



UNIVERSIDAD NACIONAL TECNOLÓGICA DEL  
CONO SUR DE LIMA  
(UNTECS)

**DISEÑO DE RED DE COMUNICACIÓN DE DATOS PARA LA  
INSTITUCIÓN EDUCATIVA PRIVADA EMILIO SOYER CABERO  
UBICADA EN EL DISTRITO DE CHORRILLOS, LIMA, PERÚ**

TRABAJO DE INVESTIGACIÓN PARA OPTAR EL TÍTULO DE  
INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER  
JHASET RAUL ORTEGA CUBAS

LIMA-PERÚ

2014

A mis amados padres, pues  
sin ellos, nada de esto habría  
sido posible

Agradezco a los señores docentes de la Escuela de Ingeniería Electrónica y Telecomunicaciones por dotarnos de las armas necesarias para llegar a ser personas útiles a la sociedad.

## INDICE

<b>INTRODUCCIÓN</b> .....	1
<b>CAPITULO I. PLANTEAMIENTO DEL PROBLEMA</b> .....	2
<b>1.1 DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA</b> .....	2
<b>1.2 JUSTIFICACIÓN DEL PROBLEMA</b> .....	2
<b>1.3 DELIMITACIÓN DE LA INVESTIGACIÓN</b> .....	3
1.3.1 Espacial .....	3
1.3.2 Temporal .....	3
<b>1.4 FORMULACIÓN DEL PROBLEMA</b> .....	3
<b>1.5 OBJETIVO</b> .....	3
<b>CAPITULO II. MARCO TEÓRICO</b> .....	4
<b>2.1 ANTECEDENTES</b> .....	4
<b>2.2 BASES TEÓRICAS</b> .....	6
<b>2.2.1 Red de comunicación de datos</b> .....	6
<b>2.2.1.1 Elementos de una Red de Comunicación de Datos</b> .....	7
<b>2.2.2 Redes de área local (LAN)</b> .....	10
<b>2.2.3 WLAN (Wireless LAN)</b> .....	13
<b>2.2.3.1 ¿Qué es una red inalámbrica?</b> .....	14
<b>2.2.3.2 Diseño de red LAN, antesala de WLAN</b> .....	15
<b>2.2.3.3 Componentes de la red inalámbrica</b> .....	15
<b>2.2.3.4 Seguridad en WLAN</b> .....	16
<b>2.2.4 Virtual LAN (VLAN)</b> .....	16
<b>2.2.5 Arquitectura de red</b> .....	18
<b>2.2.5.1 Tolerancia a fallas</b> .....	19
<b>2.2.5.2 Escalabilidad</b> .....	19
<b>2.2.5.3 Calidad de servicio (QoS)</b> .....	20
<b>2.2.5.4 Seguridad</b> .....	20
<b>2.2.6 Protocolos de comunicación</b> .....	21
<b>2.2.6.1 Reglas que rigen las comunicaciones</b> .....	21
<b>2.2.6.2 Protocolos de red</b> .....	22
<b>2.2.6.3 Suites de protocolos y estándares de la industria</b> .....	22
<b>2.2.6.4 Interacción de los protocolos</b> .....	23
<b>2.2.6.5 Protocolos independientes de la tecnología</b> .....	24

2.2.7 Modelo TCP/IP .....	25
2.2.8 Modelo OSI .....	26
2.2.9 Comparación entre el modelo OSI y el modelo TCP/IP .....	27
<b>2.3 MARCO CONCEPTUAL</b> .....	<b>29</b>
2.3.1 Determinación de términos básicos .....	30
<b>CAPITULO III. DISEÑO DE RED DE COMUNICACIÓN DE DATOS PARA LA INSTITUCIÓN EDUCATIVA PRIVADA EMILIO SOYER CABERO</b> .....	<b>33</b>
<b>3.1 ANALISIS DEL DISEÑO DE RED DE COMUNICACIÓN DE DATOS PARA LA INSTITUCIÓN EDUCATIVA PRIVADA EMILIO SOYER CABERO</b> .....	<b>33</b>
<b>3.2 DISEÑO DE RED DE COMUNICACIÓN DE DATOS PARA LA INSTITUCIÓN EDUCATIVA PRIVADA EMILIO SOYER CABERO</b> .....	<b>34</b>
3.2.1 Análisis y Diagnóstico de la Infraestructura Actual .....	34
3.2.1.1 Detalles de la Infraestructura .....	37
3.2.2 Diseño de la Red de Comunicación de Datos para la Institución Privada Emilio Soyer Cabero .....	42
3.2.2.1 Lo que se hará.....	42
3.2.2.2 Topología de Red .....	45
3.2.2.3 Diseño del Diagrama de Infraestructura Lógica .....	46
3.2.2.4 Diseño del Diagrama de Infraestructura Física .....	64
<b>3.3 REVISIÓN Y CONSOLIDACIÓN DE RESULTADOS</b> .....	<b>92</b>
3.3.1 Topología de la Red a escala en Packet Tracer.....	92
<b>CONCLUSIONES</b> .....	<b>95</b>
<b>RECOMENDACIONES</b> .....	<b>96</b>
<b>BIBLIOGRAFÍA</b> .....	<b>98</b>
<b>ANEXOS</b> .....	<b>99</b>

## **INTRODUCCIÓN**

El presente trabajo de investigación lleva por título “DISEÑO DE RED DE COMUNICACIÓN DE DATOS PARA LA INSTITUCIÓN EDUCATIVA PRIVADA EMILIO SOYER CABERO UBICADA EN EL DISTRITO DE CHORRILLOS, LIMA, PERÚ”, para optar el título de Ingeniero Electrónico y Telecomunicaciones, presentado por el alumno Jhaset Raúl Ortega Cubas.

En primer lugar se aborda la realidad problemática observada relacionada con la importancia y necesidad de diseñar una Red de Comunicación de Datos con el fin de dotar a la Institución Educativa Privada Emilio Soyer Cabero de un sistema de transmisión de información mediante la comunicación de todos los dispositivos de red que ésta maneje para ventaja de los trabajadores, docentes y alumnos.

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

## **CAPITULO I**

### **PLANTEAMIENTO DEL PROBLEMA**

#### **1.1 DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA**

Al ser la Institución Educativa Privada Emilio Soyer Cabero, ubicada en el distrito de Chorrillos, una construcción recientemente terminada, no cuenta con una Red de Comunicación de Datos hecha a la medida y diseñada para cumplir todas las expectativas de una entidad educativa privada. Entonces las autoridades de ésta Institución tienen el deseo y sobre todo la necesidad de poder implementar una infraestructura de Red de Comunicación de Datos en todo el campus y permitir así la comunicación absoluta.

#### **1.2 JUSTIFICACIÓN DEL PROBLEMA**

Debido al hecho de que la institución está a puertas de ser una gran unidad educativa en tamaño y calidad, contando así con muchas oficinas administrativas, oficinas académicas, numerosas aulas de clase, laboratorios de computo, diversos laboratorios de ciencias naturales, una gran biblioteca, un amplio auditorio y diferentes áreas de deporte y esparcimiento, así como un número considerable de alumnado, es necesario contar con un diseño de red de comunicación de datos que pueda converger y funcionar sin ningún problema, el cual permitirá manejar debidamente la información, al mismo tiempo de tener la rapidez necesaria de procesamiento y brindar la posibilidad de que los alumnos puedan siempre estar conectados con el mundo exterior a través de internet,

herramienta que es vital hoy en día. Es por eso que se requiere de una propuesta seria de una Red de Comunicación de Datos hecha a la medida de la institución.

### **1.3 DELIMITACIÓN DE LA INVESTIGACIÓN**

#### **1.3.1 Espacial**

Se realizará en la Institución Educativa Privada Emilio Soyer Cabero ubicada en el distrito de Chorrillos, Lima, Perú.

#### **1.3.2 Temporal**

Comprende el periodo SETIEMBRE 2013 a ENERO 2014

### **1.4 FORMULACIÓN DEL PROBLEMA**

¿De qué manera se podrá diseñar una Red de Comunicación de Datos para la Institución Educativa Privada Emilio Soyer Cabero que sea confiable, escalable y eficaz, logrando así una comunicación fluida, un continuo y buen manejo de información y logrando la conectividad a internet desde muchos lugares del campus educativo?

### **1.5 OBJETIVO**

Desarrollar el diseño de Red de Comunicación de Datos para la Institución Educativa Privada Emilio Soyer Cabero que sea confiable, escalable y eficaz para lograr una comunicación fluida, un continuo y buen manejo de información y lograr la conectividad a internet desde muchos lugares del campus educativo.



## **CAPITULO II**

### **MARCO TEÓRICO**

#### **2.1 ANTECEDENTES**

A lo largo de la investigación, se encontraron varias tesis que sirvieron de ayuda para el presente trabajo, entre ellas están:

CARLOS L. (2006) “Diseño de la Red LAN Colegio Liceo Pedagógico”. Este estudio surge porque el colegio liceo pedagógico tenía 2 laboratorios de sistemas con 40 ordenadores, 2 impresoras en cada sala, en el tercer y cuarto piso se requería de la implementación de una red LAN para su correcto uso ya que se maneja necesita que un administrador maneje o dos las salas y se cumplan con sus correctas funciones. Las redes debían tener disponibilidad de Internet pero sea restringido su uso como Chat, observar fotografía pornográfica, material satánico. Tras el diseño se concluyó que la red necesita tanto elementos de hardware como de software ya que permiten un complemento y si están bien diseñadas o implementadas no permitirá caídas o posibles intrusos en la red para ello debe haber un buen ingeniero de redes a cargo.

MOLINS R. (2012). “Diseño e Implementación de la Red de Telecomunicaciones en un Centro Escolar”. Este proyecto surge a causa de que en entonces la actual sede del colegio se disponía de una infraestructura de red precaria que imposibilitaba la configuración que deseaba el cliente. El problema residía en un cableado antiguo y unos componentes no configurables los cuales limitaban la seguridad de la red, además de la antigüedad de estos que producía

cuellos de botella en la red. Con la construcción de la nueva sede se realizaría una nueva infraestructura de red que solucionaría la problemática, consiguiendo notables mejoras en la velocidad y seguridad de la red. Finalizado el proyecto se concluyó que uno de los pilares del sistema informático de una empresa es la estructura de su red, y con la configuración planteada la nueva sede del Colegio Cumbres estará dotada de una infraestructura de red acorde a sus necesidades, con una velocidad y seguridad garantizadas.

ANATO J. (2006). "Modelo de una Red de Datos bajo Tecnología PLC para el Departamento de Computación y Sistemas de la Universidad de Oriente, Núcleo Anzoátegui". La problemática planteada en este estudio es que en el Departamento de computación y sistemas la calidad y rendimiento de los equipos instalados es deficiente, el ancho de banda presente es reducido y hay presencia de fallas en la transmisión. Es por eso que se propone esta tesis que consiste en la creación de una Red de Datos bajo tecnología PLC (Comunicación a través de líneas eléctricas).

MAYATTIS M. y MARTÍNEZ JOSÉ A. (2007). "Diseño de una Red de Datos bajo tecnología PLC para el edificio Decanato de la Universidad de Oriente - núcleo Anzoátegui". El estudio fue realizado debido a la problemática presentada por la red del Decanato de la Universidad debido a la obsolescencia de los equipos que sirven de embudo para disminuir la velocidad de la red. Es por ello que presentan un modelo aplicando la metodología de diseño estructurado de redes establecidas por la academia Cisco Networking para la arquitectura de red que permita ofrecer un servicio de comunicación eficaz y confiable.

## 2.2 BASES TEÓRICAS

### 2.2.1 Red de comunicación de datos

Una red de comunicación de datos es básicamente un conjunto o sistema de equipos informáticos conectados entre sí, por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos con la finalidad de compartir información y recursos y ofrecer servicios.

Por lo general, estas redes se basan en la conmutación de paquetes. Pueden clasificarse de distintas maneras de acuerdo a la arquitectura física, el tamaño y la distancia cubierta pero todas las redes tienen cuatro elementos básicos en común:

- Reglas y acuerdos para regular cómo se envían, se direccionan, reciben e interpretan los mensajes,
- Los mensajes o unidades de información que viajan de un dispositivo a otro, una forma de interconectar esos dispositivos, un medio que puede transportar los mensajes de un dispositivo a otro, y
- Los dispositivos de la red que cambian mensajes entre sí.

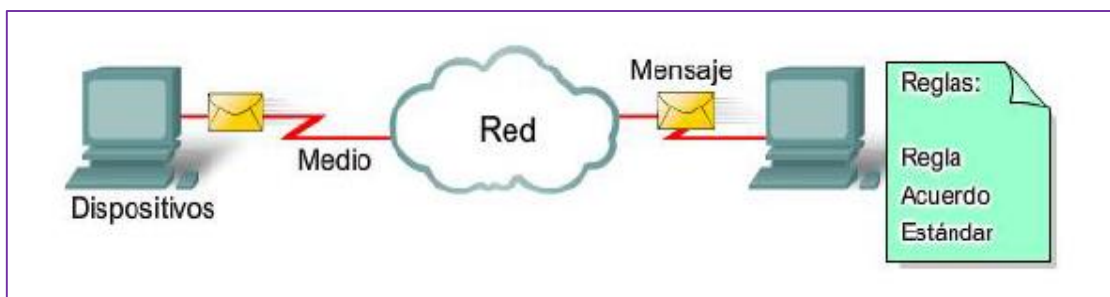


FIGURA 2.1 “Elementos Básicos de una Red de Comunicaciones” Fuente: CISCO

La estandarización de los distintos elementos de la red permite el funcionamiento conjunto de equipos y dispositivos creados por diferentes compañías. Los expertos en diversas tecnologías pueden contribuir con las

mejores ideas para desarrollar una red eficiente sin tener en cuenta la marca o el fabricante del equipo.

### 2.2.1.1 Elementos de una Red de Comunicación de Datos

En la FIGURA 2.2 se muestran los elementos de una red típica, incluyendo dispositivos, medios y servicios unidos por reglas, que trabajan en forma conjunta para enviar mensajes. Utilizamos la palabra mensajes como un término que abarca las páginas Web, los e-mails, los mensajes instantáneos, las llamadas telefónicas y otras formas de comunicación permitidas por Internet.

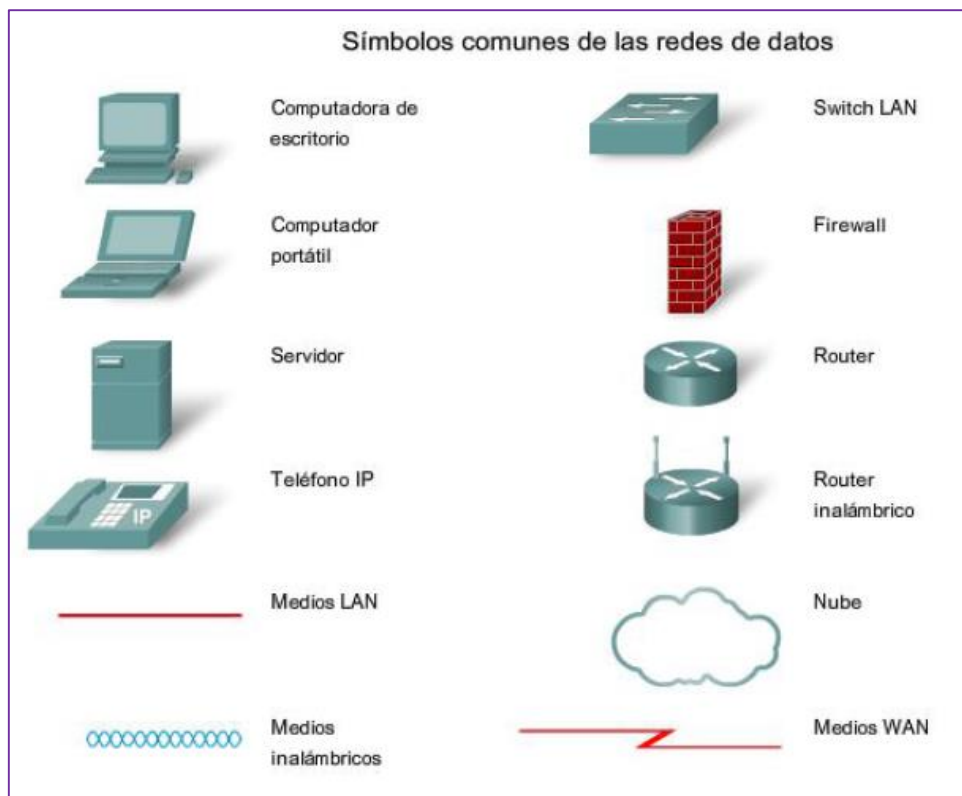


FIGURA 2.2 "Símbolos Comunes de las Redes de Datos". Fuente: CISCO

El lado derecho de la figura muestra algunos de los dispositivos intermedios más comunes, utilizados para direccionar y administrar los mensajes en la red, como así también otros símbolos comunes de interconexión de redes. Los símbolos genéricos se muestran para:

- Switch: el dispositivo más utilizado para interconectar redes de área local,
- Firewall: proporciona seguridad a las redes,
- Router: ayuda a direccionar mensajes mientras viajan a través de una red,
- Router inalámbrico: un tipo específico de router que generalmente se encuentra en redes domésticas,
- Nube: se utiliza para resumir un grupo de dispositivos de red.

Para que funcione una red de comunicación de datos, los dispositivos deben estar interconectados. Las conexiones de red pueden ser con cables o inalámbricas. En las conexiones con cables, el medio puede ser cobre, que transmite señales eléctricas, o fibra óptica, que transmite señales de luz. En las conexiones inalámbricas, el medio es la atmósfera de la tierra o espacio y las señales son microondas. Los medios de cobre incluyen cables, como el par trenzado del cable de teléfono, el cable coaxial o generalmente conocido como cable de par trenzado no blindado (UTP) de Categoría 5. Las fibras ópticas, hebras finas de vidrio o plástico que transmiten señales de luz, son otra forma de medios de Networking. Los medios inalámbricos incluyen conexiones inalámbricas domésticas entre un router inalámbrico y una computadora con una tarjeta de red inalámbrica, conexión inalámbrica terrestre entre dos estaciones de tierra o comunicación entre dispositivos en tierra y satélites. En un viaje típico a través de Internet, un mensaje puede viajar en una variedad de medios.

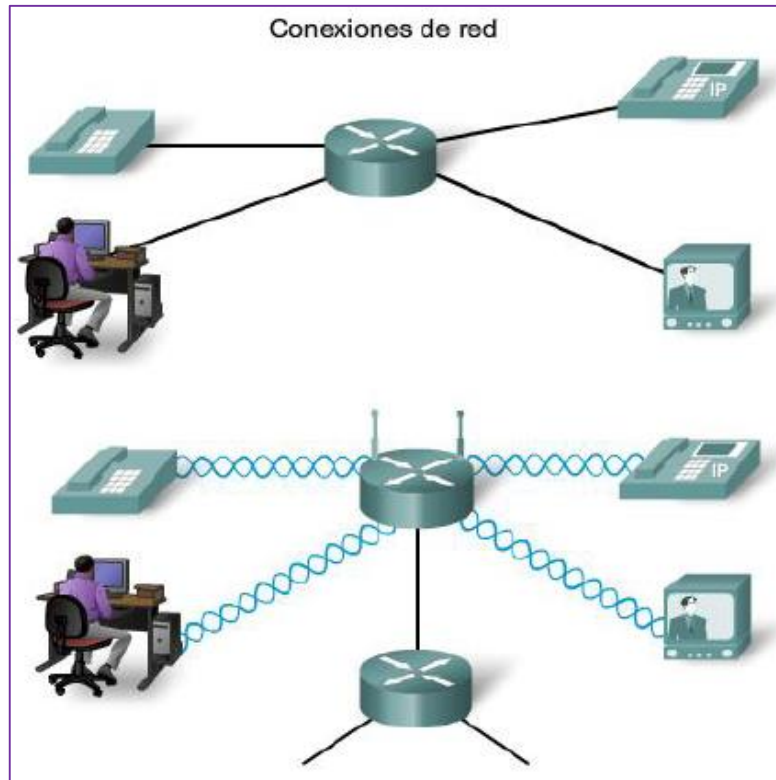


FIGURA 2.3 “Conexiones en las Redes de Comunicación de Datos”. Fuente: CISCO

Las personas generalmente buscan enviar y recibir distintos tipos de mensajes a través de aplicaciones informáticas; estas aplicaciones necesitan servicios para funcionar en la red. Algunos de estos servicios incluyen World Wide Web, email, mensajería instantánea y telefonía IP. Los dispositivos interconectados a través de medios para proporcionar servicios deben estar gobernados por reglas o protocolos. En el cuadro se enumeran algunos servicios y un protocolo vinculado en forma más directa con ese servicio.

Los protocolos son las reglas que utilizan los dispositivos de red para comunicarse entre sí. Actualmente el estándar de la industria en redes es un conjunto de protocolos denominado TCP/IP (Protocolo de control de transmisión/Protocolo de Internet). TCP/IP se utiliza en redes comerciales y domésticas, siendo también el protocolo primario de Internet. Son los protocolos TCP/IP los que especifican los mecanismos de formateo, de direccionamiento y de enrutamiento que garantizan que nuestros mensajes sean entregados a los destinatarios correctos.

Servicio	Protocolo ("Regla")
World Wide Web (WWW)	HTTP (Hypertext Transport Protocol)
E-mail	SMTP (Simple Mail Transport Protocol) POP (Post Office Protocol)
Mensaje instantáneo (Jabber; AIM)	XMPP (Extensible Messaging and Presence Protocol) OSCAR (Sistema abierto para la comunicación en tiempo real)
Telefonía IP	SIP (Session Initiation Protocol)

TABLA 2.1 "Servicios y Protocolos en las Redes de Comunicación de Datos". Fuente: CISCO

## 2.2.2 Redes de área local (LAN)

Son redes ubicadas en un área restringida, cuya propiedad es privada; pueden estar situadas en una oficina o en el edificio de la empresa. Las hogareñas también se consideran LAN siempre y cuando tengan, al menos, dos computadoras.

Para que una PC pueda tener acceso a la red, debe poseer una tarjeta de red (NIC). Los componentes de una LAN pueden ser: computadoras, servidores e impresoras, entre otros.

Los medios utilizados para conectarlas son los cables y/o el aire (el más común es el sistema WiFi, a través de un Access Point), y los dispositivos de enlace (Networking): hub, switch o router. Recordemos que estos componentes se explicarán con profundidad a lo largo de toda la obra.

La infraestructura varía según el tamaño del área por cubrir, la cantidad de usuarios que se pueden conectar, y el número y los tipos de servicios disponibles. Las características clave de las redes de área local para tener en cuenta son:

- a. Permiten impulsar tecnologías para compartir localmente archivos y hardware de manera eficiente y, así, permitir las comunicaciones internas.
- b. Son redes de propiedad privada, por ejemplo, una red hogareña, una oficina, una empresa o una pyme, entre otras.
- c. Se usan para conectar computadoras personales, con el objeto de compartir recursos e intercambiar información, y así facilitar el trabajo.
- d. Están restringidas en tamaño.
- e. Suelen emplear tecnología Ethernet (broadcast) mediante un cable sencillo (por ejemplo, UTP), a través del cual todas las computadoras se conectan a un nodo central (hub o switch).

Normalmente, las redes locales operan a velocidades que se encuentran entre 10 y 100 Mbps (megabits por segundo). En la actualidad, se manejan velocidades superiores, que van desde 1 Gb hasta 10 Gb, aunque estas últimas aún no se aplican en forma masiva; se planea su implementación a medida que aumente el tráfico de datos con el agregado de voz y video. Las redes de área local se destacan por tener bajo retardo y generar mínimos márgenes de error.

Los requerimientos que tienen hoy las redes LAN, de acuerdo con la demanda y las necesidades cotidianas, son:

- a. Escalabilidad: La red LAN debe poder absorber el crecimiento futuro, sobre la nueva red que se cree. Este detalle resulta clave, dado que una red no siempre se arma desde cero, sino que se pueden realizar mejoras sobre las ya implementadas.
- b. Administración: Es un término poco aplicado; sin embargo, las redes deben ser administradas a través de programas o de aplicaciones que permitan relevar los problemas surgidos a diario, analizarlos y darles una solución.



c. Costo-beneficio: Es un tema no menor, dado que siempre que se impulsa una nueva red o una modificación de la actual, debe primar este aspecto.

d. Alta disponibilidad: La red debe estar siempre operativa. Un factor importante para que esto suceda es contar con ambientes redundantes, tanto en las conexiones como en los dispositivos.

e. Servicios: La red debe tener la capacidad de soportar diferentes tipos de tráfico, como datos, voz y video, por lo que se requiere QoS (calidad de servicio). También exige ambientes con desarrollo de multicast (multidifusión de datos entre usuario) y, en especial, que sea segura, con buenas prácticas de resguardo.

f. Multiprotocolo: La red debe tener capacidad a través de los dispositivos de Networking y permitir el trabajo en ambientes cerrados, con protocolos propietarios, como también en ambientes con estándares, bajo normas comunes, para diferentes fabricantes.

g. Movilidad: Las redes actuales, por el continuo movimiento de las personas que conforman una empresa, deben tener la capacidad de implementar tecnología Wireless. Para cubrir las necesidades de todos los usuarios, hay que prestar atención a la convergencia de múltiples servicios, a la mayor movilidad de los usuarios, al aumento en las velocidades de conexión y a un mayor número de parámetros de seguridad ante nuevos peligros emergentes.

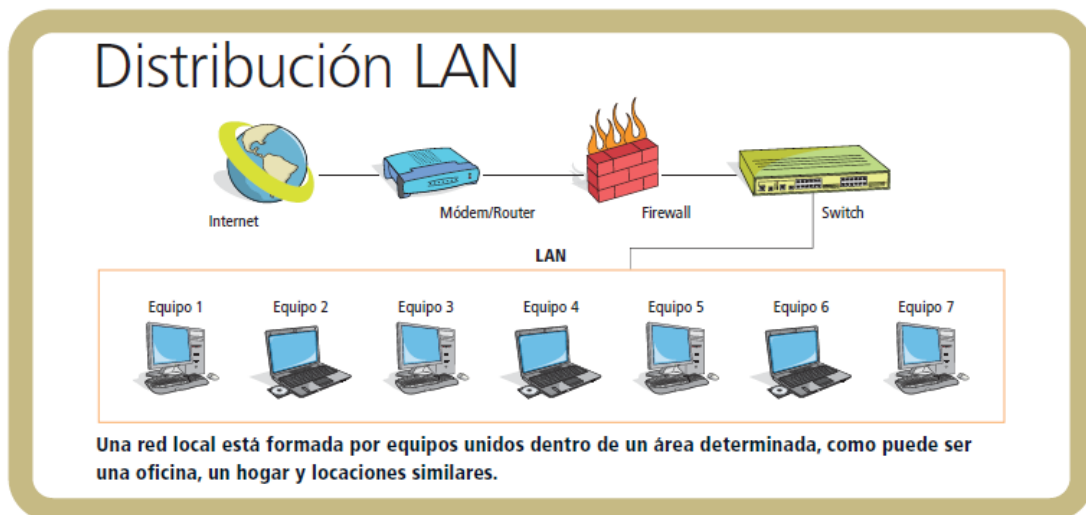


FIGURA 2.4 "Distribución LAN". Fuente: CISCO

### 2.2.3 WLAN (Wireless LAN)

En las empresas, los usuarios se conectan a la red de área local para acceder a Internet, a su correo electrónico, a servicios online o bien a la información compartida. Con la aparición de las redes inalámbricas, los usuarios pueden acceder a los mismos servicios de red sin tener que buscar algún lugar para conectarse físicamente. Al mismo tiempo, tanto las empresas como el usuario doméstico pueden configurar o ampliar su red sin pensar por dónde pasar los cables. Las redes inalámbricas ofrecen ventajas importantes con respecto a las cableadas, como por ejemplo:

- a. Mayor movilidad. Hoy en día, son cada vez más las funciones inalámbricas que se incorporan en los diferentes equipos, como palmtops, agendas, PDAs y teléfonos. Al conectarlos por medios inalámbricos a la red de la empresa, estos equipos serán herramientas fundamentales para la productividad de los empleados que no siempre trabajan en sus escritorios.
- b. Aumento en la productividad. Mediante una conexión inalámbrica, los empleados pueden trabajar desde cualquier lugar que se encuentre dentro del alcance de un Access Point (Punto de acceso), y llegar a sus aplicaciones y a

los datos basados en la red. Por este motivo, pueden mantenerse conectado desde cualquier parte y maximizar su productividad.

### **2.2.3.1 ¿Qué es una red inalámbrica?**

Una WLAN es una red de área local, pero inalámbrica; consiste en un sistema de comunicación de datos que los transmite y recibe a través del aire utilizando tecnología de radio. Las WLAN se utilizan en entornos tanto empresariales como privados, bien como extensiones de las redes existentes o en entornos de pequeñas empresas, o como una alternativa a las redes de cable. Las WLAN proporcionan todas las ventajas y características de las tecnologías de las redes de área local (LAN), sin las limitaciones que imponen los cables.

Las WLAN redefinen la forma de ver las LAN. La conectividad ya no implica una conexión física. Los usuarios pueden seguir conectados a la red mientras se desplazan por las diferentes áreas de una compañía. Con las WLAN, la infraestructura de red se puede desplazar y modificar a la misma velocidad que crece la empresa. Veamos algunos ejemplos clásicos de aplicación de la tecnología:

- a. En empresas pequeñas, las WLAN pueden ser una alternativa a las LAN con cable. Las WLAN son fáciles de instalar y ofrecen un alto grado de flexibilidad, lo que facilita el crecimiento de las empresas.
- b. En empresas medianas, las WLAN se pueden utilizar para ofrecer acceso en las salas de reuniones y en las áreas comunes. También proporcionan a los usuarios acceso en las zonas que se utilizan menos.
- c. En empresas grandes, las WLAN pueden proporcionar una red superpuesta que favorece la movilidad, con el fin de que los usuarios tengan acceso a la información que necesiten desde cualquier lugar del edificio.

### **2.2.3.2 Diseño de red LAN, antesala de WLAN**

En las redes LAN tradicionales que se utilizan en la actualidad, las computadoras de escritorio o las portátiles suelen estar conectadas a un hub o bien a un switch de LAN por medio de cables. A través de estos concentradores, los dispositivos tienen acceso a los datos compartidos, a las aplicaciones que se encuentran en los servidores o a través de un router, salen a Internet. Ésta es la visión más sencilla de una LAN.

El entorno de una WLAN es muy similar. En la topología de este ejemplo, se inserta un dispositivo llamado punto de acceso (Access Point, a partir de ahora denominado AP), que actúa como punto central y como punto de conexión entre la red con cables y la inalámbrica. El AP se encarga del tráfico de los usuarios, también llamados clientes inalámbricos, en sus áreas de cobertura. Recibe, almacena en la memoria intermedia y transmite datos entre la WLAN y la red con cable. Un solo AP puede admitir un pequeño grupo de usuarios y funcionar dentro de un alcance menor a los 100 metros. Para ampliar la conectividad inalámbrica, es posible disponer varios AP, con el fin de que sus áreas de cobertura sean adyacentes. Los usuarios finales acceden a la WLAN a través de las tarjetas de WLAN, que se implementan en las computadoras de escritorio y en las portátiles, igual que las tarjetas de red tradicionales.

### **2.2.3.3 Componentes de la red inalámbrica**

Vamos a centrarnos en cuatro componentes de la red inalámbrica:

a. Los Access Points proporcionan enlaces inteligentes entre redes inalámbricas y con cable, y actúan como conexión entre la WLAN y la LAN con cables. Los AP interiores del edificio pueden intercambiar el alcance por la velocidad, y viceversa. Por ejemplo, en interiores, un AP puede tener una velocidad de 11 Mbps con un enlace de hasta 40 metros o 1 Mbps con un enlace de 100 metros.

b. Las tarjetas WiFi existen tanto para equipos portátiles, como para PCs y servidores. Estos adaptadores tienen una antena integrada que envía y recibe ondas de radio.

#### **2.2.3.4 Seguridad en WLAN**

A muchas empresas les preocupa que las WLAN no ofrezcan el mismo nivel de seguridad que las LAN tradicionales. Hay quienes temen que las señales de las transmisiones por WLAN se puedan interceptar. Queremos enfatizar que cualquier red, con cables o inalámbricas, puede estar sujeta a riesgos de seguridad. Por lo tanto, todas las empresas deben adoptar una estrategia global de protección de la red.

Hoy en día, la tecnología WLAN cuenta con varios mecanismos para aumentar el nivel de seguridad de la propia comunicación inalámbrica.

En general, las provisiones de seguridad suelen estar integradas en las WLAN, pero pueden y deben mejorarse con otros mecanismos de seguridad. Estas redes tienen la capacidad de cifrar y descifrar las señales de datos transmitidas entre los dispositivos. También poseen conexiones tan seguras como las LAN tradicionales. Hoy es difícil, no imposible, escuchar el tráfico de las WLAN, ya que las complejas técnicas de cifrado que utiliza la tecnología inalámbrica hacen que sea muy difícil que cualquiera pueda acceder al tráfico de la red, si no tiene autorización para ello.

#### **2.2.4 Virtual LAN (VLAN)**

Una VLAN (acrónimo de virtual LAN, «red de área local virtual») es un método para crear redes lógicas independientes dentro de una misma red física.<sup>1</sup> Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar

datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4).

Una VLAN consiste en dos redes de ordenadores que se comportan como si estuviesen borrachos conectados al mismo PCI, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente fáciles. Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente algún ordenador a otra ubicación y este puede permanecer en la misma VLAN sin necesidad de cambiar la configuración de la máscara de subred vertical.

Durante todo el proceso de configuración y funcionamiento de una VLAN es necesaria la participación de una serie de protocolos entre los que destacan el IEEE 802.1Q, STP y VTP (cuyo equivalente IEEE es GVRP). El protocolo IEEE 802.1Q se encarga del etiquetado de las tramas que es asociada inmediatamente con la información de la VLAN. El cometido principal de Spanning Tree Protocol (STP) es evitar la aparición de bucles lógicos para que haya un sólo camino entre dos nodos. VTP (VLAN Trunking Protocol) es un protocolo propietario de Cisco que permite una gestión centralizada de todas las VLANs.

El protocolo de etiquetado IEEE 802.1Q es el más común para el etiquetado de las VLAN. Antes de su introducción existían varios protocolos propietarios, como el ISL (Inter-Switch Link) de Cisco, una variante del IEEE 802.1Q, y el VLT (Virtual LAN Trunk) de 3Com. El IEEE 802.1Q se caracteriza por utilizar un formato de trama similar a 802.3 (Ethernet) donde sólo cambia el valor del campo Ethertype, que en las tramas 802.1Q vale X'8100, y se añaden dos bytes para codificar la prioridad, el CFI y el VLAN ID. Este protocolo es un estándar internacional y por lo dicho anteriormente es compatible con bridges y switches sin capacidad de VLAN.

Para evitar el bloqueo de los switches debido a las tormentas broadcast, una red con topología redundante tiene que tener habilitado el protocolo STP. Los switches utilizan STP para intercambiar mensajes entre sí (BPDUs, Bridge Protocol Data Units) para lograr que en cada VLAN sólo haya activo un camino para ir de un nodo a otro.

En los dispositivos Cisco, VTP (VLAN Trunking Protocol) se encarga de mantener la coherencia de la configuración VLAN por toda la red. VTP utiliza tramas de nivel 2 para gestionar la creación, borrado y renombrado de VLANs en una red sincronizando todos los dispositivos entre sí y evitar tener que configurarlos uno a uno. Para eso hay que establecer primero un dominio de administración VTP. Un dominio VTP para una red es un conjunto contiguo de switches unidos con enlaces trunk que tienen el mismo nombre de dominio VTP.

Los switches pueden estar en uno de los siguientes modos: servidor, cliente o transparente. El servidor es el modo por defecto, anuncia su configuración al resto de equipos y se sincroniza con otros servidores VTP. Un switch cliente no puede modificar la configuración VLAN, simplemente sincroniza la configuración en base a la información que le envían los servidores. Por último, un switch está en modo transparente cuando sólo se puede configurar localmente pues ignora el contenido de los mensajes VTP.

VTP también permite «podar» (función VTP pruning), lo que significa dirigir tráfico VLAN específico sólo a los conmutadores que tienen puertos en la VLAN destino. Con lo que se ahorra ancho de banda en los posiblemente saturados enlaces trunk.

### **2.2.5 Arquitectura de red**

Las redes deben admitir una amplia variedad de aplicaciones y servicios, como así también funcionar con diferentes tipos de infraestructuras físicas. El término arquitectura de red, en este contexto, se refiere a las tecnologías que admiten la infraestructura y a los servicios y protocolos programados que pueden trasladar

los mensajes en toda esa infraestructura. Debido a que Internet evoluciona, al igual que las redes en general, descubrimos que existen cuatro características básicas que la arquitectura subyacente necesita para cumplir con las expectativas de los usuarios: tolerancia a fallas, escalabilidad, calidad del servicio y seguridad.

#### **2.2.5.1 Tolerancia a fallas**

La expectativa de que Internet está siempre disponible para millones de usuarios que confían en ella requiere de una arquitectura de red diseñada y creada con tolerancia a fallas. Una red tolerante a fallas es la que limita el impacto de una falla del software o hardware y puede recuperarse rápidamente cuando se produce dicha falla. Estas redes dependen de enlaces o rutas redundantes entre el origen y el destino del mensaje. Si un enlace o ruta falla, los procesos garantizan que los mensajes pueden enrutarse en forma instantánea en un enlace diferente transparente para los usuarios en cada extremo. Tanto las infraestructuras físicas como los procesos lógicos que direccionan los mensajes a través de la red están diseñados para adaptarse a esta redundancia. Ésta es la premisa básica de la arquitectura de redes actuales.

#### **2.2.5.2 Escalabilidad**

Una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio enviado a los usuarios actuales. Miles de nuevos usuarios y proveedores de servicio se conectan a Internet cada semana. La capacidad de la red de admitir estas nuevas interconexiones depende de un diseño jerárquico en capas para la infraestructura física subyacente y la arquitectura lógica. El funcionamiento de cada capa permite a los usuarios y proveedores de servicios insertarse sin causar interrupción en toda la red. Los desarrollos tecnológicos aumentan constantemente las capacidades de transmitir el mensaje y el rendimiento de los componentes de la estructura física en cada capa. Estos desarrollos, junto con los nuevos métodos para identificar y localizar usuarios individuales dentro de



una internetwork, están permitiendo a Internet mantenerse al ritmo de la demanda de los usuarios.

### **2.2.5.3 Calidad de servicio (QoS)**

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

### **2.2.5.4 Seguridad**

Internet evolucionó de una internetwork de organizaciones gubernamentales y educativas estrechamente controlada a un medio ampliamente accesible para la transmisión de comunicaciones personales y empresariales. Como resultado, cambiaron los requerimientos de seguridad de la red. Las expectativas de privacidad y seguridad que se originan del uso de internetworks para intercambiar información empresarial crítica y confidencial exceden lo que puede enviar la arquitectura actual. La rápida expansión de las áreas de comunicación que no eran atendidas por las redes de datos tradicionales aumenta la necesidad de incorporar seguridad en la arquitectura de red. Como resultado, se está dedicando un gran esfuerzo a esta área de investigación y desarrollo. Mientras tanto, se están implementando muchas herramientas y procedimientos para combatir los defectos de seguridad inherentes en la arquitectura de red.

## **2.2.6 Protocolos de comunicación**

### **2.2.6.1 Reglas que rigen las comunicaciones**

Toda comunicación, ya sea cara a cara o por una red, está regida por reglas predeterminadas denominadas protocolos.

Estos protocolos son específicos de las características de la conversación. En nuestras comunicaciones personales cotidianas, las reglas que utilizamos para comunicarnos a través de un medio, como el teléfono, no necesariamente son las mismas que los protocolos que se usan en otro medio, como escribir una carta.

Piense cuántas reglas o protocolos diferentes rigen los distintos métodos de comunicación que existen actualmente en el mundo.

La comunicación exitosa entre los hosts de una red requiere la interacción de gran cantidad de protocolos diferentes. Un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación se denomina suite de protocolos. Estos protocolos se implementan en el software y hardware que está cargado en cada host y dispositivo de red.

Una de las mejores maneras de visualizar de qué manera todos los protocolos interactúan en un host en particular es verlo como un stack. Una stack de protocolos muestra cómo los protocolos individuales de una suite se implementan en el host. Los protocolos se muestran como una jerarquía en capas, donde cada servicio de nivel superior depende de la funcionalidad definida por los protocolos que se muestran en los niveles inferiores. Las capas inferiores del stack competen a los movimientos de datos por la red y a la provisión de servicios a las capas superiores, concentrados en el contenido del mensaje que se está enviando y en la interfaz del usuario.

### **2.2.6.2 Protocolos de red**

A nivel humano, algunas reglas de comunicación son formales y otras simplemente sobreentendidas o implícitas basadas en los usos y costumbres.

Para que los dispositivos se puedan comunicar en forma exitosa, una nueva suite de protocolos debe describir los requerimientos e interacciones precisos.

Las suites de protocolos de Networking describen procesos como los siguientes:

- El formato o estructura del mensaje.
- El método por el cual los dispositivos de Networking comparten información sobre rutas con otras redes,
- Cómo y cuándo se pasan los mensajes de error y del sistema entre dispositivos, o
- El inicio y terminación de las sesiones de transferencia de datos.

Los protocolos individuales de una suite de protocolos pueden ser específicos de un fabricante o de propiedad exclusiva.

Propietario, en este contexto, significa que una compañía o proveedor controla la definición del protocolo y cómo funciona. Algunos protocolos propietarios pueden ser utilizados por distintas organizaciones con permiso del propietario. Otros, sólo se pueden implementar en equipos fabricados por el proveedor propietario.

### **2.2.6.3 Suites de protocolos y estándares de la industria**

Con frecuencia, muchos de los protocolos que comprenden una suite de protocolos aluden a otros protocolos ampliamente utilizados o a estándares de la industria. Un estándar es un proceso o protocolo que ha sido avalado por la

industria de Networking y ratificado por una organización de estándares, como el Instituto de ingenieros eléctricos y electrónicos (IEEE, Institute of Electrical and Electronics Engineers) o el Grupo de trabajo de ingeniería de Internet (IETF).

El uso de estándares en el desarrollo e implementación de protocolos asegura que los productos de diferentes fabricantes puedan funcionar conjuntamente para lograr comunicaciones eficientes. Si un protocolo no es observado estrictamente por un fabricante en particular, es posible que sus equipos o software no puedan comunicarse satisfactoriamente con productos hechos por otros fabricantes.

En las comunicaciones de datos, por ejemplo, si un extremo de una conversación utiliza un protocolo para regir una comunicación unidireccional y el otro extremo adopta un protocolo que describe una comunicación bidireccional, es muy probable que no pueda intercambiarse ninguna información.

#### **2.2.6.4 Interacción de los protocolos**

Un ejemplo del uso de una suite de protocolos en comunicaciones de red es la interacción entre un servidor Web y un explorador Web. Esta interacción utiliza una cantidad de protocolos y estándares en el proceso de intercambio de información entre ellos. Los distintos protocolos trabajan en conjunto para asegurar que ambas partes reciben y entienden los mensajes. Algunos ejemplos de estos protocolos son:

a. Protocolo de aplicación: Protocolo de transferencia de hipertexto (HTTP) es un protocolo común que regula la forma en que interactúan un servidor Web y un cliente Web. HTTP define el contenido y el formato de las solicitudes y respuestas intercambiadas entre el cliente y el servidor. Tanto el cliente como el software del servidor Web implementan el HTTP como parte de la aplicación. El protocolo HTTP se basa en otros protocolos para regir de qué manera se transportan los mensajes entre el cliente y el servidor

b. Protocolo de transporte: Protocolo de control de transmisión (TCP) es el protocolo de transporte que administra las conversaciones individuales entre servidores Web y clientes Web. TCP divide los mensajes HTTP en pequeñas partes, denominadas segmentos, para enviarlas al cliente de destino. También es responsable de controlar el tamaño y los intervalos a los que se intercambian los mensajes entre el servidor y el cliente.

c. Protocolo de internetwork: El protocolo internetwork más común es el Protocolo de Internet (IP). IP es responsable de tomar los segmentos formateados del TCP, encapsularlos en paquetes, asignarles las direcciones correctas y seleccionar la mejor ruta hacia el host de destino.

d. Protocolos de acceso a la red: Estos protocolos describen dos funciones principales: administración de enlace de datos y transmisión física de datos en los medios. Los protocolos de administración de enlace de datos toman los paquetes IP y los formatean para transmitirlos por los medios. Los estándares y protocolos de los medios físicos rigen de qué manera se envían las señales por los medios y cómo las interpretan los clientes que las reciben. Los transceptores de las tarjetas de interfaz de red implementan los estándares apropiados para los medios que se utilizan.

#### **2.2.6.5 Protocolos independientes de la tecnología**

Los protocolos de red describen las funciones que se producen durante las comunicaciones de red. En el ejemplo de la conversación cara a cara, es posible que un protocolo para comunicar establezca que para indicar que la conversación ha finalizado, el emisor debe permanecer en silencio durante dos segundos completos. Sin embargo, este protocolo no especifica cómo el emisor debe permanecer en silencio durante los dos segundos.

Los protocolos generalmente no describen cómo cumplir una función en particular. Al describir solamente qué funciones se requieren de una regla de comunicación en particular pero no cómo realizarlas, es posible que la implementación de un protocolo en particular sea independiente de la tecnología.

En el ejemplo del servidor Web, HTTP no especifica qué lenguaje de programación se utiliza para crear el explorador, qué software de servidor Web se debe utilizar para servir las páginas Web, sobre qué sistema operativo se ejecuta el software o los requisitos necesarios para mostrar el explorador. Tampoco describe cómo detecta errores el servidor, aunque sí describe qué hace el servidor si se produce un error.

Esto significa que una computadora y otros dispositivos, como teléfonos móviles o PDA, pueden acceder a una página Web almacenada en cualquier tipo de servidor Web que utilice cualquier tipo de sistema operativo desde cualquier lugar de Internet.

### **2.2.7 Modelo TCP/IP**

El primer modelo de protocolo en capas para comunicaciones de internet se creó a principios de la década de los setenta y se conoce con el nombre de modelo de Internet. Define cuatro categorías de funciones que deben tener lugar para que las comunicaciones sean exitosas. La arquitectura de la suite de protocolos TCP/IP sigue la estructura de este modelo. Por esto, es común que al modelo de Internet se lo conozca como modelo TCP/IP.

La mayoría de los modelos de protocolos describen un stack de protocolos específicos del proveedor. Sin embargo, puesto que el modelo TCP/IP es un estándar abierto, una compañía no controla la definición del modelo. Las definiciones del estándar y los protocolos TCP/IP se explican en un foro público y se definen en un conjunto de documentos disponibles al público. Estos documentos se denominan Solicitudes de comentarios (RFCs). Contienen las especificaciones formales de los protocolos de comunicación de datos y los recursos que describen el uso de los protocolos.

Las RFC (Solicitudes de comentarios) también contienen documentos técnicos y organizacionales sobre Internet, incluyendo las especificaciones

técnicas y los documentos de las políticas producidos por el Grupo de trabajo de ingeniería de Internet (IETF).

