

ENRUTAMIENTO Y CONFIGURACIÓN DE REDES

Ricardo López Bulla

EJE 1

Conceptualicemos

Introducción	3
¿Qué es un dispositivo de interconexión?	4
Adaptadores de red o NIC (<i>network interface card</i>)	7
Características	7
Hubs o concentradores.	8
Características	8
Puente o bridge	9
Características	9
Conmutadores o <i>switches</i>	10
Características	11
Encaminador o <i>router</i>	12
Características	12
Puntos de acceso inalámbrico	13
Características	13
Dispositivos multipropósito	14
Factores de forma del <i>switch</i>	15
¿Qué son las redes conmutadas?	17
Características de las LAN conmutadas	17
Redes convergentes	18
Características	19
¿Qué es Cisco Borderless Network?.	19
Modelo jerárquico de las redes convergentes	20
Capas del diseño jerárquico de redes	21
Bibliografía	22

¿Qué es un dispositivo
de interconexión?



Se conoce como dispositivo de interconexión el elemento que permite comunicar o interconectar dos o más dispositivos y facilita la conexión de **segmentos** y los terminales, característica vital para la comunicación en una red. Estos elementos son la parte del *hardware* dentro de la red.

Estos terminales o dispositivos finales, que suelen llamarse *hosts*, permiten el acceso a la red informática entre dos elementos claves: el usuario y la red. Entre los dispositivos finales encontramos PC (escritorio, portátiles), tabletas, *smartphones*, impresoras, teléfonos con tecnología IP (**VOIP**), cámaras para circuito cerrado, etc.

Introduciéndonos en las redes informáticas encontramos que cada *host* tiene una característica que lo hace único. Vamos a analizar esto con una analogía: cada ser humano sobre la tierra tiene un número de identificación, lo mismo pasa con los *hosts*, pero relacionándolos con una única dirección IP, la cual se aloja en el origen y el destino del mensaje a través de todo el proceso de **encapsulación** y desencapsulación en la red.



Segmentos

Grupo de equipos interconectados dentro de una red informática.

VOIP

Siglas de voice over internet protocol (voz a través de internet). Esta tecnología permite comunicaciones mediante el protocolo IP.

Encapsulación

Proceso que nos permite mantener un orden en el proceso de la comunicación partiendo del origen de los datos hasta su destino, garantizando la entrega del mensaje.

