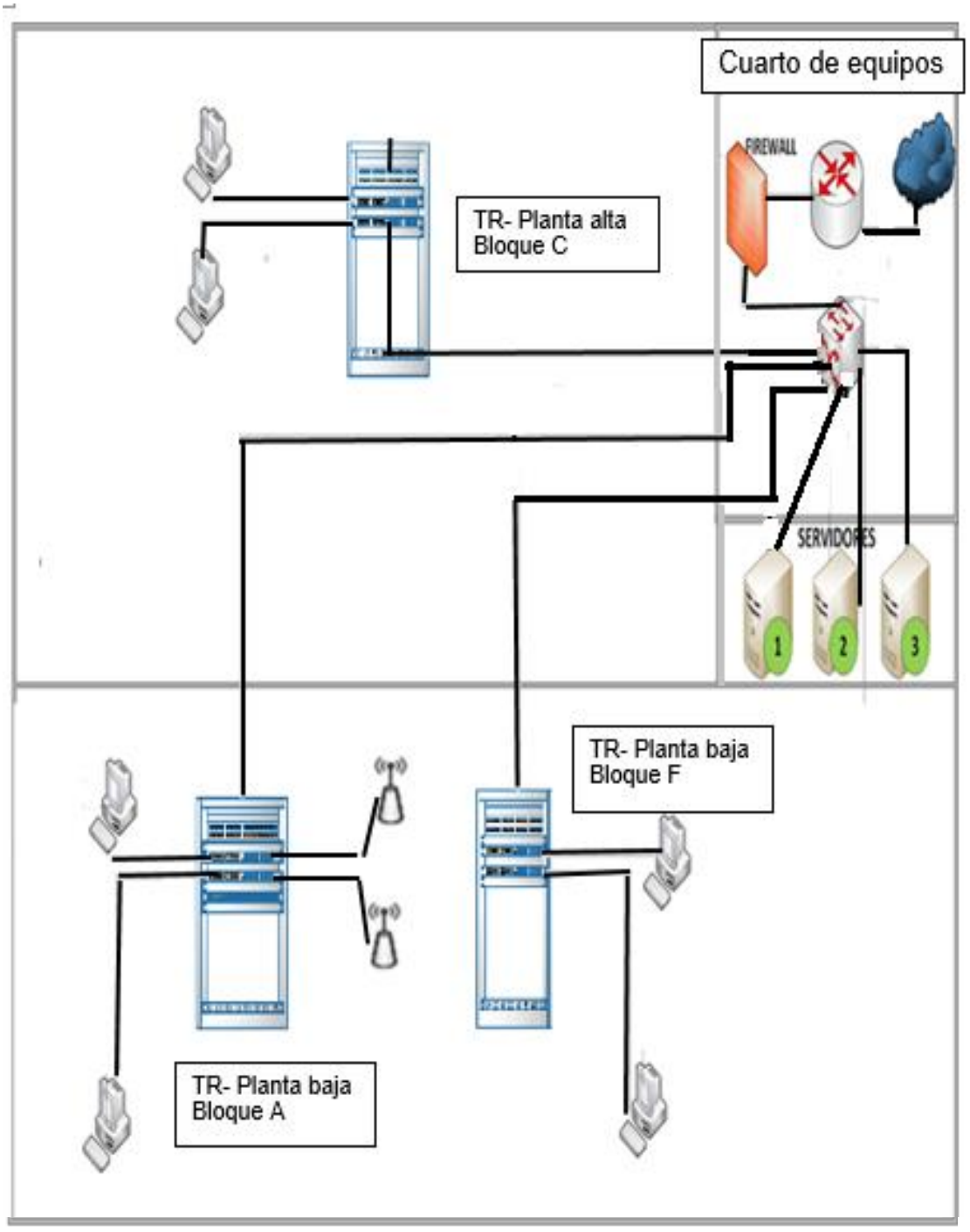


Figura 3.14: Diseño de la red LAN.

Figura 3.15: Simbologías del diseño de la red LAN.

Como se aprecia en la figura 3.14, se plantea rediseñar la red aplicando el modelo Jerárquico que nos brinda entro otros beneficios tener el tráfico de la red de una manera más organizada donde se pueda en caso de fallo conocer con más exactitud cuáles son los posibles errores, donde cada dispositivo cumple un rol importante y es posible un crecimiento de la red puesto que es una red escalable. No se reutilizarán los equipos que existen actualmente en la red de datos del hospital. En la figura 3.15 están los equipos que se utilizarán en la nueva red. A continuación, se describe la función que realiza cada capa del modelo propuesto:

- Núcleo: donde el switch conectado directamente al router será el encargado tanto de la comunicación inter-vlan como del acceso hacia los servidores del hospital por parte de los trabajadores.

- Distribución: se encarga de la comunicación entre la capa de núcleo y la capa de acceso y también entre switch de esta misma capa para brindar mayor cobertura del manejo de vlan que se explica detalladamente más adelante.
- Acceso: los switch que se implementan en esta capa son administrables, dando como ventaja el poder trabajar con Vlans. Lo que se plantea es que en la capa de distribución se asigne una Vlan al puerto que está conectado con los Switch de Acceso y así poder asignar una Vlan a ese segmento de red.

El Router será el encargado exclusivamente de enrutar los paquetes a la mayor velocidad, pero solo para los usuarios que tengan permiso de acceder hacia internet.

3.2.2. Plan de direccionamiento IP propuesto.

Para el direccionamiento IP debemos considerar que se puede trabajar tanto con IPv4 como con IPv6. Al utilizar IPv6 se tienen muchas ventajas sobre IPv4 sin embargo hay que considerar varios puntos como, si el ISP (Proveedor de Servicios) admite IPv6, si los equipos que se reutilizarán soportan IPv6, si el desempeño de la red disminuirá al manejar paquetes de IPv6. Al analizar estos puntos se decide mantener el direccionamiento con IPv4.

Se ha diseñado una segmentación de direcciones por servicios, para así tener una administración de direcciones de acuerdo con los servicios que se está ofreciendo en la red.

Se propuso a cada servicio asignar una cantidad de 20 direcciones IP adicional como método preventivo ante posible crecimiento y así no perder el orden de direcciones lo cual podría generar una confusión en el manejo de direcciones y dificultaría la corrección de errores.

Para el diseño de esta red se usó una subred con las características mencionadas en la Tabla 8.

Red	192.168.1.0
Clase	C
Mascara de Subred	255.255.255.0
Gateway	Definido por el ISP
Numero de direcciones validas	253
Dirección de Broadcast	192.168.1.255

Tabla 8: Características de la dirección de red a usarse.

Las IP serán asignadas de manera dinámicas por el servidor DHCP que será el encargado de entregar una a una las direcciones a los equipos finales, los pools de direcciones se muestran más adelante.

3.2.3. Plan de Distribución de la VLAN.

La creación de VLANs en la red, nos permitirá segmentar la red de manera lógica y cada segmento de red será por servicio, el segmento por servicio se detalla más adelante.

Después de haber realizado la implementación física de los equipos en cada uno de los lugares propuestos, se realizará la configuración de las vlan's para así segmentar el tráfico, se usará un esquema de vlan´s dinámicas donde el switch de núcleo será el que sirva a su vez de base de datos donde se almacena el registro de todos los dispositivos válidos para la red, su vlan correspondiente y asignar IP a los dispositivos que se encuentren conectados a la red. Cabe mencionar que si al conectar un dispositivo y su dirección MAC no se encuentra en la base de datos no se le asignara IP, este esquema nos brinda entre otras cosas: administración, reducir la carga de paquetes, manejar el ancho de banda y aumentar la seguridad lógica.

Los equipos activos que se utilizaran para la implementación de VLAN's soportan protocolos como IEEE 802.1Q, STP (Spanning Tree Protocol), VTP (Vlan Trunking Protocol).

A continuación, en la Tabla 9, se detalla la segmentación de la red por VLAN´S para así segmentar los servicios y trabajar de una forma más

apropiada y a su vez en caso de fallo o inestabilidad en la red poderlos corregir de una manera más eficiente y rápida.

Se han distribuido las VLANs de la siguiente forma:

VLAN	ID	SERVICIOS PERMITIDOS
Impresión	16	Vlan destinada para impresoras que proveen servicio en el hospital
Voz	42	Vlan destinada para el servicio de voz sobre IP (Se la dejara configurada, aunque en la implementación no se maneje VOIP)
Video	13	Vlan destinada para el sistema de video vigilancia mediante cámaras IP.
Datos 1	10	Acceso únicamente a la información alojada a los servidores. Pueden realizar consultas a las bases de daos, pagina web localmente.
Datos 2	11	Se permitirá el acceso a los servidores locales, bases de datos, navegación web y compartición de archivos.
Guest	14	Acceso único a navegación web temporalmente
Inalámbrica	12	Vlan para los equipos y dispositivos que necesiten el servicio de red inalámbrica.
Administración	15	Vlan para la administración de todos los dispositivos de red. Acceso a todo sin restricciones

Tabla 9: VLANs y su función.

Una vez que se han creado las VLANs por servicios, se elaboró el direccionamiento IP. A continuación, se muestra el plan de direccionamiento en la Tabla 10:

VLAN	ID	Tamaño de direcciones disponibles para las VLAN	Rango de direcciones IP y Mascara de subred
Datos 1	10	50+20 (adicionales)	192.168.1.1 - 192.168.1.126/25
Datos 2	11	63	192.168.1.129 -192.168.1.254/25
Inalámbrica	12	60	192.168.2.1 - 192.168.2.62/26
Video	13	16	192.168.2.65 - 192.168.2.94/27
Guest	14	10	192.168.2.97 - 192.168.2.110/28
Administración	15	7	192.168.2.113 -192.168.2.126/28
Impresión	16	5	192.168.2.129 -192.168.2.134/29
Voz	42	5	192.168.2.137 -192.168.2.142/29

Tabla 10: Rangos de direcciones IP por servicios.

Como se aprecia en la Tabla 10 se propone crear una Vlan de Voz, pese a que la red del Hospital no cuenta con este sistema, se espera que en un futuro se lo pueda implementar.

3.3. Diseño de la red inalámbrica.

3.3.1. Criterios del diseño de la red inalámbrica.

Al momento de implementar la red inalámbrica en el Hospital León Becerra debemos considerar los siguientes factores:

- Número de usuarios.
- Frecuencia de operaciones,
- Cobertura de los dispositivos inalámbricos.
- Identificador y seguridad de la red.

3.3.2. Cobertura de los dispositivos inalámbricos.

Actualmente, existe una red inalámbrica en una parte del sector del hospital específicamente en el área de sistemas; se desea que esta

red funcione en otros dos sectores para así proveer mayor conectividad a sus trabajadores. Los sectores en que se desea que exista conectividad mediante red inalámbrica es en el área de los consultorios de la planta baja se muestra en la Figura 3.16. Esta red solo será utilizada por los doctores y auxiliares médicos pertenecientes a cada consultorio médico.

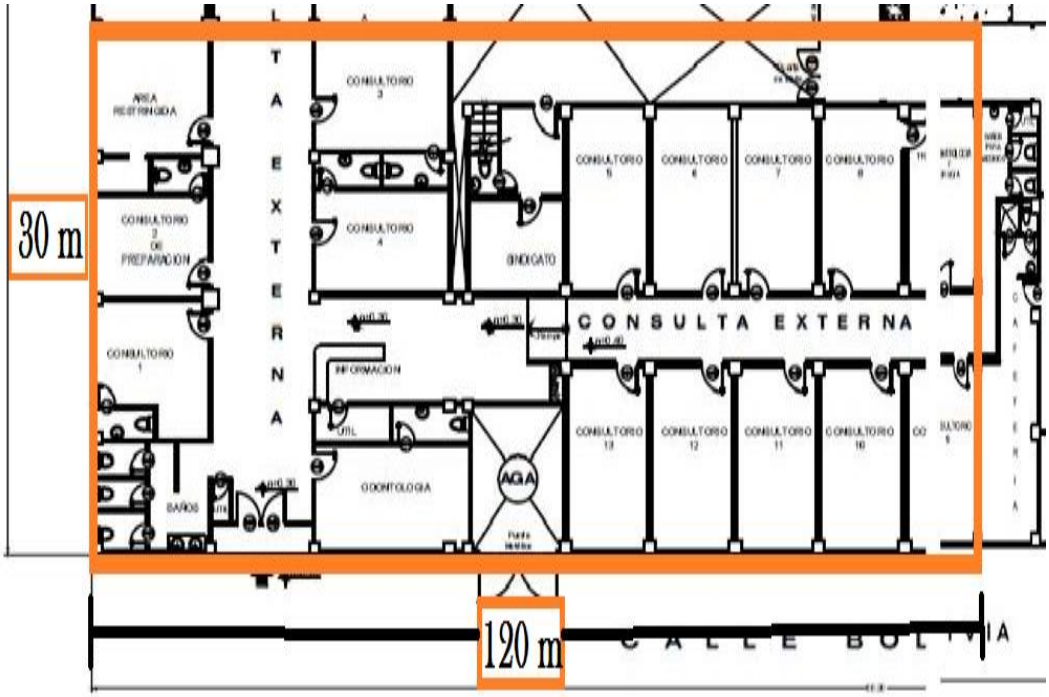


Figura 3.16: Zona donde se implementará la red inalámbrica.

Aproximadamente existen 20 personas entre doctores y auxiliares medico en toda esta zona trabajando, sin embargo, cada uno de ellos posee dos o tres dispositivo móvil por lo cual tendremos un aproximado de 60 usuarios en total, se desea que a futuro esta red crezca por lo cual se piensa que por lo menos el 30 % de las personas tendrá otro dispositivo inalámbrico aumentando así de 85 a 90 la cantidad de usuarios de la red.

En el diseño de red se utilizará 2 equipos inalámbricos Cisco Aironet Serie 700W para dar cobertura a toda la zona de consultorios, a pesar

de que un solo equipo puede manejar más de 100 direcciones MAC, el proveedor recomienda no asociar tantos equipos ya que los Access Point funcionan como concentradores inalámbricos y el desempeño o el uso de la red por parte de cada usuario hará que se disminuya el rendimiento del equipo. Por esta razón se usarán 2 equipos para cubrir esta zona.

La tecnología 802.11n que utilizan los equipos propuestos permite cubrir una zona de hasta 70 m como máximo a la redonda. La zona que deseamos cubrir tiene las medidas de 30 m por 120 m como se muestra en la Figura 3.17. Con base en el tamaño de la zona de consultorios se elaboró la siguiente propuesta de ubicación de cada AP.

Este diseño propone que el usuario pueda moverse por toda la zona de consultorios sin perder conexión.

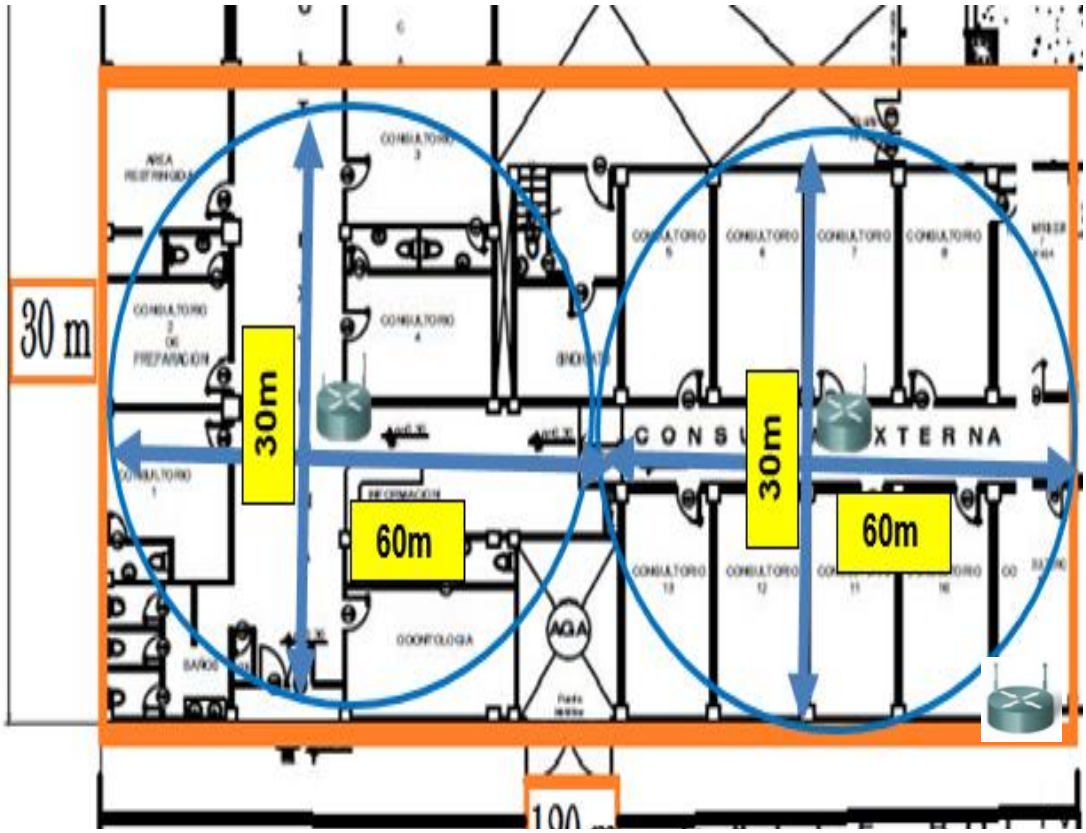


Figura 3.17: Ubicación de los AP en la zona de consultorios.

3.3.3. Frecuencia de Operación.

En el Hospital León Becerra se propone utilizar equipos que trabajen u operen con el estándar 802.11n [11], ya que este es compatible con dispositivos que trabajan con otros estándares como el 802.11 g y 802.11 b.

Se realiza la propuesta de utilizar el 802.11n con el objetivo de mejorar el rendimiento de la red inalámbrica a diferencia de otros estándares (802.11b y 802.11g) que ofrecen menor rendimiento. Existirá un incremento de 54Mbps a 600 Mbps en la velocidad de transmisión.

El estándar 802.11n agrega multiplicación MIMO (Múltiple Input Múltiple Output) que ayuda a que la señal no tenga una pérdida total en lugares como por ej. Dentro de los consultorios de los doctores que las paredes obstruyen el paso de la señal.

Las desventajas que se encuentran al utilizar este estándar es que está basada en lo siguiente:

- Incompatibilidad entre equipos. Hace un tiempo este estándar solo funcionaba cuando existían equipos de la misma marca sin embargo ya este problema se está solucionando.
- Para alcanzar una velocidad entre 150Mbps o 300Mbps se necesita una señal mayor que la que se puede usar con estándares como 802.1b y g.