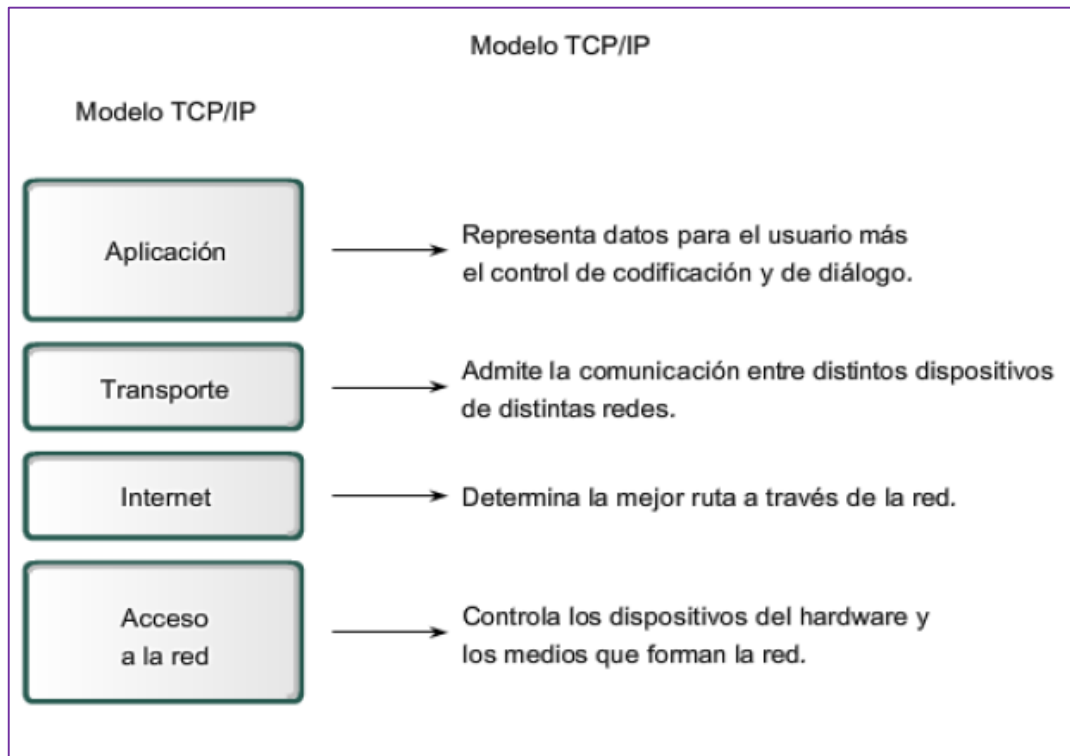


FIGURA 2.5 "Modelo TCP/IP". Fuente: CISCO

### 2.2.8 Modelo OSI

Inicialmente, el modelo OSI fue diseñado por la Organización Internacional para la Estandarización (ISO, International Organization for Standardization) para proporcionar un marco sobre el cual crear una suite de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizara para desarrollar una red internacional que no dependiera de sistemas propietarios.

Lamentablemente, la velocidad a la que fue adoptada la Internet basada en TCP/IP y la proporción en la que se expandió ocasionaron que el desarrollo y la aceptación de la suite de protocolos OSI quedaran atrás. Aunque pocos de los protocolos desarrollados mediante las especificaciones OSI son de uso masivo en la actualidad, el modelo OSI de siete capas ha realizado aportes importantes

para el desarrollo de otros protocolos y productos para todos los tipos de nuevas redes.

Como modelo de referencia, el modelo OSI proporciona una amplia lista de funciones y servicios que pueden producirse en cada capa. También describe la interacción de cada capa con las capas directamente por encima y por debajo de él.



FIGURA 2.6 “Niveles del Modelo OSI”. Fuente: CISCO

### 2.2.9 Comparación entre el modelo OSI y el modelo TCP/IP

Los protocolos que forman la suite de protocolos TCP/IP pueden describirse en términos del modelo de referencia OSI.

En el modelo OSI, la capa Acceso a la red y la capa Aplicación del modelo TCP/IP están subdivididas para describir funciones discretas que deben producirse en estas capas.



En la capa Acceso a la red, la suite de protocolos TCP/IP no especifica cuáles protocolos utilizar cuando se transmite por un medio físico; sólo describe la transferencia desde la capa de Internet a los protocolos de red física. Las Capas OSI 1 y 2 analizan los procedimientos necesarios para tener acceso a los medios y los medios físicos para enviar datos por una red.

Los paralelos clave entre dos modelos de red se producen en las Capas 3 y 4 del modelo OSI. La Capa 3 del modelo OSI, la capa Red, se utiliza casi universalmente para analizar y documentar el rango de los procesos que se producen en todas las redes de datos para direccionar y enrutar mensajes a través de una internetwork. El Protocolo de Internet (IP) es el protocolo de la suite TCP/IP que incluye la funcionalidad descrita en la Capa 3.

La Capa 4, la capa Transporte del modelo OSI, con frecuencia se utiliza para describir servicios o funciones generales que administran conversaciones individuales entre los hosts de origen y de destino. Estas funciones incluyen acuse de recibo, recuperación de errores y secuenciamiento. En esta capa, los protocolos TCP/IP, Protocolo de control de transmisión (TCP) y Protocolo de datagramas de usuario (UDP) proporcionan la funcionalidad necesaria.

La capa de aplicación TCP/IP incluye una cantidad de protocolos que proporcionan funcionalidad específica para una variedad de aplicaciones de usuario final. Las Capas 5, 6 y 7 del modelo OSI se utilizan como referencias para proveedores y programadores de software de aplicación para fabricar productos que necesitan acceder a las redes para establecer comunicaciones.

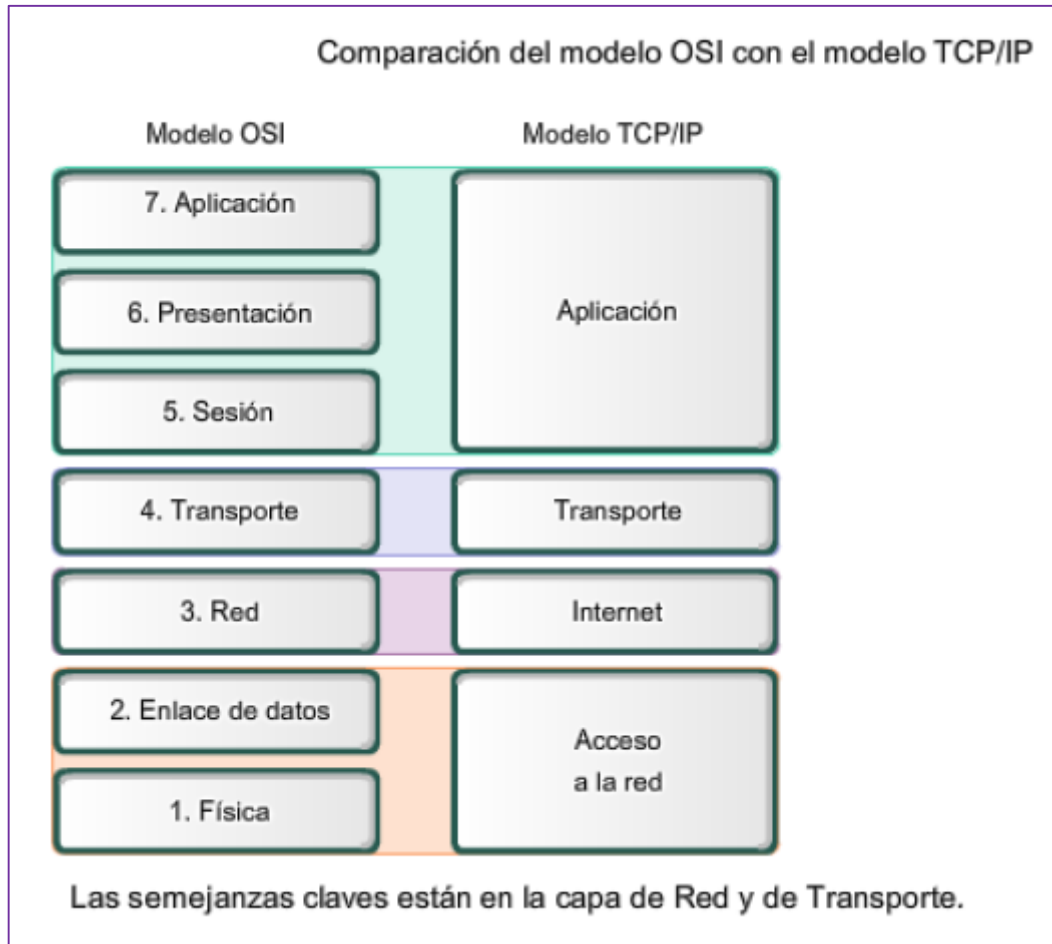


FIGURA 2.7 "Comparación del Modelo OSI con el Modelo TCP/IP". Fuente: CISCO

## 2.3 MARCO CONCEPTUAL

### ***Red de Comunicación de Datos***

*Se denomina red de comunicación de datos a aquella infraestructura que se ha diseñado específicamente a la transmisión de información mediante el intercambio de datos. Las redes de comunicación de datos se diseñan y construyen en arquitecturas que pretenden servir a sus objetivos de uso. Las redes de comunicación de datos, generalmente, están basadas en la conmutación de paquetes y se clasifican de acuerdo a su tamaño, la distancia que cubre y su arquitectura física.*

### 2.3.1 Determinación de términos básicos

1. Internet: Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como Arpanet, entre tres universidades en California y una en Utah, Estados Unidos.

2. Internet Dedicado: Producto que permite entregar acceso a Internet de alta calidad a través de una línea dedicada, la cual es conectada directamente desde los nodos del proveedor de internet hasta el cliente. Es un acceso a Internet exclusivo, donde el ancho de banda no se comparte con otros usuarios.

3. Intranet: Una red privada dentro de una organización. Las intranets suelen utilizar protocolos de Internet para entregar contenido. A menudo se protegen contra al acceso desde Internet mediante servidores.

4. IP address: (Dirección IP). Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos. Un ejemplo de dirección IP es 193.127.88.345.

5. Firewall: (Cortafuegos). Sistema que se coloca entre una red local e Internet. La regla básica es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autenticación, etc.

6. Línea de abonado digital asimétrica, ADSL (sigla del inglés Asymmetric Digital Subscriber Line) es un tipo de tecnología de línea DSL. Consiste en una transmisión analógica de datos digitales apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, siempre y cuando

la longitud de línea no supere los 5,5 km medidos desde la central telefónica, o no haya otros servicios por el mismo cable que puedan interferir.

7. Protocolo de Comunicaciones: En informática y telecomunicaciones, un protocolo de comunicaciones es un conjunto de reglas y normas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellos para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos.

8. Proxy: (Apoderado). Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red. Al mismo tiempo contiene mecanismos de seguridad (cortafuegos) que impiden accesos no autorizados desde el exterior hacia la red privada.

9. Servidor: En informática, un servidor es un nodo que, formando parte de una red, provee servicios a otros nodos denominados clientes. También se suele denominar con la palabra servidor una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de una computadora y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final. Este es el significado original del término. Es posible que un ordenador cumpla simultáneamente las funciones de cliente y de servidor.

10. Wi-Fi: es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, tales como: un ordenador personal, una consola de videojuegos, un smartphone o un reproductor de audio digital, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica. Dicho punto de acceso (o hotspot) tiene un alcance de unos 20 metros en interiores y al aire libre una distancia mayor. Pueden cubrir grandes áreas la superposición de múltiples puntos de acceso.

### CAPITULO III

## DISEÑO DE RED DE COMUNICACIÓN DE DATOS PARA LA INSTITUCIÓN EDUCATIVA PRIVADA EMILIO SOYER CABERO

### 3.1 ANALISIS DEL DISEÑO DE RED DE COMUNICACIÓN DE DATOS PARA LA INSTITUCIÓN EDUCATIVA PRIVADA EMILIO SOYER CABERO

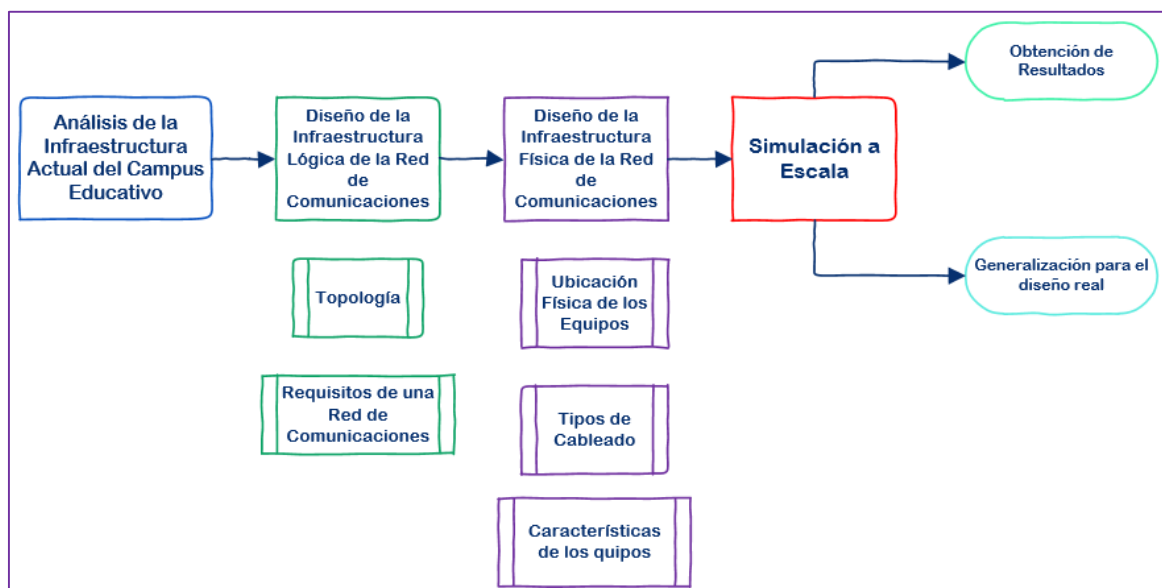


FIGURA 3.1: "Diagrama de Bloques para la secuencia del Diseño"

En la FIGURA 3.1 se puede observar la secuencia de cómo resolveremos el problema de la institución educativa. Aquí se observan los pasos fundamentales que daremos para lograr un diseño de red acorde con nuestros objetivos y necesidades.

El primer paso a dar es el **Análisis de la infraestructura actual del campus educativo**. Este paso nos permitirá saber cómo está distribuido geográficamente la institución, cómo está organizada el centro educativo institucionalmente de acuerdo a sus funciones y departamentos. Para esto necesitaremos información obtenida del plano del campus y del organigrama de la institución.

Gracias a la información previa procederemos ya al diseño de la red de comunicación de datos, tomando en cuenta las necesidades que debemos satisfacer. Esto se hará en dos pasos: el primero será el **diseño de la infraestructura lógica de red de comunicación de datos** que comprende todo lo concerniente a cómo será el camino que recorrerá la información, cómo estará estructurada la lógica de comunicación sin tomar en cuenta los detalles de cableado. El segundo será el **diseño de la infraestructura física de red de comunicación de datos**, aquí si se tomará en cuenta la parte geográfica para describir el camino que recorrerá la información, detallando el tipo de cableado del diseño.

Teniendo ya el diseño de red completado, procederemos a hacer una **simulación a escala**. Se hará un prototipo que consiste en una red más pequeña que tendrá lo más importante de la red original pero la misma estructura lógica. Esto se hará utilizando el software *Packet Tracer* con el objetivo de poder sacar conclusiones que satisfagan nuestros objetivos principales para así finalmente generalizar los resultados obtenidos.

## **3.2 DISEÑO DE RED DE COMUNICACIÓN DE DATOS PARA LA INSTITUCIÓN EDUCATIVA PRIVADA EMILIO SOYER CABERO**

### **3.2.1 Análisis y Diagnóstico de la Infraestructura Actual**

En la FIGURA 3.2 se aprecia la distribución de los edificios de la institución educativa. Como se había señalado antes, ésta cuenta con toda la construcción terminada mas no con una infraestructura de red que permita la comunicación

de todos los dispositivos para así poder transmitir la información académico-administrativa.

Se puede observar que la institución posee 11 edificios importantes: el pabellón administrativo, el pabellón académico, el pabellón A, B, C, D y E, la cafetería, el edificio donde se encuentran las piscinas, el Auditorio y la Biblioteca.

El pabellón Administrativo posee dos niveles mientras que el Académico posee tres, los pabellones A y B cuentan con tres niveles, al mismo tiempo que el pabellón C, D y E con dos niveles, la cafetería y la Biblioteca están constituidas por dos niveles, el área de piscinas es de mediano tamaño y está constituido por un solo nivel y finalmente el Auditorio que también es de un solo nivel pero grande y espacioso.



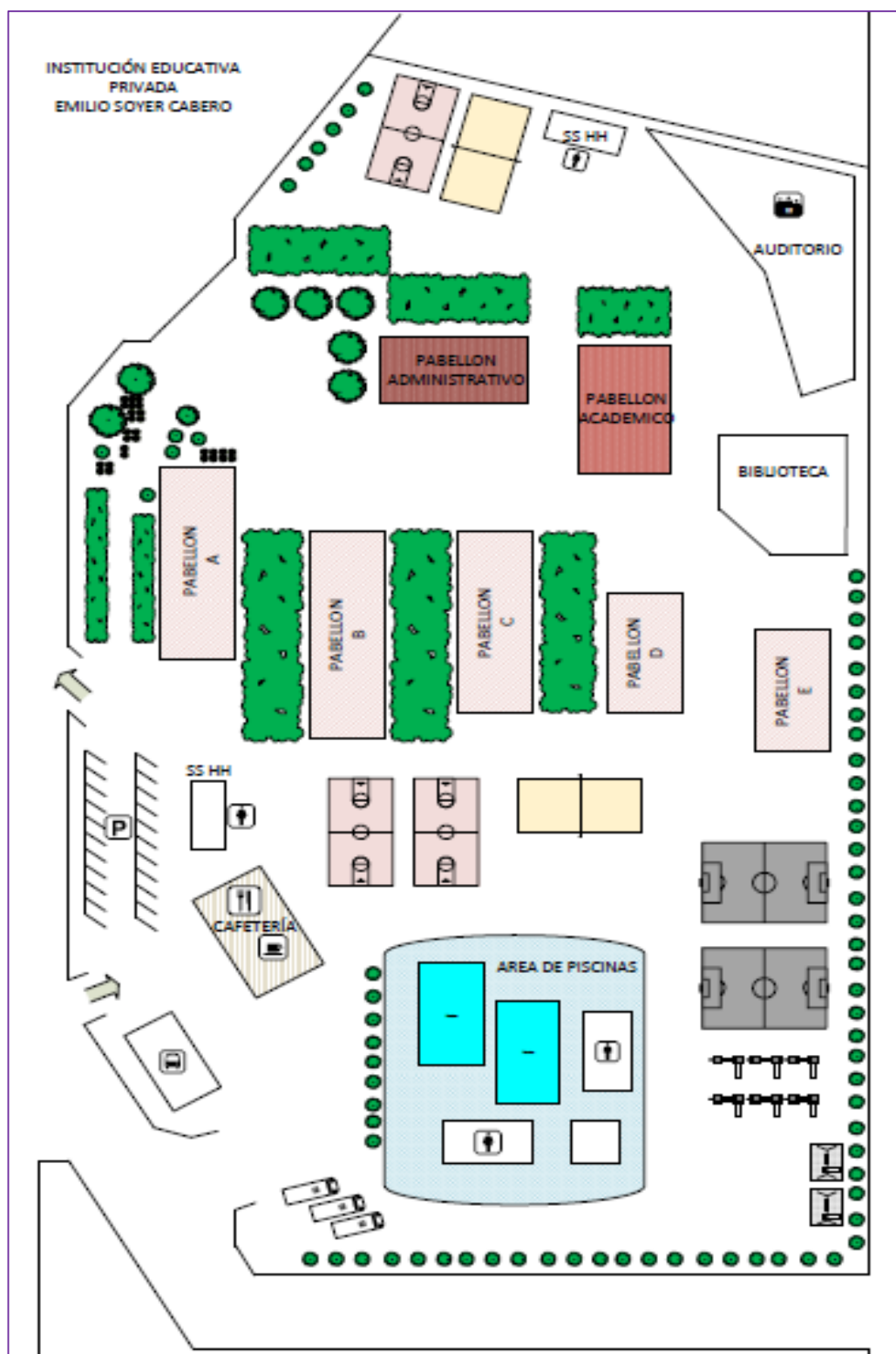


FIGURA 3.2 “Campus de la Institución Educativa Emilio Soyer Cabero”.

### **3.2.1.1 Detalles de la Infraestructura**

El pabellón administrativo, de dos niveles, cuentan con una serie de oficinas en donde se cumplirán diversas funciones que competen al campo de la administración gerencial y económica de la Institución Educativa. En cada oficina se contará con un número de ordenadores y teléfonos. Los ambientes se especifican a continuación:

#### **a. Pabellón Administrativo**

##### Primer Nivel

- Oficina de Dirección (4 hosts) (2 teléfonos)
- Oficina de Subdirección Administrativa (4 hosts) (2 teléfonos)
- Oficina de Secretaria General (4 hosts) (2 teléfonos)
- Oficina de Estadística e Informática (8 hosts) (2 teléfonos)
- Centro de Fotocopiado (12 hosts) (1 teléfono)

##### Segundo Nivel

- Oficina de RR.HH (4 hosts) (2 teléfonos)
- Mesa de Partes (4 hosts) (2 teléfonos)
- Oficina de Tesorería y Contabilidad(4 hosts) (2 teléfonos)
- Oficina de Jefatura de Servicios Generales(4 hosts) (2 teléfonos)
- Sala de Reuniones (ningún host ni teléfonos)

El Pabellón Académico, de tres niveles, es similar al administrativo, con la diferencia de que posee oficinas que cumplirán funciones competentes a la administración de la parte académica, es decir, funciones que tengan que ver con el trato del educando y la enseñanza. Estas oficinas se especifican a continuación:

## **b. Pabellón Académico**

### Primer Nivel

- Oficina de Subdirección Académica (4 hosts) (2 teléfonos)
- Oficina de Bienestar del Educando OBE(4 hosts) (2 teléfonos)
- Psicología (4 hosts) (2 teléfonos)
- Enfermería (4 host) (2 teléfonos)
- Oficina de Talleres Extracurriculares(4 hosts) (2 teléfonos)

### Segundo Nivel

- Oficina de Jefatura de Tutoría(4 hosts) (2 teléfonos)
- Sala de Tutores(12 hosts)
- Oficina de Jefatura del Cuerpo Docente(4 hosts) (2 teléfonos)
- Sala de Docentes (25 hosts)
- Oficina de Jefatura del Equipo Auxiliar(4 hosts) (2 teléfonos)
- Sala de Auxiliares(12 hosts)
- Oficina de Jefatura de Aulas, Laboratorios y Salas de Conferencias y Reuniones.(4 hosts) (2 teléfonos)
- Oficina de Jefatura de Biblioteca y Auditorio(4 hosts) (2 teléfonos)

### Tercer Nivel

- Sala de Conferencias 1 (2 hosts)
- Sala de Conferencias 2 (2 hosts)
- Sala de Conferencias 3 (2 hosts)
- Sala de Conferencias 4 (2 hosts)
- Sala de Conferencias 5 (2 hosts)

El pabellón A y B se comprenden tres niveles cada uno, en los cuales se encuentran las aulas de clases, las que tendrán una PC para uso exclusivo del docente; y diversos laboratorios de ciencias naturales, que cuentan con seis mesas de trabajo, cada una de ellas tendrán dos ordenadores, además de una PC para el docente a cargo de la clase y su respectivo teléfono. Los laboratorios

de inglés Cómputo contarán con 30 ordenadores con conexión a Internet, el ordenador del profesor y un teléfono. Los ambientes se especifican a continuación:

### **c. Pabellón A**

#### Primer Nivel

- Lab de Química (12 hosts) (1 teléfono)
- Lab de Física (12 hosts) (1 teléfono)

#### Segundo Nivel

- Primer Grado A (2 hosts)
- Primer Grado B (2 hosts)
- Primer Grado C (2 hosts)
- Primer Grado D (2 hosts)

#### Tercer Nivel

- Primer Grado E (2 hosts)
- Primer Grado F (2 hosts)
- Lab de Computación (32 hosts) (1 teléfono)

### **d. Pabellón B**

#### Primer Nivel

- Lab de Biología (12 hosts) (1 teléfono)
- Lab de Idiomas (32 hosts) (1 teléfono)

#### Segundo Nivel

- Segundo Grado A (2 hosts)
- Segundo Grado B (2 hosts)
- Segundo Grado C (2 hosts)
- Segundo Grado D (2 hosts)

### Tercer Nivel

- Segundo Grado E (2 hosts)
- Segundo Grado F (2 hosts)
- Lab de Computación (32 hosts) (1 teléfono)

El pabellón C, D y E poseen sólo dos niveles de aulas, las cuales se especifican a continuación:

### **e. Pabellón C**

#### Primer Nivel

- Tercer Grado A (2 hosts)
- Tercer Grado B (2 hosts)
- Tercer Grado C (2 hosts)
- Tercer Grado D (2 hosts)

#### Segundo Nivel

- Tercer Grado E (2 hosts)
- Tercer Grado F (2 hosts)
- Lab de Computación (32 hosts) (1 teléfono)

### **f. Pabellón D**

#### Primer Nivel

- Cuarto Grado A (2 hosts)
- Cuarto Grado B (2 hosts)
- Cuarto Grado C (2 hosts)
- Cuarto Grado D (2 hosts)

### Segundo Nivel

- Cuarto Grado E (2 hosts)
- Cuarto Grado F (2 hosts)
- Lab de Computación (32 hosts) (1 teléfono)

### **g. Pabellón E**

#### Primer Nivel

- Quinto Grado A (2 hosts)
- Quinto Grado B (2 hosts)
- Quinto Grado C (2 hosts)
- Quinto Grado D (2 hosts)

#### Segundo Nivel

- Quinto Grado E (2 hosts)
- Quinto Grado F (2 hosts)
- Lab de Computación (32 hosts) (1 teléfono)

La **cafetería** cuenta con dos niveles, ambos niveles contienen mesas, sillas y la mueblería correspondiente al servicio de comidas.

La **Biblioteca** tiene dos niveles. En el primer nivel se encuentra un espacio amplio que le sirve al alumnado para desarrollar sus labores académicas, asimismo se ubica la estantería donde se ordenan los libros y la **Recepción** donde en un par de computadoras se registrará el movimiento de los textos. En el segundo nivel se ubica un área con mesas y escritorios personales donde el alumnado se dedica a la lectura y el estudio sin ningún tipo de conectividad a la red.

El Auditorio cuenta con una pequeña **Oficina Administrativa** y el área donde se sientan las personas para la expectación de las diversas actividades a

presentar, el cual tiene una capacidad de 150 butacas. Asimismo se establecerán puntos de conexión cableado a dos host en el estrado.

Ni el **Área de Piscinas** ni la **Cafetería** tienen la necesidad de tener ninguna computadora en su interior ni conectarse a la Red para compartir datos relevantes.

Como se podría inferir, cada una de estas áreas no tienen las mismas necesidades de comunicación. Las prestaciones dependen de quién, en dónde y por dónde se conecte a la red. Es por eso que se debe diseñar una Red de Comunicación de Datos acorde a las diferentes características de toda la Institución Educativa en general.

El organigrama que se puede observar de forma general de cómo está estructurada y administrada la Institución Educativa Emilio Soyer Cabero se visualiza en la FIGURA 3.3.

### **3.2.2 Diseño de la Red de Comunicación de Datos para la Institución Privada Emilio Soyer Cabero**

Las autoridades de la Institución Educativa Privada Emilio Soyer Cabero no supieron especificar cuál sería la mecánica de comunicación, así como los parámetros ni configuraciones que debemos utilizar, sólo solicitaron tener en cuenta la ubicación de las oficinas en todo el campus, nos dio la potestad de elegir libre y criteriosamente todo lo concerniente al diseño de la red de comunicación de datos tomando en cuenta la seguridad y escalabilidad que se necesita.

#### **3.2.2.1 Lo que se hará**

Al analizar la información actual previamente, la cual comprende, el organigrama funcional y físico de la Institución Educativa Emilio Soyer Cabero, se ha optado por proponer un diseño de red de comunicaciones que consiste en lo siguiente:

- a. Proponer una topología adecuada para este caso, haciendo que la red sea escalable y tenga buen rendimiento.
  
- b. Segmentar la red de manera óptima y con buen criterio.
  
- c. Lograr que todos los integrantes de la comunidad estudiantil puedan acceder a Internet en casi todos los espacios del campus tanto de manera cableada como inalámbrica.
  
- d. No tratar de conectar directamente a la red sectores que no son necesarios.
  
- e. Lograr que la red sea segura y al mismo tiempo amigable para todo tipo de usuario.



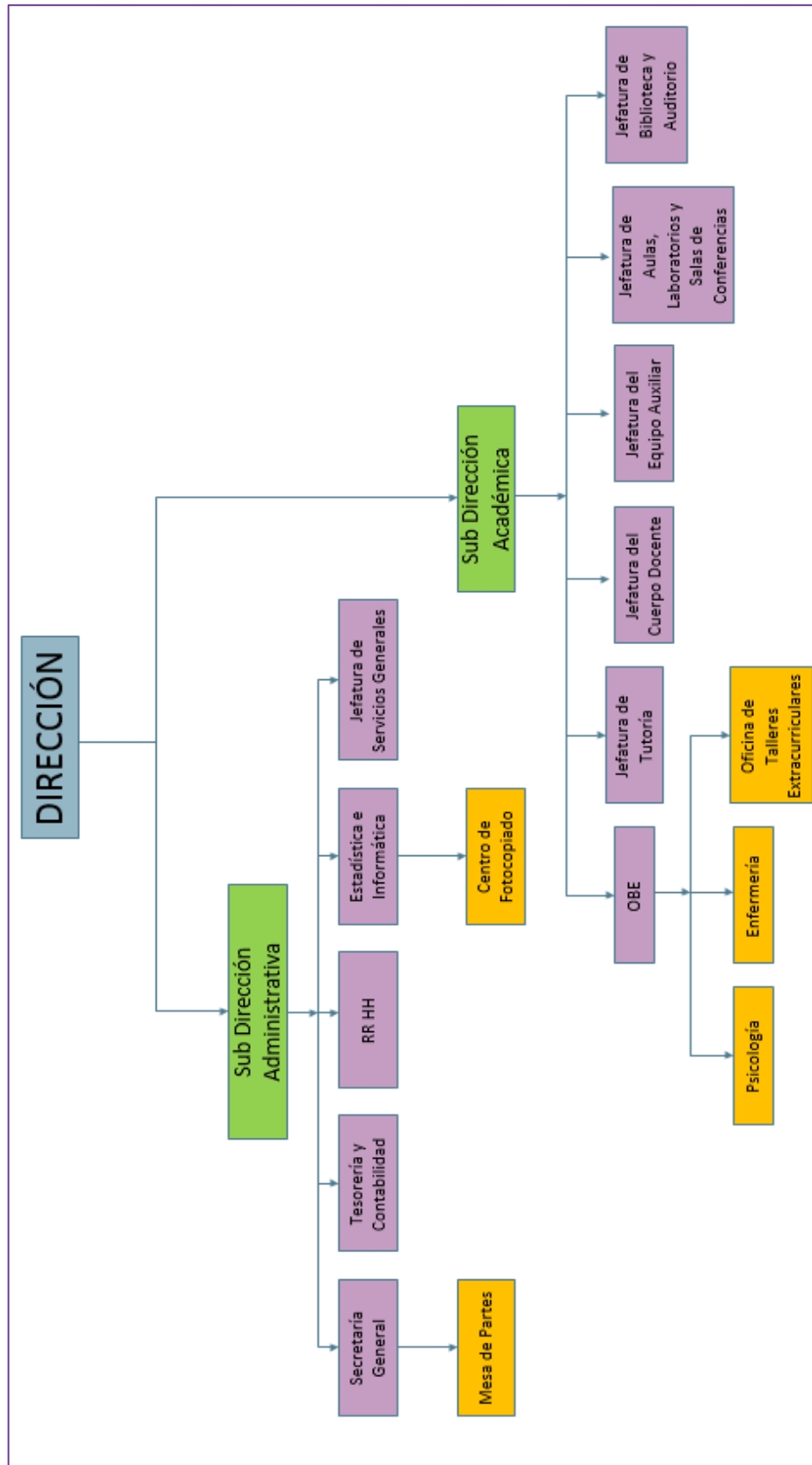


FIGURA 3.3 “Organigrama de la Institución Educativa Privada Emilio Soyer Cabero”. Fuente: Institución Educativa Privada Emilio Soyer Cabero

### 3.2.2.2 Topología de Red

Existe una variedad de opciones tanto en el aspecto físico como en el lógico para tomar en cuenta en este diseño, pero echando un vistazo al organigrama de la institución educativa, a la distribución de sus oficinas y a la necesidad de contar con un ISP, se optaría por elegir una topología lógica de broadcast y una física en árbol, proponiendo así una organización jerárquica.

La topología broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. No existe una orden que las estaciones deban seguir para utilizar la red. Es por orden de llegada, es como funciona Ethernet.

El diseño de redes jerárquicas implica la división de la red en capas independientes. Cada capa cumple funciones específicas que definen su rol dentro de la red general. La separación de las diferentes funciones existentes en una red hace que el diseño de la red se vuelva modular y esto facilita la escalabilidad y el rendimiento. En la FIGURA 3.4 se muestra este tipo de topología.

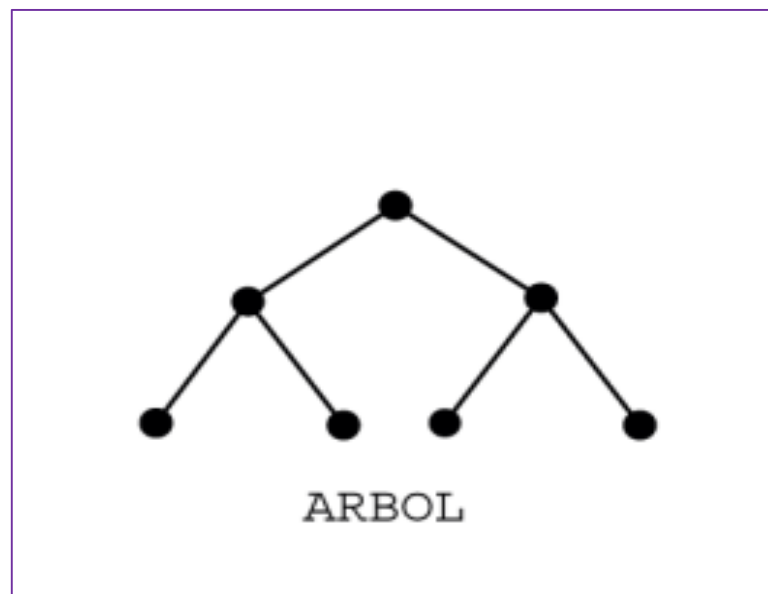


FIGURA 3.4 "Topología en Árbol"

### 3.2.2.3 Diseño del Diagrama de Infraestructura Lógica

El Diagrama de Infraestructura Lógica es el modelo de topología de red sin todos los detalles de la instalación exacta del cableado. Este diagrama es el mapa de ruta básico de la red.

Ya que el diseño será basado en una red jerárquica, existen tres capas fundamentales en este tipo de red:

- **Capa de Núcleo:** es el backbone de alta velocidad de la red. La Capa de Núcleo es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante. El área del núcleo también puede conectarse a los recursos de Internet. El núcleo agrega el tráfico de todos los dispositivos de la capa de distribución, por lo tanto debe poder reenviar grandes cantidades de datos rápidamente.
- **Capa de Distribución:** agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final. La capa de distribución controla el flujo de tráfico de la red con el uso de políticas y traza los dominios de broadcast al realizar el enrutamiento de las funciones entre las LAN virtuales (VLAN) definidas en la capa de acceso. Las VLAN permiten al usuario segmentar el tráfico sobre un switch en subredes separadas.
- **Capa de Acceso:** hace interfaz con dispositivos finales como las PC, impresoras y teléfonos IP, para proveer acceso al resto de la red. Esta capa de acceso puede incluir routers, switches, puentes, hubs y puntos de acceso inalámbricos. El propósito principal de la capa de acceso es aportar un medio de conexión de los dispositivos a la red y controlar qué dispositivos pueden comunicarse en la red.

El primer paso para llevar a cabo el diseño de la infraestructura lógica es saber con exactitud qué tipo de abonados tendremos y cuantos por cada tipo habrán.

Es por eso que la red se segmenta en varios grupos de trabajo a los cuales llamaremos subredes.

### **A. Segmentación de la Red**

Es evidente que todos los ambientes no son iguales en cuestión a la manera de cómo se conectaran a la red y que los usuarios en todo el campus no deberían tener la accesibilidad a todos los recursos que puedan existir. Por ejemplo la Pc en la enfermería no presenta el mismo tráfico que una en la Oficina de Estadística e Informática y tampoco una PC en la Oficina de Contabilidad y Tesorería no exige los mismos requerimientos en seguridad que una en el salón de clase, es por eso que se opta por segmentar la red en la cantidad de subredes necesarias para así mantener un orden.

Se observa también que varias oficinas que poseen características similares se encuentran físicamente en diferentes edificios, es por eso que se optará por hacer uso de las VLANs.

Las VLANs nos traerán muchas ventajas como:

- a. Seguridad. A los grupos que tienen datos sensibles se les separa del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial.
- b. Reducción de costos. El ahorro en el costo resulta de la poca necesidad de actualizaciones de red caras y usos más eficientes de enlaces y ancho de banda existente.
- c. Mejor rendimiento: la división de las redes planas de Capa 2 en múltiples grupos lógicos de trabajo (dominios de broadcast) reduce el tráfico innecesario en la red y potencia el rendimiento.
- d. Mitigación de la tormenta de broadcast. La división de una red en las VLAN reduce el número de dispositivos que pueden participar en una tormenta de broadcast.

e. Mayor eficiencia del personal de TI: las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN.

f. Administración de aplicación o de proyectos más simples: las VLAN agregan dispositivos de red y usuarios para admitir los requerimientos geográficos o comerciales.

Teniendo en cuenta la organización funcional, espacial y el común en varios tipos de tráfico de datos, se ha optado por separar las diversas áreas en las siguientes VLAN's:

**VLANS DE DATOS**

	<b>EDIFICIO</b>	<b>NIVEL</b>	<b>NOMBRE DEL AMBIENTE</b>	<b>Nº DE HOSTS REQUERIDOS</b>	<b>NOMBRE DE VLAN</b>	<b>NUMERO DE VLAN</b>
1	PABELLÒN ADMINISTRATIVO O	PRIMER NIVEL	Oficina de Dirección	4 hosts	DSS	VLAN 8
2	PABELLÒN ADMINISTRATIVO O	PRIMER NIVEL	Oficina de Sub Dirección Administrativa	4 hosts	DSS	VLAN 8
3	PABELLÒN ADMINISTRATIVO O	PRIMER NIVEL	Oficina de Secretaria General	4 hosts	ADM	VLAN 3
4	PABELLÒN ADMINISTRATIVO O	PRIMER NIVEL	Estadística e Informática	8 hosts	EI	VLAN 9
5	PABELLÒN ADMINISTRATIVO O	PRIMER NIVEL	Granja de Servidores	8 hosts	SERVERS	VLAN 14
6	PABELLÒN ADMINISTRATIVO O	PRIMER NIVEL	Centro de Fotocopiado	12 hosts	ADM	VLAN 3
7	PABELLÒN ADMINISTRATIVO O	SEGUNDO NIVEL	Mesa de Partes	4 hosts	ADM	VLAN 3
8	PABELLÒN ADMINISTRATIVO O	SEGUNDO NIVEL	Oficina de la Jefatura de SSGG	4 hosts	JEF	VLAN 10
9	PABELLÒN ADMINISTRATIVO O	SEGUNDO NIVEL	Oficina de Tesorería y Contabilidad	4 hosts	TES	VLAN 15
10	PABELLÒN ADMINISTRATIVO O	SEGUNDO NIVEL	Oficina de RRHH	4 hosts	ADM	VLAN 3

11	PABELLÒN ADMINISTRATIVO	SEGUNDO NIVEL	Sala de Reuniones	wifi con clave para 20 hosts	DSS	VLAN 8
12	PABELLÒN ACADEMICO	PRIMER NIVEL	Oficina de Sub Dirección Académica	4 hosts	DSS	VLAN 8
13	PABELLÒN ACADEMICO	PRIMER NIVEL	OBE	4 hosts	ACAD	VLAN 2
14	PABELLÒN ACADEMICO	PRIMER NIVEL	Psicología	4 hosts	ACAD	VLAN 2
15	PABELLÒN ACADEMICO	PRIMER NIVEL	Enfermería	4 hosts	ACAD	VLAN 2
16	PABELLÒN ACADEMICO	PRIMER NIVEL	Oficina de Talleres Extracurriculares	4 hosts	ACAD	VLAN 2
17	PABELLÒN ACADEMICO	SEGUNDO NIVEL	Oficina de Jefatura de Tutoría	4 hosts	JEF	VLAN 10
18	PABELLÒN ACADEMICO	SEGUNDO NIVEL	Sala de Tutores	12 hosts	SALAS 1	VLAN 12
19	PABELLÒN ACADEMICO	SEGUNDO NIVEL	Oficina de la Jefatura del Cuerpo Docente	4 hosts	JEF	VLAN 10
20	PABELLÒN ACADEMICO	SEGUNDO NIVEL	Sala de Docentes	25 hosts	SALAS 1	VLAN 12
21	PABELLÒN ACADEMICO	SEGUNDO NIVEL	Oficina de la Jefatura del Equipo Auxiliar	4 hosts	JEF	VLAN 10
22	PABELLÒN ACADEMICO	SEGUNDO NIVEL	Sala de Auxiliares	12 hosts	SALAS 1	VLAN 12

2 3	PABELLÒN ACADEMICO	SEGUNDO NIVEL	Oficina de la Jefatura de Aulas, Laboratorios y Salas de Conferencias y Reuniones	4 hosts	JEF	VLAN 10
2 4	PABELLÒN ACADEMICO	SEGUNDO NIVEL	Oficina de la Jefatura del Biblioteca y Auditorio	4 hosts	JEF	VLAN 10
2 5	PABELLÒN ACADEMICO	TERCER NIVEL	Sala de Conferencias I	2 hosts	SALAS 2	VLAN 13
2 6	PABELLÒN ACADEMICO	TERCER NIVEL	Sala de Conferencias II	2 hosts	SALAS 2	VLAN 13
2 7	PABELLÒN ACADEMICO	TERCER NIVEL	Sala de Conferencias III	2 hosts	SALAS 2	VLAN 13
2 8	PABELLÒN ACADEMICO	TERCER NIVEL	Sala de Conferencias IV	2 hosts	SALAS 2	VLAN 13
2 9	PABELLÒN ACADEMICO	TERCER NIVEL	Sala de Conferencias V	2 hosts	SALAS 2	VLAN 13
3 0	PABELLON A	PRIMER NIVEL	Lab de Química	12 hosts	LABS	VLAN 11
3 1	PABELLON A	PRIMER NIVEL	Lab de Física	12 hosts	LABS	VLAN 11
3 2	PABELLON A	SEGUNDO NIVEL	Primer Grado A	2 hosts	AULAS	VLAN 5
3 3	PABELLON A	SEGUNDO NIVEL	Primer Grado B	2 hosts	AULAS	VLAN 5
3 4	PABELLON A	SEGUNDO NIVEL	Primer Grado C	2 hosts	AULAS	VLAN 5



35	PABELLON A	SEGUNDO NIVEL	Primer Grado D	2 hosts	AULAS	VLAN 5
36	PABELLON A	TERCER NIVEL	Primer Grado E	2 hosts	AULAS	VLAN 5
37	PABELLON A	TERCER NIVEL	Primer Grado F	2 hosts	AULAS	VLAN 5
38	PABELLON A	TERCER NIVEL	Lab de Computación	32 hosts	LABS	VLAN 11
39	PABELLON B	PRIMER NIVEL	Lab de Biología	12 hosts	LABS	VLAN 11
40	PABELLON B	PRIMER NIVEL	Lab de Idiomas	32 hosts	LABS	VLAN 11
41	PABELLON B	SEGUNDO NIVEL	Segundo Grado A	2 hosts	AULAS	VLAN 5
42	PABELLON B	SEGUNDO NIVEL	Segundo Grado B	2 hosts	AULAS	VLAN 5
43	PABELLON B	SEGUNDO NIVEL	Segundo Grado C	2 hosts	AULAS	VLAN 5
44	PABELLON B	SEGUNDO NIVEL	Segundo Grado D	2 hosts	AULAS	VLAN 5
45	PABELLON B	TERCER NIVEL	Segundo Grado E	2 hosts	AULAS	VLAN 5
46	PABELLON B	TERCER NIVEL	Segundo Grado F	2 hosts	AULAS	VLAN 5
47	PABELLON B	TERCER NIVEL	Lab de Computación	32 hosts	LABS	VLAN 11
48	PABELLON C	PRIMER NIVEL	Tercer Grado A	2 hosts	AULAS	VLAN 5
49	PABELLON C	PRIMER NIVEL	Tercer Grado B	2 hosts	AULAS	VLAN 5
50	PABELLON C	PRIMER NIVEL	Tercer Grado C	2 hosts	AULAS	VLAN 5

51	PABELLON C	PRIMER NIVEL	Tercer Grado D	2 hosts	AULAS	VLAN 5
52	PABELLON C	SEGUNDO NIVEL	Tercer Grado E	2 hosts	AULAS	VLAN 5
53	PABELLON C	SEGUNDO NIVEL	Tercer Grado F	2 hosts	AULAS	VLAN 5
54	PABELLON C	SEGUNDO NIVEL	Lab de Computación	32 hosts	LABS	VLAN 11
55	PABELLON D	PRIMER NIVEL	Cuarto Grado A	2 hosts	AULAS	VLAN 5
56	PABELLON D	PRIMER NIVEL	Cuarto Grado B	2 hosts	AULAS	VLAN 5
57	PABELLON D	PRIMER NIVEL	Cuarto Grado C	2 hosts	AULAS	VLAN 5
58	PABELLON D	PRIMER NIVEL	Cuarto Grado D	2 hosts	AULAS	VLAN 5
59	PABELLON D	SEGUNDO NIVEL	Cuarto Grado E	2 hosts	AULAS	VLAN 5
60	PABELLON D	SEGUNDO NIVEL	Cuarto Grado F	2 hosts	AULAS	VLAN 5
61	PABELLON D	SEGUNDO NIVEL	Lab de Computación	32 hosts	LABS	VLAN 11
62	PABELLON E	PRIMER NIVEL	Quinto Grado A	2 hosts	AULAS	VLAN 5
63	PABELLON E	PRIMER NIVEL	Quinto Grado B	2 hosts	AULAS	VLAN 5
64	PABELLON E	PRIMER NIVEL	Quinto Grado C	2 hosts	AULAS	VLAN 5
65	PABELLON E	PRIMER NIVEL	Quinto Grado D	2 hosts	AULAS	VLAN 5
66	PABELLON E	SEGUNDO NIVEL	Quinto Grado E	2 hosts	AULAS	VLAN 5

67	PABELLON E	SEGUNDO NIVEL	Quinto Grado F	2 hosts	AULAS	VLAN 5
68	PABELLON E	SEGUNDO NIVEL	Lab de Computación	32 hosts	LABS	VLAN 11
69	BIBLIOTECA	PRIMER NIVEL	Área de Actividades Escolares	30 hosts	BBAE	VLAN 6
70	BIBLIOTECA	PRIMER NIVEL	Recepción para Sala de Lectura	4 hosts	JEF	VLAN 10
71	AUDITORIO	PRIMER NIVEL	Área de Butacas	wifi libre 150 hosts	AUDITORIO	VLAN 4
72	AUDITORIO	PRIMER NIVEL	Estrado	2 hosts	SALAS 2	VLAN 13
73	AUDITORIO	PRIMER NIVEL	Oficina	4 hosts	JEF	VLAN 10
74	CAMPUS	CAMPUS	CAMPUS	wifi libre 150 hosts	CAMPUS ESB	VLAN 7

TABLA 3.1: "VLANs De Datos Para la Red de Comunicaciones de la Institución Educativa Emilio Soyer Cabero"

En la TABLA 3.1 se observa cómo están agrupados los diferentes ambientes en torno a las VLANs. Se ha optado por hacer el uso de 14 VLANs de datos, los cuales son:

- a. VLAN 2 - ACAD: Esta VLAN reúne a las oficinas secundarias de la Institución en su ámbito académico, OBE, Psicología, Enfermería y Oficina de Talleres Extracurriculares. Estas oficinas reúnen el mismo tipo de tráfico y no requieren de tanta seguridad.
- b. VLAN 3 – ADM: Esta VLAN reúne a las oficinas secundarias de la Institución en su ámbito administrativo, la Oficina de Secretaria General, el Centro de

Fotocopiado, Mesa de Partes y la Oficina de RRHH. Estas oficinas reúnen el mismo tipo de tráfico y no requieren de tanta seguridad.

c. VLAN 4 – AUDITORIO: se le ha designado esta VLAN a todo el espacio libre del Auditorio, por razones de exclusividad de tráfico.

d. VLAN 5 – AULAS: esta VLAN es un muy buen ejemplo de la importancia de usar este tipo de tecnología. Reúne todas las aulas que están repartidas dentro de los pabellones A, B, C, D y E.

f. VLAN 6 – BBAE: exclusiva para el área de la biblioteca donde los alumnos podrán usar la Internet sólo para sitios web autorizados pues es para realizar las labores escolares, tareas, trabajos, etc.

g. VLAN 7 – CAMPUS: es para uso libre y exclusivo de los invitados que estén en las inmediaciones de la institución educativa, para el público en general. Reúne la característica que se podrá acceder a cualquier contenido.

h. VLAN 8 – DSS: Esta VLAN reúne a las oficinas principales de la Institución, la Dirección, la Sub Dirección Administrativa y la Subdirección Académica. Se ha decidido formar este grupo pues reúnen características similares como los mismos requerimientos de seguridad y funcionalidad.

i. VLAN 9 – EI: esta VLAN es de uso exclusivo de la Oficina de Estadística e Informática, al parecer podría haberse incluido en la VLAN que corresponde a las oficinas del pabellón administrativo pero al ser ésta un área que requiere de seguridad y que presenta mucho tráfico gracias a experimentos y pruebas informáticas, se requiero un grupo exclusivo.

j. VLAN 10 – JEF: Esta reúne las diversas jefaturas tanto de la parte administrativa como de la académica. Ya que estas oficinas reúnen características similares, se ha optado por reunir las en esta VLAN.

k. VLAN 11 – LABS: debido al gran tráfico que generan los laboratorios y al ser parte de una misma jefatura, se ha decidido reunirlos en una sola VLAN.

l. VLAN 12 – SALAS 1: esta VLAN reúne a las salas de tutores, docentes y auxiliares, las cuales requieren de seguridad pues en éstas el tráfico es confidencial, como notas, registros y contenido en general que debe ser resguardado.

m. VLAN 13 – SALAS 2: esta VLAN no requiere de tanta seguridad pues reúnen ambientes que son usados para las exposiciones de los alumnos en general.

n. VLAN 14 – SERVERS: esta VLAN no existe a causa de algún espacio físico, sino que debe ser creada para la administración de los servidores, un grupo de hosts que requieren de una máxima seguridad pues en esta se almacena toda la información de la institución al mismo tiempo que se genera un alto nivel de tráfico.

o. VLAN 15 – TES: esta VLAN es de uso exclusivo para la Oficina de Tesorería y Contabilidad, ésta pudo incluirse en la VLAN de oficinas administrativas pero ya que requiere de seguridad debido a temas contables y financieros se la ha aislado de otros ambientes.