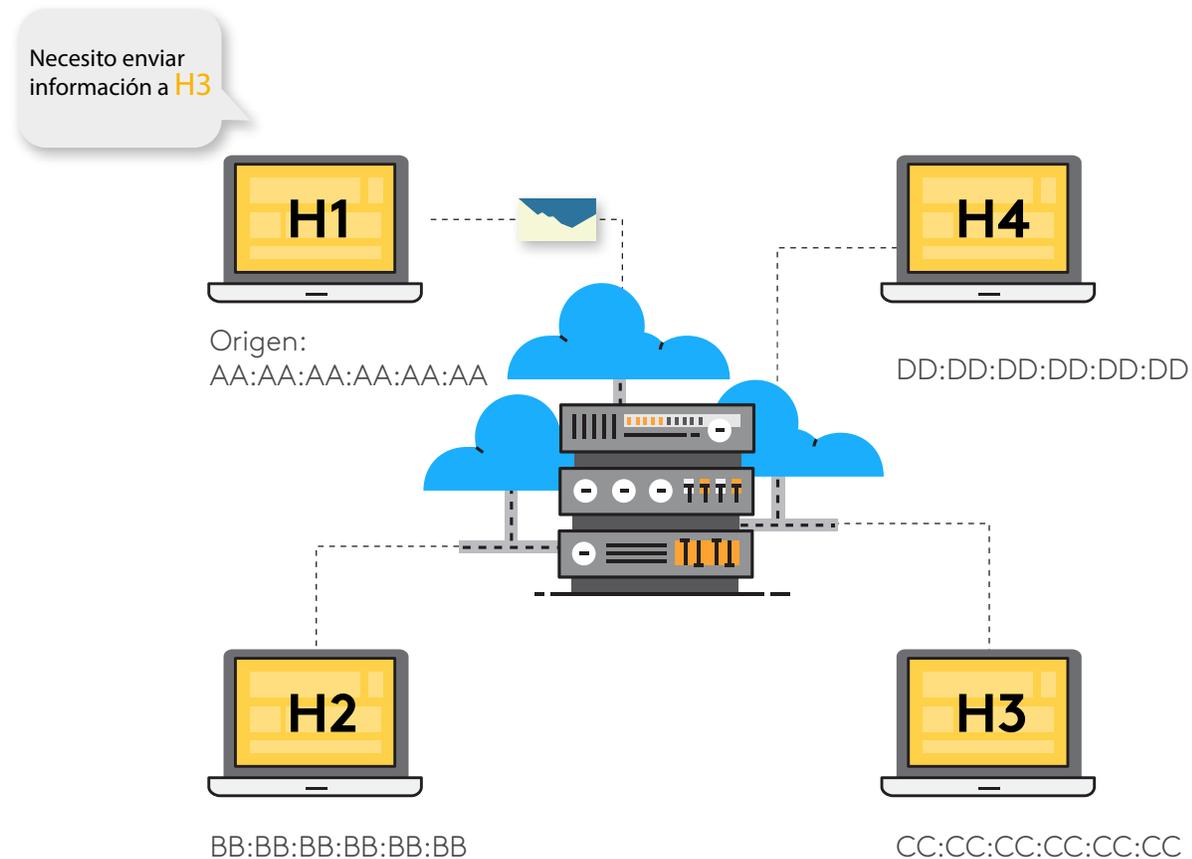


Figura 1.
Fuente: Quintero (2014)

Dentro de la red es necesario conectar dispositivos de origen y destino para que los datos sean transmitidos y poder establecer una comunicación. Esta labor la llevan a cabo los llamados dispositivos intermedios. Se pueden encontrar diversos dispositivos intermedios como: *NIC, hubs, bridge, switches, routers, routers inalámbricos y firewalls*. Cabe resaltar que para que exista el intercambio de información necesitamos unos medios de transmisión, estos pueden guiados (alámbricos) y no guiados (inalámbricos).

Los dispositivos intermedios tienen entre sus objetivos: seleccionar la mejor ruta en la red (*routers*), brindar acceso a los diferentes terminales de la red (*switch*) y garantizar seguridad en la información (*firewall*).



Ejemplo

Ejemplo claro del funcionamiento de estos elementos es una oficina postal o de mensajería. Imagine que usted es el remitente y su jefe el receptor. Lo primero que usted hace es redactar el mensaje y después lo introduce en el sobre. Al marcar el sobre, le coloca los datos del remitente y receptor o destinatario. Sin datos como dirección de origen y destino, código postal, etc., no puede enviar el sobre. Luego, usted procede a llevar el sobre a la oficina postal, donde lo radica con todos los datos mencionados. Inmediatamente, le entregan un desprendible con un radiado, el cual cuenta con un número de referencia. Ahora, usted espera la respuesta al mensaje.



Figura 2. Entrega de sobres en oficina postal
Fuente: Shutterstock/506016142

En este ejemplo podemos relacionar los dispositivos finales e intermedios y su funcionamiento, los cuales analizaremos a continuación.

Adaptadores de red o NIC (network interface card)

Antes de profundizar en los dispositivos es importante tener presente cómo los usuarios accedemos a la red. Lo hacemos a través de las NIC, las cuales se encuentran ubicadas en nuestros PC y nos facilitan conectarnos a la red local.