3.3.4. Identificación de la red inalámbrica.

Los usuarios podrán identificar la red inalámbrica del hospital mediante el SSID (Services Set Identifier) LEON BECERRA y se podrán conectar utilizando su respectivo usuario y contraseña asignada por el departamento de sistemas.

3.3.5. Seguridad para la red inalámbrica.

En el diseño planteado de red inalámbrica se toma muy en cuenta el tema de la seguridad ya que las redes inalámbricas son más susceptibles a que un intruso realice un ataque.

En esta solución se propone utilizar WPA2 [12], la cual es una versión mejorada de WPA, permite tener mayor seguridad en los Access Point a diferencia de otros como WEP. WPA2 es un método de seguridad con un algoritmo de seguridad más seguro contra intrusos.

En cuanto a la seguridad, se implementará una política de seguridad para la contraseña donde tendrá un mínimo de 8 dígitos y máximo 16 dígitos, también deberán usar letras, números y caracteres especiales.

3.4. Administración y seguridad de la red de datos.

3.4.1. Administración de la red usando Windows Server 2012 R2

Para la administración de la red se usará Windows Server 2012 R2. Las herramientas que posee ayudaran a dar una correcta administración de la red además de seguridad para trabajar de una manera confiable con los datos que se manejan tanto internos como externos**.**

Mediante el uso de una infraestructura como Active Directory que brinda muchas herramientas para administrar la seguridad de la información que es lo más importante para la organización, administrar los recursos de la red y asignar permisos específicos tanto a usuarios como a departamentos de lo que pueden o no hacer en los hosts asignados a continuación se menciona los servicios claves que implementaran con Active Directory y Windows Server 2012 R2:

- Asignar una cuenta de usuario a todos los trabajadores de la organización y que sea la única forma que puedan acceder a los recursos y servicios de la red.

- Implementación del protocolo AAA, que brinda Autenticación que permite validar si un usuario pertenece o no a la organización. Autorización dentro de la red que permisos tiene y Auditoria que nos ayuda en caso de alguna anormalidad conocer cuál es la causa del evento.
- Implementación de Firewall para así bloquear protocolos que no se utilizaran y prevenir ataques de seguridad.
- Implementación de Certificados Digitales para así asegurar integridad en los datos y saber que no ha sido modificado por alguien.
- Implementación de servidor DNS para la resolución de nombre tanto a nivel de la LAN como para la salida hacia internet.
- Implementación de servidor DHCP para asignar por departamento de una manera dinámica las direcciones IP.
- Implementación de servidor proxy para administrar a las páginas web que se deseen acceder y bloquear por departamentos el acceso a alguna página y que esté habilitada para otro departamento.
- Servicio de replicación entre estaciones de trabajo confiables es decir configurar cuales son las estaciones de trabajo confiables para que se puedan replicar la información.

3.4.2. Jerarquía de objetos.

Al implementar Active Directory podremos manejar de mejor forma los recursos de la red. Para una mejor administración hemos dividido en usuarios y equipos-computadores lo cual permite en el caso de usuarios manejar toda la información de un usuario como su nombre, grupo que pertenece, permisos y otros parámetros de manera ordenada y rápida. Así mismo, los objetos que corresponde a los equipos que pertenecen al dominio. En esta sección, la Figura 3.18 muestra cómo estará constituida nuestra infraestructura a nivel de dominio mediante un esquema de Jerarquía de Active Directory:

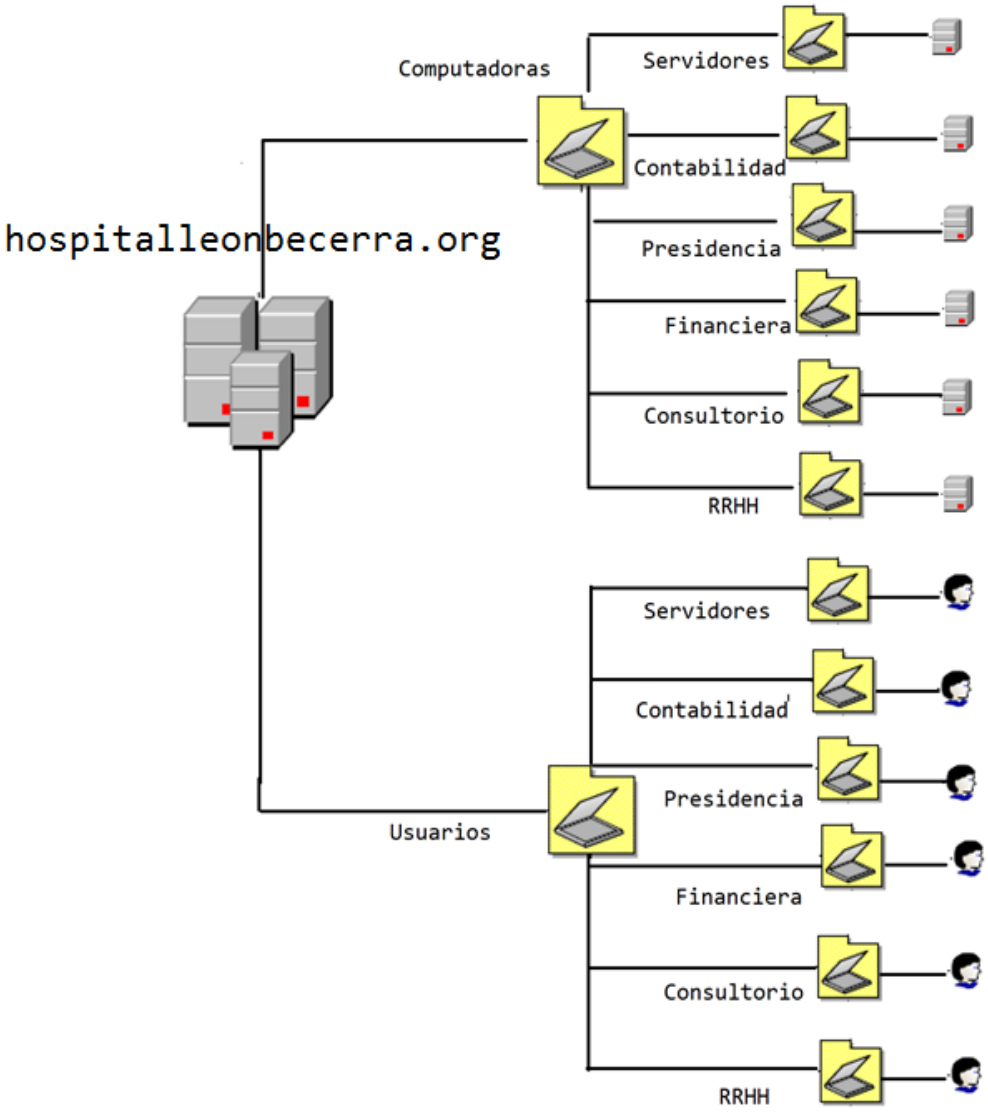


Figura 3.18: Esquema Jerárquico de Active Directory.

3.4.3. Sistema de Nombres de Dominio (Dns).

Esta implementación permitirá la resolución de nombres cuando un usuario quiera dirigirse a una página especifica se hará la traducción a la dirección IP original de la página web y así poder acceder con solo escribir el nombre del dominio de la web.

3.4.4. Utilización del protocolo AAA (Autenticación, Autorización y Auditoria).

Con la ayuda de este protocolo se brindará lo siguiente:

- Autenticación y solo accederá las personas que estén ingresas al dominio ósea solo personal del hospital
- Autorización las personas que se autentiquen tendrán acceso a los recursos que de acuerdo con los GPO tengan permiso de acceder.
- Auditoria en caso de existir algún inconveniente de seguridad se puede acceder a los logs para conocer en qué punto fue el inconveniente.

3.4.5. Políticas de seguridad.

Las políticas de seguridad son aplicadas para restringir los servicios o bloquear cualquier uso de la red por usuario o por computadora. Los usuarios y computadoras de un departamento serán agregados a un OU para poderlos agrupar por departamentos y así aplicar las políticas a nivel de departamentos debido que por lo general dentro de un departamento manejan las mismas políticas. Así se podrá asignar políticas de acuerdo a la jerarquía por cada departamento o de ser el caso a un usuario por ejemplo el administrador de la red tendría diferentes permisos que los demás de su departamento.

El personal de sistemas del hospital será el encargado de elaborar las políticas de seguridad de la empresa y también el encargado de configurar las GPO para ser asignadas a cada OU.

3.4.6. Servidor DHCP.

Se implementará un servidor DHCP el cual permitirá mejorar la asignación de direcciones IP, porque se podrá asignar direcciones IP de manera automática a los dispositivos finales. Para la asignación se tendrá el rango desde la 192.168.1.1 hasta la IP 192.168.1.254 y las

direcciones se repartirán mediante pools de direcciones, cada pool se asignará a un servicio y tendrá un rango de direcciones de acuerdo al servicio que se detalla en la tabla 11. Los rangos de direcciones se definen a continuación:

NECESIDAD	Pool de direcciones IP
DATOS 1	192.168.1.1 - 192.168.1.126/25
DATOS 2	192.168.1.129 -192.168.1.254/25
INALAMBRICA	192.168.2.1 - 192.168.2.62/26
VIDEO	192.168.2.65 - 192.168.2.94/27
GUEST	192.168.2.97 - 192.168.2.110/28
ADMINISTRACION	192.168.2.113 -192.168.2.126/28
IMPRESIÓN	192.168.2.129 -192.168.2.134/29
VOZ	192.168.2.137 -192.168.2.142/29

Tabla 11: Direcciones IP asignadas a las Vlan's por servicio.

3.4.7. Servidor Proxy.

El servidor proxy permite bloquear el acceso a páginas de las personas autorizadas a internet mediante el trabajo conjunto con las políticas del hospital; por lo tanto, el personal encargado de administrar la red serán los delegados de asignar los bloqueos de páginas.

3.4.8. Servidor Antivirus.

Se ha definido que para la red del Hospital se implemente un servidor antivirus que trabaje con Eset Internet Security su licenciamiento es por máquina y el costo por maquina es de $5. Al adquirir el licenciamiento de todas las computadoras que son en total 90 computadoras se instala el software de Eset Internet Security para la administración de las licencias y de actualizaciones, entre las ventajas de utilizar Eset Internet Security son:

- Antivirus y Antispyware
- Antiphishing
- Antispam

- Protección contra Botnets
- Sistema de Control Parental
- Sistema de Prevención de Intrusiones
- Protección para Banca y Pago en Línea
- Control de Webcam y Router

3.4.9. Propuesta de equipo Servidor.

En la figura 3.19 se observa el servidor Power Edge T430 que proponemos:

Figura 3.19: Servidor propuesto.

Para el correcto funcionamiento de los servicios es necesario un servidor que como mínimo cumpla con: 4GB DE RAM, 1 TB de disco duro y un procesador Intel Xeon E5-2600. Este servidor cumple con los requerimientos y la información completa de las características están la parte de anexos.

Este servidor será utilizado para implementar Active Directory mientras que los otros servicios se los migrará a 2 servidores HP ProLiant Easy Connect ML110 Managed Hybrid Server existentes en el Hospital León Becerra los cuales el personal IT del hospital será el encargado de realizar la migración.

3.4.10. Propuesta de Firewall HPE-5000-C VPN Firewall Appliance (JG650A).

Para brindar seguridad en la red, se implementará el firewall que filtrara los paquetes tanto los que entran a la red como los que salen de la misma tanto de internet como de las consultas que se harán a la base de datos del IESS, este además que este firewall cumplirá con las siguientes funciones:

- Filtrar los paquetes
- Implementación de ACL
- Habilitar o deshabilitar puertos.

En este caso estarán habilitados puertos como:

- SMTP
- HTTP
- HTTPS
- TELNET
- VPN
- FTP
- SSH
- POP3
- DNS

Características del Firewall

En la Tabla 12, se puede observar las características básicas de este equipo. El detalle completo de las características estará en la parte de anexos.

Accesorios incluidos	**1 HPE F5000-S/C VPN Firewall Modulo de Ventilación (JG878A)**
Puertos y ranuras de E/S	12 RJ-45 auto-negociación 10/100/1000 12 puertos fijos Gigabit Ethernet SFP **4 puertos SFP + 10GbE**

Memoria y procesador	16 GB DDR2 SDRAM, 256 MB de flash compacto
Firewall throughput	12 Gbps
VPN throughput	3 Gbps 3DES/AES
Número de VLAN	4000

Tabla 12: Características del Firewall.

CAPÍTULO 4

4. PRESUPUESTO DE PROYECTO Y DISEÑO DEL PLAN DE EJECUCIÓN.

4.1. Presupuesto.

Una vez hecho el inventario de los elementos que fueron estimados para la red del hospital León Becerra, se detalla el costo total por equipo y el costo total del proyecto, cabe mencionar que los costos se detallarán en la Tabla 13 y que el total es de $118044,00. Esta sería la inversión que tendrá el Hospital León Becerra.

Producto/Marca	Cantidad	Precio Unitario	Precio total
Red Cableada			
Cable UTP 6ª	400 Rollos Aprox de 50 m.	$ 25	$ 10.000
Conectores de red RJ45	300 aprox.	$9 (100)	$ 27
Patch Panel 48 puertos	4	$ 69	$ 276
Patch Panel 24 puertos	1	$ 28	$ 28
RACK's de piso Bea 36U	1	$ 616	$ 616
Rack de 24 U	1	$ 137	$ 137
Rack 37 U	1	$ 199	$ 199
Organizadores Horizontales	25	$ 20	$ 500
Jack datos cat. 6A blindado SIEMON	60	$ 18	$ 1.080
Faceplate dobles SIEMON	50	$ 3	$ 150
Amarras de plastico 15 cm	4 fundas	$1.50	$ 6

Amarras de plastico 25 cm	3 fundas	$ 3	$ 9
CANALETA LISA 20X12 MARFIL DEXSON	25	$1.50	$37.50
CANALETA LISA 32X12 MARFIL DEXSON	15	$2.20	$ 33
ANGULO PLANO 20X12 MARFIL DEXSON	15	$0.50	$ 8
ANGULO PLANO 32X12 MARFIL DEXSON	10	$ 1	$ 10
CAJETÍN DE CANALETA MARFIL 40MM DEXSON	100	$1.42	$ 142
TUBERÍA EMT ¾ REFORZADO	14	$1.84	$ 26
TUBERÍA EMT 1 REFORZADO	12	$2.70	$32.40
TUBERÍA EMT 1 ½ REFORZADO	10	$3.20	$ 32
TUBERÍA PVC 3´´ POLITUBO	10	$ 4	$ 40
CAJAS DE PASO 20X20X15	10	$ 6	$ 60
CAJAS DE PASO 15X15X9	7	$4.37	$30.59
BANDEJA METÁLICA 30cm X 8cm, incluye material e instalación	80m	$ 95	$ 7.600
CERTIFICACIÓN DE PUNTOS DE DATOS CAT. 6A.	350	$ 50	$ 17.500

Fibra Optica 6h Multimodo Om3 50/125 (43 Mts)	150m	$20	$3000
Patch Cord multimodo SC a LC	10	$ 53	$530
Accesorios		$200	$200
Red			
Cisco 1900 Series Wireless WAN Bundle C1921-3G-V-SEC/K9	1	$2,000.00	$2,000.00
Cisco Catalyst 6513-E	1	$4,000.00	$4,000.00
WS-C3850-24T-L Catalyst 3850 Switch	13	$3,000.00	$39,000.00
Media converter, UTP a Fibra Optica	4	$110.00	$440
HP F5000-S-EI VPN Firewall Appliance (JG213A)	1	$16,000.00	$16.000.00
AP-Cisco Aironet Serie 700W	2	$337.00	$674.00
Servidores			
PowerEdge T430	1	$ 4.000	$4000.00
Windows Server 2012 Datacenter	1	$200.00	$200.00
TOTAL INVERSION			$118044,00

Tabla 13: Presupuesto

Adicionalmente, en la Tabla 14, se hace el desglose del personal que laborará en un periodo de 32 días un total de 8 horas diarias, la remuneración de los trabajadores será por hora trabajadas para este cálculo se tomó en consideración los salarios mensuales ejemplo: Un Licenciado en Redes y Sistemas Operativos $900, los asistentes técnicos $500 y otros ayudantes $366, esos son los valores de referencia para el periodo de un mes.

PRESUPUESTO DE PERSONAL Y SERVICIOS ADQUIRIDOS				
Recursos materiales				
Gastos de movilización				$100,00
Recursos materiales				
Personal	Cantidad de personas	Dias	Precio por hora	Valor Total
Personal de I.T	2	30	$6.00	$2,880.00
Asistentes técnicos de I.T	10	20	$3,50	$5,600.00
Otros ayudantes	5	5	$2,00	$400.00
TOTAL				**8980**

Tabla 14: Costos de mano de obra.

4.2. Planificación.

Para el presente proyecto se procede a describir el desarrollo de la implementación que tendrá una duración de 30 días los mismos que como principio tendrá el desmontaje de los dispositivos y cableado de la red que será modificada, y a su vez ir marcando los lugares donde serán implementados los nuevos dispositivos.

Debido a que la implementación del proyecto es un poco extensa y para no interrumpir las labores del Hospital se hará una planificación con el personal encargado para saber con exactitud qué día será el adecuado para empezar con la implementación.

Con respecto a los equipos en su mayoría serán exportados por lo que tendría que hacerse una compra con 30 días de anticipación para tenerlos listos para

cuando se dispongan, como se mencionó se contara con 2 jefes del proyecto que serán los encargados de supervisar a los contratados.

El plan de actividades se detalla por cada tarea en la Figura 4.1 y que tendrá un tiempo total aproximado de 32 días sin incluir días feriados ni fines de semana.

DIAGRAMA DE GANTT

	Nombre de tarea	Duración	Comienzo	Fin
1	**Implementacion del proyecto**	**32 días**	**mié 01/03/1**	**jue 13/04/17**
2	Compra de los equipos	10 días	mié 01/03/1	mar 14/03/1
3	Compra de cableado	3 días	mié 15/03/1	vie 17/03/17
4	Extraccion del cableado existente	4 días	lun 20/03/17	jue 23/03/17
5	Marcar los lugares donde seran instalados los nuevos equipos	2 días	vie 24/03/17	lun 27/03/17
6	Instalacion e la parte cableada, configuracion y comprobacion de la funcionalidad	5 días	mar 28/03/17	lun 03/04/17
7	Instalacion de los dispositivos de red	3 días	mar 04/04/1	jue 06/04/17
8	Configuracion de dispositivos	3 días	vie 07/04/17	mar 11/04/1
9	Prueba y correccion de errores del total de la red	32 días	**mié 01/03/17**	jue 13/04/17

Figura 4.1: Plan de trabajo.