## **B. Red de Telefonía sobre IP**

Una de las mejores tecnologías disponibles hoy en día que permite ahorrar costos es Voz sobre IP (VoIP). VoIP se refiere a transmisión de tráfico de voz de dos vías sobre una red IP, que permite combinar transmisión de voz con comunicación de datos en una plataforma IP única e integrada. Esto quiere decir que las llamadas telefónicas corren sobre la misma red que la computadora, en lugar de utilizar líneas telefónicas tradicionales. Esto ofrece muchos beneficios a los proveedores de servicios así como a los usuarios finales.

La característica más atractiva de Voz sobre IP es el ahorro de costos. Las llamadas son enviadas sobre líneas de datos existentes, eliminando así la cuenta telefónica. De esta forma la distancia y duración de las llamadas ya no es relevante desde el punto de vista de costos.

Es por esto que hemos optado por implementar Voz sobre IP en la Institución Educativa Emilio Soyer Cabero debido al ahorro que representa en diversos sentidos.

### C.VLAN de voz

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

- Ancho de banda garantizado para asegurar la calidad de la voz.
- Prioridad de la transmisión sobre los tipos de tráfico de la red
- Capacidad para ser enrutado en áreas congestionadas de la red
- Demora de menos de 150 milisegundos (ms) a través de la red

Para cumplir estos requerimientos, se debe diseñar la red completa para que admita VoIP.

VLAN DE VOZ						
	EDIFICIO	NIVEL	NOMBRE DEL AMBIENTE	Nº DE HOSTS REQUERIDOS PARATELEFONOS IP	NOMBRE DE VLAN	NUMERO DE VLAN

1	PABELLÒN ADMINISTRATIVO	PRIMER NIVEL	Oficina de Dirección	2 hosts	VOIP	VLAN 16
2	PABELLÒN ADMINISTRATIVO	PRIMER NIVEL	Oficina de Sub Dirección Administrativa	2 hosts	VOIP	VLAN 16
3	PABELLÒN ADMINISTRATIVO	PRIMER NIVEL	Oficina de Secretaria General	2 hosts	VOIP	VLAN 16
4	PABELLÒN ADMINISTRATIVO	PRIMER NIVEL	Estadística e Informática	2 hosts	VOIP	VLAN 16
6	PABELLÒN ADMINISTRATIVO	PRIMER NIVEL	Centro de Fotocopiado	1 host	VOIP	VLAN 16
7	PABELLÒN ADMINISTRATIVO	SEGUNDO NIVEL	Mesa de Partes	1 host	VOIP	VLAN 16
8	PABELLÒN ADMINISTRATIVO	SEGUNDO NIVEL	Oficina de la Jefatura de SSGG	2 hosts	VOIP	VLAN 16
9	PABELLÒN ADMINISTRATIVO	SEGUNDO NIVEL	Oficina de Tesorería y Contabilidad	2 hosts	VOIP	VLAN 16
10	PABELLÒN ADMINISTRATIVO	SEGUNDO NIVEL	Oficina de RRHH	2 hosts	VOIP	VLAN 16
11	PABELLÒN ADMINISTRATIVO	SEGUNDO NIVEL	Sala de Reuniones	1 host	VOIP	VLAN 16
12	PABELLÒN ACADEMICO	PRIMER NIVEL	Oficina de Sub Dirección Académica	2 hosts	VOIP	VLAN 16

1 3	PABELLÒN ACADEMICO	PRIMER NIVEL	OBE	2 hosts	VOIP	VLAN 16
1 4	PABELLÒN ACADEMICO	PRIMER NIVEL	Psicología	2 hosts	VOIP	VLAN 16
1 5	PABELLÒN ACADEMICO	PRIMER NIVEL	Enfermería	1 hosts	VOIP	VLAN 16
1 6	PABELLÒN ACADEMICO	PRIMER NIVEL	Oficina de Talleres Extracurriculares	1 host	VOIP	VLAN 16
1 7	PABELLÒN ACADEMICO	SEGUND O NIVEL	Oficina de Jefatura de Tutoría	2 hosts	VOIP	VLAN 16
1 9	PABELLÒN ACADEMICO	SEGUND O NIVEL	Oficina de la Jefatura del Cuerpo Docente	2 hosts	VOIP	VLAN 16
2 1	PABELLÒN ACADEMICO	SEGUND O NIVEL	Oficina de la Jefatura del Equipo Auxiliar	2 hosts	VOIP	VLAN 16
2 3	PABELLÒN ACADEMICO	SEGUND O NIVEL	Oficina de la Jefatura de Aulas, Laboratorios y Salas de Conferencias y Reuniones	2 hosts	VOIP	VLAN 16
2 4	PABELLÒN ACADEMICO	SEGUND O NIVEL	Oficina de la Jefatura del Biblioteca y Auditorio	2 hosts	VOIP	VLAN 16
3 0	PABELLON A	PRIMER NIVEL	Lab de Química	1 host	VOIP	VLAN 16



31	PABELLON A	PRIMER NIVEL	Lab de Física	1 host	VOIP	VLAN 16
38	PABELLON A	TERCER NIVEL	Lab de Computación	1 host	VOIP	VLAN 16
39	PABELLON B	PRIMER NIVEL	Lab de Biología	1 host	VOIP	VLAN 16
40	PABELLON B	PRIMER NIVEL	Lab de Idiomas	1 host	VOIP	VLAN 16
47	PABELLON B	TERCER NIVEL	Lab de Computación	1 host	VOIP	VLAN 16
54	PABELLON C	SEGUNDO NIVEL	Lab de Computación	1 host	VOIP	VLAN 16
61	PABELLON D	SEGUNDO NIVEL	Lab de Computación	1 host	VOIP	VLAN 16
68	PABELLON E	SEGUNDO NIVEL	Lab de Computación	1 host	VOIP	VLAN 16
69	AUDITORIO	PRIMER NIVEL	Oficina	1 host	VOIP	VLAN 16
70	BIBLIOTECA	PRIMER NIVEL	Recepción para la Sala de Lectura	1 host	VOIP	VLAN 16

TABLA 3.2: “Vlan de Voz para la Red de Comunicaciones de la Institución Educativa Privada Emilio Soyer Cabero”

En la TABLA 3.2 se muestra que todos los teléfonos IP se pueden reunir en una misma VLAN (VLAN 16) pues el tráfico de voz siempre es el mismo para cualquier terminal.

Esta VLAN se ha creado para que en un futuro cercano se pueda implementar todo el cableado estructurado y se ponga en marcha ya, la red de telefonía IP. Esto es un claro ejemplo de escalabilidad y visión a futuro.

## D. Subneteo

Debido a que hemos segmentado toda la red en varias subredes, debemos aplicar la técnica del subneteo para poder hacer posible que cada red distinta tenga su campo de ip's propias.

Ya que las diversas VLANs de datos que hemos formulado y la de voz cuentan con un numero de hosts diferentes, usaremos la técnica de subneteo de mascara variable.

En esta tabla primero se toma en cuenta la cantidad de hosts necesarios para cada VLAN, seguidamente se le aumentará el 25 % del total de ip's requeridas apelando al criterio de escalabilidad y por último le adicionaremos el ip de red y el ip de broadcast.

SUBNETEO						
N° VLAN	Nombre de VLAN	Cantidad de hosts	+ 25%	+ 2 Ip's	SUBRED	MASCARA DE SUBRED
Vlan 11	LABS	288	360	362	10.0.0.0 /23	255.255.254.0
Vlan 7	CAMPUS ESB	150	188	200	10.0.2.0 /24	255.255.255.0
Vlan 4	AUDITORIO	150	188	200	10.0.3.0 /24	255.255.255.0
Vlan 5	AULAS	60	75	77	10.0.4.0 /25	255.255.255.128
Vlan 12	SALAS 1	49	62	65	10.0.4.128 /25	255.255.255.128
Vlan 16	VOIP	44	55	57	10.0.5.0 /26	255.255.255.192
Vlan 8	DSS	32	40	42	10.0.5.64 /26	255.255.255.192
Vlan 10	JEF	32	40	42	10.0.5.128 /26	255.255.255.192
Vlan 6	BBAE	30	38	40	10.0.5.192 /26	255.255.255.192
Vlan 3	ADM	24	30	32	10.0.6.0 /27	255.255.255.224
Vlan 2	ACAD	12	15	17	10.0.6.32 /27	255.255.255.224

Vlan 13	SALAS 2	12	15	17	10.0.6.64 /27	255.255.255.224
Vlan 9	EI	8	10	12	10.0.6.96 /28	255.255.255.240
Vlan 14	SERVERS	8	10	12	10.0.6.112 /28	255.255.255.240
Vlan 15	TES	4	5	7	10.0.6.128 /29	255.255.255.248

TABLA 3.3: “Planeación de Subredes para la Institución Educativa Privada Emilio Soyer Cabero”

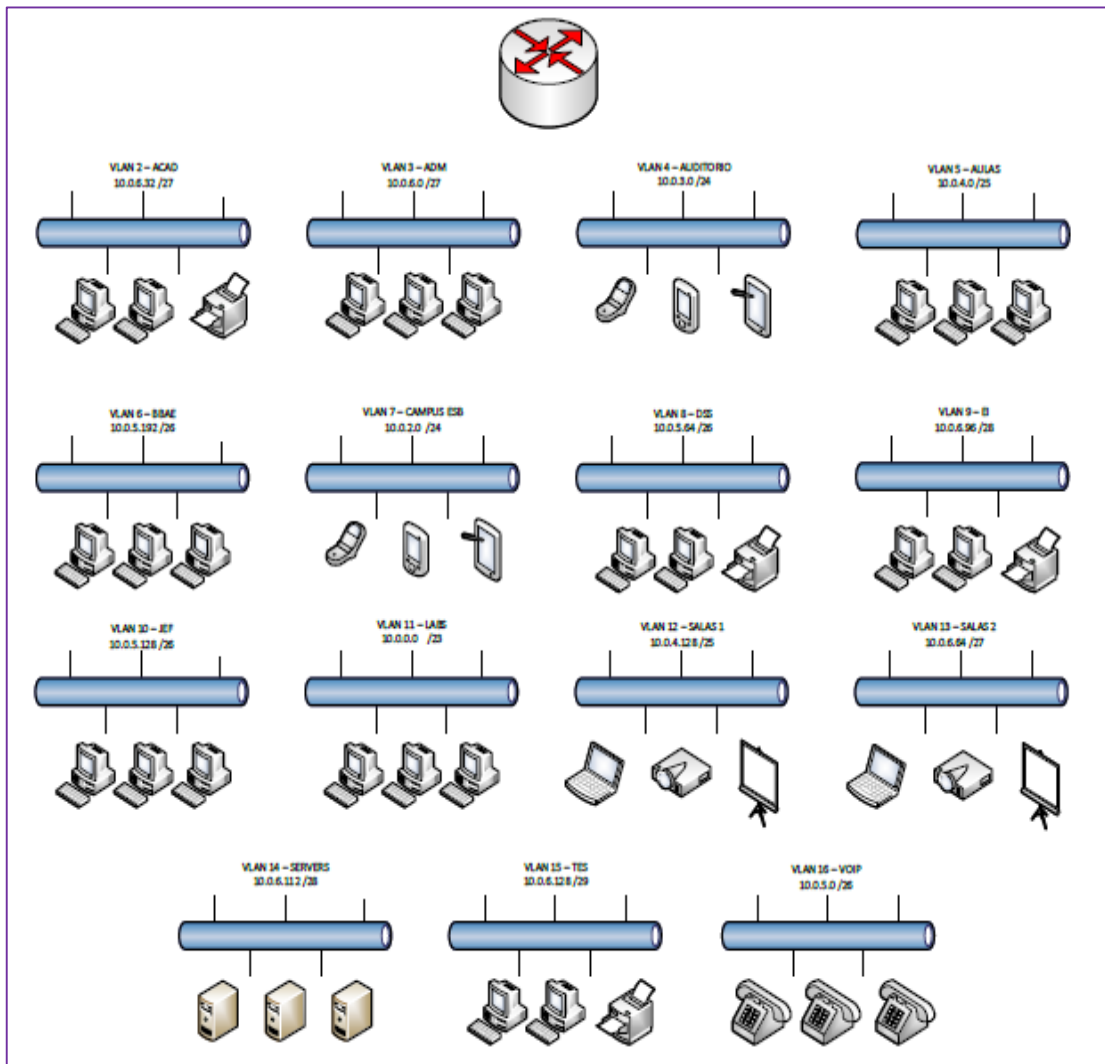


FIGURA 3.5: “Diagrama lógico de subredes”

En la FIGURA 3.5 se observa cómo se ha organizado la red, segmentándola en diferentes subredes y asignándolas a determinadas VLANs. Cabe resaltar que esta agrupación está basada en un aspecto lógico mas no físico, es decir,

los dispositivos aquí reunidos pueden estar en diferentes espacios físicos pero cada grupo conforman una subred específica.

E. Diagrama de la Infraestructura Lógica:

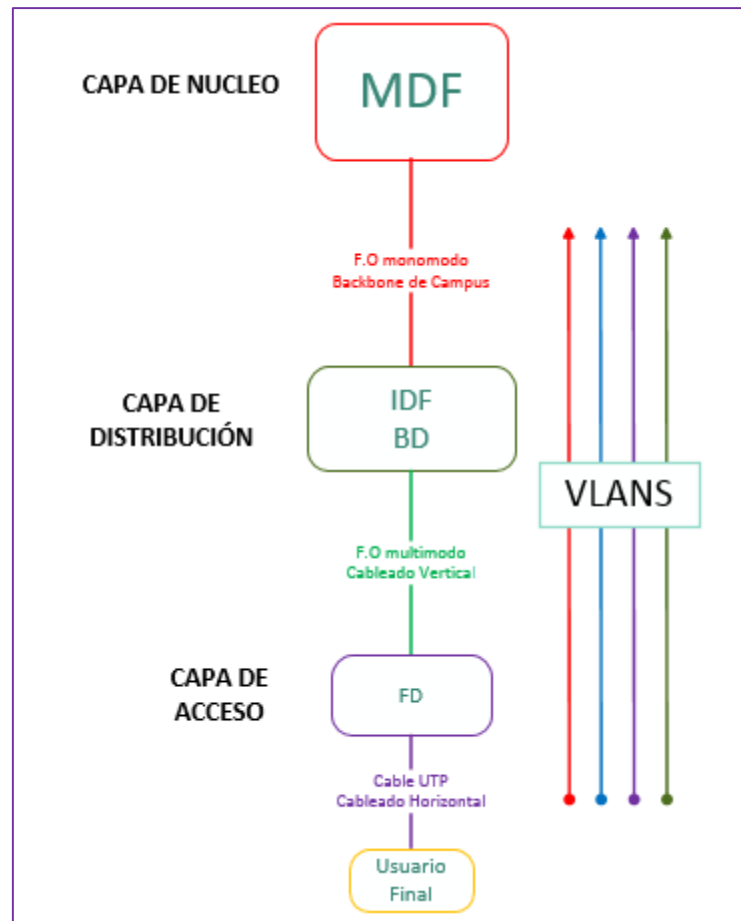


FIGURA 3.6: Diagrama de Infraestructura Lógica de la Red De Comunicación De Datos

En la FIGURA 3.6 se aprecia básicamente como viaja la información a través de la estructura de red desde un punto de vista lógico, sin especificaciones en el tipo de conexión, cableado ni prestaciones de equipos.

Desde la parte inferior, el usuario final se conecta al FD (Floor Distributor) a través de un cableado horizontal o en algunos casos inalámbricamente independientemente de a que VLAN o subred pertenezca el host. Éste FD representa a la CAPA DE ACCESO.

Los FD transmiten la información hacia el IDF (Instalación de distribución intermedia) donde se encuentra el BD (Building Distributor) el cual representa la CAPA DE DISTRIBUCIÓN, a través de un cableado vertical. El BD reúne la información y la transmite a través del cableado backbone de campus hacia el MDF.

El MDF (Instalación de distribución principal) es el lugar que gestiona el tráfico de red. Este MDF representa la CAPA DE NUCLEO en el cual el papel más representativo lo protagoniza un switch Layer 3 que trabaja como CD (Central Distributor).

#### **3.2.2.4 Diseño del Diagrama de Infraestructura Física**

Ahora debemos diseñar el diagrama de infraestructura física de la red de comunicaciones, tomando en cuenta lo siguiente:

- Ubicación física de los dispositivos.
- Tipo de cableado para el tráfico en las diferentes áreas del campus.
- Ancho de banda necesario en puntos cruciales de la red.
- Tipos de equipos a utilizar en cada punto clave del diseño.
- Cantidad de abonados en cada área que debemos de tomar en cuenta.

## A. Tipo de cableado:

### a. Cableado Horizontal:

Este tipo de cableado se dará en cada nivel de cada edificio.

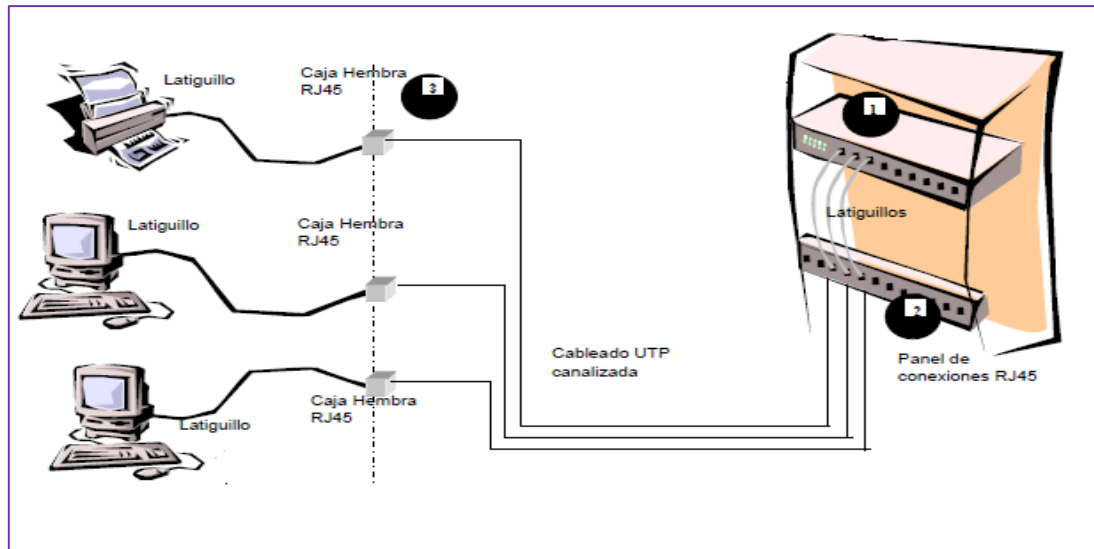


FIGURA 3.7: "Cableado Horizontal"

Como se observa en la FIGURA 3.7, desde el armario que contiene al SW L2 del FD al patch pannel, conectaremos latiguillos de cable UTP categoría 5e pues soporta 100Mbps. Asimismo este cableado también se dará desde la caja hembra RJ 45 hacia los abonados finales.

Desde el patch panel hasta la caja hembra RJ45 ira una conexión a lo largo de canaletas interiores que usaran cable UTP cruzado categoría 5e.

### b. Cableado Vertical:

Para este tipo de cableado utilizaremos un cable de fibra óptica multimodo que ira conectado desde un conversor de fibra óptica en cada SW L2 (FD) en cada nivel del edificio hacia el conector de fibra óptica del SW L3 (BD) de cada edificio. La conexión entre el distribuidor principal del edificio (BD) y los distribuidores de nivel (FD), forman el subsistema vertical o troncal del edificio.

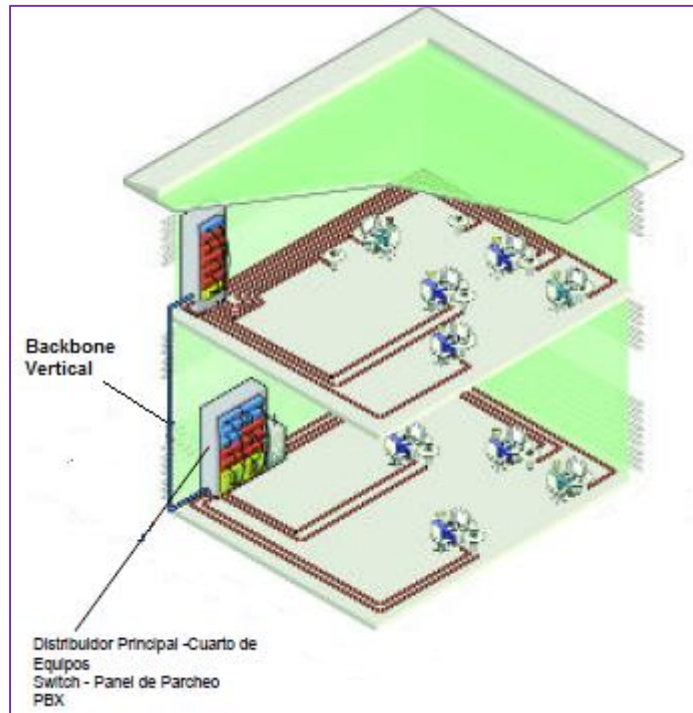


FIGURA 3.8: "Cableado Vertical"

Este subsistema, puede realizarse con cables de pares trenzados y/o cables de fibra óptica. Pero como ya se había indicado al principio de este apartado, en este caso usaremos cables de fibra óptica multimodo debido a su superior ancho de banda y su capacidad de cubrir distancias superiores a 100 metros.

La FIGURA 3.8 nos muestra lo antes descrito en el ejemplo de un edificio de dos niveles.

### c. Cableado Backbone de Campus

El Cableado troncal de campus, interconecta cada uno de los edificios. El centro del sistema, es el distribuidor central (CD). En el campus, las distancias son habitualmente altas, solo el cable de fibra óptica puede cubrir estas necesidades. El backbone de campus emplea principalmente cables de fibra óptica debido a sus bajas pérdidas y a su ancho de banda.

Son por estas razones que elegiremos cables de fibra óptica monomodo para el backbone de campus, además de tener la ventaja de la inmunidad electromagnética.

La FIGURA 3.9 nos muestra de manera general como están conectados dos edificios por medio del cableado de backbone de campus. También la misma imagen nos resume los tres tipos de cableado que se usaran en este diseño de red de comunicaciones: el horizontal, el vertical y el de backbone de campus.

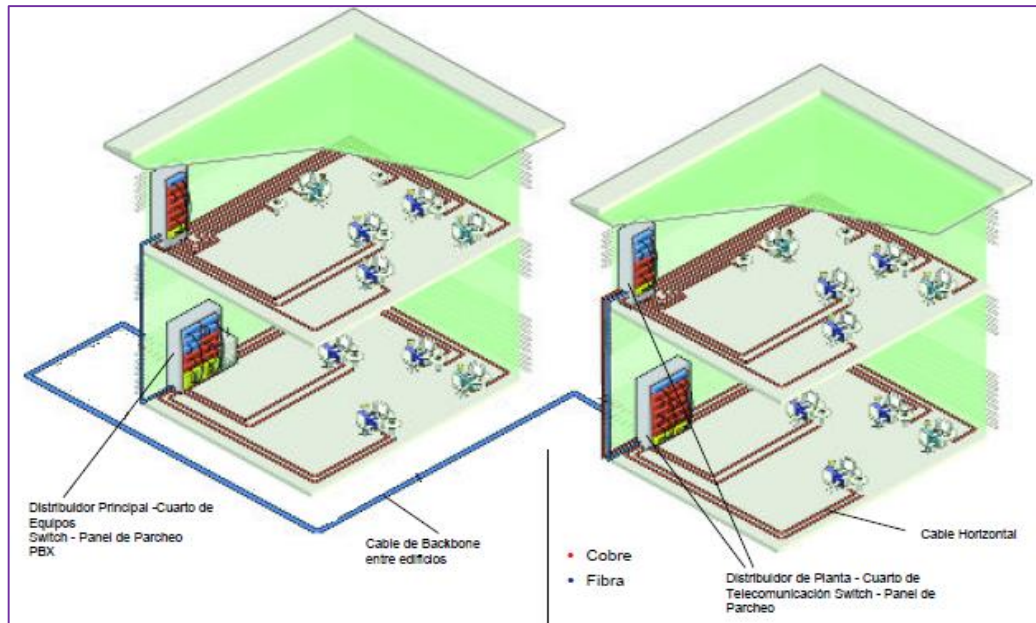


FIGURA 3.9: "Cableado De Backbone De Campus"



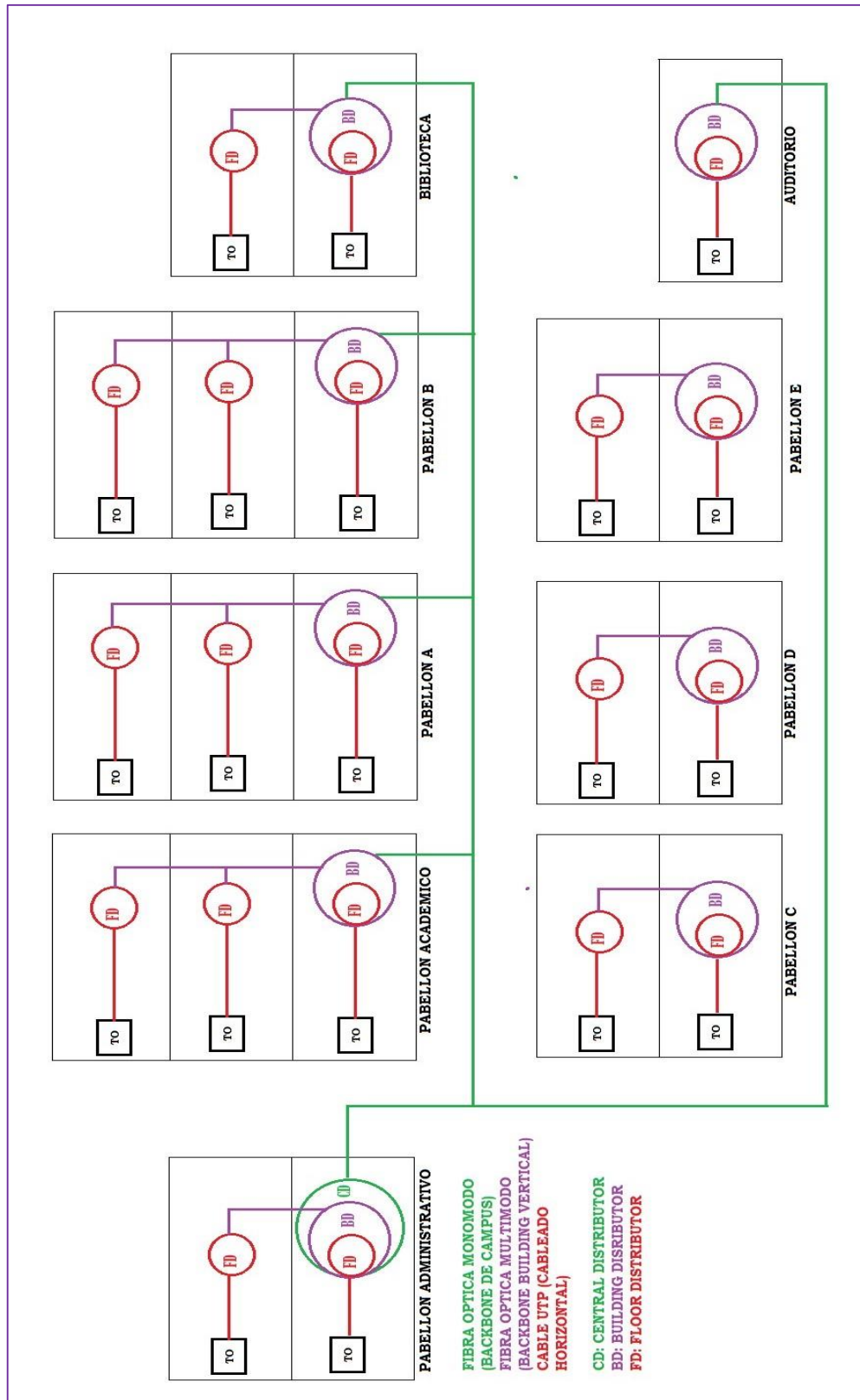


FIGURA 3.10: "Diagrama General de Cableado"

En la FIGURA 3.10 se da una amplia visión de cómo será el diseño físico de red concerniente al cableado. Dentro de nuestra red todo comienza (o termina) en el CD que se encuentra en el primer nivel del pabellón administrativo, el cual estará conformado fundamentalmente por el router de borde y el SW L3 encargado del enrutamiento entre VLANs. Éste alimentara de información al BD del mismo pabellón administrativo así como del pabellón académico, pabellón A, B, C, D y E, a la Biblioteca y Auditorio.

Los BD correspondientes a cada edificio alimentaran a su vez a los FD ubicados en cada nivel.

## **B. Equipos de Red a tomar en cuenta**

Ya que tenemos claro qué tipo de cableado se usará en las diferentes áreas de nuestra red, la cantidad de hosts a las que se les brindara información y también en que espacios se brindara acceso de manera inalámbrica, podemos elegir que tipos de dispositivos y características necesarias deben tener para poder trabajar en conjunto y hacer que este diseño sea óptimo.

- Router de borde:

Este funciona como puerta de enlace para la institución educativa, permitiendo la comunicación de ésta con la nube. Debe soportar la tecnología PoE, la cual nos permitirá que algunos dispositivos se alimenten de datos y de electricidad por el mismo puerto. Asimismo por ultimo debe soportar configuraciones de QoS para cuando en el futuro se implemente la red de telefonía IP no se necesite sustituirlo.

El router que elijamos debe contar con interfaces Gigabit Ethernet debido al gran tráfico de datos, y así poder conectarse a las interfaces Gigabit Ethernet del UTM.



FIGURA 3.11: "Router Cisco 1921" FUENTE: Cisco

El router Cisco 1921, que se muestra en la FIGURA 3.11, es elegido como buena opción para cumplir este papel en nuestra red por las siguientes razones:

- 2 puertos 10/100/1000 Ethernet integrados
- 2 ranuras para tarjetas de interfaces de alta velocidad WAN mejorada (EHWIC) que pueden alojar 2 módulos EHWIC.
- Distribución de energía totalmente integrado a los módulos de soporte 802.3af Power over Ethernet (PoE) y PoE Cisco Enhanced
- Seguridad
  - \* Encriptación VPN acelerado por hardware embebido.
  - \* Comunicaciones de colaboración altamente seguras con cifrado Grupo Transporte VPN, Dynamic Multipoint VPN, o Enhanced Easy VPN.
  - \* Control de amenazas integrado utilizando Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, Cisco IOS IPS y Cisco IOS Content Filtering.
  - \* Gestión de la identidad con la autenticación, autorización y contabilidad (AAA), y la infraestructura de clave pública.

- UTM (UnifiedThreat Management)

Se utiliza para describir los firewalls de red que engloban múltiples funcionalidades en una misma máquina.

Esta herramienta es una solución de seguridad todo en uno que integra todo lo necesario para proteger la red de comunicaciones de la institución. Con un sistema de gestión de amenazas unificada, los futuros administradores de red no se moverán con tanta frecuencia y el salto de la herramienta de seguridad a otro en la resolución de una amenaza.

El trabajo del administrador de red se verá muy reducido, ya que sólo se utilizará una única interfaz para ejecutar sus tareas de seguridad. La simplificación de los protocolos de seguridad con el uso de la UTM puede también ayudar a implementar una respuesta más rápida de seguridad. Un sistema de gestión de amenazas unificada proporciona informes detallados de seguridad, usted tendrá más tiempo para analizar las vulnerabilidades y las políticas de dispositivos para los usuarios de la red.

También permitirá ejecutar operaciones periódicas, por lo que puede definir las políticas de uso de la red o se pueden cambiar rápidamente las políticas de autenticación de la red, si detecta intrusiones en la misma. La Institución Educativa Privada Emilio Soyer Cabero estará siempre un paso adelante de los chicos malos, ya que puede poner en práctica nuevas soluciones de seguridad con la ayuda de la UTM.

No hay dudas que un sistema de gestión de amenazas unificada también es una solución rentable para de seguridad de red. Esto se debe a que elimina la necesidad de actualizar diferentes dispositivos de seguridad de diferentes proveedores que sólo se ocupará de ahora con un solo proveedor que reducirá significativamente el costo de las actualizaciones del sistema. Con una interfaz de usuario y un sistema unificado, no es necesario pasar por varios programas de capacitación. Esto significa más ahorros para su la institución y la administración de procesos más simples para el personal de seguridad de red.

EL UTM que seleccionemos para nuestra red debe contar con puertos Gigabit Ethernet para que pueda conectarse con el router de borde y pueda mandar el tráfico de datos al switch de Núcleo Layer 3.



FIGURA 3.12: "Cisco ASA 5515-X" FUENTE: Cisco

En la FIGURA 3.12 se observa una buena opción de UTM, Cisco ASA 5515-X que reúne las características y propiedades que buscamos, estas son:

- Visibilidad y control granular de las aplicaciones y los micro-aplicaciones, con controles basados en el comportamiento
- Seguridad web robusta
- Protección avanzada contra amenazas con un sistema integral, muy eficaz de prevención de intrusiones (IPS)
- Acceso remoto de alta seguridad
- Protección contra botnets
- Protección en tiempo casi real contra las amenazas de Internet
- Amplia gama de tamaños y de los factores de forma
- Proteger las redes de todos los tamaños con un rendimiento multi-escala y una amplia gama de factores de forma.

- Switch de Núcleo Layer 3 – Central Distributor

Este es el encargado de distribuir la información a los switches usados como BDs en los edificios correspondientes. Nuestro switch L3 debe ser de este tipo porque debe hacer enrutamiento entre VLANs. Al mismo tiempo debe tener puertos Gigabit Ethernet para la conexión con el UTM. Debe soportar la tecnología POE y también la configuración QoS, pensando en el futuro.

Asimismo debe contar con módulos para transceptores SFP (Transceivers-Small Form Factor), y que no son más que los elementos que dotan al switch de la capacidad de conectar un cable de fibra óptica para que este switch pueda conectarse a través del backbone de campus hacia todos los demás switches BD de capa 3 ubicados en cada edificio.

Una buena opción para este tipo de switches requeridos es el Cisco Catalyst 6503 que se adapta a las funcionalidades que requiere este nivel o punto central de conmutación en la red.



FIGURA 3.13: "Switch Catalyst 6503" FUENTE: Cisco

En la FIGURA 3.13 se observan el Switch Catalyst 6503 de Cisco, este equipo fue elegido por las siguientes razones:

- Motores de Supervisor
- Los módulos Fast Ethernet (IEEE 802.3af con Power over Ethernet [PoE])
- Módulos Ethernet Gigabit (con IEEE 802.3af PoE)
- Módulos de Ethernet 10 Gigabit
- Módulos Flex WAN
- Adaptadores de puertos compartidos/ SPA Procesadores de Interfaz
- Módulos de multi-servicio Gigabit (inalámbrica, análisis de redes y seguridad)

- Switch de Distribución - Building Distributor:

Este switch será el encargado de recibir la información a través del backbone de campus desde el switch de núcleo CD. Nuestro switch de distribución debe contar con puertos gigabit Ethernet de cobre, soportar tecnología QoS, soportar tecnología POE y contar con los puertos para transceptores SFP para recibir el SMF que llega desde el switch de núcleo y también poder repartir los datos hacia los switches capa 2 de cada nivel (FB) en el edificio a través de la fibra óptica multimodo.

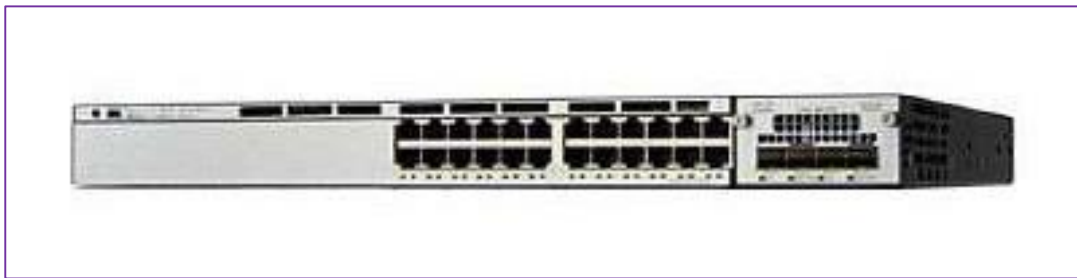


FIGURA 3.14: Switch CISCO 3750-X-24PS. FUENTE: Cisco

El Switch CISCO 3750-X-24PS mostrado en la FIGURA 3.14 es buena opción para jugar este papel en la red por las siguientes razones:

- Es apilable.
- Posee puertos FastEthernet para la conexión con los switches de capa 2 de cada nivel en los edificios, puertos GigabitEthernet.
- Posee módulos para transceptores SFP.
- Apoyo a las comunicaciones sin escalas con fuentes de alimentación intercambiables en caliente, ventiladores y módulos de red
- Prioriza el tráfico crítico para el negocio, como el vídeo a la cola de prioridad estricta (SPQ).
- Valida la disponibilidad de redes y simplificar la solución de problemas, con Mediatrace y Tráfico Simulador
- Mejora de la Eficiencia Energética
- Posee puertos PoE.

- Switch de Distribución Layer 2 -Floor Distributor:

Este switch será el más simple, no necesita ser de capa 3 pues solo servirá para repartir la información de manera horizontal. Este switch debe tener puerto FastEthernet POE, soportar implementación de VLANs y soportar QoS para la futura implementación de la red de telefonía IP. Asimismo veremos en lo subsiguiente de éste análisis que podríamos también necesitar que éste switch cuente con algunos puertos GigabitEthernet.



FIGURA 3.15: WS-C2960X-48FPD-L. FUENTE: Cisco

En FIGURA 3.15 se observa el switch Cisco WS-C2960X-48FPD-L, que puede soportar 48 puertos PoE. Este equipo es ideal para jugar el papel de switch de acceso por las siguientes razones:

- Permite apilar hasta 8 interruptores y 80 Gbps de ancho de banda con el opcional Cisco FlexStack + módulo
  - Proporciona soporte PoE y PoE + con hasta 740 W de potencia (sin fuente de alimentación externa)
  - Ofrece un control plano de la redundancia entre los conmutadores de la pila
  - Proporciona la fuente de alimentación redundante para la resistencia de potencia
- Inteligente
- Construido con cierto apilamiento - habilita QoS en toda la pila y cross-pila alta disponibilidad



- Automatiza la instalación del software para la implementación sin con Smart Install
- Configura automáticamente los puertos en función del tipo de equipo para el despliegue rápido con Auto Inteligente Puertos
- Ofrece diagnósticos proactivos y remediación de problemas de hardware y software con Smart Call Home
- Ahorra energía fuera de las horas con Cisco EnergyWise
- Modo de hibernación de bajada pone los enlaces descendentes a dormir cuando no esté en uso

- Access Point:

Este tipo de dispositivo intermediario permitirá a los usuarios conectarse a la red de manera inalámbrica. En este diseño de red de comunicación se ha tratado de usar este tipo de dispositivos en la cantidad necesaria posible, sin tener que recurrir a este recurso de manera exagerada, pues al ser un medio de comunicación sin guía de ondas, es decir, que aprovecha el espectro electromagnético, podría ser más complicado el diseño debido a que la probabilidad de interferencia con otras señales externas a la red se hace mayor en cuanto mas APs existan juntos. Como se había indicado antes en el planeamiento de las VLAN, en la TABLA 2: “VLANs de Datos para La Red de Comunicaciones de la Institución Educativa Privada Emilio Soyer Cabero”, existen grupos de IPs que forman parte de subredes inalámbricas. Estas son:

a) 20 hosts de la VLAN 8 que se destinarán para ser usada por los asistentes en la Sala de Reuniones Administrativas.

Este AP será conectado a uno de los puertos FastEthernet del SW L2 FD del primer nivel del pabellón administrativo y se colocará dentro de la Sala de Reuniones Administrativas para que los asistentes a las reuniones puedan acceder a la red.

b) Todos los 150 hosts de la VLAN 4 que se destinará para ser usada por los asistentes en el Área de Butacas del Auditorio.

Este AP será conectado a uno de los puertos GigabitEthernet del switch FD que se ubicará en el único nivel del Auditorio, el cual apunará a las butacas para que la señal pueda llegar a todos los asistentes que llegan a ser parte las presentaciones, obras teatrales y eventos por el estilo de manera libre y sin restricciones.

c) Todos los 150 hosts de la VLAN 7 que se destinará al uso del público en general en todo el Campus de la Institución Educativa.

Este AP será conectado a uno de los puertos GigabitEthernet del switch FD del tercer nivel del pabellón B. Se colocará con dirección al área deportiva para que la señal pueda llegar a la CAFETERÍA y al AREA DE PISCINAS para conectar a los host ubicados en esos edificios a la red del recinto.

Para cumplir estas funciones se elegirán dos tipos de Access Points, uno para interiores y otro para exteriores.

Para interiores se elegirá el AP Cisco Aironet 600, el cual se muestra en la FIGURA 3.16.



FIGURA 3.16: "CISCO AIRONET 600" FUENTE: Cisco

El AP Cisco Aironet 600 se ha elegido como AP de interior por las siguientes razones:

- Extiende los servicios y las políticas de red sin fronteras para el teletrabajador casa-oficina.
- Protege el ambiente corporativo con el control estándar de la industria y el punto de acceso inalámbrico de apoyo (CAPWAP).
- Admite simultáneamente la actividad de la red corporativa y personal con la segmentación del tráfico.
- Aumenta la productividad y reduce los costes celular mediante la extensión de la voz para el hogar de forma inalámbrica oa través de un puerto Ethernet con cable.
- Reduce el tiempo de configuración con el aprovisionamiento simplificado de TI.
- Posee capacidad Backward compatible con dispositivos 802.11a/b/g, así como los dispositivos 802.11n de nueva implantación.
- Diseño elegante para una cómoda colocación en interiores

Para exteriores se elegirá el AP Cisco Aironet 1552S, el cual se muestra en la FIGURA 3.17.



FIGURA 3.17: "CISCO AIRONET 1552S" FUENTE: Cisco

El AP Cisco Aironet 15552S se ha elegido como AP de interior por las siguientes razones:

- Diseñado para entornos peligrosos (Clase Certificada 1 Div2/Zone2 recinto)
- Posee tecnología Cisco CleanAir ofrece inteligencia de espectro integrado por una red de auto-configuración y auto-sanación
- Posee tecnología de múltiples entradas y múltiples salidas 2x3-(MIMO)
- Posee soporte para múltiples de radio IEEE (802.11a / n, 802.11b/g/n) 3 MIMO de antena y dos flujos espaciales
- Posee opciones de enlace ascendente Múltiples (Gigabit Ethernet-10/100/1000 BaseT, interfaz de fibra SFP)

- Servidor

Este equipo se encargara de brindar información a los ordenadores que se conecten a él. Cuando los usuarios de esta institución educativa se conecten al servidor podrán acceder a programas, archivos y otra información del servidor.



FIGURA 3.18: "UCS C240 M3" FUENTE: Cisco

Para este trabajo se elige como buena opción al Servidor Cisco UCS C240 M3, el cual se muestra en la FIGURA 3.18. Este equipo fue elegido por las siguientes razones:

- Diseñado para proporcionar tanto un gran rendimiento como capacidad de expansión para una amplia gama de cargas de trabajo que requieren un uso intensivo del almacenamiento, contemplando desde Big Data hasta aplicaciones de colaboración.

- Adecuado para casi todas las aplicaciones, de 2 sockets de almacenamiento intensivo
- Posee una tarjeta de interfaz virtual Cisco UCS 1225 (VIC): 2 x PCIe 10GE que puede soportar hasta 256 interfaces virtuales PCIe
- Posee un bloque de construcción excepcional y punto de entrada para el Sistema de Computación Unificado de Cisco
- Cuenta innovaciones continuas de Cisco en la tecnología de servidor y de todos los niveles del Sistema de Computación Unificado de Cisco
- Cálculo y elección del UPS

Un sistema de alimentación ininterrumpida, SAI, también conocido como UPS (del inglés uninterruptible power supply), es un dispositivo que, gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón a todos los dispositivos que tenga conectados.