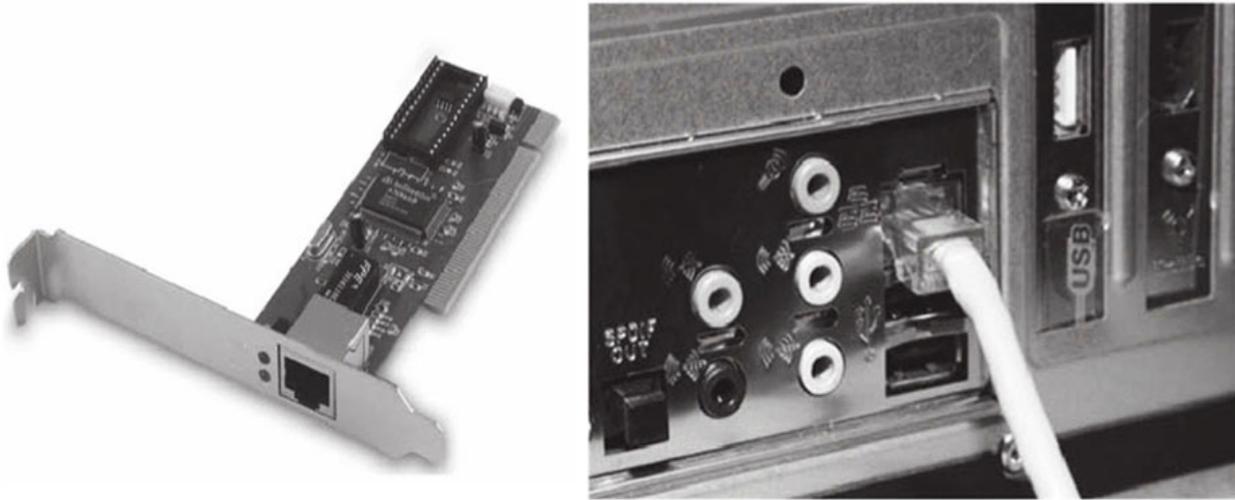


Figura 3.
Fuente: Moreno Pérez (2014)

Características

- La tecnología que manejan estos adaptadores es Ethernet, por lo cual vemos un puerto para conectar la NIC RJ45. Además, tienen una dirección MAC asociada. Esta dirección la podemos apreciar en nuestras PC mediante el comando IPconfig/all dentro del símbolo del sistema. ¿Cómo lo hacemos? Primero vamos a "Inicio", en la opción "Buscar" ingresamos el comando "CMD" seguido de "Enter", inmediatamente ingresamos el comando IPconfig/all y nos arroja nuestra dirección MAC, la cual corresponde a nuestra NIC.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\RYKE-AVILA>ipconfig/all

