	<b>UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA</b>			
	Documento	Código	Fecha	Revisión
<b>FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO</b>	<b>F-AC-DBL-007</b>	<b>10-04-2012</b>	<b>A</b>	
Dependencia	Aprobado		Pág.	
<b>DIVISIÓN DE BIBLIOTECA</b>	<b>SUBDIRECTOR ACADEMICO</b>		<b>i(148)</b>	

## RESUMEN – TRABAJO DE GRADO

AUTORES	<b>OSCAR IGNACIO LOBO DÍAZ DARWIN ACOSTA MANZANO</b>
FACULTAD	<b>FACULTAD DE INGENIERIAS</b>
PLAN DE ESTUDIOS	<b>PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS</b>
DIRECTOR	<b>FABIÁN RANULFO CUESTA QUINTERO</b>
TÍTULO DE LA TESIS	<b>DISEÑO DE UNA ARQUITECTURA BASADA EN TECNOLOGÍA “SDN” (REDES DEFINIDAS POR SOFTWARE) PARA EL LABORATORIO DE REDES Y TELECOMUNICACIONES DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA</b>

### RESUMEN

(70 palabras aproximadamente)

EN EL PRESENTE PROYECTO SE BUSCA PROPONER UN DISEÑO DE UNA ARQUITECTURA BASADA EN REDES DEFINIDAS POR SOFTWARE (SDN) QUE PUEDE APORTAR UNA MEJORA PARA LA OPTIMIZACIÓN PARA EL CONTROL DEL FLUJO DE DATOS, EN UN SISTEMA DE REDES DE COMUNICACIÓN PARA EL LABORATORIO DE REDES Y TELECOMUNICACIONES DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA.

### CARACTERÍSTICAS

PÁGINAS:	PLANOS:	ILUSTRACIONES:	CD-ROM:
----------	---------	----------------	---------



VÍA ACOLSURE, SEDE EL ALGODONAL, OCAÑA N. DE S.  
Línea Gratuita Nacional 018000 121022 / PBX: 097-5690088  
[www.ufpso.edu.co](http://www.ufpso.edu.co)



**DISEÑO DE UNA ARQUITECTURA BASADA EN TECNOLOGÍA  
“SDN” (REDES DEFINIDAS POR SOFTWARE) PARA EL  
LABORATORIO DE REDES Y TELECOMUNICACIONES DE LA  
UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA**

**AUTORES  
OSCAR IGNACIO LOBO DÍAZ  
DARWIN ACOSTA MANZANO**

**Trabajo de grado presentado como requisito para obtener el título de  
Ingeniero de Sistemas**

**DIRECTOR  
FABIÁN RANULFO CUESTA QUINTERO  
Ingeniero de Sistemas**

**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA  
FACULTAD DE INGENIERIAS  
INGENIERIA DE SISTEMAS**

**Ocaña, Colombia**

**Agosto, 2016**

## Indice

<b>Capitulo 1. Título.....</b>	<b>9</b>
<b>1.1 Planteamiento del problema.....</b>	<b>9</b>
1.2 Formulaci3n del problema de investigacion.....	10
1.3 Objetivos de la investigacion.....	10
1.3.1 General.....	10
1.3.2 Específicos.....	10
1.4 Justificaci3n .....	11
1.5 Delimitacion y alcances.....	12
1.5.1 Operativa .....	12
1.5.2 Conceptual.....	12
1.5.3 Geogr3fica. ....	12
1.5.4 Temporal.....	12
 <b>Capitulo 2. Marco de referencia .....</b>	 <b>13</b>
2.1 Antecedentes.....	13
2.1.1 Reseña Hist3rica de la Universidad Francisco de Paul Santander Ocaña .....	13
2.1.2 A nivel Internacional .....	16
2.1.3 A nivel Nacional.....	16
2.1.4 A nivel Local .....	17
2.2 Marco te3rico.....	17
2.3 Marco conceptual .....	18
2.4 Marco legal .....	27
 <b>Capitulo 3. Diseo metodol3gico.....</b>	 <b>36</b>
3.1 Tipo de investigaci3n.....	36
3.2 Diseo de la investigaci3n .....	36
3.3 Poblaci3n y muestra.....	36
<b>3.3.1 Poblaci3n Universo</b> .....	<b>36</b>
<b>3.3.2 Muestra.</b> ....	<b>37</b>
3.4 T3cnicas e instrumentos de recolecci3n .....	37
3.5 An3lisis de la informaci3n .....	37
3.5.1 Resultados encuesta a estudiantes de ingenier3a de sistemas y t3cnicos en telecomunicaciones.....	38

<b>Capítulo 4. Contexto de las redes definidas por software .....</b>	<b>44</b>
4.1 Arquitectura SDN .....	45
4.1.1 Capa de infraestructura .....	46
4.1.2 Capa de control .....	46
4.1.3 Capa de aplicación .....	47
4.2 Virtualización .....	48
4.3 Beneficios del SDN .....	51
4.3.1 Reducción de la complejidad.....	51
4.3.2 Reducción de costos. ....	51
4.3.3 Control centralizado y más granular.....	52
4.3.4 Disponibilidad, confiabilidad y seguridad.....	52
4.3.5 Agilidad en el desarrollo de aplicaciones .....	52
4.4 Usos de SDN .....	53
4.4.1 Cloud Computing. ....	53
4.4.2 Movilidad.....	53
4.4.3 Big Data. ....	54
4.4.4 Internet of Things. ....	54
4.5 Arquitectura sdn de multinacionales .....	54
4.5.1 Brocade.....	54
4.5.2 IBM.....	56
4.5.3 Hewlett-Packard .....	58
4.5.4 Vmware .....	60
4.5.5 Red de CPDs de Google .....	62
4.5.6 COMPARATIVA ENTRE CONTROLADOR DE CÓDIGO ABIERTO Y COMERCIAL.....	66
 <b>Capítulo 5. Requerimientos de la arquitectura del laboratorio .....</b>	 <b>70</b>
5.1 Esquema de direccionamiento del protocolo de la pila TCP/IP(IPv6).....	76
5.2 Diagrama fisico y logico del laboratorio .....	90
 <b>Conclusiones.....</b>	 <b>99</b>
<b>Recomendaciones .....</b>	<b>100</b>
<b>Referencias .....</b>	<b>101</b>
 <b>Apendices .....</b>	 <b>104</b>

## Lista de Tablas

Tabla 1. Sabe que es virtualización en un entorno de redes? .....	28
Tabla 2. Alguna vez instalo máquinas virtuales en el desarrollo de las asignaturas de redes .? .....	28
Tabla 3. Creé posible la manipulación de hardware de red a través de software.? .....	29
Tabla 4. Conoce alguna herramienta o software capaz de emular un entorno de redes? .....	30
Tabla 5. Durante su carrera ha escuchado el termino SDN “Redes Definidas por Software” .? .....	31
Tabla 6. Creé que adquirir conocimiento sobre tecnologías emergentes como redes .....	32
Tabla 7. Relación de equipos CISCO y Servidores del Laboratorio. ....	50
Tabla 8. Parámetros Comparativos.....	54
Tabla 9. Herramientas Openflow .....	63
Tabla 10. Hardware necesario para el desarrollo de SDN en el laboratorio. ....	58
Tabla 11. Direcccionamiento ipv6 para los dispositivos activos. ....	60
Tabla 12. Direcccionamiento ipv6 para los host. ....	63

## **Introducción**

Debido a los avances que hoy en día se tiene respecto a las comunicaciones, se evidencia un crecimiento muy significativo en las redes las cuales facilitan la interacción entre los usuarios, siendo este un elemento fundamental para enfrentar la saturación que se presentan en los medios de comunicación y luego adaptados a una necesidad específica.

El mercado actual muestra el aumento de compañías donde la tecnología es participe de este crecimiento global y se cuenta con excelentes recursos que a su vez no son suficientes para la optimización. De hecho en la actualidad se puede contar con el desarrollo de nuevas tecnologías tanto a nivel de hardware como de software aplicado a las redes, aunque sus conocimientos se centralizan en las mejoras físicas, dejando ciertos parámetros a nivel de software ya establecidos.

En el presente proyecto se busca proponer un diseño de una arquitectura basada en redes definidas por software (SDN) que puede aportar una mejora para la optimización para el control del flujo de datos, en un sistema de redes de comunicación para el laboratorio de redes y telecomunicaciones de la Universidad Francisco de Paula Santander Ocaña.

## Capítulo 1. Título

Diseño de una arquitectura basada en tecnología “sdn” (redes definidas por software) para el laboratorio de redes y telecomunicaciones de la Universidad Francisco de Paula Santander Ocaña.

### 1.1 Planteamiento del problema

Uno de los mayores retos que enfrenta la sociedad es el avance desproporcionado de las tecnologías, entre ellas las redes y telecomunicaciones, que aún a pesar de sus importantes beneficios al contexto industrial y educativo se vuelven obsoletas rápidamente, generando inconvenientes para quienes las utilizan.

Por lo tanto, las redes se han convertido en un factor crítico en el crecimiento de las comunicaciones, de igual forma la necesidad de optimizar la transmisión de información de una forma ágil y masiva, en donde es imperativo contar con elementos cuya infraestructura sea lo suficientemente idónea para la administración de los datos de una forma eficiente. La posibilidad de implementar de forma alterna herramientas de software que se adapten como funcionalidad en los sistemas de redes de la actualidad, hará que se torne más agradable y óptima para la administración de recursos que se encargan de controlar el flujo de datos (FEDESARROLLO)

En ese sentido, la manera como están concebidas las redes, hace que las investigaciones se limiten en el intento de experimentar nuevos protocolos de enrutamiento a gran escala

sobre redes reales. Esto es básicamente una de las razones por las que la infraestructura de red se ha mantenido inflexible limitando su eficiencia.

Esta problemática generalizada a nivel mundial permea además a la Universidad Francisco de Paula Santander Ocaña, limitando a los estudiantes y docentes en su búsqueda permanente, como institución superior de alternativas innovadoras; que afecta por lo tanto, aspectos como los dispositivos móviles, la virtualización de dispositivos de red, los servicios en la nube y la optimización de la transmisión de información, entre otros.

## **1.2 Formulación del problema de investigación**

¿Qué ventajas trae a la Universidad Francisco de Paula Santander Ocaña el análisis y diseño de una arquitectura basada en tecnología “SDN” (Redes Definidas por Software) para el laboratorio de Redes y Telecomunicaciones?

## **1.3 Objetivos de la investigación**

**1.3.1 General.** Diseñar una arquitectura basada en tecnología “SDN” (Redes Definidas por Software), para el laboratorio de Redes y Telecomunicaciones de la Universidad Francisco de Paula Santander Ocaña.

### ***1.3.2 Específicos.***

Realizar un estudio de caracterización técnica y operacional de arquitecturas existentes en las redes definidas por software.



Definir un esquema de direccionamiento adecuado mediante la pila de protocolo TCP/IP (IPV6) que permita la comunicación de la Arquitectura.

Diseñar el diagrama físico y lógico de la estructura de la red, de acuerdo a los parámetros establecidos en los objetivos anteriores.

#### **1.4 Justificación**

Las redes definidas por software SDN, facilitan y mejoran la transmisión de información en tiempo real, pues conlleva a que la velocidad de transmisión aumente de la misma manera que el consumo de energía de los dispositivos físicos disminuya, demostrando que puede haber menos pérdidas de conexión y mejor administración del flujo de datos y de esta manera disponer de redes más programables, automatizables y flexibles.

En los procesos de enseñanza y aprendizaje relacionados con las redes y las telecomunicaciones, resulta fundamental la realización de prácticas experimentales de laboratorio sobre sistemas reales, ya que ayudan a que el estudiante asimile fácilmente los conceptos teóricos y al desarrollo de competencias indispensables para su actividad profesional.

Por lo tanto, teniendo en cuenta que la Universidad Francisco de Paula Santander ha realizado significativas inversiones en el laboratorio de redes y telecomunicaciones se vuelve casi una exigencia el desarrollo de proyectos que fortalezcan los beneficios que brinda este, para el proceso académico.

En ese sentido surge la idea del diseño de una arquitectura basada en tecnología “SDN” (Redes Definidas por Software), para el laboratorio de Redes y Telecomunicaciones de la Universidad Francisco de Paula Santander Ocaña, que permita a los estudiantes y docentes de Ingeniería de sistemas y carreras afines disponer de una herramienta que facilite sus prácticas sobre redes reales, que fortalezcan su proceso de formación, conocedores de las ventajas que conlleva la utilización de este tipo de arquitecturas.

## **1.5 Delimitacion y alcances**

**1.5.1 Operativa.** Esta propuesta se limita a proponer una arquitectura que sirva como guía de referencia para los estudiantes de Ingeniería de Sistemas y el Técnico Profesional en Telecomunicaciones de la Universidad Francisco de Paula Santander de Ocaña en lo relacionado a Redes Definidas por Software. No incluye la implementación de la arquitectura.

**1.5.2 Conceptual.** Para elaborar de manera adecuada el proyecto se tendrá en cuenta los siguientes conceptos: Red de datos, Proveedor de servicio de internet (ISP), Zona Militarizada (DM), Zona Desmilitarizada (DMZ), Open Signaling, Active networking, Netconf, Ethane, Openflow, Topología.

**1.5.3 Geográfica.** El lugar donde se va a llevar a cabo la propuesta es en la ciudad de Ocaña, Norte de Santander, específicamente en el laboratorio de Redes y Telecomunicaciones de la Universidad Francisco de Paula Santander Ocaña.

**1.5.4 Temporal.** La realización de la propuesta presupone un tiempo máximo de tres (3) meses calendario, a partir de la aprobación del anteproyecto.

## Capítulo 2. Marco de referencia

### 2.1 Antecedentes

*2.1.1 Reseña Histórica de la Universidad Francisco de Paul Santander Ocaña* . En noviembre de 1973 se suscribió un contrato para la realización de un estudio de factibilidad denominado "un centro de educación superior para Ocaña" que fue terminado y sugirió la creación pronta de un programa de educación a nivel de tecnología en énfasis en ciencias sociales, matemáticas y física. En diciembre de ese mismo año, el rector de la Universidad Francisco de Paula Santander, José Luís Acero Jordán, le envió copia de dicho estudio al Icfes, Instituto que conceptúo que el proyecto para abrir el centro de estudios en Ocaña, era recomendable (Ocaña).

Según Acuerdo No. 03 del 18 de Julio de 1974, por parte del Consejo Superior de la Universidad Francisco de Paula Santander Cúcuta, se crea la Universidad Francisco de Paula Santander Ocaña, como máxima expresión cultural y patrimonio de la región; como una entidad de carácter oficial seccional, con AUTONOMIA administrativa y patrimonio independiente, adscrito al Ministerio de Educación Nacional.

Su primer coordinador el doctor Aurelio Carvajalino Cabrales, buscó un lugar adecuado para funcionar la sede, en los claustros Franciscanos al costado del templo de la Gran Convención y con las directivas del colegio José Eusebio Caro, se acordó el uso compartido del laboratorio de física.

En 1975 comenzó la actividad académica en la entonces seccional de la Universidad Francisco de Paula Santander con un total de 105 estudiantes de Tecnología en Matemáticas y Física, y su primera promoción de licenciados en Matemáticas y Física se logró el 15 de diciembre de 1980.

La consecución de 27 hectáreas de la Hacienda El Rhin, en las riberas del Río Algodonal, en comodato a la Universidad por 50 años, que la antigua Escuela de Agricultura de Ocaña cedió a la Universidad, permitió la creación del programa de Tecnología en Producción Agropecuaria, aprobado por el Consejo Superior mediante el Acuerdo No. 024 del 21 de agosto de 1980, y luego el ICFES otorgó la licencia de funcionamiento el 17 de febrero del año siguiente. Luego se crean las Facultades.

La **Facultad de Ciencias Agrarias y del Ambiente**, fue creada según Acuerdo 084 del 11 de septiembre de 1995 conformada por los departamentos de Ciencias Agrícolas y del Ambiente y el departamento Ciencias Pecuarias junto a los programas académicos de Tecnología Agropecuaria (Acuerdo N° 024 del 21 de agosto de 1980), Zootecnia (Acuerdo N°057 y 058 del 27 de junio de 2007), e Ingeniería Ambiental (Acuerdo 089 del 9 de octubre 1995 con resolución **10542 de 8-ago-2013** del MEN).

La **Facultad de Ciencias Administrativas y Económicas**, fue creada según Acuerdo No. 008 del 05 de marzo de 2003; está conformada por el departamento de Ciencias Administrativas y Departamento de Ciencias Contables y Financieras. Están adscritos los

programas académicos de Tecnología en Gestión Comercial y Financiera (Acuerdo No, 024 del 29 de Junio de 1988 con la resolución **9886 de 31-jul-2013** del MEN), Administración de Empresas (Acuerdo No, 024 del 29 de Junio de 1988 ) y la profesionalización (Acuerdo No. 118 del 16 de Noviembre de 1994 Resolución **1867 de 26-feb-2013**); Contaduría Pública (Acuerdo No. 007 del 05 de Marzo de 2003 y según resolución **13873 del 8-oct-2013** del MEN).

La **Facultad de Ingenierías** fue creada según acuerdo 007 del 20 de febrero de 2006, conformada con los departamentos de Ingeniería Civil, Ingeniería Mecánica y el departamento de Sistemas e Informática. Con los registros calificados de los programas completos de acuerdo a la Resolución 2909 de julio 21 de 2005 para el programa de Ingeniería Civil (Resolución **6779 de 20-jun-2012**) e Ingeniería Mecánica (Resolución **6233 de 7-jun-2012**), Ingeniería de Sistemas (Resolución **9950 de 31-jul-2013**). La creación del Técnico Profesional en Telecomunicaciones con registro calificado (Resolución 5366 de agosto 25 de 2008) y el Técnico Profesional en Informática con registro calificado (Resolución 4613 de julio 18 de 2008).

La **Facultad de Educación, Artes y Humanidades** de la Universidad Francisco de Paula Santander Ocaña fue creada según acuerdo 063 del 20 de noviembre de 2006, está conformada con los departamentos: de Matemáticas, Física y Computación y el Departamento de Humanidades. Según el Acuerdo No. 010, marzo 29 de 2004 se crea el plan de estudios del programa de Comunicación Social (Resolución **5363 de 10-may-2013**,) y Derecho con registro calificado (Resolución 10185 de noviembre 22 de 2010). En el mes de noviembre de

2005, se suscribió el convenio de asociación No. 1744/05 con el Ministerio de Cultura, con el objeto de apoyar el proceso de estructuración académica de la Escuela de Bellas Artes.

**2.1.2 A nivel Internacional.** Implementación de un prototipo de red definida por software (SDN). Empleando una solución basada en software. Diana Gabriela Morillo Fuentala. Escuela Politécnica Nacional. Quito, mayo de 2014. Debido a que las redes se están volviendo la parte crítica de la infraestructura de las empresas, hogares e instituciones educativas, es necesario trabajar en el desarrollo de las redes programables, con equipos de conectividad programables que, usando virtualización incrementen la tasa de innovación en la infraestructura de red <sup>(Hidalgo)</sup>.

**2.1.3 A nivel Nacional.** Diseño e implementación de una aplicación de red bajo la arquitectura SDN. Ing. Diego Armando Maldonado Hidalgo. Pontificia Universidad Javeriana. Facultad de Ingeniería. Maestría en ingeniería electrónica. Bogotá, mayo de 2014. Este proyecto pretende ser pionero en la implementación de una aplicación SDN sobre interfaces físicas a nivel educativo en Colombia (Hidalgo).

Propuesta para la implementación de un laboratorio de acceso remoto usando redes definidas en software. Ana Milena Rojas Calero. Facultad de Ingeniería Departamento Académico de Tecnologías de Información y Comunicaciones. Maestría en Gestión informática y telecomunicaciones. Santiago de Cali, 2012. Dentro de los objetivos propuestos está la definición de las interfaces de experimentación de tal forma que estas puedan ser accedidas desde internet y el diseño de la arquitectura del laboratorio (Calero).

**2.1.4 A nivel Local.** Proyectos relacionados directamente con arquitectura SDN, no se encontraron dentro de la Universidad Francisco de Paula Santander Ocaña.

## 2.2 Marco teórico

Para García (2015), una de las principales características de SDN es que concibe la red como un elemento unificado, lo que permite, entre otras cosas centralizar el control y aplicar políticas altamente granulares desde una única consola de mando. Aunque hasta ahora no se ha hecho demasiado hincapié en la seguridad como una de las facetas más interesantes de este enfoque de arquitectura, lo cierto es que SDN tiene mucho que aportar al área de la seguridad de TI, y la seguridad puede ser un importante incentivo para las empresas a la hora de adoptar SDN en los próximos años (García).

En la encuesta de Packet Design correspondiente al año 2014, donde se sondearon a 60 proveedores de servicios, 40 menos que en 2013, llegando a la conclusión de que el 53% ya tiene **redes definidas por software (SDN)** en producción, frente al 19% del año pasado. Como motivo de la adopción, conseguir una mayor agilidad para dar soporte al lanzamiento de nuevos servicios aparece en primer lugar, con un incremento del 150% respecto de 2013 (Network World).

Las redes definidas por software (SDN) permiten a las organizaciones acelerar la implementación y la distribución de aplicaciones reduciendo drásticamente los costos de TI mediante la automatización del flujo de trabajo basada en políticas. La tecnología SDN habilita arquitecturas de nube mediante distribución y movilidad de aplicaciones de manera

automatizada, a pedido y a escala. Las SDN incrementan los beneficios de la virtualización del centro de datos, ya que aumentan la flexibilidad y la utilización de recursos y reducen los gastos generales y los costos de infraestructura.

Para lograr estos objetivos empresariales, las SDN convergen la administración de los servicios de red y aplicaciones en plataformas de coordinación centralizadas y ampliables que pueden automatizar el aprovisionamiento y la configuración de toda la infraestructura.

Políticas de TI centralizadas comunes unifican grupos y flujos de trabajo de TI dispares. El resultado es una infraestructura moderna que puede distribuir nuevas aplicaciones y servicios en minutos, en vez de días o semanas como antes.

Las SDN proporcionan velocidad y agilidad al implementar nuevas aplicaciones y servicios empresariales. La flexibilidad, las políticas y la programabilidad son las señas de identidad de las soluciones SDN de Cisco, con una plataforma capaz de manejar las necesidades más exigentes de la red, tanto presentes como futuras.

### **2.3 Marco conceptual**

Para elaborar de manera adecuada el proyecto se tendrá en cuenta los siguientes conceptos: Red de telecomunicación, red de datos, Proveedor de servicio de internet (ISP), Zona Militarizada (DM), Zona Desmilitarizada (DMZ), Open Signaling, Active networking, Netconf, Ethane, Openflow, Topología.

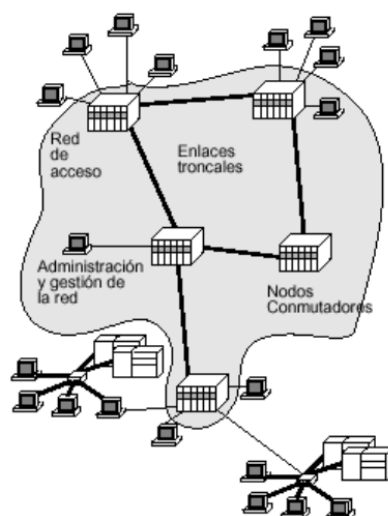
**Redes de Telecomunicación.** Las redes de telecomunicación se diseñan y construyen con el objetivo de prestar servicios de comunicación de diversa naturaleza (voz, datos e



imagen). Tradicionalmente éstas, independientemente de ser públicas o privadas, se han clasificado en redes de voz y de datos aunque hoy en día no tenga mucha validez. Ya se ha conseguido transmitir voz por una red de datos IP.

Según el Anexo de la Ley 11/1998 de la Ley General de Telecomunicaciones, "una red de telecomunicaciones está formada por los sistemas de transmisión y, cuando proceda, los equipos de conmutación y demás recursos que permitan la transmisión de señales entre puntos de terminación definidos mediante cable, medios ópticos o de otra índole".

En una red de telecomunicación, ver Figura 1. Red de Telecomunicaciones, se distingue la red de transporte, la red de conmutación y la red de acceso. La red de transporte contiene los elementos de transmisión y de interconexión entre los distintos elementos de red, además puede ser válida y compartida por distintos tipos de servicio (voz, imagen,..). La red de conmutación, en cambio, suele ser específica para el servicio prestado (conmutación de circuitos en RTB y de paquetes en X.25, Frame Relay, ATM). Por último, la red de acceso la constituyen los elementos que permiten conectar a cada abonado con la central local de la que dependa.



**Figura 1. Red de Telecomunicaciones**

Fuente: <http://personales.unican.es/zorrillm/MaterialOLD/redes.pdf>

**Redes dedicadas, de conmutación y difusión.** Con independencia de su estructura, las redes de telecomunicación pueden ser dedicadas, de conmutación o de difusión.

Las redes dedicadas son redes de uso exclusivo que se caracterizan por ser alquiladas por uno o varios usuarios estando cerradas para el resto. Pueden ser de tipo punto a punto, es decir, que conectan dos terminales, lo que tiene un coste alto pero ofrece seguridad y alta velocidad; o, multipunto, que conecta un nodo con varios terminales.

Las redes de conmutación establecen el camino por el que va a discurrir la información, bien antes del envío (caso de la voz) o durante el mismo (caso de los datos).

Las redes de difusión, caso de la televisión, la radio y las LAN, poseen un único medio de transmisión para conectar entre sí todos los equipos, por lo que es necesaria la multiplexación.

**Redes públicas, privadas y virtuales:** Las redes de comunicación de ámbito público son generalmente proporcionados por operadores con licencia para ello en cada país y constan de líneas conmutadas, líneas punto a punto y de una red pública de datos como por ejemplo Iberpac en España. Esta solución ofrece a todos los usuarios las mismas opciones, teniéndose que adaptar expresamente a ellos. Puede tener interés desde el punto de vista económico pero nada más.

La redes privadas aunque hacen uso de ciertos elementos proporcionados por los operadores, la mayor parte son privados y, cabe destacar que la gestión y el control de la misma la realiza el propio usuario o bien lo subcontrata. La solución de red privada virtual consiste en reservar, para uso exclusivo de un usuario o empresa, los recursos de transmisión y conmutación de la red pública que requiere siendo el operador quien se responsabiliza de su control y mantenimiento.

**Servicios de valor añadido** Los servicios de valor añadido son servicios ofrecidos por distintas empresas u organismos a través de redes de telecomunicación que se caracterizan por:

- Estar abiertas a cualquier usuario

- Proporciona un buen aprovechamiento de recursos y alta rentabilidad al ser utilizados por muchos usuarios. Como por ejemplo son los servicios de telealarma, videoconferencia, fax, correo electrónico.

### **Organismos de normalización.**

Unión Internacional de Telecomunicaciones (UIT), fundada en 1865, es la más universal. Es el principal organismo encargado de la emisión de normas de las telecomunicaciones. Es muy compleja y extensa y desde 1992 consta de tres subsectores:

- ITU-I Unión Internacional de Telecomunicaciones - sector telecomunicaciones.
- ITU-R Unión Internacional de Telecomunicaciones - sector comunicaciones de radio.
- ITU-D Unión Internacional de Telecomunicaciones - sector desarrollo.

La Organización Internacional de Normalización (ISO) integrada por usuarios y fabricantes. Ha definido un modelo de referencia que establece unas normas para interconectar diferentes equipos y posibilitar su comunicación.

El Institución de Ingenieros Eléctrico y Electrónicos (IEEE) colabora en el desarrollo de estándares. Últimamente centrados en los estándares que desarrollan el nivel 1 y 2 del modelo OSI (802.3, 802.4, 802.5).

El Instituto Americano de Estándares Nacionales (ANSI) que coordina la estandarización del sector privado. Colabora con el ISO.

**Openflow.** Es uno de los más recientes hallazgos en lo que a innovación de protocolos de comunicación se refiere. Tuvo un predecesor llamado que Ethane, dio las pautas para lo que sería más adelante su desarrollo (Organismos de Normalización).