En el caso de nuestra red, se tendrá conectado al UPS los equipos dentro del rack de comunicaciones ubicado en la Oficina de Informática, los cuales figuran en la tabla, la cual también especifica la potencia máxima consumida por cada equipo.

Equipo	Potencia Máxima requerida (watts)
<b>Router 1921</b>	200
<b>UTM ASA 5515-X</b>	680
<b>Switch 6503</b>	1400
<b>Server UCS 240 M3</b>	1200

Tabla 3.4: “Potencia máxima requerida en los equipos del rack de comunicaciones”

Para calcular la capacidad en watts que debe tener nuestro UPS debemos sumar la potencia máxima requerida de cada dispositivo, luego tomando en

cuenta que es muy poco probable que todos los equipos funcionen a su máxima capacidad al mismo tiempo, se le restara un 33% de capacidad. Finalmente se le multiplicara por el factor de 1.3 a este resultado debido a un posible crecimiento a futuro, y así se obtendrá finalmente la capacidad que debe tener nuestro UPS.

- Total de potencia máxima requerida (watts) =  $200 + 680 + 1400 + 1200 = 3480$

- Capacidad normal de todos los componentes en el rack de comunicaciones (disminuyendo el 33%)

$67\% \times 3480 = 2332$  watts

- Aumento del 30 % debido al posible crecimiento a futuro

$1.3 \times 2332 = \mathbf{3032}$  watts

Con este resultado debemos tener en cuenta un UPS que tenga la capacidad de dotar energía para una carga de 3032 watts, para esto escogemos el UPS APC SURT5000XLICH, el cual se muestra en la FIGURA 3.19.



FIGURA 3.19: "UPS APC SURT5000XLICH" FUENTE: APC

Este modelo de UPS es una buena opción por las siguientes razones:

- Ser un APC Smart-UPS On-Line, 3500 Watts / 5000 VA, Entrada 230V / Salida 230V.
- Proporciona administración de energía remota al SAI a través de la red.
- Posee Indicadores LED de estado Comprender rápidamente la unidad y de la alimentación mediante indicadores ópticos

El UPS SURT5000XLICH entrará en funcionamiento automáticamente en ausencia del fluido eléctrico, alimentando los componentes en el rack de comunicaciones por aproximadamente 8 minutos.

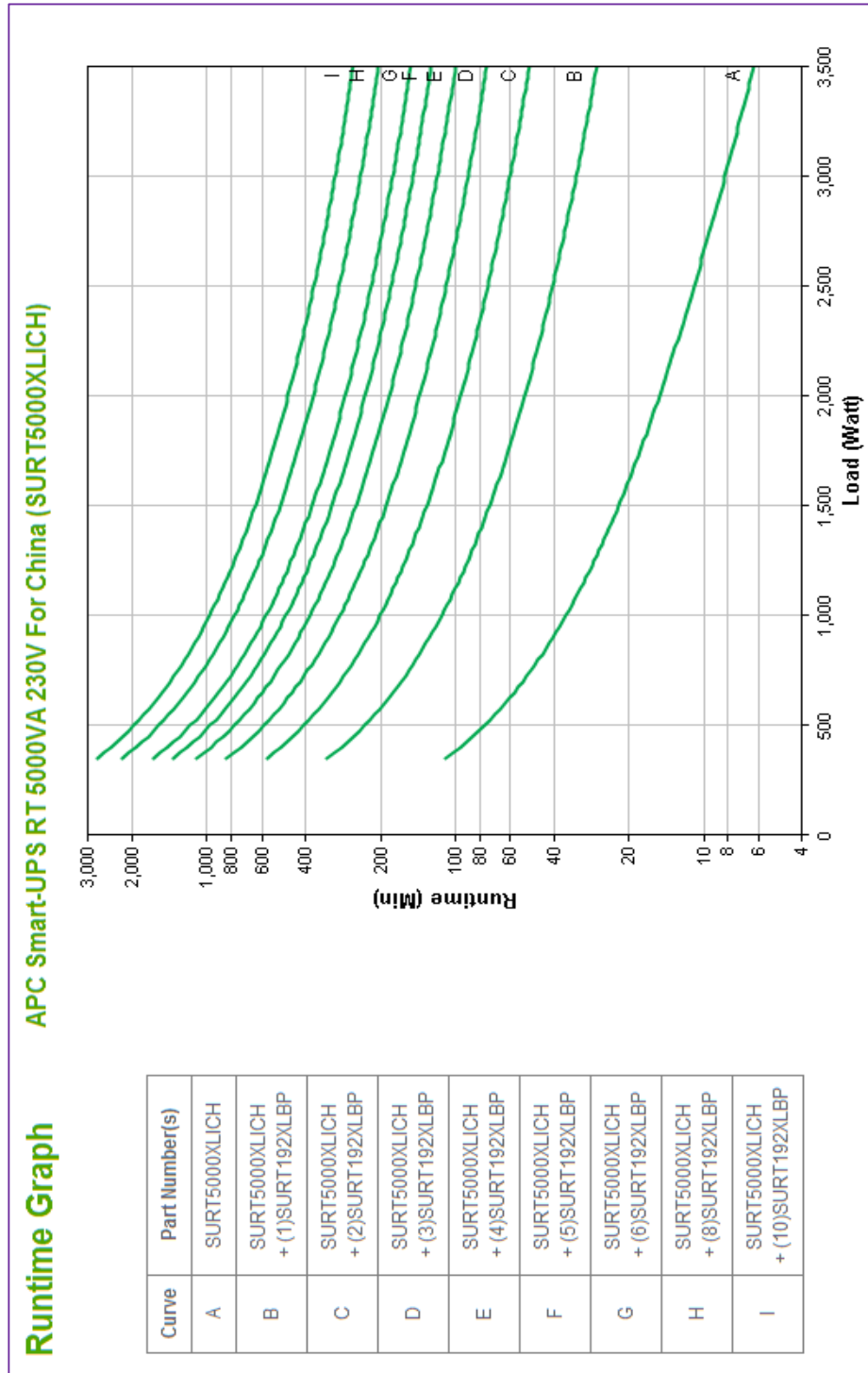


FIGURA 3.20: “Autonomía del UPS APC SURT5000XLICH” FUENTE: APC

En la FIGURA 3.20 se puede apreciar el tiempo de autonomía que será alimentado nuestro rack por el UPS. Nótese que el tiempo puede ser elevado gracias a la adición de los módulos SURT192XLBP.

### **C. Diagrama de Infraestructura Física**

Ya que anteriormente se han mostrado diagramas que reflejan la manera general de cómo funcionará la red de comunicaciones (FIGURA 3.21 y FIGURA 3.22) y que ahora ya tenemos claro las características de los equipos a usar y el tipo de conexiones entre ellas para el transporte de datos, se ha elaborado un diagrama de infraestructura, el cual nos dará una visión más detallada de la red teniendo en cuenta la ubicación de los dispositivos y el tipo tendido de las líneas de conexión.

En las FIGURAS 3.21 y 3.22 se aprecia cómo está estructurada la red de comunicaciones desde un punto de vista más físico. Se observa en la FIGURA 3.20 que el Router de borde estará conectado por dos cables Gigabit Ethernet hacia el UTM de nuestra elección, éste a su vez estará conectado por otros dos puertos Gigabit Ethernet al Switch Layer 3 que se encargará de ser el distribuidor central de la red, estos tres dispositivos forman la Capa de Núcleo. Este arreglo de dispositivos se ubicará en un rack en un espacio de la Oficina de Estadística e Informática.

En esta figura también observamos que la Granja de Servidores estará conectado directamente a los puertos Gigabit del Switch de Núcleo, se optó por esto para que los servidores cuenten con más ancho de banda para comunicarse ya que éstos gestionan una gran cantidad de información proveniente de toda la red.

Posteriormente en la misma figura se aprecia que el Switch de núcleo a través de su puerto de fibra óptica reparte la información por medio del cable de backbone de campus (fibra óptica monomodo) a los edificios del Pabellón



Administrativo y el pabellón académico, como también a los demás edificios que se detallan en la FIGURA 3.22.

Regresando a la FIGURA 3.21, cada pabellón se conecta a la capa de núcleo por medio de un Switch que sirve de distribuidor de edificio. Cada uno de estos se conectan por el otro extremo a switches más simples que servirán como distribuidores de nivel.

Nótese que el switch distribuidor de edificio al estar en el mismo nivel que el switch del nivel 1, se conecta a él por medio de un cable utp conectado directamente a un puerto GigabitEthernet por ambos extremos. Pero para que el Switch distribuidor de edificio pueda conectarse a niveles superiores debe hacerse uso del cable de fibra óptica multimodo, que cumplirá el papel de cable de tendido vertical, este cable se conectara por un extremo a un puerto de fibra óptica del switch distribuidor de edificio y por el otro extremo a un puerto de fibra óptica del switch distribuidor de nivel.

El distribuidor de nivel de cada piso en cada edificio utilizara un tendido horizontal por medio de cables utp conectados a puertos FastEthernet por un extremo y luego de pasar por patchs cords, rosetas e intermedios de este tipo, llegará finalmente al abonado.

Asimismo también en la FIGURA 3.21 se puede apreciar que en el segundo nivel del pabellón administrativo, un Access Point se conecta al Switch por medio de un cable utp conectado por ambos extremos a puertos FastEthernet. Esto se debe a que en la Sala de Reuniones Administrativas se vio conveniente hacer uso de la conexión sin cables para poder mantener conectados a los asistentes.

En la FIGURA 3.22 se observa que se continúa con el despliegue de datos por medio del cable de backbone de campus (cable de fibra óptica monomodo) que está conectado a uno de los puertos de fibra óptica del switch de núcleo. Este cable de fibra óptica se conecta por el otro extremo a los switches

distribuidores de edificio del pabellón A, B, C, D, y E, así como también al Auditorio y Biblioteca.

Nótese también que se vuelve a repetir el caso de la conexión entre el switch distribuidor de edificio al switch distribuidor de nivel del primero piso por medio de un cable utp conectado a puertos GigabitEthernet por ambos extremos, como sucedió en la FIGURA 3.21.

También se aprecia que existen conexiones a Access Point pero esta vez con cable utp conectado a puertos GigabitEthernet ya que en el caso del switch de distribución de nivel del tercer piso del Pabellón B se conectara un AP que pueda dotar de internet al espacio libre del campus de la institución demandando gran capacidad de tráfico en el medio. De manera similar ocurre con el switch de nivel del único piso de la Biblioteca el cual se conecta a un AP por medio de un cable utp que por ambos extremos está conectado a puertos GigabitEthernet, ya que este AP tendrá el trabajo de proveer de internet a todos los asistentes a los eventos que se llevaran a cabo en el Auditorio.

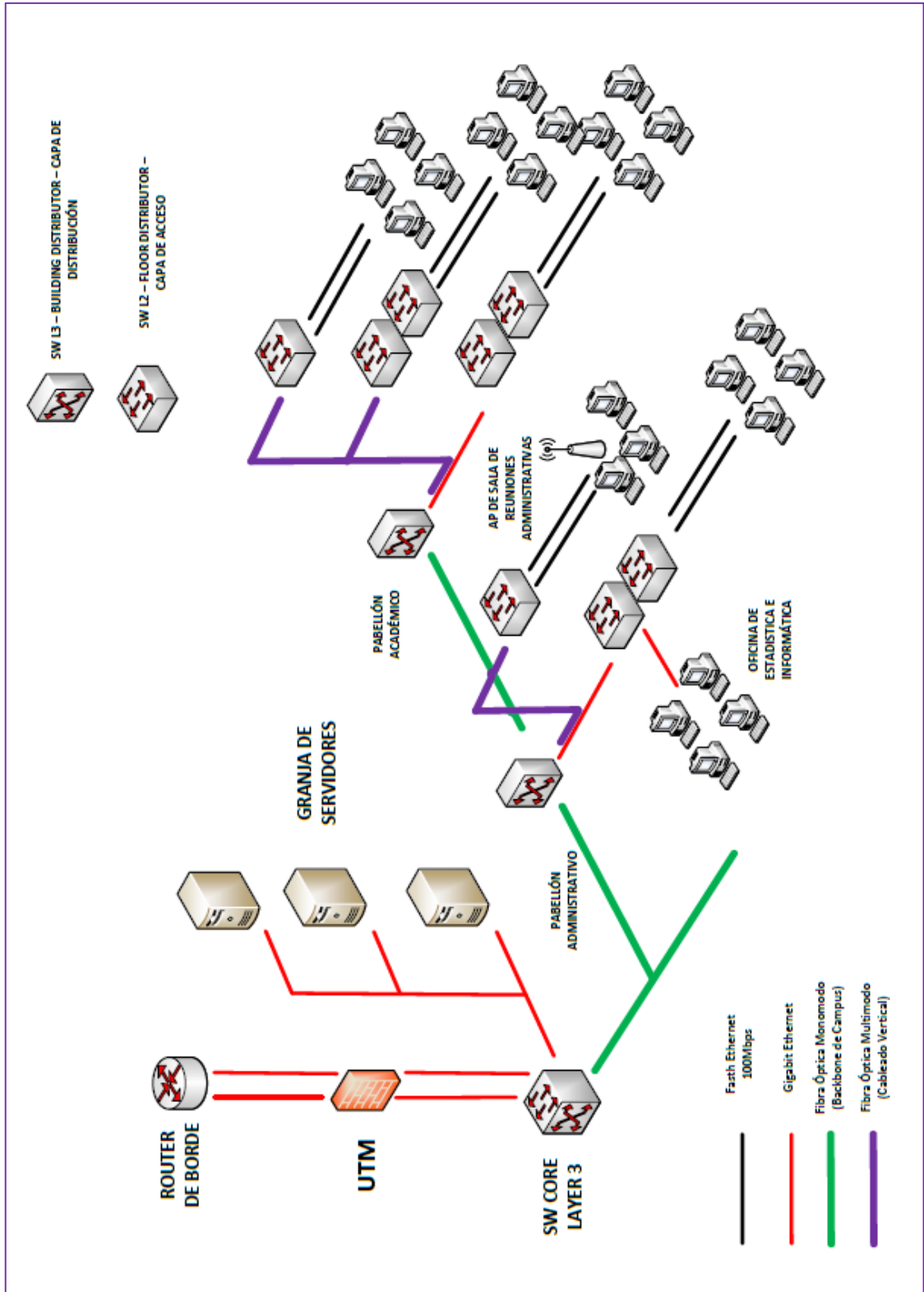


FIGURA 3.21: "MAPA FISICO DE LA RED DE COMUNICACIÓN DE DATOS 1"

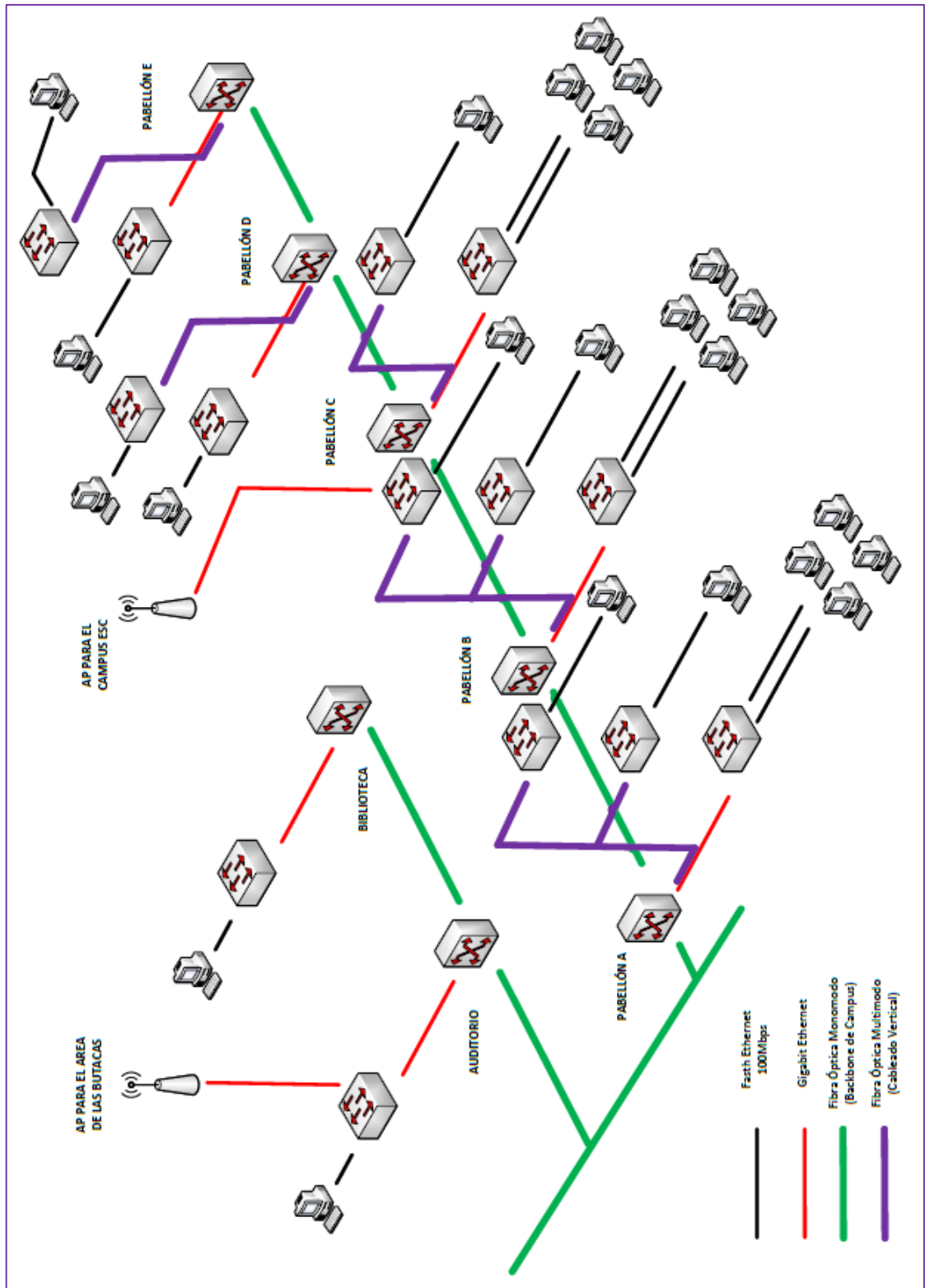


FIGURA 3.22: “MAPA FISICO DE LA RED DE COMUNICACIÓN DE DATOS 2”

Para seguir detallando este Diagrama de Infraestructura física, en la TABLA 3.4 especificaremos que tipo y cuántos puertos necesitara cada Switch en todo el campus.

	<b>EDIFICIO</b>	<b>CANTIDAD MINIMA DE PUERTOS REQUERIDOS PARA EL SW DE EDIFICIO</b>	<b>NIVEL</b>	<b>CANTIDAD MINIMA DE PUERTOS REQUERIDOS PARA EL SW DE NIVEL</b>
1	PABELLÒN ADMINISTRATIVO	1 puerto GigabitEthernet	PRIMER NIVEL	41 puertos FastEthernet 5 puertos GigabitEthernet
2	PABELLÒN ADMINISTRATIVO	2 puertos de F.O	SEGUNDO NIVEL	1 puerto de F.O 25 puertos FastEthernet
3	PABELLÒN ACADEMICO	1 puerto GigabitEthernet	PRIMER NIVEL	1 puerto GigabitEthernet 29 puertos FastEthernet
4	PABELLÒN ACADEMICO	3 puertos de F.O	SEGUNDO NIVEL	1 puerto de F.O 1 puerto GigabitEthernet 77 puertos FastEthernet

5	PABELLÒN ACADEMICO		TERCER NIVEL	1 puerto de F.O 1 puerto GigabitEthernet 10 puertos FastEthernet
6	PABELLON A	1 puerto GigabitEthernet	PRIMER NIVEL	1 puerto GigabitEthernet 26 puertos FastEthernet
7	PABELLON A	3 puertos de F.O	SEGUNDO NIVEL	1 puerto de F.O 1 puerto GigabitEthernet 8 puertos FastEthernet
8	PABELLON A		TERCER NIVEL	1 puerto de F.O 1 puerto GigabitEthernet 37 puertos FastEthernet
9	PABELLON B	1 puerto GigabitEthernet	PRIMER NIVEL	1 puerto GigabitEthernet 46 puertos FastEthernet
10	PABELLON B	3 puertos de F.O	SEGUNDO NIVEL	1 puerto de F.O

				1 puerto GigabitEthernet 8 puertos FastEthernet
1 1	PABELLON B		TERCER NIVEL	1 puerto de F.O 2 puertos GigabitEthernet 37 puertos FastEthernet
1 2	PABELLON C	1 puerto GigabitEthernet	PRIMER NIVEL	1 puerto GigabitEthernet 8 puertos FastEthernet
1 3	PABELLON C	2 puertos de F.O	SEGUNDO NIVEL	1 puerto de F.O 1 puerto GigabitEthernet 37 puertos FastEthernet
1 4	PABELLON D	1 puerto GigabitEthernet	PRIMER NIVEL	1 puerto GigabitEthernet 37 puertos FastEthernet
1 5	PABELLON D	2 puertos de F.O	SEGUNDO NIVEL	1 puerto de F.O 1 puerto GigabitEthernet

				t 37 puertos FastEthernet
16	PABELLON E	1 puerto GigabitEthernet	PRIMER NIVEL	1 puerto GigabitEthernet t 37 puertos FastEthernet
17	PABELLON E	2 puertos de F.O	SEGUNDO NIVEL	1 puerto de F.O 1 puerto GigabitEthernet t 37 puertos FastEthernet
18	BIBLIOTECA	1 puerto GigabitEthernet 1 puertos de F.O	PRIMER NIVEL	1 puerto GigabitEthernet t 34 puertos FastEthernet
20	AUDITORIO	1 puerto GigabitEthernet 1 puertos de F.O	PRIMER NIVEL	2 puertos GigabitEthernet t 3 puertos FastEthernet

TABLA 3.5: "Puertos necesarios en los switches FD y BD"



### **3.3 REVISIÓN Y CONSOLIDACIÓN DE RESULTADOS**

En ésta parte de la investigación se simulará un diseño a escala del que hemos hecho de la Red de Comunicación de Datos de la Institución Educativa Privada Emilio Soyer Cabero. Reuniremos en esta pequeña simulación aspectos importantes y necesarios de la red, logrando así una red a escala que refleje esencialmente como trabajará la red completa, sin detalles innecesarios para explicar su funcionamiento pero logrando mostrar el mismo que la original.

Utilizaremos el software de simulación *Packet Tracer*, el cual es la herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta nos permite crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales.

Cabe resaltar que también estaremos delimitados por las características del mismo software de simulación, ciñéndonos así sus prestaciones. No obstante esto no influirá de manera determinante a la generalización de nuestros resultados debido a que la simulación de la red a escala seguirá manteniendo la misma esencia que la real.

#### **3.3.1 Topología de la Red a escala en Packet Tracer**

En la FIGURA 3.22 se aprecia el modelo a escala de nuestro diseño original. Se observa que aunque no es la red completa, ya es relativamente mediana en tamaño.

Hemos seleccionado partes importantes del diseño, sectores en la topología que son relevantes y necesarios de simular.

Como se aprecia, esta topología sigue el mismo modelo de la real, el router de borde conectado al switch core, y éste conectado a los switches distribuidores de edificios. Se observa que los servidores están directamente conectados al

switch core y que se está dando uso del Access Point ubicado en el pabellón administrativo para uso de los asistentes a la sala de reuniones administrativas.

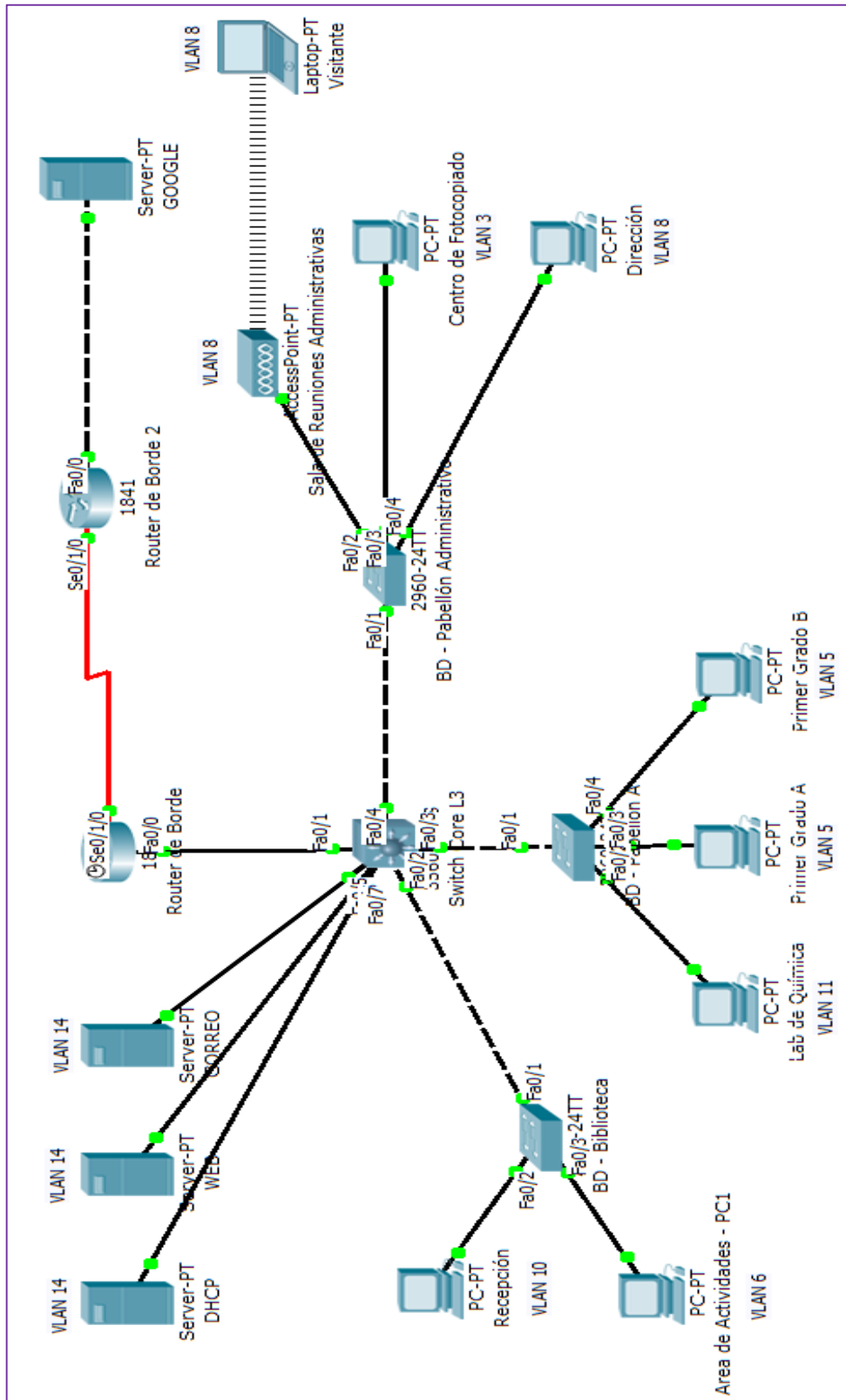


FIGURA 3.22: “Simulación del modelo a escala”

Se observa también que el único tipo de cableado que se ha considerado es el de UTP FastEthernet, esto es por comodidad y característica del mismo simulador pues al final no tiene relevancia para demostrar la lógica de red que tendrá nuestro diseño original.

Finalmente hacemos una conexión del router de borde de la institución educativa con otro router de borde de un buscador muy conocido por medio de un enlace WAN. Esto se hace para representar una conexión con otra LAN a través de la nube de internet por medio de un ISP.

Como se puede apreciar se ha tratado de mantener en todo lo posible la semejanza con el diseño original, la configuración real y la estructura propuesta. Esto se refleja en los hosts, los cuales tienen las direcciones IP calculadas y también la pertenencia a las VLAN ya designadas.

## CONCLUSIONES

- Se ha diseñado una red jerárquica, compuesta por tres capas de trabajo, cada una de ellas se ha tomado en cuenta pensando en la eficacia y escalabilidad que fueron requisitos necesarios antes de iniciar el diseño.
- Se ha tomado en cuenta antes de desarrollar el diseño, aspectos de infraestructura física y organizacional acerca de la Institución Educativa.
- Se han creado VLAN's de trabajo, cada una representando una subred, la cual reúne varias oficinas según el tipo de funciones, grados de seguridad y aspectos de capacidad en el tráfico de datos.
- En la simulación a escala se hacen dos tipos de comunicación, el primero que no es entre VLAN's, es decir dos hosts de diferentes VLAN's no pueden comunicarse entre ellas y por el otro lado uno que es inter-VLAN que sí hace posible que dos hosts de diferentes VLAN's puedan comunicarse.
- Se ha propuesto determinados equipos para cumplir un papel específico, sin embargo estos posibles dispositivos pueden ser reemplazados por otros que cumplan sus mismas características.
- Se ha indicado qué tipo de cableado debe ir para determinadas conexiones utilizando así cables de fibra óptica monomodo, multimodo, cables de cobre FastEthernet y GigaEthernet.
- Queda claro que el software de simulación Packet Tracer es una herramienta que nos ayudará a comprender y verificar que lo esencial de nuestro diseño está funcionando bien. Pero al mismo tiempo debemos ceñirnos a sus limitaciones.
- Se dispondrá de un UPS marca APC modelo SURT5000XLICH el cual alimentara de energía al rack de comunicaciones automáticamente cuando no haya fluido eléctrico por el tiempo aproximado de 8 minutos.

## RECOMENDACIONES

- Cuando se tienen redes organizacionales de este tipo, es recomendable usar un planeamiento jerárquico debido a sus diversas ventajas de administración y funcionamiento.
- Siempre que se vaya a diseñar una red de comunicaciones como ésta, se debe tomar en cuenta aspectos de ubicación geográfica como la distancia entre edificios, tamaño de los mismos y ubicación de las oficinas, tanto como aspectos organizacionales como funciones de las diversas áreas de trabajo, para lograr una visión general y detallada al mismo tiempo de lo que se debe hacer para iniciar el diseño.
- Si en algún momento se desea agregar una VLAN que represente a un grupo de trabajo, se recomienda tener mucho cuidado con el proceso de subneteo, cuidando de escoger bien desde que punto de la segmentación se va a partir y qué clase de direcciones tomar.
- Se recomienda profundamente tener una serie de políticas muy cuidadosas al configurar el UTM, para asegurarnos que hosts pertenecientes a una VLAN determinada puedan comunicarse sólo con los demás hosts de su misma VLAN o puedan comunicarse entre otras VLAN también.
- Cuando se diseñe y se implemente una nueva red informática se debe diseñar en lo posible con equipos activos, (switch, router), de una misma marca de fabricación con la finalidad de poder explotar al máximo todos los beneficios que nos da cada fabricante, porque cuando se utiliza equipos de diferente fabricante algunas características técnicas de un fabricante no son compatibles con las de otro fabricante, pese a que los dos equipos estén estandarizados para realizar una función específica.
- Es muy importante seguir las normas estandarizadas en el aspecto de cableado estructurado para poder garantizar que la comunicación de nuestra red se eficaz y confiable.

- Si cabe la posibilidad, se recomienda hacer uso de un software que permita simular la red de comunicación de una manera más real para así poder observar a más detalle si nuestra red funcionara bien.
- Se recomienda el uso de un grupo electrógeno para proveer de energía al rack de comunicaciones cuando el UPS llegue al máximo de autonomía y aun no se cuente con fluido eléctrico. La elección del grupo electrógeno debe ser un trabajo del especialista en energía o Ing. Eléctrico.

## BIBLIOGRAFÍA

1. Forouzan B. Transmisión de Datos y Redes de Comunicaciones. 4a ed. Madrid: McGraw Hill; 2006.
2. Tanenbaum A. Redes de Computadoras. 4a ed. México: Pentice Hall; 2003.
3. Ruffalo A., Oppenheimer., Woodward B., Brady G. Aspectos básicos de redes, CCNA Exploration Labs y Guía de Estudio. 1a ed. México: Cisco Press; 2008.
4. Morales M. Análisis y Diseño de una Infraestructura de Redes Basado en VLAN's para la Comandancia del Ejército [Tesis]. Quito: Escuela Politécnica Nacional. Escuela de Ingeniería; 2006.
5. Cisco Systems, Inc - Cisco [Internet]. California: CISCO; c1995-2007 [consultado 20 enero 2014]. Disponible en: <http://www.cisco.com//>.

# **ANEXOS**



# **ANEXO 1**

## **NORMAS TÉCNICAS**

## 1. IEEE 802.3

<b>ESTÁNDAR ETHERNET</b>	<b>FECHA</b>	<b>DESCRIPCIÓN</b>
<b>Ethernet experimental</b>	1972 (patentado en 1978) <sup>1</sup>	2,85 Mbit/s sobre cable coaxial en topología de bus.
<b>Ethernet II (DIX v2.0)</b>	1982	10 Mbit/s sobre coaxial fino (thinnet) - La trama tiene un campo de tipo de paquete. El protocolo IP usa este formato de trama sobre cualquier medio.
<b>IEEE 802.3</b>	1983	10BASE5 10 Mbit/s sobre coaxial grueso (thicknet). Longitud máxima del segmento 500 metros - Igual que DIX salvo que el campo de Tipo se substituye por la longitud.
<b>802.3a</b>	1985	10BASE2 10 Mbit/s sobre coaxial fino (thinnet o cheapernet). Longitud máxima del segmento 200 metros.
<b>802.3b</b>	1985	10BROAD36
<b>802.3c</b>	1985	Especificación de repetidores de 10 Mbit/s
<b>802.3d</b>	1987	FOIRL (Fiber-Optic Inter-Repeater Link) enlace de fibra óptica entre repetidores.
<b>802.3e</b>	1987	1BASE5 o StarLAN
<b>802.3i</b>	1990	10BASE-T 10 Mbit/s sobre par trenzado no blindado (UTP). Longitud máxima del segmento 150 metros.

<b>802.3j</b>	1993	10BASE-F 10 Mbit/s sobre fibra óptica. Longitud máxima del segmento 1000 metros.
<b>802.3u</b>	1995	100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet a 100 Mbit/s con auto-negociación de velocidad.
<b>802.3x</b>	1997	Full Duplex (Transmisión y recepción simultáneas) y control de flujo.
<b>802.3y</b>	1998	100BASE-T2 100 Mbit/s sobre par trenzado no blindado (UTP). Longitud máxima del segmento 100 metros
<b>802.3z</b>	1998	1000BASE-X Ethernet de 1 Gbit/s sobre fibra óptica.
<b>802.3ab</b>	1999	1000BASE-T Ethernet de 1 Gbit/s sobre par trenzado no blindado
<b>802.3ac</b>	1998	Extensión de la trama máxima a 1522 bytes (para permitir las "Q-tag") Las Q-tag incluyen información para 802.1Q VLAN y manejan prioridades según el estandar 802.1p.
<b>802.3ad</b>	2000	Agregación de enlaces paralelos. Movido a 802.1AX
<b>802.3ae</b>	2003	Ethernet a 10 Gbit/s ; 10GBASE-SR, 10GBASE-LR
<b>IEEE 802.3af</b>	2003	Alimentación sobre Ethernet (PoE).
<b>802.3ah</b>	2004	Ethernet en la última milla.
<b>802.3ak</b>	2004	10GBASE-CX4 Ethernet a 10 Gbit/s sobre cable bi-axial.

<b>802.3an</b>	2006	10GBASE-T Ethernet a 10 Gbit/s sobre par trenzado no blindado (UTP)
<b>802.3ap</b>	en proceso (borrador)	Ethernet de 1 y 10 Gbit/s sobre circuito impreso.
<b>802.3aq</b>	en proceso (borrador)	10GBASE-LRM Ethernet a 10 Gbit/s sobre fibra óptica multimodo.
<b>802.3ar</b>	en proceso (borrador)	Gestión de Congestión
<b>802.3as</b>	en proceso (borrador)	Extensión de la trama

## 2. IEEE 802.11

La versión original del estándar IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) 802.11 publicada en 1997 especifica dos velocidades de transmisión teóricas de 1 y 2 megabits por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR). IR sigue siendo parte del estándar, si bien no hay implementaciones disponibles.

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

### 802.11a

La revisión 802.11a fue aprobada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 GHz y utiliza 52 subportadoras orthogonal frequency-division multiplexing (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales sin solapa, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede interoperar con

equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

#### 802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el mismo método de acceso definido en el estándar original CSMA/CA. El estándar 802.11b funciona en la banda de 2,4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5,9 Mbits sobre TCP y 7,1 Mbit/s sobre UDP.

#### 802.11 c

Es menos usado que los primeros dos, pero por la implementación que este protocolo refleja. El protocolo 'c' es utilizado para la comunicación de dos redes distintas o de diferentes tipos, así como puede ser tanto conectar dos edificios distantes el uno con el otro, así como conectar dos redes de diferente tipo a través de una conexión inalámbrica. El protocolo 'c' es más utilizado diariamente, debido al costo que implica las largas distancias de instalación con fibra óptica, que aunque más fidedigna, resulta más costosa tanto en instrumentos monetarios como en tiempo de instalación.

"El estándar combinado 802.11c no ofrece ningún interés para el público general. Es solamente una versión modificada del estándar 802.1d que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos capa 2 del modelo OSI)".

#### 802.11d

Es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo móvil.

#### 802.11e

La especificación IEEE 802.11e ofrece un estándar inalámbrico que permite interoperar entre entornos públicos, de negocios y usuarios residenciales, con la capacidad añadida de resolver las necesidades de cada sector. A diferencia de otras iniciativas de conectividad sin cables, ésta puede considerarse como uno de los primeros estándares inalámbricos que permite trabajar en entornos domésticos y empresariales. La especificación añade, respecto de los estándares 802.11b y 802.11a, características QoS y de soporte multimedia, a la vez que mantiene compatibilidad con ellos. Estas prestaciones resultan fundamentales para las redes domésticas y para que los operadores y

proveedores de servicios conformen ofertas avanzadas. El documento que establece las directrices de QoS, aprobado el pasado mes de noviembre, define los primeros indicios sobre cómo será la especificación que aparecerá a finales de 2001. Incluye, asimismo, corrección de errores (FEC) y cubre las interfaces de adaptación de audio y vídeo con la finalidad de mejorar el control e integración en capas de aquellos mecanismos que se encarguen de gestionar redes de menor rango. El sistema de gestión centralizado integrado en QoS evita la colisión y cuellos de botella, mejorando la capacidad de entrega en tiempo crítico de las cargas. Estas directrices aún no han sido aprobadas. Con el estándar 802.11, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:

- (EDCA) Enhanced Distributed Channel Access, equivalente a DCF.
- (HCCA) HCF Controlled Access, equivalente a PCF.

En este nuevo estándar se definen cuatro categorías de acceso al medio (Ordenadas de menos a más prioritarias).

- Background (AC\_BK)
- Best Effort (AC\_BE)
- Video (AC\_VI)
- Voice (AC\_VO)

Para conseguir la diferenciación del tráfico se definen diferentes tiempos de acceso al medio y diferentes tamaños de la ventana de contención para cada una de las categorías.

#### 802.11f

Es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el protocolo IAPP que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como itinerancia.

#### 802.11g

En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g, que es la evolución de 802.11b. Este utiliza la banda de 2,4 Ghz (al igual que 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22,0 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte

del proceso de diseño del nuevo estándar lo tomó el hacer compatibles ambos modelos. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación que fue dada aprox. el 20 de junio del 2003. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas o equipos de radio apropiados.

Existe una variante llamada 802.11g+ capaz de alcanzar los 108Mbps de tasa de transferencia. Generalmente sólo funciona en equipos del mismo fabricante ya que utiliza protocolos propietarios.

Interacción de 802.11g y 802.11b.

802.11g tiene la ventaja de poder coexistir con los estándares 802.11a y 802.11b, esto debido a que puede operar con las Tecnologías RF DSSS y OFDM. Sin embargo, si se utiliza para implementar usuarios que trabajen con el estándar 802.11b, el rendimiento de la celda inalámbrica se verá afectado por ellos, permitiendo solo una velocidad de transmisión de 22 Mbps. Esta degradación se debe a que los clientes 802.11b no comprenden OFDM.

Suponiendo que se tiene un punto de acceso que trabaja con 802.11g, y actualmente se encuentran conectados un cliente con 802.11b y otro 802.11g, como el cliente 802.11b no comprende los mecanismos de envío de OFDM, el cual es utilizado por 802.11g, se presentarán colisiones, lo cual hará que la información sea reenviada, degradando aún más nuestro ancho de banda.

Suponiendo que el cliente 802.11b no se encuentra conectado actualmente, el Punto de acceso envía tramas que brindan información acerca del Punto de acceso y la celda inalámbrica. Sin el cliente 802.11b, en las tramas se verían la siguiente información:

NON\_ERP present: no

Use Protection: no

ERP (Extended Rate Physical), esto hace referencia a dispositivos que utilizan tasas de transferencia de datos extendidos, en otras palabras, NON\_ERP hace referencia a 802.11b. Si fueran ERP, soportarían las altas tasas de transferencia que soportan 802.11g.

Cuando un cliente 802.11b se asocia con el AP (Punto de acceso), éste último alerta al resto de la red acerca de la presencia de un cliente NON\_ERP. Cambiando sus tramas de la siguiente forma:

NON\_ERP present: yes

Use Protection: yes

Ahora que la celda inalámbrica sabe acerca del cliente 802.11b, la forma en la que se envía la información dentro de la celda cambia. Ahora cuando un cliente 802.11g quiere enviar una trama, debe advertir primero al cliente 802.11b enviándole un mensaje RTS (Request to Send) a una velocidad de 802.11b para que el cliente 802.11b pueda comprenderlo. El mensaje RTS es enviado en forma de unicast. El receptor 802.11b responde con un mensaje CTS (Clear to Send).

Ahora que el canal está libre para enviar, el cliente 802.11g realiza el envío de su información a velocidades según su estándar. El cliente 802.11b percibe la información enviada por el cliente 802.11g como ruido.

La intervención de un cliente 802.11b en una red de tipo 802.11g, no se limita solamente a la celda del Punto de acceso en la que se encuentra conectado, si se encuentra trabajando en un ambiente con múltiples AP en Roaming, los AP en los que no se encuentra conectado el cliente 802.11b se transmitirán entre sí tramas con la siguiente información:

NON\_ERP present: no

Use Protection: yes

La trama anterior les dice que hay un cliente NON\_ERP conectado en uno de los AP, sin embargo, al tenerse habilitado Roaming, es posible que éste cliente 802.11b se conecte en alguno de ellos en cualquier momento, por lo cual deben utilizar los mecanismo de seguridad en toda la red inalámbrica, degradando de esta forma el rendimiento de toda la celda. Es por esto que los clientes deben conectarse preferentemente utilizando el estándar 802.11g. Wi-Fi (802.11b / g)

#### 802.11h

La especificación 802.11h es una modificación sobre el estándar 802.11 para WLAN desarrollado por el grupo de trabajo 11 del comité de estándares LAN/MAN del IEEE (IEEE 802) y que se hizo público en octubre de 2003. 802.11h intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de Radar o Satélite.

El desarrollo del 802.11h sigue unas recomendaciones hechas por la ITU que fueron motivadas principalmente a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones (ERO) estimó convenientes para minimizar el impacto de abrir la banda de 5 GHz, utilizada generalmente por sistemas militares, a aplicaciones ISM (ECC/DEC/(04)08).

Con el fin de respetar estos requerimientos, 802.11h proporciona a las redes 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión.

#### Selección Dinámica de Frecuencias y Control de Potencia del Transmisor

DFS (Dynamic Frequency Selection) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz con el fin de evitar interferencias co-



canal con sistemas de radar y para asegurar una utilización uniforme de los canales disponibles.

TPC (Transmitter Power Control) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz para asegurar que se respetan las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite.

#### 802.11i

Está dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (Estándar de Cifrado Avanzado). Se implementa en WPA2.

#### 802.11j

Es equivalente al 802.11h, en la regulación Japonesa

#### 802.11k

Permite a los conmutadores y puntos de acceso inalámbricos calcular y valorar los recursos de radiofrecuencia de los clientes de una red WLAN, mejorando así su gestión. Está diseñado para ser implementado en software, para soportarlo el equipamiento WLAN sólo requiere ser actualizado. Y, como es lógico, para que el estándar sea efectivo, han de ser compatibles tanto los clientes (adaptadores y tarjetas WLAN) como la infraestructura (puntos de acceso y conmutadores WLAN).

#### 802.11n

En enero de 2004, el IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 300 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y unas 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO Multiple Input – Multiple Output, que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas (3). Existen también otras propuestas alternativas que podrán ser consideradas. El estándar ya está redactado, y se viene implantando desde 2008. A principios de 2007 se aprobó el segundo boceto del estándar. Anteriormente ya había dispositivos adelantados al protocolo y que ofrecían de forma no oficial este estándar (con la promesa de actualizaciones para cumplir

el estándar cuando el definitivo estuviera implantado). Ha sufrido una serie de retrasos y el último lo lleva hasta noviembre de 2009. Habiéndose aprobado en enero de 2009 el proyecto 7.0 y que va por buen camino para cumplir las fechas señaladas. A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

El estándar 802.11n fue ratificado por la organización IEEE el 11 de septiembre de 2009 con una velocidad de 600 Mbps en capa física.

En la actualidad la mayoría de productos son de la especificación b o g, sin embargo ya se ha ratificado el estándar 802.11n que sube el límite teórico hasta los 600 Mbps. Actualmente ya existen varios productos que cumplen el estándar N con un máximo de 300 Mbps (80-100 estables).

El estándar 802.11n hace uso simultáneo de ambas bandas, 2,4 Ghz y 5 Ghz. Las redes que trabajan bajo los estándares 802.11b y 802.11g, tras la reciente ratificación del estándar, se empiezan a fabricar de forma masiva y es objeto de promociones por parte de los distintos ISP, de forma que la masificación de la citada tecnología parece estar en camino. Todas las versiones de 802.11xx, aportan la ventaja de ser compatibles entre sí, de forma que el usuario no necesitará nada más que su adaptador wifi integrado, para poder conectarse a la red.

Sin duda esta es la principal ventaja que diferencia wifi de otras tecnologías propietarias, como LTE, UMTS y Wimax, las tres tecnologías mencionadas, únicamente están accesibles a los usuarios mediante la suscripción a los servicios de un operador que está autorizado para uso de espectro radioeléctrico, mediante concesión de ámbito nacional.

La mayor parte de los fabricantes ya incorpora a sus líneas de producción equipos wifi 802.11n, por este motivo la oferta ADSL, ya suele venir acompañada de wifi 802.11n, como novedad en el mercado de usuario doméstico.

Se conoce que el futuro estándar sustituto de 802.11n será 802.11ac con tasas de transferencia superiores a 1 Gb/s.

802.11p

Este estándar opera en el espectro de frecuencias de 5,90 GHz y de 6,20 GHz, especialmente indicado para automóviles. Será la base de las comunicaciones dedicadas de corto alcance (DSRC) en Norteamérica. La tecnología DSRC permitirá el intercambio de datos entre vehículos y entre automóviles e infraestructuras en carretera.