Windows IP Configuration

Host Name . . . . . : RYKE-AVILA
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Wireless LAN adapter Wireless Network Connection 3:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Virtual WiFi Miniport Adapter #
Physical Address . . . . . : 68-5D-43-E8-66-FF
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wireless Network Connection 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Virtual WiFi Miniport Adapter
Physical Address . . . . . : 68-5D-43-E8-66-FF
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : Intel(R) Centrino(R) Wireless-N 2230
Description . . . . . : Intel(R) Centrino(R) Wireless-N 2230
Physical Address . . . . . : 68-5D-43-E8-66-FF
DHCP Enabled. . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b83c:eb1c:c5c5:dd46x13(Preferred)
IPv4 Address. . . . . : 192.168.164.126(Preferred)
Subnet Mask . . . . . : 255.255.248.0
Lease Obtained. . . . . : sábado, 08 de julio de 2017 02:30:07 p.m.
Lease Expires . . . . . : sábado, 08 de julio de 2017 04:23:21 p.m.
Default Gateway . . . . . : 192.168.168.240
DHCP Servers . . . . . : 19.238.3.82
DHCPv6 IAID . . . . . : 292052291
DHCPv6 Client DUID. . . . . : 00-01-00-01-1F-07-21-50-68-5D-43-E8-66-FF
DNS Servers . . . . . : 200.75.51.132
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter {6DD3D070-F2EC-4C7D-B5A2-E0FF30D262DA}:
```

Figura 4.
Fuente: propia

- Las NIC operan en las capas física y enlace de datos del modelo OSI.
- Las tarjetas de red necesitan un controlador o *driver* para que funcionen con el sistema operativo de la PC. Este lo da el fabricante.
- Las NIC pueden encontrarse para conexiones inalámbricas. Estos adaptadores en la actualidad trabajan en las tecnologías como *bluetooth* y *wifi*. En la figura que veremos a continuación encontraremos una NIC para *wifi* tipo Pcmcia de Linsys.



Figura 5.
Fuente: Moreno Pérez (2014)

Hubs o concentradores

Son elementos de red Ethernet que permiten conectar varios *hosts* en una red punto a punto.

Características

- Pueden tener en su configuración desde cuatro hasta 32 puertos mediante conector RJ45.
- Trabajan en la capa física del modelo OSI.
- Ventaja: no requieren de una configuración previa, lo cual quiere decir que solamente se dedican a repetir una señal de entrada.
- Desventaja: al enviar mensajes al tiempo se produce una colisión, lo cual causa pérdidas en tiempo real debido a que los mensajes no podrán ser decodificados.
- ¿Qué opinan con relación al ancho de banda? Esta sería otra desventaja porque es-

taríamos manejando el mismo ancho de banda, dado que los dispositivos finales compartirían el canal a la hora del envío y recepción de los mensajes.

- En un tiempo, las topologías estrellas utilizaban estos elementos, después fueron reemplazados por *switches*.

A continuación, se aprecia del HUB 3com SuperStack II Dual Speed Hub 500 24-Port.

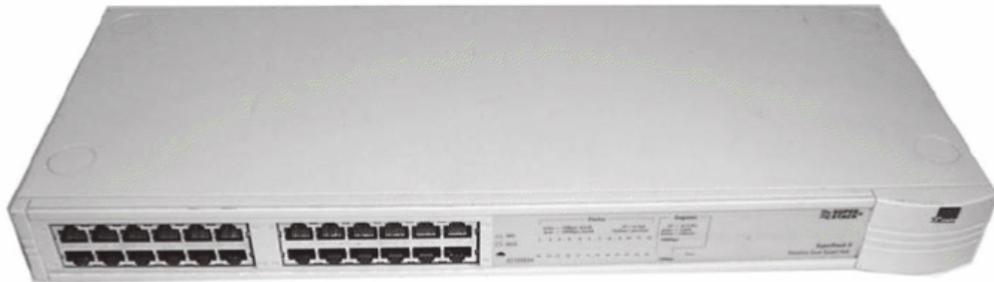


Figura 6.

Fuente: <https://www.cnet.com/products/3com-superstack-ii-dual-speed-hub-500-24-port/specs/>

Puente o bridge

Este dispositivo cuenta con conectores de diferentes tecnologías, lo cual le permite establecer comunicación con redes distintas.

Características

- Tiene semejanza con una estación corriente en la capa de enlace de datos del modelo OSI.
- Si realizamos una analogía con los hubs, los puentes solo permiten el tráfico de un host A instalado en la **subred** A hacia un host ubicado en la subred B, pero que esté destinado hacia esa subred B. Esta particularidad del puente se conoce como filtro. Esta característica se procesa debido al conocimiento de las dos subredes, dado que ambas están conectadas al puente. En caso de que el puente no identifique al destinatario inundará los demás puertos, ignorando el que le dio el mensaje.



Subred

Término que se asocia a redes secundarias de una red existente.



Figura 7.

Fuente: http://www.produktinfo.conrad.com/datenblaetter/00000-24999/001092789-an-01-es-LINKSYS_WES610N_4PT_DB_BRIDGE.pdf

A continuación, se aprecia el puente Linksys WES610N/WET610N, el cual tiene la capacidad de conectar dispositivos con tecnología Ethernet a la red inalámbrica.