Según sus creadores, es un protocolo Openflow para operar redes SDN. Fue desarrollado con base en switches Ethernet; es un standard abierto de comunicación entre un controlador (elemento principal de las SDN) y dispositivos de conmutación (McKeown et al., 2008). Al igual que TCP, su estructura está diseñada por mensajes, que establecen una comunicación y generan las acciones correspondientes.

Openflow versión 1.1.0 (Pfa, y otros, 2011) detalla cómo se componen estos mensajes, al igual que los tipos y valores que los componen. Algunos de estos mensajes son:

- Header (Encabezado de todos los paquetes)
- Type (Tipo de mensaje), pueden tener valores como:
  - Mensajes inmutables
  - Mensajes de configuración
  - Mensajes asíncronos
  - Mensajes con comandos al controlador
  - Mensajes estadísticos
  - Mensajes de barrera
  - Mensajes de configuración de colas

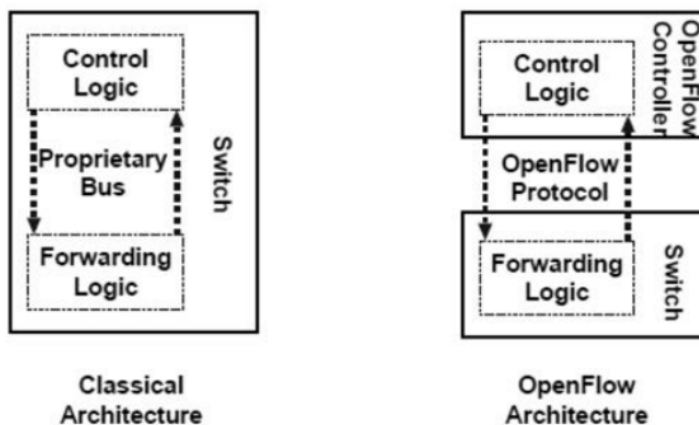
Asimismo, define la estructura de puertos: su descripción, convenciones, características. También la estructura de colas: descripción, propiedades etc., toda la documentación que sustenta:

- Entradas de flujos, el respectivo “wildcard” para identificación de puerto
- Vlan
- Tipo de trama Ethernet
- Tipo de servicio
- Protocolos de red o transporte como TCP, UDP, IP, MPLS, y todo lo relacionado con el flujo de instrucciones y acciones para cada uno de ellos.

En últimas, un protocolo es un lenguaje; por tanto, la comunicación sólo es posible establecerse con un emisor y un receptor. Openflow es el lenguaje de comunicación entre el controlador y los switches Openflow.

**Funcionamiento de Openflow.** El funcionamiento de este protocolo está dado porque al separar el plano de datos del plano de control, se puede tener un mejor control de la red, y por tanto, mayor eficiencia.

Los dispositivos actuales tienen sus propios Firmware. En ellos se define cómo deben ser tratados los paquetes de acuerdo con la configuración realizada; además son propietarios, por tanto, difíciles de integrar.



## Figura 2. Protocolo OpenFlow

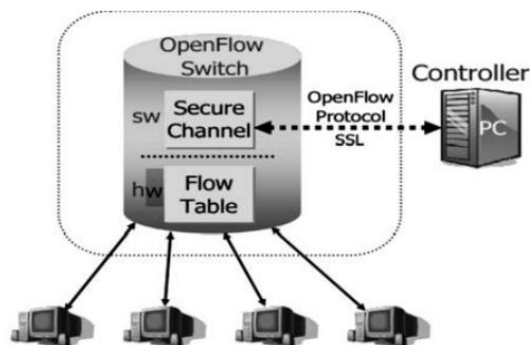
Fuente: Sherwood et al., 2009

La disociación del control de datos supone delegar esto a un controlador externo, es decir, se puede programar fuera del dispositivo la manera cómo van a ser procesados los flujos de paquetes. Estos últimos serán inventariados dentro de una tabla de flujos, que consignará la información del flujo de paquetes (MAC's, IP, puertos, etc.); así habrá un tipo de “Learning” que permitirá conocer qué orígenes y destinos han pasado por el dispositivo.

Con el transcurrir del tiempo se ha hecho evidente la necesidad de una tecnología de transporte que funcione con un plano de control centralizado. Además, que facilite la administración de todos los elementos de la red, para analizar y procesar el tráfico que fluye a través de ella.

Iniciativas como la gestión de redes busca, de alguna forma, utilizar aplicaciones que permitan entender el tráfico que transportan las redes. No obstante, sólo permiten obtener datos estadísticos; no hay programación que pueda reparar fallos o desviar rutas, por ejemplo. El funcionamiento de contempla esta Openflow necesidad. El protocolo es el medio por el cual un dispositivo opera según la configuración que se haga en el controlador.

En la Figura 3. Arquitectura Openflow Switch (McKeown et al., 2008) se ilustra el (OFS) y sus componentes.



**Figura 3. Arquitectura Openflow Switch**

Fuente: <http://blogs.salleurl.edu/nice-rack/2014/04/22/data-center-management/>

El muestra claramente cómo se Openflow Switch ubica el protocolo entre él y el controlador. switch También a nivel del canal de software comunicación que establece con el protocolo SSL, y a nivel de hardware, la tabla de flujos.

Estos 3 componentes necesarios para el funcionamiento, realizan:

1) Tabla de flujos: Acción asociada a cada entrada, que determina cómo el debe switch procesar el flujo.

2) SSL ( ): Capa de Secure Sockets Layer conexión segura, protocolo de conexión usado para el controlador y los dispositivos de conmutación.

3) OFP (Openflow Protocol): Un estándar abierto de comunicación entre el controlador y los dispositivos.

Las acciones que puede realizar el OFS son:

1) Forwarding: Reenvío de flujo de paquetes por un(os) puerto(s) específicos.

2) Encrypting: Encapsular y cifrar flujos de paquetes de datos para un controlador.



3) Drop: Borrado de paquetes por seguridad para frenar ataques de DDoS . Estas acciones son consignadas en la tabla de flujos, que tiene 3 campos especiales, donde queda almacenada la información:

- Header: Encabezado del paquete, define el flujo.
- Action: La acción. Cómo se procesará el flujo.
- Statistics: Estadísticas de procesamiento, número de paquetes y por cada flujo.

En este orden, el (camino de datos) de datapath un con asocia una acción a cada Switch Openflow flujo de entrada.

De acuerdo con la política (establecida desde el controlador), dicha acción es registrada, luego le indica al dispositivo cómo debe procesarla.

Ahora bien, los fabricantes de tecnología (específicamente de para redes) han sido hardware por muchos años, dueños del para sus Firmware máquinas. Ese “secreto industrial” ha sido en gran medida lo que ha posibilitado que se busquen estándares para que exista interoperabilidad entre ellos.

## **2.4 Marco legal**

A continuación se presentan las diferentes leyes y decretos que ofrecen una base legal para el desarrollo este proyecto.

**Ley 1570 de 2012.** "Por medio de la cual se aprueba el "Convenio Interamericano sobre Permiso Internacional de Radioaficionado", adoptado el 8 de junio de 1995 en Montrouis,

República de Haití, y el "Protocolo de Modificaciones al Convenio Interamericano sobre el Permiso Internacional de Radioaficionado", adoptado el 10 de junio de 2003 en Santiago, República de Chile".

**Ley 873 de 2004.** Por medio de la cual se aprueban el Instrumento de Enmienda a la Constitución de la Unión Internacional de Telecomunicaciones (Ginebra, 1992), con las enmiendas adoptadas por la Conferencia de Plenipotenciarios (Kyoto, 1994) (Enmiendas adoptadas por la Conferencia de Plenipotenciarios (Minneapolis, 1998), firmado en Minneapolis, el seis (6) de noviembre de mil novecientos noventa y ocho (1998), y el Instrumento de Enmienda al Convenio de la Unión Internacional de Telecomunicaciones (Ginebra, 1992), con las enmiendas adoptadas por la Conferencia de Plenipotenciarios (Kyoto, 1994) (Enmiendas adoptadas por la Conferencia de Plenipotenciarios (Minneapolis, 1998), firmado en Minneapolis, el seis (6) de noviembre de mil novecientos noventa y ocho (1998).

**Ley 1341 de 2009.** Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones (República, 2009).

Artículos 12 y 68 reglamentados por el Decreto 2044 del 19 de septiembre de 2013. Ley reglamentada por el Decreto 2693 del 21 de diciembre de 2012. Parágrafo 2° del artículo 57 modificado por el artículo 59 de la Ley 1450 de 2011, Inciso 1° y 3° y el parágrafo 1° y 2° del artículo 69 derogado por el artículo 276 de la Ley 1450 de 2011. numerales 6 y 7 del artículo 18, el numeral 11, del artículo 28 y el artículo 29 de la Ley 1341 de 2009 derogados por el Decreto 4169 del 2011.

**Estándar 802.11.** El estándar 'IEEE 802.11' define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de Funcionamiento en una WLAN. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana.

**TIA-568B: TIA/EIA-568-B** tres estándares que tratan el cableado comercial para productos y servicios de telecomunicaciones.

**ANSI / TIA / EIA – 569:** Norma De Construcción Comercial EIA/TIA-569 Para espacios Y Recorridos De Telecomunicaciones.

Además de esto, en el marco legal se incluyen los decretos y resoluciones del Ministerio de Comunicaciones en lo referente al espectro electromagnético y a la asignación de frecuencias para telecomunicaciones, dispositivos y tecnologías inalámbricas.

**Constitución Política de Colombia.** En su artículo 75 en el inciso 1° establece: "El espectro electromagnético es un bien público inajenable e imprescriptible sujeto a la gestión y control del Estado. Se garantiza la igualdad de oportunidades en el acceso a su uso en los términos que fije la ley"; Para garantizar el pluralismo informativo y la competencia, el Estado intervendrá por mandato de la ley para evitar las prácticas monopolísticas en el uso del espectro electromagnético (Constituyente).

Con este artículo se refleja claramente que existen unas reglamentaciones nacionales que rigen la utilización del espectro electromagnético, por lo tanto deben seguirse las

disposiciones del Estado colombiano para su uso, las cuales serán descritas en el presente proyecto.

**Política de territorios digitales.** Es necesario destacar la importancia de los territorios digitales en los siguientes términos:

Desde la perspectiva de Nación, el Ministerio de Comunicaciones en el marco del Plan de Desarrollo pretende que “En el 2019, el sector de telecomunicaciones debe ser uno de los principales impulsores del crecimiento económico y del desarrollo social del país, y contribuir a una sociedad informada, conectada e integrada al entorno global (Política de Territorios Digitales , 2011).

Ministerio de Comunicaciones, República de Colombia – Política de Territorios Digitales 2006-2010.

Siendo así, la visión estratégica del sector se ha traducido en 6 metas:

Adaptar el marco normativo e institucional a la convergencia tecnológica y promover la competencia.

Preparar al sector para la globalización de servicios.

Garantizar niveles apropiados de acceso y servicio universal.

Lograr coberturas de servicios de voz y datos (Internet), acorde con las metas de desarrollo económico del país.

Disponer de una infraestructura moderna y confiable para la televisión pública. Contar con un sector postal eficiente e integrado a la economía global.

En el marco conceptual propuesto por el Ministerio de Comunicaciones, respecto a los procesos de creatividad y de innovación, a nivel territorial, ubica los territorios digitales como procesos de generación de información y aplicación de conocimiento, en las regionales con el propósito de dinamizar transformaciones con innovación de tecnologías, cambios económicos, transformaciones sociales y cambios espaciales.

La Política de los territorios digitales tiene por objetivo llevar a nivel local y territorial, estrategias de desarrollo social y económico haciendo uso de las Tecnologías de Información y las Comunicaciones –TIC, en las actividades de gobierno, de las empresas, de la educación, de salud y de entretenimiento. Siendo así, el proceso de transformación combina factores como: innovaciones tecnológicas, cambios económicos, transformaciones sociales y cambios espaciales; todo lo anterior, soportado por ciertas tecnologías de la información y la comunicación.

Así mismo, contempla la estrategia de sumar esfuerzos de las autoridades locales, los operadores de telecomunicaciones, cámara de comercio, otras organizaciones sociales y el Gobierno Nacional a través del Ministerio de Comunicaciones, en desarrollo de los esquemas:

Gobierno: Trámites en línea, Gestión pública más eficiente y transparente, reducción costos de operación, menor tiempo de respuestas, seguimiento a proyectos, y rendición de cuentas.

Educación: Formación de capacidades, soporte y gestión educativa, acceso comunidad a salas informáticas, Tecnologías de Información y las Comunicaciones - TIC en Bibliotecas.

Comunicación: Comercio, Pymes digitales, empresarismo, banco de oportunidades, digitalización de procesos empresariales.

Gestión Pública: Iniciativas Tecnologías de Información y las Comunicaciones- Tics de la comunidad, Participación Comunitaria.

La directriz desde el orden nacional, pretende que las autoridades locales y regionales incorporen las Tecnologías de Información y las Comunicaciones- Tics en los Planes de Desarrollo, como “indispensable, articuladora y transversal de la generación de riqueza y bienestar social”<sup>15</sup>.

**Decreto 2103 de 2003.** Por el cual se reglamentan los servicios de telecomunicaciones que utilicen sistemas de radiocomunicación convencional de voz y/o datos, y se dictan otras disposiciones.

Mediante el presente se pretende reglamentar los servicios de telecomunicaciones que utilicen sistemas de radiocomunicación convencional de voz y/o datos, establecer las condiciones bajo las cuales se otorgarán concesiones, y fijar los mecanismos para la autorización de las redes y el otorgamiento de los permisos (Decreto 2013 de 2003, 2003).

En el Artículo 3°. Concesión, se expone que las concesiones para la prestación de servicios de telecomunicaciones que utilicen sistemas de radiocomunicación convencional de voz y/o datos dentro del territorio nacional, se otorgarán por el Ministerio de Comunicaciones mediante licencia, a solicitud de parte.

Por otra parte, en el Artículo 4°, se estipulan los requerimientos para ser titular de la licencia para la utilización de sistemas de radiocomunicación, los cuales son:

- Ser sociedad especializada en la prestación al público de servicios de telecomunicaciones, y acreditar una duración no inferior a la del plazo de la concesión y un año más.

- No estar incurso en alguna causal de inhabilidad, incompatibilidad o prohibición de orden constitucional o legal.

15 Ministerio de Comunicaciones, República de Colombia – Política de Territorios Digitales 2006-2010.

En el Artículo 5°, se establecen los lineamientos para la duración y prórroga de las licencias, las cuales otorgarán por un término máximo de diez (10) años, el cual podrá ser prorrogado hasta por un período igual. En todo caso, la duración total de la licencia, incluyendo sus prórrogas no podrá exceder de veinte (20) años.

Las características técnicas esenciales de la red, se establecen en el Artículo 7º, donde se consideran características técnicas esenciales de la red de telecomunicaciones, las siguientes:

Frecuencias radioeléctricas asignadas.

Tipo de emisión y ancho de banda.

Área de servicio.

Ubicación de las estaciones repetidoras y bases fijas principales.

Ganancia, altura y patrón de radiación de las antenas.

Potencia autorizada.

Horario de utilización.

Toda modificación de las características técnicas esenciales de la red de telecomunicaciones autorizada destinada a la prestación de servicios de telecomunicaciones que utilicen sistemas de radiocomunicación convencional de voz y/o datos, requiere autorización previa y expresa del Ministerio de Comunicaciones.

Por su parte, el Artículo 8º, de este decreto, expone los aspectos relacionados con el otorgamiento del permiso para uso del espectro radioeléctrico, afirmando que éste se otorgará por el Ministerio de Comunicaciones a solicitud de parte, salvo cuando se presente algún evento, en los cuales el otorgamiento se hará previo el desarrollo de un procedimiento administrativo que permita la concurrencia de interesados.

**Resolución número 000689 de 2004.** Por la cual se atribuyen unas bandas de frecuencias para su libre utilización dentro del territorio nacional, mediante sistemas de acceso



inalámbrico y redes inalámbricas de área local, que utilicen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia, y se dictan otras disposiciones.

Como resultado de esta norma, la distribución de las bandas de frecuencia se presenta en el Artículo 5°. Bandas de frecuencias. El cual dice textualmente: “Se atribuyen dentro del territorio nacional, a título secundario, para operación sobre una base de no-interferencia y no protección de interferencia, los siguientes rangos de frecuencias radioeléctricas, para su libre utilización por sistemas de acceso inalámbrico y redes inalámbricas de área local, que empleen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia, en las condiciones establecidas por esta resolución (Comunicaciones)

- a) Banda de 902 a 928 MHz;
- b) Banda de 2 400 a 2 483,5 MHz;
- c) Banda de 5 150 a 5 250 MHz;
- d) Banda de 5 250 a 5 350 MHz;
- e) Banda de 5 470 a 5 725 MHz;
- f) Banda de 5 725 a 5 850 MHz

## Capítulo 3. Diseño metodológico

### 3.1 Tipo de investigación

El tipo de investigación que se llevó a cabo fue descriptiva, ya que con este proyecto se buscaba analizar y describir, además los estudios descriptivos utilizan el método de análisis para lograr caracterizar un objeto de estudio o una situación concreta, señalar sus características y propiedades, combinada con ciertos criterios de clasificación, sirve para ordenar, agrupar o sistematizar los objetos involucrados en el trabajo indagatorio.

### 3.2 Diseño de la investigación

En busca de cumplir con los objetivos propuestos para la realización del presente proyecto; y teniendo en cuenta que el tipo de investigación a empleada fue la descriptiva, es necesario emplear el método inductivo que se inicia de un caso específico, para llegar a una conclusión, en este caso que plantee la necesidad elaborar un diseño. Este método permite la formación de hipótesis, investigación de leyes científicas, y las demostraciones. La inducción puede ser completa o incompleta. Para aplicar el método inductivo se requiere que el conocimiento comience teniendo contacto directo con los elementos reales, y a la vez, parta de la determinación aproximada de la serie de fenómenos que se van a inducir.

### 3.3 Población y muestra

**3.3.1 Población Universo.** Para este proyecto, el universo lo conforman los estudiantes de ingeniería de sistemas y técnicos en telecomunicaciones que desarrollan sus clases y

prácticas en el laboratorio de redes y telecomunicaciones de la Universidad Francisco de Paula Santander Ocaña, es decir 99 estudiantes.

**3.3.2 Muestra.** Es una parte del universo, que reúne todas las condiciones o características de la población, de manera que sea lo más pequeña posible, pero sin perder exactitud. En este caso por ser una muestra finita, se tomó la misma población. Por lo tanto se trabajara con el 100% de la misma

### **3.4 Técnicas e instrumentos de recolección**

Las técnicas e instrumentos de recolección a emplear para la obtención de la información necesaria para el desarrollo del proyecto, son la encuesta y la revisión documental.

La encuesta, está compuesta de un cuestionario, que contiene una serie de preguntas, en cuya formulación se observa el problema que se desea estudiar. A través de ellas se especificarán los requerimientos para el presente proyecto y serán aplicadas a los supuestos clientes.

Toda la información necesaria para definir el marco teórico del proyecto, se obtendrá por medio de revisión documental de material bibliográfico y en Internet.

### **3.5 Análisis de la información**

Los resultados de la encuesta se tabularon, se graficaron y se analizaron cuantitativa de acuerdo a los resultados, pues se buscaba obtener los datos suficientes para lograr la ejecución de este proyecto.

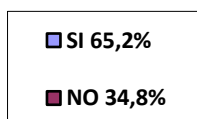
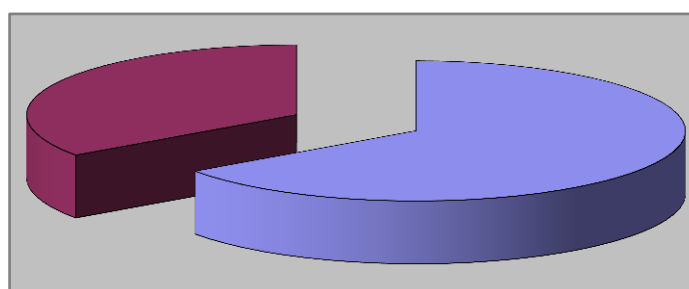
### 3.5.1 Resultados encuesta a estudiantes de ingeniería de sistemas y técnicos en telecomunicaciones.

**Tabla 1.**

*¿Sabe que es virtualización en un entorno de redes?*

RESPUESTA	FRECUENCIA	PORCENTAJE
SI	65	65.2%
NO	34	34.8%
<b>TOTAL</b>	<b>99</b>	<b>100%</b>

Nota fuente: Autores del proyecto de investigación



**Figura 4. Sabe que es virtualización en un entorno de redes?**

Nota fuente: Autores del proyecto de investigación

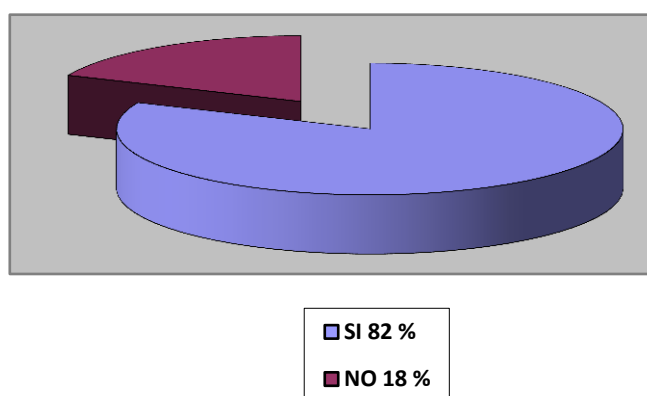
Evidentemente, la comunidad estudiantil tiene conocimientos en lo referente a virtualización.

**Tabla 2.**

*Alguna vez instalo máquinas virtuales en el desarrollo de las asignaturas de redes .?*

RESPUESTA	FRECUENCIA	PORCENTAJE
SI	81	82%
NO	18	18%
<b>TOTAL</b>	<b>99</b>	<b>100%</b>

Nota fuente: Autores del proyecto de investigación



**Figura 5.** *Alguna vez instalo máquinas virtuales en el desarrollo de las asignaturas de redes.*

Nota fuente: Autores del proyecto de investigación

En la encuesta realizada, se pudo evidenciar que la comunidad estudiantil ha adquirido competencias en la asignatura de redes en lo referente a virtualización.

**Tabla 3.**

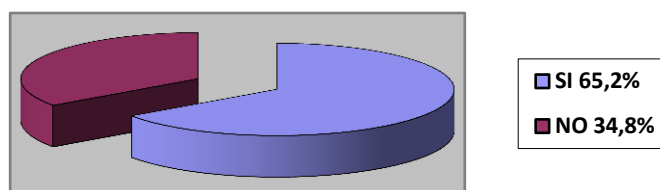
*Creé posible la manipulación de hardware de red a través de software*

RESPUESTA	FRECUENCIA	PORCENTAJE
SI	65	65.2%
NO	34	34.8%

**TOTAL** **99** **100%**

---

Nota fuente: Autores del proyecto de investigación



**Figura 6. Creé posible la manipulación de hardware de red a través de software?**

Nota fuente: Autores del proyecto de investigación

En su mayoría la comunidad de ingeniería de sistemas contestó si, los técnicos en telecomunicaciones fueron reacios a esta pregunta porque dentro de su pensum no ven programación.

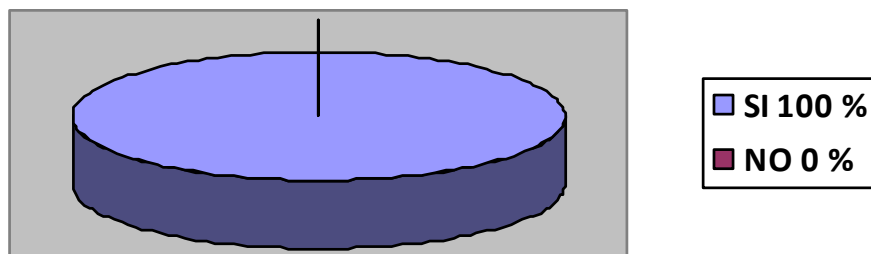
**Tabla 4.**

*Conoce alguna herramienta o software capaz de emular un entorno de redes*

<b>RESPUESTA</b>	<b>FRECUENCIA</b>	<b>PORCENTAJE</b>
SI	99	100%
NO	0	0%
<b>TOTAL</b>	<b>99</b>	<b>100%</b>

---

Nota fuente: Autores del proyecto de investigación



**Figura 7. Conoce alguna herramienta o software capaz de emular un entorno de redes?**

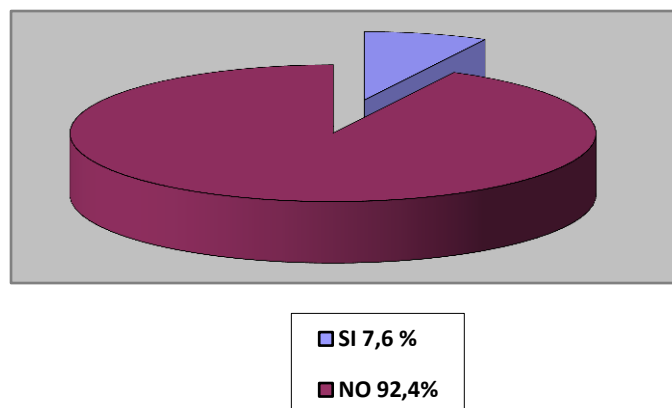
Nota fuente: Autores del proyecto de investigación

Todos coinciden en conocer algún software o herramienta, mencionaron el packet tracer de CISCO.

**Tabla 5. Durante su carrera ha escuchado el termino SDN “Redes Definidas por Software**

RESPUESTA	FRECUENCIA	PORCENTAJE
SI	9	7.6%
NO	90	92.4%
<b>TOTAL</b>	<b>99</b>	<b>100%</b>

Nota fuente: Autores del proyecto de investigación



**Figura 8. Durante su carrera ha escuchado el termino SDN “Redes Definidas por Software”**

Nota fuente: Autores del proyecto de investigación

La mayoría de los estudiantes de ingeniería de sistemas como los técnicos en telecomunicaciones aseguran no haber escuchado información relacionada con las redes definidas por software.

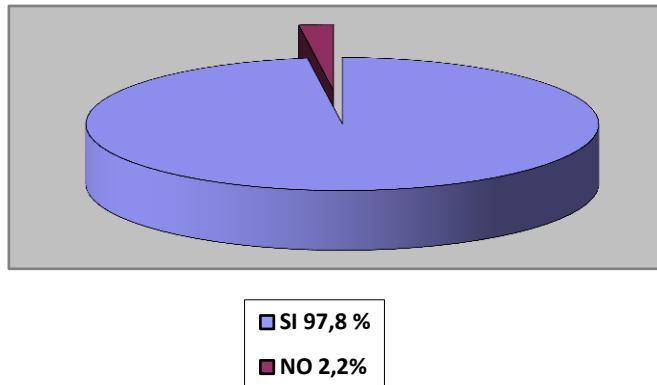
**Tabla 6.**

*Creé que adquirir conocimiento sobre tecnologías emergentes como redes definidas por software darán un valor agregado en su competencia profesional?*

RESPUESTA	FRECUENCIA	PORCENTAJE
SI	96	97.8%
NO	3	2.2%
<b>TOTAL</b>	<b>99</b>	<b>100%</b>

Nota fuente: Autores del proyecto de investigación





**Figura 9. Creé que adquirir conocimiento sobre tecnologías emergentes como redes definidas por software darán un valor agregado en su competencia profesional?**

Nota fuente: Autores del proyecto de investigación

Es evidente que los estudiantes quieren adquirir competencias relacionadas con tecnologías emergentes.