CONCLUSIONES Y RECOMENDACIONES

A continuación, se muestran las conclusiones a las que se llega después de haber realizado el diseño:

El tener una red de datos con una infraestructura tecnológica de punta permite mejorar el sistema de atención en el hospital, agilizar la administración y acceder rápido a la información de sus pacientes.

Aplicar las normas ANSI/EIA/TIA, permiten tener un mejor cuidado y orden del cableado estructurado y tener protegidos los equipos en los lugares instalados.

Implementar mecanismos de seguridad, permite que la información que circula tanto dentro de la red como fuera de la red se mantenga confiable y segura.

Tener una red segmentada, permite tener una comunicación más ágil, dinámica y segura, para así tener balanceo de carga de los paquetes de datos y una administración más efectiva.

Tener políticas de seguridad facilita controlar el acceso tanto a la red como a todos los recursos de la misma.

Para poder tener un mayor beneficio de lo que se propone en este proyecto se dan las siguientes recomendaciones:

Sabiendo que la información que se genera en el hospital es muy delicada y se necesita una conexión siempre activa con internet para actualizar datos, ver diagnósticos, entre otra información se recomienda contratar un proveedor adicional de internet es decir tener 2 proveedores, ya que en caso de que uno de ellos falle, el otro proveedor estará activo lo que evitara que el Hospital quede incomunicado.

Se recomienda dar mantenimiento a toda la red por lo menos una vez al año para su óptimo funcionamiento.

El servidor antivirus, así como su licencia deberán ser renovados cada año, así como también los antivirus clientes deberán ser actualizados cada vez que exista una nueva actualización.

Para que la red conserve la seguridad y el rendimiento deseado es recomendable que se prohíba el acceso al cuarto de telecomunicaciones. Solo debe ingresar el personal IT encargado.

Para mantener los datos seguros se debe realizar un almacenamiento redundante el cual permite duplicar los datos consiguiendo así hacer el “Backup”. Este sistema de almacenamiento redundante se lo puede habilitar en el servidor que maneja Active Directory.

Los equipos recomendados en este proyecto pueden ser modificados siempre y cuando se logre los objetivos que son: Que no afecte el rendimiento de la red, tenga capacidad para manejar los recursos de la red y que los equipos tengan la capacidad de ser administrables.

Al momento de realizar la implementación se recomienda que se siga lo establecido en las especificaciones planteadas debido a que se ha tomado en cuenta normas internacionales que permiten tener una infraestructura tecnología adecuada para el correcto desempeño de las labores del hospital.

BIBLIOGRAFÍA

[1]“Data Cabling – ACTIONCTI ”. [Online]. Disponible en: http://www.actioncti.com/data-cabling/. [Accedido: 19-abr-2017].

[2]“HTTP Archive – Trends: Peso promedio de las páginas web”. [Online]. Disponible en: http://httparchive.org/trends.php. [Accedido: 19-abr-2017].

[3]“Formula para calcular un ancho de banda de una sede principal | General | Cisco Support Community”. [Online]. Disponible en: https://supportforums.cisco.com/es/discussion/12085581. [Accedido: 19-abr-2017].

[4] LEVITON Network Solutions (2012), Sistemas de cableado y normas en las intalaciones de salud . “3801b_NL_CrossTalk_Mar_Apr_2012_Spanish .pdf”. .

[5] COMMSCOPE 2011. ”Normas de cableado TIA-1179”. [Online]. Disponible en: https://www.sistemamid.com/download.php?a=1012

[8]U. Desarrollo, «Normas sobre Cableado Estructurado - Unitel Telecomunicaciones», *Unitel - Soluciones e infraestructuras Tecnológicas*, 24-sep-2013. [Online]. Disponible en: https://unitel-tc.com/normas-sobre-cableado-estructurado/. [Accedido: 10-dic-2016].

[9] “TIA Standards Store | IHS Markit Standards Store”. [Online]. Disponible en: https://global.ihs.com/search_res.cfm?RID=TIA&INPUT_DOC_NUMBER=TIA-568. [Accedido: 19-abr-2017].

[10]”Cableado horizontal”.- SISCOMTEL PERU S.A.C. [Online]. Disponible en: http://siscomtelperu.com.pe/cableado-horizontal. [Accedido: 10-dic-2016].

[11]”IEEE-SA -IEEE Get 802 Program - 802.11: Wireless LANs”. [Online]. Disponible en: http://standards.ieee.org/about/get/802/802.11.html. [Accedido: 19-abr-2017].

[12]”IEEE 802.11, The Working Group Setting the Standards for Wireless LANs”. [Online]. Disponible en: http://www.ieee802.org/11/. [Accedido: 19-abr-2017].

ANEXOS

A: Configuraciones de los equipos.

Seguridad de los equipos de red.

- **Seguridad de los Switch's.**

  Los switch's permitirán interconectar segmentos de red, pasando datos de un segmento de red origen a segmento de red destino. Estos equipos deben tener establecido un nivel alto de seguridad para evitar posibles ataques, robo de información y fallas en la red.

  Sugerimos establecer los siguientes parámetros de seguridad a los dispositivos switch administrables:

  Establecer contraseñas de acceso a cada dispositivo. Para esto usaremos los comandos:

  switch # conf t
  switch(config) # line console 0
  switch (config-line)# password cisco
  switch (config-line)# login

  Al ejecutar los comandos anteriores asignaremos una contraseña segura para el ingreso a la consola del switch. Luego habilitaremos mediante una contraseña el ingreso al switch mediante conexiones telnet con el siguiente comando:

  switch (config-line)# line vty 0 15
  switch (config-line)# password cisco
  switch (config-line)# login
  switch (config-line)# exit
  switch (config)# enable secret class

  Luego de establecer seguridad de acceso al switch podemos dar mayor seguridad a cada uno de sus puertos

```
 switch# conf t
switch(config)# int fa0/1
switch(config-if)#switchport mode access
switch(config-if)#switchport port-security
switch(config-if)#switchport port-security maximum 2
switch(config-if)#switchport port-security mac-address sticky
switch(config-if)#switchport port-security violation protect
switch(config-if)#exit
```

Explicación: Ingresamos a la interfaz fa0/1. Configuramos que ese puerto sea tipo “acceso”, se activa el modo de seguridad de puerto con el comando switchport port-security , se establece que máximo dos dispositivos se conectaran a este puerto con el comando switchport port-security maximum 2, luego con el siguiente comando switchport port-security mac-address sticky, le indicamos que el primer equipo que se conecte será seguro cada vez que se conecte a ese puerto y finalmente con el comando switchport port-security violation protect, le indicara al switch que rechaza los paquetes si es que la MAC del equipo que se conecta no es segura, sin embargo no advierte que existe una violación de seguridad. En este último comando tendremos tres variantes: Restrict, Protect y shutdown, cada una realiza una función diferente.

Creacion de Vlan´s

Para la creación de una Vlan se usará los siguientes comandos:

```
SW1(config)#vlan 10
```

Y se le asigna un nombre a la Vlan para poderla identificar:

```
SW1(config-vlan)#name SERVICIOS
```

Lo mismo se hace con todas las Vlan´s de los demás servicios y en los otros switches.

Los puertos para la conexion entre switches serán en modo troncal.

```
Switch(config)#int f0/14

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk encapsulation dot1q
```

Para asignar una Vlan a un Puerto y este a su vez para que se pueda comunicar con el dispositivo final (computadora) se la asignara el puerto en modo acceso del switch se realiza con los siguientes comandos:

Switch(config)#int f0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

Configuración de VTP en switch:

Sugerimos configurar VTP ya que es un protocolo que permite propagar las Vlans que están bajo su dominio en un switch. Por lo tanto para que el switch pertenezca al mismo dominio y se propaguen las vlans deben cumplir los siguientes parámetros:

- Debe tener activada la misma versión de VTP y la misma contraseña
- Debe configurarse con el mismo dominio

El switch puede ser configurado de tres modos:

Servidor: Configuramos las vlans que deseamos propagar a los demás equipos.

Cliente: Este equipo recibirá las vlans y las podrá utilizar.

Transparente: No aprende del switch modo servidor pero tampoco descarta las configuraciones las cuales las reenvía a los switchs cercanos que están en modo cliente. Podemos crear vlans localmente.

Los comandos de configuración son los siguientes:

Switch(config)#vtp mode [MODO]

Switch(config)#vtp domain [DOMINIO]

Switch(config)#vtp password [CONTRASEÑA]

- **Seguridad del Router**

  Seguridad VTY

  R1#line vty 0 4

  R1#password cisco

  R1# enable secret cisco

  Seguridad de acceso por consola

  R1#line con 0

  R1#password cisco

  R1#login

  Seguridad Aux

  R1#line aux 0

  R1#password cisco

  R1#login

  Seguridad de las claves y de inactividad

  R1#security password min-length 8

  R1#exec-timeout 10 0

  R1# service password-encryption

  R1#username Admin secret cisco12345

  Bloqueo en caso de error de contraseña

  R1#login authentication telnet_lines

  Para la conexión entre vlan´s se la realizara con los siguientes comandos:

  R1(config)#interface fastEthernet 0/0.10

  R1(config-subif)#encapsulation dot1Q 10

R1(config-subif)#ip address 192.168.1.1 255.255.255.0

Seguridad aplicando modelo AAA.

Para la implementación del modelo AAA será con los siguientes comandos:

R1#configure terminal

R1#aaa new-model

R1#aa authentication login default group radius none

R1#aa authentication login telnet_lines group radius

R1#radius-server host “colocar direccion ip” auth-port 1645 key hospleon

R1#line vty 0 4

R1#login authentication telnet_lines

B: Datasheet de los equipos usados en el proyecto.

Cisco 1905 Series Integrated Services Routers

Product Names: CISCO 1905/K9 and CISCO 1905-SEC/K9

Cisco® 1900 Series Integrated Services Routers (ISRs) build on 25 years of Cisco innovation and product leadership. The new platforms are architected to enable the next phase of branch-office evolution, providing rich-media collaboration to the branch office while maximizing operational cost savings. The Cisco Integrated Services Routers Generation 2 (ISR G2) platforms are future-enabled with multicore CPUs, Gigabit Ethernet Switching with enhanced Power over Ethernet (PoE), and new energy monitoring and control capabilities that enhance overall system performance. Additionally, a new Cisco IOS® Software Universal image enables you to decouple the deployment of hardware and software, providing a stable technology foundation that can quickly adapt to evolving network requirements. Overall, the Cisco 1900 Series offers exceptional total cost of ownership (TCO) savings and network agility through the intelligent integration of market-leading security, unified communications, wireless, and application services.

Product Overview

The Cisco 1905 builds on the best-in-class offering of the Cisco 1841 Integrated Services Routers. All Cisco 1900 Series ISRs offer embedded hardware encryption acceleration, optional firewall, intrusion prevention, and advanced security services. In addition, the Cisco 1905 Integrated Services Router has an integrated serial interface module and an enhanced high-speed WAN interface card (EWHIC) slot that supports a choice of LAN, 3G or ISDN modules (Figure 1).

Figure 1. Cisco 1905 Integrated Services Router

Key Business Benefits

The Cisco ISR G2 routers provide superior services integration and agility. Designed for scalability, the modular architecture of these platforms enables you to grow and adapt with your business needs. Table 1 lists the business benefits of the Cisco 1905 Series Integrated Services Routers.

Table 1. Key Features and Benefits of the Cisco 1905 Integrated Services Router

Benefits	Description
Service integration	• The Cisco 1905 offers increased levels of services integration with data, security, wireless, and mobility services enabling greater efficiencies and cost savings.
Services on demand	• A single Cisco IOS Software Universal image is installed on each Cisco ISR G2. The Universal image contains all of the Cisco IOS Software technology sets that can be activated with a software license, allowing your business to quickly deploy advanced features without downloading a new Cisco IOS Software image. Additionally, larger default memory is included to support the new capabilities.
High performance with integrated services	• The Cisco 1905 enables deployment in high-speed WAN environments with concurrent services enabled up to 10 Mbps.

Benefits	Description
Network agility	• Designed to address customer business requirements, the Cisco 1900 Series with the modular architecture offers a performance range of modular interfaces and services as your network needs grow. • Modular interfaces offer increased bandwidth, a diversity of connection options, and network resiliency.
Energy efficiency	• The Cisco 1900 Series architecture provides energy-savings features that include the following: ◦ Intelligent power management allowing you to control power to the modules based on the time of day. Cisco EnergyWise™ technology will be supported in the future. ◦ Services integration and modularity on a single platform performing multiple functions optimizes raw-materials consumption and energy usage. ◦ Platform flexibility and ongoing development of both hardware and software capabilities lead to a longer product lifecycle, lowering all aspects of the TCO, including materials and energy use. ◦ High-efficiency power supplies are provided with each platform.
Investment protection	• The Cisco 1900 Series maximizes investment protection: ◦ Reuse of a broad array of existing modules supported on the original ISRs provides a lower TCO. ◦ A rich set of Cisco IOS Software features is carried forward from the original ISRs and delivered in the universal image. ◦ This router gives you the flexibility to grow as your business needs evolve.

Architecture and Modularity

The Cisco 1905 is architected to meet the application demands of today's branch offices with design flexibility for future applications. The modular architecture is designed to support expanding customer requirements, increased bandwidth, and fully integrated power distribution to modules supporting 802.3af Power over Ethernet (PoE) and Cisco Enhanced PoE (ePoE). Table 2 lists the architectural features and benefits of the Cisco 1905.

Table 2. Architectural Features and Benefits

Architectural Feature	Benefits
Modular platform	• The Cisco 1905 ISR is a modular platform with an integrated serial interface and an additional high-speed WAN interface card (HWIC) slot to provide connectivity and services for varied branch-office network requirements. • It offers a choice of LAN, Serial, 3G, or ISDN modules to accommodate field upgrades to future technologies without requiring replacement of the platform.
Processors	• The Cisco 1905 is powered by high-performance multicore processors that support growing demands of branch-office networks by supporting high-throughput WAN requirements.
Embedded IP Security/Secure Sockets Layer (IPsec/SSL) VPN hardware acceleration	• Embedded hardware encryption acceleration is enhanced to provide higher scalability, which, combined with an optional Cisco IOS Security license, enables WAN link security and VPN services (both IPsec and SSL acceleration). • The onboard encryption hardware (co-processor) outperforms the advanced integration modules (AIMs) of previous generations.
Integrated Gigabit Ethernet ports	• All onboard WAN ports are 10/100/1000 Gigabit Ethernet WAN-routed ports.
Serial port	• The Cisco 1905 has an integrated serial port (HWIC-1T) for serial WAN connectivity.
Innovative universal-serial-bus (USB)-based console access	• A new, innovative, mini-Type B USB console port supports management connectivity when traditional serial ports are not available. • The traditional console and auxiliary ports are also available. You can use either the USB-based console or the RJ-45-based console port to configure the router.
Optional external PoE power supply for distribution of power	• An optional upgrade to the power supply provides inline power, 802.3af-compliant PoE, and Cisco Standard Inline Power to optional integrated switch modules.

Modularity Features and Benefits

The Cisco 1905 provides enhanced modular capabilities (refer to Table 3) that offer you investment protection. A sub-set of modules available on previous generations of Cisco routers, such as the Cisco 1841 ISR, are supported on the Cisco 1905. Additionally, you can easily interchange modules used on the Cisco 1905 with other Cisco routers to provide maximum investment protection. Taking advantage of common interface cards across a network greatly reduces the complexity of managing inventory requirements, implementing large network rollouts, and maintaining configurations across a variety of branch-office sizes.

Table 3. Modularity Features and Benefits

Feature	Benefits
Cisco Enhanced High-Speed WAN Interface Card (EHWIC) 	• The EHWIC slot replaces the HWIC slot and can natively support HWICs and WAN interface cards (WICs). • One integrated EHWIC slot is available on the Cisco 1905 for flexible configurations supporting a choice of LAN, Serial, 3G, or ISDN modules.
USB 2.0 ports	• One high-speed USB 2.0 port is supported. The USB port enables another mechanism for secure token capabilities and storage.

Cisco IOS Software

The Cisco 1905 Integrated Services Routers deliver innovative technologies running on industry-leading Cisco IOS Software. Developed for wide deployment in the world's most demanding enterprise, access, and service provider networks, Cisco IOS Software Releases 15M and T support a comprehensive portfolio of Cisco technologies, including new functions and features delivered in Releases 12.4 and 12.4T, and new innovations that span multiple technology areas, including security, high availability, IP Routing and Multicast, quality of service (QoS), IP Mobility, Multiprotocol Label Switching (MPLS), VPNs, and embedded management.

Cisco IOS Software Licensing and Packaging

A single Cisco IOS Universal image encompassing all functions is delivered with the platforms. You can enable advanced features by activating a software license on the Universal image. In previous generations of access routers, these feature sets required you to download a new software image. Technology packages and feature licenses, enabled through the Cisco software licensing infrastructure, simplify software delivery and decrease the operational costs of deploying new features.

Three major technology licenses are available on the Cisco 1905 Series Integrated Services Routers; you can activate the licenses through the Cisco software activation process identified at http://www.cisco.com/go/sa.

- IP Base: This technology package is available as default
- Data
- Security (SEC) or Security with No Payload Encryption (SEC-NPE)

For additional information and details about Cisco IOS Software licensing and packaging on Cisco 1905 Series Integrated Services Routers, please visit http://www.cisco.com/go/sa.

Key Branch-Office Services

The industry-leading Cisco Integrated Services Routers offer unprecedented levels of services integration. Designed to meet the requirements of the branch office, these platforms provide a complete solution with security, mobility, and data services. Businesses enjoy the benefit by deploying a single device that meets all their needs and saves on capital expenditures (CapEx) and operating expenses (OpEx).

Integrated Network Security for Data and Mobility

Security is essential to protect a business' intellectual property while also ensuring business continuity and providing the ability to extend the corporate workplace to employees who need anytime, anywhere access to company resources. As part of the architectural framework of the SAFE Blueprint from Cisco that allows organizations to identify, prevent, and adapt to network security threats - the Cisco 1900 Series Integrated Services Routers facilitate secure business transactions and collaboration.

The Cisco IOS Software Security technology package license for the Cisco 1900 Series offers a wide array of common security features such as advanced application inspection and control, threat protection, and encryption architectures for enabling more scalable and manageable VPN networks in one solution set. The Cisco 1905 offers native hardware-based encryption acceleration in its co-processor to provide greater IPsec throughput with less overhead for the router processor when compared with software-based encryption solutions. Cisco Integrated Services Routers offer a comprehensive and adaptable security solution for branch-office routers that include features such as:

- Secure connectivity: Achieve secure collaborative communications with Group Encrypted Transport VPN, Dynamic Multipoint VPN (DMVPN), or Enhanced Easy VPN.
- Integrated threat control: Respond to sophisticated network attacks and threats using Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, Cisco IOS IPS, and Cisco IOS Content Filtering and Flexible Packet Matching (FPM).
- Identity management: Intelligently protect endpoints using technologies such as authentication, authorization, and accounting (AAA) and public key infrastructure (PKI).