- Un puente permite un mayor rendimiento en cuanto a las conexiones que se pueden implementar en varias redes. ¿Cómo se produce esto? Enfoquémonos en el siguiente ejemplo: tenemos que diseñar una red LAN con 700 *hosts*. Podemos dividir esta LAN en dos subredes mediante un puente, cada subred con 350 *hosts*. Con esto se garantiza optimizar la congestión y, por supuesto, el tráfico.
- Los puentes hoy en día, con la aparición de los conmutadores, muy poco se tienen en cuenta, debido a que los *switches* presentan mayor número de puertos y velocidad en cada uno de ellos.

Conmutadores o switches

Los *switches* son dispositivos llamados *switches* LAN. Estos proporcionan conexiones a varios segmentos en una red de área local de manera física a redes más complejas. ¿Qué creen ustedes que sucede al introducir un **conmutador** por primera vez a la red? Al introducirse en una red, los conmutadores no tienen conocimiento sobre los *hosts* que están conectados en los diferentes puertos, debido a esto se origina una **difusión** (*broadcast*) hacia estos dispositivos, lo que le permite al conmutador aprender las direcciones MAC de los *hosts* donde se originan los mensajes y armar su tabla de enrutamiento. El proceso de los conmutadores no acaba aún, el *host* al cual va destinado el mensaje recibe dicho mensaje y, automáticamente, da una respuesta al *host* que intenta comunicarse con él, en este caso, el *host* emisor. Cuando se da este proceso de envío y recepción del mensaje a través de los *hosts*, el conmutador podrá indagar sobre direcciones (IP o MAC) de fuente o de origen de los mensajes de respuesta, lo cual le brinda la posibilidad de identificar en qué puertos están conectados estos *hosts* de destino. Una vez el conmutador esté en operación, se genera una tabla dentro de él, en la cual se alojará información pertinente sobre los *hosts* que están conectados por los diferentes puertos.



Conmutador

Elemento que permite la conexión de diferentes equipos dentro de las redes. Un conmutador puede conectar varios dispositivos a la vez que segmentos dentro de las redes, con el objetivo de establecer comunicación entre un *host* de origen y un *host* al cual está destinado el mensaje.

Difusión

Hace referencia al hecho de propagar los mensajes a todos los *hosts* conectados a la red.

Características

- Presentan en su configuración un número de puertos determinados (4, 8, 24, etc.).
- Se desempeñan en la capa de enlace de datos del modelo OSI.
- Con los conmutadores se tiene un mayor rendimiento de la red, debido a que se entra en detalle a mirar cuál es el mensaje de origen y hacia dónde va dirigido. En contexto, se reducen las colisiones.
- Unos de los *switches* que están a la vanguardia es el Cisco Catalyst WS-C2960X-24PSQ-L (Cool). En la figura podrán apreciar este conmutador.



Figura 8.

Fuente: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/data_sheet_c78-728232.html

Se trata de un conmutador de 24 puertos de 10M/100M/1000M que puede alimentar hasta ocho puertos de PoE (los primeros ocho puertos solamente) con capacidad para entregar una suma total de 110W de potencia PoE. Este conmutador tiene cuatro enlaces ascendentes Gigabit Ethernet: dos de ellos SFP y los otros dos interfaces de cobre de 10M/100M/1000M, que permiten elegir la conectividad de fibra o cobre al punto de agregación. Otras características son:

- Se maneja en la capa de enlace de datos del modelo OSI.
- Tiene calidad del servicio. QoS avanzada.
- Seguridad, disponibilidad, escalabilidad y administración avanzadas.
- Rendimiento básico.

Encaminador o router

Ahora analicemos el encaminador o *router*, el dispositivo de interconexión con mayor grado de relevancia en las redes informáticas. Este dispositivo es capaz de interconectar redes ubicadas en el mismo nivel o en niveles diferentes. Ejemplo: puede conectar redes que se encuentren en la misma capa de red del modelo OSI o conectar redes que se encuentren en la capa de enlace de datos con la capa de red. Así, el *router* se desenvuelve en la capa de red del modelo OSI (capa 3).