## Capítulo 4. Contexto de las redes definidas por software

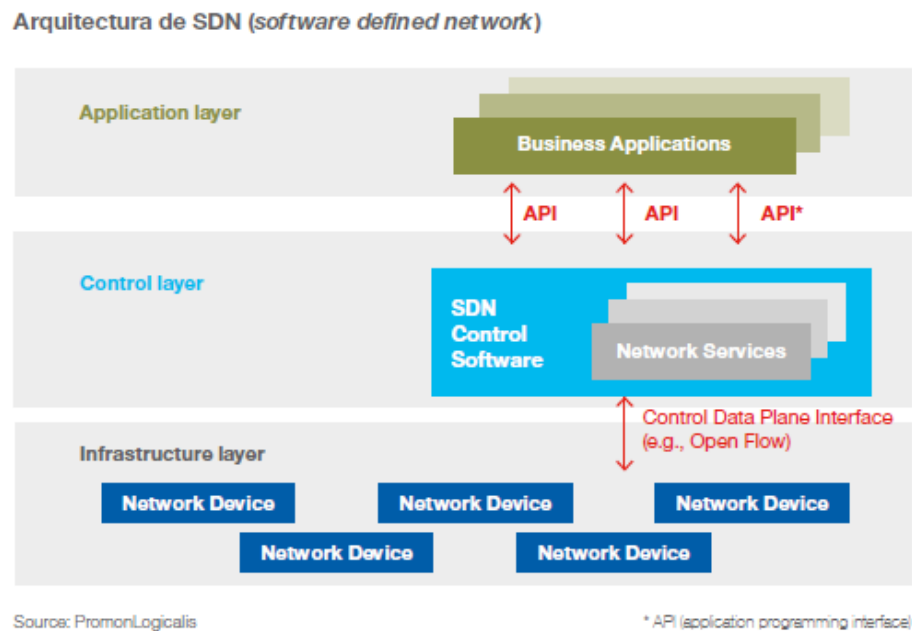
SDN es una arquitectura que prevé la separación entre los planes de control (la inteligencia de un elemento de red, por ejemplo: el software responsable por definir los procesos de enrutamiento, la política de seguridad, la ingeniería de tráfico) y el plan de datos (responsable de envío de los paquetes, o sea, Forwarding Information Base). Mientras en la arquitectura tradicional los controles están a nivel de los elementos de red – y, por lo tanto, basados en sistemas propietarios desarrollados por los fabricantes de equipos -, el nuevo concepto “retira la inteligencia” del hardware, separando los planes de control y de datos. Así, los elementos de red pasan a ser responsables solo de encaminar físicamente los paquetes, mientras que todo el control del enrutamiento se realiza por medio de software, en una capa superior. Como resultado, se logran redes menos complejas y al mismo tiempo más flexibles, cuyas políticas de tráfico pueden ser redefinidas rápidamente conforme surgen las demandas de negocios, en la capa de control, sin la necesidad de la configuración de cada switch y de cada router individualmente. Además, se torna posible la interacción de los aplicativos con los elementos de red, permitiendo que el comportamiento de la infraestructura sea definido con base en la aplicación, trayendo al mundo de Networking conceptos que la virtualización llevó, hace algunos años, a los Data Centers. Por lo tanto, fue creado el concepto de redes programables. A partir de esa arquitectura, los elementos de red (routers, switches, firewall, etc.) pasan a tener en su sistema operacional interfaces (APIs) que crearán la posibilidad que aplicaciones no desarrolladas por los fabricantes del hardware interactúen con el plan de control del sistema, tomando decisiones de ingeniería de tráfico basadas en patrones no usuales, tales como: temperatura, costo del link, consumo de energía, entre otros.

A continuación se explicaran algunos conceptos de SDN [14].

- ✓ Arquitectura
- ✓ Virtualización
- ✓ Beneficios
- ✓ Campos de aplicación

#### 4.1 Arquitectura SDN

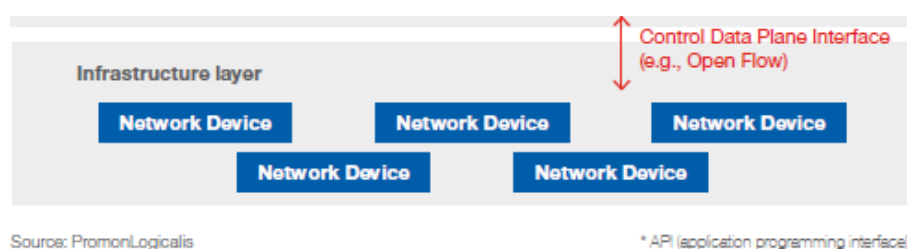
La arquitectura (o la arquitectura SDN) define como un sistema de redes y la computación puede ser construido utilizando una combinación de tecnologías abiertas y basadas en software y hardware de red de los productos básicos que separan el plano de control y la capa de datos de la pila de red, la arquitectura SDN se divide en tres capas: [15]



**Figura 10. Arquitectura SDN**

Nota fuente. <https://www.sdxcentral.com/resources/sdn/inside-sdn-architecture/>

**4.1.1 Capa de infraestructura.** Es la capa más baja de SDN donde se encuentran los dispositivos físicos o virtuales como (switch, routers) los cuales están conectados a través de una interfaz abierta que permite el switcheo y envío de paquetes en una conexión de red. Estas conexiones se hacen a través de medios de transmisión diferentes, incluyendo, cobre, redes inalámbricas, y fibra óptica. Si bien las preocupaciones básicas están asociadas a esta capa ya que dependen de estos dispositivos para el correcto funcionamiento de las SDN.



**Figura 11. Capa de Infraestructura**

Nota fuente. <https://www.sdxcentral.com/resources/sdn/inside-sdn-architecture/>

**4.1.2 Capa de control.** La función de control software está centralizada y permite a los desarrolladores de aplicaciones utilizar capacidades de la red, pero abstrayéndolos de su topología o funciones. El controlador SDN es una entidad software que tiene control exclusivo sobre un conjunto abstracto de recursos de plano de control, es decir, es la entidad que controla y configura los nodos de red para dirigir correctamente los flujos de tráfico. El controlador SDN elimina la inteligencia de conmutación y encaminamiento de datos de los nodos que realizan dicha función, pasando al controlador SDN, que toma esas decisiones y selecciona el mejor camino para el tráfico. La arquitectura describe una serie de funciones internas al controlador SDN y al elemento de red, pero sólo se especifica el comportamiento

de aquellos aspectos que son necesarios para asegurar la interoperabilidad. La arquitectura es agnóstica a los protocolos utilizados entre interfaces. La arquitectura permite que un controlador SDN gestione un amplio rango de recursos de plano de datos, lo cual ofrece el potencial de unificar y simplificar su configuración.



**Figura 12. Capa de Control**

Nota fuente. <https://www.sdxcentral.com/resources/sdn/inside-sdn-architecture/>

**4.1.3 Capa de aplicación.** Consiste en las aplicaciones de negocio de los usuarios finales, que utilizan servicios de comunicación de SDN a través de las API hacia arriba (northbound) de la capa de control, tales como REST, JSON, XML, etc., permite a los servicios y aplicaciones simplificar y automatizar las tareas de configuración, provisión y gestionar nuevos servicios en la red, ofreciendo a los operadores nuevas vías de ingresos, diferenciación e innovación.



**Figura 13. Capa de Aplicación**

Nota fuente. <https://www.sdxcentral.com/resources/sdn/inside-sdn-architecture/>

## 4.2 Virtualización

La virtualización es una técnica que pretende simular hardware y elementos de red mediante software. No es un concepto que provenga específicamente del mundo del networking sino que, de hecho, surgió más bien en el mundo de las Tecnologías de la información, de los grandes servidores de aplicaciones y los data centers. La virtualización abstrae las máquinas reales, el hardware real, en lo que se denomina la máquina virtual, esto es, una máquina ficticia implementada en software pero a la que se asigna memoria, espacio en disco, etc, como si de una máquina real se tratase. De esta forma las aplicaciones ven, por decirlo de alguna manera, una máquina adaptada a sus necesidades pero del alguna forma independiente del hardware real que la soporta. Para crear y gestionar esas máquinas virtuales se emplea un software que se denomina hypervisor.

Aunque, ya en el campo del networking SDN y virtualización son conceptos diferentes, lo cierto es que en realidad aparecen muy unidos. Y lo hacen en el sentido de que las funciones de control centralizadas se suelen implementar como switches virtuales (es decir, la simulación de un switch en software) ejecutándose en máquinas virtuales alojadas sobre unos servidores físicos y gestionadas mediante un hypervisor.

Un concepto relacionado con la virtualización y el SDN es el de virtualización de funciones de red (Network Functions Virtualization, NFV). Lo que significa este concepto es la centralización de funciones de red en servidores de propósito general virtualizados. Así, por ejemplo, se pueden centralizar funciones en el campo de la seguridad AAA (Authentication, Authorization and Accounting).

Mientras que es posible construir redes virtualizadas hoy en día utilizando una serie de técnicas diferentes, las redes definidas por software (SDN) hacen objeto de muchas discusiones, volviéndose rápidamente en el método preferido de la empresa actual. Las SDN ofrecen la separación necesaria que permite operar el plano de control de forma completamente independiente del plano de envío. Establece un marco para crear una red virtualizada que aparece en los servicios de capa superior, como los sistemas operativos y las aplicaciones, como si fuera una red física ordinaria. Esto permite proporcionar servicios y aplicaciones sin necesitar ser configurado para un entorno diferente.

En una red virtual basada en SDN, se pueden asignar los recursos de red según se necesite, al igual que la capacidad de procesamiento y el almacenamiento son provisionados de forma dinámica con un servidor virtualizado. Y al cambiar el enfoque de protocolos abiertos a interfaces de programación de aplicaciones (APIs), las redes virtuales basadas en SDN permiten nuevos grados de flexibilidad programable solo limitados por la visión del desarrollador.

Construir una red virtual sin utilizar SDN es ciertamente posible, pero probablemente no es tan útil. La virtualización mapea múltiples redes lógicas en una tela física común. Sin embargo, la administración del estado sofisticado se convierte en un problema técnico lleno de desafíos cuando las redes lógicas podrían estar ubicadas en cualquier parte. Ahí es donde la utilidad de SDN entra en juego. Resulta que las SDN son muy buenas a la hora de manejar grandes números de estados. Al mismo tiempo, pueden proporcionar un grado razonable de consistencia operativa, porque las SDN están diseñadas para permitir cambios en el plano de

envío. Sin las capacidades de gestión del estado que permiten las SDN, la utilidad operativa de la virtualización de red disminuye considerablemente (Rec2).

Con las SDN como mejor base para la virtualización de red, se pueden construir centros de datos enteros solamente con software y, por supuesto, el centro de datos definido por software (SDDC) es el próximo paso lógico. Cada vez más, el propio despliegue de aplicaciones requiere una infraestructura finamente ajustada para soportarlo. Este ajuste se está volviendo cada vez más específico según la aplicación, incluyendo políticas de QoS dirigidas, atribuciones de recursos a tiempo (para cumplir con picos de demanda), conocimiento de transacciones (para propósitos de contabilidad de coste), y caminos de red diferenciados. El equipo de red monolítico no puede adaptarse a estos requisitos específicos de la aplicación. Los SDDCs eliminan las grandes cajas de infraestructura y las sustituyen con servicios de red basados en software separados del hardware subyacente y dedicado así como ajustado a las necesidades de cada aplicación individual.

En un mundo en que los presupuestos de TI a menudo se reducen y en que cambia la tecnología frecuentemente, es imprescindible que las empresas reduzcan los costes operativos, mientras mejoran la flexibilidad y la agilidad. Por lo tanto, merece la pena tomar en consideración la virtualización en el centro de datos. Las redes virtuales basadas en SDN pueden proporcionar a las empresas las herramientas que necesitan para entregar las aplicaciones de forma efectiva mientras simplifican también la infraestructura física subyacente. Muchas empresas ya están realizando grandes beneficios de la continua



proliferación de la virtualización en el centro de datos y serán dichas organizaciones las que se pondrán en cabeza a medida que vayamos yendo hacia un entorno definido por software.

### 4.3 Beneficios del SDN

**4.3.1 Reducción de la complejidad.** Uno de los principales problemas de la arquitectura de redes tradicional es la complejidad, generada principalmente por la necesidad de “apilamiento” de protocolos creados para atender a diversas demandas.

Así, para cada alteración en la infraestructura son necesarias configuraciones en diversos niveles, en cada elemento. Con Software Defined Networking no hay necesidad de usar protocolos, ya que los controles no son hechos en el nivel de los equipos. Además, el SDN hace posible el desarrollo de herramientas que automatizan muchas actividades de gestión de la red que hoy es realizada manualmente. De esta manera, la complejidad de la red es reducida significativamente, posibilitando la reducción de la mano de obra, al mismo tiempo que disminuye la inestabilidad (causada por errores de configuración) y permite modelos de suministro mucho más ágiles.

**4.3.2 Reducción de costos.** Con una infraestructura más simple no resulta difícil prever la ecuación que lleva a la reducción de los gastos con mano de obra especializada:

Además de ser necesario un menor número de profesionales, el nivel de especialización también es reducido con la independencia en relación a los grandes proveedores. El costo total de propiedad (TCO) y los costos operacionales de la infraestructura también son reducidos,

proporcionando más economía a los administradores. En los *Data Centers*, esa reducción se refleja directamente en los costos de interface, permitiendo la adopción de velocidades mayores en el acceso, como 40G *ethernet*. Este tipo de velocidades permiten la reducción en la cantidad de interfaces, lo que resulta en una reducción de costos de cableado y OPEX.

**4.3.3 Control centralizado y más granular.** Al mismo tiempo en que, por un lado, la arquitectura de las redes definidas por *software* garantiza el control centralizado de la infraestructura (permitiendo gerenciar múltiples devices, de diferentes proveedores, a partir de un punto central), SDN también posibilita la aplicación de políticas en un nivel extremadamente granular. La combinación de estas dos características garantiza la agilidad y la flexibilidad de las redes basadas en la nueva arquitectura.

**4.3.4 Disponibilidad, confiabilidad y seguridad.** Gracias a su capacidad de definición de políticas y reglas específicas, en un nivel bastante granular, las arquitecturas SDN pueden garantizar mayor disponibilidad, confiabilidad y seguridad del ambiente, ya que se elimina la necesidad de configuración manual e individual a cada adición o cambio de elementos de red, reduciendo el riesgo de fallas y consecuentes indisponibilidades.

**4.3.5 Agilidad en el desarrollo de aplicaciones.** Una de las características más aclamadas por sus defensores es la rápida respuesta de las redes basadas en *software* a las demandas de negocios. Con una configuración más simple y control centralizado, los administradores de red consiguen adecuar la infraestructura conforme la necesidad del usuario final. La virtualización del ambiente de red permite aún la definición de políticas de tráfico –

escalables y flexibles – basadas en la aplicación. La idea principal es permitir que alteraciones en las aplicaciones o nuevos *deployments* se reflejen directamente en la capa de red (logicalis).

#### 4.4 Usos de SDN

Las redes SDN tienen aplicaciones en una gran variedad de entornos de red. Separando los planos de control y de datos, las redes programables permiten un control personalizado y una oportunidad para de eliminar middleboxes y con ello simplificar el desarrollo y la implementación de nuevos servicios y protocolos. A continuación, se examinarán diferentes entornos para los que han sido propuestas o aplicadas soluciones SDN [18].

**4.4.1 Cloud Computing.** Diferente del mundo cliente-servidor, en que la comunicación es bidireccional entre dos puntos, en el mundo Cloud las aplicaciones necesitan acceder a múltiples bancos de datos y servidores, generando tráfico en múltiples sentidos y ampliando la complejidad del ambiente. Entregar servicios de TI con agilidad y en el modelo “Self-Service” prepago por Cloud Computing exige que el procesamiento, almacenamiento y capacidad de red sean escalables.

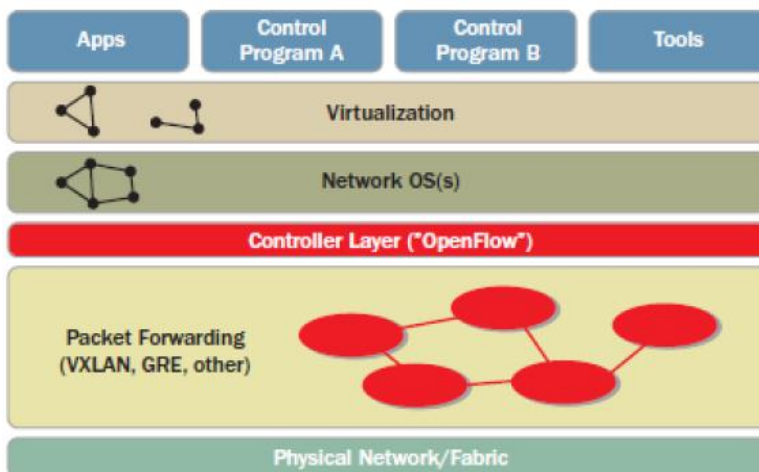
**4.4.2 Movilidad.** No resulta una novedad que los usuarios corporativos están demandando más movilidad, exigiendo la posibilidad de acceder a sistemas e informaciones en cualquier momento, en cualquier lugar y usando cualquier dispositivo, incluido su teléfono personal. Este cambio de comportamiento de los usuarios está alterando también los patrones de tráfico en las redes y en los Data Centers.

**4.4.3 Big Data.** El gerenciamiento, almacenamiento y acceso a los datos corporativos viene cambiando significativamente en los últimos años. Al mismo tiempo en que el volumen de informaciones no-estructuradas aumentó exponencialmente, las arquitecturas de los Data Warehouses está cambiando, adaptándose a las nuevas necesidades y a las nuevas tecnologías propuestas por los proveedores. Esos cambios también demandan alteraciones en la arquitectura de las redes y en el standard de enrutamiento de los datos.

**4.4.4 Internet of Things.** Las llamadas “Redes de sensores” y/o “Redes de comunicación entre máquinas (M2M)”, que darán origen a Internet de las Cosas (IoT, en la sigla en inglés), exigen que la latencia de las redes sea la menor posible, la disponibilidad debe ser cercana a 100% y que los sistemas de seguridad no interfieran en las operaciones normal. En ese contexto, características como disponibilidad, confiabilidad, flexibilidad y seguridad son fundamentales.

## **4.5 Arquitectura sdn de multinacionales**

**4.5.1 Brocade.** Brocade es una compañía estadounidense especializada en gestión de datos y productos de almacenamiento en red. Posee una división especializada en virtualización de redes y equipos de networking basado en software. Fue un miembro inicial cuando la ONF fue fundada. En 2010 fue uno de los primeros fabricantes en aprobar openFlow, y como miembro de la ONF participa en su desarrollo y su estandarización. [19]. A través de la familia Brocade VCS Fabric Technology proporciona equipos de red compatibles tanto con soluciones propietarias tipo VMware NSX como con controladores basados en OpenFlow.



**Figura 14.- OpenFlow-based SDN stack**

Nota fuente. <https://developer.cisco.com/media/XNCJavaDocs/overview-summary.html> [última visita 2016].

Inicialmente, Brocade implementó OpenFlow en equipos destinados a grandes carriers como la serie MLX de routers y los switches/routers Netron CES/CER 2000. La capacidad de estos equipos es hasta 100Gbps y son capaces de manejar 128k flujos.

Una innovación que ha incorporado Brocade es su modo híbrido de gestión de los puertos. En este modo un puerto puede implementar routing y/o switching tradicional y OpenFlow al mismo tiempo [19]. De esta manera se pueden implementar redes SDN simultáneamente con redes tradicionales sin necesidad de que haya una separación de puertos.

Brocade es uno de los fabricantes más comprometidos con SDN y otro de los conceptos ligados con él, NFV (Networks Function Virtualization). No ha desarrollado una arquitectura propietaria, sino que ha adoptado los estándares openFlow y openStack en sus equipos, y ha

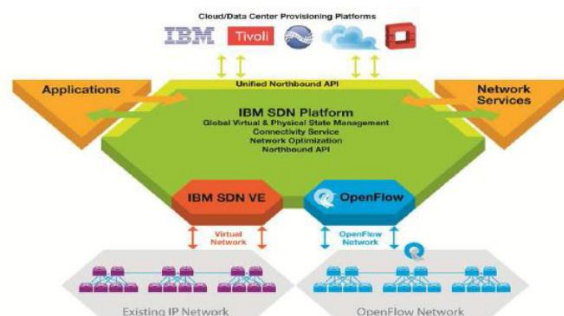
desarrollado componentes virtuales a fin de implementar overlays sobre infraestructuras existentes. [19]. Estos componentes son por ejemplo la familia Brocade Vyatta vRouter 5X00. [20]. De todas maneras, es muy posible que esta ausencia de una solución integral y propietaria, más allá de la implementación de openFlow en determinados equipos, tenga los días contados, ya que está formando un equipo especializado en SDN y NFV. Su última contratación ha sido la del creador de la arquitectura de Cisco OnePK, Kevin Woods.

#### **4.5.2 IBM.** IBM es una de los fabricantes líderes de equipamiento de red.

Tradicionalmente ha estado ligada a los estándares abiertos y proyectos Open Source. Como miembro fundador de ONF y de OpenDaylight, ha incorporado a su propuesta el modelo SDN open-source, con las particularidades que veremos. En general, hay dos aproximaciones a SDN [21]:

- ✓ **Virtual Network Overlays:** pensado para clientes que no desean hacer una gran inversión en nuevos routers y switches. En estas implementaciones, se diseña una red virtual sobre una infraestructura ya existente. El desacoplamiento de la red virtual y la red física se consigue mediante un elemento llamado hypervisor. Diferentes nodos en el Overlay se conectan mediante enlaces virtuales, que pueden atravesar varios enlaces físicos. De esta manera, nuevos servicios, nodos, enlaces, rutas, pertenecientes a diferentes usuarios pueden ser implementados vía software y ser separados, a pesar de compartir una infraestructura común.
- ✓ **Redes OpenFlow:** pensadas para clientes que implementan nuevas redes e infraestructuras. Esto permite seguir el modelo open-source SDN basado en OpenFlow, independizarse de los diferentes planos de control de los fabricantes y conseguir todas las ventajas ya mencionadas de SDN.

IBM ha incorporado ambas soluciones a su gama de productos, como se puede ver en la siguiente figura:



**Figura 15. Solución propuesta por IBM**

Nota fuente. <http://www.projectfloodlight.org/> [última visita 2015]

En la figura 15 se pueden identificar las diferentes capas de SDN: en el centro el controlador de SDN, que se comunica con las aplicaciones (y servicios de red), mediante las Unified Northbound APIs. Como Southbound APIs se pueden observar OpenFlow y IBM SDN VE, dependiendo de qué tipo de red se esté implementando (una Virtual Overlay, para redes ya existentes o una red OpenFlow).

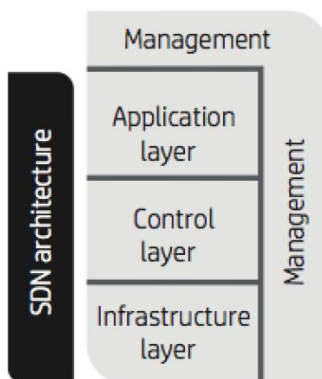
Respecto la solución OpenFlow, IBM ofrece una completa gama de productos:

- ✓ Switches que incorporan OpenFlow (G8052, G8264, G8264T, G8316, EN4093/R): soportan tanto el controlador propio de IBM (IBM Programmable Network Controller) como otros controladores OpenFlow (NEC pFlow, Floodlight, BigSwitch, y otros).

- ✓ IBM Programmable Network Controller (PNC). Controlador de red capaz de definir las políticas de flujos en cualquier entorno OpenFlow.

**4.5.3 Hewlett-Packard.** Hewlett-Packard (HP) es otro de los grandes fabricantes de dispositivos presentes en el mercado. Pero a diferencia de Cisco, ésta no es su actividad básica. Está presente en el mercado de ordenadores personales, soluciones empresariales, consultoría, impresión, grandes servidores, etc. Respecto a las redes, en sus propias palabras, son el único proveedor de ISPs tier-1 que ha sido capaz de presentar una solución integral y basada en lo que hasta ahora más se parece a un standard: OpenFlow. [22]

- ✓ **HP Virtual Application Network.** La estrategia de HP es la llamada HP Virtual Application Network. Como miembro de la Open Networking Foundation sigue una arquitectura semejante a la definida por ésta:



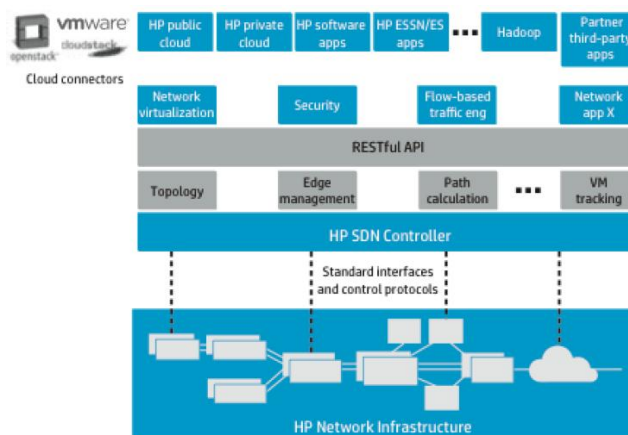
**Figura 16. Entorno HP Virtual Application Networks**

Nota fuente. Solutions for HP Virtual Application Networks - HP Corp.

Su estrategia va dirigida a hacer girar la red en torno a las aplicaciones, de forma que esta plataforma HP Virtual Application Networks Manager se integra en forma de plugin en



su HP Intelligent Management Center, su centro de comandamiento centralizado de redes. Han desarrollado un controlador (HP Virtual Application Networks SDN Controller[23]), del que se puede disponer en forma de software o de dispositivo. Este controlador, como se ve en la figura, se podría decir que reproduce fielmente la arquitectura SDN:



**Figura 17. Arquitectura HP SDN**

Nota fuente. <http://docplayer.es/8278556-Software-defined-networking.html>

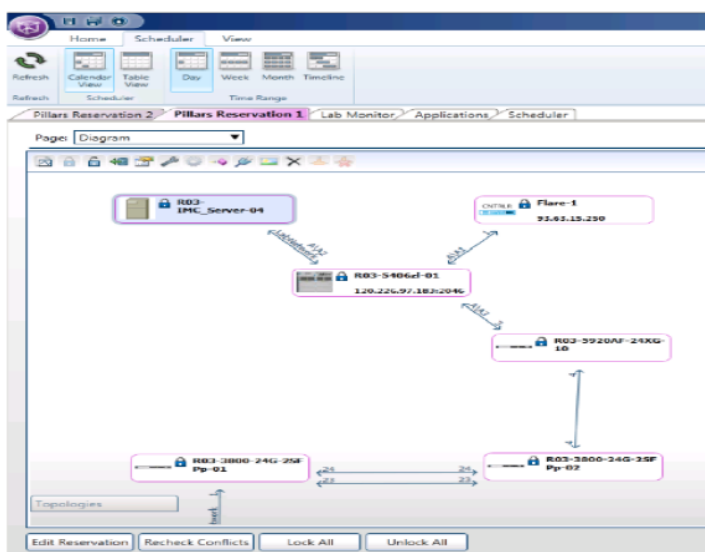
**HP Virtual Application Networks SDN Applications.** HP ha desarrollado aplicaciones para ser integradas en su arquitectura, como por ejemplo:

Virtual Cloud Network, un gestor de overlays sobre redes.

Sentinel Security, una aplicación de seguridad.

Con el foco puesto en las aplicaciones, y de la misma manera que Apple desarrolló su App Store y Google su Google Play, HP ha desarrollado una tienda de aplicaciones SDN donde el cliente pueda navegar, buscar e instalar directamente en el controlador diferentes aplicaciones desarrolladas por terceros o por la propia HP. [24]

De la misma manera, HP ha desarrollado el llamado HP SDN Developer KIT (SDK). Se trata de una herramienta abierta para crear, probar validar aplicaciones ideadas para SDN y para ser instaladas en su controlador, por supuesto. El SDK proporciona APIs y documentación, guías de programación, Graphical User Interface (GUI), ejemplos de código y aplicaciones y un entorno de simulación. De esta forma, HP quiere tomar una posición de dominio en el incipiente mercado SDN y posicionar su dispositivo en base a un entorno abierto de creación y suministro de aplicaciones.



**Figura 18. Simulation Suite de HP**

**4.5.4 VMware.** VMware es una filial de la empresa EMC. Su principal producto es un software de virtualización de ordenadores compatibles x86.

Un sistema de virtualización por software es un programa que toma un sistema físico existente, con unos determinados recursos (memoria RAM, almacenamiento, microprocesadores, etc.) como un pool y lo divide entre una serie de máquinas virtuales (VM).