802.11r

También se conoce como Fast Basic Service Set Transition, y su principal característica es permitir a la red que establezca los protocolos de seguridad que identifican a un dispositivo en el nuevo punto de acceso antes de que abandone

el actual y se pase a él. Esta función, que una vez enunciada parece obvia e indispensable en un sistema de datos inalámbricos, permite que la transición entre nodos demore menos de 50 milisegundos. Un lapso de tiempo de esa magnitud es lo suficientemente corto como para mantener una comunicación vía VoIP sin que haya cortes perceptibles.

802.11v

IEEE 802.11v servirá para permitir la configuración remota de los dispositivos cliente. Esto permitirá una gestión de las estaciones de forma centralizada (similar a una red celular) o distribuida, a través de un mecanismo de capa 2. Esto incluye, por ejemplo, la capacidad de la red para supervisar, configurar y actualizar las estaciones cliente. Además de la mejora de la gestión, las nuevas capacidades proporcionadas por el 11v se desglosan en cuatro categorías: mecanismos de ahorro de energía con dispositivos de mano VoIP Wi-Fi en mente; posicionamiento, para proporcionar nuevos servicios dependientes de la ubicación; temporización, para soportar aplicaciones que requieren un calibrado muy preciso; y coexistencia, que reúne mecanismos para reducir la interferencia entre diferentes tecnologías en un mismo dispositivo.

802.11w

Todavía no concluido. TGw está trabajando en mejorar la capa del control de acceso del medio de IEEE 802.11 para aumentar la seguridad de los protocolos de autenticación y codificación. Las LANs inalámbricas envían la información del sistema en tramas desprotegidas, que los hace vulnerables. Este estándar podrá proteger las redes contra la interrupción causada por los sistemas malévolos que crean peticiones desasociadas que parecen ser enviadas por el equipo válido. Se intenta extender la protección que aporta el estándar 802.11i más allá de los datos hasta las tramas de gestión, responsables de las principales operaciones de una red. Estas extensiones tendrán interacciones con IEEE 802.11r e IEEE 802.11u.

# **ANEXO 2**

## **DATASHEETS**

# Cisco 1921 Series Integrated Services Routers

Product Names: CISCO 1921/K9, CISCO 1921-SEC/K9, and CISCO 1921DC/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 1921 builds on the best-in-class offering of the Cisco 1841 Integrated Services Routers. All Cisco 1900 Series Integrated Services Routers offer embedded hardware encryption acceleration, optional firewall, intrusion prevention, and advanced security services. In addition, the platforms support the industry's widest range of wired and wireless connectivity options such as Serial, T1/E1, xDSL, Gigabit Ethernet, and third-generation (3G) wireless (Figure 1).

Figure 1. Cisco 1921 Integrated Services Router



## Key Business Benefits

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 1900.

Table 1. Key Features and Benefits of the Cisco 1921 Integrated Services Router

Benefits	Description
<b>Service integration</b>	<ul style="list-style-type: none"> <li>The Cisco 1921 offers increased levels of services integration with data, security, wireless, and mobility services, enabling greater efficiencies and cost savings.</li> </ul>
<b>Services on demand</b>	<ul style="list-style-type: none"> <li>A single Cisco IOS Software Universal image is installed on each 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.</li> </ul>
<b>High performance with integrated services</b>	<ul style="list-style-type: none"> <li>The Cisco 1900 Series enables deployment in high-speed WAN environments with concurrent services enabled up to 15 Mbps.</li> </ul>

Benefits	Description
<b>Network agility</b>	<ul style="list-style-type: none"> <li>Designed to address customer business requirements, the Cisco 1921 with the modular architecture offers a performance range of modular interfaces and services as your network needs grow.</li> <li>Modular interfaces offer increased bandwidth, a diversity of connection options, and network resiliency.</li> </ul>
<b>Energy efficiency</b>	<ul style="list-style-type: none"> <li>The Cisco 1921 architecture provides energy-savings features that include the following: <ul style="list-style-type: none"> <li>The Cisco 1900 Series offers intelligent power management and allows you to control power to the modules based on the time of day. Cisco EnergyWise technology will be supported in the future.</li> <li>Services integration and modularity on a single platform performing multiple functions optimizes raw-materials consumption and energy usage.</li> <li>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.</li> <li>High-efficiency power supplies are provided with each platform.</li> <li>DC Power option available (CISCO1921DC/K9).</li> </ul> </li> </ul>
<b>Investment protection</b>	<ul style="list-style-type: none"> <li>The Cisco 1921 maximizes investment protection: <ul style="list-style-type: none"> <li>Reuse of a broad array of existing modules supported on the original ISRs provides a lower TCO.</li> <li>A rich set of Cisco IOS Software features is carried forward from the original ISRs and delivered in the Universal image.</li> <li>This router gives you the flexibility to grow as your business needs evolve.</li> </ul> </li> </ul>

## Architecture and Modularity

The Cisco 1921 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 PoE and Cisco Enhanced PoE (ePoE). Table 2 lists the architectural features and benefits of the Cisco 1921.

**Table 2.** Architectural Features and Benefits


Architectural Feature	Benefits
<b>Modular platform</b>	<ul style="list-style-type: none"> <li>The Cisco 1921 ISRs are highly modular platforms with multiple module slots to provide connectivity and services for varied branch-office network requirements.</li> <li>The ISRs offer an industry-leading breadth of LAN and WAN connectivity options through modules to accommodate field upgrades to future technologies without requiring replacement of the platform.</li> </ul>
<b>Processors</b>	<ul style="list-style-type: none"> <li>The Cisco 1921 is powered by high-performance multicore processors that support growing demands of branch-office networks by supporting high-throughput WAN requirements.</li> </ul>
<b>Embedded IP Security/Secure Sockets Layer (IPsec/SSL) VPN hardware acceleration</b>	<ul style="list-style-type: none"> <li>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).</li> <li>The onboard encryption hardware outperforms the advanced integration modules (AIMs) of previous generations.</li> </ul>
<b>Integrated Gigabit Ethernet ports</b>	<ul style="list-style-type: none"> <li>All onboard LAN and WAN ports are 10/100/1000 Gigabit Ethernet routed ports.</li> </ul>
<b>Innovative universal-serial-bus (USB)-based console access</b>	<ul style="list-style-type: none"> <li>A new, innovative, mini-Type B USB console port supports management connectivity when traditional serial ports are not available.</li> <li>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.</li> </ul>
<b>Optional external power supply for distribution of PoE</b>	<ul style="list-style-type: none"> <li>An optional upgrade to the power supply provides inline power (802.3af-compliant PoE) and Cisco Standard Inline Power to optional integrated switch modules.</li> </ul>

## Modularity Features and Benefits

The Cisco 1921 provides significantly enhanced modular capabilities (refer to Table 3) that offer you investment protection. Most of the modules available on previous generations of Cisco routers, such as the Cisco 1841 ISR, are supported on the Cisco 1921. Additionally, you can easily interchange modules used on the Cisco 1921 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.

A complete list of supported modules is available at <http://www.cisco.com/go/1921>.

**Table 3.** Modularity Features and Benefits

Feature	Benefits
<p><b>Cisco Enhanced High-Speed WAN Interface Card (EHWIC)</b></p> 	<ul style="list-style-type: none"> <li>• The EHWIC slot replaces the high-speed WAN interface card (HWIC) slot and can natively support HWICs, WAN interface cards (WICs), and voice/WAN interface cards (VWICs).</li> <li>• Two integrated EHWIC slots are available on the Cisco 1921 for flexible configurations for support of two modules: One doublewide HWIC-D or two singlewide EHWIC/HWIC modules are supported.</li> <li>• Each EHWIC slot offers high-data-throughput capability.</li> </ul>
<b>USB 2.0 ports</b>	<ul style="list-style-type: none"> <li>• One high-speed USB 2.0 port is supported. The USB port enables another mechanism for secure-token capabilities and storage.</li> </ul>

## Cisco IOS Software

The Cisco 1921 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.

Four major technology licenses are available on the Cisco 1921 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 1921 Integrated Services Routers, please visit <http://www.cisco.com/go/1921>.

## 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 and operational expenses.

---

## **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 ISRs 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 1921 offers native hardware-based encryption acceleration to provide greater IPsec throughput with less overhead for the router processor when compared with software-based encryption solutions. Cisco ISRs 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 ScanSafe Web Security 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 ISRs, please visit <http://www.cisco.com/go/3g>.

### **Integrated LAN Switching**

The Cisco 1921 Integrated Services Router will support the EHWIC LAN modules when they become available in the future. The Cisco 1921 supports the existing singlewide Cisco EtherSwitch® HWIC and the doublewide HWIC-D modules, which greatly expand 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 expenditures (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 operating expense (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.

Tables 4 through 6 give details about Cisco IOS software feature and protocol support, Cisco IOS software management capabilities, and Cisco Network Management applications for Cisco 1921 Integrated Services Routers.

**Table 4.** Cisco 1921 with Cisco IOS Software Feature and Protocol High-Level Support

Feature	Description
<b>Protocols</b>	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 (BFD), IPv4-to-IPv6 Multicast, MPLS, Layer 2 Tunneling Protocol Version 3 (L2TPv3), 802.1ag, 802.3ah, and Layer 2 and Layer 3 VPN.
<b>Encapsulations</b>	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.
<b>Traffic management</b>	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).

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
<a href="#">WSMA</a>	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.
<a href="#">EEM</a>	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.
<a href="#">IPSLA</a>	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.
<a href="#">SNMP</a> , <a href="#">RMON</a> , <a href="#">syslog</a> , <a href="#">NetFlow</a> , and <a href="#">TR-069</a>	Cisco 1900 Series ISRs 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	<a href="#">Cisco Configuration Professional</a>	<ul style="list-style-type: none"> <li>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.</li> </ul>
Networkwide deployment, configuration, monitoring, and troubleshooting	<a href="#">CiscoWorks LMS</a>	<ul style="list-style-type: none"> <li>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 ISRs, using new instrumentation such as Cisco IOS EEM.</li> <li>In addition to supporting basic platform services of the ISR, CiscoWorks also provides added-value support for the Cisco Services-Ready Engine (SRE) by enabling the management and distribution of software images to the SRE, thereby reducing the time and complexities associated with image management.</li> </ul>
Networkwide staging, configuration, and compliance	<a href="#">CiscoWorks NCM</a>	<ul style="list-style-type: none"> <li>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.</li> </ul>
Security staging, configuration, and monitoring	<a href="#">Cisco Security Manager</a>	<ul style="list-style-type: none"> <li>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.</li> </ul>
Configuration and provisioning	<a href="#">Cisco Unified Provisioning Manager</a>	<ul style="list-style-type: none"> <li>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.</li> </ul>
Staging, deployment, and changes of licenses	<a href="#">Cisco License Manager</a>	<ul style="list-style-type: none"> <li>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.</li> </ul>
Staging, deployment, and changes to configuration and image files	<a href="#">Cisco Configuration Engine</a>	<ul style="list-style-type: none"> <li>Cisco Configuration Engine is a secure network management product that provides zero-touch image and configuration distribution through centralized, template-based management.</li> </ul>

## 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 1921 offers these solutions by providing enhanced performance and increased modular density to support multiple services. The Cisco 1921 is designed to consolidate the functions of separate devices into a single, compact system that can be remotely managed. Table 7 gives specifications of the Cisco 1921.

## Product Specifications

**Table 7.** Product Specifications of Cisco 1921 Integrated Services Router

	Cisco 1921 Integrated Services Router
<b>Services and Slot Density</b>	
Embedded hardware-based cryptography acceleration (IPsec + SSL)	Yes
RJ-45 onboard LAN/WAN 10/100/1000 ports	2
EHWIC slots	2
Doublewide EHWIC slots (use of a doublewide EHWIC slot will consume 2 EHWIC slots)	1
Cisco Integrated Services Module (ISM) slots	0
Memory (DDR2 DRAM): Default/maximum	512 MB/512 MB
USB flash memory (internal): Default/maximum	256 MB/256 MB
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 and DC power-supply models
Power-supply options	POE (external) - on AC models only
Redundant-power-supply support	No
<b>Power Specifications</b>	
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
DC power input	32-60 VDC, 4A, positive or negative, single source
DC input wire size	AWG 14 (2.0 mm <sup>2</sup> )
Safety ground-wire size	AWG 14 (2.0 mm <sup>2</sup> ), minimum
Wire terminal (lug)	Amp/Tyco No.32957
Overcurrent protection	20A maximum
<b>Physical Specifications</b>	
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)	6.75 lb
Weight: With PoE power supply (no modules)	7.5 lb
Airflow	Back to sides

Cisco 1921 Integrated Services Router	
<b>Environmental Specifications</b>	
<b>Operating Conditions</b>	
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	10,000 ft (3,000m)
Humidity	10 to 85% relative humidity (RH)
Acoustic: Sound pressure (typical/maximum)	32.99/58.33 dBA
Acoustic: Sound power (typical/maximum)	41.99/67.22 dBA
<b>Transportation and Storage Conditions</b>	
Temperature	-40 to 158°F (-40 to 70°C)
Humidity	5 to 95% RH
Altitude	15,000 ft (4,570m)
<b>Regulatory Compliance</b>	
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

Cisco 1921 Integrated Services Routers support a wide range of modules that span industry-leading breadths of services at the branch office. Please refer to the following link for the list of modules supported on the Cisco 1900: [http://www.cisco.com/en/US/products/ps10538/products\\_relevant\\_interfaces\\_and\\_modules.html](http://www.cisco.com/en/US/products/ps10538/products_relevant_interfaces_and_modules.html).

## Ordering Information

For more information about the Cisco 1900 Series, visit <http://www.cisco.com/go/1921>.

Table 8 gives ordering information for the Cisco 1921 Router; also refer to the [Cisco Ordering Home Page](#). For information about how to order the Cisco 1900 Series, please visit the Cisco 1900 Series Ordering Guide. 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 1921 Basic Ordering Information

Product Number	Product Description
<b>Cisco1921/K9</b>	Cisco 1921 with 2 onboard GE, 2 EHWIC slots, 256MB USB Flash (internal) 512MB DRAM, IP Base Lic
<b>Cisco1921-SEC/K9</b>	Cisco 1921 with 2 onboard GE, 2 EHWIC slots, 256MB USB Flash (internal) 512MB DRAM, SEC Feature Lic
<b>Cisco1921DC/K9</b>	Cisco 1921 Modular Router DC Power,2GE,2EHWICslots,512MB, IP Base
<b>C1921-AX/K9</b>	Cisco 1921 Router, 256MB CF, 512MB DRAM, IP Base, SEC, AX
<b>C1921-4G-V-SEC/K9</b>	C1921 4G LTE 700MHz (B13) For Verizon Networks with security
<b>Cisco1921-T1SEC/K9</b>	Cisco 1921 SEC T1 bundle with HWIC-1DSU-T1, 256F/512D, IOS SEC Lic
<b>C1921-VA/K9</b>	Cisco 1921 ISR with EHWIC-VA-DSL-A bundle
<b>C1921VAM/K9</b>	Cisco 1921 ISR with Multimode EHWIC for VDSL/ADSL2+ Annex M
<b>C1921-4SHDSL-EA/K9</b>	Cisco 1921 4pair Double Wide EHWIC-4SHDSL-EA bundle, IP Base
<b>PWR-1900-POE</b>	POE Power Adapter for Cisco1921

To download the Cisco 1921 with Cisco IOS Software, go to [Download Software](#), click "Router Software", and go to "Cisco ISR 1921 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 Office

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<sup>®</sup> 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](http://www.cisco.com/go/offices).

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

# 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
<b>Scalability</b>	
<b>3, 4, 6, 9, 9-V and 13-slot modular chassis</b>	Allows flexibility and room for future growth
<b>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.</b>	Scales the system capacity for future needs
<b>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 Tbpps of system capacity.</b>	
<b>High interface capacity</b>	Scales to high-density 40 Gigabit Ethernet, 10 Gigabit Ethernet and Gigabit Ethernet configurations
<b>Increased resiliency</b>	
<b>Standby fabric hot sync</b>	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
<b>Redundant control channel</b>	Increases resiliency to protect against backplane control channel failures
<b>Redundant supervisor engine option</b>	Increases availability with redundant supervisor engine options
<b>Redundant power supply option</b>	Supports redundant power supplies for increased availability
<b>Fan tray</b>	Supports hot-swappable fan tray The 6509-V-E provides for redundant, hot-swappable fan trays
<b>Environmental</b>	
<b>Side-to-side airflow (except Cisco Catalyst 6509-V-E)</b>	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
<b>AC and DC power supply</b>	Supports both AC and DC power supply options, including AC and DC mixing
<b>Network Equipment Building Standards Layer 3 (NEBS L3) compliant</b>	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
<b>Number of Slots</b>	3	4	6	9	9	13
<b>Supervisor Compatibility</b>	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					
<b>Power Supply Compatibility</b> * 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
<b>Module Compatibility</b>	All modules based on the software release in the system					



	6503-E	6504-E	6506-E	6509-E	6509-V-E	6513-E
<b>Software Compatibility</b> (Minimum Software Version)						
<b>With Supervisor Engine 32</b>	• 12.2(18)SXF	• 12.2(18)SXF	• 12.2(18)SXF	• 12.2(18)SXF	• 12.2(18)SXF10	• 12.2(33)SX11 • 12.2(33)SXH2 • 12.2(18)SXF14
<b>With Supervisor Engine 720</b>	• 12.2(14)SX	• 12.2(18)SXE	• 12.2(14)SX	• 12.2(14)SX	• 12.2(18)SXF10	• 12.2(33)SX11 • 12.2(33)SXH2 • 12.2(18)SXF14
<b>With Supervisor Engine 720-10 GE</b>	• 12.2(33)SXH	• 12.2(33)SXH	• 12.2(33)SXH	• 12.2(33)SXH	• 12.2(33)SXH	• 12.2(33)SX11 • 12.2(33)SXH2
<b>With Supervisor Engine 2T-10 GE</b>	• 15.0(1)SY	• 15.0(1)SY	• 15.0(1)SY	• 15.0(1)SY	• 15.0(1)SY	• 15.0(1)SY
<b>Reliability and Availability</b> Calculated Mean Time Between Failure (MTBF)	860,868	677,643	441,418	348,935	330,888	311,778
<b>MIBS</b>	Check the corresponding supervisor engine data sheet					
<b>Network Management</b>	Check the corresponding supervisor engine data sheet					
<b>Physical Dimensions</b>						
<b>Inches</b>	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
<b>Centimeters</b>	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
<b>Rack Units (RU)</b>	4	5	11	14	21	19
<b>Weight</b>						
<b>Chassis Only (lbs)</b>	33	40	50	60	121	102
<b>Fully Configured (lbs)</b>	85.4	97	159	190	270	280
<b>Input Voltage</b>	100 to 240 VAC -48 to -60 VDC					
<b>Safety</b>	UL 60950 Second Edition CAN/CSA-C22.2 No. 60950 Second Edition EN 60950 Second Edition IEC 60950 Second Edition AS/NZS 60950					
<b>EMC</b>	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					
<b>NEBS/ETSI</b>	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
<b>ATIS Pb free and Energy Efficiency</b>	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)					
<b>Operating Environment</b>						
<b>Operating Temperature</b>	32°F to 104°F (0 to 40°C)					
<b>Storage Temperature</b>	-4 to 149°F (-20 to 65°C)					
<b>Thermal Transition</b>	0.5°C per minute (hot to cold) 0.33°C per minute (cold to hot)					
<b>Relative Humidity</b>	Ambient (noncondensing) operating: 5% to 90% Ambient (noncondensing) nonoperating and storage: 5% to 95%					
<b>Operating Altitude</b>	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](http://www.cisco.com/go/offices).

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

# Cisco Catalyst 3750X-24P-S (WS-C3750X-24P-S)

## Catalyst 3750X 24P-S Managed 24-port Switch



### Price details:

Price excl. VAT: 3,141.39 €

Eco fees: 0.00 €

VAT 21 %: 659.69 €

### Product details:

Product code: WS-C3750X-24P-S

EAN: 0882658330544

Manufacturer: Cisco

**3,801.08 €**

\* VAT included

PDF generated on: 17 March, 2014



Cisco is pleased to introduce the new Cisco Catalyst 3750-X and 3560-X Series Switches. The Cisco Catalyst 3750-X and 3560-X Series Switches are an enterprise-class lines of stackable and standalone switches, respectively. These switches provide high availability, scalability, security, energy efficiency, and ease of operation with innovative features such as Cisco StackPower, IEEE 802.3at Power over Ethernet Plus (PoE+) configurations, optional network modules, redundant power supplies, and Media Access Control Security (MACsec) features.

The Cisco Catalyst 3750-X Series with StackWise Plus technology provides scalability, ease of management and investment protection for the evolving business needs. The Cisco Catalyst 3750-X and 3560-X enhance productivity by enabling applications such as IP telephony, wireless, and video for borderless network experience.

### Main specifications:

#### Management features

Switch type:	Managed
Quality of Service (QoS) support:	Y
Multicast support:	Y

#### Ports & interfaces

Basic switching RJ-45 Ethernet ports quantity:	24
SFP/SFP+ slots quantity:	4

#### Networking

Full duplex:	Y
Link aggregation:	Y
Broadcast storm control:	Y
DHCP client:	Y
DHCP server:	Y
IGMP snooping:	Y
Auto MDI/MDI-X:	Y
Spanning tree protocol:	Y

#### Data transmission

Supported data transfer rates:	10/100/1000 Mbps
Switching capacity:	160 Gbit/s
Maximum data transfer rate:	10 Gbit/s
Jumbo frames support:	Y

#### Security

MAC address filtering:	Y
SSH/SSL support:	Y

#### Protocols

Management protocols:	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP
-----------------------	---

Data link protocols:	Ethernet, Fast Ethernet, Gigabit Ethernet
<b>Weight &amp; dimensions</b>	
Weight:	7200 g
<b>Technical details</b>	
Rack mounting:	Y
Stackable:	Y
Colour of product:	Silver
Form factor:	1U
<b>Certificates</b>	
Certification:	FCC Part 15 (CFR 47) Class AICES-003 Class AEN 55022 Class ACISPR 22 Class AAS/NZS 3548 Class ABSMI Class A (AC input models only)VCCI Class AEN 55024, EN300386, EN 50082-1, EN 61000-3-2, EN 61000-3-3EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN 61000-6-1
<b>Operational conditions</b>	
Operating temperature (T-T):	-5 - 40 °C
Storage temperature (T-T):	-40 - 70 °C
Operating relative humidity (H-H):	5 - 95 %
Operating altitude:	0 - 3000 m
Non-operating altitude:	0 - 15000 m
Non-operating relative humidity (non-condensing):	5 - 95 %
<b>Memory</b>	
Internal memory:	256 MB
Flash memory:	128 MB
<b>Illumination/Alarms</b>	
LED indicators:	Y
<b>Power over Ethernet (PoE)</b>	
Power over Ethernet (PoE) support:	N
<b>Other features</b>	
Dimensions (WxDxH):	445 x 460 x 44.5 mm
Connectivity technology:	Wired
Power supply:	715 W
Power supply type:	AC
Connectivity LEDs:	Y
Input frequency:	50/60 Hz
Input voltage:	100 - 240 V

\*PLEASE NOTE: Every effort has been made to ensure the accuracy of all information contained herein. Lasystems makes no warranty expressed or implied with respect to accuracy of the information, including price, editorials or specifications. Lasystems or its suppliers shall not be liable for incidental, consequential or special damages arising from, or as a result of, any electronic transmission or the accuracy of the information contained herein, even if Lasystems has been advised of the possibility of such damages. Product and manufacturer names are used only for the purpose of identification.

## Cisco Catalyst 2960-X Series Switches

Cisco® Catalyst® 2960-X Series Switches are fixed-configuration, stackable Gigabit Ethernet switches that provide enterprise-class access for campus and branch applications (Figure 1). Designed for operational simplicity to lower total cost of ownership, they enable scalable, secure and energy-efficient business operations with intelligent services and a range of advanced Cisco IOS® Software features.

**Figure 1.** A Cisco Catalyst 2960-X Series Switch Family



### Product Highlights

Cisco Catalyst 2960-X switches feature:

- 24 or 48 Gigabit Ethernet ports with line-rate forwarding performance
- Gigabit Small Form-Factor Pluggable (SFP) or 10G SFP+ uplinks
- FlexStack Plus for stacking of up to 8 switches with 80 Gbps of stack throughput (optional)
- Power over Ethernet Plus (PoE+) support with up to 740W of PoE budget
- Reduced power consumption and advanced energy management features
- USB and Ethernet management interfaces for simplified operations
- Application visibility and capacity planning with integrated NetFlow-Lite
- LAN Base or LAN Lite Cisco IOS® software features
- Enhanced limited lifetime warranty (E-LLW) offering next-business-day hardware replacement

Cisco Catalyst 2960-XR models also offer:

- Power resiliency with optional dual field-replaceable power supplies
- IP Lite Cisco IOS® software with dynamic routing and Layer 3 features

## Switch Models and Configurations

Catalyst 2960-X switches include a single fixed power supply and are available with either the Cisco IOS LAN Base or LAN Lite feature set. Catalyst 2960-XR switch models include a field-replaceable modular power supply and can accommodate a second power supply. Catalyst 2960-XR is available only with the Cisco IOS IP Lite feature set.

**Table 1.** Cisco Catalyst 2960-X Configurations

Model	10/100/1000 Ethernet Ports	Uplink Interfaces	Cisco IOS Software Image	Available PoE Power	FlexStack-Plus Capability
Cisco Catalyst 2960X-48FPD-L	48	2 SFP+	LAN Base	740W	√
Cisco Catalyst 2960X-48LPD-L	48	2 SFP+	LAN Base	370W	√
Cisco Catalyst 2960X-24PD-L	24	2 SFP+	LAN Base	370W	√
Cisco Catalyst 2960X-48TD-L	48	2 SFP+	LAN Base	-	√
Cisco Catalyst 2960X-24TD-L	24	2 SFP+	LAN Base	-	√
Cisco Catalyst 2960X-48FPS-L	48	4 SFP	LAN Base	740W	√
Cisco Catalyst 2960X-48LPS-L	48	4 SFP	LAN Base	370W	√
Cisco Catalyst 2960X-24PS-L	24	4 SFP	LAN Base	370W	√
Cisco Catalyst 2960X-24PSQ-L	24 (8PoE)	2 SFP, 2 10/100/1000BT	LAN Base	92W	
Cisco Catalyst 2960X-48TS-L	48	4 SFP	LAN Base	-	√
Cisco Catalyst 2960X-24TS-L	24	4 SFP	LAN Base	-	√
Cisco Catalyst 2960X-48TS-LL	48	2 SFP	LAN Lite	-	-
Cisco Catalyst 2960X-24TS-LL	24	2 SFP	LAN Lite	-	-

**Table 2.** Cisco Catalyst 2960-XR Configurations

Model	10/100/1000 Ethernet Ports	Uplink Interfaces	Cisco IOS Software Image	Available PoE Power	Power Supply
Cisco Catalyst 2960XR-48FPD-I	48	2 SFP+	IP Lite	740W	1025WAC
Cisco Catalyst 2960XR-48LPD-I	48	2 SFP+	IP Lite	370W	640WAC
Cisco Catalyst 2960XR-24PD-I	24	2 SFP+	IP Lite	370W	640WAC
Cisco Catalyst 2960XR-48TD-I	48	2 SFP+	IP Lite	-	250WAC
Cisco Catalyst 2960XR-24TD-I	24	2 SFP+	IP Lite	-	250WAC
Cisco Catalyst 2960XR-48FPS-I	48	4 SFP	IP Lite	740W	1025WAC
Cisco Catalyst 2960XR-48LPS-I	48	4 SFP	IP Lite	370W	640WAC
Cisco Catalyst 2960XR-24PS-I	24	4 SFP	IP Lite	370W	640WAC
Cisco Catalyst 2960XR-48TS-I	48	4 SFP	IP Lite	-	250WAC
Cisco Catalyst 2960XR-24TS-I	24	4 SFP	IP Lite	-	250WAC

## Catalyst 2960-X series Software Features

All Catalyst 2960-X Series Switches use a single Universal Cisco IOS Software Image for all SKUs. Depending on the switch model, the Cisco IOS image automatically configures either the LAN Lite, LAN Base, or IP Lite feature set.

LAN Lite models have reduced functionality and scalability for small deployments with basic requirements. Cisco Catalyst 2960-X Family of Switches are available with the LAN Base and LAN Lite feature sets and Catalyst 2960-XR Family of switches are available IP Lite feature sets.

---

Note that each switch model is tied to a specific feature level; LAN Lite cannot be upgraded to LAN Base and LAN Base cannot be upgraded to IP Lite.

For more information about the features included in the LAN Lite, LAN Base and IP Lite feature sets, refer to Cisco Feature Navigator: <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>.

## Cisco Catalyst 2960-XR IP-Lite High-Performance Routing

The Cisco hardware routing architecture delivers extremely high-performance IP routing in the Cisco Catalyst 2960-XR IP-Lite Switches:

- **IP unicast routing protocols (Static, Routing Information Protocol Version 1 [RIPv1], and RIPv2, RIPv2, and RIPv2)** are supported for small-network routing applications.
- **Advanced IP unicast routing protocols (OSPF for Routed Access)** are supported for load balancing and constructing scalable LANs. IPv6 routing (OSPFv3) is supported in hardware for maximum performance.
- **Equal-cost routing** facilitates Layer 3 load balancing and redundancy across the stack.
- **Policy-based routing (PBR)** allows superior control by facilitating flow redirection regardless of the routing protocol configured.
- **Hot Standby Routing Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP)** provides dynamic load balancing and failover for routed links.
- **Protocol Independent Multicast (PIM)** for IP multicast is supported, including PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), PIM sparse-dense mode and Source Specific Multicast (SSM).

## Network Security

The Cisco Catalyst 2960-X Series Switches provide a range of security features to limit access to the network and mitigate threats, including:

- **Cisco TrustSec uses SXP** to simplify security and policy enforcement throughout the network. For more information about Cisco TrustSec security solutions, visit [cisco.com/go/TrustSec](http://cisco.com/go/TrustSec).
- **Comprehensive 802.1X** Features to control access to the network, including Flexible Authentication, 802.1x Monitor Mode, and RADIUS Change of Authorization.
- **IPv6 First-Hop Security** enhances Layer-2 and Layer-3 network access from proliferating IPv6 devices especially BYOD devices. It protects against rogue router advertisements, address spoofing, fake DHCP replies and other risks introduced by IPv6 technology.
- **Device Sensor and Device Classifier** enable seamless versatile device profiles including BYOD devices. They also enable Cisco Identity Services Engine (ISE) to provision identity based security policies (ISE is supported in 2960-XR SKUs only).
- **Cisco Trust Anchor Technology (TAT)** enables easy distribution of a single universal image for all models of Catalyst 2960-X by verifying the authenticity of IOS images. This technology allows the switch to perform IOS integrity checks at boot-up by verifying the signature, verifying the Trusted Asset under Management (TAM) and authenticating the license.
- **Cisco Threat Defense** features including Port Security, Dynamic ARP Inspection, and IP Source Guard.
- **Private VLANs** restrict traffic between hosts in a common segment by segregating traffic at Layer 2, turning a broadcast segment into a nonbroadcast multi access like segment. This feature is available in IP-Lite feature set only.



- **Private VLAN Edge** provides security and isolation between switch ports, which helps ensure that users cannot snoop on other users' traffic.
- **Unicast Reverse Path Forwarding (RPF)** 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. This feature is available in IP-Lite feature set only.
- **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.
- **Access Control Lists** for Pv6 and IPv4 for security and QoS ACEs.
  - **VLAN ACLs** on all VLANs prevent unauthorized data flows from being bridged within VLANs.
  - **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.
- **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.
- **Switched Port Analyzer (SPAN)**, with bidirectional data support, allows Cisco Intrusion Detection System (IDS) to take action when an intruder is detected.
- **TACACS+ and RADIUS authentication** facilitates centralized control of the switch and restricts unauthorized users from altering the configuration.
- **MAC Address Notification** allows administrators to be notified of users added to or removed from the network.
- **Multilevel security on console access** prevents unauthorized users from altering the switch configuration.
- **Bridge protocol data unit (BPDU) Guard** shuts down Spanning Tree Port Fast-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.
- **IGMP filtering** provides multicast authentication by filtering out nonsubscribers and limits the number of concurrent multicast streams available per port.
- **Dynamic VLAN assignment** is supported through implementation of VLAN Membership Policy Server client capability to provide flexibility in assigning ports to VLANs. Dynamic VLAN facilitates the fast assignment of IP addresses.

## Redundancy and Resiliency

Cisco Catalyst 2960-X Series Switches offer a number of redundancy and resiliency features to prevent outages and help ensure that the network remains available:

- **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 100 milliseconds.

- **IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP)** provide rapid spanning-tree convergence independent of spanning-tree timers and also offer the benefit of Layer 2 load balancing and distributed processing. Stacked units behave as a single spanning-tree node.
- **Per-VLAN Rapid Spanning Tree (PVRST+)** allows rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances.
- **Cisco Hot Standby Router Protocol (HSRP)** is supported to create redundant, fail safe routing topologies in 2960-XR IP-Lite SKUs.
- **Switch-port auto-recovery (Error Disable)** automatically attempts to reactivate a link that is disabled because of a network error.
- **Power redundancy** with an optional second power supply on 2960-XR models, or with an external RPS on 2960-X models.

## Enhanced Quality of Service

The Cisco Catalyst 2960-X Series Switches offers intelligent traffic management that keeps everything flowing smoothly. Flexible mechanisms for marking, classification, and scheduling deliver superior performance for data, voice, and video traffic, all at wire speed. Primary QoS features include:

- Up to **eight egress queues** per port (four on the 2960-X or when stacking the 2960-XR) and strict priority queuing so that the highest priority packets are serviced ahead of all other traffic.
- **Shaped Round Robin (SRR)** scheduling and **Weighted Tail Drop (WTD)** congestion avoidance.
- **Flow-based rate limiting** and up to 256 aggregate or individual policers per port.
- **802.1p class of service (CoS)** and **Differentiated Services Code Point (DSCP)** classification, with marking and reclassification on a per-packet basis by source and destination IP address, MAC address, or Layer 4 TCP/UDP port number.
- **Cross-stack QoS** to allow QoS to be configured across a stack of 2960-X series switches.
- **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.

## Cisco FlexStack-Plus

Cisco FlexStack-Plus provides stacking of up to eight 2960-X switches with the optional FlexStack-Plus module ([Figure 2](#)).

The FlexStack-Plus module is hot swappable and can be added to any Cisco Catalyst 2960-X or Catalyst 2960-XR with a FlexStack-Plus slot. Switches connected to a stack will automatically upgrade to the stack's Cisco IOS Software version and transparently join the stack without additional intervention.

Cisco FlexStack-Plus and Cisco IOS Software offer true stacking, with all switches in a stack acting as a single switch unit. FlexStack-Plus provides a unified data plane, unified configuration, and single IP address for switch management. The advantages of true stacking include lower total cost of ownership and higher availability through simplified management as well as cross-stack features including EtherChannel, SPAN, and FlexLink.

To provide investment protection, FlexStack-Plus is backwards-compatible with FlexStack. Cisco Catalyst 2960-X LAN Base switches equipped with a FlexStack-Plus module can be stacked with Catalyst 2960-S and 2960-SF LAN Base switches equipped with a FlexStack module (see [Table 5](#)).

**Table 3.** FlexStack and FlexStack Plus Supported Combinations

	2960-XR IP Lite	2960-X LAN Base	2960-S/SF LAN Base
<b>2960-XR IP Lite</b>	Yes	-	-
<b>2960-X LAN Base</b>	-	Yes	Yes
<b>2960-S or 2960-SF LAN Base</b>	-	Yes	Yes

**Table 4.** FlexStack-Plus Scalability and Performance

Stack Members	Stack Bandwidth	Stack Limit	Cisco IOS Feature Set
<b>2960-XR IP Lite</b>	80G	8	IOS IP Lite
<b>2960-XLAN Base</b>	80G	8	IOS LAN Base
<b>2960-X LAN Base mixed with 2960-S/SF LAN Base</b>	40G	4	IOS LAN Base

**Figure 2.** Cisco FlexStack-Plus Switch Stack



## Power Supply

The Catalyst 2960-X switches comes with one fixed power-supply and options for an external redundant power supply source (RPS2300).

The Catalyst 2960-XR switches support dual redundant power supplies. The Catalyst 2960-XR ships with one power supply by default. The second power supply can be purchased at the time of ordering the switch or as a spare. These power supplies have in-built fans to provide cooling.

**Figure 3.** 2960-XR Family Power Supply



The following table shows the different power supplies available in these switches and the available PoE power.

**Table 5.** 2960-XR Default Power Supply Configurations

Models	Default Power Supply	Available PoE Power
WS-C2960XR-24TS-I WS-C2960XR-48TS-I WS-C2960XR-24TD-I WS-C2960XR-48TD-I	PWR-C2-250WAC	-
WS-C2960XR-24PD-I WS-C2960XR-48LPD-I WS-C2960XR-24PS-I WS-C2960XR-48LPS-I	PWR-C2-640WAC	370W
WS-C2960XR-48FPD-I WS-C2960XR-48FPS-I	PWR-C2-1025WAC	740W

### Intelligent Power over Ethernet Plus

Cisco Catalyst 2960-Xseries switches support both IEEE 802.3af Power over Ethernet (PoE) and IEEE 802.3at PoE+ (up to 30W per port) to deliver lower total cost of ownership for deployments that incorporate Cisco IP phones, Cisco Aironet® wireless access points, or other standards-compliant PoE/PoE+ end devices. PoE removes the need to supply wall power to PoE-enabled devices and eliminates the cost of adding electrical cabling and circuits that would otherwise be necessary in IP phone and WLAN deployments.

The Catalyst 2960-X series PoE power allocation is dynamic and power mapping scale up to a maximum of 740W PoE+ power.

The 2960-XR switch configurations offer the additional benefit of dual redundant power supplies. If both power supplies are used, then the 2960-XR shares the load between the two power supplies for non stop power.

**Table 6.** 2960-X PoE and PoE+ Power Capacity

Switch Model	Maximum Number of PoE+ (IEEE 802.3at) Ports*	Maximum Number of PoE (IEEE 802.3af) Ports*	Available PoE Power (Single PS Source)
Cisco Catalyst 2960X-48FPD-L	24 ports up to 30W	48 ports up to 15.4W	740W
Cisco Catalyst 2960X-48LPD-L	12 ports up to 30W	24 ports up to 15.4W	370W
Cisco Catalyst 2960X-24PD-L	12 ports up to 30W	24 ports up to 15.4W	370W
Cisco Catalyst 2960X-48FPS-L	24 ports up to 30W	48 ports up to 15.4W	740W
Cisco Catalyst 2960X-48LPS-L	12 ports up to 30W	24 ports up to 15.4W	370W
Cisco Catalyst 2960X-24PS-L	12 ports up to 30W	24 ports up to 15.4W	370W
Cisco Catalyst 2960X-24PSQ-L	3 ports up to 15.4W	6 ports up to 15.4W	92W
Cisco Catalyst 2960XR-48FPD-I	24 ports up to 30W	48 ports up to 15.4W	740W
Cisco Catalyst 2960XR-48LPD-I	12 ports up to 30W	24 ports up to 15.4W	370W
Cisco Catalyst 2960XR-24PD-I	12 ports up to 30W	24 ports up to 15.4W	370W
Cisco Catalyst 2960XR-48FPS-I	24 ports up to 30W	48 ports up to 15.4W	740W
Cisco Catalyst 2960XR-48LPS-I	12 ports up to 30W	24 ports up to 15.4W	370W
Cisco Catalyst 2960XR-24PS-I	12 ports up to 30W	24 ports up to 15.4W	370W

\* Intelligent power management allows flexible power allocation across all ports.

**Table 7.** 2960-XR Available PoE and Switch Power Capabilities with Different Combinations of Power Supplies

Primary Power Supply	Secondary Power Supply	Available Power for PoE+	Switch Power Redundancy	Available PoE Power When One PS fails
PWR-C2-250WAC	-	-	No	-
PWR-C2-250WAC	PWR-C2-250WAC	-	Yes	-
PWR-C2-640WAC	-	370W	No	-
PWR-C2-640WAC	PWR-C2-640WAC	370W	Yes	370W
PWR-C2-1025WAC	-	740W	No	-
PWR-C2-1025WAC	PWR-C2-1025WAC	740W	Yes	740W

## Application Visibility

Catalyst 2960-X Series Switches support **NetFlow Lite**, which enables IT teams to understand the mix of traffic on their network and identify anomalies by capturing and recording specific packet flows. NetFlow Lite supports flexible sampling of the traffic, and exports flow data in the NetFlow Version 9 format for analysis on a wide range of Cisco and third-party collectors.

NetFlow Lite is included on all Catalyst 2960-X and 2960-XR LAN Base and IP Lite models.

## Cisco Catalyst SmartOperations

Cisco Catalyst SmartOperations is a comprehensive set of capabilities that simplify LAN planning, deployment, monitoring, and troubleshooting. Deploying SmartOperations tools reduces the time and effort required to operate the network and lowers total cost of ownership (TCO).

- **Cisco Smart Install** services enable minimal-touch deployment by providing automated Cisco IOS Software image installation and configuration when new switches are connected to the network. This enables network administrators to remotely manage IOS image installs and upgrades.
- **Cisco Auto SmartPorts** services enable automatic configuration of switch ports as devices connect to the switch, with settings optimized for the device type resulting in zero-touch port-policy provisioning.
- **Cisco Auto QoS** is a service that automatic configuration of QoS that allows switch to manage QoS policies based on traffic types resulting in zero-touch traffic engineering.
- **Cisco Smart Troubleshooting** is an extensive array of diagnostic commands and system health checks within the switch, including Smart Call Home. The Cisco GOLD<sup>®</sup> (Generic Online Diagnostics) and Cisco online diagnostics on switches in live networks help predicting and detecting failures faster.

For more information about Cisco Catalyst SmartOperations, visit [cisco.com/go/SmartOperations](http://cisco.com/go/SmartOperations).

## Operational Simplicity Features

- **Dynamic Host Configuration Protocol (DHCP)** autoconfiguration of multiple switches through a boot server eases switch deployment.
- **Stacking master configuration management** and Cisco FlexStack Plus technology helps ensure 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.
- **Autonegotiation** on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth.

- **Dynamic Trunking Protocol (DTP)** facilitates dynamic trunk configuration across all switch ports.
- **Port Aggregation Protocol (PAgP)** automates the creation of Cisco Fast EtherChannel<sup>®</sup> 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.
- **Automatic media-dependent interface crossover (MDIX)** automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed.
- **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.
- **Switching Database Manager (SDM)** templates for access, routing, and VLAN deployment allow the administrator to easily maximize memory 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.
- **VLAN1 minimization** allows VLAN1 to be disabled on any individual VLAN trunk.
- **Smart Multicast, with Cisco FlexStack-Plus technology**, allows the Cisco Catalyst 2960-X Series to offer greater efficiency and support for more multicast data streams such as video by putting each data packet onto the backplane only once.
- **Internet Group Management Protocol (IGMP) Snooping** for IPv4 and IPv6 MLD v1 and v2 Snooping provide fast client joins and leaves of multicast streams and limit bandwidth-intensive video traffic to only the requestors.
- **Multicast VLAN Registration (MVR)** continuously sends multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons.
- **Per-port broadcast, multicast, and unicast storm control** prevents faulty end stations from degrading overall systems performance.
- **Voice VLAN** simplifies telephony installations by keeping voice traffic on a separate VLAN for easier administration and troubleshooting.
- **Cisco VLAN Trunking Protocol (VTP)** supports dynamic VLANs and dynamic trunk configuration across all switches.
- **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 trace route** eases troubleshooting by identifying the physical path that a packet takes from source to destination.
- **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.

---

## Power Management

The 2960-X switches offer a range of industry leading features for effective energy efficiency and energy management.

**Switch Hibernation Mode (SHM)** is an industry first and available on all 2960-X series switches. This feature puts the switch in ultra low power mode during periods of non-operation such as nights or weekends. Switch Hibernation Mode on the 2960-X switches can be scheduled using EnergyWise compliant management software.

**IEEE 802.3az EEE (Energy Efficient Ethernet)** enables ports to dynamically sense idle periods between traffic bursts and quickly switch the interfaces into a low power idle mode, reducing power consumption.

**Cisco EnergyWise** policies can be used to control the power consumed by PoE-powered endpoints, desktop and data-center IT equipment, and a wide range of building infrastructure. EnergyWise technology is included on all Cisco Catalyst 2960-X Series Switches.

For more information about Cisco EnergyWise™, visit [cisco.com/go/energywise](http://cisco.com/go/energywise).

## Network Management

The Cisco Catalyst 2960-X Series Switches offer a superior CLI for detailed configuration and administration. 2960-X Series Switches are also supported in the full range of Cisco network management solutions.

### Cisco Prime Infrastructure

Cisco Prime™ network management solutions provide comprehensive network lifecycle management. Cisco Prime Infrastructure provides an extensive library of easy-to-use features to automate the initial and day-to-day management of your Cisco network. Cisco Prime integrates hardware and software platform expertise and operational experience into a powerful set of workflow-driven configuration, monitoring, troubleshooting, reporting, and administrative tools.

For detailed information about Cisco Prime, visit [cisco.com/go/prime](http://cisco.com/go/prime).

### Cisco Network Assistant

A Cisco network management application designed for small and medium-sized business (SMB) networks with up to 250 users that runs on PCs, Tablets and even SmartPhones, Cisco Network Assistant offers centralized network management and configuration capabilities. This application also features an intuitive GUI where users can easily apply common services across Cisco switches, routers, and access points.

For detailed information about Cisco Network Assistant, visit [cisco.com/go/cna](http://cisco.com/go/cna).

## Security Management

**Cisco Identity Services Engine (ISE)** support enables the 2960-XR switches to offer security management for all devices connected to it.

## Technical Specifications

**Table 8.** Cisco Catalyst 2960-X Series Hardware

Hardware Specifications	
Flash memory	128 MB for LAN Base & IP Lite SKUs, 64 MB for LAN Lite SKUs
DRAM	512 MB
CPU	APM86392 600MHz dual core
Console Ports	USB (Type-B), Ethernet (RJ-45)
Storage Interface	USB (Type-A) for external flash storage
Network Management Interface	10/100 Mbps Ethernet (RJ-45)

**Table 9.** Cisco Catalyst 2960-X Series Performance

Performance and Scalability			
	2960-X LAN Lite	2960-X LAN Base	2960-XR IP Lite
Forwarding bandwidth	50 Gbps	108 Gbps	108 Gbps
Switching bandwidth*	100 Gbps	216 Gbps	216 Gbps
Maximum active VLANs	64	1023	1023
VLAN IDs available	4096	4096	4096
Maximum transmission unit (MTU) - L3 packet	9198 bytes	9198 bytes	9198 bytes
Jumbo frame - Ethernet frame	9216 bytes	9216 bytes	9216 bytes

\* Switching bandwidth is full-duplex capacity.