Detailed information about the security features and solutions supported on the Cisco 1900 Series routers is available at http://www.cisco.com/go/routersecurity.

Mobility Services

Wireless WAN

Cisco 3G wireless WAN (WWAN) modules combine traditional enterprise router functions such as remote management, advanced IP services such as voice over IP (VoIP), and security, with mobility capabilities of 3G WAN access. Using high-speed 3G wireless networks, routers can replace or complement existing landline infrastructure, such as dialup, Frame Relay, and ISDN. Cisco 3G solutions support 3G standards High-Speed Packet Access (HSPA) and Evolution Data Only/Evolution Data Optimized (EVDO), offering you a true multipath WAN backup and the ability to rapidly deploy primary WAN connectivity. For more information about 3G solutions on Cisco Integrated Services Routers, please visit http://www.cisco.com/go/3g.

Integrated LAN Switching

The Cisco 1905 Integrated Services Router will support the EHWIC LAN modules when they become available in the future. The Cisco 1905 supports the existing singlewide Cisco EtherSwitch® HWIC, which greatly expands the capabilities of the router by integrating industry-leading Layer 2 switching.

Managing Your Integrated Services Routers

Network management applications are instrumental in lowering operating expenses (OpEx) while improving network availability by simplifying and automating many of the day-to-day tasks associated with managing an end-to-end network. “Day-one device support” provides immediate manageability support for the ISR, enabling quick and easy deployment, monitoring, and troubleshooting from Cisco and third-party applications.

Organizations rely on Cisco, third-party, and in-house-developed network management applications to achieve their OpEx and productivity goals. Underpinning those applications are the embedded management features available in every ISR. The new ISRs continue a tradition of broad and deep manageability features within the devices. Features such as Cisco IOS IP Service-Level Agreements (IP SLAs), Cisco IOS Embedded Event Manager (EEM), and NetFlow allow you to know what is going on in your network at all times. These features along with Simple Network Management Protocol (SNMP) and syslog support enable your organization’s management applications.

Refer to Tables 4 through 6 for details about Cisco IOS software feature and protocol support, Cisco IOS software management capabilities, and Cisco Network Management applications for Cisco 1905 Integrated Services Routers.

Table 4. Cisco 1905 with Cisco IOS Software Feature and Protocol Support

Feature	Description
Protocols	IPv4, IPv6, static routes, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3) Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPsec, generic routing encapsulation (GRE), Bidirectional Forwarding Detection (BVD), IPv4-to-IPv6 Multicast, MPLS, Layer 2 Tunneling Protocol Version 3 (L2TPv3), 802.1ag, 802.3ah, and Layer 2 and Layer 3 VPN.
Encapsulations	Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), Frame Relay, Multilink Frame Relay (MLFR) (FR.15 and FR.16), High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, X.21, V.35, and EIA-530), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.
Traffic management	QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing (PfR), and Network-Based Application Recognition (NBAR).

Note: For a more comprehensive list of features supported in Cisco IOS Software, refer to the Feature Navigator tool at: http://www.cisco.com/go/fn.

Table 5 highlights several ISR management capabilities that are available within Cisco IOS Software.

Table 5. Cisco IOS Software Management Capabilities

Feature	Description of Feature Supported by Cisco Integrated Services Routers
WSMA	The Web Services Management Agent (WSMA) defines a mechanism through which you can manage a network device, retrieve configuration data information, and upload and manipulate new configuration data. WSMA uses XML-based data encoding that is transported by the Simple Object Access Protocol (SOAP) for the configuration data and protocol messages.
EEM	Cisco IOS EEM is a distributed and customized approach to event detection and recovery offered directly in a Cisco IOS Software device. It offers the ability to monitor events and take informational, corrective, or any desired EEM action when the monitored events occur or when a threshold is reached.
IPSLA	Cisco IOS IP SLAs enable you to assure new business-critical IP applications, as well as IP services that use data, voice, and video, in an IP network.
SNMP, RMON, syslog, NetFlow, and TR-069	Cisco 1900 Series ISRs also support SNMP, Remote Monitoring (RMON), syslog, NetFlow, and TR-069 in addition to the embedded management features previously mentioned.

Cisco Network Management Applications

The applications listed in Table 6 are standalone products that you can purchase or download to manage your Cisco network devices. The applications are built for the different operational phases; you can select the ones that best fit your needs.

Table 6. Network Management Solutions

Operational Phase	Application	Description
Device staging and configuration	Cisco Configuration Professional	• Cisco Configuration Professional is a GUI device-management tool for Cisco IOS Software-based access routers. This tool simplifies routing, firewall, IPS, VPN, unified communications, and WAN and LAN configuration through GUI-based easy-to-use wizards.
Networkwide deployment, configuration, monitoring, and troubleshooting	CiscoWorks LMS	• CiscoWorks LAN Management Solution (LMS) is a suite of integrated applications for simplifying day-to-day management of a Cisco end-to-end network, lowering OpEx while increasing network availability. CiscoWorks LMS offers network managers an easy-to-use web-based interface for configuring, administering, and troubleshooting the Cisco integrated Services Routers, using new instrumentation such as Cisco IOS EEM. • In addition to supporting basic platform services of the ISR, CiscoWorks also provides added-value support for the Cisco Services-Ready Engine, (SRE) enabling the management and distribution of software images to the SRE, thereby reducing the time and complexities associated with image management.
Networkwide staging, configuration, and compliance	CiscoWorks NCM	• CiscoWorks Network Compliance Manager (NCM) tracks and regulates configuration and software changes throughout a multivendor network infrastructure. It provides superior visibility into network changes and can track compliance with a broad variety of regulatory, IT, corporate governance, and technology requirements.
Security staging, configuration, and monitoring	Cisco Security Manager	• Cisco Security Manager is a leading enterprise-class application for managing security. It delivers provisioning of firewall, VPN, and intrusion-prevention-system (IPS) services across Cisco routers, security appliances, and switch service modules. The suite also includes the Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) for monitoring and mitigation.
Configuration and provisioning	Cisco Unified Provisioning Manager	• Cisco Unified Provisioning Manager provides a reliable and scalable web-based solution for managing a company's crucial next-generation communications services. It manages unified communications services in an integrated IP telephony, voicemail, and messaging environment.
Staging, deployment, and changes of licenses	Cisco License Manager	• Easily manage Cisco IOS Software activation and license management for a wide range of Cisco platforms running Cisco IOS Software as well as other operating systems with the secure client-server application Cisco License Manager.
Staging, deployment, and changes to configuration and image files	Cisco Configuration Engine	• Cisco Configuration Engine is a secure network management product that provides zero-touch image and configuration distribution through centralized, template-based management.

Summary and Conclusion

As businesses strive to lower the TCO in running their networks and increase their overall employee productivity with more centralized and collaborative network applications, more intelligent branch-office solutions are required. The Cisco 1905 offers these solutions by providing enhanced performance and increased modular density to support multiple services. The Cisco 1905 is designed to consolidate the functions of separate devices into a single, compact system that can be remotely managed.

Product Specifications

Table 7. Product Specifications of Cisco 1905 Integrated Services Router

	Cisco 1905 Integrated Services Router
Services and Slot Density	
Embedded hardware-based cryptography acceleration (IPsec + SSL)	Yes
RJ-45 onboard LAN 10/100/1000 ports	2
Serial port	Slot 0 (integrated HWIC-1T)
EHWIC slot	1
Memory (DDR2 DRAM): Default/maximum	256 MB/512 MB (license upgradable)
USB Flash memory: Default/maximum	256 MB/256 MB (internal)
External USB flash-memory slots (Type A)	1
USB console port (mini-Type B) (up to 115.2 kbps)	1
Serial console port (up to 115.2 kbps)	1
Serial auxiliary port (up to 115.2 kbps)	1
Integrated power supply	AC
Power-supply options	PoE (external)
Redundant power-supply support	No
Power Specifications	
AC input voltage	100-240V ~
AC input frequency	47-63 Hz
AC input current range AC power supply (maximum) (amps)	1.5-0.6
AC input surge current	<50A
Typical power (no modules)	25W
Maximum power capacity with AC power supply	60W
Maximum power capacity with PoE power supply (platform only)	70W
Maximum PoE device power capacity with PoE power supply	80W
Physical Specifications	
Dimensions (H x W x D)	1.75 x 13.5 x 11.5 in. (4.45 x 34.29 x 29.21 cm)
Rack height	1 rack unit (1RU)
Rack-mount 19 in. (48.3 cm) EIA	Optional
Wall-mount (refer to installation guide for approved orientation)	Yes
Weight: With AC power supply (no modules)	8 lb (3.175 kg)
Weight: With PoE power supply (no modules)	12.8 lb
Maximum weight: Fully configured	14 lb
Airflow	Back to side
Environmental Specifications	
Operating Condition	
Temperature: 5906 ft (1800m) maximum altitude	32-104˚F (0-40˚C)
Temperature: 9843 ft (3000m) maximum altitude	32-77˚F (0-25˚C)
Altitude	10000 ft (3000m)
Humidity	10 to 85 percent relative humidity (RH)
Acoustic: Sound pressure (typical/maximum)	32.9/58.3 dBA
Acoustic: Sound power (typical/maximum)	41.9/67.2 dBA

	Cisco 1905 Integrated Services Router
Transportation and Storage Condition	
Temperature	(-40 to 158˚F (-40 to 70˚C)
Humidity	5 to 95 percent RH
Altitude	15000 ft (4570m)
Regulatory Compliance	
Safety	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1
EMC	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI V-3 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1
Telecom	TIA/EIA/IS-968 CS-03 ANSI T1.101 IEEE 802.3 RTTE Directive

Supported Modules

The Cisco 1905 supports a wide range of modules that span industry-leading breadth of services at the branch office. Please refer to Table 8 for the list of modules supported on the Cisco 1905.

Ordering Information

Table 8 gives ordering information for the Cisco 1905 Router. For information about how to order the Cisco 1900 Series, please visit the Cisco 1900 Series Ordering Guide. To place an order, visit the Cisco Ordering Home Page. For additional product numbers, including the Cisco 1900 Series bundle offerings, please check the Cisco 1900 Series Integrated Services Router Price List or contact your local Cisco account representative.

Table 8. Cisco 1905 Series Basic Ordering Information

Product Number	Product Description
Cisco1905/K9	Cisco 1905 with 2 GE, 1 HWIC-1T, CAB-SS-V35MT, 1 EHWIC slot, 256MB USB Flash (internal), 256MB DRAM, IP Base
Cisco1905-SEC/K9	Cisco 1905 with 2 GE, 1 HWIC-1T, CAB-SS-V35MT, 1 EHWIC slot, 256MB USB Flash (internal), 256MB DRAM, SEC Lic
Software License	
SL-19-IPB-K9(=)	IP Base License (Paper) for Cisco 1900
SL-19-DATA-K9(=)	Data License (Paper) for Cisco 1900
SL-19-SEC-K9(=)	Security License (Paper) for Cisco 1900
Feature License	
FL-SSLVPN10-K9(=)	Cisco SSLVPN Feature license PAK (Paper) - 10 users

Product Number	Product Description
FL-SSLVPN25-K9(=)	Cisco SSLVPN Feature license PAK (Paper) - 25 users
Memory License	
FL-1900-256U512MB*	Cisco 1905 Memory License 256MB to 512MB DRAM Upgrade
Modules (Slot 1)	
HWIC-3G-HSPA	3G HWIC (Non-US) HSPA/UMTS 850/1900/2100MHz 4-band EDGE/GPRS
HWIC-4ESW	Four port 10/100 Ethernet switch interface card
WIC-1B-S/T-V3	1-Port ISDN WAN Interface Card (dial and leased line)
HWIC-1T	1-Port Serial WAN Interface Card
HWIC-1B-U	1-Port ISDN BRI U High-Speed WAN Interface Card
HWIC-4B-S/T	4-port ISDN BRI High-Speed WAN Interface Card
EHWIC-3G-HSPA-U	3.5G EHWIC (Non-US) HSPA/UMTS 850/900/1900/2100MHz with SMS/GPS
EHWIC-3G-HSPA+7	(Non-US) 3.7G HSPA+ Release 7 EHWIC w/ SMS/GPS
EHWIC-4ESG	4-port single-wide Gb Ethernet switch EHWIC

* 512MB is required for SEC and Data Technology Package License with IOS Software Version 15.3(1)T and onwards.

To download the Cisco 1905 with Cisco IOS Software, go to Download Software, click "Router Software", and go to “Cisco ISR 1905 Integrated Services Router.”

ISR Migration Options

Cisco 1900 Series Routers are included in the standard Cisco Technology Migration Program (TMP). Refer to http://www.cisco.com/go/TMP and contact your local Cisco account representative for program details.

Warranty Information

The Cisco 1900 Series Integrated Services Routers have a 1-year limited liability warranty.

Cisco and Partner Services for the Branch

Services from Cisco and our certified partners can help you reduce the cost and complexity of branch-office deployments. We have the depth and breadth of experience across technologies to architect a blueprint for a branch-office solution to meet your company’s needs. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help maintain operational health, strengthen software application functions, solve performance problems, and lower expenses. Optimization services are designed to continually improve performance and help your team succeed with new technologies. For more information, please visit http://www.cisco.com/go/services.

Cisco SMARTnet® technical support for the Cisco 1900 Series is available on a one-time or annual contract basis. Support options range from help-desk assistance to proactive, onsite consultation. All support contracts include:

- Major Cisco IOS Software updates in protocol, security, bandwidth, and feature improvements
- Full access rights to Cisco.com technical libraries for technical assistance, electronic commerce, and product information
- Access to the industry’s largest dedicated technical support staff 24 hours a day

For More Information

For more information about the Cisco 1900 Series, visit http://www.cisco.com/go/1900 or contact your local Cisco account representative.

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.

Printed in USA C78-598372-04 11/13

Cisco Catalyst 6500-E Series Chassis

Product Overview

Cisco introduces the Cisco® Catalyst® 6500 Enhanced Series Chassis (6500-E Series) delivering up to 2 terabits per second of system bandwidth capacity and 80 Gbps of per-slot bandwidth. In a system configured for VSS, this translates to a system capacity of 4 Tbps. The Cisco® Catalyst® 6500 Enhanced Series Chassis will be capable of delivering up to 180 Gbps of per-slot bandwidth with a system capacity of up to 4 terabits per second. A system configured for VSS will be capable of delivering up to 8 Tbps of system bandwidth.

The Cisco Catalyst 6500-E Series Switch offers the broadest range of interface modules with industry-leading performance and advanced feature integration. The Cisco Catalyst 6500-E Series Switch also offers high port densities and comes in 3-, 4-, 6-, 9, 9-Vertical, and 13-slot versions that make it ideal for a range of deployment scenarios.

The Cisco Catalyst 6500-E Series Chassis provides superior investment protection by supporting multiple generations of products in the same chassis, lowering the total cost of ownership. The Cisco Catalyst 6500-E Series Chassis (Figure 1) supports all the Cisco Catalyst 6500 Supervisor Engines up to and including the Cisco Catalyst 6500 Series Supervisor Engine 2T, and associated LAN, WAN, and services modules.

Figure 1. Cisco Catalyst 6500-E Series Chassis

Applications

The versatile Cisco Catalyst 6500-E Series Chassis is ideal for addressing high-performance, high- port-density Fast Ethernet, Gigabit Ethernet, and 10 and 40 Gigabit Ethernet applications in all parts of the network. This series is ideally suited for enterprise core and aggregation environments. The Cisco Catalyst 6500-E Series chassis offers industry-leading 10/100/1000 Gigabit Ethernet, 10 Gigabit Ethernet and 40 Gigabit Ethernet port densities while providing high levels of network resilience.

Features and Benefits

Table 1 lists the Cisco Catalyst 6500-E Series Chassis features and benefits.

Table 1. Features and benefits

Feature	Benefit
Scalability	
3, 4, 6, 9, 9-V and 13-slot modular chassis	Allows flexibility and room for future growth
Delivers up to 2 terabits per second of system bandwidth capacity and 80 Gbps per-slot for all slots. A system configured for VSS has a system capacity of 4 terabits per second. **Capable of delivering up to 4 terabits per second of system bandwidth and 180Gbps of per-slot bandwidth. A system configured for VSS will be capable of delivering up to 8 Tbps of system capacity.**	Scales the system capacity for future needs
High interface capacity	Scales to high-density 40 Gigabit Ethernet, 10 Gigabit Ethernet and Gigabit Ethernet configurations
Increased resiliency	
Standby fabric hot sync	Decreases the supervisor engine switchover time of Supervisor Engine 720 and Supervisor Engine 2T based systems to between 50 and 200 ms, depending on the modules being used
Redundant control channel	Increases resiliency to protect against backplane control channel failures
Redundant supervisor engine option	Increases availability with redundant supervisor engine options
Redundant power supply option	Supports redundant power supplies for increased availability
Fan tray	Supports hot-swappable fan tray The 6509-V-E provides for redundant, hot-swappable fan trays
Environmental	
Side-to-side airflow (except Cisco Catalyst 6509-V-E)	Allows ease of access to ports and cables 6509-V-E has front-to-back air flow to support hot aisle or cold aisle designs
AC and DC power supply	Supports both AC and DC power supply options, including AC and DC mixing
Network Equipment Building Standards Layer 3 (NEBS L3) compliant	Supports NEBS L3 compliance for deployment in demanding environments

Product Specifications

Table 2 lists the Cisco Catalyst 6500-E Series Product Specifications.