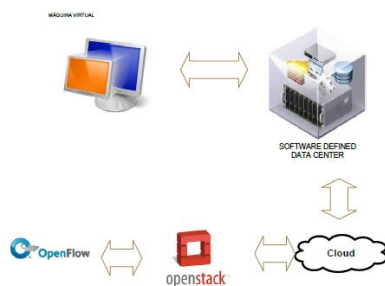
En otras palabras, permite implementar múltiples máquinas virtuales que trabajan dividiéndose entre ellas los recursos disponibles en el sistema físico anfitrión. Evidentemente, la velocidad de ejecución de una VM será menor que si tuviera asignados recursos físicos en exclusiva, pero será suficiente para mantener la funcionalidad del servicio que presta.

El concepto de virtualización ha sido una revolución en el mundo de la informática:

Permite desligar el espacio disponible del número de servidores. En un solo “hierro” es posible disponer de decenas de servidores. Produce un evidente ahorro en hardware, consumo de energía, etc. Entronca directamente con el concepto de software defined data center (SDDC) y cloud computing.

La virtualización de servidores es exactamente el mismo concepto que virtualización de redes: definir redes virtuales sobre un pool de capacidad de transmisión disponible físicamente. De hecho existe otra rama de investigación llamada NFV (Network Function Virtualization) que estudia diferentes soluciones a esta cuestión. Si estas redes virtuales se definen por software en base a requerimientos de las aplicaciones, ya tenemos lo que queríamos: SDN.

Así se relacionan varias de las nuevas disciplinas de la computación:

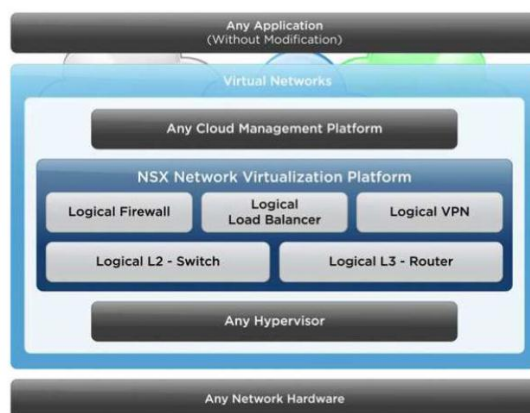


**Figura 19. Virtual Machine-Software defined Data Center-Cloud Computing-Network Function Virtualization-Software Defined Networking.**

Nota fuente. <http://docplayer.es/8278556-Software-defined-networking.html>

Siendo VMware el líder en virtualización es lógico que esté interesado en SDN. Por esto, en julio de 2012 compró la empresa fundada por los creadores de OpenFlow, NICIRA, por la cifra de 1260 millones de dólares. [25]

**NSX.** Justo un año después de la adquisición de Nicira, VMware presenta su plataforma para la virtualización de redes, llamada NSX. En palabras de Brad Hedlund, ingeniero arquitecto de VMware, el propósito de NSX es “ser capaz de desplegar una red virtual para una aplicación con la misma velocidad y eficiencia que se implementa una máquina virtual.” [26], La arquitectura desarrollada de NSX es la siguiente:



**Figura 20. Arquitectura NSX.**

Nota fuente. S Skiena. Dijkstra's algorithm. Implementing Discrete Mathematics: Combinatorics and Graph Theory with Mathematica, Reading, MA: Addison-Wesley, pages 225–227, 1990.

**4.5.5 Red de CPDs de Google.** Uno de los casos más paradigmáticos de implantación de SDN es el caso de Google. Esta empresa se encuentra entre los más grandes proveedores de contenido (entendiéndose por contenido búsquedas, cloud computing, video, datos de usuario,

aplicaciones empresariales, etc...) que existen. Sus servicios se proporcionan a través de unos Centros de Proceso de Datos diseminados por los cinco continentes, de forma que proporcionan redundancia y alta disponibilidad.

La arquitectura de la red de Google es la siguiente:

- ✓ Una WAN que interactúa con múltiples dominios de Internet. Esta es la red que intercambia tráfico con los usuarios. Éstos envían sus consultas, búsquedas, y acceden a sus datos guardados en la nube, a Google, y éste gestiona estas peticiones a los CPDs, que las atienden. Esta red tiene unos requerimientos muy especiales: debe poder interpretar múltiples protocolos, al interactuar con miles de usuarios; debe poseer una topología especialmente densa, para poder soportar miles de conexiones simultáneamente; finalmente, debe estar dotada de una muy alta disponibilidad.
  
- ✓ Una WAN interna (B4) que interconecta los CPDs de la empresa. Esta red soporta diferentes tipos de tráfico: volcados de datos asíncronos, búsquedas por índices para los servicios interactivos y finalmente copias de seguridad de los datos de usuario para conservación/alta disponibilidad. Se calcula que aproximadamente el 90% del tráfico interno de Google circula por esta red.

Esta red interna tiene la siguiente estructura: una docena de CPDs diseminados por el mundo e interconectados entre sí de forma redundante.



**Figura 21. Red Interna**

Nota fuente. Jordan R. Energy efficient ethernet: Technology, application and why you should care. Technical report, Intel Corporation, 2011

Esta red posee unas características especialmente indicadas para el despliegue del paradigma SDN. Por ejemplo, todas las aplicaciones, servidores y redes locales están controladas por Google totalmente, hasta el borde de la red. Las aplicaciones realizan copias de ingentes volúmenes de datos de un CPD a otro, y se pueden beneficiar más de un alto nivel de ancho de banda medio. Además, su tasa de transmisión puede ser modulada en base a la capacidad disponible. Y finalmente, los sitios que han de interconectarse son limitados, por lo que se pueden gestionar fácilmente tablas de flujos no muy grandes.

Las motivaciones de Google para implementar SDN fueron que el rápido crecimiento del ancho de banda de Internet, a pesar del crecimiento que se imprimió a la red B4 (incluso más rápido), llevaron a la empresa a pensar que no podrían mantenerse sus niveles de escalabilidad, tolerancia a fallos, control y costes con tecnologías de WAN tradicionales. Por ejemplo, en cuanto a costes, las aproximaciones tradicionales llevan a aprovisionar un ancho de banda al 30-40% ( 2 o 3 veces más costosa que un enlace utilizado al 100%) para prevenir fallos y pérdida de paquetes, lo que unido a las tasas de crecimiento de tráfico previstas hacían las proyecciones de costes insostenibles.

Sin entrar en detalles de la implementación, ya proporcionados en [27], se puede decir que Google implementó nuevos protocolos usando principios de SDN y el protocolo openFlow. Otro de sus objetivos fue simultanear la utilización de tecnologías tradicionales y una aplicación de Traffic Engineering centralizada.

Esta aplicación permitía a Google gestionar las peticiones de ancho de banda más eficientemente en períodos de alta utilización, así como reposicionar dinámicamente el ancho de banda en función de la demanda de las distintas aplicaciones. Estas características permitieron que la red B4 de Google funcione con una ratio de utilización cercana al 100% y de media un 70% en largos períodos de tiempo, ratio que se corresponde con un incremento de la eficiencia de dos a tres veces, comparándola con las tecnologías de gestión estándares.

En la actualidad, la red SDN de Google sirve más tráfico que su red "pública", y tiene una ratio de crecimiento mayor. Sin embargo, también han experimentado inconvenientes. Uno de ellos es que se han experimentado "bottlenecks" o cuellos de botella, especialmente al enviar paquetes del plano de control al plano de datos. Estos cuellos de botella tienen que ver con el rendimiento o capacidad del controlador, tema al que nos referiremos más adelante.

Del caso de Google se pueden extrapolar ideas a un gran número de implementaciones de SDN en la vida real. A pesar de las particularidades de su red interna hay una serie de prácticas a considerar. Una de ellas es la aproximación híbrida, que consiste en que la red soporte los protocolos tradicionales a la vez que openFlow, de forma que la transición no es traumática y elimina suspicacias a la hora de adoptar SDN. Definitivamente, y por la

magnitud y relevancia de la compañía, éste es un caso paradigmático en la implementación de SDN, un "acelerador" de esta tecnología y un ejemplo a seguir por otras muchas compañías.

#### ***4.5.6 COMPARATIVA ENTRE CONTROLADOR DE CÓDIGO ABIERTO Y COMERCIAL.***

El laboratorio de redes y telecomunicaciones de la universidad francisco de paula Santander Ocaña, busca la implementación de alguna arquitectura SDN a través de un controlador bien sea comercial o no comercial.

#### **Controladores comerciales**

- **Infraestructura de Políticas de Aplicaciones (APIC) de Cisco.** Es un cluster de controladores, centraliza las funciones en una API, con un repositorio de datos globales y repositorio de datos de políticas.
- **El controlador SDN Virtual Application Networks (VAN) de HP.** Se ejecuta en switches habilitados para OpenFlow con el centro de datos; permitiendo un control centralizado y automatización, para la integración de la red y el sistema de negocios. Puede establecerse clusters del controlador para respaldar las funciones si en algún momento alguno falla.
- **El controlador ProgrammableFlow PF6800 de NEC.** Proporciona un punto de control para las redes físicas y de gestión para las redes virtuales y físicas.



- **El Controlador de Servicios Virtualizados (VSC) de Nuage Networks.** Establece un directorio de servicios con políticas basado en roles basados en las reglas de la red. Pueden añadirse inquilinos siendo detectados por el controlador cuando se conectan o se desconectan.
- **El controlador NSX de VMware.** Es un sistema de gestión distribuido que usa APIs northbound mientras mantiene información de las máquinas virtuales, hosts, switches lógicos y VXLANs se considera un sistema de gestión de estado distribuido que controla las redes virtuales y superpone los túneles de transporte.

Los cinco controladores comerciales mencionados son muy fuertes en el mercado actual, pero no todos ofrecen un descuento por academia, la UFPS Ocaña actualmente pertenece a la zona del nororiente CISCO Colombia, lo que permitiría hacer una alianza más para adquirir este tipo de controlador, nuestro laboratorio cuenta con una gran variedad de dispositivos CISCO lo que permitiría hacer una unificación más integrada y soporte eficaz.

### **Controladores de código abierto.**

- **Beacon** <sup>[34]</sup> Es un controlador programado en Java, presenta un interfaz de usuario y visualización de la red. Por sus características Open Source puede manipularse el código.

- **Pox.** Es un controlador multiplataforma desarrollado en lenguaje Python.
- **Floodlight.** Controlador desarrollado en Java con la capacidad de manejar paquetes y tablas de flujo.
- **Nox.** Es un controlador desarrollado en C++ para administrar el flujo de datos, con la capacidad de manejar grandes cantidades de flujos de datos.
- **Trema.** Es un controlador que tiene integrado un emulador de red *Openflow* que hace no necesario equipos de usuario final para aprobar las aplicaciones

La tabla número 22 muestra algunos parámetros que permiten realizar una comparativa de controladores de código abierto de acuerdo a sus características más relevantes.

Tabla 9.

#### Parámetros comparativos

Controlador	Parámetros comparativos				
	Desarrollo	Plataforma	Openflow	Virtualización	openStack
NOX	C++	Linux	Si	Mininet y open vSwitch	No
POX	Python	Linux, Mac OS, Windows	Si	Mininet y open vSwitch	No
BEACON	Java	Linux, Mac OS, Windows y Android para móviles	Si	Mininet y open vSwitch	No
FLOODLIGHT	Java	Linux, Mac OS, Windows	Si	Mininet y open vSwitch	Si
TREMA	Ruby/C	Linux	Si	Construcción de una herramienta virtual de simulación	Si

Nota fuente. Autores del proyecto.

De acuerdo a la tabla comparativa, existe un parámetro muy relevante y es la plataforma que soporta, en nuestro caso recomendaríamos cualquiera de POX, Beacon o Floodlight, el primero ofrece un desarrollo con un lenguaje de programación fácil de manejar, el segundo ofrece soporte para todas las plataformas e incluye Android, pero se necesita conocimientos elevado en java, y el tercero tiene una ventaja sobre los demás que es el de ofrecer un stak de código abierto.

## Capítulo 5. Requerimientos de la arquitectura del laboratorio

La Universidad Francisco de Paula Santander Ocaña actualmente cuenta con un laboratorio de Redes y Telecomunicaciones, este laboratorio tiene equipos con tecnología cisco, y cableado estructurado que incluye la Categoría 7a, en la siguiente figura se puede apreciar las instalaciones del laboratorio.



**Figura 22. Laboratorio de redes y telecomunicaciones UFPSO**

Nora fuente. Autores del proyecto

A continuación se relacionan los equipos CISCO empresariales que se encuentran en el laboratorio

**Tabla 8.**

*Relación de equipos CISCO y Servidores del Laboratorio*

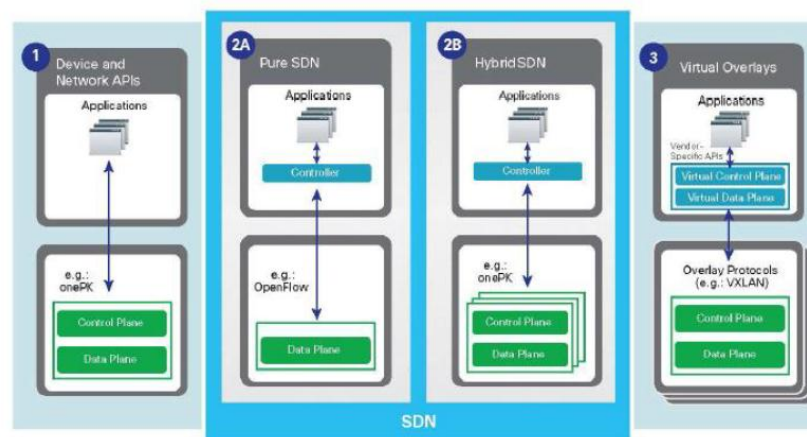
Equipo	Serie	Cantidad	Soporte Openflow
Router	1800	6	No
Router	1900	3	No
Switch	2950	3	No
Switch	2960	3	No

Servidor	No existe
----------	-----------

Nota fuente. Autores del proyecto.

De acuerdo a la tabla anterior los equipos actuales no soportan el objetivo general del proyecto. Se puede evidenciar que en el laboratorio de redes y telecomunicaciones los dispositivos más empleados son de tecnología cisco, por esta razón queremos definir una arquitectura que mantenga estos lineamientos pensando en futuras certificaciones, podemos decir que CISCO ostenta la posición dominante en el mercado de dispositivos. De acuerdo a informes de la consultora Synergy Group, cerca de un 70% de los equipos que se venden a empresas, son suyos [28]. En palabras de ejecutivos de la compañía, el advenimiento de SDN podría disminuir la cifra de negocio de 43000 a 22000 millones de dólares[28]. No es de extrañar que se haya llamado a SDN el “anti-cisco”, ya que en teoría , sería el principal damnificado de una revolución como propone SDN.

En nuestro esquema utilizaremos la infraestructura que ofrece CISCO, y a continuación la describiremos.

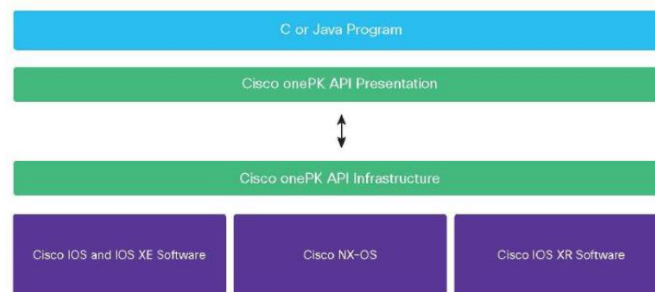


**Figura 23. Modelos de desarrollo para Open Networking**

Nota fuente. <https://maven.apache.org/> [última visita 2016].

**Open Network Environment (ONE).** Esta solución implementa la programabilidad de la red, uno de los objetivos de SDN.

La solución propuesta es el Open Network Environment. En sus propias palabras, es una “aproximación holística para aproximar la red a las aplicaciones.” [29] Se ofrece la ONE Platform Kit (onePK). Se trata de un kit de desarrollo específico para tecnología (de Cisco) que incorpora una arquitectura propia de Cisco, como se muestra en la siguiente figura:



**Figura 24. Cisco onePK Software Architecture**

Nota fuente. <https://maven.apache.org/> [última visita 2016].

Los elementos principales son los siguientes:

- ✓ Programas escritos en Java o C (otros lenguajes en el futuro).
- ✓ Una capa de presentación, o conjunto de APIs que enlazan las diferentes funciones y librerías de cada dispositivo y a través de cada sistema operativo de red.
- ✓ Un canal de comunicación entre la capa de presentación y una capa de infraestructura, que accede a los diferentes elementos de la red.
- ✓ La capa de infraestructura, que implementa el código específico de cada plataforma.
- ✓ Las implementaciones de las librerías Cisco onePK en las diferentes plataformas.

Esta arquitectura no especifica separación física entre plano de control y plano de datos. De hecho, los diferentes SO de red pertenecen a los dispositivos de Cisco. En palabras de la propia Cisco, ofrece la

aproximación más cercana a las redes programables, incluyendo los controladores SDN, APIs abiertas y redes virtuales a través de una gran variedad de modelos.

A fin de aprovechar las funcionalidades de esta arquitectura y mostrar cómo onePK proporciona mejores prestaciones y mayor flexibilidad que otras implementaciones de SDN, Cisco ha desarrollado el Cisco Unified Access Data Plane (UADP). Se trata de un ASIC que soporta las APIs onePK, y que ha sido incorporado en switches de la compañía (concretamente el Catalyst 3850 Unified Access). Este ASIC proporciona acceso a métricas de bajo nivel de la red, así como una disminución del time-to-market de aplicaciones onePK.

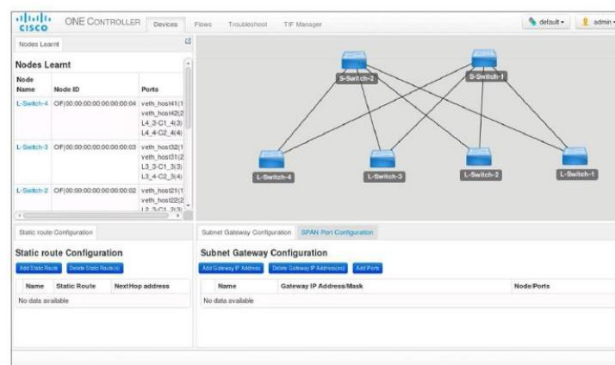
Como punto a favor de esta arquitectura, se puede mencionar que no es una arquitectura cerrada. Por ejemplo, nuevos protocolos, como OpenFlow, se pueden incorporar como agentes a onePK, permitiendo la transición a modelos estrictos de SDN.

**Cisco eXtensible Network Controller (XNC).** Está diseñado para soportar OpenFlow y funcionar con dispositivos de Cisco y de otros fabricantes. [29]

- ✓ Soporta OpenFlow y onePK.
- ✓ Posee funciones avanzadas tales como descubrimiento de topología de red (al estilo de Cisco Discovery Protocol), gestión de la red, acceso a métricas de análisis, programabilidad, etc.
- ✓ Interfaz gráfica de comunicación con las aplicaciones (o en su defecto, mediante Northbound APIs estándar)
- ✓ Características de seguridad (RBAC), políticas de AAA, y protocolos de control seguros. [29]

El controlador XNC puede coexistir con los tradicionales planos de control de los diferentes dispositivos, a fin de implementar un modelo de red híbrido (ya descrito por la ONF). De esta manera, los dispositivos podrían continuar ejecutando los protocolos (por ejemplo) OSPF o Spanning Tree, y ser complementado por las funcionalidades de OpenFlow.

La interfaz gráfica de comunicación con las aplicaciones (GUI) ha sido construida de tal manera que todo lo que se implemente mediante ella es accesible a otras aplicaciones externas. Su aspecto es el siguiente:



**Figura 25. Cisco XNC GUI**

Fuente. <https://maven.apache.org/> [última visita 2016].

Como fabricante de equipos, Cisco ha incorporado agentes OpenFlow a diferentes modelos de sus familias de switches Catalyst y Nexus, permitiendo de esta manera la utilización de sus chasis en diferentes modelos de SDN. Asimismo, soportan la incorporación de nuevos protocolos (como por ejemplo Interface to Routing Systems (IR2S), desarrollado por el IETF) permitiendo mayor flexibilidad a los desarrolladores de aplicaciones SDN.



**Application Centric Infrastructure (ACI).** Como ya se ha mencionado, Cisco obtiene sus beneficios de la venta de unos equipos que proporcionan unos enormes márgenes, por tanto, no renunciará a incorporar SDN al hardware.

A pesar de que SDN es eminentemente una solución software, la idea de Cisco es que no es suficiente con el software para implementarla de una forma eficiente. Para ello, y a través de una extraña maniobra consistente en la fundación y posterior compra de una startup llamada Insieme, desarrolla una familia de productos llamada Application Centric Infrastructure (ACI). ACI está compuesta de tres grandes ramas:

- ✓ Una nueva línea de switches de la familia Nexus 9000.
- ✓ Un controlador llamado APIC (Application Policy Infrastructure Controller).
- ✓ Un sistema operativo de red (NX-OS), residente en el switch.

Hay críticos que argumentan que el hardware implementa dos ASICs, uno fabricado por Broadcom y otro propio de Cisco. Si se utiliza el de Broadcom, se pueden usar otras soluciones de SDN basadas en estándares. Si se utiliza el de Cisco, se obtienen funcionalidades extra y una mejor funcionalidad de la red. También se argumenta que esta solución no es compatible con el antiguo equipamiento, por lo que se ha de renovar toda la red con dispositivos Cisco compatibles. [30]

Quisimos hacer una tabla donde se evidencian algunas herramientas de licencia libre donde se pueden crear entornos de redes definidas por software.

## **Tabla 9.**

### *Herramientas Openflow*

Software	Descripción
MiniNet	Máquina virtual para crear prototipos para redes definidas en software Se puede crear cualquier tipo de topología. MiniNet apoya la investigación, desarrollo, aprendizaje, desarrollo de prototipos, pruebas, depuración, y cualesquiera otras tareas que podrían beneficiarse de tener una red experimental completa en un ordenador portátil o cualquier otro PC.
OFTrace	Imprime los tiempos de procesamiento del, es decir, la diferencia de tiempo entre cuando un controlador recibe un mensaje.
Nagios	Es un sistema de monitorización de redes de código abierto ampliamente utilizado, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.

Nota fuente. [http://www.openflow.org/wk/index.php/Main\\_Page](http://www.openflow.org/wk/index.php/Main_Page)

### [5.1 Esquema de direccionamiento del protocolo de la pila TCP/IP\(IPv6\)](#)

IPv6 es la abreviatura de "Versión 6 del Protocolo de Internet". IPv6 es el protocolo de Internet de última generación que se ha diseñado para sustituir al protocolo de Internet actual: la Versión 4 del Protocolo de Internet.

Para poder comunicarse a través de Internet, los ordenadores y otros dispositivos deben tener direcciones de emisor y receptor. A estas direcciones numéricas se las conoce como direcciones del Protocolo de Internet. A medida que Internet y el número de personas que lo utilizan crecen exponencialmente, crece también la necesidad de contar con direcciones IP.

IPv6 es un estándar que ha desarrollado el Grupo de Trabajo de Ingeniería de Internet (IETF, por sus siglas en inglés), una organización que desarrolla tecnologías de Internet. El IETF, anticipándose a la necesidad de contar con un mayor número de direcciones IP, ha creado el protocolo IPv6 para dar cabida al creciente número de usuarios y dispositivos que acceden a Internet.

IPv6 permite que un mayor número de usuarios y dispositivos se comuniquen a través de Internet utilizando números de mayor tamaño para crear direcciones IP. En el protocolo IPv4, cada dirección IP se compone de 32 bits, lo que permite la existencia de 4300 millones de direcciones únicas.<sup>[31]</sup>

### ***protocolo TCP/IP (IPv6)***<sup>[32]</sup>

***Espacio mayor de direccionamiento.*** El IPv6 incrementa el tamaño de la dirección IP de 32 bits a 128 bits para así soportar más niveles en la jerarquía de direccionamiento y un número mucho mayor de nodos direccionables. El diseño del protocolo agrega múltiples beneficios en seguridad, manejo de calidad de servicio, una mayor capacidad de transmisión y mejora la facilidad de administración, entre otras cosas.

Mientras que IPv4 soporta 4,294,967,296 ( $2^{32}$ ) direcciones que es poco menos de 4.3 billones, IPv6 ofrece  $3.4 \times 10^{38}$  ( $2^{128}$ ) direcciones, un número similar a  $6.67126144781401e+23$  direcciones IP por cada metro cuadrado sobre la superficie de la Tierra. Adicionalmente, la dirección IPv6 se diseñó para ser subdividida en dominios de enrutamiento jerárquico que reflejan la topología del Internet actual.

### ***Características de IPv6***

- El esquema de direcciones de 128 bits provee una gran cantidad de direcciones IP, con la posibilidad de asignar direcciones únicas globales a nuevos dispositivos.
- Los múltiples niveles de jerarquía permiten juntar rutas, promoviendo un enrutamiento eficiente y escalable al Internet.
- El proceso de autoconfiguración permite que los nodos de la red IPv6 configuren sus propias direcciones IPv6, facilitando su uso.
- La transición entre proveedores de IPv6 es transparente para los usuarios finales con el mecanismo de reenumerado.
- La difusión ARP es reemplazada por el uso de multicast en el link local.
- El encabezado de IPv6 es más eficiente que el de IPv4: tiene menos campos y se elimina la suma de verificación del encabezado.
- Puede hacerse diferenciación de tráfico utilizando los campos del encabezado.
- Las nuevas extensiones de encabezado reemplazan el campo Opciones de IPv4 y proveen mayor flexibilidad.
- IPv6 fue esbozado para manejar mecanismos de movilidad y seguridad de manera más eficiente que el protocolo IPv4.
- Se crearon varios mecanismos junto con el protocolo para tener una transición sin problemas de las redes IPv4 a las IPv6.

***Modos de configuración de IPv6. Autoconfiguración.*** Definida en el RFC 2462 y también es conocida como *Configuración Automática de Dirección Sin Estado IPv6*. Esta funcionalidad permite que un ruteador IPv6 envíe, a través del enlace local, la información de red a las computadoras y que ellas puedan configurarse correctamente. La información enviada es el prefijo de IPv6 del enlace local y

la ruta por defecto del mismo protocolo. Mediante este mecanismo cada computadora y servidor de IPv6 añade su dirección de capa de enlace (dirección MAC) en el formato EUI-64 al prefijo de IPv6 de unicast global único anunciado en la subred.

*Configuración mediante servidor.* Las computadoras que utilizan IPv6 pueden obtener sus parámetros y direcciones de configuración de un servidor de DHCP versión 6. Este modo es llamado *Configuración de Direcciones con Estado IPv6*.

**Renumeración.** El proceso de reenumeración de IPv6 fue diseñado para ser transparente entre los proveedores de IPv6 unicast y los usuarios finales. Esto se logra con el mecanismo de autoconfiguración que permite una reenumeración sencilla a las computadoras con sólo enviarles el nuevo prefijo IPv6 unicast para la red. Una desventaja de este mecanismo es la pérdida de las sesiones TCP y UDP que ocurren entre las computadoras y los servidores al momento exacto de la transición. Esto es algo que también ocurre actualmente con IPv4.

**Multicasting.** La difusión del Protocolo de Resolución de Dirección (Address Resolution Protocol, ARP) de IPv4 afecta la eficiencia de la red. Esta situación no ha sido incluida en IPv6, y en su lugar se utiliza el Multicasting el cual funciona de la siguiente manera:

- Se crea un grupo Multicast, formado por conjunto de interfaces de red.
- Si se está interesado en que cierta computadora reciba los paquetes de difusión del grupo se agrega una interfaz de red, de esa forma se envía un paquete multicast al grupo X.
- Ese paquete sólo llegará a aquellas computadoras que tengan su interfaz incluida en el grupo multicast X. Con ello se permite tener niveles de eficiencia de red superiores a los presentados en IPv4, lo cual se verá traducido en la disminución de los ciclos de procesamiento de CPU de las

computadoras en la red local al no procesar paquetes de difusión que no van dirigidos a ellos y de la misma manera se estará eliminando el problema de las tormentas de paquetes de difusión de IPv4.