**Table 10.** Cisco Catalyst 2960-X Series Forwarding Performance

Forwarding Rate: 64-Byte L3 Packets	
<b>Catalyst 2960-X Family</b>	
Cisco Catalyst 2960X-48FPD-L	130.9 Mpps
Cisco Catalyst 2960X-48LPD-L	130.9 Mpps
Cisco Catalyst 2960X-24PD-L	95.2 Mpps
Cisco Catalyst 2960X-48TD-L	130.9 Mpps
Cisco Catalyst 2960X-24TD-L	95.2 Mpps
Cisco Catalyst 2960X-48FPS-L	107.1 Mpps
Cisco Catalyst 2960X-48LPS-L	107.1 Mpps
Cisco Catalyst 2960X-24PS-L	71.4 Mpps
Cisco Catalyst 2960X-24PSQ-L	71.4 Mpps
Cisco Catalyst 2960X-48TS-L	107.1 Mpps
Cisco Catalyst 2960X-24TS-L	71.4 Mpps
Cisco Catalyst 2960X-48TS-LL	104.2 Mpps
Cisco Catalyst 2960X-24TS-LL	68.5 Mpps
<b>Catalyst 2960-XR Family</b>	
Cisco Catalyst 2960XR-48FPD-I	130.9 Mpps
Cisco Catalyst 2960XR-48LPD-I	130.9 Mpps
Cisco Catalyst 2960XR-24PD-I	95.2 Mpps
Cisco Catalyst 2960XR-48TD-I	130.9 Mpps
Cisco Catalyst 2960XR-24TD-I	95.2 Mpps



Forwarding Rate: 64-Byte L3 Packets	
Cisco Catalyst 2960XR-48FPS-I	107.1 Mpps
Cisco Catalyst 2960XR-48LPS-I	107.1 Mpps
Cisco Catalyst 2960XR-24PS-I	71.4 Mpps
Cisco Catalyst 2960XR-48TS-I	107.1 Mpps
Cisco Catalyst 2960XR-24TS-I	71.4 Mpps

**Table 11.** Cisco Catalyst 2960-X Series Mechanical Specifications

Models		
Dimensions	Inches (H x D x W)	Centimeters (H x D x W)
WS-C2960X-48FPD-L	1.75 x 14.5 x 17.5	4.5 x 36.8 x 44.5
WS-C2960X-48LPD-L	1.75 x 14.5 x 17.5	4.5 x 36.8 x 44.5
WS-C2960X-48TD-L	1.75 x 11.0 x 17.5	4.5 x 27.9 x 44.5
WS-C2960X-24PD-L	1.75 x 14.5 x 17.5	4.5 x 36.8 x 44.5
WS-C2960X-24TD-L	1.75 x 11.0 x 17.5	4.5 x 27.9 x 44.5
WS-C2960X-48FPS-L	1.75 x 14.5 x 17.5	4.5 x 36.8 x 44.5
WS-C2960X-48LPS-L	1.75 x 14.5 x 17.5	4.5 x 36.8 x 44.5
WS-C2960X-48TS-L	1.75 x 11.0 x 17.5	4.5 x 27.9 x 44.5
WS-C2960X-24PS-L	1.75 x 14.5 x 17.5	4.5 x 36.8 x 44.5
WS-C2960X-24PSQ-L	1.75 x 14.5 x 17.5	4.5 x 36.8 x 44.5
WS-C2960X-24TS-L	1.75 x 11.0 x 17.5	4.5 x 27.9 x 44.5
WS-C2960X-48TS-LL	1.75 x 11.0 x 17.5	4.5 x 27.9 x 44.5
WS-C2960X-24TS-LL	1.75 x 11.0 x 17.5	4.5 x 27.9 x 44.5
Weights	Pounds	Kilograms
WS-C2960X-48FPD-L	12.9 lbs	5.8 Kg
WS-C2960X-48LPD-L	12.9 lbs	5.8 Kg
WS-C2960X-48TD-L	9.6 lbs	4.3 Kg
WS-C2960X-24PD-L	12.7 lbs	5.7 Kg
WS-C2960X-24TD-L	8.9 lbs	4.0 Kg
WS-C2960X-48FPS-L	12.9 lbs	5.8 Kg
WS-C2960X-48LPS-L	12.9 lbs	5.8 Kg
WS-C2960X-48TS-L	9.4 lbs	4.2 Kg
WS-C2960X-24PS-L	12.8 lbs	5.8 kg
WS-C2960X-24PSQ-L	12.8 lbs	5.8 kg
WS-C2960X-24TS-L	8.9 lbs	4.0 kg
WS-C2960X-48TS-LL	8.9 lbs	4.0kg
WS-C2960X-24TS-LL	8.2 lbs	3.7 kg

**Table 12.** Cisco Catalyst 2960-XR Series Mechanical Specifications

Models		
Dimensions	Inches (H x D x W)	Centimeters (H x D x W)
WS-C2960XR-48FPD-I	1.75 x 16.0 x 17.5	4.45 x 40.8 x 44.5
WS-C2960XR-48LPD-I	1.75 x 16.0 x 17.5	4.45 x 40.8 x 44.5
WS-C2960XR-48TD-I	1.75 x 16.0 x 17.5	4.45 x 40.8 x 44.5
WS-C2960XR-24PD-I	1.75 x 16.0 x 17.5	4.45 x 40.8 x 44.5
WS-C2960XR-24TD-I	1.75 x 16.0 x 17.5	4.45 x 40.8 x 44.5
WS-C2960XR-48FPS-I	1.75 x 16.0 x 17.5	4.45 x 40.8 x 44.5
WS-C2960XR-48LPS-I	1.75 x 16.0x 17.5	4.45 x 40.8 x 44.5
WS-C2960XR-48TS-I	1.75 x 16.0 x 17.5	4.45 x 40.8 x 44.5
WS-C2960XR-24PS-I	1.75 x 16.0 x 17.5	4.45 x 40.8 x 44.5
WS-C2960XR-24TS-I	1.75 x 16.0 x 17.5	4.45 x 40.8 x 44.5
Weights	Pounds	Kilograms
WS-C2960XR-48FPD-I	14.6	6.6
WS-C2960XR-48LPD-I	14.0	6.4
WS-C2960XR-48TD-I	13.3	6.1
WS-C2960XR-24PD-I	13.6	6.2
WS-C2960XR-24TD-I	13.0	5.9
WS-C2960XR-48FPS-I	14.7	6.7
WS-C2960XR-48LPS-I	14.2	6.4
WS-C2960XR-48TS-I	13.2	6.0
WS-C2960XR-24PS-I	13.7	6.2
WS-C2960XR-24TS-I	13.0	5.9

**Table 13.** Cisco Catalyst 2960-X Series Environmental Specifications

Environmental Ranges		
	Fahrenheit	Centigrade
Operating temperature up to 5000 ft (1500 m)	23°F to 113°F	-5°C to 45°C
Operating temperature up to 10,000 ft (3000 m)	23°F to 104°F	-5°C to 40°C
Short-term exception at sea level <sup>†</sup>	23°F to 131°F	-5°C to 55°C
Short-term exception up to 5000 feet (1500 m) <sup>†</sup>	23°F to 122°F	-5°C to 50°C
Short-term exception up to 10,000 feet (3000 m) <sup>†</sup>	23°F to 113°F	-5°C to 45°C
Short-term exception up to 13,000 feet (4000 m) <sup>†</sup>	23° to 104°F	-5°C to 40°C
Storage temperature up to 15,000 feet (4573 m)	-13° to 158°F	-25° to 70°C
	Feet	Meters
Operating altitude	Up to 10,000	Up to 3000
Storage altitude	Up to 13,000	Up to 4000
Operating relative humidity	10% to 95% noncondensing	
Storage relative humidity	10% to 95% noncondensing	
Acoustic Noise		
<i>Measured per ISO 7779 and declared per ISO 9296.</i>		
<i>Bystander positions operating mode at 25°C ambient.</i>		

Environmental Ranges				
Model	Sound Pressure		Sound Power	
	LpA (Typical)	LpAD (Maximum)	LwA (Typical)	LwAD (Maximum)
Cisco Catalyst 2960X-48FPD-L	54dB	57dB	6.3B	6.6B
Cisco Catalyst 2960X-48LPD-L				
Cisco Catalyst 2960X-24PD-L				
Cisco Catalyst 2960X-48TD-L	40dB	43dB	4.9B	5.2B
Cisco Catalyst 2960X-24TD-L				
Cisco Catalyst 2960X-48FPS-L	54dB	57dB	6.3B	6.6B
Cisco Catalyst 2960X-48LPS-L				
Cisco Catalyst 2960X-24PS-L				
Cisco Catalyst 2960X-24PSQ-L	N/A	N/A	N/A	N/A
Cisco Catalyst 2960X-48TS-L	45dB	48dB	5.4B	5.7B
Cisco Catalyst 2960X-24TS-L				
Cisco Catalyst 2960X-48TS-LL	40dB	43dB	4.9B	5.2B
Cisco Catalyst 2960X-24TS-LL				
Cisco Catalyst 2960XR-48FPD-I	46dB	48dB	5.5B	5.7B
Cisco Catalyst 2960XR-48LPD-I	45dB	48dB	5.4B	5.7B
Cisco Catalyst 2960XR-24PD-I	45dB	48dB	5.4B	5.7B
Cisco Catalyst 2960XR-48TD-I	42dB	45dB	5.1B	5.4B
Cisco Catalyst 2960XR-24TD-I	42dB	45dB	5.1B	5.4B
Cisco Catalyst 2960XR-48FPS-I	46dB	48dB	5.5B	5.7B
Cisco Catalyst 2960XR-48LPS-I	45dB	48dB	5.4B	5.7B
Cisco Catalyst 2960XR-24PS-I	45dB	48dB	5.4B	5.7B
Cisco Catalyst 2960XR-48TS-I	42dB	45dB	5.1B	5.4B
Cisco Catalyst 2960XR-24TS-I	42dB	45dB	5.1B	5.4B
Predicted Reliability				
Model	MTBF in hours <sup>™</sup>			
Cisco Catalyst 2960X-48FPD-L	233,370			
Cisco Catalyst 2960X-48LPD-L	277,960			
Cisco Catalyst 2960X-24PD-L	325,780			
Cisco Catalyst 2960X-48TD-L	445,460			
Cisco Catalyst 2960X-24TD-L	569,520			
Cisco Catalyst 2960X-48FPS-L	232,610			
Cisco Catalyst 2960X-48LPS-L	276,870			
Cisco Catalyst 2960X-24PS-L	324,280			
Cisco Catalyst 2960X-24PSQ-L	462,680			
Cisco Catalyst 2960X-48TS-L	442,690			
Cisco Catalyst 2960X-24TS-L	564,910			
Cisco Catalyst 2960X-48TS-LL	476,560			
Cisco Catalyst 2960X-24TS-LL	622,350			
Cisco Catalyst 2960X-STACK	17,128,090			
Cisco Catalyst 2960XR-48FPD-I	231,590			
Cisco Catalyst 2960XR-48LPD-I	275,430			
Cisco Catalyst 2960XR-24PD-I	322,740			
Cisco Catalyst 2960XR-48TD-I	440,880			

Environmental Ranges	
Cisco Catalyst 2960XR-24TD-I	561,890
Cisco Catalyst 2960XR-48FPS-I	230,860
Cisco Catalyst 2960XR-48LPS-I	274,380
Cisco Catalyst 2960XR-24PS-I	321,290
Cisco Catalyst 2960XR-48TS-I	438,130
Cisco Catalyst 2960XR-24TS-I	557,320
Cisco PWR-C2-250WAC	1,000,000
Cisco PWR-C2-640WAC	1,000,000
Cisco PWR-C2-1025WAC	1,000,000

\* Not more than the following in a 1-year period: 96 consecutive hours, or 360 hours total, or 15 occurrences.

\*\* Currently estimates; Later will be Based on Telcordia SR-332 Issue 2 methodology.

**Table 14.** Connectors and Interfaces

Connectors and Interfaces
<b>Ethernet Interfaces</b> <ul style="list-style-type: none"> <li>• 10BASE-T ports: RJ-45 connectors, 2-pair Category 3, 4, or 5 unshielded twisted-pair (UTP) cabling</li> <li>• 100BASE-TX ports: RJ-45 connectors, 2-pair Category 5 UTP cabling</li> <li>• 1000BASE-T ports: RJ-45 connectors, 4-pair Category 5 UTP cabling</li> <li>• 1000BASE-T SFP-based ports: RJ-45 connectors, 4-pair Category 5 UTP cabling</li> </ul>
<b>SFP and SFP+ Interfaces</b> <p>For information about supported SFP/SFP+ modules, refer to the Transceiver Compatibility matrix tables at <a href="http://cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html">cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html</a>.</p>
<b>Indicator LEDs</b> <ul style="list-style-type: none"> <li>• Per-port status: Link integrity, disabled, activity, speed, and full duplex</li> <li>• System status: System, RPS, Stack link status, link duplex, PoE, and link speed</li> </ul>
<b>Stacking Interfaces</b> <p>Cisco Catalyst 2960-XFlexStack-Plus stacking cables:</p> <ul style="list-style-type: none"> <li>• CAB-STK-E-0.5M FlexStack-Plus stacking cable with a 0.5 m length</li> <li>• CAB-STK-E-1M FlexStack-Plus stacking cable with a 1.0 m length</li> <li>• CAB-STK-E-3M FlexStack-Plus stacking cable with a 3.0 m length</li> </ul>
<b>Console</b> <p>Cisco Catalyst 2960-X console cables:</p> <ul style="list-style-type: none"> <li>• CAB-CONSOLE-RJ45 Console cable 6 ft. with RJ-45</li> <li>• CAB-CONSOLE-USB Console cable 6 ft. with USB Type A and mini-B connectors</li> </ul>
<b>Power</b> <ul style="list-style-type: none"> <li>• The internal power supply is an auto-ranging unit and supports input voltages between 100 and 240V AC</li> <li>• Use the supplied AC power cord to connect the AC power connector to an AC power outlet</li> <li>• The Cisco RPS connector offers connection for an optional Cisco RPS 2300 that uses AC input and supplies DC output to the switch</li> <li>• Only the Cisco RPS 2300 (model PWR-RPS2300) should be attached to the redundant-power-system receptacle</li> </ul>

**Table 15.** Management and Standards Support

Category	Specification	
<b>Management</b>	<ul style="list-style-type: none"> <li>• BRIDGE-MIB</li> <li>• CISCO-CABLE-DIAG-MIB</li> <li>• CISCO-CDP-MIB</li> <li>• CISCO-CLUSTER-MIB</li> <li>• CISCO-CONFIG-COPY-MIB</li> <li>• CISCO-CONFIG-MAN-MIB</li> <li>• CISCO-DHCP-SNOOPING-MIB</li> <li>• CISCO-ENTITY-VENDORTYPE-OID-MIB</li> <li>• CISCO-ENVMON-MIB</li> <li>• CISCO-ERR-DISABLE-MIB</li> <li>• CISCO-FLASH-MIB</li> <li>• CISCO-FTP-CLIENT-MIB</li> <li>• CISCO-IGMP-FILTER-MIB</li> <li>• CISCO-IMAGE-MIB</li> <li>• CISCO-IP-STAT-MIB</li> <li>• CISCO-LAG-MIB</li> <li>• CISCO-MAC-NOTIFICATION-MIB</li> <li>• CISCO-MEMORY-POOL-MIB</li> <li>• CISCO-PAGP-MIB</li> <li>• CISCO-PING-MIB</li> <li>• CISCO-POE-EXTENSIONS-MIB</li> <li>• CISCO-PORT-QOS-MIB</li> <li>• CISCO-PORT-SECURITY-MIB</li> <li>• CISCO-PORT-STORM-CONTROL-MIB</li> <li>• CISCO-PRODUCTS-MIB</li> <li>• CISCO-PROCESS-MIB</li> <li>• CISCO-RTTMON-MIB</li> <li>• CISCO-SMI-MIB</li> <li>• CISCO-STP-EXTENSIONS-MIB</li> <li>• CISCO-SYSLOG-MIB</li> </ul>	<ul style="list-style-type: none"> <li>• CISCO-TC-MIB</li> <li>• CISCO-TCP-MIB</li> <li>• CISCO-UDLD-MIB</li> <li>• CISCO-VLAN-IFTABLE</li> <li>• RELATIONSHIP-MIB</li> <li>• CISCO-VLAN-MEMBERSHIP-MIB</li> <li>• CISCO-VTP-MIB</li> <li>• ENTITY-MIB</li> <li>• ETHERLIKE-MIB</li> <li>• IEEE8021-PAE-MIB</li> <li>• IEEE8023-LAG-MIB</li> <li>• IF-MIB</li> <li>• INET-ADDRESS-MIB</li> <li>• OLD-CISCO-CHASSIS-MIB</li> <li>• OLD-CISCO-FLASH-MIB</li> <li>• OLD-CISCO-INTERFACES-MIB</li> <li>• OLD-CISCO-IP-MIB</li> <li>• OLD-CISCO-SYS-MIB</li> <li>• OLD-CISCO-TCP-MIB</li> <li>• OLD-CISCO-TS-MIB</li> <li>• RFC1213-MIB</li> <li>• RMON-MIB</li> <li>• RMON2-MIB</li> <li>• SNMP-FRAMEWORK-MIB</li> <li>• SNMP-MPD-MIB</li> <li>• SNMP-NOTIFICATION-MIB</li> <li>• SNMP-TARGET-MIB</li> <li>• SNMPv2-MIB</li> <li>• TCP-MIB</li> <li>• UDP-MIB</li> <li>• ePM MIB</li> <li>• CISCO-FLEXSTACK-PLUS-MIB (2960-X)</li> </ul>
For an updated list of supported MIBs, refer to the MIB Locator at <a href="http://cisco.com/go/mibs">cisco.com/go/mibs</a> .		
<b>Standards</b>	<ul style="list-style-type: none"> <li>• IEEE 802.1D Spanning Tree Protocol</li> <li>• IEEE 802.1p CoS Prioritization</li> <li>• IEEE 802.1Q VLAN</li> <li>• IEEE 802.1s</li> <li>• IEEE 802.1w</li> <li>• IEEE 802.1X</li> <li>• IEEE 802.1ab (LLDP)</li> <li>• IEEE 802.3ad</li> <li>• IEEE 802.3af and IEEE 802.3at</li> <li>• IEEE 802.3ah (100BASE-X single/multimode fiber only)</li> <li>• IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports</li> </ul>	<ul style="list-style-type: none"> <li>• IEEE 802.3 10BASE-T</li> <li>• IEEE 802.3u 100BASE-TX</li> <li>• IEEE 802.3ab 1000BASE-T</li> <li>• IEEE 802.3z 1000BASE-X</li> <li>• RMON I and II standards</li> <li>• SNMP v1, v2c, and v3</li> <li>• IEEE 802.3az</li> <li>• IEEE 802.3ae 10Gigabit Ethernet</li> <li>• IEEE 802.1ax</li> </ul>

Category	Specification
<b>RFC compliance</b>	<ul style="list-style-type: none"> <li>• RFC 768 - UDP</li> <li>• RFC 783 - TFTP</li> <li>• RFC 791 - IP</li> <li>• RFC 792 - ICMP</li> <li>• RFC 793 - TCP</li> <li>• RFC 826 - ARP</li> <li>• RFC 854 - Telnet</li> <li>• RFC 951 - Bootstrap Protocol (BOOTP)</li> <li>• RFC 959 - FTP</li> <li>• RFC 1112 - IP Multicast and IGMP</li> <li>• RFC 1157 - SNMP v1</li> <li>• RFC 1166 - IP Addresses</li> <li>• RFC 1256 - Internet Control Message Protocol (ICMP) Router Discovery</li> <li>• RFC 1305 - NTP</li> <li>• RFC 1492 - TACACS+</li> <li>• RFC 1493 - Bridge MIB</li> <li>• RFC 1542 - BOOTP extensions</li> <li>• RFC 1643 - Ethernet Interface MIB</li> <li>• RFC 1757 - RMON</li> </ul> <ul style="list-style-type: none"> <li>• RFC 1901 - SNMP v2C</li> <li>• RFC 1902-1907 - SNMP v2</li> <li>• RFC 1981 - Maximum Transmission Unit (MTU) Path Discovery IPv6</li> <li>• RFC 2068 - HTTP</li> <li>• RFC 2131 - DHCP</li> <li>• RFC 2138 - RADIUS</li> <li>• RFC 2233 - IF MIB v3</li> <li>• RFC 2373 - IPv6 Aggregatable Addrs</li> <li>• RFC 2460 - IPv6</li> <li>• RFC 2461 - IPv6 Neighbor Discovery</li> <li>• RFC 2462 - IPv6 Autoconfiguration</li> <li>• RFC 2463 - ICMP IPv6</li> <li>• RFC 2474 - Differentiated Services (DiffServ) Precedence</li> <li>• RFC 2597 - Assured Forwarding</li> <li>• RFC 2598 - Expedited Forwarding</li> <li>• RFC 2571 - SNMP Management</li> <li>• RFC 3046 - DHCP Relay Agent Information Option</li> <li>• RFC 3376 - IGMP v3</li> <li>• RFC 3580 - 802.1X RADIUS</li> </ul>

**Table 16.** Voltage and Power Ratings

Input Voltage and Current			
Model	Voltage (Auto ranging)	Current	Frequency
Cisco Catalyst 2960X-48FPD-L	100 to 240 VAC	9A-4A	50 to 60Hz
Cisco Catalyst 2960X-48LPD-L		5A-2A	
Cisco Catalyst 2960X-24PD-L		5A-2A	
Cisco Catalyst 2960X-48TD-L		1A - 0.5A	
Cisco Catalyst 2960X-24TD-L		1A to 0.5A	
Cisco Catalyst 2960X-48FPS-L		9A - 4A	
Cisco Catalyst 2960X-48LPS-L		5A - 2A	
Cisco Catalyst 2960X-24PS-L		5A - 2A	
Cisco Catalyst 2960X-24PSQ-L		2A - 4A	
Cisco Catalyst 2960X-48TS-L		1A-0.5A	
Cisco Catalyst 2960X-24TS-L		1A - 0.5A	
Cisco Catalyst 2960X-48TS-LL		1A - 0.5A	
Cisco Catalyst 2960X-24TS-LL		1A - 0.5A	
Cisco Catalyst 2960XR-48FPD-I		100 to 240 VAC	
Cisco Catalyst 2960XR-48LPD-I	6A to 3 A		
Cisco Catalyst 2960XR-24PD-I	6A to 3 A		
Cisco Catalyst 2960XR-48TD-I	1A to 0.5 A		
Cisco Catalyst 2960XR-24TD-I	1A to 0.5 A		
Cisco Catalyst 2960XR-48FPS-I	10A to 5 A		
Cisco Catalyst 2960XR-48LPS-I	6A to 3 A		
Cisco Catalyst 2960XR-24PS-I	6A to 3 A		
Cisco Catalyst 2960XR-48TS-I	1A to 0.5 A		
Cisco Catalyst 2960XR-24TS-I	1A to 0.5 A		

Power Rating (Switch maximum consumption values)	
Cisco Catalyst 2960X-48FPD-L	0.89 kVA
Cisco Catalyst 2960X-48LPD-L	0.48 kVA
Cisco Catalyst 2960X-24PD-L	0.47 kVA
Cisco Catalyst 2960X-48TD-L	0.049 kVA
Cisco Catalyst 2960X-24TD-L	0.034 kVA
Cisco Catalyst 2960X-48FPS-L	0.89 kVA
Cisco Catalyst 2960X-48LPS-L	0.49 kVA
Cisco Catalyst 2960X-24PS-L	0.49 kVA
Cisco Catalyst 2960X-24PSQ-L	0.16 kVA
Cisco Catalyst 2960X-48TS-L	0.051 kVA
Cisco Catalyst 2960X-24TS-L	0.039 kVA
Cisco Catalyst 2960X-48TS-LL	0.46KVA
Cisco Catalyst 2960X-24TS-LL	0.035KVA
Cisco Catalyst 2960XR-48FPD-I	0.89KVA
Cisco Catalyst 2960XR-48LPD-I	0.48KVA
Cisco Catalyst 2960XR-24PD-I	0.46KVA
Cisco Catalyst 2960XR-48TD-I	0.047KVA
Cisco Catalyst 2960XR-24TD-I	0.039KVA
Cisco Catalyst 2960XR-48FPS-I	0.89KVA
Cisco Catalyst 2960XR-48LPS-I	0.47KVA
Cisco Catalyst 2960XR-24PS-I	0.46KVA
Cisco Catalyst 2960XR-48TS-I	0.046KVA
Cisco Catalyst 2960XR-24TS-I	0.038KVA

DC Input Voltages (RPS Input) - Only for 2960-X LAN Base Switches		
	12V	53V
Cisco Catalyst 2960X-48FPD-L	4A	15A
Cisco Catalyst 2960X-48LPD-L	4A	8A
Cisco Catalyst 2960X-24PD-L	3A	8A
Cisco Catalyst 2960X-48TD-L	4A	N/A
Cisco Catalyst 2960X-24TD-L	3A	N/A
Cisco Catalyst 2960X-48FPS-L	4A	15A
Cisco Catalyst 2960X-48LPS-L	4A	8A
Cisco Catalyst 2960X-24PS-L	3A	8A
Cisco Catalyst 2960X-24PSQ-L	N/A	N/A
Cisco Catalyst 2960X-48TS-L	5A	N/A
Cisco Catalyst 2960X-24TS-L	4A	N/A

**Note:** The wattage rating on the power supply does not represent actual power draw. It indicates the maximum power draw possible by the power supply. This rating can be used for facility capacity planning. For PoE switches, cooling requirements are smaller than total power draw as a significant portion of the load is dissipated in the endpoints.

**Table 17.** Power Consumption<sup>1</sup>

Measured Power Consumption in Watts <sup>2</sup>				
Model	0% Traffic <sup>3</sup>	10% Traffic	100% Traffic	Weighted Average
Cisco Catalyst 2960X-48FPD-L	50.8	65.9	66.7	66.0
Cisco Catalyst 2960X-48LPD-L	45.7	61.1	62.0	61.2
Cisco Catalyst 2960X-24PD-L	44.7	52.3	53.1	52.3
Cisco Catalyst 2960X-48TD-L	32.9	47.0	47.8	47.1
Cisco Catalyst 2960X-24TD-L	24.9	32.2	33.1	32.3
Cisco Catalyst 2960X-48FPS-L	51.9	66.6	66.8	66.6
Cisco Catalyst 2960X-48LPS-L	46.7	60.8	61.1	60.9
Cisco Catalyst 2960X-24PS-L	41.4	49.0	49.2	49.0
Cisco Catalyst 2960X-24PSQ-L	28.5	32.8	34.8	33.0
Cisco Catalyst 2960X-48TS-L	34.9	49.5	49.7	49.5
Cisco Catalyst 2960X-24TS-L	28.0	36.8	37.1	36.9
Cisco Catalyst 2960X-48TS-LL	31.4	44.3	44.5	44.4
Cisco Catalyst 2960X-24TS-LL	25.2	32.0	32.0	32.0
Cisco Catalyst 2960XR-48FPD-I	46.7	61.8	62.5	61.9
Cisco Catalyst 2960XR-48LPD-I	40.7	54.6	55.9	54.8
Cisco Catalyst 2960XR-24PD-I	36.1	42.9	43.7	43.0
Cisco Catalyst 2960XR-48TD-I	29.7	44.7	45.6	44.8
Cisco Catalyst 2960XR-24TD-I	29.3	37.2	38.1	37.3
Cisco Catalyst 2960XR-48FPS-I	44.8	58.5	58.8	58.5
Cisco Catalyst 2960XR-48LPS-I	37.9	52.8	53.0	52.9
Cisco Catalyst 2960XR-24PS-I	36.5	43.2	43.4	43.2
Cisco Catalyst 2960XR-48TS-I	30.0	44.8	45.0	44.8
Cisco Catalyst 2960XR-24TS-I	28.8	36.0	36.2	36.0

**Table 18.** Safety and Compliance

Specification	Description
<b>Safety</b>	UL 60950-1 Second Edition CAN/CSA-C22.2 No. 60950-1 Second Edition EN 60950-1 Second Edition IEC 60950-1 Second Edition AS/NZS 60950-1
<b>EMC - Emissions</b>	47CFR Part 15 (CFR 47) 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 CNS13438 Class A

<sup>1</sup> Disclaimer: All power consumption numbers were measured under controlled laboratory conditions and are provided as estimates.

<sup>2</sup> ATIS Methodology

<sup>3</sup> All Traffic measured with EEE enabled.



Specification	Description
<b>EMC - Immunity</b>	EN55024 CISPR24 EN300386 KN24
<b>Environmental</b>	Reduction of Hazardous Substances (RoHS) including Directive 2011/65/EU
<b>Telco</b>	Common Language Equipment Identifier (CLEI) code
<b>US Government Certifications</b>	USGv6 and IPv6 Ready Logo

## Cisco Enhanced Limited Lifetime Hardware Warranty

Cisco Catalyst 2960-X Series Switches come with an enhanced limited lifetime warranty (E-LLW). The E-LLW provides the same terms as Cisco's standard limited lifetime warranty but adds next business day delivery of replacement hardware, where available, and 90 days of 8X5 Cisco Technical Assistance Center (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 19.** Warranty Terms

Cisco Enhanced Limited Lifetime Hardware Warranty	
<b>Device covered</b>	Applies to all Cisco Catalyst 2960-X Series Switches.
<b>Warranty duration</b>	As long as the original end user continues to own or use the product, provided that: fan and power supply warranty is limited to five (5) years.
<b>End-of-life policy</b>	In the event of discontinuance of product manufacture, Cisco warranty support is limited to five (5) years from the announcement of discontinuance.
<b>Hardware replacement</b>	Cisco or its service center will use commercially reasonable efforts to ship a Cisco Catalyst 2960-X replacement part for next business day delivery, where available. Otherwise, a replacement will be shipped within ten (10) working days after the receipt of the RMA request. Actual delivery times may vary depending on customer location.
<b>Effective date</b>	Hardware warranty commences from the date of shipment to customer (and in case of resale by a Cisco reseller, not more than ninety [90] days after original shipment by Cisco).
<b>TAC support</b>	Cisco will provide during customer's local business hours, 8 hours per day, 5 days per week basic configuration, diagnosis, and troubleshooting of device-level problems for up to 90 days from the date of shipment of the originally purchased Cisco Catalyst 2960-X product. This support does not include solution or network-level support beyond the specific device under consideration.
<b>Cisco.com Access</b>	Warranty allows guest access only to Cisco.com.

## Software Policy

Customers with Cisco Catalyst IP Lite, LAN Base and LAN Lite 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.

This policy supersedes any previous warranty or software statement and is subject to change without notice.

## Technical Support and Services

**Table 20.** Technical Services Available for Cisco Catalyst 2960-X Series Switches

Technical Services
<p><b>Cisco SMARTnet Service</b></p> <ul style="list-style-type: none"> <li>• Around-the-clock, global access to the Cisco TAC</li> <li>• Unrestricted access to the extensive Cisco.com knowledge base and tools</li> <li>• Next-business-day, 8x5x4, 24x7x4, or 24x7x2 advance hardware replacement and onsite parts replacement and installation available<sup>1</sup></li> <li>• Ongoing operating system software updates within the licensed feature set<sup>2</sup></li> <li>• Proactive diagnostics and real-time alerts on Smart Call Home enabled devices</li> </ul>
<p><b>Cisco Smart Foundation Service</b></p> <ul style="list-style-type: none"> <li>• Next-business-day advance hardware replacement as available</li> <li>• Access to SMB TAC during business hours (access levels vary by region)</li> <li>• Access to Cisco.com SMB knowledge base</li> <li>• Online technical resources through Smart Foundation Portal</li> <li>• Operating system software bug fixes and patches</li> </ul>
<p><b>Cisco Smart Care Service</b></p> <ul style="list-style-type: none"> <li>• Network-level coverage for the needs of small and medium-sized businesses</li> <li>• Proactive health checks and periodic assessments of Cisco network foundation, voice, and security technologies</li> <li>• Technical support for eligible Cisco hardware and software through Smart Care Portal</li> <li>• Cisco operating system and application software updates and upgrades<sup>2</sup></li> <li>• Next-business-day advance hardware replacement as available, 24x7x4 option available<sup>1</sup></li> </ul>
<p><b>Cisco SP Base Service</b></p> <ul style="list-style-type: none"> <li>• Around-the-clock, global access to the Cisco TAC</li> <li>• Registered access to Cisco.com</li> <li>• Next-business-day, 8x5x4, 24x7x4, and 24x7x2 advance hardware replacement. Return to factory option available<sup>1</sup></li> <li>• Ongoing operating system software updates<sup>2</sup></li> </ul>
<p><b>Cisco Focused Technical Support Services</b></p> <p>Three levels of premium, high-touch services are available:</p> <ul style="list-style-type: none"> <li>• Cisco High-Touch Operations Management Service</li> <li>• Cisco High-Touch Technical Support Service</li> <li>• Cisco High-Touch Engineering Service</li> </ul> <p>Valid Cisco SMARTnet or SP Base contracts are required on all network equipment</p>

<sup>1</sup> 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 next-business-day (NBD) delivery. Where NBD is not available, same day shipping is provided. Restrictions apply; please review the appropriate service descriptions for details.

<sup>2</sup> Cisco operating system updates include the following: maintenance releases, minor updates, and major updates within the licensed feature set.

## Ordering Information

**Table 21.** Cisco Catalyst 2960-X Series Switches Ordering Information

Part Number	10/100/1000 Ethernet Interfaces	Uplink Interfaces	Cisco IOS Software Feature Set	Available PoE Power	FlexStack-Plus Stacking
WS-C2960X-48FPD-L	48	2 SFP+	LAN Base	740W	Optional
WS-C2960X-48LPD-L	48	2 SFP+	LAN Base	370W	Optional
WS-C2960X-24PD-L	24	2 SFP+	LAN Base	370W	Optional
WS-C2960X-48TD-L	48	2 SFP+	LAN Base	-	Optional
WS-C2960X-24TD-L	24	2 SFP+	LAN Base	-	Optional
WS-C2960X-48FPS-L	48	4 SFP	LAN Base	740W	Optional

Part Number	10/100/1000 Ethernet Interfaces	Uplink Interfaces	Cisco IOS Software Feature Set	Available PoE Power	FlexStack-Plus Stacking
WS-C2960X-48LPS-L	48	4 SFP	LAN Base	370W	Optional
WS-C2960X-24PS-L	24	4 SFP	LAN Base	370W	Optional
WS-C2960X-24PSQ-L	24	2 SFP, 2 10/100/1000BT	LAN Base	92W	Optional
WS-C2960X-48TS-L	48	4 SFP	LAN Base	-	Optional
WS-C2960X-24TS-L	24	4 SFP	LAN Base	-	Optional
WS-C2960X-48TS-LL	48	2 SFP	LAN Lite	-	No
WS-C2960X-24TS-LL	24	2 SFP	LAN Lite	-	No

**Table 22.** Cisco Catalyst 2960-XR Configurations Ordering Information

Part Number	10/100/1000 Ethernet Interfaces	Uplink Interfaces	Cisco IOS Software Feature Set	Available PoE Power	Second FRU Power Supply Option	FlexStack-Plus Stacking
WS-C2960XR-48FPD-I	48	2 SFP+	IP Lite	740W	1025W	Optional
WS-C2960XR-48LPD-I	48	2 SFP+	IP Lite	370W	640W	Optional
WS-C2960XR-24PD-I	24	2 SFP+	IP Lite	370W	640W	Optional
WS-C2960XR-48TD-I	48	2 SFP+	IP Lite	-	250W	Optional
WS-C2960XR-24TD-I	24	2 SFP+	IP Lite	-	250W	Optional
WS-C2960XR-48FPS-I	48	4 SFP	IP Lite	740W	1025W	Optional
WS-C2960XR-48LPS-I	48	4 SFP	IP Lite	370W	640W	Optional
WS-C2960XR-24PS-I	24	4 SFP	IP Lite	370W	640W	Optional
WS-C2960XR-48TS-I	48	4 SFP	IP Lite	-	250W	Optional
WS-C2960XR-24TS-I	24	4 SFP	IP Lite	-	250W	Optional

**Table 23.** Cisco Catalyst 2960-X Accessories

Part Numbers	Description
C2960X-STACK	FlexStack-Plus hot-swappable stacking module
CAB-STK-E-0.5M	FlexStack-Plus stacking cable with a 0.5 m length
CAB-STK-E-1M	FlexStack-Plus stacking cable with a 1.0 m length
CAB-STK-E-3M	FlexStack-Plus stacking cable with a 3.0 m length
CAB-CONSOLE-RJ45	Console cable 6 feet with RJ45
CAB-CONSOLE-USB	Console cable 6 feet with USB Type A and mini-B connectors
PWR-CLP	Power cable restraining clip
RCKMNT-1RU-2KX=	Spare rack-mount kit for Cisco Catalyst 2960-X and 2960-XR Series for 19-inch racks
RCKMNT-REC-2KX=	1 RU recessed rack-mount kit for Cisco Catalyst 2960-X and 2960-XR Series

**Table 24.** Cisco Catalyst 2960-X Redundant Power Supply Options

Part Numbers	Description
PWR-RPS2300	Cisco Redundant Power System 2300 and blower, no power supply
BLNK-RPS2300=	Spare bay insert for Cisco Redundant Power System 2300 for Cisco Catalyst 2960 and Cisco Catalyst 2960-X switches
CAB-RPS2300-E=	Spare RPS2300 cable for Cisco Catalyst 2960-X switches
BLWR-RPS2300=	Spare 45 CFM blower for RPS 2300
C3K-PWR-750WAC=	RPS 2300 750W AC power supply spare for Cisco Catalyst 2960-X

For more information about the RPS-2300, visit [cisco.com/en/US/products/ps7130/index.html](http://cisco.com/en/US/products/ps7130/index.html).

**Table 25.** Cisco Catalyst 2960-XR Power Supply Options

Part Numbers	Description
<b>PWR-C2-250WAC<sup>4</sup></b>	Second FRU power supply and fan for all non-PoE 2960-XR switches, provides 250W AC of power
<b>PWR-C2-640WAC<sup>4</sup></b>	Second FRU power supply and fan for all 370W PoE+ 2960-XR switches, provides 640W AC of power
<b>PWR-C2-1025WAC<sup>4</sup></b>	Second FRU power supply and fan for all 740W PoE+ 2960-XR switches, provides 1025W AC of power
<b>PWR-C2-250WAC=</b>	Spare FRU power supply and fan for all non-PoE 2960-XR switches, provides 250W AC of power
<b>PWR-C2-640WAC=</b>	Spare FRU power supply and fan for all 370W PoE+ 2960-XR switches, provides 640W AC of power
<b>PWR-C2-1025WAC=</b>	Spare FRU power supply and fan for all 740W PoE+ 2960-XR switches, provides 1025W AC of power

**Table 26.** Cisco Catalyst 2960-X and 2960-XR SFP/SFP+ Modules

SFP and SFP+ Modules
For the list of supported SFP and SFP+ modules, visit <a href="http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html">http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html</a> .

**Table 27.** Power Cords for Cisco Catalyst 2960-X Product Family

Part Numbers	Description
<b>CAB-16AWG-AC</b>	AC power cord, 16AWG
<b>CAB-ACE</b>	AC power cord (Europe), C13, CEE 7, 1.5M
<b>CAB-L620P-C13-US</b>	Power cord, 250VAC, 15A, NEMA L6-20 to C13, US
<b>CAB-ACI</b>	AC power cord (Italy), C13, CEI 23-16, 2.5m
<b>CAB-ACU</b>	AC power cord (UK), C13, BS 1363, 2.5m
<b>CAB-ACA</b>	AC power cord (China/Australia), C13, AS 3112, 2.5m
<b>CAB-ACS</b>	AC power cord (Switzerland), C13, IEC 60884-1, 2.5m
<b>CAB-ACR</b>	AC power cord (Argentina), C13, EL 219 (IRAM 2073), 2.5m
<b>CAB-ACC</b>	CORD, PWR, CHINA, 10A, IEC 320, C13 (APN=CS-PWR-CH)
<b>CAB-JPN-12A</b>	CABASY, POWER CORD, JAPAN 2P, PSE, 12A @125VAC
<b>CAB-L620P-C13-JPN</b>	Power cord, 250VAC, 15A, NEMA L6-20 to C13, JAPAN
<b>CAB-IND</b>	Power cable for India
<b>CAB-C15-ISR</b>	Power cable for Israel
<b>CAB-ACSA</b>	Power cable for South Africa
<b>CAB-AC15A-90L-US</b>	15A AC power cord, left angle (United States)
<b>CAB-ACE-RA</b>	Power cord Europe, right angle
<b>CAB-ACI-RA</b>	Power cord Italian, right angle
<b>CAB-ACU-RA</b>	Power cord UK, right angle
<b>CAB-ACC-RA</b>	Power cord China, right angle
<b>CAB-ACA-RA</b>	Power cord, Australian, right angle
<b>CAB-ACS-RA</b>	Power cord for Switzerland, right angle
<b>CAB-ACR-RA</b>	Power cord, Argentina, right angle
<b>CAB-JPN-RA</b>	Power cord, Japan, right angle
<b>CAB-C15-CBN</b>	Cabinet jumper power cord, 250 VAC 13A, C14-C15 connectors
<b>CAB-ACBZ-12A</b>	AC power cord (Brazil) 12A/125V BR-3-20 plug for less than 12A device

<sup>4</sup> The first FRU power supply and fan module is configured automatically when the switch is ordered. The second redundant FRU power supply and fan module is an option while configuring the order.

**Table 28.** Power Cords for Cisco Catalyst 2960-XR Product Family

Part Numbers	Description
<b>CAB-3KX-AC</b>	AC Power Cord for Catalyst 2960-XR (North America)
<b>CAB-3KX-AC-AP</b>	AC Power Cord for Catalyst 2960-XR (Australia)
<b>CAB-3KX-AC-AR</b>	AC Power Cord for Catalyst 2960-XR (Argentina)
<b>CAB-3KX-AC-SW</b>	AC Power Cord for Catalyst 2960-XR (Switzerland)
<b>CAB-3KX-AC-UK</b>	AC Power Cord for Catalyst 2960-XR (United Kingdom)
<b>CAB-3KX-AC-JP</b>	AC Power Cord for Catalyst 2960-XR (Japan)
<b>CAB-3KX-AC-EU</b>	AC Power Cord for Catalyst 2960-XR (Europe)
<b>CAB-3KX-AC-IT</b>	AC Power Cord for Catalyst 2960-XR (Italy)
<b>CAB-3KX-AC-IN</b>	AC Power Cord for Catalyst 2960-XR (India)
<b>CAB-3KX-AC-CN</b>	AC Power Cord for Catalyst 2960-XR (China)
<b>CAB-3KX-AC-DN</b>	AC Power Cord for Catalyst 2960-XR (Denmark)
<b>CAB-3KX-AC-IS</b>	AC Power Cord for Catalyst 2960-XR (Israel)
<b>CAB-3KX-250VAC-JP</b>	Japan 250V AC Power Cord
<b>CAB-C15-CBN</b>	Cabinet Jumper Power Cord, 250 VAC 13A, C14-C15 Connectors
<b>CAB-ACBZ-10A</b>	AC Power Cord (Brazil) 10A/250V BR-3-10 plug for <10A device
<b>CAB-ACBZ-12A</b>	AC Power Cord (Brazil) 12A/125V BR-3-20 plug for <12A device

## Contact Cisco

For more information about Cisco products, contact:

- Phone: +1 800 553-NETS (6387)
- [Worldwide Product Support](#)
- Company Website: [cisco.com](http://cisco.com)



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](http://www.cisco.com/go/offices).

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

# Cisco Aironet 1552S Outdoor Access Point



**Outdoor Access Point for Wireless Sensor Networks**

- Integrated ISA100.11a compatible backbone router for wireless sensor networks
- Designed for hazardous environments (Certified Class 1 Div2/Zone2 enclosure)
- Compatibly with the Honeywell OneWireless™ Solution
- Cisco CleanAir® technology provides integrated spectrum intelligence for a self-configuring and self-healing network
- Cisco® ClientLink technology improves reliability and coverage for legacy Wi-Fi clients
- Improved 802.11n range and performance with 2 x 3 multiple-input multiple-output (MIMO) technology
- Multiple IEEE radio support (802.11a/n, 802.11b/g/n)
- Diversity antenna support for 802.15.4 sensor radio
- Multiple uplink options (Gigabit Ethernet-10/100/1000 BaseT, fiber Small Form-Factor Pluggable (SFP) interface)

**Cisco Aironet 1552SA Outdoor Access Point**

- 100-240 VAC power supply

**Cisco Aironet 1552SD Outdoor Access Point**

- 19-30 VDC power supply



## High-Performance Outdoor Access Point for Wireless Sensor Networks

The Cisco® Aironet® 1552S Outdoor Access Point is the latest model in the Cisco Aironet 1550 Series. The 1552S merges the ruggedized outdoor [802.11n](#) access point with an integrated, ISA100-compliant backbone router to provide a seamless solution for wireless sensor networks. The ISA100.11a radio has been designated specifically for mission-critical wireless connectivity to industrial sensor equipment. With an ISA100.11a radio integrated in an 802.11n-based access point, a single solution addresses the growing need for wireless mobility while also providing mission-critical connectivity for industrial sensing and monitoring equipment, such as gauges for water treatment plants, sensors for chemical plants, and vibration monitoring solutions for oil rigs.

This allows customers to combine business use cases, such as:

- Monitoring a chemical treatment plant while providing onsite security via wireless video surveillance
- Monitoring the equipment and gauges on an oil rig while an onsite worker downloads schematics, blueprints, or work instructions to a handheld Wi-Fi tablet
- Providing real-time information to an onsite engineer about changes to processes and equipment so that abnormalities can be dealt with immediately

The Cisco Aironet 1552S Access Point is also Class 1, Div 2/Zone 2 hazardous location certified. This means it is designed specifically for hazardous environments like oil and gas refineries, chemical plants, mining pits, and manufacturing facilities. The 1552S offers a single-box solution rather than requiring two separate wireless networks—one for 802.11n and one for ISA100 sensor networks.

By eliminating the extra power and network connections, which can be expensive to deploy in hazardous locations, the 1552S saves costs by reducing deployment times while offering a flexible, secure, and scalable mesh network

---

for high-performance wireless coverage for both Wi-Fi clients and ISA100.11a field instruments across large facilities. With all these benefits, the Cisco Aironet 1552S Outdoor Access Point can improve overall plant reliability, safety, and profitability.

The Cisco Aironet 1552S Outdoor Access Point supports multiple-device and multiple network application delivery methods, such as real-time seamless mobility, video surveillance, 3rd Generation (3G) and 4G data offload, and public and private Wi-Fi access. Designed to meet customer needs in a broad range of industries, the Cisco Aironet 1552S Outdoor Access Point offers the following additional benefits:

- **Flexible deployment options:** Access or mesh network, extension of an Ethernet network, and Ethernet, fiber, or wireless backhaul.
- **Cisco CleanAir® technology:** Integrated spectrum intelligence to detect, classify, and mitigate RF interference from unauthorized wireless bridges or malicious devices.
- **High-bandwidth video surveillance:** Video surveillance over Wi-Fi without the high cost of installing cables over long distances.
- **High-performance, multipurpose network:** Provides low CapEx and OpEx.
- **Integrated wired and wireless:** The Cisco Borderless Network Architecture provides cost savings with end-to-end network access solutions that include wireless, switching, routing, and security.

### Flexible, High-Performance Mesh

The Cisco Aironet 1552S Outdoor Access Point offers a flexible, secure, and scalable mesh platform that is part of the [Cisco Unified Wireless Network](#). It offers high-performance mobility across large oil and gas facilities, chemical plants, manufacturing yards, and mining pits. The 1552S provides high-performance device access through improved radio sensitivity and range with 802.11a/b/g/n multiple-input multiple-output (MIMO) technology including two spatial streams. Multiple uplink and power options are available. The 802.3af-compliant, Power-over-Ethernet (PoE) interface makes it easy to connect IP devices, such as IP video cameras. The housing is certified for Class 1, Div 2/Zone 2 deployment areas and provides a robust system that can withstand demanding, hazardous environments.

### Cisco CleanAir Technology

As part of the Cisco Aironet 1550 Series with Cisco CleanAir technology, the 1552S provides the highest-performance 802.11n connectivity for mission-critical outdoor networks by detecting interference from unauthorized devices, as well as common outdoor interference sources such as WiMAX networks and wireless bridging products. The 1550 Series uses chip-level intelligence to create a spectrum-aware, self-healing, and self-optimizing wireless network that mitigates the impact of wireless interference. Cisco CleanAir technology is a systemwide feature of the Cisco Unified Wireless Network that improves wireless network quality by detecting RF interference that other systems can't recognize, identifying the source, locating it, and then making automatic adjustments to optimize wireless coverage.