Table 2. Product Specifications

	6503-E	6504-E	6506-E	6509-E	6509-V-E	6513-E
Number of Slots	3	4	6	9	9	13
Supervisor Compatibility	Cisco Catalyst 6500 Series Supervisor Engine 32 Cisco Catalyst 6500 Series Supervisor Engine 720-3B Cisco Catalyst 6500 Series Supervisor Engine 720-3BXL Cisco Catalyst 6500 Series Supervisor Engine 720-10G-3C Cisco Catalyst 6500 Series Supervisor Engine 720-10G-3CXL Cisco Catalyst 6500 Series Supervisor Engine 2T					
Power Supply Compatibility * Indicates EoS Power Supply	AC: 1400W, 950W* DC: 950W*	AC: 2700W DC: 2700W	AC: 2500W*, 3000W, 4000W, 6000W, 8700W DC: 2500W, 4000W, 6000W	AC: 2500W*, 3000W, 4000W, 6000W, 8700W DC: 2500W, 4000W, 6000W	AC: 2500W*, 3000W, 4000W, 6000W, 8700W DC: 2500W, 4000W, 6000W	AC: 3000W, 4000W, 6000W, 8700W DC: 2500W, 4000W, 6000W
Module Compatibility	All modules based on the software release in the system					

	6503-E	6504-E	6506-E	6509-E	6509-V-E	6513-E
Software Compatibility (Minimum Software Version)						
With Supervisor Engine 32	• 12.2(18)SXF	• 12.2(18)SXF	• 12.2(18)SXF	• 12.2(18)SXF	• 12.2(18)SXF10	• 12.2(33)SXI1 • 12.2(33)SXH2 • 12.2(18)SXF14
With Supervisor Engine 720	• 12.2(14)SX	• 12.2(18)SXE	• 12.2(14)SX	• 12.2(14)SX	• 12.2(18)SXF10	• 12.2(33)SXI1 • 12.2(33)SXH2 • 12.2(18)SXF14
With Supervisor Engine 720-10 GE	• 12.2(33)SXH	• 12.2(33)SXH	• 12.2(33)SXH	• 12.2(33)SXH	• 12.2(33)SXH	• 12.2(33)SXI1 • 12.2(33)SXH2
With Supervisor Engine 2T-10 GE	• 15.0(1)SY	• 15.0(1)SY	• 15.0(1)SY	• 15.0(1)SY	• 15.0(1)SY	• 15.0(1)SY
Reliability and Availability Calculated Mean Time Between Failure (MTBF)	860,868	677,643	441,418	348,935	330,888	311,778
MIBS	Check the corresponding supervisor engine data sheet					
Network Management	Check the corresponding supervisor engine data sheet					
Physical Dimensions						
Inches	7 x 17.37 x 21.75	8.75 x 17.5 x 21.75	19.2 x 17.5 x 18	24.5 x 17.5 x 18.2	36.65 x 17.2 x 20.7	32.7 x 17.3 x 18.1
Centimeters	17.8 x 44.1 x 55.2	22.2 x 44.45 x 55.25	48.8 x 44.5 x 46.0	62.2 x 44.5 x 46.0	93.3 x 43.1 x 53.3	83.0 x 43.9 x 46
Rack Units (RU)	4	5	11	14	21	19
Weight						
Chassis Only (lbs)	33	40	50	60	121	102
Fully Configured (lbs)	85.4	97	159	190	270	280
Input Voltage	100 to 240 VAC -48 to -60 VDC					
Safety	UL 60950 Second Edition CAN/CSA-C22.2 No. 60950 Second Edition EN 60950 Second Edition IEC 60950 Second Edition AS/NZS 60950					
EMC	FCC Part 15 (CFR 47) Class A VCCI Class A EN55022 Class A CISPR 22 Class A CE marking AS/NZS 3548 Class A ETS300 386 EN55024 EN61000-6-1 EN50082-1					
NEBS/ETSI	GR-1089-Core NEBS Level 3 ETS 300 019 Storage Class 1.1 ETS 300 019 Transportation Class 2.3 ETS 300 019 Stationary Use Class 3.1					

	6503-E	6504-E	6506-E	6509-E	6509-V-E	6513-E
ATIS Pb free and Energy Efficiency	ATIS-0600020.2010 Pb Free circuit packs ATIS-0600015-2009 General Energy Efficiency Requirements (TEER) ATIS-0600015.03-2009 Switch and Router Energy Efficiency ATIS-0600015.01-2009 Server Energy Efficiency VZ.TPR.9205 Verizon Energy Efficiency Requirements for Telecommunication Equipment (TEEER)					
Operating Environment						
Operating Temperature	32°F to 104°F (0 to 40°C)					
Storage Temperature	-4 to 149°F (-20 to 65°C)					
Thermal Transition	0.5°C per minute (hot to cold) 0. 33°C per minute (cold to hot)					
Relative Humidity	Ambient (noncondensing) operating: 5% to 90% Ambient (noncondensing) nonoperating and storage: 5% to 95%					
Operating Altitude	Certified for operation: 0 to 6500 ft (0 to 2000 m) Designed and tested for operation: -200 to 10,000 ft (-60 to 3000 m)					

Ordering Information

Table 3 lists the ordering information for the Cisco Catalyst 6500-E Series Chassis. To place an order, visit the Cisco ordering homepage.

Table 3. Ordering Information

Product Name	Part Number
Cisco Catalyst 6503 Enhanced Chassis	WS-C6503-E
Cisco Catalyst 6503 Enhanced Chassis Spare	WS-C6503-E=
Cisco Catalyst 6503 Enhanced Chassis Fan Tray Spare	WS-C6503-E-FAN=
Cisco Catalyst 6504 Enhanced Chassis	WS-C6504-E
Cisco Catalyst 6504 Enhanced Chassis Spare	WS-C6504-E=
Cisco Catalyst 6504 Enhanced Chassis Fan Tray Spare	WS-C6504-E-FAN=
Cisco Catalyst 6506 Enhanced Chassis	WS-C6506-E
Cisco Catalyst 6506 Enhanced Chassis Spare	WS-C6506-E=
Cisco Catalyst 6506 Enhanced Chassis Fan Tray Spare	WS-C6506-E-FAN=
Cisco Catalyst 6509 Enhanced Chassis	WS-C6509-E
Cisco Catalyst 6509 Enhanced Chassis Spare	WS-C6509-E=
Cisco Catalyst 6509 Enhanced Chassis Fan Tray Spare	WS-C6509-E-FAN=
Cisco Catalyst 6509 Vertical Enhanced Chassis	WS-C6509-V-E
Cisco Catalyst 6509 Vertical Enhanced Chassis Spare	WS-C6509-V-E=
Cisco Catalyst 6509 Vertical Enhanced Chassis Fan Tray Spare	WS-C6509-V-E-FAN=
Cisco Catalyst 6513 Enhanced Chassis	WS-C6513-E
Cisco Catalyst 6513 Enhanced Chassis Spare	WS-C6513-E=
Cisco Catalyst 6513 Enhanced Chassis Fan Tray Spare	WS-C6513-E-FAN=
Cisco Catalyst 6500 1400 W AC Power Supply	PWR-1400-AC=
Cisco Catalyst 6500 2700W AC Power Supply	PWR-2700-AC/4=
Cisco Catalyst 6500 3000W AC Power Supply	WS-CAC-3000W=
Cisco Catalyst 6500 6000W AC Power Supply	WS-CAC-6000W=
Cisco Catalyst 6500 8700W Enhanced AC Power Supply	WS-CAC-8700W-E=
Cisco Catalyst 6500 4000W AC Power Supply for US	WS-CAC-4000W-US=

Product Name	Part Number
Cisco Catalyst 6500 4000W AC Power Supply for International	WS-CAC-4000W-INT=
Cisco Catalyst 6500 2500W DC Power Supply	WS-CDC-2500W=
Cisco Catalyst 6500 2700W DC Power Supply	PWR-2700-DC/4=
Cisco Catalyst 6500 4000W DC Power Supply	PWR-4000-DC=
Cisco Catalyst 6500 6000W DC Power Supply	PWR-6000-DC=

For More Information

For more information about the Cisco Catalyst 6500-E Series chassis, visit: http://www.cisco.com/en/US/partner/products/hw/switches/ps708.

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.

Printed in USA C78-708665-01 10/12

Cisco Catalyst 3850 Series Switches

The Digital Transformation: Converged Wired and Wireless Access and Aggregation

The promise of digital for your business is all about innovating more quickly while reducing risk, cost, and complexity. It will be your network that forms the foundation of your business's transformation.

But supporting your digital organization will require your network to move beyond just connectivity to be a platform for insights, automation, and security.

This is the power of the Cisco® Digital Network Architecture (DNA).

Cisco DNA is a monumental shift on how to design and build networks. The Cisco Catalyst® 3850 Series, as part of the Cisco DNA portfolio of next-generation enterprise-class stackable Ethernet and Multigigabit Ethernet access and aggregation layer switches, securely enables time-saving virtualization, greater automation, and valuable analytics data that directly address your evolving business needs, including less cost to install and operate.

The Cisco Catalyst 3850 Series provides capabilities that ideally suited to support the convergence of wired and wireless access. The new Cisco 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 802.3at 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.

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 throughput[1]
- Cisco StackPower™ technology provides power stacking among stack members for power redundancy[1]

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

- Five optional uplink modules[2] with 4 x Gigabit Ethernet, 2 x 10 Gigabit Ethernet, 4 x 10 Gigabit Ethernet[3], 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
- IEEE 802.3bz (2.5/5 G/s BASE-T) to go beyond 1 Gb/s with existing Cat5e and Cat6
- IEEE 802.1ba Audio Video Bridging (AVB) built in to provide a better AV experience, including improved time synchronization and quality of service (QoS)
- 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
- DNA services delivered through Cisco ONE™ Software, providing simplified, high-value solutions with license portability and flexibility
- 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 Models and 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

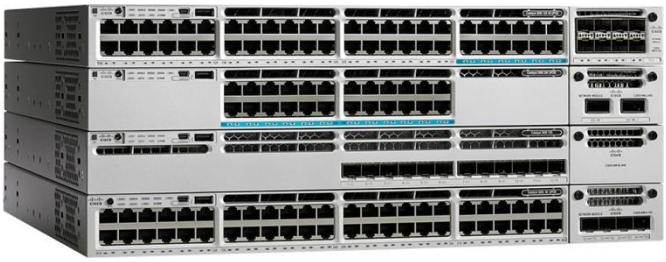
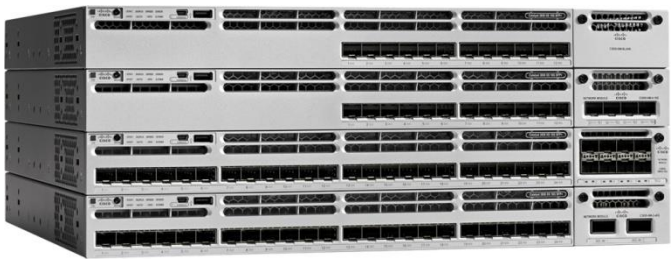


Figure 2. Cisco Catalyst 3850 Switches with 12 and 24 1/10 Gigabit Ethernet SFP+ Ports



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

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

Figure 4. Cisco Catalyst 3850 Switches with 10 Gigabit Ethernet 48 ports

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 module[6]. At the time of switch purchase the customer has the flexibility to choose from the network modules described in Table 2.

[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:

- 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 5. Network Modules with Four Gigabit Ethernet, Two 10 Gigabit Ethernet SFP+, or Four 10 Gigabit Ethernet SFP+ Interfaces

Figure 6 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 6. 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-C3850-12X48U	WS-C3850-12XS 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

	Interface Options	
Network Module	**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 supplies[7]. 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 7.)

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

Figure 7. 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
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

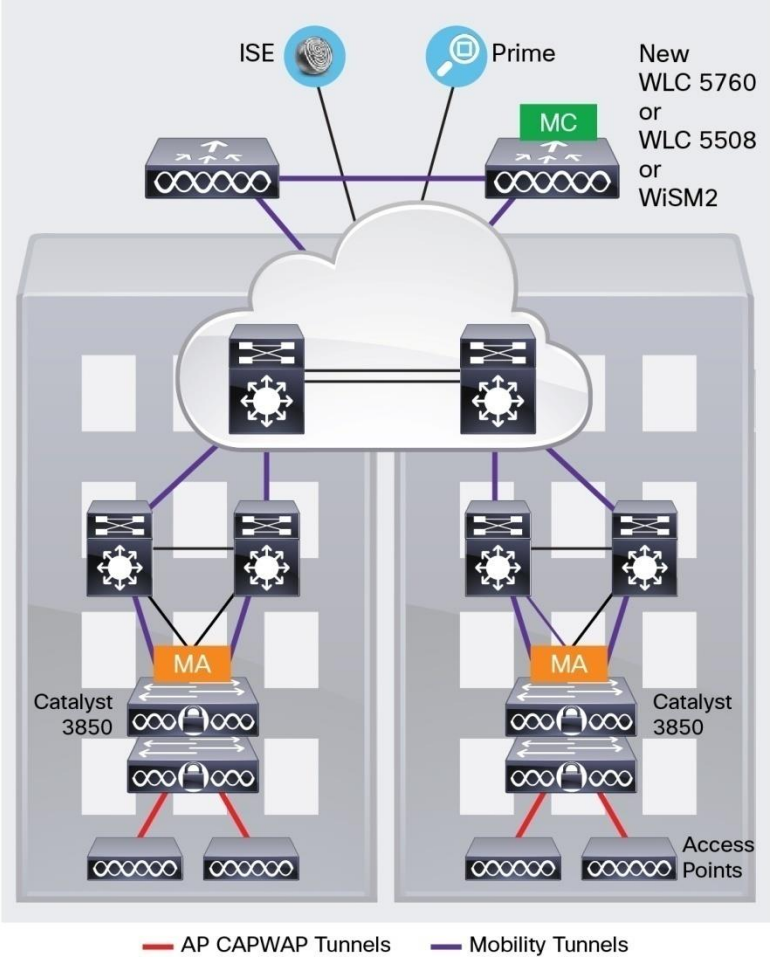
The Cisco Catalyst 3850 is the first stackable access switching platform that enables wired plus wireless services on a single Cisco IOS XE Software-based platform. With this, Cisco has pioneered a host of rich capabilities such as high availability based on stateful switchover (SSO) on stacking, granular 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 8):

- **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** x 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 8. 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 architecture[8]. 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 the 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 StackPower[9] 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 switches[10] 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 9.)

Figure 9. 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
- Audio Video Bridging

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.
- AV Bridging provides reliable time synchronized transmission with no pops or clicks or video dropouts.

- 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.
  - AV Bridging provides reliable A/V streaming without the need for the installer to perform extensive hand tuning of the network.
- 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 StackPower[11], 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.

* 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, RIPng, 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.

Audio Video Bridging

With Cisco IOS® XE Software Release 16.3, Cisco Catalyst 3850 MultiGigabit and 3850 10G SFP+ now support the IEEE 802.1 AVB standard. This standard provided the means for highly reliable delivery of low-latency, time-synchronized AV streaming services through Layer 2 Ethernet networks. The standard also makes it easier to integrate new services and for AV equipment from different vendors to interoperate. Whether the AV endpoint connections are analog or are inflexible digital one to one, the network transport enables many-to-many transparent plug-and-play connections for multiple AV endpoints.

Benefits:

- Improves quality of experience by lowering jitter and latency for time-synchronized delivery of high-quality AV
- Provides scalability of applications across networked deployments, including expansive and complex AV infrastructure
- Lowers total cost of ownership (TCO) with reduced cabling (lowers CapEx) and no license fees (lowers OpEx)

*For more details about AVB and specific models supported, check http://www.cisco.com/go/avb.

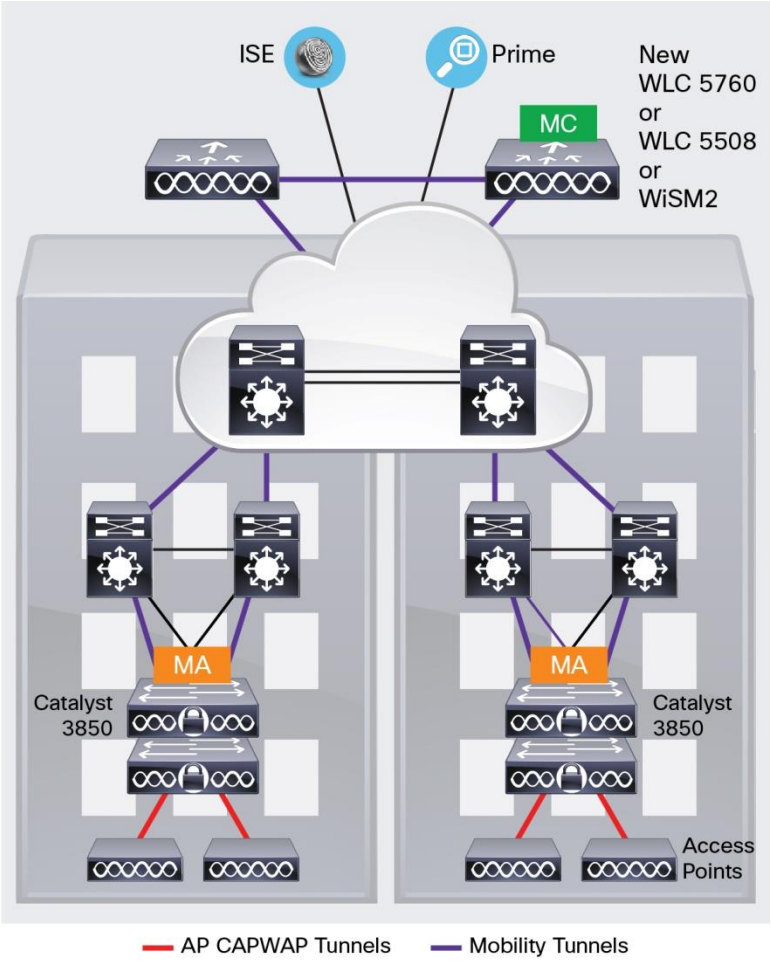
Deployment Options

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 10 shows a Cisco Catalyst 3850 in the campus type deployment.