***Encabezado eficiente.*** El nuevo encabezado de IPv6 es más sencillo que el de IPv4. Del encabezado de IPv4 se removieron 6 campos: Longitud de encabezado, Identificación, Banderas, Desplazamiento por fragmentación, Suma de verificación de encabezado, Opciones y Relleno. Al pasar de un encabezado de IPv4 con longitud variable a IPv6 con menos campos y longitud fija se obtiene una reducción en los ciclos de CPU de los ruteadores al momento de enviar los paquetes de IPv6. Lo anterior conlleva un mejor desempeño de la red.

***Etiqueta de flujo.*** Dentro del encabezado de IPv6 existe un nuevo campo llamado *Etiqueta de Flujo*, éste es usado por el nodo fuente para solicitar un manejo especial de secuencias específicas de paquetes. La etiqueta está dirigida al procesamiento de la estación destino, no para los ruteadores, y es de gran utilidad para aplicaciones como videoconferencias y voz sobre protocolo de Internet (VoIP). Asimismo agrupa todas aquellas que requieren un tratamiento especial de Calidad de Servicio (Quality of Service, QoS) en los ruteadores de la trayectoria.

***Extensiones de encabezado.*** La utilización del campo *Opciones* en el encabezado de IPv4 presenta desventajas a la transmisión de los paquetes y a la eficiencia de la red. En lo que respecta a la variación del tamaño del encabezado es debido a que tiene campos opcionales. En el segundo caso todos los ruteadores que procesan el paquete deben computar el encabezado con su campo de longitud variable lo que introduce retardos y gasto de la capacidad del CPU en ciclos de procesamiento que son innecesarios.

Para resolver la situación anterior, IPv6 sustituye el campo *Opciones* al final del encabezado por las *Extensiones de Encabezado*, formando un encadenamiento de encabezados enlazados por un campo llamado *Siguiente Encabezado*. Se presenta un campo *Siguiente Encabezado* dentro de cada *Extensión de Encabezado* usado por IPv6. Este diseño con extensiones permite una mejor eficiencia en el procesamiento de los paquetes, ya que asegura que los ruteadores y nodos computan los encabezados dirigidos a ellos a lo largo de la trayectoria.

**Movilidad.** Debido a que la movilidad es una característica importante y deseable por las compañías proveedoras y los consumidores finales el *Protocolo de Internet Móvil (MobileIP)* esta capacidad está disponible tanto en IPv4 como en IPv6. Cabe destacar que en este último la movilidad se construyó dentro del protocolo en lugar de ser una nueva función agregada como en IPv4. Ello implica que cualquier nodo IPv6 puede usar un IP *Móvil* tanto como lo requiera. IPv6 *Móvil* utiliza dos Extensiones de Encabezado: un *Encabezado de Enrutamiento* para el registro y un *Encabezado de Destinopara* entrega del datagrama entre los nodos móviles y sus nodos fijos correspondientes.

**Seguridad.** El protocolo *IPSec* estandarizado por el Grupo Especial sobre Ingeniería de Internet provee las funciones de:

- Limitar el acceso a sólo aquellos autorizados.
- Certifica la autenticación de la persona que envía los datos.
- Encripta los datos transmitidos a través de la red.
- Asegura la integridad de los datos.
- Invalida la repetición de sesiones, para evitar que no sean repetidas por usuarios maliciosos.

Los protocolos que respaldan el funcionamiento de *IPSec* son: la *Autenticación de Encabezado* (*Authentication Header, AH*) y la *Carga de Seguridad Encapsulada* (*Encapsulated Security Payload, ESP*). Al estar incluidos en cada implementación de IPv6 se provee mayor seguridad ya que IPSec está presente en todos los nodos de la red.

***Mecanismos de Transición.*** Actualmente no existe una fecha definida para dejar de utilizar IPv4 o comenzar a utilizar IPv6 completamente, por lo que al diseñar IPv6 se optó por incluir mecanismos que permitan una coexistencia de ambos esquemas de direccionamiento y que en el largo plazo permitan tener una transición sin complicaciones hacia IPv6. Estos esquemas son los siguientes:

- Nodos de Doble Pila sobre redes IPv4.
- Islas de Nodos de Sólo IPv6 sobre redes IPv4.
- Nodos de IPv4 que puedan comunicarse con redes IPv6.
- Nodos de IPv6 que puedan comunicarse con redes IPv4.

***Estructura del Protocolo IPv6.*** Como se especifica en el RFC 2460 *Especificación del Protocolo de Internet Versión 6*, el encabezado básico de IPv6 consta de 8 campos, 4 menos que el de IPv4, lo que da un total de 40 octetos.

Entre las mejoras propuestas se encuentra el campo Etiqueta de Flujo y las Extensiones de Encabezado. A continuación se presentan todos los campos con su descripción:

- *Versión (4 bits)*. Se refiere a la versión de IP y contiene el valor de 6 en lugar de 4, el cual es contenido en un paquete IPv4.



- *Clase de Tráfico (8 bits)*. Este campo y sus funciones son similares al de Tipo de Servicio en IPv4. Este campo etiqueta el paquete IPv6 con un Punto de Código de Servicios Diferenciados (DSCP) que especifica cómo debe ser manejado.
- *Etiqueta de Flujo (20 bits)*. La etiqueta sirve para marcar un flujo o secuencia de paquetes IPv6 que requieran un tratamiento especial a lo largo de la trayectoria de comunicación.
- *Longitud de Carga Útil (16 bits)*. La carga útil es la parte que sigue al encabezado de IPv6.
- *Siguiente Encabezado (8 bits)*. Define el tipo de información que va a seguir al encabezado de IPv6 básico, la cual puede ser un protocolo de capa superior como TCP o UDP o puede ser alguna de las Extensiones de Encabezado. Este campo es similar al campo Número de Protocolo en IPv4.
- *Límite de Saltos (8 bits)*. Define el número máximo de saltos (ruteadores intermedios) que un paquete IP puede atravesar. Cada salto disminuye el valor por 1, al igual que en IPv4 cuando el campo contiene el valor 0 el paquete es destruido y se envía de regreso al nodo fuente un mensaje ICMP versión 6 de Tipo 3 que significa Tiempo Excedido.
- *Dirección Fuente (128 bits)*. Identifica la dirección fuente IPv6 del transmisor.
- *Dirección Destino (128 bits)*. Muestra la dirección destino IPv6 del paquete.

**Extensiones de Encabezado.** Son encabezados opcionales, enlazados uno después de otro, que van después del encabezado básico de IPv6. Un paquete IPv6 puede llevar uno o múltiples extensiones de encabezados o inclusive no llevar ninguno. A continuación se definen las Extensiones de Encabezados:

- *Encabezado de Opciones Salto-por-Salto (protocolo 0)*. Este campo es leído y procesado por cada nodo y enrutado a lo largo de la trayectoria de envío. Éste es usado para paquetes Jumbograma y la Alerta de Ruteador.

- *Encabezado de Opciones de Destino (protocolo 60)*. Lleva información opcional que está específicamente dirigida a la dirección de destino del paquete.
- *Encabezado de Enrutamiento (protocolo 43)*. Puede ser usado por un nodo fuente IPv6 para forzar a que un paquete atraviese ruteadores específicos en su trayectoria al destino. Se puede especificar una lista de ruteadores intermediarios dentro del encabezado cuando se pone en 0 el campo de Tipo de Enrutamiento.
- *Encabezado de Fragmentación (protocolo 44)*. En IPv6 se recomienda que el mecanismo PMTUD esté en todos los nodos. Si un nodo no soporta PMTUD y debe enviar un paquete más grande que el MTU se utiliza el Encabezado de Fragmentación. Cuando esa situación ocurre el nodo fragmenta el paquete y envía cada parte utilizando Encabezados de Fragmentación, los cuales son acumulados en el extremo receptor donde el nodo destino los reensambla para formar el paquete original.
- *Encabezado de Autenticación (protocolo 51)*. Este se utiliza en IPSec para proveer autenticación, integridad de datos y protección ante una repetición, e incluye también protección a algunos campos del encabezado básico de IPv6. Este encabezado es conocido como *AH*.
- *Encabezado de Carga de Seguridad Encapsulada (protocolo 50)*. Es usado en IPSec para proveer autenticación, integridad de datos, protección ante repetición y confidencialidad del paquete IPv6. Es conocido como *ESP*.

***Direccionamiento.*** Los cambios introducidos por IPv6 no sólo son en cantidad de direcciones sino que incluyen nuevos tipos, representaciones y sintaxis.

***Tipos de direcciones IPv6.*** Una dirección IPv6 puede ser clasificada en alguno de los tres tipos creados:

- *Unicast.* Se utiliza únicamente para identificar una interfase de un nodo IPv6. Un paquete enviado a una dirección unicast es entregado a la interfase identificada por esa dirección.
- *Multicast.* Se utiliza para identificar a un grupo de interfases IPv6. Un paquete enviado a una dirección multicast es procesado por todos los miembros del grupo multicast.
- *Anycast.* Se asigna a múltiples interfases (usualmente en múltiples nodos). Un paquete enviado a una dirección anycast es entregado a una de estas interfases, usualmente la más cercana.

Cada uno de los tres tipos se subdivide en direcciones diseñadas para resolver casos específicos de direccionamiento IP, los cuales a continuación se presentan y describen.

Unicast agrupa los siguientes tipos:

- Enlace Local (Link-Local).
- Sitio Local (Site-Local).
- Agregable Global (Aggregatable Global).
- Loopback.
- Sin-Especificar (Unspecified).
- Compatible con IPv4.

Anycast agrupa:

- Agregable Global (Aggregatable Global).
- Sitio Local (Site Local).
- Enlace Local (Link Local).

Multicast agrupa:

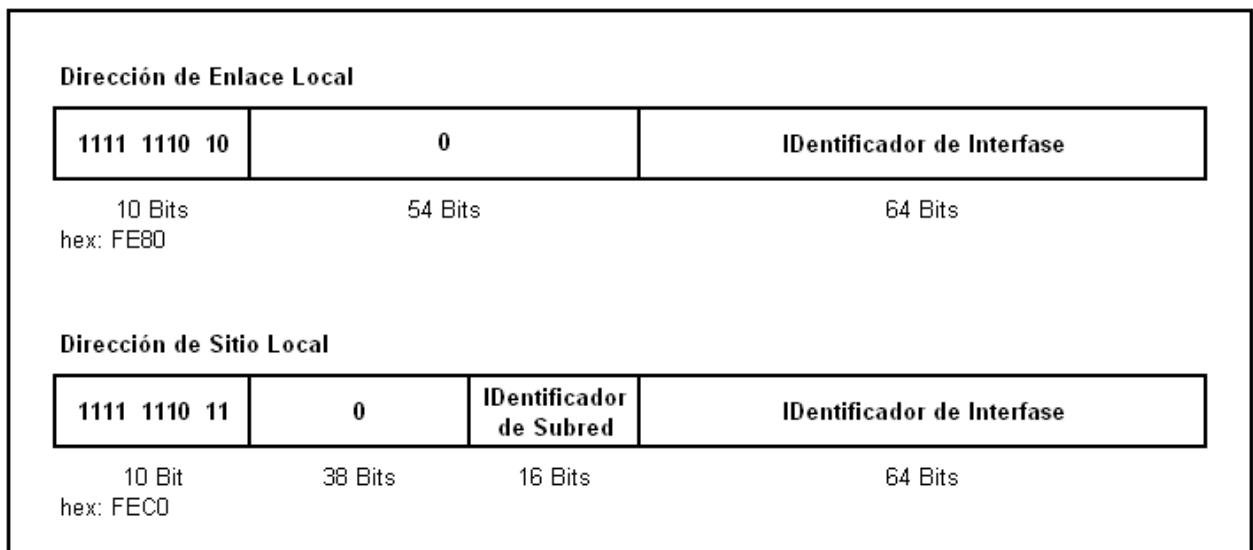
- Asignada (Assigned).

- Nodo Solicitado (Solicited Node).

*Enlace Local.* Se utiliza en un enlace sencillo y no debe nunca ser enrutada. Se usa para mecanismos de autoconfiguración, descubrimiento de vecinos y en redes sin ruteadores. Es útil para crear redes temporales. Puede ser utilizada sin un prefijo global.

*Sitio Local.* Contiene información de subred dentro de la dirección. Son enrutadas dentro de un sitio, pero los ruteadores no deben enviarlas fuera de éste. Además es utilizada sin un prefijo global.

**Figura 26. Formato de direcciones de Enlace Local y Sitio Local.**



Nota fuente. <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

El prefijo **FE80** identifica a una dirección de Enlace Local y el prefijo **FEC0** identifica a un Sitio local, ambos en hexadecimal.

*Agregable Global.* Son las direcciones IPv6 utilizadas para el tráfico de IPv6 genéricos en el Internet de IPv6 y son similares a las direcciones unicast usadas para comunicarse a través del Internet de IPv4. Representan la parte más importante de la arquitectura de direccionamiento de IPv6 y su estructura

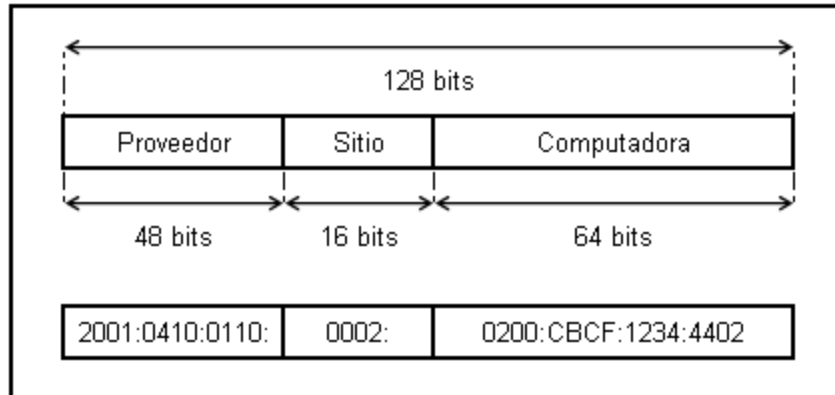
permite una agregación estricta de prefijos de enrutamiento para limitar el tamaño de la tabla de enrutamiento global de Internet.

Cada Dirección Agregable Global consta de tres partes:

- Prefijo recibido del proveedor: el prefijo asignado a una organización por un proveedor debe ser al menos de 48 bits (recomendado por el RFC 3177). El prefijo asignado a la organización es parte del prefijo del proveedor.
- Sitio: con un prefijo de 48 bits distribuido a una organización por medio de un proveedor, se abre la posibilidad para esa organización de tener 65,535 subredes (asignando un prefijo de 64 bits a cada una de las subredes). La organización puede usar los bits 49 a 64 (16 bits) del prefijo recibido para subredes.
- Computadora: utiliza cada Identificador de interfase del nodo. Esta parte de la dirección IPv6, que representa los 64 bits de más bajo orden de la dirección, es llamada Identificador de Interfase.

La siguiente figura muestra como ejemplo al prefijo 2001:0410:0110::/48 que es asignado por un proveedor a una organización. Dentro de la organización el prefijo 2001:0410:0110:0002::/64 es habilitado en una subred. Finalmente, un nodo en esta subred tiene la dirección 2001:0410:0110:0002:0200:CBCF:1234:4402.

### **Figura 27. Asignaciones de la ipv6**



Nota fuente. <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

*Loopback.* Al igual que en IPv4, cada dispositivo tiene una dirección loopback, que es usada por el nodo mismo. En IPv6 se representa en el formato preferido por el prefijo

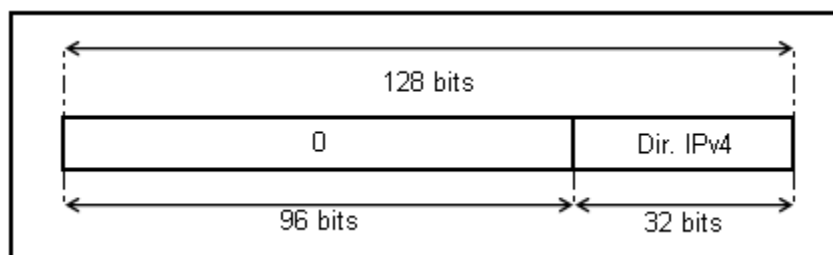
0000:0000:0000:0000:0000:0000:0000:0001 y en el formato comprimido por ::1.

*Sin-Especificar.* Es una dirección unicast sin asignar a alguna interfase. Indica la ausencia de una dirección y es usada para propósitos especiales. Es representada en el formato preferido con el prefijo 0000:0000:0000:0000:0000:0000:0000:0000 y con :: en el formato comprimido.

*Compatible con IPv4.* Es utilizada por los mecanismos de transición en computadoras y ruteadores para crear automáticamente túneles IPv4. De esa forma se entregan paquetes IPv6 sobre redes IPv4.

En la siguiente figura se muestra el formato descriptivo de una dirección IPv6 compatible con IPv4. En éste el prefijo se crea con el bit puesto a cero del de más alto nivel de los 96 bits, y los restantes 32 bits de menor nivel representan la dirección en formato decimal.

**Figura 28.**



Nota fuente. <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

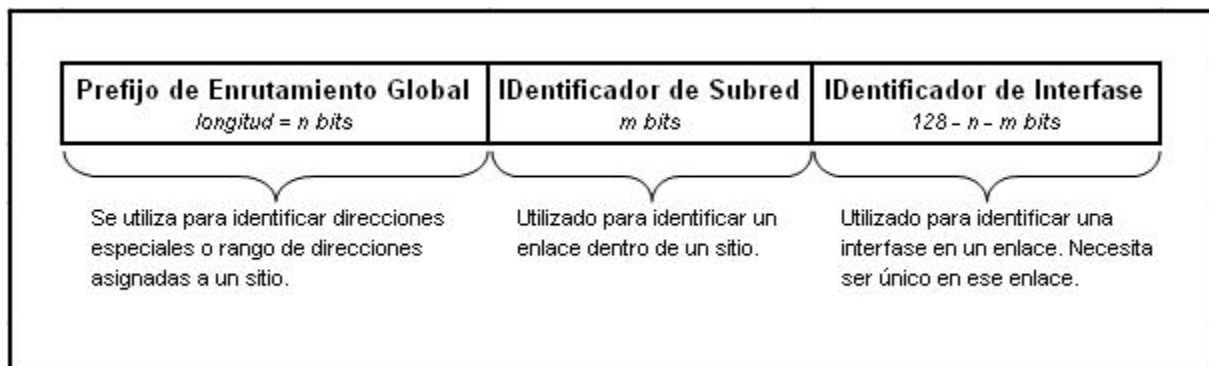
**Reglas de Utilización.** Las direcciones IPv6 son asignadas a interfaces, no a nodos, por lo que cada interfase de un nodo necesita al menos una dirección unicast. A una sola interfase se le pueden asignar múltiples direcciones IPv6 de cualquier tipo (unicast, anycast, multicast). Por lo cual un nodo puede ser identificado por la dirección de cualquiera de sus interfaces.

Existe la posibilidad de asignar una dirección unicast a múltiples interfaces para balanceo de cargas.

Una dirección típica de IPv6 consiste de tres partes como se muestra en la figura de abajo:

- a. El prefijo de enrutamiento global
- b. El IDentificador de subred
- c. El IDentificador de interfase

**figura 29.**



Nota fuente. <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

**Enrutamiento con IPv6.** El protocolo IPv6 no cambió los fundamentos del enrutamiento del protocolo IP, el cual todavía se basa en:

- La coincidencia del mayor prefijo.
- El posible uso de enrutamiento fuente.
- Redirecciona con ICMP.

- Los mismos protocolos de enrutamiento: RIP, OSPF, IS-IS y BGP.

No hay cambios mayores en el enrutamiento, de esa forma el cambio a IPv6 es transparente para el administrador de redes. Únicamente se realizaron modificaciones a la forma en que se maneja el enrutamiento para hacerlo más eficiente o para hacer uso de las características de IPv6.

*Rutas Estáticas* – Son utilizadas para forzar el enrutamiento de algunos prefijos a través de ruteadores específicos. La ruta por omisión (::/0) es un ejemplo de ruta estática. Las rutas estáticas en una tabla de enrutamiento tienen una mayor preferencia sobre rutas aprendidas por protocolos de enrutamiento.

Una ruta estática contiene el prefijo a ser enrutado y la dirección IP del ruteador. Dicha ruta tiene como nombre el siguiente salto, es el responsable de enrutar cualquier paquete con un destino dentro del rango de prefijo dado. No existen diferencias entre IPv4 e IPv6 para las rutas estáticas, sin embargo, se debe usar una dirección de enlace local como la dirección de siguiente salto.

## 5.2 Diagrama físico y lógico del laboratorio

Los diagramas a tener en cuenta en nuestra propuesta seguirán el modelo de red conmutada sin fronteras de CISCO para poder garantizar la máxima disponibilidad, flexibilidad, seguridad y facilidad de administración.

### **Principios fundamentales de los entornos CISCO en los diagramas**

**Jerárquico:** facilita la comprensión de la función de cada dispositivo en cada nivel, simplifica la implementación, el funcionamiento y la administración, y reduce los dominios de error en cada nivel.

**Modularidad:** permite la expansión de la red y la habilitación de servicios integrados sin inconvenientes y a petición.

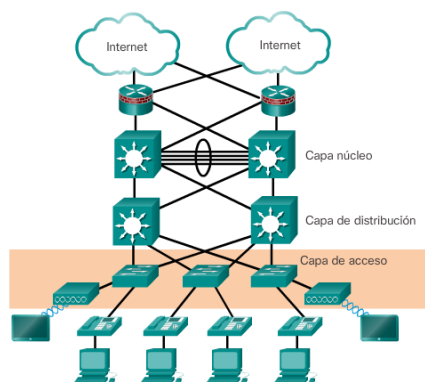


**Resistencia:** satisface las expectativas del usuario al mantener la red siempre activa.

**Flexibilidad:** permite compartir la carga de tráfico de forma inteligente mediante el uso de todos los recursos de red.

### Capas del modelo jerárquico de CISCO

Cada capa se puede considerar como un módulo estructurado bien definido, con funciones y roles específicos en la red de campus. La introducción de la modularidad en el diseño jerárquico de campus asegura aún más que la red de campus mantenga la resistencia y la flexibilidad suficientes para proporcionar servicios de red fundamentales. La modularidad también permite el crecimiento y los cambios que ocurren con el tiempo.



**Figura 25. Capas del modelo jerárquico**

Nota fuente. <https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#>

**Capa de acceso.** Representa el perímetro de la red, por donde entra o sale el tráfico de la red de campus. Tradicionalmente, la función principal de los switches de capa de acceso es proporcionar acceso de red al usuario. Los switches de capa de acceso se conectan a los switches de capa de

distribución, que implementan tecnologías de base de red como el routing, la calidad de servicio y la seguridad.

Para satisfacer las demandas de las aplicaciones de red y de los usuarios finales, las plataformas de switching de última generación ahora proporcionan servicios más convergentes, integrados e inteligentes a diversos tipos de terminales en el perímetro de la red. La incorporación de inteligencia en los switches de capa de acceso permite que las aplicaciones funcionen de manera más eficaz y segura en la red.

**Capa de distribución.** La capa de distribución interactúa entre la capa de acceso y la capa de núcleo para proporcionar muchas funciones importantes, incluidas las siguientes:

- Agregar redes de armario de cableado a gran escala.
- Agregar dominios de difusión de capa 2 y límites de routing de capa 3.
- Proporcionar funciones inteligentes de switching, de routing y de política de acceso a la red para acceder al resto de la red.
- Proporcionar una alta disponibilidad al usuario final mediante los switches de capa de distribución redundantes, y rutas de igual costo al núcleo.
- Proporcionar servicios diferenciados a distintas clases de aplicaciones de servicio en el perímetro de la red.

**Capa núcleo.** La capa de núcleo es el backbone de una red. Esta conecta varias capas de la red de campus. La capa de núcleo funciona como agregador para el resto de los bloques de campus y une el campus con el resto de la red. El propósito principal de la capa de núcleo es proporcionar el aislamiento de fallas y la conectividad de backbone de alta velocidad.

Teniendo en cuenta los principios y capas definidas por CISCO, tendríamos entonces el siguiente esquema.

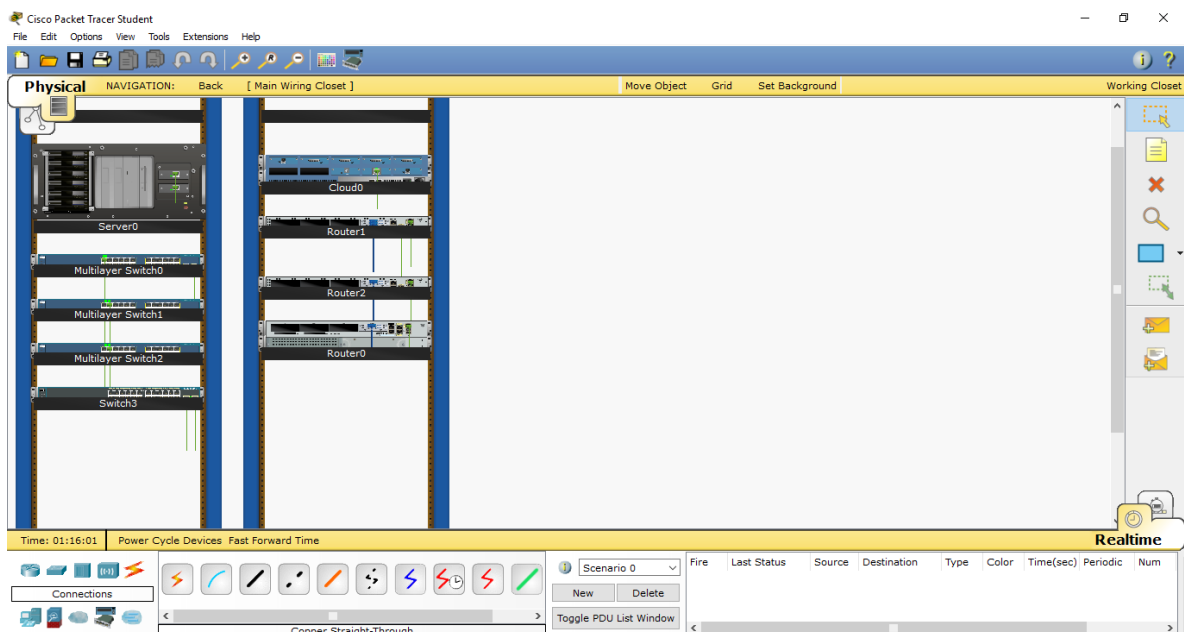
**Tabla 9.**

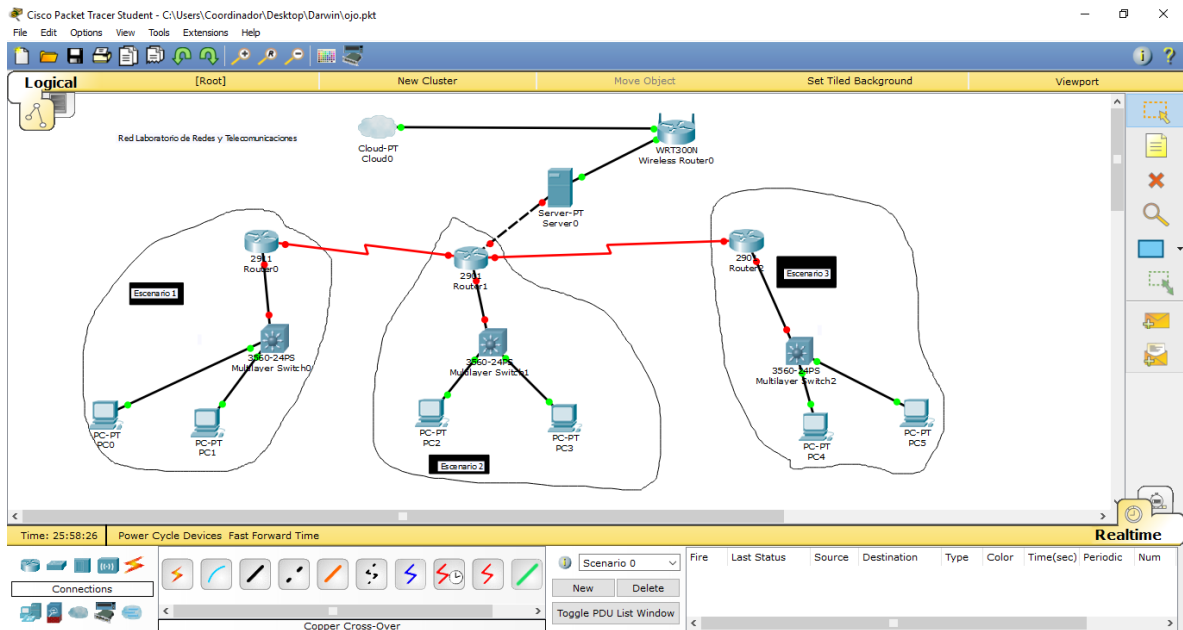
*Hardware necesario para el desarrollo de SDN en el laboratorio*

Cant	Dispositivo	serie	Existencia
3	Switch	3000	NO
3	Switch	2960	SI
1	Servidor Cisco	UCS C220	NO
24	Portátiles existentes	Hp Probook	SI

En la sección de anexos estarán disponibles los data sheet correspondientes a estos dispositivos.