---

## RF Excellence

Building on the Cisco Aironet heritage of RF excellence, the Cisco Aironet 1550 Series delivers industry-leading performance for secure and reliable wireless connections. Industrial-grade parts, enterprise-class silicon-level intelligence, and optimized radios deliver a robust mobility experience. The Cisco Aironet 1550 Series provides a set of tools that deliver the robust, scalable wireless foundation required to realize the true potential of outdoor wireless mobility:

- [Cisco ClientLink technology](#) to raise the downlink performance to 802.11a/g clients, providing improved coverage and throughput to existing clients
- Radio resource management (RRM) for automated channel selection and power setting management of access points
- Advanced capabilities to select data rates, adjust power, and manage quality of service (QoS) for access points

## Centrally Managed Mesh Network

Central management and troubleshooting of the Cisco outdoor wireless access points prevent costly maintenance service calls to outdoor locations. The Cisco Prime Network Control System (NCS) works in conjunction with the Cisco Aironet Access Points and Cisco Wireless LAN Controllers to configure and manage the wireless networks. With Cisco Prime NCS, network administrators have a single solution for RF prediction, policy provisioning, network optimization, troubleshooting, security monitoring, and wireless LAN systems management. Cisco CleanAir technology is integrated into Cisco Prime NCS to provide real-time information on your outdoor network. Wireless network security is also a part of a unified wired and wireless solution. Cisco [wireless network security](#) offers the highest level of network security, which helps ensure that data remains private and secure and that the network is protected from unauthorized access.

## 802.11n Outdoor Access Point

The Cisco Aironet 1552S Outdoor Access Point contains a dual-radio system with radios that are compliant with IEEE 802.11a/n (5-GHz) and 802.11b/g/n (2.4-GHz) standards. The 1552S has three external antenna connections for three dual-band antennas. It has Ethernet and fiber Small Form-Factor Pluggable (SFP) backhaul options. This access point also has a PoE-out port and can power a video surveillance camera. A highly flexible model, the Cisco Aironet 1552S is designed for hazardous environments like oil and gas refineries, chemical plants, mining pits, and manufacturing factories. The Cisco Aironet 1552S Outdoor Access Point is Class 1, Div 2/Zone 2 hazardous location certified.

## ISA100-compliant Backbone Router

The Cisco Aironet 1552S Outdoor Access Point houses an ISA100.11a-compliant backbone router (BBR) that provides backhaul transport of the wireless sensor network traffic. The dual-radio BBR is based on the IEEE 802.15.4 standard and communicates to all ISA100.11a-compliant wireless field sensor devices. The BBR can also receive secure configuration codes via a windowed, infrared (IR) receiver.



## External Antennas

The Cisco Aironet 1552S use three Cisco AIR-ANT2547V-N-HZ antennas. These dual-band, omnidirectional, stick antennas have a gain of 4 dBi (2.4 GHz) and 7 dBi (5 GHz) and are IP66 rated for robustness in corrosive environments.

The Cisco Aironet 1552S also uses two Cisco AIR-ANT2450V-N-HZ antennas for the 802.15.4 diversity radios. These 2.4-GHz band omnidirectional, stick antennas have a gain of 5 dBi and are IP66 rated.

## Product Specifications

Table 1 lists specifications for the Cisco Aironet 1552S Outdoor Access Point.

**Table 1.** Cisco Aironet 1552S Outdoor Access Point Product Specifications

Item	Specification
<b>Part numbers</b>	<p><b>Cisco Aironet 1552S Access Point with AC power supply</b></p> <ul style="list-style-type: none"> <li>• AIR-CAP1552SA-A-K9</li> <li>• AIR-CAP1552SA-C-K9</li> <li>• AIR-CAP1552SA-E-K9</li> <li>• AIR-CAP1552SA-K-K9</li> <li>• AIR-CAP1552SA-M-K9</li> <li>• AIR-CAP1552SA-N-K9</li> <li>• AIR-CAP1552SA-Q-K9</li> <li>• AIR-CAP1552SA-R-K9</li> <li>• AIR-CAP1552SA-S-K9</li> <li>• AIR-CAP1552SA-T-K9</li> </ul> <p><b>Cisco Aironet 1552S Access Point with DC power supply</b></p> <ul style="list-style-type: none"> <li>• AIR-CAP1552SD-A-K9</li> <li>• AIR-CAP1552SD-C-K9</li> <li>• AIR-CAP1552SD-E-K9</li> <li>• AIR-CAP1552SD-K-K9</li> <li>• AIR-CAP1552SD-M-K9</li> <li>• AIR-CAP1552SD-N-K9</li> <li>• AIR-CAP1552SD-Q-K9</li> <li>• AIR-CAP1552SD-R-K9</li> <li>• AIR-CAP1552SD-S-K9</li> <li>• AIR-CAP1552SD-T-K9</li> </ul> <p>Not all regulatory domains have been approved. Refer to the Cisco WLAN compliance page to the latest information.</p>
<b>802.11n Capabilities</b>	<ul style="list-style-type: none"> <li>• 2 x 3 multiple-input multiple-output (MIMO) with two spatial streams</li> <li>• Legacy beamforming</li> <li>• 20- and 40-MHz channels</li> <li>• PHY data rates up to 300 Mbps</li> <li>• Packet aggregation: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)</li> <li>• 802.11 dynamic frequency selection (DFS)</li> <li>• Cyclic shift diversity (CSD) support</li> </ul>
<b>ISA100 Backbone Router Capabilities</b>	<p>ISA100.11a backbone router provides:</p> <ul style="list-style-type: none"> <li>• 802.15.4 radios with diversity receivers (1 Tx, 2 Rx)</li> <li>• Designed to meet ISA100.11a specifications</li> <li>• External IR receiver for receiving secure network keys from IrDA-compatible device</li> </ul>

Item	Specification				
<b>Data Rates Supported</b>	<b>802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps</b>				
	<b>802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps</b>				
	<b>802.11n data rates (2.4 GHz and 5 GHz):</b>				
	<b>MCS Index<sup>1</sup></b>				
	<b>GI<sup>2</sup> = 800 ns</b>				
	<b>GI = 400 ns</b>				
	<b>20-MHz Rate (Mbps)</b>	<b>40-MHz Rate (Mbps)</b>	<b>20-MHz Rate (Mbps)</b>	<b>40-MHz Rate (Mbps)</b>	
	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
	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	
	<b>Note:</b> The above numbers represent the over-the-air supported rates. Actual usable throughput will be determined by factors such as protocol overhead, RF channel contention, and interference.				
<b>Frequency Band and 20-MHz Operating Channels</b>	-A Domain: <ul style="list-style-type: none"> <li>• 2.400 to 2.4835 GHz; 11 channels</li> <li>• 5.250 to 5.850 GHz; 14 channels</li> </ul> -C Domain: <ul style="list-style-type: none"> <li>• 2.400 to 2.4835 GHz; 13 channels</li> <li>• 5.725 to 5.850 GHz; 5 channels</li> </ul> -E Domain: <ul style="list-style-type: none"> <li>• 2.401 to 2.4835 GHz; 13 channels</li> <li>• 5.470 to 5.725 GHz; 8 channels</li> </ul> -K Domain: <ul style="list-style-type: none"> <li>• 2.400 to 2.4835 GHz; 11 channels</li> <li>• 5.250 to 5.825 GHz; 14 channels</li> </ul> -M Domain: <ul style="list-style-type: none"> <li>• 2.400 to 2.4835 GHz; 13 channels</li> <li>• 5.470 to 5.850 GHz; 12 channels</li> </ul> -N Domain: <ul style="list-style-type: none"> <li>• 2.400 to 2.4835 GHz; 11 channels</li> <li>• 5.725 to 5.850 GHz; 5 channels</li> </ul> -Q Domain: <ul style="list-style-type: none"> <li>• 2.400 to 2.4835 GHz; 13 channels</li> <li>• 5.470 to 5.725 GHz; 11 channels</li> </ul> -R Domain: <ul style="list-style-type: none"> <li>• 2.400 to 2.4835 GHz; 13 channels</li> </ul>				

<sup>1</sup> MCS Index: The Modulation and Coding Scheme (MCS) index determines the number of spatial streams, the modulation, the coding rate, and data rate values.

<sup>2</sup> GI: A guard interval (GI) between symbols helps receivers overcome the effects of multipath delays.

Item	Specification	
<b>Frequency range (802.15.4 radio)</b>	<ul style="list-style-type: none"> <li>• 5.250 to 5.725 GHz; 11 channels</li> </ul> -S Domain: <ul style="list-style-type: none"> <li>• 2.400 to 2.4835 GHz; 13 channels</li> <li>• 5.725 to 5.850 GHz; 5 channels</li> </ul> -T Domain: <ul style="list-style-type: none"> <li>• 2.400 to 2.4835 GHz; 11 channels</li> <li>• 5.470 to 5.850 GHz; 13 channels</li> <li>• 2.405 to 2.475 GHz</li> </ul>	
<b>Note:</b> This varies by regulatory domain. Refer to the product documentation for specific details for each regulatory domain.		
<b>Maximum Number of Nonoverlapping Channels</b>	<b>2.4 GHz</b> <ul style="list-style-type: none"> <li>• 802.11b/g:               <ul style="list-style-type: none"> <li>◦ 20 MHz: 3</li> </ul> </li> <li>• 802.11n:               <ul style="list-style-type: none"> <li>◦ 20 MHz: 3</li> </ul> </li> </ul>	<b>5 GHz</b> <ul style="list-style-type: none"> <li>• 802.11a:               <ul style="list-style-type: none"> <li>◦ 20 MHz: 16</li> </ul> </li> <li>• 802.11n:               <ul style="list-style-type: none"> <li>◦ 20 MHz: 16</li> <li>◦ 40 MHz: 8</li> </ul> </li> </ul>
<b>Note:</b> This varies by regulatory domain. Refer to the product documentation for specific details for each regulatory domain.		
<b>Maximum Transmit Power</b>	<b>2.4 GHz</b> <ul style="list-style-type: none"> <li>• 802.11b (Complementary Code Keying [CCK])               <ul style="list-style-type: none"> <li>◦ 28 dBm with 2 antennas</li> </ul> </li> <li>• 802.11g (non HT duplicate mode)               <ul style="list-style-type: none"> <li>◦ 28 dBm with 2 antennas</li> </ul> </li> <li>• 802.11n (HT20)               <ul style="list-style-type: none"> <li>◦ 28 dBm with 2 antennas</li> </ul> </li> <li>• 802.15.4               <ul style="list-style-type: none"> <li>◦ 18 dBm with 1 antenna</li> </ul> </li> </ul>	<b>5 GHz</b> <ul style="list-style-type: none"> <li>• 802.11a               <ul style="list-style-type: none"> <li>◦ 28 dBm with 2 antennas</li> </ul> </li> <li>• 802.11n non-HT duplicate (802.11a duplicate) mode               <ul style="list-style-type: none"> <li>◦ 28 dBm with 2 antennas</li> </ul> </li> <li>• 802.11n (HT20)               <ul style="list-style-type: none"> <li>◦ 27 dBm with 2 antennas</li> </ul> </li> <li>• 802.11n (HT40)               <ul style="list-style-type: none"> <li>◦ 27 dBm with 2 antennas</li> </ul> </li> </ul>
<b>Note:</b> The maximum power setting will vary by channel and according to individual country regulations. Refer to the product documentation for specific details.		
<b>Network Interface</b>	<ul style="list-style-type: none"> <li>• 10/100/1000BASE-T Ethernet, autosensing (RJ-45)</li> <li>• Fiber SFP</li> </ul>	
<b>Dimensions (W x L x H)</b>	12.0 in. x 7.8 in. x 6.4 in. (30.48 cm x 19.81 cm x 16.26 cm) (including antenna mount)	
<b>Weight</b>	1552S: 17.6 lb (8 kg) Pole mounting bracket: 6.1 lb (2.8 kg)	
<b>Environmental</b>	Operating temperature: -40 to 55°C (-40 to 131°F) plus Solar Loading Storage temperature: -50 to 85°C (-58 to 185°F) Humidity: 0-100% (condensing) Wind resistance: <ul style="list-style-type: none"> <li>• Up to 100 MPH sustained winds</li> <li>• Up to 165 MPH wind gusts</li> </ul>	
<b>Environmental Ratings</b>	<ul style="list-style-type: none"> <li>• IP67</li> <li>• NEMA Type 4X</li> </ul>	
<b>Antenna Gain</b>	<ul style="list-style-type: none"> <li>• External Dual-Band Omnidirectional Antennas (AIR-ANT2547V-N-HZ)               <ul style="list-style-type: none"> <li>◦ 4 dBi (2.4 GHz), 7 dBi (5 GHz)</li> </ul> </li> <li>• External 2.4 GHz Omnidirectional Antennas (AIR-ANT2450V-N-HZ)               <ul style="list-style-type: none"> <li>◦ 5 dBi</li> </ul> </li> </ul>	
<b>Powering Options</b>	<b>1552SA</b> <ul style="list-style-type: none"> <li>• 100-240 VAC, 47-63 Hz</li> <li>• 12 VDC</li> <li>• 47 W</li> </ul>	<b>1552SD</b> <ul style="list-style-type: none"> <li>• 19-30 VDC</li> <li>• 12 VDC</li> <li>• 39 W</li> </ul>
<b>Note:</b> The power consumption above does not include powering an external PoE (802.3af) device; allow for an additional 20 W. If using fiber SFP backhaul, add an additional 1 W.		
<b>Warranty</b>	90 days	

Item	Specification
Compliance	<p><b>Safety</b></p> <ul style="list-style-type: none"> <li>• UL 60950, 2nd Edition</li> <li>• CAN/CSA-C22.2 No. 60950, 2nd Edition</li> <li>• IEC 60950, 2nd Edition</li> <li>• EN 60950, 2nd Edition</li> </ul> <p><b>Immunity</b></p> <ul style="list-style-type: none"> <li>• &lt;= 5 mJ for 6kV/3kA @ 8/20 ms waveform</li> <li>• ANSI/IEEE C62.41</li> <li>• EN61000-4-5 Level 4 AC Surge Immunity</li> <li>• EN61000-4-4 Level 4 Electrical Fast Transient Burst Immunity</li> <li>• EN61000-4-3 Level 4 EMC Field Immunity</li> <li>• EN61000-4-2 Level 4 ESD Immunity</li> <li>• EN60950 Overvoltage Category IV</li> </ul> <p><b>Radio approvals</b></p> <ul style="list-style-type: none"> <li>• FCC Part 15.247, 15.407</li> <li>• FCC Bulletin OET-65C</li> <li>• RSS-210</li> <li>• RSS-102</li> <li>• AS/NZS 4268.2003</li> <li>• EN 300 328</li> <li>• EN 301 893</li> </ul> <p><b>EMI and susceptibility</b></p> <ul style="list-style-type: none"> <li>• FCC part 15.107, 15.109</li> <li>• ICES-003</li> <li>• EN 301 489-1, -17</li> </ul> <p><b>Security</b></p> <ul style="list-style-type: none"> <li>• Wireless bridging/mesh <ul style="list-style-type: none"> <li>◦ X.509 digital certificates</li> <li>◦ MAC address authentication</li> <li>◦ Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP)</li> </ul> </li> <li>• Wireless access <ul style="list-style-type: none"> <li>◦ 802.11i, Wi-Fi Protected Access (WPA2), WPA</li> <li>◦ 802.1X authentication, including Extensible Authentication Protocol and Protected EAP (EAP-PEAP), EAP Transport Layer Security (EAP-TLS), EAP-Tunneled TLS (EAP-TTLS), and Cisco LEAP</li> <li>◦ Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP)</li> <li>◦ VPN passthrough</li> <li>◦ IP Security (IPsec), Layer 2 Tunneling Protocol (L2TP)</li> </ul> </li> <li>• MAC address filtering</li> </ul> <p><b>Other</b></p> <ul style="list-style-type: none"> <li>• CSA: Class I, Division 2, Groups A, B, C and D</li> <li>• ATEX: Class I, Zone 2; Ex nA II, T5</li> </ul>

## Plan, Build, and Run Services for a Seamless Outdoor Experience

Professional services from Cisco and Cisco Advanced Wireless LAN Specialized Partners facilitate a smooth deployment of the next-generation wireless outdoor solution, while tightly integrating it with the wired and indoor wireless networks. Based on proven methodologies for planning and deploying end-to-end solutions with secure voice, video, and data technologies and years of experience designing and implementing some of the world's most complex, enterprise-class wireless networks, our specialists can help you optimize mobile connectivity to transform your business operations.

We work with your IT staff to see that your architecture, physical sites, and operational staff are ready to support Cisco's integrated, next-generation, outdoor wireless solution that combines the high performance of the 802.11n standard and Cisco CleanAir technology.

---

## For More Information

For more information about Cisco wireless mesh, contact your local account representative or visit:

<http://www.cisco.com/go/outdoorwireless>

For more information about the Cisco Unified Wireless Network framework, visit:

<http://www.cisco.com/go/unifiedwireless>

For more information about the Cisco service provider Wi-Fi solution, visit:

<http://www.cisco.com/go/ap1550>

For more information about the Cisco Wireless LAN Services, 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](http://www.cisco.com/go/offices).

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

# Cisco Aironet 600 Series OfficeExtend Access Points


<p><b>Performance with Investment Protection</b></p> <ul style="list-style-type: none"> <li>• Dual-radio, 802.11n access point avoids congestion from cordless phones, baby monitors, wireless game consoles, and microwave ovens</li> <li>• Backward-compatible with 802.11a/b/g clients</li> </ul>
<p><b>Remote Connectivity to Corporate Resources</b></p> <ul style="list-style-type: none"> <li>• Supports up to three corporate service set identifiers (SSIDs) and 15 wireless clients</li> <li>• Four Ethernet ports: Up to two for corporate access and the rest for personal use</li> <li>• Supports voice-over-Wi-Fi with dual-mode phones, soft phones, or Cisco Unified Wireless IP Phones</li> <li>• Split tunnel for printing - use your personal printer while connected to the corporate WLAN</li> </ul>
<p><b>Easy Installation</b></p> <ul style="list-style-type: none"> <li>• Sleek design ideal for desktop placement</li> </ul>
<p><b>Simplified Network Management</b></p> <ul style="list-style-type: none"> <li>• Minimal setup and maintenance requirements (zero-touch end-user deployment)</li> <li>• Numerous controller-based deployment options</li> <li>• Management similar to corporate WLAN, using the same infrastructure and devices</li> </ul>
<p><b>Secure Connections</b></p> <ul style="list-style-type: none"> <li>• Supports highly secure corporate wireless connectivity to employees' homes</li> <li>• Allows spouses, partners, and children to access the Internet without introducing additional security risks to corporate policy</li> </ul>



## Powerful [802.11n](#) Dual-Radio Performance

The Cisco® Aironet® 600 Series OfficeExtend [Access Points](#) provide highly secure enterprise [wireless](#) coverage to the home. These dual-band, 802.11n access points extend the corporate network to home teleworkers and mobile contractors. The access point connects to the home's broadband Internet access and establishes a highly secure tunnel to the corporate network so that remote employees can access data, voice, video, and cloud services for a [mobility](#) experience consistent with that at the corporate office. The dual-band, simultaneous support for 2.4-GHz and 5-GHz radio frequencies helps assure that corporate devices are not affected by congestion caused by common household devices that use the 2.4-GHz band. The Cisco Aironet 600 Series OfficeExtend Access Points are purposely designed for the teleworker by supporting secure corporate data access and maintaining connectivity for personal home devices with segmented home traffic.

## How It Works

The same services that are available on the [wireless network](#) at the corporate office are securely accessed through the Cisco Aironet

600 Series from a remote location. Data, voice, and video as well as applications such as Cisco Unified MeetingPlace® conferencing, Cisco WebEx® technology, and dual-mode phones are supported by the Cisco Aironet 600 Series.

For the initial setup at a home office, the remote worker plugs the access point into a home router connected to or integrated with their broadband modem. The Cisco Aironet 600 Series access point is provisioned in advance and will automatically set up a secure tunnel to the corporate headquarters with a Cisco [wireless controller](#). A preregistered corporate IP phone can also automatically connect with Cisco Unified Communications Manager to access the corporate phone number, voicemail, and user settings.

## How the Remote Workforce Benefits

The Cisco Aironet 600 Series helps improve workforce productivity, business resiliency, and work schedule flexibility while reducing travel costs and carbon emissions. It is targeted toward commercial, enterprise, and service provider networks across all industries. The Cisco Aironet 600 Series is appropriate for employees who need reliable and consistent access to networked business services at home or at work, as well as telecommuters who require the same wireless connectivity as at the corporate site. Voice costs are reduced, since users can use Wi-Fi instead of cellular coverage for voice calls.

Table 1 lists the features and benefits of the Cisco Aironet 600 Series OfficeExtend [Access Points](#).

**Table 1.** Features and Benefits

Feature	Benefits
<b>Performance</b>	<ul style="list-style-type: none"> <li>Dual-radio, dual-band, 802.11n access point for the home that provides highly secure, reliable wired and wireless connectivity to home or remote offices.</li> <li>Supports both the 2.4-GHz and 5-GHz radio frequency band simultaneously, allowing users to avoid congestion from home devices.</li> </ul>
<b>Simplified operations and management</b>	<ul style="list-style-type: none"> <li>Extends real-time services such as voice, wireless, video, and data to remote locations that have no IT staff.</li> <li>Management is similar to that of the corporate <a href="#">wireless LAN</a>, using the same infrastructure and devices (Cisco wireless controllers, Cisco Prime™ Infrastructure, and Cisco Aironet access points).</li> <li>Cisco Unified Wireless IP Phones may be preconfigured or added in the future.</li> </ul>
<b>Robust security</b>	<ul style="list-style-type: none"> <li>The Cisco Aironet 600 Series establishes a secure Datagram Transport Layer Security (DTLS) connection between the access point and the controller to offer remote WLAN connectivity, using the same profile as at the corporate office.</li> <li>Secure tunneling mitigates risks of viruses and attacks on the corporate network found in split-tunneling scenarios.</li> <li>Segmentation of home and corporate traffic maintains home-device connectivity without introducing security risks to corporate policy.</li> </ul>
<b>End-to-end voice services</b>	<ul style="list-style-type: none"> <li>Supports <a href="#">unified communications</a> for improved collaboration through messaging, presence, and conferencing.</li> <li>Supports all <a href="#">Cisco Unified Wireless IP Phones</a> for cost-effective, real-time voice services.</li> </ul>
<b>Environmentally responsible</b>	<ul style="list-style-type: none"> <li>Enables best practices for green initiatives by reducing commuting hours and emissions.</li> </ul>

## Product Specifications

Table 2 lists the product specifications for the Cisco Aironet 600 Series OfficeExtend Access Points.

**Table 2.** Product Specifications

Item	Specification
<b>Part numbers</b>	<p><b>Cisco Aironet 600 OfficeExtend Series Access Points</b></p> <ul style="list-style-type: none"> <li>AIR-OEAP602I-x-K9: Dual-band controller-based 802.11a/g/n</li> <li>AIR-OEAP602I-xK910: Eco-pack (dual-band 802.11a/g/n) 10 quantity controller-based access points</li> </ul> <p><b>Regulatory domains: (x = regulatory domain)</b></p> <p>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, visit <a href="http://www.cisco.com/go/aironet/compliance">http://www.cisco.com/go/aironet/compliance</a>.</p>
<b>Software</b>	<ul style="list-style-type: none"> <li>Cisco Unified Wireless Network Software Release 7.0 MR1 or later</li> </ul>
<b>Controllers supported</b>	<ul style="list-style-type: none"> <li>Cisco Virtual, 2500, 5500, 7500, and 8500 Series Wireless Controllers and Cisco Wireless Services Module 2 (WiSM2)</li> </ul>
<b>802.11n</b>	<ul style="list-style-type: none"> <li>Multiple-input multiple-output (MIMO) with two spatial streams</li> <li>Maximal ratio combining (MRC)</li> <li>20- and 40-MHz channels</li> <li>PHY data rates up to 300 Mbps<sup>1</sup></li> <li>Packet aggregation: A-MPDU (Tx/Rx)</li> <li>Cyclic shift diversity (CSD) support</li> </ul>

<sup>1</sup> For encrypted corporate traffic, the maximum throughput supported is 10 Mbps.

Item	Specification				
Data rates supported	<b>802.11a:</b> 6, 9, 12, 18, 24, 36, 48, and 54 Mbps				
	<b>802.11g:</b> 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps				
	<b>802.11n data rates (2.4 GHz and 5 GHz):</b>				
	MCS Index <sup>2</sup>	GI <sup>3</sup> = 800 ns		GI = 400 ns	
		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
	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	<b>A Regulatory Domain:</b>		<b>N Regulatory Domain:</b>		
	<ul style="list-style-type: none"> <li>• 2.412 to 2.462 GHz; 11 channels</li> <li>• 5.180 to 5.240 GHz; 4 channels</li> <li>• 5.745 to 5.825 GHz; 5 channels</li> </ul>		<ul style="list-style-type: none"> <li>• 2.412 to 2.462 GHz; 11 channels</li> <li>• 5.180 to 5.240 GHz; 4 channels</li> <li>• 5.745 to 5.825 GHz; 5 channels</li> </ul>		
	<b>C Regulatory Domain:</b>		<b>P Regulatory Domain:</b>		
	<ul style="list-style-type: none"> <li>• 2.412 to 2.472 GHz; 13 channels</li> <li>• 5.745 to 5.825 GHz; 5 channels</li> </ul>		<ul style="list-style-type: none"> <li>• 2.412 to 2.472 GHz; 13 channels</li> <li>• 5.180 to 5.240 GHz; 4 channels</li> </ul>		
	<b>E Regulatory Domain:</b>		<b>R Regulatory Domain:</b>		
	<ul style="list-style-type: none"> <li>• 2.412 to 2.472 GHz; 13 channels</li> <li>• 5.180 to 5.240 GHz; 4 channels</li> </ul>		<ul style="list-style-type: none"> <li>• 2.412 to 2.472 GHz; 13 channels</li> <li>• 5.180 to 5.240 GHz; 4 channels</li> <li>• 5.745 to 5.805 GHz; 4 channels</li> </ul>		
	<b>I Regulatory Domain:</b>		<b>S Regulatory Domain:</b>		
	<ul style="list-style-type: none"> <li>• 2.412 to 2.472 GHz; 13 channels</li> <li>• 5.180 to 5.240 GHz; 4 channels</li> </ul>		<ul style="list-style-type: none"> <li>• 2.412 to 2.472 GHz; 13 channels</li> <li>• 5.180 to 5.240 GHz; 4 channels</li> <li>• 5.745 to 5.825 GHz; 5 channels</li> </ul>		
	<b>K Regulatory Domain:</b>		<b>T Regulatory Domain:</b>		
	<ul style="list-style-type: none"> <li>• 2.412 to 2.472 GHz; 13 channels</li> <li>• 5.180 to 5.240 GHz; 4 channels</li> <li>• 5.745 to 5.805 GHz; 4 channels</li> </ul>		<ul style="list-style-type: none"> <li>• 2.412 to 2.462 GHz; 11 channels</li> <li>• 5.745 to 5.825 GHz; 5 channels</li> </ul>		
<b>Note:</b> This varies by regulatory domain. Refer to the product documentation for specific details for each regulatory domain.					
Maximum number of nonoverlapping channels	<b>2.4 GHz</b>		<b>5 GHz</b>		
	<ul style="list-style-type: none"> <li>• 802.11b/g: 20 MHz: 3</li> <li>• 802.11n: 20 MHz: 3</li> </ul>		<ul style="list-style-type: none"> <li>• 802.11a: 20 MHz: 9</li> <li>• 802.11n: 20 MHz: 9, 40 MHz: 4</li> </ul>		
<b>Note:</b> This varies by regulatory domain. Refer to the product documentation for specific details for each regulatory domain.					

<sup>2</sup> MCS Index: The Modulation and Coding Scheme (MCS) index determines the number of spatial streams, the modulation, the coding rate, and data rate values.

<sup>3</sup> GI: A Guard Interval (GI) between symbols helps receivers overcome the effects of multipath delays.



Item	Specification	
<b>Receive sensitivity</b>	<b>2.4 GHz</b> <ul style="list-style-type: none"> <li>802.11b: -87 dBm typical @ 11 Mbps</li> <li>802.11g: -77 dBm typical @ 54 Mbps</li> <li>802.11n 20 MHz: -71 dBm typical @ MCS15</li> <li>802.11n 40 MHz: -68 dBm typical @ MCS15</li> </ul>	<b>5 GHz</b> <ul style="list-style-type: none"> <li>802.11a: -74 dBm typical @ 54 Mbps</li> <li>802.11n 20 MHz: -68 dBm typical @ MCS15</li> <li>802.11n 40 MHz: -65 dBm typical @ MCS15</li> </ul>
<b>Maximum transmit power</b>	<b>2.4 GHz</b> <ul style="list-style-type: none"> <li>802.11b (CCK): 20 dBm with one antenna</li> <li>802.11g: 20 dBm with 2 antennas</li> <li>802.11n (HT20): 20 dBm with 2 antennas</li> <li>802.11n (HT40): 20 dBm with 2 antennas</li> </ul>	<b>5 GHz</b> <ul style="list-style-type: none"> <li>802.11a: 20 dBm with 2 antennas</li> <li>802.11n (HT20): 20 dBm with 2 antennas</li> <li>802.11n (HT40): 20 dBm with 2 antennas</li> </ul>
<p><b>Note:</b> The maximum power setting will vary by channel and according to individual country regulations. Refer to the product documentation for specific details.</p>		
<b>Integrated antenna</b>	<ul style="list-style-type: none"> <li>2.4 GHz, gain 3.5 dBi, horizontal beamwidth 360°</li> <li>5 GHz, gain 4.0 dBi, horizontal beamwidth 360°</li> </ul>	
<b>Interfaces</b>	<ul style="list-style-type: none"> <li>4x 10/100/1000BASE-T autosensing (RJ-45)</li> <li>1x 10/100/1000BASE-T WAN port (RJ-45)</li> <li>USB (not used)</li> </ul>	
<b>Indicators</b>	<ul style="list-style-type: none"> <li>Status LED indicates boot loader status, association status, operating status, boot loader errors, port status</li> </ul>	
<b>Dimensions (W x L x H)</b>	<ul style="list-style-type: none"> <li>Access point (without cradle): 7.75 x 7 x 1.6 in. (195.3 x 176.3 x 39.65 mm)</li> <li>Access point (with cradle): 8.1 x 7.0 x 2.7 in. (206.15 x 176.3 x 67 mm)</li> </ul>	
<b>Weight</b>	<ul style="list-style-type: none"> <li>0.99 lb (0.452 kg) without cradle</li> <li>1.44 lb (0.653 kg) with cradle</li> </ul>	
<b>Environmental</b>	<ul style="list-style-type: none"> <li>Nonoperating (storage) temperature: -13° to +140°F (-25° to 60°C)</li> <li>Operating temperature: 32° to 104°F (0° to 40°C)</li> <li>Operating humidity: 10% to 80% relative humidity (noncondensing)</li> </ul>	
<b>System memory</b>	<ul style="list-style-type: none"> <li>64 MB DRAM</li> <li>16 MB flash</li> </ul>	
<b>Power options</b>	<ul style="list-style-type: none"> <li>Cisco AP600 local power supply: 100 to 240 VAC; 50 to 60 Hz (AIR-PWR-ADTR-cc, where cc is country code as follows: AP=Asia Pacific; AR=Argentina/Uruguay; AU=Australia; BR=Brazil; CE=Central Europe; CH=China; DM=Denmark; IS=Israel; IT=Italy; JP=Japan; NA=North America; SA=South Africa; SW=Switzerland; UK=United Kingdom)</li> </ul>	
<b>Power draw</b>	<ul style="list-style-type: none"> <li>Consumption: 12W normal, 15W maximum</li> </ul>	
<b>Warranty</b>	Limited Lifetime Hardware Warranty	
<b>Compliance and safety standards</b>	<ul style="list-style-type: none"> <li><b>Safety</b> <ul style="list-style-type: none"> <li>UL 60950-1, 2<sup>nd</sup> Edition</li> <li>CAN/CSA-C22.2 No. 60950-1, 2<sup>nd</sup> Edition</li> <li>IEC 60950-1, 2<sup>nd</sup> Edition</li> <li>EN 60950-1, 2<sup>nd</sup> Edition</li> </ul> </li> <li><b>Radio Approvals</b> <ul style="list-style-type: none"> <li>FCC Part 15.247, 15.407</li> <li>RSS-210 (Canada)</li> <li>EN 300 328, EN 301 893 (Europe)</li> <li>ARIB-STD 33 (Japan)</li> <li>ARIB-STD 66 (Japan)</li> <li>ARIB-STD T71 (Japan)</li> <li>AS/NZS 4268.2003 (Australia and New Zealand)</li> <li>EMI and susceptibility (Class B)</li> <li>FCC Part 15.107 and 15.109</li> <li>ICES-003 (Canada)</li> <li>VCCI (Japan)</li> <li>EN 301 489-1 and -17 (Europe)</li> </ul> </li> <li><b>IEEE Standard</b> <ul style="list-style-type: none"> <li>IEEE 802.11a/b/g, IEEE 802.11n, IEEE 802.11h, IEEE 802.11d</li> </ul> </li> </ul>	

Item	Specification
	<ul style="list-style-type: none"> <li>• <b>Security</b> <ul style="list-style-type: none"> <li>◦ 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA</li> <li>◦ 802.1X</li> <li>◦ Advanced Encryption Standard (AES), Temporal Key Integrity Protocol (TKIP)</li> </ul> </li> <li>• <b>EAP Type(s)</b> <ul style="list-style-type: none"> <li>◦ Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)</li> <li>◦ EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2)</li> <li>◦ Protected EAP (PEAP) v0 or EAP-MSCHAPv2</li> <li>◦ Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)</li> <li>◦ PEAPv1 or EAP-Generic Token Card (GTC)</li> <li>◦ EAP-Subscriber Identity Module (SIM)</li> </ul> </li> <li>• <b>Multimedia</b> <ul style="list-style-type: none"> <li>◦ Wi-Fi Multimedia (WMM)</li> </ul> </li> <li>• <b>Other</b> <ul style="list-style-type: none"> <li>◦ FCC Bulletin OET-65C</li> <li>◦ RSS-102</li> </ul> </li> </ul>

## Service and Support

Realize the full business value of your Cisco Unified Wireless Network more quickly with intelligent, personalized services from Cisco and our partners. Cisco Services offer proven wireless architectures aligned to your business goals and tightly integrated with media-rich, real-time mobility applications. With our breadth and depth of expertise, we support your success every step of the way as you deploy, manage, and scale integrated wireless solutions for optimized performance, security, and management. Sharing knowledge and leading practices, we can help you create a secure, mobile, and interactive business environment to provide a foundation for innovation, agility, and differentiation.

## For More Information

For more information about the Cisco Aironet 600 Series OfficeExtend Access Points, visit <http://www.cisco.com/go/wireless> or contact your local 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](http://www.cisco.com/go/offices).

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

# Cisco ASA 5500-X Series Next-Generation Firewalls

## Product Overview

Cisco® ASA 5500-X Series Next-Generation Firewalls integrate the world's most proven stateful inspection firewall with a comprehensive suite of next-generation firewall services for networks of all sizes - small and midsize businesses with one or more locations, large enterprises, service providers, and mission-critical data centers. Cisco ASA 5500-X Series Next-Generation Firewalls deliver Cisco MultiScale™ performance with industry-leading service flexibility, modular scalability, feature extensibility, and low deployment and operation costs.

## Features and Benefits

The Cisco ASA 5500-X Series Next-Generation Firewalls are designed to meet the network, budget, and performance needs of small offices while delivering enterprise-strength security. Available in a wide range of sizes, all models deliver the same level of security that protects the networks of some of the largest and most security-conscious companies in the world. They also provide next-generation firewall services such as Cisco Application Visibility and Control, web security, botnet filtering and intrusion prevention, so you can take advantage of new applications and devices without compromising security.

Cisco ASA 5500-X Series Next-Generation Firewalls for small offices and branch locations protect critical assets through:

- Exceptional next-generation firewall services that provide the visibility and detailed control that your enterprise needs to safely take advantage of new applications and devices<sup>1</sup>
- Cisco Application Visibility and Control (AVC) to control specific behaviors within allowed microapplications
- Cisco Web Security Essentials (WSE) to restrict web and web application use based on the reputation of a site
- Broad and deep network security through an array of integrated cloud- and software-based next-generation firewall services backed by Cisco Security Intelligence Operations (SIO)
- A highly effective intrusion prevention system (IPS) with Cisco Global Correlation
- A high-performance VPN and always-on remote access
- The ability to enable additional security services quickly and easily in response to changing needs

---

<sup>1</sup> Please contact your sales representative for availability.

## Cisco ASA 5500-X Series Next Generation Firewalls






The Cisco ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X are next-generation firewalls that combine the most widely deployed stateful inspection firewall in the industry with a comprehensive suite of next-generation network security services - for comprehensive security without compromise. They provide multiple security services and redundant power supplies and enable consistent security enforcement throughout the organization. In addition to comprehensive stateful inspection firewall capabilities, optional features include integrated cloud- and software-based security services - Cisco Application Visibility and Control (AVC), Cisco Web Security Essentials (WSE), Cisco Cloud Web Security (CWS), and IPS. Cisco Next-Generation Firewalls are managed by [Cisco Prime Security Manager](#). These models range in their performance and throughput capabilities not only in the hardware platforms but also in the services and number of users that can be supported on each model. Depending on the customer requirements and performance needs, they can be deployed at small office, Internet edge, and even data center locations.

This series of next-generation firewalls is built on the same proven security platform as the rest of the ASA Family of firewalls and delivers exceptional application visibility and control along with superior performance and operational efficiency. These firewalls provide next-generation services that make it possible to take advantage of new applications and devices without compromising security. Unlike other firewalls, the Cisco ASA 5500-X Series keeps pace with rapidly evolving needs by offering end-to-end network intelligence gained from combining the visibility of local traffic with in-depth global network intelligence. The Cisco ASA 5500-X Series is supported by:

- [Cisco TrustSec® technology](#)
- [Cisco AnyConnect® Secure Mobility Solution for unique mobile client insight](#)
- [Cisco SIO for near-real-time threat information and proactive protection](#)
- [Cisco ASA Next-Generation Firewall Services](#)

Table 1 compares the features and capacities of the different ASA 5500-X Series Next-Generation Firewalls for small offices, branch locations, and Internet edge deployments.

**Table 1.** Cisco ASA 5500-X Series Next-Generation Firewalls

Feature	Cisco ASA 5512-X, Security Plus	Cisco ASA 5515-X	Cisco ASA 5525-X	Cisco ASA 5545-X	Cisco ASA 5555-X
					
Stateful inspection throughput (maximum <sup>2</sup> )	1 Gbps	1.2 Gbps	2 Gbps	3 Gbps	4 Gbps
Stateful inspection throughput (multiprotocol <sup>3</sup> )	500 Mbps	600 Mbps	1 Gbps	1.5 Gbps	2 Gbps
ASA IPS throughput <sup>4</sup>	250 Mbps (extra hardware not required)	400 Mbps (extra hardware not required)	600 Mbps	900 Mbps (extra hardware not required)	1.3 Gbps (extra hardware not required)

<sup>2</sup> Maximum throughput measured with UDP traffic under ideal conditions.

<sup>3</sup> Multiprotocol = Traffic profile consisting primarily of TCP-based protocols/applications like HTTP, SMTP, FTP, IMAPv4, BitTorrent, and DNS.

<sup>4</sup> Firewall traffic that does not go through the IPS service can have higher throughput.

Feature	Cisco ASA 5512-X, Security Plus	Cisco ASA 5515-X	Cisco ASA 5525-X	Cisco ASA 5545-X	Cisco ASA 5555-X
Next-generation firewall throughput <sup>5</sup> (multiprotocol)	200 Mbps	350 Mbps	650 Mbps	1 Gbps	1.4 Gbps
Triple Data Encryption Standard/Advanced Encryption Standard (3DES/AES) VPN throughput <sup>6</sup>	200 Mbps	250 Mbps	300 Mbps	400 Mbps	700 Mbps
Users/nodes	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
IPsec VPN peers	250	250	750	2500	5000
Cisco Cloud Web Security users	100	250	500	1500	3000
Cisco AnyConnect Premium VPN peers (included; maximum)	2; 250	2; 250	2;750	2; 2500	2; 5000
Concurrent connections	100,000	250,000	500,000	750,000	1,000,000
New connections per second	10,000	15,000	20,000	30,000	50,000
Virtual interfaces (VLANs)	50; 100	100	200	300	500
Security contexts <sup>7</sup> (included; maximum)	0,0;2,5	2,5	2; 20	2; 50	2; 100
High availability	Not supported; Active/Active and Active/Standby	Active/Active and Active/Standby	Active/Active and Active/Standby	Active/Active and Active/Standby	Active/Active and Active/Standby
Expansion slot	1 interface card	1 interface card	1 interface card	1 interface card	1 interface card
User-accessible Flash slot	No	No	0	-	0
USB 2.0 ports	2	2	2	2	2
Integrated I/O	6 Gigabit Ethernet (GE) copper	6 GE copper	8 GE copper	8 GE copper	8 GE copper
Expansion I/O	6 GE copper or 6 GE Small Form-Factor Pluggable (SFP)	6 GE copper or 6 GE SFP	6 GE copper or 6 GE SFP	6 GE copper or 6 GE SFP	6 GE copper or 6 GE SFP
Dedicated management port	Yes (1 GE)	Yes (1 GE)	Yes (1 GE)	Yes (1 GE)	Yes (1 GE)
Serial ports	1 RJ-45 console	1 RJ-45 console	1 RJ-45 console	1 RJ-45 console	1 RJ-45 console
Solid-state drive	1 slot, 120 GB multiline configurator self-encrypting drive (MLC SED)	1 slot, 120 GB MLC SED	1 slot, 120 GB MLC SED	2 slots, RAID 1 120 GB MLC SED	2 slots, RAID 1 120 GB MLC SED
Memory	4 GB	8 GB	8 GB	12 GB	16 GB
Minimum system flash	4 GB	8 GB	8 GB	8 GB	8 GB
System bus	Multibus architecture	Multibus architecture	Multibus architecture	Multibus architecture	Multibus architecture
<b>Operating</b>					
Temperature	23 to 104°F (-5 to 40°C)	23 to 104°F (-5 to 40°C)	23 to 104°F (-5 to 40°C)	23 to 104°F (-5 to 40°C)	23 to 104°F (-5 to 40°C)

<sup>5</sup> Throughput was measured using ASA CX Software Release 9.1.1 with multiprotocol traffic profile with both AVC and WSE. Traffic logging was enabled as well.

<sup>6</sup> PN throughput and sessions count depend on the ASA device configuration and VPN traffic patterns. These elements should be taken into consideration as part of your capacity planning.

<sup>7</sup> Separately licensed feature; includes two SSL licenses with base system.