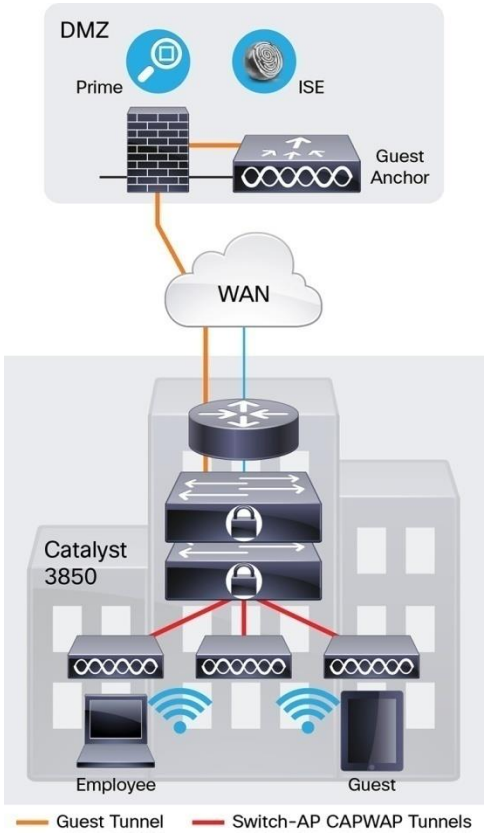
Figure 10. Mobility Controller (MC) and Mobility Agent (MA)



Branch

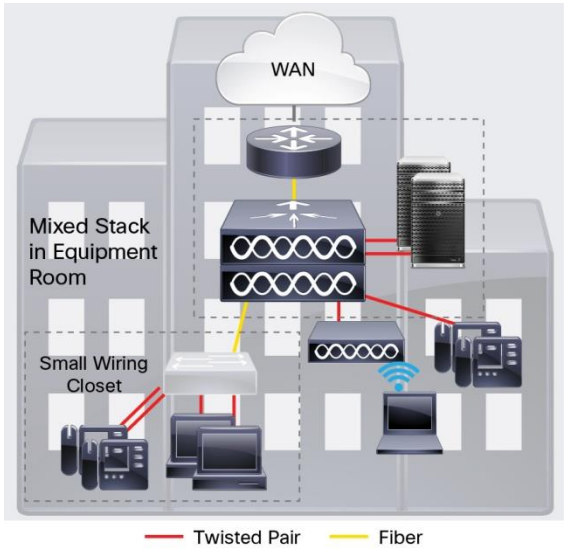
The Cisco Catalyst 3850 is optimized for branch deployments when it operates in mobility controller mode. In this mode, not only can the switch terminate CAPWAP tunnels from the access points and provide client connectivity, it can also manage mobility within the branch. This eliminates the need for 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 11 shows a Cisco Catalyst 3850 in a branch access type deployment.

Figure 11. 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 12).

Figure 12. 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 Aironet 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 **WS-C3850-24P** **WS-C3850-24S**	68.4 Mpps
WS-C3850-48T **WS-C3850-48P** **WS-C3850-48F**	130.95 Mpps
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 Range[12]

Dimensions (H x W x D)	Inches	Centimeters
WS-C3850-12S **WS-C3850-24S** **WS-C3850-24T** **WS-C3850-24P** **WS-C3850-48T** **WS-C3850-48P**	1.75 x 17.5 x 17.7	4.45 x 44.5 x 45.0
WS-C3850-48F **WS-C3850-48U** **WS-C3850-24U** **WS-C3850-24XU** **WS-C3850-12X48U**	1.75 x 17.5 x 19.2	4.45 x 44.5 x 48.8
WS-C3850-12XS **WS-C3850-24XS**	1.75 x 17.5 x 17.7	4.45 X 44.5 x 45.0
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

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

C3850-NM-4-10G	0.75	0.34
C3850-NM-8-10G	0.74	0.34
C3850-NM-2-40G	0.62	0.28
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: • -5ºC to +45ºC, up to 5000 feet (1500m) • -5ºC to +40ºC, up to 10,000 feet (3000m) * Minimum ambient temperature for cold start is 32°F (0°C) Short-term* exceptional conditions: • -5ºC to +50ºC, up to 5000 feet (1500m) • -5ºC to +45ºC, up to 10,000 feet (3000m) • -5ºC to +45ºC, at sea level 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: • -5ºC to +45ºC, up to 6000 feet (1800m) • -5ºC to +40ºC, up to 10,000 feet (3000m) • -5ºC to +35ºC, up to 13,000 feet (4000m) Short-term* exceptional conditions: • -5ºC to +55ºC, up to 6000 feet (1800m) • -5ºC to +50ºC, up to 10,000 feet (3000m) • -5ºC to +45ºC, up to 13,000 feet (4000m) • -5ºC to +45ºC, at sea level 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 9296** **Bystander positions operating to an ambient temperature of 25°C**	With AC or DC power supply (with 24 PoE+ ports loaded): • LpA: 43dB typical, 45dB maximum • LwA: 5.2B typical, 5.5B maximum Typical: Noise emission for a typical configuration Maximum: Statistical maximum to account for variation in production
Storage environment	Temperature: -40ºC to 70ºC 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	• 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	• 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-SNMP-TARGET-EXT-MIB
	CISCO-AUTH-FRAMEWORK-MIB	CISCO-STACKMAKER-MIB
	CISCO-BGP4-MIB, BGP4-MIB	CISCO-MEMORY-POOL-MIB
	CISCO-BRIDGE-EXT-MIB	CISCO-STP-EXTENSIONS-MIB
	CISCO-BULK-FILE-MIB	CISCO-SYSLOG-MIB
	CISCO-CABLE-DIAG-MIB	CISCO-TCP-MIB
	CISCO-CALLHOME-MIB	CISCO-UDLDP-MIB
	CISCO-CEF-MIB	CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB
	CISCO-CIRCUIT-INTERFACE-MIB	CISCO-VLAN-MEMBERSHIP-MIB
	CISCO-ENTITY-VENDORTYPE-OID-MIB	CISCO-VTP-MIB
	CISCO-CONTEXT-MAPPING-MIB	EtherLike-MIB
	CISCO-DEVICE-LOCATION-MIB	HC-RMON-MIB
	CISCO-DHCP-SNOOPING-MIB	IEEE8021-PAE-MIB
	CISCO-EIGRP-MIB	IEEE8023-LAG-MIB
	CISCO-EMBEDDED-EVENT-MGR-MIB	IF-MIB
	CISCO-ENTITY-FRU-CONTROL-MIB	IGMP-MIB
	CISCO-ENTITY-SENSOR-MIB	IGMP-STD-MIB
	ENTITY-MIB	IP-FORWARD-MIB
	CISCO-ERR-DISABLE-MIB	IP-MIB
	CISCO-CONFIG-COPY-MIB	IPMROUTE-STD-MIB
	CISCO-FLOW-MONITOR-MIB	LLDP-EXT-MED-MIB
	CISCO-FTP-CLIENT-MIB	LLDP-MIB
	CISCO-HSRP-EXT-MIB	NOTIFICATION-LOG-MIB
	CISCO-HSRP-MIB	OLD-CISCO-MEMORY-MIB
	CISCO-IETF-ISIS-MIB	CISCO-CDP-MIB
	CISCO-IF-EXTENSION-MIB	POWER-ETHERNET-MIB
	CISCO-IGMP-FILTER-MIB	RMON2-MIB
	CISCO-CONFIG-MAN-MIB	RMON-MIB
	CISCO-IP-CBR-METRICS-MIB	SNMP-COMMUNITY-MIB
	CISCO-IPMROUTE-MIB	SNMP-FRAMEWORK-MIB
	CISCO-IP-STAT-MIB	SNMP-MPD-MIB
	CISCO-IP-URPF-MIB	SNMP-NOTIFICATION-MIB
	CISCO-L2L3-INTERFACE-CONFIG-MIB	SNMP-PROXY-MIB
	CISCO-LAG-MIB	SNMP-TARGET-MIB
	CISCO-LICENSE-MGMT-MIB	SNMP-USM-MIB
	CISCO-MAC-AUTH-BYPASS-MIB	SNMPv2-MIB
	CISCO-MAC-NOTIFICATION-MIB	SNMP-VIEW-BASED-ACM-MIB
	CISCO-MDI-METRICS-MIB	TCP-MIB
	CISCO-FLASH-MIB	UDP-MIB
	CISCO-OSPF-MIB	CISCO-IMAGE-MIB
	CISCO-OSPF-TRAP-MIB	CISCO-STACKWISE-MIB
	CISCO-PAE-MIB	AIRESPMACE-WIRELESS-MIB
	CISCO-PAGP-MIB	CISCO-LWAPP-IDS-MIB
	CISCO-PIM-MIB	CISCO-LWAPP-AP-MIB
	CISCO-PING-MIB	CISCO-LWAPP-CCX-RM-MIB
	CISCO-PORT-QOS-MIB	CISCO-LWAPP-CLIENT-ROAMING-MIB
	CISCO-PORT-SECURITY-MIB	CISCO-LWAPP-DOT11-CCX-CLIENT-DIAG-MIB
	CISCO-PORT-STORM-CONTROL-MIB	CISCO-LWAPP-DOT11-CCX-CLIENT-MIB
	CISCO-POWER-ETHERNET-EXT-MIB	CISCO-LWAPP-DOT11-CLIENT-CCX-REPORTS-MIB
	CISCO-PRIVATE-VLAN-MIB	

Description	Specification	
	CISCO-PROCESS-MIB CISCO-PRODUCTS-MIB CISCO-RF-MIB CISCO-RTP-METRICS-MIB CISCO-RTTMON-MIB CISCO-SMART-INSTALL-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
Standards	IEEE 802.1as 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 802.3bz 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 802.1Qat Stream Reservation Protocol IEEE 802.1Qav 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

Description	Specification			
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).			
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

Models	Uplink Module	Power Consumption (W) (No More Than)			
		0% Traffic	10% Traffic	100% Traffic	Weighted Average
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
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
Cisco SMARTnet Service • 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
Cisco Smart Foundation Service • 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
Cisco SP Base Service • 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 available[2] • Ongoing operating system software updates[1]
Cisco Focused Technical Support Services • Three levels of premium, high-touch services are available: ◦ 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)

Product Number	Product Description
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)
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

Product Number	Product Description
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
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

Product Number	Product Description
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
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)

Product Number	Product Description
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)
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.

Printed in USA C78-720918-24 04/17

Hewlett Packard Enterprise

HPE Firewall Series

Key features

- High performance with up to 40 Gbps throughput
- Advanced virtual firewall
- Rich VPN functions, IPSec/GRE/L2TP
- Comprehensive security protection
- Carrier-grade reliability

Product overview

Built on the latest state-of-the-art multicore CPU platform and with advanced hardware acceleration, the HPE Firewall Series enables advanced scalable network protection from the network core to the network edge with firewall throughput at up to 40 Gbps. The series also features rich VPN abilities, including GRE, L2TP, and IPSec tunneling technologies, which makes it ideal for building VPN gateways. The appliances combine built-in protection against denial-of-service (DoS) attacks, hacking attacks, zonal and virtual stateful packet inspection firewalls, application bandwidth management, audio/video IP multicast routing, and email attachment filtering. The series includes all the advanced security capabilities found in the unified software platform of HPE switches and routers that deliver easy integration, simple management, and network deployment infrastructure, lowering a network's total cost of ownership.

Features and benefits

Firewall

- High performance

  Up to 40 Gbps throughput secures traffic without compromising network performance; a maximum of 4 million concurrent connections and 180,000 new connections per second enables high-volume networks to remain secure under peak traffic

- Application Specific Packet Filter (ASPF)

  Dynamically determines whether to forward or drop a packet by checking its application layer protocol information (such as FTP, HTTP, SMTP, RTSP, and other application layer protocols based on TCP/UDP) and monitoring the connection-based application layer protocol status

- Zone-based access policies

  Groups virtual LANs (VLANs) logically into zones that share common security policies; allows both unicast and multicast policy settings by zones instead of by individual VLANs

- Virtualization

  Multicore architecture enables both multiple zones and multiple separate firewall instances to be created on the same device; support for 256/512 security zones, 256 virtual firewalls, and 4,094 VLANs offers robust protection to all corners of the network; centralized deployment of a single device offering multiple virtual firewalls lowers total cost of ownership through streamlined training, simplified deployment and management, and reduced power consumption

- Application-level gateway (ALG)

  Discovers the IP address and service port information embedded in the application data using deep packet inspection in the firewall; firewall then dynamically opens appropriate connections for specific applications

- NAT

  Fully support NAT applications, including many-to-one, many-to-many, static NAT, dual translation, easy IP, and DNS mapping; supports NAT traversal with multiple protocols, and delivers NAT ALG functions such as DNS, FTP, H.323, and NBT

Virtual private network (VPN)

- IPSec

  Provides secure tunneling over an untrusted network such as the Internet or a wireless network; offers data confidentiality, authenticity, and integrity between two network endpoints

- Layer 2 Tunneling Protocol (L2TP)

  an industry standard-based traffic encapsulation mechanism supported by many common operating systems; will tunnel the Point-to-Point Protocol (PPP) traffic over the IP and non-IP networks; may use the IP/UDP transport mechanism in IP networks

- Generic Routing Encapsulation (GRE)

  Transports Layer 2 connectivity over a Layer 3 path in a secured way; enables the segregation of traffic from site to site

- Manual or automatic Internet Key Exchange (IKE)

  Provides both manual or automatic key exchange required for the algorithms used in encryption or authentication; auto-IKE allows automated management of the public key exchange, providing the highest levels of encryption

Management

- Complete session logging

  Provides detailed information for problem identification and resolution

- Manager and operator privilege levels

  Provides read-only (operator) and read/write (manager) access on CLI and Web browser management interfaces

- Secure Web GUI

  Provides a secure, easy-to-use graphical interface for configuring the module via HTTPS

- Command-line interface (CLI)

  Provides a secure, easy-to-use CLI for configuring the module via SSH or a switch console; provides direct real-time session visibility

- SNMPv1, v2c, and v3

  Facilitate centralized discovery, monitoring, and secure management of networking devices

- Remote monitoring (RMON)

  Uses standard SNMP to monitor essential network functions; supports events, alarm, history, and statistics group plus a private alarm extension group

- FTP, TFTP, and SFTP support

  Offers different mechanisms for configuration updates; FTP allows bidirectional transfers over a TCP/IP network; trivial FTP (TFTP) is a simpler method using User Datagram Protocol (UDP); Secure File Transfer Protocol (SFTP) runs over an SSH tunnel to provide additional security

Layer 3 routing

- Static IP routing

  Provides manually configured routing; includes ECMP capability

- Routing Information Protocol (RIP)

  Provides RIPv1 and RIPv2 routing

- OSPF

  Includes host-based ECMP to provide link redundancy/scalable bandwidth and NSSA

- Border Gateway Protocol 4 (BGP-4)

  Delivers an implementation of the Exterior Gateway Protocol (EGP) utilizing path vectors; uses TCP for enhanced reliability for the route discovery process; reduces bandwidth consumption by advertising only incremental updates; supports extensive policies for increased flexibility; scales to very large networks

- Dual IP stack

  Maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design

- Policy routing

  Allows custom filters for increased performance and security; supports ACLs, IP prefix, AS paths, community lists, and aggregate policies

- Layer 3 IPv6 routing

  Provides routing of IPv6 at media speed; supports static routes, RIPng, OSPFv3, BGP+, policy route, and PIM-SM/DM

Security

- Defense against attacks

  Provides defense against various attacks, such as DoS/DDoS, ARP spoofing, large ICMP packet, address/port scanning, Tracert, IP packets with the Record Route option, and static and dynamic blacklists; also supports binding of MAC address and IP addresses, as well as intelligent defense of worm viruses

- Application layer content filtering

  Supports mail filtering based on SMTP mail address, titles, attachments, and content; supports Web page filtering, including HTTP URL and content filtering

- Multiple security authentication services

  Support RADIUS and HWTACACS authentications, certificate-based (x.509 format) PKI/CA authentication, user identity management (different users own different rights to execute commands), and levels of user views (users of different levels have different management rights)

- Centralized management and auditing

  Provide logging, traffic statistics and analysis, events monitoring and statistics, and mail notification of alarms

Warranty and support

- 1-year warranty

  See hpe.com/networking/warrantysummary for warranty and support information included with your product purchase.

- Software releases

  To find software for your product, refer to hpe.com/networking/support; for details on the software releases available with your product purchase, refer to hpe.com/networking/warrantysummary

HPE Firewall Series

SPECIFICATIONS	HPE F5000 Firewall Standalone Chassis (JG216A)	 HPE F5000-S VPN Firewall Appliance (JG370A)	 HPE 5000-C VPN Firewall Appliance (JG650A)
Included accessories	1 HPE A-F5000 Fan Assembly (JG217A)	1 HPE F5000-S/C VPN Firewall Fan Module (JG878A)	1 HPE F5000-S/C VPN Firewall Fan Module (JG878A)
I/O ports and slots	4 I/O module slots	12 RJ-45 auto-negotiating 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T) 12 fixed Gigabit Ethernet SFP ports 4 SFP+ 10GbE ports (IEEE 802.3ae Type 10GBASE-ER, IEEE 802.3ae Type 10GBASE-LR, IEEE 802.3ae Type 10GBASE-SR) 1 open module slot	12 RJ-45 auto-negotiating 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T) 12 fixed Gigabit Ethernet SFP ports 4 SFP+ 10GbE ports (IEEE 802.3ae Type 10GBASE-ER, IEEE 802.3ae Type 10GBASE-LR, IEEE 802.3ae Type 10GBASE-SR) 1 open module slot
Additional ports and slots	1 MPU (for management modules) slot	1 RJ-45 serial console port 1 Compact Flash port	1 RJ-45 serial console port 1 Compact Flash port
Physical characteristics			
Dimensions	17.17(w) x 18.43(d) x 12.13(h) in (43.61 x 46.81 x 30.81 cm)	17.32(w) x 17.44(d) x 3.47(h) in (43.99 x 44.3 x 8.81 cm) (2U height)	17.32(w) x 17.44(d) x 3.47(h) in (43.99 x 44.3 x 8.81 cm) (2U height)
Weight	55.12 lb (25 kg)	34.61 lb (15.7 kg)	34.61 lb (15.7 kg)
Full configuration weight	97 lb (44 kg)		
Memory and processor	4 GB DDR2 SDRAM, 256 MB compact flash	32 GB DDR2 SDRAM, 256 MB compact flash	16 GB DDR2 SDRAM, 256 MB compact flash
Performance			
Firewall throughput	40 Gbps	20 Gbps	12 Gbps
VPN throughput	2 Gbps 3DES/AES	4 Gbps 3DES/AES	3 Gbps 3DES/AES
Dedicated IPsec VPN tunnels	5,000	8,000	6,000
Connections per second	180,000	200,000	150,000
Concurrent sessions	4 million	4 million	4 million
Number of policies	50,000	50,000	50,000
Number of VLANs	4,000	4,000	4,000
Environment			
Operating temperature	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)
Operating relative humidity	10% to 95%, noncondensing	10% to 95%, noncondensing	10% to 95%, noncondensing

SPECIFICATIONS	HPE F5000 Firewall Standalone Chassis (JG216A)	HPE F5000-S VPN Firewall Appliance (JG370A)	HPE 5000-C VPN Firewall Appliance (JG650A)
Electrical characteristics			
Frequency	50/60 Hz	50/60 Hz	50/60 Hz
AC voltage	100 - 120 / 200 - 240 VAC	100 - 240 VAC	100 - 240 VAC
DC voltage	-48 to -60 VDC	-48 to -60 VDC	-48 to -60 VDC
Current	10/25 A	10 A	10 A
Maximum power rating	650 W	300 W	300 W
Emissions	CISPR 22; EN 55022; ICES-003; AS/NZS CISPR 22; FCC Part 15; EN 61000-3-2; EN 61000-3-3; VCCI V-3	CISPR 22; EN 55022; ICES-003; AS/NZS CISPR 22; FCC Part 15; EN 61000-3-2; EN 61000-3-3; VCCI V-3	CISPR 22; EN 55022; ICES-003; AS/NZS CISPR 22; FCC Part 15; EN 61000-3-2; EN 61000-3-3; VCCI V-3
Immunity			
ESD	EN300 386/EN 55024/EN61000-4-2/ EN301489-1/EN301489-17/ IEC 61000-4-2	EN300 386/EN 55024/EN61000-4-2/ EN301489-1/EN301489-17/ IEC 61000-4-2	EN300 386/EN 55024/EN61000-4-2/ EN301489-1/EN301489-17/ IEC 61000-4-2
Radiated	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-3/ IEC 61000-4-3	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-3/I EC 61000-4-3	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-3/ IEC 61000-4-3
EFT/Burst	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-4/ IEC 61000-4-4	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-4/ IEC 61000-4-4	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-4/ IEC 61000-4-4
Surge	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-5/ IEC 61000-4-5	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-5/ IEC 61000-4-5	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-5/ IEC 61000-4-5
Conducted	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-6/ IEC 61000-4-6	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-6/ IEC 61000-4-6	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-6/ IEC 61000-4-6
Power frequency magnetic field	EN 55024/EN 61000-4-8/ IEC 61000-4-8	EN 55024/EN 61000-4-8/ IEC 61000-4-8	EN 55024/EN 61000-4-8/ IEC 61000-4-8
Voltage dips and interruptions	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-11/ IEC 61000-4-11	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-11/ IEC 61000-4-11	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-11/ IEC 61000-4-11
Management	IMC - Intelligent Management Center; command-line interface; Web browser; SNMP Manager; Telnet; HTTPS; FTP	IMC - Intelligent Management Center; command-line interface; Web browser; SNMP Manager; Telnet; HTTPS; FTP	IMC - Intelligent Management Center; command-line interface; Web browser; SNMP Manager; Telnet; HTTPS; FTP
Notes	Performance • 256 virtual firewalls, max • 1,024 security zones, max	Performance • 256 virtual firewalls, max • 1,024 security zones, max	Performance • 256 virtual firewalls, max • 1,024 security zones, max
Services	Refer to the Hewlett Packard Enterprise website at hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.	Refer to the Hewlett Packard Enterprise website at hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.	Refer to the Hewlett Packard Enterprise website at hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.