En nuestro caso la capa de acceso estará a cargo de los switch 2960 y de la capa de distribución y núcleo los switch de la serie 3750-X o 3560-X. en la siguiente figura se muestran los diagramas planteados.





**Figura 26. Diagrama físico de la red**

Nota fuente. Autores del proyecto

Para nuestro ejemplo vamos a suponer que la División de Sistemas actuando como ISP de del laboratorio, asigna la siguiente dirección Global IPv6:

2001:0DB8:CAFE:0000:0000:0000:0000/48, de acuerdo a esta dirección, vamos a suponer que en el escenario 1 existirán 120 host, escenario 2 existirán 64, escenario 3 existirán 20 host, a continuación se describirá el cálculo de las subredes.

#### **Para la subred 1: Necesitamos 120 host router 0**

Cantidad de host  $120 = 2^7$  potencia de host deseada =128,  $128-7=121$  prefijo

#### **Para la subred 2: Necesitamos 64 host router 1**

Cantidad de host  $64 = 2^6$  potencia de host deseada =64,  $218-6=122$  prefijo

#### **Para la subred 3: Necesitamos 20 host router 2**

Cantidad de host  $20 = 2^5$  potencia de host deseada =32,  $128-5=123$  prefijo

#### **Para la subred 4: Necesitamos 2 host enlace serial 1**

Cantidad de host  $2 = 2^{(1)}$  potencia de host deseada =2,  $128-1=127$  prefijo

**Para la subred 5: Necesitamos 2 host enlace serial 2**

Cantidad de host  $2 = 2^{(1)}$  potencia de host deseada =2,  $128-1=127$  prefijo

**Para la subred 6: Necesitamos 2 host enlace servidor**

Cantidad de host  $2 = 2^{(1)}$  potencia de host deseada =2,  $128-1=127$  prefijo

**Tabla 10.**

*Direccionamiento ipv6 para los dispositivos activos*

<b>DIRECCIONAMIENTO IPv6 PARA LOS DISPOSITIVOS ACTIVOS</b>			
<b>Escenario 1: Router 0</b>			
Interfaz giga 0/0 2001:DB8:CAFE:1::1/121	Interfaz serial 0/0/0 2001:DB8:CAFE:4::0/127		Cargo DTE
<b>Escenario 2: Router 1</b>			
Interfaz giga 0/0 2001:DB8:CAFE:2::1/122	Interfaz serial 0/0/0 2001:DB8:CAFE:4::1/127	Interfaz serial 0/0/1 2001:DB8:CAFE:5::0/127	Cargo DCE
<b>Escenario 3: Router 2</b>			
Interfaz giga 0/0 2001:DB8:CAFE:3::1/123	Interfaz serial 0/0/0 2001:DB8:CAFE:5::1/127		Cargo DTE

Nota fuente. Autores del proyecto

A continuación mostramos la configuración de los equipos activos de red utilizando OSPF, cabe aclarar que esta configuración es solo para los router propuestos en la arquitectura y está basada en lo aprendido en las materias de redes del programa.

**Configuración de las interfaces y el reloj**

**Para el router 0**

```
Router>enable
Router#configure terminal
Router(config)#hostname Router0
Router0(config)#ipv6 unicast-routing
Router0(config)#interface giga 0/0
Router0(config-if)#ipv6 address 2001:db8:cafe:1::1/121
Router0(config-if)#no shutdown
Router0(config-if)#exit
Router0(config)#interface serial 0/0/0
Router0(config-if)#ipv6 address 2001:db8:cafe:4::0/127
```

```
Router0(config-if)#no shutdown
Router0(config-if)#exit
Router0(config)#
```

### Para el router 1

```
Router>enable
Router#configure terminal
Router(config)#hostname Router1
Router1(config)#ipv6 unicast-routing
Router1(config)#interface giga 0/0
Router1(config-if)#ipv6 address 2001:db8:cafe:2::1/122
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface serial 0/0/0
Router1(config)#clock rate 128000
Router1(config-if)#ipv6 address 2001:db8:cafe:4::1/127
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface serial 0/0/1
Router1(config)#clock rate 128000
Router1(config-if)#ipv6 address 2001:db8:cafe:5::0/127
Router1(config-if)#no shutdown
Router1(config-if)#exit
```

### Para el router 2

```
Router>enable
Router#configure terminal
Router(config)#hostname Router0
Router2(config)#ipv6 unicast-routing
Router2(config)#interface giga 0/0
Router2(config-if)#ipv6 address 2001:db8:cafe:3::1/123
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#interface serial 0/0/0
Router2(config-if)#ipv6 address 2001:db8:cafe:5::1/127
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#
```

## Configuración de un protocolo de enrutamiento en nuestro caso elegimos el OSPF

### Para el router 0

```
Router0>enable
Router0#configure terminal
Router0(config)#ipv6 router ospf 10
Router0(config-rtr)#router-id 1.1.1.1
Router0(config-rtr)#exit
Router0(config)#interface giga 0/0
Router0(config-if)#ipv6 ospf 10 area 0
Router0(config-if)#exit
Router0(config)#interface serial 0/0/0
```

```
Router0(config-if)#ipv6 ospf 10 area 0
Router0(config-if)#exit
Router0(config)#
```

### Para el router 1

```
Router1>enable
Router1#configure terminal
Router1(config)#ipv6 router ospf 10
Router1(config-rtr)#router-id 2.2.2.2
Router1(config-rtr)#exit
Router1(config)#interface giga 0/0
Router1(config-if)#ipv6 ospf 10 area 0
Router1(config-if)#exit
Router1(config)#interface serial 0/0/0
Router1(config-if)#ipv6 ospf 10 area 0
Router1(config-if)#exit
Router1(config)#interface serial 0/0/1
Router1(config-if)#ipv6 ospf 10 area 0
Router1(config-if)#exit
Router1(config)#
```

### Para el router 2

```
Router2>enable
Router2#configure terminal
Router2(config)#ipv6 router ospf 10
Router2(config-rtr)#router-id 3.3.3.3
Router2(config-rtr)#exit
Router2(config)#interface giga 0/0
Router2(config-if)#ipv6 ospf 10 area 0
Router2(config-if)#exit
Router2(config)#interface serial 0/0/0
Router2(config-if)#ipv6 ospf 10 area 0
Router2(config-if)#exit
Router2(config)#
```

## Tabla 11.

*Direccionamiento ipv6 para los host*

DIRECCIONAMIENTO IPV6 PARA LOS HOST				
<b>Escenario 1: Host</b>				
IPv6 Address	Prefijo	Link Local Address (EUI-64)	IPv6 Gateway	
2001:DB8:CAFE:1::10	121	FE80::203:E4FF:FE0A:2934	2001:DB8:CAFE:1::1	
<b>Escenario 2: Host</b>				
IPv6 Address	Prefijo	Link Local Address (EUI-64)	IPv6 Gateway	
2001:DB8:CAFE:2::10	122	FE80::205:5EFF:FE4A:C338	2001:DB8:CAFE:2::1	
<b>Escenario 3: Host</b>				

IPv6 Address	Prefijo	Link Local Address (EUI-64)	IPv6 Gateway
2001:DB8:CAFE:3::10	123	FE80::260:70FF:FE12:E559	2001:DB8:CAFE:3::1

Nota fuente. Autores del proyecto



## Conclusiones

A pesar de ser un cambio de paradigma, la migración para la arquitectura de las redes definidas por *software* tiende a ser un camino natural, aunque lleve algún tiempo para que sea efectivamente absorbido por los proveedores y, principalmente, usuarios.

Tendencias como la movilidad del usuario, la virtualización de servidores, o la necesidad para responder a las cambiantes condiciones de negocio, significan nuevas demandas sobre redes. Las redes definidas por software forman un nuevo paradigma que habilita la programación de la red.

Podemos concluir que las SDN consisten en separar el control de la red (centralizándolo) de la conmutación de los paquetes de datos. De esta manera los equipos tales como switches, routers, etc... simplemente conmutan los datos en función de las instrucciones que reciben del plano de control de la red. Este plano de control, a su vez, recibe instrucciones de las aplicaciones del usuario. De esta forma las aplicaciones definen el comportamiento de la infraestructura.

Uno de los problemas relacionados con el control centralizado es la vulnerabilidad de la red. Un fallo en el controlador puede afectar negativamente a la resistencia de la red y por tanto comprometiendo la información que está viajando en ella. De igual manera, debido a que el control se encuentra centralizado, la posibilidad de ataques de denegación de servicio es mayor.

## Recomendaciones

SDN es una tecnología de redes reciente y en constante actividad de desarrollo e investigación, se recomienda aplicar la arquitectura aquí planteada ya que es la que más se ajusta a nuestro laboratorio.

A la hora de implementar una red definida por software en el laboratorio de la universidad sugerimos crear entornos de respaldo o *backup* que permitan contrarrestar las vulnerabilidades y ataque de denegaciones de servicio.

## Referencias

- [1] Constitución Política de Colombia. Artículo 75. 2014. [Citado 19 de septiembre de 2015] [En Línea] Disponible en <http://www.constitucioncolombia.com/titulo-2/capitulo-2/articulo-75>
- [2] Decreto 2133 de 2003. 2003. 2014. [Citado 21 de septiembre de 2015] [En Línea] Disponible en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=9244>
- [3] GARCIA, José Carlos. Network World. [Citado 29 de agosto de 2015] [En Línea] Disponible en: <http://www.networkworld.es/sdn/que-puede-aportar-sdn-a-la-seguridad-tic>
- [4] LEY 1341 DE 2009, 2009. [Citado 19 de septiembre de 2015] [En Línea] Disponible en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913>
- [5] MALDONADO HIDALGO, Diego Armando. Pontificia Universidad Javeriana. [Citado 25 de agosto de 2015] [En Línea] Disponible en: <http://bibdigital.epn.edu.ec/bitstream/15000/7360/1/CD-5509.pdf>
- [6] MINISTERIO DE COMUNICACIONES, Resolución número 000689 de 2004, 2004. [Citado 19 de septiembre de 2015] [En Línea] Disponible en: <http://archivos.bogotamesh.org/Documentos/Leyes/Resoluci%F3n%20689%20de%202004.pdf>
- [7] NETWORK WORLD. *La presencia de SDN crece un 200% entre los proveedores de servicios.* [Citado 29 de agosto de 2015] [En Línea] Disponible en: <http://www.networkworld.es/sdn/la-presencia-de-sdn-crece-un-200-entre-los-proveedores-de-servicios>
- [8] Organismos de Normalización. [Citado 31 de agosto de 2015] [En Línea] Disponible en: <http://personales.unican.es/zorrillm/MaterialOLD/redes.pdf>
- [9] Política de Territorios Digitales. 2011. [Citado 19 de septiembre de 2015] [En Línea] Disponible en <http://es.slideshare.net/frajaroterritorios-digitales-hacia-territorios-del-conocimiento-7079003>
- [10] RESEÑA HISTÓRICA. Universidad Francisco de Paula Santander Ocaña. [Citado 19 de agosto de 2015] [En Línea] Disponible en: <http://www.ufpso.edu.co/ufpso/general.html#historia>.
- [11] <http://personales.unican.es/zorrillm/MaterialOLD/redes.pdf>
- [12] <http://blogs.salleurl.edu/nice-rack/2014/04/22/data-center-management/>
- [13] <http://www.ramonmillan.com/tutoriales/sdnredesinteligentes.php>
- [14] Opendaylight [URL: <http://www.opendaylight.org>, última visita 2015].
- [15] Arquitectura SDN [URL: <https://www.sdxcentral.com/resources/sdn/inside-sdn-architecture/>]

- [16] SDN como base para la virtualización de red [URL: <http://www.techweek.es/virtualizacion/opinion/1013779005901/sdn-base-virtualizacion-red.1.html>]
- [17] Beneficios del SDN [http://www.la.logicalis.com/globalassets/latin-america/advisors/es/advisor\\_sdn.pdf](http://www.la.logicalis.com/globalassets/latin-america/advisors/es/advisor_sdn.pdf)
- [18] Bruno Nunes, Manoel Mendonca, Xuan-Nam Nguyen, Katia Obraczka, Thierry Turletti, et al. A survey of software-defined networking: Past, present, and future of programmable networks. *Communications Surveys & Tutorials*, IEEE, 16(3):1617–1634, 2014.
- [19] Srini Seetharaman. Opendaylight helium application developers’ tutorial. URL: <http://sdnhub.org/tutorials/opendaylight-helium/> [última visita 2015].
- [20] Cisco. Opendaylight api. URL: <https://developer.cisco.com/media/XNCJavaDocs/overview-summary.html> [última visita 2015].
- [21] Floodlight Web. URL: <http://www.projectfloodlight.org/> [última visita 2015].
- [22] Iperf [URL: <https://iperf.fr/>, última visita 2015].
- [23] Wireshark web. URL: <https://www.wireshark.org/> [última visita 2015].
- [24] Wireshark Wikipedia. URL: <https://es.wikipedia.org/wiki/Wireshark> [última visita 2015].
- [25] Woon Hau Chin, Zhong Fan, and R. Haines. Emerging technologies and research challenges for 5g wireless networks. *Wireless Communications*, IEEE, 21(2):106–112, April 2014. doi:10.1109/MWC.2014.6812298.
- [26] Frank Durr. Developing osgi components for opendaylight.
- [27] Jordan R. Energy efficient ethernet: Technology, application and why you should care. Technical report, Intel Corporation, 2011.
- [28] Srini Seetharaman, Anirudh Ramachandran, and Sriram Natarajan. Sdn hub. URL: <http://sdnhub.org/> [última visita 2015].
- [29] Maven Web. URL: <https://maven.apache.org/> [última visita 2015].
- [30] Brian Linkletter. How to use miniedit, mininet’s graphical user interface. URL: <http://www.brianlinkletter.com/how-to-use-miniedit-mininets-graphical-user-interface/> [última visita 2015].
- [31] <https://support.apple.com/es-es/HT202236>
- [32] <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

- [33] "Cinco controladores SDN comerciales que hay que conocer", *SearchDataCenter en Español*, 2016. [Online]. Available: <http://searchdatacenter.techtarget.com/es/cronica/Cinco-controladores-SDN-comerciales-que-hay-que-conocer>. [Accessed: 01- Jul- 2016].
- [34] D. Erickson, "Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking", in *The Beacon Openflow Controller*, Hong Kong, China, 2013, p. 13.

# Apendices

## Apendice A. Encuesta



### Apendice A. Modelo de Entrevista

Universidad Francisco de Paula Santander Ocaña  
Facultad de Ingenierías

**Objetivo:** Obtener Información relevante para determinar una arquitectura basada en tecnología “SDN” (Redes Definidas por Software), para el laboratorio de Redes y Telecomunicaciones de la Universidad Francisco de Paula Santander Ocaña.

1. Sabe que es virtualización en un entorno de redes.? • Si \_\_\_\_\_  
NO \_\_\_\_\_

---



---

2. Alguna vez instalo máquinas virtuales en el desarrollo de las asignaturas de redes .? • Si \_\_\_\_\_  
NO \_\_\_\_\_

---



---

3. Creé posible la manipulación de hardware de red a través de software.? • Si \_\_\_\_\_  
NO \_\_\_\_\_

---



---

4. Conoce alguna herramienta o software capaz de emular un entorno de redes? • Si \_\_\_\_\_  
NO \_\_\_\_\_

---



---

5. Durante su carrera ha escuchado el termino SDN “Redes Definidas por Software”.? • Si \_\_\_\_\_  
NO \_\_\_\_\_

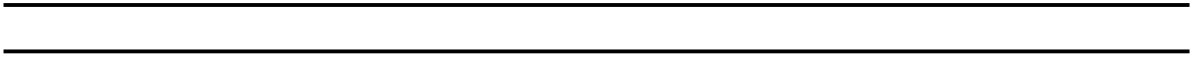
---



---


6. Creé que adquirir conocimiento sobre tecnologías emergentes como redes definidas por software darán un valor agregado en su competencia profesional?

• Si \_\_\_\_\_ NO \_\_\_\_\_





## Apndice B. Listado de alumnus encuestados

 <b>Universidad Francisco de Paula Santander Ocaña Al</b>			
Jueves Mayo 12 2016 11:28 AM			
<b>Codigo</b>	<b>Nombres</b>	<b>Direccion</b>	<b>Telefono</b>
190010	HERNANDEZ ROJAS LEIDI LILIANA	CALLE 8 No. 19-69	5622047
190066	SEPULVEDA PEÑARANDA FREDY ALFONSO		
190262	MORENO SANDOVAL ANDRES ALFREDO	CALLE 6 NO. 23-38	
190263	OCHOA GUERRERO DIEGO ARMANDO	CALLE 3 # 22 - 36	5690210
190323	PINTO QUINTERO MARIA DEL ROSARIO		
190434	CORDOBA VASQUEZ VICTOR ALFONSO	KDX 34-A	3144716181
190448	VILA ALVAREZ ARLEY MAURICIO	CARRERA 17A #3-10	
190496	LAZARO ORTIZ CRISTO LEANDRO	CRA 10 B # 18 - 32	3124505629
190509	LOBO VERGEL MARIO IVAN	KDX 393 - 420	3167660370
190519	BOHORQUEZ LOBO NAIN ANDREY	VEREDA LAS CHIRCA	3155510127
190526	NAVARRO NAVARRO LEYNA LILIANA	CARRERA 45 NO. 5A-50	5610798
190543	MORENO RIZO ALVARO JAVIER	CALLE 3A NRO 24A-54	5694240
190597	MEDINA HERRERA JHON JAIRO	KDX110-620	3112700822
190607	OROZCO ALVAREZ LIGDY MILENA	KDX 088-120	3145011921
190612	AREVALO CARVAJAL CAROLINA	KDX 405 160	3164308921
190655	PEÑA LOZANO TOBIAS	CLL19B13-14KDX035-340	3178099761
190674	GONZALEZ MORENO EDWIN MAURICIO	CALLE 13 # 11-71	5626452
190675	BALLESTEROS CORONEL ANGIE LORENA	CALLE 13 NO 10-28	3165189389
190678	CACERES GALEANO KAREN LORENA	KDX 166-420	3125892932
190709	ROMERO CARDENAS SAMIR	CRA 3 NO 13	3184530677
190712	PEREZ ORTEGA DIANA MARCELA	KDX 088-540	3102328699
190732	AFANADOR DELGADO CRISTIAN ANDRES	KDX 194-380	3182183261
190735	GOMEZ VELASQUEZ MAIRA CECILIA	CALLE 9 0-27	5692301
190736	MALDONADO MORENO JULIO CESAR	KDX 111-370	3176557693
190748	ROJAS PEREZ JESUS ALBERTO	CALLE 4 # 44A-02	
190749	CASTILLA CONTRERAS ANDREY	CALLE 5 #27-56	3123309640
190756	TORRADO MEJIA CHRISTIAN JHOAN	CRA 13B N° 13-78	5626049
190763	MONTAÑEZ VERJEL OSCAR JOSE	KDX 4 - 10	
190774	PEINADO HERNANDEZ WENDY MILENA	CL 7 NO 7-42	3105660633
190777	MANCIPE GUTIERREZ MARIA CAROLAIN	CRA 10 3-96	3178793976
190781	MENDEZ SANJUAN LICETH LORENA	KDX 9-1	3208554752
190783	CAMARGO PEREZ JESUS ALBERTO	CALLE 3 B # 27A -111	3112740970
190787	QUINTERO SANABRIA FLOR MARIA	CALLE 8 15-22	3164816341
190793	ORTEGA QUINTERO NARLY KARINA	CRA 27 B # 9-43	3128179305
190816	FONTECHA GUERRERO YEIMY LICETH	CRA 19 A #2 - 36	3125186574
190985	VEGA QUINTERO JOHN JHADER	CALLE 4 44A-41	5612902
191018	SANCHEZ TORRES BRAYAN	KDX 865-160	3152775657
191215	NUMA PICON VANESSA	CL 12A NO 23-08	3213216729
191217	SANCHEZ JULIO BRAYAN FERNANDO	KDX 384-410	3152794244
191218	PALACIO TORRADO YEFERSON ANDREY	KDX F8360	3144368730
191222	TORRADO TORRADO VICTOR MANUEL	KDX T3-340	3133311885
191241	MACHADO LOBO ALEJANDRA	CARRERA 26 N13-34	3163845283
191248	PEREZ TRIGOS JULIAN DAVID	KDX 866 - 120	3112826558
191261	CRiado AFANADOR IVAN MAURICIO	CALLE 5 CRA 47-03 SANTA CLARA	3217856567
191283	GARCIA TORRES MARIA FERNANDA	KDX 825-279	5610513
191296	URIBE LOZANO JEIMMY CAROLINA	CALLE 13B 25A 19	5695398
191307	AREVALO CAÑIZARES FABIAN ANDRES	CRA 10A # 13B-19	3158917121



## Universidad Francisco de Paula Santander Ocaña Al

Jueves Mayo 12 2016 11:28 AM

Codigo	Nombres	Direccion	Telefono
191308	SANTANA DUARTE CIRO ARCESIO	CALLE 15# 26-04	3156784484
191314	TORRES TORRES JHON DAIRO	CLL 11 KDX 111-280	3186293923
191320	CARRASCAL SALAZAR DIEGO ARMANDO	CARRERA 49 # 51-35	3145637360
191321	BAIRON JOSE AMAYA MANZANO	KDX 713	3208151667
191342	MOJICA QUINTERO OSWALD ANDRES	CARRERA 7 NO 9-45 LOS ALMENDROS	3146102038
191345	PINZON TARAZONA YISELA PATRICIA	KDX50	3115195568
191346	VERGEL BELTRAN JOSE MANUEL	55502 CTO 2	3182976460
191347	SANCHEZ SANCHEZ CAMILO ANDREY	CRR 26 # 14-52	3166243605
191362	PINTO DUARTE SEBASTIAN	KX 403-240	3184065738
191363	VELASQUEZ DURAN YENJHADER	KDX 403-240	3163850405
191369	TRIGOS MUÑOZ FABIAN RICARDO	KDX 386	3204905907
191374	CANIZARES CASTRILLON KEYLA MARCELA	TRV 7#23-81 PISO 1	3155979055
191394	ESCALANTE MORALES JAIRO ANDRES	CALLE 12B N 8B 36	3107599974
191429	BONILLA ORTEGA KEVIN	CALLE 11B 28E-55	3126043212
620194	MOLINA ORTIZ JESUS ENRIQUE	CXALLE 12 KRA 27B-43	
620205	JACOME JACOME LINEY	KDX 527-440	3213505886
620209	CARVAJALINO ORTIZ URIEL	CALLE 15 N 16 40	3188772651
620212	PUERTA COMAS ARTURO EDUARDO	CL 1A # 19-04	3107262631
620218	QUINTERO MARTINEZ JUAN SEBASTIAN	CRA 7 NO 23-85	3187955303
620224	TORRADO FAJARDO FELIPE ANDRES	KDX 396-140	3154457113
620230	MORENO NOBLES MARIA MONICA	CARRERA 12 # 9-32	3188257889
620241	ARENAS CARRASCAL ANGY SUSANA	KDX 357-265	3207459791
620246	CARRASCAL PARRA CARLOS EDUARDO	KDX 3 FINCA EL HATILLO	3155316402
620247	CALY ROJAS LILIANA CAROLINA	CALLE 22 8 A 25	3115529912
620249	JAIMES BAYONA EDWIN HUMBERTO	CALLE 12 NO. 25 A 41 B. EL RETIRO	5613391
620251	CARREÑO BLOISE LEDWIN JESUS	KDX 180 - 280	3112118375
620252	CASTRO PEREZ RAUL ERNESTO	AV CIRCUNVALAR	3173571052
620260	LOBO RINCON MARCIO CAMILO	CRA 25A N° 4-39	3187992815
620265	TORRES BERMON DIRLIANY ANDREA	CRA 8A N°23-33	3185885224
620268	TORRES SAMPAYO MANUEL JOSE	CARRERA 5 # 4-26	3013838492
620276	CHONA ROBLES JHON MARIO	CRA 15B NO 10-80	3143564603
620277	TRIANA ALVAREZ EFRAIN ALEJANDRO	KDX 265-380	3184782163
620278	PAEZ PORTILLO ANGELA PATRICIA	CRA 16 # 7 -82	3133435954
620279	CORONEL URQUIJO JHON JAIRO	CRA 8B # 23-41	3178332852
620280	ROCHEL VERGEL JOSE MIGUEL	CRA 11 NO 13-46	3173382723
620282	PEÑARANDA RIBON DAVINSON CAMILO	CARRERA 23 N° 5 - 11	3168720584
620285	ALBA QUINTERO DIEGO ARMANDO	KDX 359-180	3156423925
620286	ARENAS GOMEZ FABIAN GREGORIO	CRA 9 NO. 10-38	3208588440
620288	PABON SANTIAGO HERNAN ANDRES	CRA 15B NO 10-80	3114698513
620293	VIDES CABRALES EDUARDO AUGUSTO	CRA 12 NO 16-64	3152905538
620294	QUINTERO PEREZ JOSE DOMINGO	CLL 12 # 3-66	3008483992
620300	SANTIAGO PEREZ JUAN JOSE	CARRERA 22 #2B-05	3185258893
620313	CONTRERAS RINCON JHOAN HERNANDO	CALLE 7 #12-41	5691256
620314	RANGEL CHAPARRO LEIDY JUANITA	CRA 28D KDX 111-100	3188519650
620315	ALBA QUINTERO YAJAIRA	KDX 267-760	3184592796
620316	NAVARRO ALBA ADRIANA JIMENA	KDX 267-760	3043315043
620317	PACHECO PEÑARANDA JUAN CAMILO	CL 3 NO 3-04	3114265865



## Universidad Francisco de Paula Santander Ocaña Al

Jueves Mayo 12 2016 11:28 AM

<b>Codigo</b>	<b>Nombres</b>	<b>Direccion</b>	<b>Telefono</b>
620318	ROSADO PANTOJA ANGIE PAOLA	KDK 112-660 PISO 1	3105594748
620319	ANDRADE OJEDA ROBER JULIAN	CALLE 5 7 -85	3173373909
620331	GALVIS JAIMES RUTH BELYARIT	LOS SAUCES	
620332	ARIAS ALBA JUAN JOSE	COLINAS DE LA FLORIDA	
620333	GUERRERO QUINTERO NELSON AUGUSTO	CALLE 7B #49-10 LOS CRISTALES OCA??A	

99

## Apendice C. Cisco UCS C220 M3 Rack Server



# Cisco UCS C220 M3 Rack Server

## Product Overview

The Cisco<sup>®</sup> Unified Computing System<sup>™</sup> (Cisco UCS) combines Cisco UCS C-Series Rack Servers and B-Series Blade Servers with networking and storage access into 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<sup>®</sup> UCS C220 M3 Rack Server (one rack unit [1RU]) and Cisco UCS C240 M3 Rack Server (2RU) 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, disk drives and with faster I/O. Together these server improvements and complementary Cisco UCS advancements deliver the best combination of features and cost efficiency required to support IT's diverse server needs.