Feature	Cisco ASA 5512-X, Security Plus	Cisco ASA 5515-X	Cisco ASA 5525-X	Cisco ASA 5545-X	Cisco ASA 5555-X
<b>Relative humidity</b>	10 to 90 percent noncondensing	10 to 90 percent noncondensing	90 percent	90 percent	90 percent
<b>Altitude</b>	Designed and tested for 0 to 15,000 ft (4572 m)	Designed and tested for 0 to 15,000 ft (4572 m)	Designed and tested for 0 to 10,000 ft (3050 m)	Designed and tested for 0 to 10,000 ft (3050 m)	Designed and tested for 0 to 10,000 ft (3050 m)
<b>Shock</b>	70 G, 4.22 m/sec	70 G, 4.22 m/sec	50 G, 2 m/sec	50 G, 2 m/sec	50 G, 2 m/sec
<b>Vibration</b>	0.41 Grms2 (3 to 500 Hz) random input	0.41 Grms2 (3 to 500 Hz) random input	0.41 Grms2 (3 to 500 Hz) random input	0.41 Grms2 (3 to 500 Hz) random input	0.41 Grms2 (3 to 500 Hz) random input
<b>Acoustic noise</b>	64.2 A-weighted decibels (dBA) max	64.2 dBA max	64.2 dBA max	67.9 dBA max	67.9 dBA max
<b>Nonoperating</b>					
<b>Temperature</b>	-13 to 158°F (-25 to 70°C)	-13 to 158°F (-25 to 70°C)	-13 to 158°F (-25 to 70°C)	-13 to 158°F (-25 to 70°C)	-13 to 158°F (-25 to 70°C)
<b>Relative humidity</b>	10 to 90 percent noncondensing	10 to 90 percent noncondensing	10 to 90 percent	10 to 90 percent	10 to 90 percent
<b>Altitude</b>	Designed and tested for 0 to 15,000 ft (4570 m)	Designed and tested for 0 to 15,000 ft (4570 m)	Designed and tested for 0 to 15,000 ft (4572 m)	Designed and tested for 0 to 15,000 ft (4572 m)	Designed and tested for 0 to 15,000 ft (4572 m)
<b>Shock</b>	70G, 4.22 m/sec	70G, 4.22 m/sec	70G, 4.22 m/sec	70G, 4.22 m/sec	70G, 4.22 m/sec
<b>Vibration</b>	1.12 Grms2 (3 to 500 Hz) random input	1.12 Grms2 (3 to 500 Hz) random input	1.12 Grms2 (3 to 500 Hz) random input	1.12 Grms2 (3 to 500 Hz) random input	1.12 Grms2 (3 to 500 Hz) random input
<b>Power</b>					
<b>Input (per power supply)</b>					
<b>AC range line voltage</b>	100 to 240 volts alternating current (VAC)	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC
<b>AC normal line voltage</b>	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC
<b>AC current</b>	4.85A	4.85A	4.85A	5A, 100 to 120V 2.5A, 200 to 240V	5A, 100 to 120V 2.5A, 200 to 240V
<b>AC frequency</b>	50/60 Hz	50/60 Hz	50/60 Hz	50/60 Hz	50/60 Hz
<b>Dual-power supplies</b>	None	None	None	Yes	Yes
<b>DC domestic line voltage</b>	-40.5 to 56 volts direct current (VDC) (-48 VDC nominal)	-40.5 to 56 VDC (-48 VDC nominal)	-40.5 to 56 VDC (-48 VDC nominal)	-40.5 to 56 VDC (-48 VDC nominal)	-40.5 to 56 VDC (-48 VDC nominal)
<b>DC international line voltage</b>	-55 to -72 VDC (-60 VDC nominal)	-55 to -72 VDC (-60 VDC nominal)	-55 to -72 VDC (-60 VDC nominal)	-55 to -72 VDC (-60 VDC nominal)	-55 to -72 VDC (-60 VDC nominal)
<b>DC current</b>	15A (maximum input)	15A (maximum input)	15A (maximum input)	15A (maximum input)	15A (maximum input)
<b>Output</b>					
<b>Steady state</b>	51W	65W	75W	86W	90W
<b>Maximum peak</b>	56W	70W	108W	125W	134W
<b>Maximum heat dissipation</b>	192 British thermal units (Btu)/hr	239 Btu/hr	369 Btu/hr	427 Btu/hr	458 Btu/hr
<b>Form factor</b>	1 rack unit (RU), 19-in. rack-mountable	1RU, 19-in. rack-mountable	1RU, 19-in. rack-mountable	1RU, 19-in. rack-mountable	1RU, 19-in. rack-mountable
<b>Dimensions (H x W x D)</b>	1.67 x 16.7 x 15.6 in (4.24 x 42.9 x 39.5 cm)	1.67 x 16.7 x 15.6 in (4.24 x 42.9 x 39.5 cm)	1.75 x 17.5 x 14.25 in. (4.45 x 20.04 x 36.20 cm)	1.67 x 16.7 x 19.1 in. (4.24 x 42.9 x 48.4 cm)	1.67 x 16.7 x 19.1 in. (4.24 x 42.9 x 48.4 cm)

Feature	Cisco ASA 5512-X, Security Plus	Cisco ASA 5515-X	Cisco ASA 5525-X	Cisco ASA 5545-X	Cisco ASA 5555-X
<b>Weight (with AC power supply)</b>	13.39 lb (6.07 kg)	13.39 lb (6.07 kg)	22.0 lb (10 kg)	16.82 lb (7.63 kg) with single power supply 18.86 lb (8.61 kg) with dual power supply	16.82 lb (7.63 kg) with single power supply 18.86 lb (8.61 kg) with dual power supply
<b>Safety</b>	IEC 60950-1: 2005, 2 <sup>nd</sup> Edition; EN 60950-1:2006+A11: 2009; UL 60950-1:2007, 2 <sup>nd</sup> Edition; CSA C22.2 No. 60950-1-07, 2 <sup>nd</sup> Edition	IEC 60950-1: 2005, 2 <sup>nd</sup> Edition EN 60950-1:2006+A11: 2009 UL 60950-1:2007, 2 <sup>nd</sup> Edition; CSA C22.2 No. 60950-1-07, 2 <sup>nd</sup> Edition	IEC 60950-1: 2005, 2 <sup>nd</sup> Edition EN 60950-1:2006+A11: 2009 UL 60950-1:2007, 2 <sup>nd</sup> Edition; CSA C22.2 No. 60950-1-07, 2 <sup>nd</sup> Edition	IEC 60950-1: 2005, 2 <sup>nd</sup> Edition EN 60950-1:2006+A11: 2009 UL 60950-1:2007, 2 <sup>nd</sup> Edition; CSA C22.2 No. 60950-1-07, 2 <sup>nd</sup> Edition	IEC 60950-1: 2005, 2 <sup>nd</sup> Edition EN 60950-1:2006+A11: 2009 UL 60950-1:2007, 2 <sup>nd</sup> Edition; CSA C22.2 No. 60950-1-07, 2 <sup>nd</sup> Edition
<b>Electromagnetic compatibility (EMC)</b>	CE: EN55022 2006+A1: 2007 Class A; EN55024 1998+A1:2001+A2:2003; EN61000-3-2 2009; EN61000-3-3 2008; FCC: CFR 47, Part 15 Subpart B Class A 2010, ANSI C63.4 2009; ICES-003 issue 4 February 2004; VCCI: V-3/2011.04; C-TICK: AS/NZS CISPR 22,2009 KC: KN22 & KN24	CE: EN55022 2006+A1: 2007 Class A; EN55024 1998+A1:2001+A2:2003; EN61000-3-2 2009; EN61000-3-3 2008; FCC: CFR 47, Part 15 Subpart B Class A 2010, ANSI C63.4 2009; ICES-003 issue 4 February 2004; VCCI: V-3/2011.04; C-TICK: AS/NZS CISPR 22,2009 KC: KN22 & KN24	CE: EN55022 2006+A1: 2007 Class A; EN55024 1998+A1:2001+A2:2003; EN61000-3-2 2009; EN61000-3-3 2008; FCC:CFR 47, Part 15 Subpart B Class A 2010,ANSI C63.4 2009; ICES-003 issue 4 February 2004; VCCI:V-3/2011.04; C-TICK:AS/NZS CISPR 22,2009 KC:KN22 & KN24	CE: EN55022 2006+A1: 2007 Class A; EN55024 1998+A1:2001+A2:2003; EN61000-3-2 2009;EN61000-3-3 2008; FCC:CFR 47, Part 15 Subpart B Class A 2010,ANSI C63.4 2009; ICES-003 issue 4 February 2004; VCCI:V-3/2011.04; C-TICK:AS/NZS CISPR 22,2009 KC:KN22 & KN24	CE: EN55022 2006+A1: 2007 Class A; EN55024 1998+A1:2001+A2:2003; EN61000-3-2 2009;EN61000-3-3 2008; FCC:CFR 47, Part 15 Subpart B Class A 2010,ANSI C63.4 2009; ICES-003 issue 4 February 2004; VCCI:V-3/2011.04; C-TICK:AS/NZS CISPR 22,2009 KC:KN22 & KN24
<b>Industry certifications</b>	In process	In process	In process	In process	In process



## Cisco ASA 5500-X Series 6-Port GE Interface Cards

Cisco ASA 5500-X Series 6-port GE Interface Cards extend the I/O profile of the Cisco ASA 5512-X and Cisco ASA 5515-X by providing additional GE ports. The cards provide the following benefits:

- Better segmentation of network traffic (into separate security zones)
- Fiber-optic cable connectivity for long-distance communication
- Load sharing of traffic as well as protection against link failure through the use of EtherChannel
- Support for jumbo Ethernet frames of up to 9000 bytes
- Protection against cable failure for the most demanding Active/Active failover and full-mesh firewall deployments

Table 2 lists the characteristics of the Cisco ASA 5500-X Series 6-Port GE Interface Cards.

**Table 2.** Characteristics of Cisco ASA 5500-X Series 6-Port GE Interface Cards

Feature	Cisco ASA 5500-X Series 6-Port 10/100/1000	Cisco ASA 5500-X Series 6-Port GE SFP SX, LH, and LX
		
<b>Technical Specifications</b>		
<b>Integrated ports</b>	Six 10/100/1000BASE-T	Six GE Optical SFP 1000BASE-SX, 1000BASE-LX, or 1000BASE-LH transceiver supported

Feature	Cisco ASA 5500-X Series 6-Port 10/100/1000	Cisco ASA 5500-X Series 6-Port GE SFP SX, LH, and LX
<b>Environmental Operating Ranges</b>		
<b>Operating</b>		
Temperature	32 to 113°F (0 to 45°C)	32 to 113°F (0 to 45°C)
Relative humidity	5 to 95 percent noncondensing	5 to 95 percent noncondensing
<b>Nonoperating</b>		
Temperature	-40 to 149°F (-40 to 65°C)	-40 to 149°F (-40 to 65°C)
Power consumption	25W maximum	25W maximum
<b>Physical Specifications</b>		
Dimensions (H x W x D)	1.57 x 5.31 x 9.09 in. (3.99 x 13.49 x 23.09 cm)	1.57 x 5.31 x 9.09 in. (3.99 x 13.49 x 23.09 cm)
Weight	1.00 lb (0.45 kg)	1.00 lb (0.45 kg)
<b>Regulatory and Standards Compliance</b>		
Safety	UL 60950, CSA C22.2 No. 60950, EN 60950 IEC 60950, AS/NZS60950	UL 60950, CSA C22.2 No. 60950, EN 60950 IEC 60950, AS/NZS60950
Electromagnetic compatibility (EMC)	CE marking, FCC Part 15 Class A, AS/NZS CISPR22 Class A, VCCI Class A, EN55022 Class A, CISPR22 Class A, EN61000-3-2, EN61000-3-3	CE marking, FCC Part 15 Class A, AS/NZS CISPR22 Class A, VCCI Class A, EN55022 Class A, CISPR22 Class A, EN61000-3-2, EN61000-3-3

## Ordering Information

To place an order, visit the [Cisco ordering homepage](#). Table 3 provides ordering information for the Cisco ASA 5500 Series and ASA 5500-X Next-Generation Firewall Series.

**Table 3.** Ordering Information

Product Description	Part Number
<b>Cisco ASA Next-Generation Firewall Services</b>	
Cisco ASA 5512-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, DES encryption, and solid-state drive (SSD) 120 GB	ASA5512-SSD120-K8
Cisco ASA 5512-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, 3DES/AES encryption, SSD 120 GB	ASA5512-SSD120-K9
Cisco ASA 5515-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, DES encryption, SSD 120 GB	ASA5515-SSD120-K8
Cisco ASA 5515-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, 3DES/AES encryption, SSD 120 GB	ASA5515-SSD120-K9
Cisco ASA 5525-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, DES encryption, SSD 120 GB	ASA5525-SSD120-K8
Cisco ASA 5525-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, 3DES/AES encryption, SSD 120 GB	ASA5525-SSD120-K9
Cisco ASA 5545-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, DES encryption, 2 SSD 120 GB	ASA5545-2SSD120-K8
Cisco ASA 5545-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, 3DES/AES encryption, 2 SSD 120 GB	ASA5545-2SSD120-K9
Cisco ASA 5555-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, DES encryption, 2 SSD 120 GB	ASA5555-2SSD120-K8
Cisco ASA 5555-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, 3DES/AES encryption, 2 SSD 120 GB	ASA5555-2SSD120-K9
<b>Cisco ASA 5500-X Series Firewall Edition Bundles</b>	
Cisco ASA 5512-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, no payload encryption	ASA5512-K7
Cisco ASA 5512-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, DES encryption	ASA5512-K8



Product Description	Part Number
Cisco ASA 5512-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 DC power supply, DES license	ASA5512-DC-K8
Cisco ASA 5512-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, 3DES/AES encryption	ASA5512-K9
Cisco ASA 5515-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, no payload encryption	ASA5515-K7
Cisco ASA 5515-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, DES encryption	ASA5515-K8
Cisco ASA 5515-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 DC power supply, DES license	ASA5515-DC-K8
Cisco ASA 5515-X Firewall Edition; includes firewall services, 250 IPsec VPN peers, 2 SSL VPN peers, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, 3DES/AES encryption	ASA5515-K9
Cisco ASA 5525-X Firewall Edition; includes firewall services, 750 IPsec VPN peers, 2 SSL VPN peers, 8 copper GE data ports, 1 copper GE management port, 1 AC power supply, Active/Active high availability, 2 security contexts, no payload encryption	ASA5525-K7
Cisco ASA 5525-X Firewall Edition; includes firewall services, 750 IPsec VPN peers, 2 SSL VPN peers, 8 copper GE data ports, 1 copper GE management port, 1 AC power supply, Active/Active high availability, 2 security contexts, DES license	ASA5525-K8
Cisco ASA 5525-X Firewall Edition; includes firewall services, 750 IPsec VPN peers, 2 SSL VPN peers, 8 copper GE data ports, 1 copper GE management port, 1 DC power supply, Active/Active high availability, 2 security contexts, DES license	ASA5525-DC-K8
Cisco ASA 5525-X Firewall Edition; includes firewall services, 750 IPsec VPN peers, 2 SSL VPN peers, 8 copper GE data ports, 1 copper GE management port, 1 AC power supply, Active/Active high availability, 2 security contexts, 3DES/AES license	ASA5525-K9
Cisco ASA 5545-X Firewall Edition; includes firewall services, 2500 IPsec VPN peers, 2 SSL VPN peers, 8 copper GE data ports, 1 copper GE management port, 1 AC power supply, Active/Active high availability, 2 security contexts, no payload encryption	ASA5545-K7
Cisco ASA 5545-X Firewall Edition; includes firewall services, 2500 IPsec VPN peers, 2 SSL VPN peers, 8 copper GE data ports, 1 copper GE management port, 1 AC power supply, Active/Active high availability, 2 security contexts, DES license	ASA5545-K8
Cisco ASA 5545-X Firewall Edition; includes firewall services, 2500 IPsec VPN peers, 2 SSL VPN peers, 8 copper GE data ports, 1 copper GE management port, 1 DC power supply, Active/Active high availability, 2 security contexts, DES license	ASA5545-DC-K8
Cisco ASA 5545-X Firewall Edition; includes firewall services, 2500 IPsec VPN peers, 2 SSL VPN peers, 8 copper GE data ports, 1 copper GE management port, 1 AC power supply, Active/Active high availability, 2 security contexts, 3DES/AES license	ASA5545-K9
Cisco ASA 5545-X Firewall Edition; includes firewall services, 2500 IPsec VPN peers, 2 SSL VPN peers, 14 copper GE data ports, 1 copper GE management port, 1+1 AC power supply, Active/Active high availability, 2 security contexts, 3DES/AES license	ASA5545-CU-2AC-K9
Cisco ASA 5555-X Firewall Edition; includes firewall services, 5000 IPsec VPN peers, 2 SSL VPN peers, 8 copper GE data ports, 1 copper GE management port, 1 AC power supply, Active/Active high availability, 2 security contexts, no payload encryption	ASA5545-K7
Cisco ASA 5555-X Firewall Edition; includes firewall services, 5000 IPsec VPN peers, 2 SSL VPN peers, 8 copper GE data ports, 1 copper GE management port, 1 AC power supply, Active/Active high availability, 2 security contexts, DES license	ASA5545-K8
Cisco ASA 5555-X Firewall Edition; includes firewall services, 5000 IPsec VPN peers, 2 SSL VPN peers, 8 copper GE data ports, 1 copper GE management port, 1 DC power supply, Active/Active high availability, 2 security contexts, DES license	ASA5555-DC-K8
Cisco ASA 5555-X Firewall Edition; includes firewall services, 5000 IPsec VPN peers, 2 SSL VPN peers, 8 copper GE data ports, 1 copper GE management port, 1 AC power supply, Active/Active high availability, 2 security contexts, 3DES/AES license	ASA5545-K9
Cisco ASA 5555-X Firewall Edition; includes firewall services, 5000 IPsec VPN peers, 2 SSL VPN peers, 14 copper GE data ports, 1 copper GE management port, 1+1 AC power supply, Active/Active high availability, 2 security contexts, 3DES/AES license	ASA5555-CU-2AC-K9
<b>Cisco ASA 5500-X Series ASA IPS Edition Bundles</b>	
Cisco ASA 5512-X IPS Edition; includes IPS service, 250 IPsec VPN peers, 2 SSL VPN peers, firewall services, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, DES license	ASA5512-IPS-K8
Cisco ASA 5512-X IPS Edition; includes IPS service, 250 IPsec VPN peers, 2 SSL VPN peers, firewall services, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, DES license	ASA5512-IPS-K9

Product Description	Part Number
Cisco ASA 5515-X IPS Edition; includes IPS service, 250 IPsec VPN peers, 2 SSL VPN peers, firewall services, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, DES license	ASA5515-IPS-K8
Cisco ASA 5515-X IPS Edition; includes IPS service, 250 IPsec VPN Peers, 2 SSL VPN peers, firewall services, 6 copper GE data ports, 1 copper GE management port, 1 AC power supply, DES license	ASA5515-IPS-K9
Cisco ASA 5525-X IPS Edition; includes IPS service, 750 IPsec VPN peers, 2 SSL VPN peers, firewall services, 8 copper GE data ports, 1 copper GE Management, 1 AC power supply, Active/Active high availability, 2 security contexts, DES license	ASA5525-IPS-K8
Cisco ASA 5525-X IPS Edition; includes IPS service, 750 IPsec VPN peers, 2 SSL VPN peers, firewall services, 8 copper GE data ports, 1 copper GE management port, 1 AC power supply, Active/Active high availability, 2 security contexts, 3DES/AES license	ASA5525-IPS-K9
Cisco ASA 5545-X IPS Edition; includes IPS service, 2500 IPsec VPN peers, 2 SSL VPN peers, firewall services, 8 copper GE data ports, 1 copper GE management port, 1 AC power supply, Active/Active high availability, 2 security contexts, DES license	ASA5545-IPS-K8
Cisco ASA 5545-X IPS Edition; includes IPS service, 2500 IPsec VPN peers, 2 SSL VPN peers, firewall services, 8 copper GE data ports, 1 copper GE management port, 1 AC power supply, Active/Active high availability, 2 security contexts, 3DES/AES license	ASA5545-IPS-K9
Cisco ASA 5555-X IPS Edition; includes IPS service, 5000 IPsec VPN peers, 2 SSL VPN peers, firewall services, 8 copper GE data ports, 1 copper GE management port, 1 AC power supply, Active/Active high availability, 2 security contexts, DES license	ASA5555-IPS-K8
Cisco ASA 5555-X IPS Edition; includes IPS service, 5000 IPsec VPN peers, 2 SSL VPN peers, firewall services, 8 copper GE data ports, 1 copper GE management port, 1 AC power supply, Active/Active high availability, 2 security contexts, 3DES/AES license	ASA5555-IPS-K9
<b>Cisco Interface Cards</b>	
Cisco ASA Interface Card with 6 copper GE data ports for ASA 5512-X and ASA 5515-X	ASA-IC-6GE-CU-A
Cisco ASA Interface Card with 6 copper GE data ports for ASA 5525-X	ASA-IC-6GE-CU-B
Cisco ASA Interface Card with 6 copper GE data ports for ASA 5545-X and ASA 5555-X	ASA-IC-6GE-CU-C
Cisco ASA Interface Card with 6 SFP GE data ports (SX, LH, and LX) for ASA 5512-X and ASA 5515-X	ASA-IC-6GE-SFP-A
Cisco ASA Interface Card with 6 SFP GE data ports (SX, LH, and LX) for ASA 5525-X	ASA-IC-6GE-SFP-B
Cisco ASA Interface Card with 6 SFP GE data ports (SX, LH, and LX) for ASA 5545-X and ASA 5555-X	ASA-IC-6GE-SFP-C
Cisco ASA Interface Card with 6 copper GE data ports for ASA 5512-X and ASA 5515-X (spare)	ASA-IC-6GE-CU-A=
Cisco ASA Interface Card with 6 copper GE data ports for ASA 5525-X (spare)	ASA-IC-6GE-CU-B=
Cisco ASA Interface Card with 6 copper GE data ports for ASA 5545-X and ASA 5555-X (spare)	ASA-IC-6GE-CU-C=
Cisco ASA Interface Card with 6 SFP GE data ports (SX, LH, and LX) for ASA 5512-X and ASA 5515-X (spare)	ASA-IC-6GE-SFP-A=
<b>Cisco ASA 5500 Series Software</b>	
Cisco ASA Software one-time upgrade for nonsupport customers (spare)	ASA-SW-UPGRADE=
<b>ASA Next-Generation Firewall Services Software Subscriptions: 3-year term (1-year and 5-year service software bundle subscriptions can be purchased as well as individual Cisco AVC, WSE, and Next-Generation Firewall IPS service software subscriptions with 1-year, 3-year, and 5-year terms)</b>	
ASA 5512-X with Cisco AVC, WSE, and IPS, 3-year	ASA5512-AW13Y
ASA 5515-X AVC, WSE, and IPS, 3-year	ASA5515-AW13Y
ASA 5525-X AVC, WSE, and IPS, 3-year	ASA5525-AW13Y
ASA 5545-X AVC, WSE, and IPS, 3-year	ASA5545-AW13Y
ASA 5555-X AVC, WSE, and IPS, 3-year	ASA5555-AW13Y
ASA 5512-X AVC and WSE, 3-year	ASA5512-AW3Y
ASA 5515-X AVC and WSE, 3-year	ASA5515-AW3Y
ASA 5525-X AVC and WSE, 3-year	ASA5525-AW3Y
ASA 5545-X AVC and WSE, 3-year	ASA5545-AW3Y
ASA 5555-X AVC and WSE, 3-year	ASA5555-AW3Y
ASA 5515-X AVC and NGFW IPS, 3-year	ASA5515-AI3Y
ASA 5525-X AVC and NGFW IPS, 3-year	ASA5525-AI3Y

Product Description	Part Number
ASA 5545-X AVC and NGFW IPS, 3-year	ASA5545-AI3Y
ASA 5555-X AVC and NGFW IPS, 3-year	ASA5555-AI3Y
<b>Intrusion Prevention (I) Software Subscriptions</b>	
Cisco ASA 5512-X IPS; 1-year	ASA5512-NI1Y
Cisco ASA 5512-X IPS; 3-year	ASA5512-NI3Y
Cisco ASA 5512-XIPS; 5-year	ASA5512-NI5Y
Cisco ASA 5515-X IPS; 1-year	ASA5515-NI1Y
Cisco ASA 5515-X IPS; 3-year	ASA5515-NI3Y
Cisco ASA 5515-X IPS; 5-year	ASA5515-NI5Y
Cisco ASA 5525-X IPS; 1-year	ASA5525-NI1Y
Cisco ASA 5525-X IPS; 3-year	ASA5525-NI3Y
Cisco ASA 5525-X IPS; 5-year	ASA5525-NI5Y
Cisco ASA 5545-X IPS; 1-year	ASA5545-NI1Y
Cisco ASA 5545-X IPS; 3-year	ASA5545-NI3Y
Cisco ASA 5545-X IPS; 5-year	ASA5545-NI5Y
Cisco ASA 5555-X IPS; 1-year	ASA5555-NI1Y
Cisco ASA 5555-X IPS; 3-year	ASA5555-NI3Y
Cisco ASA 5555-X IPS; 5-year	ASA5555-NI5Y
<b>Cisco ASA 5500 Series Accessories</b>	
Cisco ASA 5500 Series compact flash, 256 MB (spare)	ASA5500-CF-256MB=
Cisco ASA 5512-X through 5555-X 120 GB MLC SED SSD(spare)	ASA5500X-SSD120=
Cisco ASA 5500 Series compact flash, 512 MB (spare)	ASA5500-CF-512MB=
Cisco ASA 180W AC power supply (spare)	ASA-180W-PWR-AC=
Cisco GE optical SFP connector, 1000BASE-SX short-wavelength transceiver (spare)	GLC-SX-MM=
Cisco GE optical SFP connector, 1000BASE-LX/LH long-wavelength/long-haul transceiver (spare)	GLC-LH-SM=
Cisco GE optical SFP connector, 1000BASE-SX short-wavelength transceiver, digital optical monitoring (DOM) (spare)	GLC-SX-MMD=
Cisco GE optical SFP connector, 1000BASE-LX/LH long-wavelength/long-haul transceiver, DOM (spare)	GLC-LH-SMD=
Cisco ASA 5580 AC power supply (spare)	ASA5580-PWR-AC=
Cisco ASA 5580 rail kit (spare)	ASA5580-RAILS=
Cisco ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X rail kit (spare)	ASA-RAILS=
Cisco ASA 5512-X, 5515-X, 5525-X brackets for rack mounting (spare)	ASA-BRACKETS=
Cisco ASA 5545-X/5555-X AC power supply (spare)	ASA-PWR-AC=
Cisco ASA 5545-X/5555-X DC power supply	ASA-PWR-DC
Cisco ASA 5512-X and 5515-X interface card (blank) (spare)	ASA-IC-A-BLANK=
Cisco ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X spare hard drive slot cover (spare)	ASA-HD-BLANK=
Cisco ASA 5525-X, 5545-X, and 5555-X hard drive slot (blank) (spare)	ASA-HD-BLANK=
Cisco ASA 5525-X interface card slot (blank) (spare)	ASA-IC-B-BLANK=
Cisco ASA 5545-X and 5555-X interface card slot (blank) (spare)	ASA-IC-C-BLANK=

## To Download the Software

Visit the [Cisco Software Center](#) to download Cisco ASA Software.

---

## Service and Support

Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business.

Included in the “Operate” phase of the service lifecycle are the Cisco Security IntelliShield Alert Manager Service, Cisco SMARTnet<sup>®</sup> Service, Cisco Service Provider Base, and Cisco Services for IPS. These services are suitable for enterprise, commercial, and service provider customers.

The Cisco Security IntelliShield Alert Manager Service provides a customizable, web-based threat and vulnerability alert service that enables organizations to easily access timely, accurate, and credible information about potential vulnerabilities in their environment.

Cisco Services for ASA IPS support modules, platforms, and bundles of platforms and modules that feature IPS capabilities. Cisco SMARTnet and Service Provider Base support other products in this family.

## For More Information

For more information, please visit the following links:

- Cisco ASA 5500-X Series Next-Generation Firewalls: <http://www.cisco.com/go/asa>
- Cisco Adaptive Security Device Manager: <http://www.cisco.com/go/asdm>
- Cisco Prime Security Manager: <http://www.cisco.com/go/prsm>
- Cisco Security Services:  
[http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv\\_group\\_home.html](http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html)
- Cisco ASA 5500-X Series Licensing Information:  
[http://www.cisco.com/en/US/products/ps6120/products\\_licensing\\_information\\_listing.html](http://www.cisco.com/en/US/products/ps6120/products_licensing_information_listing.html)



---

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](http://www.cisco.com/go/offices).

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

# Cisco UCS C240 M3 Rack Server

## Product Overview

The form-factor-agnostic Cisco® Unified Computing System™ (Cisco UCS™) combines Cisco UCS C-Series Rack Servers and B-Series Blade Servers with networking and storage access in a single converged system that simplifies management and delivers greater cost efficiency and agility with increased visibility and control. The latest expansion of the Cisco UCS portfolio includes the new Cisco UCS C240 M3 Rack Server (two rack units [2RU]) and Cisco UCS C220 M3 Rack Server (1RU) and the Cisco UCS B200 M3 Blade Server. These three new servers increase compute density through more cores and cache balanced with more memory capacity and disk drives and faster I/O. Together these server improvements and complementary Cisco UCS advancements deliver the combination of features and cost efficiency required to support IT's diverse server needs.

The Cisco UCS C240 M3 Rack Server (Figure 1) is designed for both performance and expandability over a wide range of storage-intensive infrastructure workloads, from big data to collaboration. Building on the success of the Cisco UCS C210 M2 Rack Server, the enterprise-class Cisco UCS C240 M3 server further extends the capabilities of the Cisco UCS portfolio in a 2RU form factor with the addition of the Intel® Xeon® processor E5-2600 and E5-2600 v2 product families, which deliver an outstanding combination of performance, flexibility, and efficiency gains. The Cisco UCS C240 M3 offers up to two Intel® Xeon® processor E5-2600 or E5-2600 v2 processors, 24 DIMM slots, 24 disk drives, and four 1 Gigabit Ethernet LAN-on-motherboard (LOM) ports to provide exceptional levels of internal memory and storage expandability and exceptional performance.

The Cisco UCS C240 M3 interfaces with Cisco UCS using another Cisco innovation, the Cisco UCS Virtual Interface Card. The Cisco UCS Virtual Interface Card is a virtualization-optimized Fibre Channel over Ethernet (FCoE) PCI Express (PCIe) 2.0 x8 10-Gbps adapter designed for use with Cisco UCS C-Series Rack Servers. The VIC is a dual-port 10 Gigabit Ethernet PCIe adapter that can support up to 256 PCIe standards-compliant virtual interfaces, which can be dynamically configured so that both their interface type (network interface card [NIC] or host bus adapter [HBA]) and identity (MAC address and worldwide name [WWN]) are established using just-in-time provisioning. In addition, the Cisco UCS VIC 1225 can support network interface virtualization and Cisco® Data Center Virtual Machine Fabric Extender (VM-FEX) technology.

**Figure 1.** Cisco UCS C240 M3 Server



## Applications

Not all storage-intensive workloads are alike, and the Cisco UCS C240 M3 server's disk configuration delivers balanced performance and expandability to best meet individual workload requirements. With up to 12 LFF (Large Form Factor) or 24 SFF (Small Form Factor) internal drives, the Cisco UCS C240 M3 optionally offers 10,000-RPM and 15,000-RPM SAS drives to deliver a high number of I/O operations per second for transactional

---

workloads such as database management systems. In addition, high-capacity SATA drives provide an economical, large-capacity solution. Superfast SSDs are a third option for workloads that demand extremely fast access to smaller amounts of data. A choice of RAID controller options also helps increase disk performance and reliability.

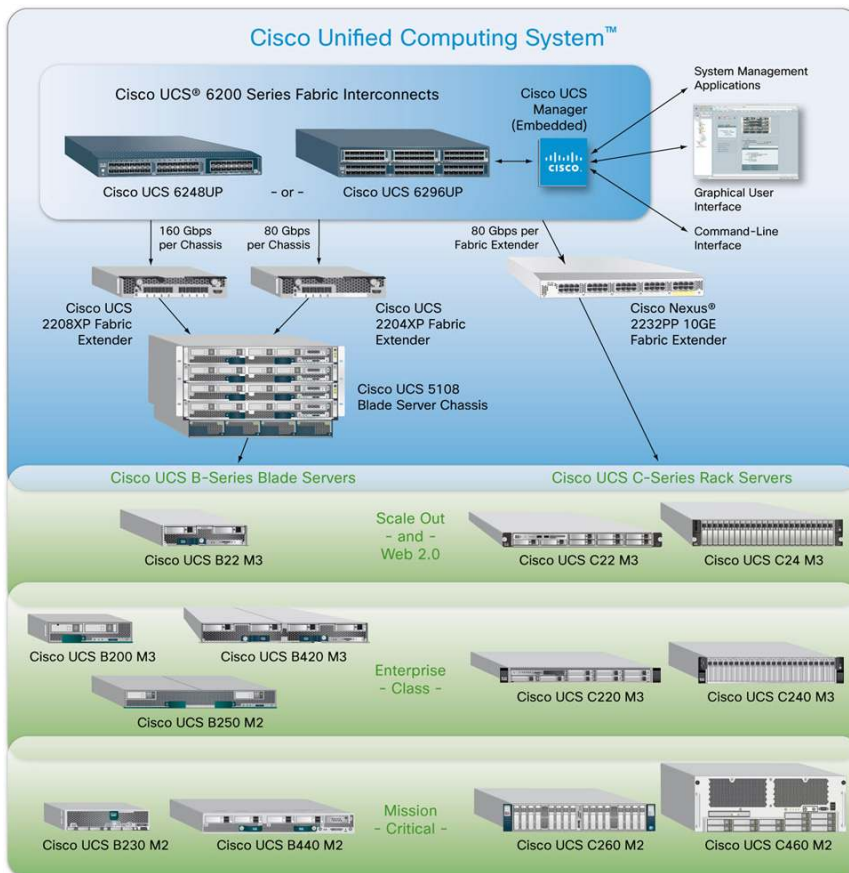
The Cisco UCS C240 M3 further increases performance and customer choice over many types of storage-intensive applications such as:

- Collaboration
- Small and medium-sized business (SMB) databases
- Big data infrastructure
- Virtualization and consolidation
- Storage servers
- High-performance appliances

### Cisco UCS Servers Change the Economics of the Data Center

IT infrastructure matters now more than ever, as organizations seek to achieve the full potential of infrastructure as a service (IaaS), bare metal, virtualized servers, and cloud computing. Cisco continues to lead in data center innovation with the introduction of new building blocks for Cisco Unified Computing System that extend its exceptional simplicity, agility, and efficiency (Figure 2) - Innovations such as the Cisco UCS C240 M3 rack server.

**Figure 2.** Cisco UCS Components



Cisco innovations, such as Cisco UCS Manager, allows administrators to create a software definition for a desired server (using Cisco service profiles and templates) and then instantiate that server and its I/O connectivity by associating a service profile with physical resources. This approach contrasts with the traditional method of configuring each system resource manually, one at a time, through individual element managers. Unlike with the products of other vendors, Cisco service profiles can be moved from rack server to rack or blade server, or between blade or rack servers in different chassis. In other words, Cisco UCS Manager and service profiles are form-factor agnostic.

Other Cisco UCS building blocks include enhanced server I/O options and expanded Cisco UCS fabric interconnects that extend scalability and management simplicity for both blade and rack systems across bare-metal, virtualized, and cloud-computing environments. Cisco helps ensure that nearly all parts of Cisco UCS offer investment protection and are backward compatible. For example, fabric extenders can be upgraded using the same fabric interconnects and same Cisco UCS VIC 1225. Fabric interconnect hardware can be upgraded independently of fabric extenders and blade chassis. Cisco continues to innovate in all these areas, helping ensure that both now and in the future, more powerful, rack servers with larger, faster memory have adequate I/O bandwidth and computing power. Cisco completes this vision through continuous innovation in VIC, ASIC, fabric extender, fabric interconnect, blade server, blade chassis, rack server technologies and form-factor-agnostic Cisco UCS Manager software that ties all these ever-advancing hardware pieces together.

The Cisco UCS C240 M3 is also part of a large family of rack servers: the Cisco C-Series Rack Servers. Designed to operate both in standalone environments and as part of Cisco UCS, the Cisco UCS C-Series servers employ Cisco technology to help customers handle the most challenging workloads. The Cisco UCS C-Series complements a standards-based unified network fabric, Cisco Data Center VM-FEX virtualization support, Cisco UCS Manager Software, Cisco fabric extender and fabric interconnect architectures, and Cisco Extended Memory Technology. Again, Cisco is innovating across all these technologies. With Cisco UCS architectural advantages, software advances, continuous innovation, and unique blade server and chassis designs, Cisco UCS is the first truly unified data center platform. In addition, Cisco UCS can transform IT departments through policy-based automation and deep integration with familiar systems management and orchestration tools.

## Features and Benefits

The Cisco UCS C240 M3 is one of the first rack servers available anywhere with a built-in entry point to unified computing. Table 1 summarizes the features and benefits of the Cisco UCS C240 M3 Rack Server.

**Table 1.** Features and Benefits

Feature	Benefit
<b>10-Gbps unified network fabric</b>	<ul style="list-style-type: none"> <li>• Low-latency, lossless, 10-Gbps Ethernet and industry-standard FCoE and native Fibre Channel fabric</li> <li>• Wire-once deployment model in which changing I/O configurations no longer means installing adapters and recabling racks and switches</li> <li>• Fewer interface cards, cables, and upstream network ports to purchase, power, configure, and maintain</li> </ul>
<b>Virtualization optimization</b>	<ul style="list-style-type: none"> <li>• Cisco Data Center VM-FEX and Adapter-FEX technologies, I/O virtualization, and Intel Xeon processor E5-2600 and E5-2600 v2 product family features, extending the network directly to virtual machines</li> <li>• Consistent and scalable operational model</li> <li>• Increased security and efficiency with reduced complexity</li> </ul>
<b>Unified management (when integrated into Cisco Unified Computing System)</b>	<ul style="list-style-type: none"> <li>• Entire solution managed as a single entity with Cisco UCS Manager, improving operation efficiency and flexibility</li> <li>• Service profiles and templates that implement role- and policy-based management, enabling more effective use of skilled server, network, and storage administrators</li> <li>• Automated provisioning and increased business agility, allowing data center managers to provision applications in minutes rather than days</li> <li>• Capability to move virtual machines and their security features and policies from rack to rack or rack to blade or blade to blade</li> </ul>
<b>Intel Xeon processor E5-2600 and E5-2600 v2 product families</b>	<ul style="list-style-type: none"> <li>• Automated energy efficiency reduces energy costs by automatically putting the processor and memory in the lowest available power state while still delivering the performance required and flexible virtualization technology that optimizes performance for virtualized environments, including processor support for migration and direct I/O</li> <li>• Up to twice the performance for floating-point operations. Intel Advanced Vector Extensions (AVX) provides new instructions that can significantly improve performance for applications that rely on floating-point or vector computations</li> <li>• Cisco C-Series servers keep pace with Intel Xeon processor innovation by offering the latest processors with an increase in processor frequency and improved security and availability features. With the increased performance provided by the Intel Xeon processor E5-2600 and E5-2600 v2 product families, Cisco UCS C-Series servers offer an improved price-to-performance ratio, making Cisco UCS servers among the best values in the industry</li> <li>• Advanced reliability features, including Machine Check Architecture Recovery, automatically monitor, report, and recover from hardware errors to maintain data integrity and keep mission-critical services online</li> <li>• Hardened protection for virtual and cloud Environments: Establish trusted pools of virtual resources with Intel® Trusted Execution Technology (Intel® TXT). Intel TXT ensures that physical servers and hypervisors boot only into cryptographically verified "known good states." It safeguards your business more effectively by protecting your platform from the insertion of malware during or prior to launch</li> </ul>
<b>High-capacity, flexible internal storage</b>	<ul style="list-style-type: none"> <li>• Up to 12 LFF or 16/24 SFF front-accessible, hot-swappable, SAS, SATA, or SSD drives for local storage, providing redundancy options and ease of serviceability</li> <li>• Balanced performance and capacity to meet application needs: <ul style="list-style-type: none"> <li>◦ SATA SSDs</li> <li>◦ 15,000 RPM SAS drives for highest performance</li> <li>◦ 10,000 RPM SAS drives for high performance and value</li> <li>◦ 7200-RPM SATA drives for high capacity and value</li> </ul> </li> </ul>
<b>RAID 0, 1, 5, 6, 10, 50, and 60 support</b>	A choice of RAID controllers to provide data protection for up to 12 or 24 SAS, SATA, or SSD drives in PCIe and mezzanine card form factors



Feature	Benefit
<b>Cisco UCS C-Series Integrated Management Controller (CIMC)</b>	<ul style="list-style-type: none"> <li>• Web user interface for server management; remote keyboard, video, and mouse (KVM); virtual media; and administration</li> <li>• Virtual media support for remote CD and DVD drives as if local</li> <li>• Intelligent Platform Management Interface (IPMI) 2.0 support for out-of-band management through third-party enterprise management systems</li> <li>• Command-line interface (CLI) for server management</li> </ul>
<b>Fast-memory support</b>	24 DIMM slots supporting up to 1866 MHz of memory for optimal performance
<b>Redundant fans and power supplies</b>	<ul style="list-style-type: none"> <li>• Dual-redundant fans and power supplies for enterprise-class reliability and uptime</li> <li>• Power efficiency through Cisco Common Form-Factor Platinum Power Supplies (650W or 1200W or 930W DC)</li> </ul>
<b>5 PCIe 3.0 slots</b>	<ul style="list-style-type: none"> <li>• Flexibility, increased performance, and compatibility with industry standards</li> <li>• PCIe 3.0 slots, which are estimated to substantially increase the bandwidth over the previous generation and offer more flexibility while maintaining compatibility with PCIe 2.0</li> <li>• 2 PCIe generation 3 x16 slots: both full height, and three-quarters length (10.5-in)</li> <li>• 3 PCIe generation 3 x8 slots: 1 full height and three-quarters length, 1 full height and half length, and 1 half height and half length</li> </ul>
<b>Integrated quad-port Gigabit Ethernet</b>	<ul style="list-style-type: none"> <li>• Outstanding network I/O performance and increased network efficiency and flexibility</li> <li>• Increased network availability when configured in failover configurations</li> </ul>
<b>Trusted Platform Module (TPM)</b>	<ul style="list-style-type: none"> <li>• TPM is a chip (microcontroller) that can securely store artifacts used to authenticate the platform (server). These artifacts can include passwords, certificates, or encryption keys</li> <li>• TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy, helping ensure authentication and authorization</li> </ul>
<b>Tool-free access</b>	<ul style="list-style-type: none"> <li>• Enhanced serviceability through tool-free access to all serviceable items and color coded indicators to guide users to hot-pluggable and serviceable items</li> </ul>
<b>Cisco Flexible Flash (FlexFlash)</b>	<ul style="list-style-type: none"> <li>• The server supports up to two internal Cisco FlexFlash drives (secure digital [SD] cards)</li> <li>• The first SD card is preloaded with 4 virtual drives, which contain the Cisco Server Configuration Utility, the Cisco Host Upgrade Utility, the Cisco C-Series server drivers set, and a blank virtual drive on which you can install an OS or a hypervisor. The second SD card is blank and can be used to mirror the first SD card</li> </ul>
<b>GPU Virtualization Support</b>	Offload graphics and compute processing from the C240 M3 server CPU to the NVIDIA Kepler™ enabled GPU and accelerate applications in physical and virtualized environments. For details, refer to <a href="#">NVIDIA Grid K1 and K2 datasheet</a>

## Product Specifications

Table 2 lists the specifications for the Cisco UCS C240 M3 server.

**Table 2.** Product Specifications

Item	Specification
<b>Processors</b>	<ul style="list-style-type: none"> <li>• 1 or 2 Intel Xeon processor E5-2600 or E5-2600 v2 product families</li> <li>• For a complete list of processor options, please refer to the corresponding SFF <a href="#">SpecSheet</a> or LFF <a href="#">SpecSheet</a></li> </ul>
<b>Memory</b>	<ul style="list-style-type: none"> <li>• 24 DIMM slots</li> <li>• Support for DDR3 registered DIMMs</li> <li>• Support for DDR3 low-voltage DIMMs</li> <li>• Advanced error-correcting code (ECC)</li> <li>• Mirroring option</li> </ul>
<b>PCIe slots</b>	<ul style="list-style-type: none"> <li>• 5 PCIe generation-3 slots: <ul style="list-style-type: none"> <li>◦ 2 PCIe Generation 3, x16 slots: both full height, 3/4 length (10.5-in);</li> <li>◦ 2 PCIe Generation 3, x8 slots: one full height, 1/2 length and one full height 3/4 length;</li> <li>◦ 1 PCIe Generation 3, x8 slots: 1/2 height and 1/2 length</li> </ul> </li> </ul>
<b>RAID card</b>	<ul style="list-style-type: none"> <li>• For a complete list of RAID options, please refer to the corresponding SFF <a href="#">SpecSheet</a> or LFF <a href="#">SpecSheet</a></li> </ul>
<b>Hard drives</b>	Up to 24 front-accessible, hot-swappable, 2.5-inch SAS, SATA or SSD or up to 12 front-accessible, hot-swappable, 3.5-inch SAS, SATA drives
<b>Hard disk options</b>	<p><b>2.5-inch SFF drive options:</b></p> <ul style="list-style-type: none"> <li>• For a complete list of drive options, please refer to the corresponding SFF <a href="#">SpecSheet</a></li> </ul> <p><b>3.5-inch LFF drive options:</b></p>

Item	Specification
<b>Cisco Flexible Flash (FlexFlash) Internal USB</b>	<ul style="list-style-type: none"> <li>For a complete list of drive options, please refer to the corresponding LFF <a href="#">SpecSheet</a></li> </ul> <p>The server supports up to two internal 16GB Cisco FlexFlash drives (SD cards). One SD card is preloaded with four virtual drives. The four virtual drives contain, respectively, the Cisco Server Configuration Utility, the Cisco Host Upgrade Utility, the Cisco C-Series server drivers set, and a blank virtual drive on which you can install an OS or a hypervisor. The second SD card is blank and can be used to mirror the first SD card.</p>
<b>Internal USB</b>	The server supports one internal USB flash drive
<b>Cisco UCS Integrated Management Controller</b>	<ul style="list-style-type: none"> <li>Integrated Emulex Pilot-3 Baseboard Management Controller (BMC)</li> <li>IPMI 2.0 compliant for management and control</li> <li>One 10/100/1000 Ethernet out-of-band management interface</li> <li>CLI and WebGUI management tool for automated, lights-out management</li> <li>KVM</li> </ul>
<b>Front-panel connector</b>	One KVM console connector (supplies 2 USB, 1 VGA, and 1 serial connector)
<b>Front-panel locator LED</b>	Indicator to help direct administrators to specific servers in large data center environments
<b>Additional rear connectors</b>	Additional interfaces including a VGA video port, 2 USB 2.0 ports, 1 Gigabit Ethernet dedicated management port, quad 1 Gigabit Ethernet ports, and an RJ-45 serial port
<b>Physical dimensions (HxWxD)</b>	2RU: 3.4 x 17.5 x 28.0 in. (8.7 x 44.5 x 71.2 cm)
<b>Temperature: Operating</b>	41 to 104°F (5 to 40°C) derate the maximum temperature by 1°C per every 305 m of altitude above sea level
<b>Temperature: Nonoperating</b>	-40 to 158°F (-40 to 70°C)
<b>Humidity: Operating</b>	10 to 90% noncondensing
<b>Humidity Nonoperating</b>	5 to 93% noncondensing
<b>Altitude: Operating</b>	0 to 10,000 ft (0 to 3000m); maximum ambient temperature decreases by 1°C per 300m)
<b>Altitude: Nonoperating</b>	40,000 ft (12,000m)

## Regulatory Standards

Table 3 lists regulatory standards compliance information.

**Table 3.** Regulatory Standards Compliance: Safety and EMC

Specification	Description
<b>Safety</b>	<ul style="list-style-type: none"> <li>UL 60950-1 No. 21CFR1040 Second Edition</li> <li>CAN/CSA-C22.2 No. 60950-1 Second Edition</li> <li>IEC 60950-1 Second Edition</li> <li>EN 60950-1 Second Edition</li> <li>IEC 60950-1 Second Edition</li> <li>AS/NZS 60950-1</li> <li>GB4943 2001</li> </ul>
<b>EMC: Emissions</b>	<ul style="list-style-type: none"> <li>47CFR Part 15 (CFR 47) Class A</li> <li>AS/NZS CISPR22 Class A</li> <li>CISPR2 2 Class A</li> <li>EN55022 Class A</li> <li>ICES003 Class A</li> <li>VCCI Class A</li> <li>EN61000-3-2</li> <li>EN61000-3-3</li> <li>KN22 Class A</li> <li>CNS13438 Class A</li> </ul>
<b>EMC: Immunity</b>	<ul style="list-style-type: none"> <li>EN55024</li> <li>CISPR24</li> <li>EN300386</li> <li>KN24</li> </ul>

---

## Ordering Information

For a complete list of options, please refer to the corresponding SFF [SpecSheet](#) or LFF [SpecSheet](#).

## Cisco Unified Computing Services

Using a unified view of data center resources, Cisco and our industry-leading partners deliver services that accelerate your transition to a Cisco UCS C-Series Rack Server solution. Cisco Unified Computing Services helps you quickly deploy the servers, optimize ongoing operations to better meet your business needs, and migrate to Cisco's unified computing architecture. For more information, visit

<http://www.cisco.com/go/unifiedcomputingservices>.

## For More Information

Please visit <http://www.cisco.com/go/unifiedcomputing>.



---

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](http://www.cisco.com/go/offices).

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

# APC Smart-UPS RT 5000VA (SURTD5000XLI)

Smart-UPS RT 5000VA 230V



## Price details:

Price excl. VAT: 2,298.63 €

Eco fees: 0.08 €

VAT 21 %: 482.73 €

## Product details:

Product code: SURTD5000XLI

EAN: 0731304240266

Manufacturer: APC

PDF generated on: 18 March, 2014



# 2,781.44 €

\* VAT included

APC Smart-UPS RT, 3500 Watts / 5000 VA, Input 230V / Output 230V, Interface Port DB-9 RS-232, RJ-45 10/100 Base-T, Smart-Slot, Extended runtime model, Rack Height 3 U

Includes: CD with software, Smart UPS signalling RS-232 cable, User Manual, Web/SNMP Management Card

## Main specifications:

### Power

Output power capacity (VA):	5000 VA
Output power:	3500 W
Surge energy rating:	480 J
Emergency Power Off (EPO):	Y

### Ports & interfaces

Ethernet LAN (RJ-45) ports:	1
-----------------------------	---

### Battery

Battery technology:	Sealed Lead Acid (VRLA)
Battery recharge time:	2.5 h
Typical backup time at half load:	15.4 min
Typical backup time at full load:	5 min
Replacement battery cartridge:	RBC44

### Design

Colour of product:	Black
--------------------	-------

### Performance

Noise level:	55 dB
LED indicators:	Y
Audible alarms:	Y

### Operational conditions

Operating temperature (T-T):	0 - 40 °C
Storage temperature (T-T):	-15 - 45 °C
Operating relative humidity (H-H):	0 - 95 %
Storage relative humidity (H-H):	0 - 95 %
Operating altitude:	0 - 3000 m
Non-operating altitude:	0 - 15000 m

### Certificates

Certification:	C-tick, CE, EN 50091-1, EN 50091-2, EN 55022 Class A, EN 60950, EN 61000-3-2, GOST, VDE
----------------	---

### Weight & dimensions

Weight: 54550 g

#### Other features

Interface:	DB-9 RS-232,Smart-Slot
Output connections:	8 - IEC 320 C13 2 - IEC 320 C19 6 - IEC Jumpers
Dimensions (WxDxH):	130 x 660 x 432 mm
Nominal output voltage:	230 V
Output voltage note:	230-240 V
Nominal input voltage:	230 V