HPE Firewall Series

SPECIFICATIONS	HPE F1000-E VPN Firewall Appliance (JD272A)	HPE F1000-EI VPN Firewall Appliance (JG214A)	HPE F1000-S-EI VPN Firewall Appliance (JG213A)
I/O ports and slots	4 dual-personality ports; auto-sensing 10/100/1000BASE-T or SFP 2 HIM slots	12 dual-personality ports; auto-sensing 10/100/1000BASE-T or SFP 2 I/O module slots	12 dual-personality ports; auto-sensing 10/100/1000BASE-T or SFP 2 I/O module slots
Additional ports and slots	1 RJ-45 serial console port 1 RJ-45 Aux port 1 Compact Flash port	1 RJ-45 serial console port	1 RJ-45 serial console port
Physical characteristics			
Dimensions	17.4(w) x 18.43(d) x 1.74(h) in (44.2 x 46.8 x 4.42 cm)	17.4(w) x 15.75(d) x 1.73(h) in (44.2 x 40.01 x 4.39 cm)	17.4(w) x 15.75(d) x 1.73(h) in (44.2 x 40.01 x 4.39 cm)
Weight	14.55 lb (6.6 kg)	12.13 lb (5.5 kg)	12.13 lb (5.5 kg)
Memory and processor	4 GB DDR2 SDRAM, 256 MB compact flash	4 GB DDR2 SDRAM, 1 GB flash	4 GB DDR2 SDRAM, 1 GB flash
Performance			
Firewall throughput	8 Gbps	4 Gbps	2 Gbps
VPN throughput	2 Gbps 3DES/AES	1 Gbps 3DES/AES	600 Mbps 3DES/AES
Dedicated IPsec VPN tunnels	5,000	2,000	2,000
Connections per second	60,000	25,000	25,000
Concurrent sessions	2 million	1 million	1 million
Number of policies	50,000	20,480	20,480
Number of VLANs	4,000	4,000	4,000
Environment			
Operating temperature	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)
Operating relative humidity	10% to 95%, noncondensing	10% to 95%, noncondensing	10% to 95%, noncondensing
Electrical characteristics			
Frequency	50/60 Hz	50/60 Hz	50/60 Hz
AC voltage	100 - 240 VAC	100 - 120 / 200 - 240 VAC	100 - 120 / 200 - 240 VAC
DC voltage		-48 to -60 VDC	-48 to -60 VDC
Current	1 A	1 A	1 A
Maximum power rating	150 W	150 W	150 W
Emissions	CISPR 22; EN 55022; ICES-003; AS/NZS CISPR 22; FCC Part 15; EN 61000-3-2; EN 61000-3-3; VCCI V-3	CISPR 22; EN 55022; ICES-003; AS/NZS CISPR 22; FCC Part 15; EN 61000-3-2; EN 61000-3-3; VCCI V-3	CISPR 22; EN 55022; ICES-003; AS/NZS CISPR 22; FCC Part 15; EN 61000-3-2; EN 61000-3-3; VCCI V-3

SPECIFICATIONS	HPE F1000-E VPN Firewall Appliance (JD272A)	HPE F1000-EI VPN Firewall Appliance (JG214A)	HPE F1000-S-EI VPN Firewall Appliance (JG213A)
Immunity			
ESD	EN300 386/EN 55024/EN61000-4-2/ EN301489-1/EN301489-17/ IEC 61000-4-2	EN300 386/EN 55024/EN61000-4-2/ EN301489-1/EN301489-17/ IEC 61000-4-2	EN300 386/EN 55024/EN61000-4-2/ EN301489-1/EN301489-17/ IEC 61000-4-2
Radiated	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-3/ IEC 61000-4-3	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-3/ IEC 61000-4-3	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-3/ IEC 61000-4-3
EFT/Burst	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-4/ IEC 61000-4-4	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-4/ IEC 61000-4-4	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-4/ IEC 61000-4-4
Surge	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-5/ IEC 61000-4-5	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-5/ IEC 61000-4-5	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-5/ IEC 61000-4-5
Conducted	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-6/ IEC 61000-4-6	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-6/ IEC 61000-4-6	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-6/ IEC 61000-4-6
Power frequency magnetic field	EN 55024/EN 61000-4-8/IEC 61000-4-8	EN 55024/EN 61000-4-8/IEC 61000-4-8	EN 55024/EN 61000-4-8/IEC 61000-4-8
Voltage dips and interruptions	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-11/ IEC 61000-4-11	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-11/ IEC 61000-4-11	EN300 386/EN 55024/EN301489-1/ EN301489-17/EN 61000-4-11/ IEC 61000-4-11
Management	IMC - Intelligent Management Center; command-line interface; Web browser; SNMP Manager; Telnet; HTTPS; FTP	IMC - Intelligent Management Center; command-line interface; Web browser; SNMP Manager; Telnet; HTTPS; FTP	IMC - Intelligent Management Center; command-line interface; Web browser; SNMP Manager; Telnet; HTTPS; FTP
Notes	Performance • 256 virtual firewalls, max • 1,024 security zones, max	Performance • 128 virtual firewalls, max • 512 security zones, max	Performance • 64 virtual firewalls, max • 256 security zones, max
Services	Refer to the Hewlett Packard Enterprise website at hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.	Refer to the Hewlett Packard Enterprise website at hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.	Refer to the Hewlett Packard Enterprise website at hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.

HPE Firewall Series

FEATURES	
Firewall operation mode	Routing mode Transparent mode Hybrid mode
AAA service	Local authentication Standard RADIUS HWTACACS+ RADIUS domain authentication
ASPF	General TCP/UDP application FTP/SMTP/HTTP/RTSP/H323 Protocol State Detection SIP/MGCP/QQ/MSN Protocol State Detection Java/ActiveX blocking and detection Port mapping Support for fragmented packets
NAT	NAPT PAT NAT server Port mapping Bidirectional NAT Static NAT
Network security	Ability to add blacklist by hand or automatically IP and MAC binding ARP reverse query ARP cheat check Management ports closed by default
DDOS	DNS query flood SYN flood Auto starts TCP Proxy when detects SYN flood ICMP flood UDP flood IP spoofing SQL injection filter
L2TP VPN	LNS, LAC L2TP Multi-instance
GRE	GRE tunneling protocol
IPSec	AH/ESP ESP Transport/tunnel NAT traversal Strategy template
IKE	DH Pre-share key authentication method Support for aggressive mode and main exchange mode IKE DPD, PKI/CA

FEATURES

Network feature	IEEE 802.1q VLAN 4K subinterface Static and dynamic ARP Multicast, PIM IGMPv1/v2/v3
Routing	RIP OSPF BGP Static route Policy route
High availability	Active/active mode Active/passive mode Session synchronization for firewall
System management	Web management supports Internet Explorer/Firefox Command-line interface (Console/Telnet/SSH) Classification Manager Unified management through IMC SNMPv2c/v3
Administration	Software upgrades Configuration backup and restore
Logging/Monitoring	Syslog Mini-RMON NTP NAT/ASPF/firewall log stream (binary log)
IPv6 routing and multicast	RIPng OSPFv3 BGP4+ Static route Policy route PIM-SM/PIM-DM
IPv6 security	NAT-PT Manual tunnel IPv6 over IPv4 GRE tunnel 6to4 tunnel (RFC 3056) ISATAP tunnel IPv6 packet filter RADIUS NAT64

STANDARDS AND PROTOCOLS
(applies to all products in series)

IPv6	RFC 1981 IPv6 Path MTU Discovery RFC 2460 IPv6 Specification	RFC 3484 Default Address Selection for IPv6 RFC 3513 IPv6 Addressing Architecture	RFC 3587 IPv6 Global Unicast Address Format RFC 4007 IPv6 Scoped Address Architecture RFC 4862 IPv6 Stateless Address Auto-configuration
Security	IEEE 802.1X:Port-Based Network Access Control (2001) RFC 1321 The MD5 Message-Digest Algorithm RFC 1334 PPP Authentication Protocols (PAP) RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP) RFC 2104 Keyed-Hashing for Message Authentication	RFC 2138 RADIUS Authentication RFC 2618 RADIUS Authentication Client MIB RFC 2620 RADIUS Accounting Client MIB RFC 2716 PPP EAP TLS Authentication Protocol RFC 2865 RADIUS Authentication RFC 2866 RADIUS Accounting	RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support RFC 2868 RADIUS Attributes for Tunnel Protocol Support RFC 2869 RADIUS Extensions draft-grant-tacacs-02 (TACACS)
VPN	RFC 1701 Generic Routing Encapsulation (GRE) RFC 1702 Generic Routing Encapsulation over IPv4 networks. RFC 1828 IP Authentication using Keyed MD5 RFC 1829 The ESP DES-CBC Transform RFC 1853 IP in IP Tunneling RFC 2085 HMAC-MD5 IP Authentication with Replay Prevention RFC 2401 Security Architecture for the Internet Protocol RFC 2402 IP Authentication Header	RFC 2403 The Use of HMAC-MD5-96 within ESP and AH RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH RFC 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV RFC 2406 IP Encapsulating Security Payload (ESP) RFC 2410 The NULL Encryption Algorithm and Its Use With IPSec RFC 2411 IP Security Document Roadmap RFC 2451 The ESP CBC-Mode Cipher Algorithms RFC 2473 Generic Packet Tunneling in IPv6 Specification	RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels RFC 2661 Layer Two Tunneling Protocol "L2TP" RFC 2784 Generic Routing Encapsulation (GRE) RFC 2868 RADIUS Attributes for Tunnel Protocol Support RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPSec RFC 4214 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
IKEv1	RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)	RFC 2409 The Internet Key Exchange (IKE) RFC 2412 The OAKLEY Key Determination Protocol	RFC 3526 More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
PKI	RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols RFC 2511 Internet X.509 Certificate Request Message Format	RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	draft-nourse-scep-06: PKCS#1 PKCS#10 PKCS#12 PKCS#7

HPE Firewall Series accessories

Software	HPE Firewall Manager (JD295A)
Memory	HPE X600 1G Compact Flash Card (JC684A) HPE X600 512M Compact Flash Card (JC685A) HPE X600 256M Compact Flash Card (JC686A)
HPE F5000 Firewall Standalone Chassis (JG216A)	HPE F5000 8-port Gig-T / 4-port GbE Combo Module (JD263A) HPE F5000 2-port 10GbE XFP Module (JD264A) HPE F5000 8-port GbE SFP / 4-port GbE Combo Module (JG212A) HPE F5000 Firewall Main Processing Unit (JG215A) HPE 7500 650W DC Power Supply (JD209A) HPE 7500 650W AC Power Supply (JD217A) HPE F5000 Fan Assembly (JG217A)
HPE F5000-S VPN Firewall Appliance (JG370A)	HPE F5000-S/C 12-port 10/100/1000BASE-T/12-port GbE SFP/6-port 10-GbE SFP+ Module (JG651A) HPE 5800 300W AC Power Supply (JC087A) HPE 5800 300W DC Power Supply (JC090A) HPE F5000-S/C VPN Firewall Fan Module (JG878A)
HPE 5000-C VPN Firewall Appliance (JG650A)	HPE F5000-S/C 12-port 10/100/1000BASE-T/12-port GbE SFP/6-port 10-GbE SFP+ Module (JG651A) HPE 5800 300W AC Power Supply (JC087A) HPE 5800 300W DC Power Supply (JC090A) HPE F5000-S/C VPN Firewall Fan Module (JG878A)
HPE F1000-E VPN Firewall Appliance (JD272A)	HPE 6600 4-port Gig-T HIM Module (JC163A) HPE 6600 8-port Gig-T HIM Module (JC164A) HPE 6600 1-port 10-GbE XFP HIM Module (JC168A) HPE 6600 4-port GbE SFP HIM Module (JC171A)
HPE F1000-EI VPN Firewall Appliance (JG214A)	HPE F1000-S/A 2-port 10GbE SFP+ Module (JG317A) HPE 5800/5500 150W AC Power Supply (JD362A) HPE 5800/5500 150W DC Power Supply (JD366A)
HPE F1000-S-EI VPN Firewall Appliance (JG213A)	HPE F1000-S/A 2-port 10GbE SFP+ Module (JG317A) HPE 5800/5500 150W AC Power Supply (JD362A) HPE 5800/5500 150W DC Power Supply (JD366A)

Learn more at
hpe.com/networking

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA3-7159ENW, November 2015, Rev. 3

Cisco Aironet 700W Series Access Point

KEY FEATURES
Performance with Investment Protection • Six times faster than 802.11a/g networks • Dual-radio, simultaneous 2.4GHz and 5GHz support • Backward-compatible with 802.11a/b/g clients
Wired Access Support • 4 x 10/100/1000BASE-T local Ethernet ports for wired device connectivity • 1 local Ethernet port includes Power-over-Ethernet (PoE) out • 1 x 10/100/1000BASE-T Power-over-Ethernet (PoE) Uplink port
Easy Installation and Power Efficient • 802.11n performance with existing PoE switches • Can be installed with single Ethernet cable powering the unit with PoE to save on additional cabling expenses • Sleek compact design blends into a variety of indoor environments
Secure Interoperability • 802.11n compliant
Simplified Network Management • Controller-based deployment options
Secure Connections • Supports rogue access point detection and denial of service attacks
Greater Network Capacity • Dynamic frequency selection 2 (DFS-2) compliant • U-NII-2 and U-NII-2 extended band support
Easy-to-Install, Small profile Mounting Bracket • Small, compact form factor designed for easy installations for indoor deployments • Included hidden Torx screw and Kensington lock for theft protection

The Cisco® Aironet® 700W Series offers a compact wall plate mountable access point for hospitality and education focused customers looking to modernize their networks to handle today's increasingly complex wireless access demands.

With 802.11n dual-radio 2 x 2 multiple-input multiple-output (MIMO) technology providing at least six times the throughput of existing 802.11a/g networks, the Cisco Aironet 700W Series offers the performance advantage of 802.11n quality at a competitive price.

As part of the Cisco Unified Wireless Network, the 700W Series Access Point provides low total cost of ownership and investment protection by integrating seamlessly with the existing network.

RF Excellence

Building on the Cisco Aironet heritage of RF excellence, the 700W Series Access Point delivers secure and reliable wireless connections with:

- Simultaneous dual band, dual radio with support for 2.4GHz and 5GHz in a compact form factor
- Optimized antenna and radio designs: Consistent network transmit and receive for optimized rate versus range
- Radio resource management (RRM): Automated self-healing optimizes the unpredictability of RF to reduce dead spots and help ensure high-availability client connections
- Cisco BandSelect improves 5-GHz client connections in mixed-client environments

- Advanced security features including Rogue Detection, wIPS and Context-Aware

Product Specifications

Table 1 lists the product specifications for Cisco Aironet 700W Series Access Points.

Table 1. Product Specifications for Cisco Aironet 700W Series Access Points

Item	Specification
Part Numbers	**The Cisco Aironet 700W Wall Plate Access Point: Indoor environments, with internal antennas** ● AIR-CAP702W-x-K9 - Dual-band controller-based 802.11a/g/n ● AIR-CAP702W-xK910 - Eco-pack (dual-band controller-based 802.11a/g/n) 10 quantity access points **Cisco SMARTnet® Service for the Cisco Aironet 700W Series Access Point** ● CON-SNT-AIRCAP7x - SMARTnet 8x5xNBD 702w access point (dual-band 802.11 a/g/n) (e.g. CON-SNT-AIRCAP7A for 702w internal antenna for A Domain) **Cisco Wireless LAN Services** ● AS-WLAN-CNSLT - Cisco Wireless LAN Network Planning and Design Service ● AS-WLAN-CNSLT - Cisco Wireless LAN 802.11n Migration Service ● AS-WLAN-CNSLT - Cisco Wireless LAN Performance and Security Assessment Service **Regulatory domains: (x = regulatory domain)** Customers are responsible for verifying approval for use in their individual countries. To verify approval and to identify the regulatory domain that corresponds to a particular country, please visit: http://www.cisco.com/go/aironet/compliance. Not all regulatory domains have been approved. As they are approved, the part numbers will be available on the Global Price List.
Authentication & Security	● TKIP for WPA, AES for WPA2 ● 802.1X, Radius, AAA (authentication, authorization, accounting) ● 802.11i
Software	● Cisco Unified Wireless Network Software Release ● Cisco IOS® Software Release (future)
802.11n	● 2 x 2 multiple-input multiple-output (MIMO) with two spatial streams ● Maximal ratio combining (MRC) ● 20- and 40-MHz channels ● PHY data rates up to 300 Mbps ● Packet aggregation: A-MPDU (Tx/Rx), A-MSDU (/Rx) ● 802.11 dynamic frequency selection (DFS)[4] ● Cyclic shift diversity (CSD) support ● Antenna Diversity
Data Rates Supported	**802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps** **802.11bg: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps** **802.11n data rates (2.4 GHz[1] and 5 GHz):**

MCS Index[2]	GI[3] = 800ns		GI = 400ns	
	20-MHz Rate (Mbps)	40-MHz Rate (Mbps)	20-MHz Rate (Mbps)	40-MHz Rate (Mbps)
0	6.5	13.5	7.2	15
1	13	27	14.4	30
2	19.5	40.5	21.7	45
3	26	54	28.9	60
4	39	81	43.3	90
5	52	108	57.8	120
6	58.5	121.5	65	135

[1] 2.4 GHz does not support 40 MHz.
[2] MCS Index: The Modulation and Coding Scheme (MCS) index determines the number of spatial streams, the modulation, the coding rate, and data rate values.
[3] GI: A Guard Interval (GI) between symbols helps receivers overcome the effects of multipath delays.