The Cisco UCS C220 M3 Rack Server (Figure 1) is designed for performance and density over a wide range of business workloads, from web serving to distributed databases. Building on the success of the Cisco UCS C200 M2 Rack Server, the enterprise-class Cisco UCS C220 M3 server further extends the capabilities of the Cisco UCS portfolio in a 1RU form factor with the addition of the Intel<sup>®</sup> Xeon<sup>®</sup> processor E5-2600 and E5-2600 v2 product families, which deliver significant performance and efficiency gains. In addition, the Cisco UCS C220 M3 server offers up to two Intel<sup>®</sup> Xeon<sup>®</sup> processor E5-2600 or E5-2600 v2 processors, 16 DIMM slots, eight disk drives, and two 1 Gigabit Ethernet LAN-on-motherboard (LOM) ports, delivering outstanding density and performance in a compact package.

The Cisco UCS C220 M3 interfaces with Cisco UCS using another unique 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 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<sup>®</sup> Data Center Virtual Machine Fabric Extender (VM-FEX) technology.

**Figure 1.** Cisco UCS C220 M3 Server



© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Page 1 of 6

## Applications

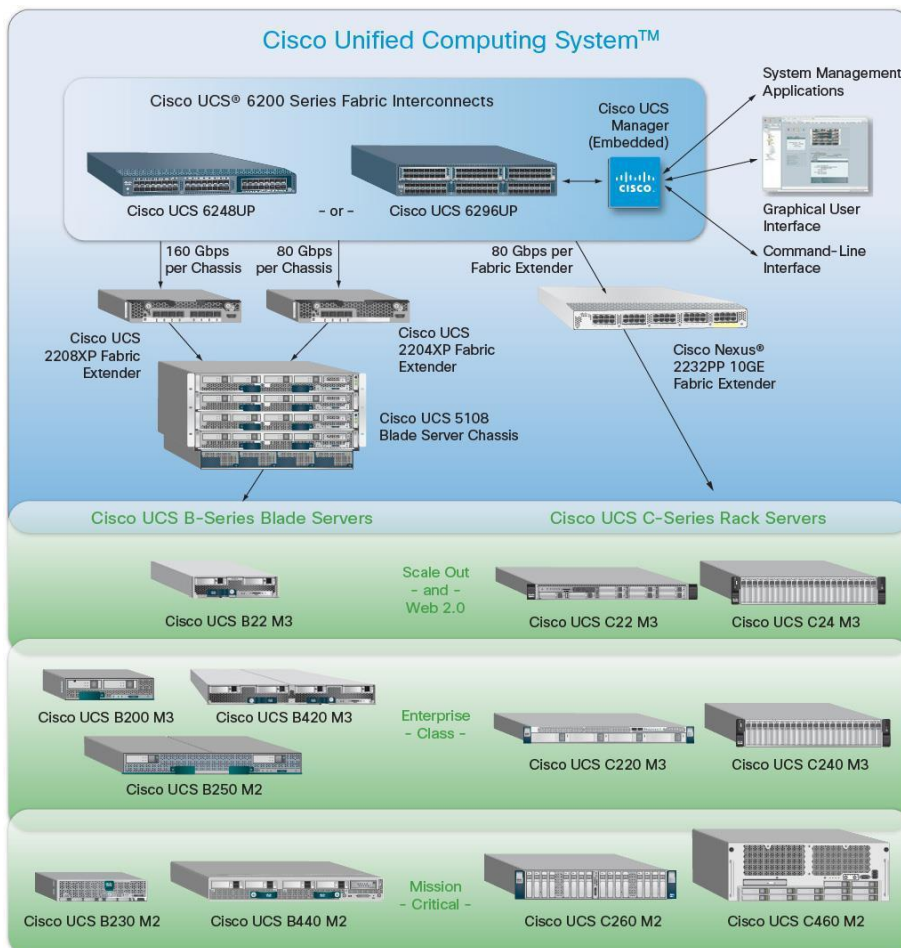
The Cisco UCS C220 M3 server is a high-density general-purpose 2-socket server optimized to deliver high performance for a large range of workloads, including:

- Distributed database clusters
- Middleware
- High-performance virtual desktops
- IT and web infrastructure

## 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 UCS that extend its exceptional simplicity, agility, and efficiency (Figure 2). Cisco leadership with new innovations such as the third-generation Cisco UCS C220 M3 rack server.

**Figure 2.** Cisco UCS Components



Cisco innovations, such as Cisco UCS Manager, allow 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 approach of configuring each system resource manually, one at a time, through individual element managers. Unlike 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 both form-factor agnostic and can bridge blade chassis boundaries.

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 the 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 compute power. Cisco completes this vision through continuous innovation in VIC, fabric extender, fabric interconnect, blade server, blade chassis, and rack server technologies and form-factor-agnostic Cisco UCS Manager Software.

The Cisco UCS C220 M3 is part of a family of rack servers: the Cisco C-Series Rack Servers. Cisco UCS C-Series servers extend unified computing innovations to an industry-standard form factor to help reduce total cost of ownership (TCO) and increase business agility. 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.

## Unique Benefits in a Familiar Package

The Cisco UCS C220 M3 server extends Cisco's product portfolio to meet the needs of customers that choose to deploy rack servers. Available from Cisco and its data center partners, the Cisco UCS C220 M3 advances the rack server market with the features outlined in Table 1.

**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> <li>• Capability to move virtual machine security features and policies from rack to rack or rack to blades</li> </ul>

Feature	Benefit
<b>Unified management (when integrated into Cisco UCS)</b>	<ul style="list-style-type: none"> <li>□ Entire solution managed as a single entity with Cisco UCS Manager, improving operational 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 by associating a service profile with a new, added or repurposed Cisco UCS C220 M3 server</li> <li>□ Capability to move service profiles from rack server to another rack server, or blade to rack server, or rack to blade server in minutes instead of hours or days</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 (Intel AVX) provides new instructions that can significantly improve performance for applications that rely on floating-point or vector computations</li> <li>□ Cisco UCS C-Series servers keep pace with Intel Xeon processor innovation by offering the latest processors with an increase in processor frequency and improved security features. With the increased performance provided by the Intel Xeon processor E5-2600 and E5-2600 v2 product families, Cisco UCS C-Series rack 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, to 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<sup>®</sup> Trusted Execution Technology (Intel<sup>®</sup> 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>Hot-swappable SAS, SATA, or SSD drives</b>	<ul style="list-style-type: none"> <li>□ Up to 4 LFF or 8 SFF front-accessible, hot-swappable, internal SAS, SATA, or SSD drives, providing redundancy options and ease of serviceability</li> <li>□ Balanced performance and capacity to best 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 provides data protection for up to 8 SAS, SATA, or SSD drives in PCIe and mezzanine card form factors.
<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>	16 DIMM slots supporting DDR3 1866-MHz memory for optimal performance
<b>Redundant fans and power supplies</b>	<ul style="list-style-type: none"> <li>● Dual-redundant fans and hot-swappable, redundant power supplies for enterprise-class reliability and uptime</li> <li>● Power efficiency through Cisco Common Form-Factor Platinum Power Supplies (450W and 650W)</li> </ul>
<b>Support for up to 2 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>● I/O performance and flexibility with one x8, half-height and half-length slot and one x16, full-height and half-length slot</li> </ul>
<b>Integrated dual-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>	Tool-free access to all serviceable items, and color-coded indicators to guide users to hot-pluggable and serviceable items
<b>Cisco Flexible Flash (FlexFlash) memory</b>	The server supports up to two internal Cisco FlexFlash drives (secure digital [SD] cards). The first 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.



## Product Specifications

Table 2 lists the specifications for the Cisco UCS C220 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 LFF <a href="#">SpecSheet</a> or SFF <a href="#">SpecSheet</a></li> </ul>
<b>Memory</b>	<ul style="list-style-type: none"> <li>16 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>2 PCIe Generation 3.0 slots available</li> <li>I/O performance and flexibility with one x8 half-height and half-length slot, and one x16 full-height and half-length slot</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 8 front-accessible, hot-swappable, 2.5-inch SAS, SATA or SSD or up to 4 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 <a href="#">SpecSheet</a></li> </ul> <p><b>3.5 inch "LFF" drive options:</b></p> <ul style="list-style-type: none"> <li>For a complete list of drive options, please refer to the <a href="#">SpecSheet</a></li> </ul>
<b>Cisco Flexible Flash (FlexFlash)</b>	<ul style="list-style-type: none"> <li>The server supports up to two internal 16GB Cisco FlexFlash drives (SD cards)</li> <li>The first 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 one of the supported OS's or hypervisors: <ul style="list-style-type: none"> <li>ESXi 5.0 U2, U3</li> <li>ESXi 5.1 U1, 5.1 U2</li> <li>ESXi 5.5, 5.5 U1, 5.5 U2</li> </ul> </li> <li>The second SD card is blank and can be used to mirror the first.</li> </ul>
<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, an RJ45 serial port, 1 Gigabit Ethernet management port, and dual 1 Gigabit Ethernet ports
<b>Physical dimensions (H x W x D)</b>	1RU: 1.7 x 16.9 x 28.5 in. (4.32 x 43 x 72.4 cm)
<b>Temperature: Operating</b>	32 to 104°F (0 to 40°C) (operating, sea level, no fan fail, no CPU throttling, turbo mode)
<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>	0 to 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 part numbers, 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 help 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>.



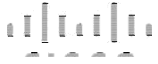
Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

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)



## Appendix D. Cisco Catalyst 2960-Plus Series Switches

Data Sheet

# Cisco Catalyst 2960-Plus Series Switches

The Cisco<sup>®</sup> Catalyst<sup>®</sup> 2960-Plus Series Switches are fixed-configuration Fast Ethernet switches (Figure 1) that provide enterprise-class Layer 2 switching for branch offices, conventional workspaces, and infrastructure applications. They enable reliable and secure operations with lower total cost of ownership through a range of Cisco IOS<sup>®</sup> software features, including Cisco Catalyst SmartOperations.

Figure 1. Cisco Catalyst 2960-Plus Series Switches



### Product Highlights

Cisco Catalyst 2960-Plus switches feature:

- 24 or 48 Fast Ethernet ports
- Small Form-Factor Pluggable (SFP) and 1000BASE-T Gigabit Ethernet uplinks
- IEEE 802.3af-compliant Power over Ethernet (PoE)
- LAN Base or LAN Lite Cisco IOS<sup>®</sup> Software feature set
- SmartOperations tools that simplify deployment and reduce the cost of network administration
- Cisco EnergyWise technology to manage energy consumed by connected devices
- An enhanced limited lifetime hardware warranty (E-LLW), providing next-business-day replacement

### Applications and Benefits

The Cisco Catalyst 2960-Plus Series provides cost-effective, enterprise class Ethernet switching for:

- Branch offices, remote sites, and retail locations
- Conventional desktop workspaces
- Building infrastructure, physical security, and other nontraditional access applications

Benefits of the 2960-Plus include:

- Robust quality of service (QoS) that prioritizes voice and critical business applications

- Flexible security features that can limit access to the network and mitigate threats
- Tools that reduce total cost of ownership through simplified operations and automation

## Switch Configurations

Table 1 shows Cisco Catalyst 2960-Plus Series configurations.

**Table 1.** Cisco Catalyst 2960-Plus Series Configurations

Model	10/100 Ethernet Interfaces	Uplink Interfaces	Cisco IOS Software Feature Set	Available PoE Power
Cisco Catalyst 2960-Plus 48PST-L	48	2 SFP and 2 1000BASE-T	LAN Base	370W
Cisco Catalyst 2960-Plus 24PC-L	24	2 (SFP or 1000BASE-T)	LAN Base	370W
Cisco Catalyst 2960-Plus 24LC-L	24	2 (SFP or 1000BASE-T)	LAN Base	123W
Cisco Catalyst 2960-Plus 48TC-L	48	2 (SFP or 1000BASE-T)	LAN Base	-
Cisco Catalyst 2960-Plus 24TC-L	24	2 (SFP or 1000BASE-T)	LAN Base	-
Cisco Catalyst 2960-Plus 48PST-S	48	2 SFP and 2 1000BASE-T	LAN Lite	370W
Cisco Catalyst 2960-Plus 24PC-S	24	2 (SFP or 1000BASE-T)	LAN Lite	370W
Cisco Catalyst 2960-Plus 24LC-S	24	2 (SFP or 1000BASE-T)	LAN Lite	123W
Cisco Catalyst 2960-Plus 48TC-S	48	2 (SFP or 1000BASE-T)	LAN Lite	-
Cisco Catalyst 2960-Plus 24TC-S	24	2 (SFP or 1000BASE-T)	LAN Lite	-

## Robust Security

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

- Features to control access to the network, including Flexible Authentication, 802.1x Monitor Mode, and RADIUS Change of Authorization
- Threat defense features including Port Security, Dynamic ARP Inspection, and IP Source Guard
- Private VLAN Edge to provide isolation between switch ports

For more information about Cisco security solutions, visit [cisco.com/go/trustsec](http://cisco.com/go/trustsec).

## Enterprise-Class Quality of Service

The Cisco 2960-Plus Series Switches offer 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:

- Four egress queues per port 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 64 aggregate or individual policers per port
- 802.1p class of service (CoS) and differentiated services code point (DSCP) field 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

## 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** enables zero-touch deployment by providing automated Cisco IOS Software image installation and configuration when new switches are connected to the network.

**Cisco Auto Smartports** enables automatic configuration of switch ports as devices connect to the switch, with settings optimized for the device type.

**Cisco Smart Troubleshooting** is an extensive array of diagnostic commands and system health checks within the switch, including Smart Call Home.

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

## Cisco EnergyWise

Cisco EnergyWise™ empowers IT teams to measure and manage the power consumed by devices connected to the network, providing measurable energy savings and reduced greenhouse gas emissions. 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-Plus Series Switches.

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

## Power over Ethernet

Cisco Catalyst 2960-Plus switches support IEEE 802.3af Power over Ethernet (PoE) to deliver lower total cost of ownership for deployments that incorporate Cisco IP phones, Cisco Aironet® wireless access points, or other standards-compliant 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. Table 2 shows the total PoE power available with each 2960-Plus model.

**Table 2.** Switch PoE Power Capacity

Switch Model	Maximum Number of PoE (IEEE 802.3af) Ports*	Available PoE Power
Cisco Catalyst 2960-Plus 48PST-L	24 ports up to 15.4W	370W
Cisco Catalyst 2960-Plus 24PC-L	24 ports up to 15.4W	370W
Cisco Catalyst 2960-Plus 24LC-L	8 ports up to 15.4W	123W
Cisco Catalyst 2960-Plus 48PST-S	24 ports up to 15.4W	370W
Cisco Catalyst 2960-Plus 24PC-S	24 ports up to 15.4W	370W
Cisco Catalyst 2960-Plus 24LC-S	8 ports up to 15.4W	123W

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

## Network Management

The Cisco Catalyst 2960-Plus Series Switches offer a superior CLI for detailed configuration and administration. 2960-Plus 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 PC-based network management application designed for small and medium-sized business (SMB) networks with up to 250 users, 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).

## Cisco IOS Software

Cisco Catalyst 2960-Plus Series Switches are available with the LAN Base and LAN Lite feature sets. LAN Lite models provide reduced functionality and scalability for small deployments with basic requirements.

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

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

## Technical Specifications

Tables 3 through 10 list information about hardware, performance, forwarding performance, mechanical and environmental specifications, connectors and interfaces, management and standards support, voltage and power ratings, and power consumption, respectively.

**Table 3.** Cisco Catalyst 2960-Plus Series Hardware

Hardware Specifications	
Flash memory	64 MB
DRAM	128 MB

**Table 4.** Cisco Catalyst 2960-Plus Series Performance

Performance and Scalability	Performance and Scalability	
	LAN Base (-L) Models	LAN Lite (-S) Models
Forwarding bandwidth	16 Gbps	16 Gbps
Maximum active VLANs	255	64
VLAN IDs available	4K	4K
Maximum transmission unit (MTU) - L3 packet	9000 bytes	9000 bytes
Jumbo frame - Ethernet frame	9018 bytes	9018 bytes

\* Switching bandwidth is full-duplex capacity.

**Table 5.** Cisco Catalyst 2960-Plus Series Forwarding Performance

Forwarding Rate: 64-Byte L3 Packets, Millions of packets per second	
Cisco Catalyst 2960-Plus 48PST-L	13.1
Cisco Catalyst 2960-Plus 24PC-L	6.5
Cisco Catalyst 2960-Plus 24LC-L	6.5
Cisco Catalyst 2960-Plus 48TC-L	10.1
Cisco Catalyst 2960-Plus 24TC-L	6.5
Cisco Catalyst 2960-Plus 48PST-S	13.1
Cisco Catalyst 2960-Plus 24PC-S	6.5
Cisco Catalyst 2960-Plus 24LC-S	6.5
Cisco Catalyst 2960-Plus 48TC-S	10.1
Cisco Catalyst 2960-Plus 24TC-S	6.5

**Table 6.** Cisco Catalyst 2960-Plus Mechanical and Environmental Specifications

Dimensions (H x W x D)		
Model	Inches	Centimeters
Cisco Catalyst 2960-Plus 48PST-L	1.73 x 17.70 x 13.07	4.4 x 45.0 x 33.2
Cisco Catalyst 2960-Plus 24PC-L		
Cisco Catalyst 2960-Plus 24LC-L		
Cisco Catalyst 2960-Plus 48TC-L	1.73 x 17.70 x 9.52	4.4 x 45.0 x 24.2
Cisco Catalyst 2960-Plus 24TC-L		
Cisco Catalyst 2960-Plus 48PST-S	1.73 x 17.70 x 13.07	4.4 x 45.0 x 33.2
Cisco Catalyst 2960-Plus 24PC-S		
Cisco Catalyst 2960-Plus 24LC-S		
Cisco Catalyst 2960-Plus 48TC-S	1.73 x 17.70 x 9.52	4.4 x 45.0 x 24.2
Cisco Catalyst 2960-Plus 24TC-S		
Weight		
Model	Pounds	Kilograms
Cisco Catalyst 2960-Plus 48PST-L	12	5.4
Cisco Catalyst 2960-Plus 24PC-L	12	5.4
Cisco Catalyst 2960-Plus 24LC-L	10	4.5
Cisco Catalyst 2960-Plus 48TC-L	8	3.6
Cisco Catalyst 2960-Plus 24TC-L	8	3.6
Cisco Catalyst 2960-Plus 48PST-S	12	5.4
Cisco Catalyst 2960-Plus 24PC-S	12	5.4
Cisco Catalyst 2960-Plus 24LC-S	10	4.5
Cisco Catalyst 2960-Plus 48TC-S	8	3.6
Cisco Catalyst 2960-Plus 24TC-S	8	3.6
Environmental Ranges		
	Fahrenheit	Centigrade
Operating temperature up to 5000 ft (1500 m)	23° to 113°F	-5° to 45°C
Operating temperature up to 10,000 ft (3000 m)	23° to 104°F	-5° to 40°C
Short-term exception at sea level <sup>*</sup>	23° to 131°F	-5° to 55°C



Short-term exception up to 5000 feet (1500 m) *	23° to 122°F	-5° to 50°C		
Short-term exception up to 10,000 feet (3000 m) *	23° to 113°F	-5° to 45°C		
Short-term exception up to 13,000 feet (4000 m) *	23° to 104°F	-5° to 40°C		
Storage temperature up to 15,000 feet (4573 m)	23° to 158°F	-25° to 70°C		
	<b>Feet</b>	<b>Meters</b>		
Operating altitude	Up to 10,000	Up to 3,000		
Storage altitude	Up to 13,000	Up to 4,000		
Operating relative humidity	10% to 95% noncondensing			
Storage relative humidity	10% to 95% noncondensing			
<b>Acoustic Noise</b>				
Measured per ISO 7779 and declared per ISO 9296.				
Bystander positions operating mode at 25°C ambient.				
	<b>Sound Pressure, dBA</b>		<b>Sound Power, dbA</b>	
<b>Model</b>	<b>Typical, LpAm</b>	<b>Maximum, LpAD</b>	<b>Typical, LwA</b>	<b>Maximum, LwAD</b>
Cisco Catalyst 2960-Plus 48PST-L	41	44	51	54
Cisco Catalyst 2960-Plus 24PC-L	43	46	53	56
Cisco Catalyst 2960-Plus 24LC-L	43	46	53	56
Cisco Catalyst 2960-Plus 48TC-L	33	36	43	46
Cisco Catalyst 2960-Plus 24TC-L	33	36	43	46
Cisco Catalyst 2960-Plus 48PST-S	41	44	51	54
Cisco Catalyst 2960-Plus 24PC-S	43	46	53	56
Cisco Catalyst 2960-Plus 24LC-S	43	46	53	56
Cisco Catalyst 2960-Plus 48TC-S	33	36	43	46
Cisco Catalyst 2960-Plus 24TC-S	33	36	43	46
<b>Predicted Reliability</b>				
<b>Model</b>	<b>MTBF in thousands of hours**</b>			
Cisco Catalyst 2960-Plus 48PST-L	312			
Cisco Catalyst 2960-Plus 24PC-L	382			
Cisco Catalyst 2960-Plus 24LC-L	498			
Cisco Catalyst 2960-Plus 48TC-L	623			
Cisco Catalyst 2960-Plus 24TC-L	667			
Cisco Catalyst 2960-Plus 48PST-S	312			
Cisco Catalyst 2960-Plus 24PC-S	381			
Cisco Catalyst 2960-Plus 24LC-S	498			
Cisco Catalyst 2960-Plus 48TC-S	623			
Cisco Catalyst 2960-Plus 24TC-S	667			

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

\*\* Based on Telcordia SR-332 Issue 3 methodology.

**Table 7.** Connectors and Interfaces

<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>
---



ces
<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>
<ul style="list-style-type: none"> <li>Per-port status: Link integrity, disabled, activity, speed, and full duplex</li> <li>System status, Port Status, RPS, link duplex, PoE, and link speed</li> </ul>
<p>Cisco Catalyst console cables:</p> <ul style="list-style-type: none"> <li>CAB-CONSOLE-RJ45 Console cable 6 ft. with RJ-45</li> </ul>
<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 8.** Management and Standards Support

Category	Specification
Management	BRIDGE-MIB
	CISCO-CABLE-DIAG-MIB
	CISCO-CDP-MIB
	CISCO-CLUSTER-MIB
	CISCO-CONFIG-COPY-MIB
	CISCO-CONFIG-MAN-MIB
	CISCO-DHCP-SNOOPING-MIB
	CISCO-ENTITY-VENDORTYPE-OID-MIB
	CISCO-ENVMON-MIB
	CISCO-ERR-DISABLE-MIB
	CISCO-FLASH-MIB
	CISCO-FTP-CLIENT-MIB
	CISCO-IGMP-FILTER-MIB
	CISCO-IMAGE-MIB
	CISCO-IP-STAT-MIB
	CISCO-LAG-MIB
	CISCO-MAC-NOTIFICATION-MIB
	CISCO-MEMORY-POOL-MIB
	CISCO-PAGP-MIB
	CISCO-PING-MIB
	CISCO-POE-EXTENSIONS-MIB
	CISCO-PORT-QOS-MIB
	CISCO-PORT-SECURITY-MIB
	CISCO-PORT-STORM-CONTROL-MIB
	CISCO-PRODUCTS-MIB
	CISCO-PROCESS-MIB
	CISCO-RTTMON-MIB
	CISCO-SMI-MIB
	CISCO-STP-EXTENSIONS-MIB
	CISCO-SYSLOG-MIB
	CISCO-TC-MIB
	CISCO-TCP-MIB
	CISCO-UDLDP-MIB
CISCO-VLAN-IFTABLE	
RELATIONSHIP-MIB	
CISCO-VLAN-MEMBERSHIP-MIB	
CISCO-VTP-MIB	
ENTITY-MIB	
ETHERLIKE-MIB	
IEEE8021-PAE-MIB	
IEEE8023-LAG-MIB	
IF-MIB	
INET-ADDRESS-MIB	
OLD-CISCO-CHASSIS-MIB	
OLD-CISCO-FLASH-MIB	
OLD-CISCO-INTERFACES-MIB	
OLD-CISCO-IP-MIB	
OLD-CISCO-SYS-MIB	
OLD-CISCO-TCP-MIB	
OLD-CISCO-TS-MIB	
RFC1213-MIB	
RMON-MIB	
RMON2-MIB	
SNMP-FRAMEWORK-MIB	
SNMP-MPD-MIB	
SNMP-NOTIFICATION-MIB	
SNMP-TARGET-MIB	
SNMPv2-MIB	
TCP-MIB	
UDP-MIB	
ePM MIB	

For an updated list of supported MIBs, refer to the MIB Locator at [cisco.com/go/mibs](http://cisco.com/go/mibs).

Category	Specification
<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</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>
<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>• 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> </ul>
	<ul style="list-style-type: none"> <li>• RFC 1901 - SNMP v2C</li> <li>• RFC 1902-1907 - SNMP v2</li> <li>• RFC 1981 - Path MTU Discovery for 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 Adrrs</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 9.** Voltage and Power Ratings

Input Voltage and Current			
Model	Voltage (Autoranging)	Current (Amperes)	Frequency
Cisco Catalyst 2960-Plus 48PST-L	100 to 240 VAC	4.0 - 2.0	50 to 60Hz
Cisco Catalyst 2960-Plus 24PC-L		4.0 - 2.0	
Cisco Catalyst 2960-Plus 24LC-L		1.4 - 0.8	
Cisco Catalyst 2960-Plus 48TC-L		0.6 - 0.3	
Cisco Catalyst 2960-Plus 24TC-L		0.4 - 0.2	
Cisco Catalyst 2960-Plus 48PST-S		4.0 - 2.0	
Cisco Catalyst 2960-Plus 24PC-S		4.0 - 2.0	
Cisco Catalyst 2960-Plus 24LC-S		1.4 - 0.8	
Cisco Catalyst 2960-Plus 48TC-S		0.6 - 0.3	
Cisco Catalyst 2960-Plus 24TC-S		0.4 - 0.2	
Power Rating (kVA)			
Cisco Catalyst 2960-Plus 48PST-L	0.46		
Cisco Catalyst 2960-Plus 24PC-L	0.43		
Cisco Catalyst 2960-Plus 24LC-L	0.16		

Cisco Catalyst 2960-Plus 48TC-L	0.04	
Cisco Catalyst 2960-Plus 24TC-L	0.03	
Cisco Catalyst 2960-Plus 48PST-S	0.46	
Cisco Catalyst 2960-Plus 24PC-S	0.43	
Cisco Catalyst 2960-Plus 24LC-S	0.16	
Cisco Catalyst 2960-Plus 48TC-S	0.04	
Cisco Catalyst 2960-Plus 24TC-S	0.02	
<b>DC Input Voltages (RPS Input)</b>		
Cisco Catalyst 2960-Plus 48PST-L	3A at 12V	7A at -52V
Cisco Catalyst 2960-Plus 24PC-L	2A at 12V	7A at -52V
Cisco Catalyst 2960-Plus 24LC-L	2A at 12V	3A at -52V
Cisco Catalyst 2960-Plus 48TC-L	3A at 12V	-
Cisco Catalyst 2960-Plus 24TC-L	2A at 12V	-
Cisco Catalyst 2960-Plus 48PST-S	3A at 12V	7A at -52V
Cisco Catalyst 2960-Plus 24PC-S	2A at 12V	7A at -52V
Cisco Catalyst 2960-Plus 24LC-S	2A at 12V	3A at -52V
Cisco Catalyst 2960-Plus 48TC-S	3A at 12V	-
Cisco Catalyst 2960-Plus 24TC-S	2A at 12V	-

**Table 10.** Power Consumption

Power Consumption, Watts				
Model	0% traffic	10% traffic	100% traffic	ATIS weighted average
Cisco Catalyst 2960-Plus 48PST-L	51.1	50.8	51.4	50.9
Cisco Catalyst 2960-Plus 24PC-L	35.4	35.3	35.6	35.3
Cisco Catalyst 2960-Plus 24LC-L	25.9	25.7	26.1	25.8
Cisco Catalyst 2960-Plus 48TC-L	30.4	30.2	30.6	30.2
Cisco Catalyst 2960-Plus 24TC-L	18.4	18.3	18.6	18.3
Cisco Catalyst 2960-Plus 48PST-S	50.8	50.3	51.1	50.5
Cisco Catalyst 2960-Plus 24PC-S	35.0	34.8	35.2	34.9
Cisco Catalyst 2960-Plus 24LC-S	25.9	25.7	26.1	25.8
Cisco Catalyst 2960-Plus 48TC-S	29.9	29.7	30.2	29.8
Cisco Catalyst 2960-Plus 24TC-S	18.8	18.7	19.1	18.8

\* Using ATIS-0600015.03.2009 methodology.

**Disclaimer:** All power consumption numbers were measured under controlled laboratory conditions and are provided as an estimate.

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 because a significant portion of the load is dissipated in the endpoints.

Table 11 provides safety and compliance information.

**Table 11.** Safety and Compliance

Category	Certifications
<b>Regulatory Compliance</b>	Products should comply with CE Marking per directives 2004/108/EC and 2006/95/EC
<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
<b>EMC - Immunity</b>	EN55024 CISPR24 EN300386 KN24
<b>Environmental</b>	Reduction of Hazardous Substances (RoHS) including Directive 2011/65/EU
<b>Telco</b>	

## Cisco Enhanced Limited Lifetime Hardware Warranty

Cisco Catalyst 2960-Plus 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 (Table 12), visit [cisco.com/go/warranty](http://cisco.com/go/warranty).

**Table 12.** Warranty Terms

Cisco Enhanced Limited Lifetime Hardware Warranty	
<b>Device covered</b>	Applies to all Cisco Catalyst 2960-Plus Series Switches.
<b>Warranty duration</b>	As long as the original end user continues to own or use the product.
<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-Plus 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).

ed Lifetime Hardware Warranty	
<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-Plus 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 Update Policy

Software updates for the Cisco Catalyst 2960-Plus are available for free to registered customers at [cisco.com/go/support](http://cisco.com/go/support).

For more information about the Cisco Catalyst software update policy, visit [http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps4324/product\\_bulletin\\_c25-696974\\_ps10745\\_Products\\_Bulletin.html](http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps4324/product_bulletin_c25-696974_ps10745_Products_Bulletin.html).

## Technical Support and Services

Table 13 provides information about relevant technical services.

**Table 13.** Technical Services Available for Cisco Catalyst 2960-Plus Series Switches

<b>Cisco SMARTnet Service</b>	
<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>	
<b>Cisco Smart Foundation Service</b>	
<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>	
<b>Cisco Smart Care Service</b>	
<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>	
<b>Cisco SP Base Service</b>	
<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>	
<b>Cisco Focused Technical Support Services</b>	
Three levels of premium, high-touch services are available:	<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>
Valid Cisco SMARTnet <sup>®</sup> or SP Base contracts are required on all network equipment.	

<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; 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

Tables 14 through 18 provide information about ordering, accessories, redundant power supplies, SFP modules, and power cords, respectively.

**Table 14.** Cisco Catalyst 2960-Plus Series Switches Ordering Information

Part Number	10/100 Ethernet Interfaces	Optical Interfaces	Cisco IOS Software Feature Set	Available PoE Power
WS-C2960+48PST-L	48	2 SFP and 2 1000BASE-T	LAN Base	370W
WS-C2960+24PC-L	24	2 (SFP or 1000BASE-T)	LAN Base	370W
WS-C2960+24LC-L	24	2 (SFP or 1000BASE-T)	LAN Base	123W
WS-C2960+48TC-L	48	2 (SFP or 1000BASE-T)	LAN Base	-
WS-C2960+24TC-L	24	2 (SFP or 1000BASE-T)	LAN Base	-
WS-C2960+48PST-S	48	2 SFP and 2 1000BASE-T	LAN Lite	370W
WS-C2960+24PC-S	24	2 (SFP or 1000BASE-T)	LAN Lite	370W
WS-C2960+24LC-S	24	2 (SFP or 1000BASE-T)	LAN Lite	123W
WS-C2960+48TC-S	48	2 (SFP or 1000BASE-T)	LAN Lite	-
WS-C2960+24TC-S	24	2 (SFP or 1000BASE-T)	LAN Lite	-

**Table 15.** Cisco Catalyst 2960-Plus Accessories

Part Numbers	Description
CAB-CONSOLE-RJ45	Console cable 6 ft with RJ45
RCKMNT-1RU=	Spare rack-mount kit for Cisco Catalyst 2960 and 2960-Plus Series for 19- and 24-inch racks
RCKMNT-REC-1RU=	1 RU recessed rack-mount kit for Cisco Catalyst 2960 and 2960-Plus Series
PWR-CLP	Power cable restraining clip

**Table 16.** Cisco Catalyst 2960-Plus Redundant Power Supply Options

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

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

**Table 17.** Cisco Catalyst 2960-Plus SFP Modules

es

For the list of supported SFP and SFP+ modules, visit [cisco.com/en/US/products/hw/modules/ps5455/products\\_device\\_support\\_tables\\_list.html](https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html).





**Table 18.** Power Cords for Cisco Catalyst 2960-Plus Series

Part Numbers	Description
<b>CAB-AC</b>	AC Power Cord (US, Canada), C13, NEMA 5-15P, 2.5m
<b>CAB-ACE</b>	AC Power Cord (Europe), C13, CEE 7, 1.5m
<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>	AC Power Cord (China), C13, PRC/3 GB2099/GB1002
<b>CAB-JPN</b>	AC Power Cord (Japan), C13, Japan 2-prong, 1.8m
<b>CAB-IND-10A</b>	AC Power Cord (India), C13, IS1293, 2.5m
<b>CAB-ACBZ-10A</b>	AC Power Cord (Brazil), C13, BR-3-20, 10A
<b>CAB-ACSA</b>	AC Power Cord (South Africa), C15, SABS 164-1, 1.8m

## Contact Cisco

For more information about Cisco products, contact:

- United States and Canada: (toll free) 800 553-NETS (6387)
- Europe: 32 2 778 4242
- Australia: 612 9935 4107
- Other: 408 526-7209
- URL: [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)

## Appendix E. Cisco Industrial Ethernet 3000 Series Switches

Data Sheet



### Cisco Industrial Ethernet 3000 Series Switches

#### Product Overview

The Cisco<sup>®</sup> Industrial Ethernet 3000 (IE3000) Series Switches are a new family of switches that provide a rugged, easy-to-use, secure switching infrastructure for harsh environments. The Cisco IE3000 family features industrial design and compliance; tools for ease of deployment, management, and replacement; and network security based on open standards. The Cisco IE3000 is an ideal product for Industrial Ethernet applications, including factory automation, intelligent transportation systems (ITSs), substations, and other deployments in harsh environments.

The Cisco IE3000 offers:

- Design for Industrial Ethernet applications, including extended environmental, shock/vibration, and surge ratings; a complete set of power input options; convection cooling; and DIN-rail or 19" rack mounting
- Support for 300 different hardware configurations
- Easy setup and management using the Cisco Device Manager Web interface and supporting tools, including Cisco Network Assistant and CiscoWorks
- Easy switch replacement using removable memory, allowing the user to replace a switch without having to reconfigure
- High availability, guaranteed determinism, and reliable security using Cisco IOS<sup>®</sup> Software
- Recommended software configurations for industrial applications that can be applied at the touch of a button
- Compliance to a wide range of Industrial Ethernet specifications covering industrial automation, ITS, substation, railway, and other markets
- Support for IEEE1588, a timing protocol with nanosecond-level precision for high-performance applications

#### Configurations

The Cisco IE3000 Series comprises the following products (refer to Table 1):

- **Cisco IE3000-4TC:** Industrial Ethernet switch with four Ethernet 10/100 ports and two dual-purpose uplink ports (a dual-purpose port has one 10/100/1000BaseTX port and one Small Form-Factor Pluggable [SFP] port, port active)
- **Cisco IE3000-8TC:** Industrial Ethernet switch with eight Ethernet 10/100 ports and two dual-purpose uplink ports
- **Cisco IE3000-8FE:** Expansion module for Cisco IE3000-4TC and Cisco IE3000-8TC with eight Ethernet 10/100 ports

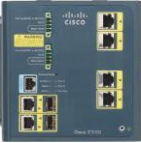




- **Cisco IE3000-8FX:** Expansion module for Cisco IE3000-4TC and Cisco IE3000-8TC with eight 100BaseFX ports
- **Cisco IE3000-PWR:** Expansion module supporting AC and extended DC power inputs

## Solution Specifications



The Cisco IE3000 Series software, based on Cisco IOS Software, is a rich suite of intelligent services, supporting high availability, quality of service (QoS), and security features. The SFP-based uplink ports accommodate a range of industrial-grade SFP transceivers, including 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX, 100BASE-FX, and 100BASE-LX10.

**Table 1.** Cisco IE3000 Switches

Description	Specification
<b>Cisco IE3000-4TC</b> 	4 Ethernet 10/100 ports and 2 Dual-Purpose Uplinks (Each Dual Purpose Uplink port has one 10/100/1000 Ethernet Port and one SFP based Gigabit Ethernet port, one port active) Each switch supports two (2) Cisco IE3000-8FE modules, one (1) Cisco IE3000-8FX module, or one (1) Cisco IE3000-8FE module and one (1) Cisco IE3000-8FX module
<b>Cisco IE3000-8TC</b> 	8 Ethernet 10/100 ports and 2 Dual-Purpose Uplinks (Each Dual Purpose Uplink port has one 10/100/1000 Ethernet Port and one SFP based Gigabit Ethernet port, one port active) Each switch supports two (2) Cisco IE3000-8FE modules, one (1) Cisco IE3000-8FX module, or one (1) Cisco IE3000-8FE module and one (1) Cisco IE3000-8FX module
<b>Cisco IE3000-8FE</b> 	Expansion Module for Cisco IE3000-4TC and Cisco IE3000-8TC Switches, 8 10/100 TX ports
<b>Cisco IE3000-8FX</b> 	Expansion Module for Cisco IE3000-4TC and Cisco IE3000-8TC Switches, 8 100 FX ports
<b>Cisco IE3000-PWR</b> 	Expansion Power Module for Cisco IE3000-4TC and Cisco IE3000-8TC Switches, supports 110/220VAC and 90-300VDC (base switches support 18VDC-60VDC)



## Industrial Ethernet Applications

The new Cisco IE3000 Series is an ideal product for a variety of Industrial Ethernet applications:

- **Industrial automation:** The Cisco IE3000 is designed to support a wide array of Industrial Ethernet protocols for automation. The Cisco IE3000 features a programmable logic controller (PLC) form-factor design with extended environmental ratings, convection cooling, DIN-rail mounting, redundant 24VDC power input, alarm relays, and surge/noise immunity. The Cisco IE3000 software and configuration tools allow for easy setup, optimized for Industrial Ethernet applications, including Ethernet/IP, ProfiNet, Modbus TCP, FoundationFieldbus High-Speed Ethernet (FFB HSE), and others. Multicast control, traffic prioritization, and security features are specified in default templates recommended for these protocols.
- **ITSs:** The Cisco IE3000 supports ITS and other applications for outdoor video and traffic or transportation systems control. The switch supports compliance to NEMA TS-2, a variety of gigabit fiber uplinks, and AC and DC power input options, while the Cisco IOS Software supports critical ITS features, including virtual LAN (VLAN), QoS, Internet Group Management Protocol (IGMP) snooping, and security access control lists (ACLs).
- **Substations:** The Cisco IE3000 is fully compliant to substation automation specifications, including IEC61850 and IEEE1613. The switch supports high-speed ring recovery; fiber access and uplink ports; and AC, 48VDC, and 125VDC power input options for the substation environments.
- **Other applications:** The Cisco IE3000 can be deployed in railway, military, metro Ethernet, and other applications requiring unique environmental, form factor, or power inputs in harsh environments.

Table 1 gives the features and benefits of the Cisco IE3000 Series. Table 2 gives the hardware specifications, and Table 3 gives the power specifications. Table 4 lists the management and standards support, and Table 5 provides the safety and compliance information.

**Table 2.** Features and Benefits of Cisco IE3000 Series

Category	Feature/Benefit
<b>Designed for Industrial Applications</b>	<p>Extended temperature, vibration, shock and surge, and noise immunity ratings comply to specifications for automation, ITS, and substation environments.</p> <p>Compact, PLC-style form factor is ideal for deployment in industrial environments.</p> <p>DIN-rail, wall, and 19" rack mount options allow for deployments in a variety of control systems.</p> <p>24/48/125VDC and 100-220VAC power input options cover a wide range of power requirements for Industrial Ethernet applications.</p> <p>Up to 300 deployment configurations, supporting a range of access port densities, copper and fiber uplinks, fiber access ports, and power input delivers flexibility in deployment.</p> <p>Support for SFP modules provides uplink connectivity supporting 100BASE-LX, 100BASE-FX, 1000BASE-SX, 1000BASE-LX, and 1000BASE-ZX options.</p> <p>Alarm relay contacts can be used for an external alert system.</p>





Category	Feature/Benefit
<b>Ease of Deployment, Management, and Replacement</b>	<p>Cisco Express Setup simplifies initial configuration with a Web browser, eliminating the need for more complex terminal emulation programs.</p> <p>Cisco Smartports templates provide the option to apply a default global or interface-level macro with a recommended configuration, allowing the user to easily set up the switch in a configuration optimized for the specific application.</p> <ul style="list-style-type: none"> <li>● Smartports templates for Ethernet/IP provide an optimized setup for these Industrial Ethernet protocols at the touch of a button.</li> <li>● Swappable Flash memory is ideal for quick and easy switch replacement. Memory can be moved from one switch to another, so a switch can be replaced without the need to reconfigure software features.</li> <li>● The Common Industrial Protocol (CIP) management objects are supported. The including a custom profile for primary Ethernet switch features. The Cisco IE3000 can be managed by CIP-based management tools, allowing the user to manage an entire industrial automation system with one tool.</li> <li>● PROFINET IO enables the Cisco IE3000 to exchange data, alarms and diagnostics information with the PROFINET automation controllers and IO devices.</li> <li>● Simple Network Management Protocol (SNMP) (v1/v2/v3) support allows for management using traditional IT-based management tools including CiscoWorks.</li> <li>● Cisco Network Assistant is a no-charge, Windows-based application that simplifies the administration of networks of up to 250 users. It supports the Cisco IE3000 and a wide range of Cisco Catalyst<sup>®</sup> intelligent switches. With Cisco Network Assistant, users can manage Cisco Catalyst switches and launch the device managers of Cisco integrated services routers and Cisco Aironet<sup>®</sup> WLAN access points. Configuration wizards need just a few user inputs to automatically configure the switch to optimally handle different types of traffic: control, voice, video, multicast, and high-priority data.</li> </ul>
<b>Availability and Scalability</b>	<p>Virtual LANs (VLANs) allow for logical segmentation for a network for optimal use of bandwidth.</p> <p>QoS classifies and prioritizes data, guaranteeing determinism for mission-critical data.</p> <p>IGMPv3 snooping provides fast client joins and leaves of multicast streams and limits bandwidth-intensive traffic to only the requestors. An additional querier allows this operation in a Layer 2 only environment.</p> <p>IGMP filtering provides multicast authentication by filtering out no subscribers and limits the number of concurrent multicast streams available per port.</p> <p>Per-port broadcast, multicast, and unicast storm control prevents faulty end stations from degrading overall systems performance.</p> <p>IEEE 802.1d Spanning Tree Protocol support for redundant backbone connections and loop-free networks simplifies network configuration and improves fault tolerance.</p> <p>Resilient Ethernet Protocol (REP) provides network redundancy of up to 200 nodes at a convergence speed of 50ms or less.</p>
<b>Security</b>	<p>IEEE 802.1x with VLAN assignment, guest VLAN, and voice VLAN allows dynamic port-based security, providing user authentication.</p> <p>Port-based ACLs for Layer 2 interfaces allow application of security policies on individual switch ports.</p> <p>MAC address filtering prevents the forwarding of any type of packet with a matching MAC address.</p> <p>Secure Shell (SSH) Protocol v2 and SNMPv3 provide network security by encrypting administrator traffic during Telnet and SNMP sessions. SSHv2 and the cryptographic version of SNMPv3 require a special cryptographic software image because of U.S. export restrictions.</p> <p>TACACS+ and RADIUS authentication enable centralized control of the switch and restrict unauthorized users from altering the configuration.</p> <p>MAC address notification allows administrators to be notified of users added to or removed from the network.</p> <p>Dynamic Host Configuration Protocol (DHCP) snooping allows administrators to help ensure consistent mapping of IP to MAC addresses. This can be used to prevent attacks that attempt to poison the DHCP binding database, and to rate limit the amount of DHCP traffic that enters a switch port.</p> <p>DHCP Interface Tracker (Option 82) augments a host IP address request with the switch port ID.</p> <p>Port security secures the access to an access or trunk port based on MAC address.</p> <p>After a specific time frame, the aging feature removes the MAC address from the switch to allow another device to connect to the same port.</p> <p>Trusted Boundary provides the ability to trust the QoS priority settings if an IP phone is present and to disable the trust setting if the IP phone is removed, thereby preventing a malicious user from overriding prioritization policies in the network.</p> <p>Up to 512 ACLs are supported, with two profiles: Security (384 Security ACL entries and 128 QoS policies), and QoS (128 Security ACL entries and 384 QoS policies).</p>



**Table 3.** Cisco IE3000 Series Switch Hardware

Description	Specification
<b>Performance</b>	Wire-speed switching 128 MB DRAM 64 MB Flash memory Configurable up to 8000 MAC addresses Configurable up to 255 IGMP groups Configurable maximum transmission unit (MTU) of up to 9000 bytes, with a maximum Ethernet frame size of 9018 bytes (Jumbo frames) for bridging on Gigabit Ethernet ports, and up to 1998 bytes for bridging of Multiprotocol Label Switching (MPLS) tagged frames on both 10/100 and 10/100/1000 ports
<b>Connectors and Cabling</b>	10BASE-T ports: RJ-45 connectors, two-pair Category 3, 4, or 5 unshielded twisted-pair (UTP) cabling 100BASE-TX ports: RJ-45 connectors, two-pair Category 5 UTP cabling 1000BASE-T ports: RJ-45 connectors, four-pair Category 5 UTP cabling 1000BASE-SX, -LX/LH, -ZX SFP-based ports: LC fiber connectors (single/multimode fiber) 100BASE-LX10, -FX: LC fiber connectors (single/multimode fiber)
<b>Power Connectors</b>	The internal power supply supports voltages between 18VDC and 60VDC. The extended power adapter (Cisco IE3000-PWR) supports 90-300VAC and 90-300VDC. Use the supplied cable to connect the extended power adapter to the switch power input.
<b>Indicators</b>	Per-port status LED: Link integrity, disabled, activity, speed, full-duplex indications System-status LED: System, link status, link duplex, link speed, indications
<b>Dimensions (H x W x D)</b>	Cisco IE3000-4TC: 6.0"W x 5.8"H x 4.4"D (152mm H x 147mm W x 112mm D) Cisco IE3000-8TC: 6.0"W x 5.8"H x 4.4"D (152mm H x 147mm W x 112mm D) Cisco IE3000-8FE: 3.8"W x 5.8"H x 4.4"D (97mm H x 147mm W x 112mm D) Cisco IE3000-8FX: 3.8"W x 5.8"H x 4.4"D (97mm H x 147mm W x 112mm D) Cisco IE3000-PWR: 3.8"W x 5.8"H x 4.4"D (97mm H x 147mm W x 112mm D)
<b>Weight</b>	Cisco IE3000-4TC: 4.0 lb (3.6 kg) Cisco IE3000-8TC: 4.0 lb (3.6 kg) Cisco IE3000-8FE: 2.0 lb (1.8kg) Cisco IE3000-8FX: 2.0 lb (1.8 kg) Cisco IE3000-PWR: 2.0 lb (1.8 kg)
<b>Environmental Ranges</b>	Operating temperature: 32 to 113°F (–40 to 70°C) Storage temperature: -13 to 158°F (–25 to 70°C) Operating relative humidity: 10 to 95% (condensing) Operating altitude: Up to 10,000 ft (3049m) Storage altitude: Up to 15,000 ft (4573m)
<b>Mean Time Between Failure (MTBF)</b>	Cisco IE3000-4TC: 384,509 Cisco IE3000-8TC: 338,801 Cisco IE3000-8FE: 1,002,788 Cisco IE3000-8FX: 265,492 Cisco IE3000-PWR: 350,000

**Table 4.** Power Specifications for Cisco IE300 Series Switch

Description	Specification
<b>Maximum Power Consumption</b>	31W (Cisco IE3000-4TC and Cisco IE3000-8TC)
<b>Input Voltage and Currents Supported</b>	18-60VDC, (Cisco IE3000-4TC and Cisco IE3000-8TC) 85-265VAC/88-300VDC, 1.3-0.8A, 50-60 Hz (with addition of Cisco IE3000-PWR)
<b>Power Rating</b>	Cisco IE3000-4TC: .05KVA Cisco IE3000-8TC: .05KVA



**Table 5.** Management and Standards Support for Cisco IE3000 Series Switch

Description	Specification	
<b>Standards</b>	100BASE-X (SFP) 1000BASE-X (SFP) 1000BASE-SX 1000BASE-LX/LH 1000BASE-ZX RMON I and II standards SNMPv1, SNMPv2c, and SNMPv3	100BASE-X (SFP) 1000BASE-X (SFP) 1000BASE-SX 1000BASE-LX/LH 1000BASE-ZX RMON I and II standards SNMPv1, SNMPv2c, and SNMPv3

**Table 6.** Compliance Specifications

Description	Specification
<b>Standard Safety Certifications</b>	UL to UL 60950, Third Edition C-UL to CAN/CSA C22.2 No. 60950-00, Third Edition TUV/GS to EN 60950:2000 CB to IEC 60950 with all country deviations NOM to NOM-019-SCFI CE Marking
<b>Industrial Safety Certifications</b>	UL 508 CSA 22.2 / 142 EN60204-1 EN61010-1 EN61131-2 EN61140
<b>Mechanical Stability</b>	Shock—15g (Operational), 30g (Nonoperational)
<b>EMC Interface Immunity</b>	IEC61000-4-2 [Criteria A—Class 2] IEC61000-4-3/ENV50204 [Criteria A] IEC61000-4-4 [Criteria A / Criteria B] IEC61000-4-5 [Criteria B] IEC61000-4-6 [Criteria A]
<b>Standard Electromagnetic Emissions Certifications</b>	FCC Part 15 Class A EN 55022: 1998 (CISPR22) EN 55024: 1998 (CISPR24) VCCI Class A AS/NZS 3548 Class A CE CNS 13438 Class A MIC
<b>Industrial Electromagnetic Emissions Certifications</b>	EN 50081-2 EN 50082-2 EN 61131-2 EN 61326-1 CISPR11
<b>Industry Specifications</b>	IEC 61850-3 (Substations) IEEE1613 (Substations) NEMA TS-2 (ITSs) EN50155 (Railway) ODVA Common Industrial Protocol IEEE 1588v2 PROFINET IO
<b>Hazardous Locations</b>	UL 1602 Class 1, Div 2 A-D CSA 22.2 / 213 Class 1, Div 2 A-D IEC 60079-15 EN 50021—Class 1, Zone 2



Description	Specification
<b>Telco</b>	Common Language Equipment Identifier (CLEI) code
<b>Warranty</b>	One year limited warranty

## Service and Support

Cisco is committed to minimizing total cost of ownership (TCO). The company offers a portfolio of technical support services to help ensure that its products operate efficiently, remain highly available, and benefit from the most up-to-date system software. The services and support programs described in Table 6 are available as part of the Cisco Desktop Switching Service and Support solution and are available directly from Cisco and through resellers.

**Table 7.** Cisco Services and Support Programs

Service and Support	Features	Benefits
<b>Advanced Services</b>		
Cisco Total Implementation Solutions (TIS), available direct from Cisco Cisco Packaged TIS, available through resellers Cisco SMARTnet and SMARTnet Onsite support, available direct from Cisco Cisco Packaged SMARTnet support program, available through resellers Cisco SMB Support Assistant	Project management Site survey, configuration, and deployment Installation, text, and cutover Training Major moves, adds, and changes Design review and product staging Access to software updates 24 hours Web access to technical repositories Telephone support through the Cisco Technical Assistance Center (TAC) Advance replacement of hardware parts	Supplements existing staff Helps ensure that functions meet needs Mitigates risk Helps enable proactive or expedited issue resolution Lowers TCO by taking advantage of Cisco expertise and knowledge Minimizes network downtime

## Ordering Information

Table 7 gives ordering information for the Cisco IE3000 Series.

**Table 8.** Ordering Information for Cisco IE3000 Series

Part Numbers	Description
<b>IE3000-4TC</b>	Industrial Ethernet switch 4 Ethernet 10/100 ports and 2 dual-purpose uplinks (each dual-purpose uplink port has one 10/100/1000 Ethernet port and one SFP-based Gigabit Ethernet port, one port active) Each switch supports two (2) Cisco IE3000-8FE modules, one (1) Cisco IE3000-8FX module, or one (1) Cisco IE3000-8FE module and one (1) Cisco IE3000-8FX module IE Base image Installed
<b>IE3000-8TC</b>	Industrial Ethernet switch 8 Ethernet 10/100 ports and 2 dual-purpose uplinks (each dual-purpose uplink port has one 10/100/1000 Ethernet port and one SFP-based Gigabit Ethernet port, one port active) Each switch supports two (2) Cisco IE3000-8FE modules, one (1) Cisco IE3000-8FX module, or one (1) Cisco IE3000-8FE module and one (1) Cisco IE3000-8FX module IE Base image Installed
<b>IEM-3000-8TM=</b>	Expansion module for Cisco IE3000-4TC and Cisco IE3000-8TC Switches 8 10/100 TX ports
<b>IEM-3000-8TM=</b>	Expansion module for Cisco IE3000-4TC and Cisco IE3000-8TC Switches 8 100 FX ports
<b>PWR-IE3000-AC=</b>	Expansion power module for Cisco IE3000-4TC and Cisco IE3000-8TC Switches Supports 110/220VAC and 90-300VDC (base switches support 18VDC-60VDC)
<b>GLC-LX-SM-RGD</b>	Gigabit Ethernet SFP, LC connector, LH (1Gps single mode) transceiver
<b>GLC-SX-MM-RGD</b>	Gigabit Ethernet SFP, LC connector, SX (1Gps multimode) transceiver
<b>GLC-ZX-SM-RGD</b>	Gigabit Ethernet SFP, LC connector, ZX (1Gbps single mode, 40km) transceiver
<b>GLC-FE-100FX-RGD</b>	Fast Ethernet SFP, LC connector, FX (100Mb/s multimode) transceiver





Part Numbers	Description
<b>GLC-FE-100LX-RGD</b>	Fast Ethernet SFP, LC connector, LX (100Mb/s single mode) transceiver
<b>CAB-SM-LCSC-1M</b>	1m-fiber single-mode LC-to-SC connectors
<b>CAB-SM-LCSC-5M</b>	5m-fiber single-mode LC-to-SC connectors

For more information about Cisco products, contact:

United States and Canada: 800 553-6387

Europe: 32 2 778 4242

Australia: 612 9935 4107

Other: 408 526-7209

World Wide Web URL: <http://www.cisco.com>



**Americas Headquarters**  
 Cisco Systems, Inc.  
 170 West Tasman Drive  
 San Jose, CA 95134-1706  
 USA  
[www.cisco.com](http://www.cisco.com)  
 Tel: 408 526-4000  
 800 553-NETS (6387)  
 Fax: 408 527-0883

**Asia Pacific Headquarters**  
 Cisco Systems, Inc.  
 168 Robinson Road  
 #28-01 Capital Tower  
 Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
 Tel: +65 6317 7777  
 Fax: +65 6317 7799

**Europe Headquarters**  
 Cisco Systems International BV  
 Haarlerbergpark  
 Haarlerbergweg 13-19  
 1101 CH Amsterdam  
 The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
 Tel: +31 0 800 020 0791  
 Fax: +31 0 20 357 1100

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).

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0705R)