Item	Specification				
	7	65	135	72.2	150
	8	13	27	14.4	30
	9	26	54	28.9	60
	10	39	81	43.3	90
	11	52	108	57.8	120
	12	78	162	86.7	180
	13	104	216	115.6	240
	14	117	243	130	270
	15	130	270	144.4	300

Frequency Band and 20-MHz Operating Channels	**A Regulatory Domain:** • 2.412 to 2.462 GHz; 11 channels • 5.180 to 5.320 GHz; 8 channels • 5.500 to 5.700 GHz; 8 channels (excludes 5.600 to 5.640 GHz) • 5.745 to 5.825 GHz; 5 channels **C Regulatory Domain:** • 2.412 to 2.472 GHz; 13 channels • 5.745 to 5.825 GHz; 5 channels **D (D regulatory domain):** • 2.412 to 2.462 GHz; 11 channels • 5.180 to 5.320 GHz; 8 channels • 5.745 to 5.825 GHz; 5 channels **E Regulatory Domain:** • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels • 5.500 to 5.700 GHz; 8 channels (excludes 5.600 to 5.640 GHz) **H (H regulatory domain):** • 2.412 to 2.472 GHz; 13 channels • 5.150 to 5.350 GHz; 8 channels • 5.745 to 5.825 GHz; 5 channels **I Regulatory Domain:** • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels **K Regulatory Domain:** • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels • 5.500 to 5.620 GHz; 7 channels • 5.745 to 5.805 GHz; 4 channels	**N Regulatory Domain:** • 2.412 to 2.462 GHz; 11 channels • 5.180 to 5.320 GHz; 8 channels • 5.745 to 5.825 GHz; 5 channels **Q Regulatory Domain:** • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels • 5.500 to 5.700 GHz; 11 channels **R Regulatory Domain:** • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels • 5.660 to 5.805 GHz; 7 channels **S Regulatory Domain:** • 2.412 to 2.472 GHz; 13 channels • 5.180 to 5.320 GHz; 8 channels • 5.500 to 5.700 GHz; 11 channels • 5.745 to 5.825 GHz; 5 channels **T Regulatory Domain:** • 2.412 to 2.462 GHz; 11 channels • 5.280 to 5.320 GHz; 3 channels • 5.500 to 5.700 GHz; 11 channels • 5.745 to 5.825 GHz; 5 channels **Z Regulatory Domain:** • 2.412 to 2.462 GHz; 11 channels • 5.180 to 5.320 GHz; 8 channels • 5.500 to 5.700 GHz; 11 channels (excludes 5.600 to 5.640 GHz) • 5.745 to 5.825 GHz; 5 channels
Maximum Number of Nonoverlapping Channels	**2.4 GHz** • 802.11b/g: ◦ 20 MHz: 3 • 802.11n: ◦ 20 MHz: 3	**5 GHz** • 802.11a: ◦ 20 MHz: 21 • 802.11n: ◦ 20 MHz: 21 ◦ 40 MHz: 9
Note: This varies by regulatory domain. Refer to the product documentation for specific details for each regulatory domain.		

Receive sensitivity (Combined sensitivity)	**802.11b** -98 dBm @ 1 Mb/s -95 dBm @ 2 Mb/s -93 dBm @ 5.5 Mb/s -91 dBm @ 11 Mb/s	**802.11g** -94dBm @ 6 Mb/s -92 dBm @ 9 Mb/s -91 dBm @ 12 Mb/s -89 dBm @ 18 Mb/s -85 dBm @ 24 Mb/s -82 dBm @ 36 Mb/s	**802.11a** -93 dBm @ 6 Mb/s -91 dBm @ 9 Mb/s -90 dBm @ 12 Mb/s -87 dBm @ 18 Mb/s -84 dBm @ 24 Mb/s -81 dBm @ 36 Mb/s

Item	Specification		
		-78 dBm @ 48 Mb/s -76 dBm @ 54 Mb/s	-76 dBm @ 48 Mb/s -75 dBm @ 54 Mb/s
	2.4-GHz **802.11n (HT20)** -93 dBm @ MCS0 -90 dBm @ MCS1 -88 dBm @ MCS2 -85 dBm @ MCS3 -81 dBm @ MCS4 -77 dBm @ MCS5 -75 dBm @ MCS6 -74 dBm @ MCS7 -91dBm @ MCS8 -88 dBm @ MCS9 -86 dBm @ MCS10 -83 dBm @ MCS11 -79 dBm @ MCS12 -75 dBm @ MCS13 -73 dBm @ MCS14 -72 dBm @ MCS15	**5-GHz** **802.11n (HT20)** -93 dBm @ MCS0 -90 dBm @ MCS1 -87 dBm @ MCS2 -83 dBm @ MCS3 -80 dBm @ MCS4 -75 dBm @ MCS5 -74 dBm @ MCS6 -72 dBm @ MCS7 -91 dBm @ MCS8 -88 dBm @ MCS9 -85 dBm @ MCS10 -81 dBm @ MCS11 -78 dBm @ MCS12 -73 dBm @ MCS13 -72 dBm @ MCS14 -70 dBm @ MCS15	**5-GHz** **802.11n (HT40)** -89 dBm @ MCS0 -86 dBm @ MCS1 -83 dBm @ MCS2 -79 dBm @ MCS3 -76 dBm @ MCS4 -72 dBm @ MCS5 -71 dBm @ MCS6 -70 dBm @ MCS7 -88 dBm @ MCS8 -84 dBm @ MCS9 -81 dBm @ MCS10 -77 dBm @ MCS11 -74 dBm @ MCS12 -70 dBm @ MCS13 -69 dBm @ MCS14 -68 dBm @ MCS15
Maximum Transmit Power	**2.4 GHz** ● 802.11b ◦ 20 dBm with one antenna ● 802.11g ◦ 20 dBm with two antennas ● 802.11n (HT20) ◦ 20 dBm with two antennas		**5 GHz** ● 802.11a ◦ 20 dBm with one antenna ● 802.11n non-HT duplicate mode ◦ 20 dBm with two antennas ● 802.11n (HT20) ◦ 20 dBm with two antennas ● 802.11n (HT40) ◦ 20 dBm with two antennas
Note: The maximum power setting will vary by channel and according to individual country regulations. Refer to the product documentation for specific details.			
Available Transmit Power Settings	**2.4 GHz** 20 dBm (100 mW) 17 dBm (50 mW) 14 dBm (25 mW) 11 dBm (12.5 mW) 8 dBm (6.25 mW) 5 dBm (3.13 mW) 2 dBm (1.56 mW) -1 dBm (0.78 mW)		**5 GHz** 20 dBm (100 mW) 17 dBm (50 mW) 14 dBm (25 mW) 11 dBm (12.5 mW) 8 dBm (6.25 mW) 5 dBm (3.13 mW) 2 dBm (1.56 mW) -1 dBm (0.78mW)
Note: The maximum power setting will vary by channel and according to individual country regulations. Refer to the product documentation for specific details.			
Integrated Antennas	● 2.4 GHz, gain 2.0 dBi ● 5 GHz, gain 4.0 dBi		
Interfaces	● 10/100/1000BASE-T PoE Uplink port ● Management console port (RJ-45) ● 4 x 10/100/1000BASE-T ports (RJ-45) (local Ethernet ports) ● 1 PoE out port (when powered by 802.3at Ethernet switch, or Cisco power injector AIR-PWRJ4=, or Cisco Local Power Supply) ● DC power connector		

Item	Specification
Indicators	• Status LED indicates boot loader status, association status, operating status, boot loader warnings, boot loader errors • Per-port status for local Ethernet ports
Dimensions (W x L x H)	• Access point (without mounting bracket): 6 x 4 x 1.6 inches (152.4 x 101.6 x 40.6 mm)
Weight	• Access point (without mounting bracket): 0.86 lb (0.39 Kg)
Environmental	**Cisco Aironet 700W** • Non-operating (storage) temperature: -22 to 158°F (-30 to +70°C) • Non-operating (storage) maximum altitude: 25°C, 15,000 ft. • Operating temperature: 32 to 104°F (0 to 40°C) • Operating humidity: 10 to 90% percent (noncondensing) • Operating maximum altitude: 40°C, 9843 ft.
System	• 128 MB DRAM • 128 MB flash • 560MHz System CPU
Input Power Requirements	• 44 to 57 VDC • Optional - Power Supply and Power Injector: 100 to 240 VAC; 49 to 60 Hz
Powering Options	• 802.3af/at Ethernet Switch • Optional - Cisco Power Injectors (AIR-PWRINJ5=, AIR-PWRINJ4=) • Optional - Cisco Local Power Supply (AIR-PWR-C=)
Power Draw	• Maximum values: 11.6W with no PoE out, 22.1W with PoE Class 2 out, and 29.2W with PoE Class 0 out • **Note:** When deployed using PoE, the power draw numbers listed above include the power loss in 100m of cabling on the Uplink port and the 100m of cabling on the PoE Out port.
Accessories	• Mounting brackets: AIR-AP-BRACKET-W • Cisco Local Power Supply: AIR-PWR-C= (sold separately)
Warranty	Limited Lifetime Hardware Warranty
Compliance	**Standards** • **Safety:** ◦ UL 60950-1 ◦ CAN/CSA-C22.2 No. 60950-1 ◦ IEC 60950-1 ◦ EN 60950-1 • **Radio approvals:** ◦ FCC Part 15.247, 15.407 ◦ RSS-210 (Canada) ◦ EN 300.328, EN 301.893 (Europe) ◦ ARIB-STD 33 (Japan) ◦ ARIB-STD 66 (Japan) ◦ ARIB-STD T71 (Japan) ◦ AS/NZS 4268.2003 (Australia and New Zealand) ◦ EMI and susceptibility (Class B) ◦ FCC Part 15.107 and 15.109 ◦ ICES-003 (Canada) ◦ VCCI (Japan) ◦ SRRC (China) ◦ EN 301.489-1 and -17 (Europe) ◦ EN 60601-1-2 EMC requirements for the Medical Directive 93/42/EEC • **IEEE Standard:** ◦ IEEE 802.11a/b/g, IEEE 802.11n, IEEE 802.11h, IEEE 802.11d • **Security:** ◦ 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA ◦ 802.1X ◦ Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP)

Item	Specification
	• **EAP Type(s):** ◦ Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) ◦ EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) ◦ Protected EAP (PEAP) v0 or EAP-MSCHAPv2 ◦ Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) ◦ PEAPv1 or EAP-Generic Token Card (GTC) ◦ EAP-Subscriber Identity Module (SIM) • **Multimedia:** ◦ Wi-Fi Multimedia (WMM™) • **Other:** ◦ FCC Bulletin OET-65C ◦ RSS-102

Limited Lifetime Hardware Warranty

The Cisco Aironet 700W Series Access Point comes with a Limited Lifetime Warranty that provides full warranty coverage of the hardware for as long as the original end user continues to own or use the product. The warranty includes 10-day advance hardware replacement and ensures that software media is defect-free for 90 days. For more details, visit: http://www.cisco.com/go/warranty.

Cisco Wireless LAN Services

Realize the full business value of your technology investments faster with intelligent, customized services from Cisco and our partners. Backed by deep networking expertise and a broad ecosystem of partners, Cisco Wireless LAN Services enable you to deploy a sound, scalable mobility network that enables rich media collaboration while improving the operational efficiency gained from a converged wired and wireless network infrastructure based on the Cisco Unified Wireless Network. Together with partners, we offer expert plan, build, and run services to accelerate your transition to advanced mobility services while continuously optimizing the performance, reliability, and security of that architecture after it is deployed. For more details, visit: http://www.cisco.com/go/wirelesslanservices.

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.

Printed in USA C78-728968-01 04/14

PowerEdge T430

The powerful and reliable PowerEdge T430 two-socket tower server delivers performance, expandability, and quiet operation to office environments.

The PowerEdge T430 is an excellent fit for a wide range of office workloads, including workgroup collaboration and productivity applications, mail and messaging, file and print serving, and web serving. The T430 is an ideal choice for small office and remote office/branch office (ROBO) sites in need of single-server performance and capacity.

Deliver peak performance

Accelerate performance across a wide range of workloads with the latest Intel® Xeon® processor E5-2600 v4 product family. Drive fast response times and expand memory capacity over time with 12 DIMM slots and DDR4 memory. Boost I/O performance with 6 x PCIe 3.0 slots delivering 2x data throughput compared to PCIe 2.0.

Discover greater versatility

Install performance where it's needed with a rackable tower form factor, short 22-inch depth and quiet office acoustics. Grow data storage over time with a choice of internal hard drive form factors and capacities, guarded by RAID options for data protection and optimized performance. Adapt flexibly to changing workload conditions with an expandable virtualization-ready platform.

Maximize operational efficiency

Save time and reduce potential for error with simplified, intuitive systems management, and help reduce costs with energy-efficient features. Protect IT investments by using the management tools you know — Dell OpenManage Essentials, BMC® Software, Microsoft® System Center, VMware® vCenter®. Harness your budget with energy-efficient processors, memory and power supplies and Fresh Air 2.0 capability.

Innovative management with intelligent automation

The Dell OpenManage systems management portfolio includes innovative solutions that simplify and automate essential server lifecycle management tasks — making IT operations more efficient and Dell servers the most productive, reliable and cost effective. Leveraging the incomparable agent-free capabilities of the PowerEdge embedded integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller technology, server deployment, configuration and updates are streamlined across the OpenManage portfolio and through integration with third-party management solutions.

Monitoring and control of Dell and third-party data center hardware is provided by OpenManage Essentials and with anytime, anywhere mobile access, through OpenManage Mobile. OpenManage Essentials now also delivers Server Configuration Management capabilities that automate one-many PowerEdge bare-metal server and OS deployments, quick and consistent replication of configurations and ensure compliance to a predefined baseline with automated drift detection.

PowerEdge T430

- Short 22" depth and quiet office acoustics
- Intel Xeon processor E5-2600 v4 product family
- 12 x DIMMs DDR4 memory
- 4 x PCIe 3.0, 2 x PCIe 2.0 slots

Feature	PowerEdge T430 technical specification
Form factor	Tower (5U rackable)
Processors	Intel® Xeon® processor E5-2600 v4 product family **Chipset**: Intel C610 series chipset **Processor sockets**: 2 **Internal interconnect**: Two QPI links at 9.6 GT/s **Cache**: 2.5MB per core; core options: 4, 6, 8, 10, 12, 14
Memory	12 DIMM slots: 4GB/8GB/16GB/32GB DDR4 up to 2400MT/s
I/O slots	Support for up to 6 full height slots: 4 x PCIe 3.0, 2 x PCIe 2.0
RAID controller	Support for a maximum of 1 internal controller and 1 external controller PERC H730, PERC H730P and PERC H830
Network controller	2 x 1GbE LOMs
Hard drives	SAS, SATA, nearline SAS, SSD
Communications	Broadcom® 5720 Click here for T430 supported network interface cards (NICs) and host bus adapters (HBAs) and scroll to "Additional Network Cards" section.
Power supply	495W, 750W, 1100W PSU; 450W cabled non-redundant PSU
Availability	Hot-plug drives bays; high-efficiency, hot-plug, redundant power supply units; fan redundancy; extended thermal support; Dell fault-resilient memory; Internal dual SD modules
Systems management	**Systems management:** IPMI 2.0 compliant; Dell OpenManage Essentials; Dell OpenManage Mobile; Dell OpenManage Power Center **Remote management** iDRAC8 with Lifecycle Controller, iDRAC8 Express (default), iDRAC8 Enterprise (upgrade), 8GB vFlash media (upgrade), 16GB vFlash media (upgrade) Dell OpenManage Integrations: • Dell OpenManage Integration Suite for Microsoft System Center • Dell OpenManage Integration for VMware® vCenter® Dell OpenManage Connections: • HP Operations Manager, IBM Tivoli® Netcool® and CA Network and Systems Management • Dell OpenManage Plug-in for Oracle® Database Manager
Rack support	All configurations support rackable, except the 3.5" x 4 cabled chassis configuration
Optional supported hypervisors	Citrix® XenServer® VMware vSphere® ESXi™ Red Hat® Enterprise Virtualization
Operating systems	Microsoft® Windows Server® 2008 R2 Microsoft Windows Server 2012 Microsoft Windows Server 2012 R2 Novell® SUSE® Linux Enterprise Server Red Hat Enterprise Linux For more information on specific versions and additions, visit Dell.com/OSsupport.
OEM-ready version	From bezel to BIOS to packaging, your servers can look and feel as if they were designed and built by you. For more information, visit Dell.com/OEM.
Recommended support	Dell ProSupport Plus for critical systems or Dell ProSupport for premium hardware and software support for your PowerEdge solution. Consulting and deployment offerings are also available. Contact your Dell representative today for more information. Availability and terms of Dell Services vary by region. For more information, visit Dell.com/ServiceDescriptions.

End-to-end technology solutions

Reduce IT complexity, lower costs and eliminate inefficiencies by making IT and business solutions work harder for you. You can count on Dell for end-to-end solutions to maximize your performance and uptime. A proven leader in Servers, Storage and Networking, Dell Enterprise Solutions and Services deliver innovation at any scale. And if you're looking to preserve cash or increase operational efficiency, Dell Financial Services™ has a wide range of options to make technology acquisition easy and affordable. Contact your Dell Sales Representative for more information.**

Learn More at Dell.com/PowerEdge.

April 2016 | Version 2.0
Dell_PowerEdge_T430_SpecSheet