Características

- Como el *router* se maneja en la capa de red del modelo OSI, su función principal es encaminar los paquetes que llegan dirigidos a él hacia el destino correspondiente, siempre con la facultad de distinguir la ruta adecuada o el mejor camino. Este proceso en redes informáticas se conoce como *routing*.
- Los *routers* trabajan de la mano con los **protocolos** de la capa de red del modelo OSI IPv4-IPv6.
- Los *routers* son optimizadores de recursos, debido a que facilitan la comunicación de cualquier **host** con otro *host* a nivel global, regulando el tráfico de información.
- La complejidad de los procesos que realiza como, por ejemplo, decidir cuál es la mejor ruta, enviar mensajes, informar cambios en la red, etc., permite que el *router* tenga un comportamiento como el de un computador. Por esto, dentro del *router* podemos encontrar elementos como:
 - Unidad central de proceso (CPU): su función principal es ejecutar las instrucciones del sistema operativo (SO), como la inicialización. Además, tiene funciones de enrutamiento y conmutación.
 - Memoria RAM (*random access memory*): almacena aplicaciones y procesos, como Cisco IOS, archivo de configuración en ejecución, tabla de enrutamiento IP y caché ARP.
 - Sistema operativo (SO): intérprete entre la máquina y los demás *softwares*.
 - Memoria Nvram (memoria de acceso aleatorio no volátil): permite el almacenamiento permanente para el archivo de configuración de inicio (*startup-config*). Esta característica permite que no se pierda la información una vez se apaga el *router*.
 - Sistemas básicos de entrada y salida (BIOS): permiten el arranque de los ordenadores. Son parte de la ROM.
 - Memoria *flash* (no volátil): permite el almacenamiento permanente para el IOS y otros archivos que tienen relación directa con el sistema.
 - Memoria ROM (*read only memory*): consiste en un *firmware* incorporado en un circuito integrado en los enruta-



Protocolos

Se entienden como protocolo las normas que manejan los administradores de red para poder establecer comunicaciones efectivas dentro de las redes.

dores, con la propiedad de que al apagar este dispositivo no se pierde el contenido en los *routers*. La memoria ROM permite almacenar instrucciones de arranque, *software* de diagnóstico básico e IOS limitado.

En la siguiente imagen veremos *routers* que en la actualidad está enfocando Cisco para sucursales en donde proporcionará características como: **virtualización**, colaboración multimedia y ahorro de costos en las operaciones. Nos referimos a Cisco 1941 y Cisco 1941W. Estos ofrecen la integración del punto de acceso IEEE 802.11n y se conocen como dispositivos multipropósito (funcionan como *router*, *switch* y AP).



Virtualización

Hace referencia al uso de la tecnología de una manera que se pueden usar los recursos en cualquier momento y lugar de manera online. Ejemplo: hoy en día servidores virtuales, o sea, en la nube, son los que resguardan nuestra información.



Figura 9.

Fuente: http://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78_556319.html?dtid=ossdc000283

Puntos de acceso inalámbrico

Hoy en día, la mayoría de las empresas adoptan tecnologías que garanticen buena comunicación, buen rendimiento y que estén al alcance de sus bolsillos. Por estas razones, encontramos dispositivos como los puntos de acceso inalámbrico.

Características

- Tienen un radio de operaciones para su funcionamiento, debido a que no tienen estipulados cables en sus conexiones de red.
- Dan practicidad a la hora de que los usuarios dentro de la red accedan a dicha red de manera inalámbrica sin perturbaciones.
- Dependiendo del radio al cual se van a someter los puntos de acceso, se hace necesario saber la potencia para que el rendimiento sea el adecuado. La conexión entre varios puntos de acceso se logra a través de

medios guiados y no guiados. Con esta descripción surge la pregunta: ¿qué medios utiliza una antena de tecnología móvil y cuáles medios utiliza un punto de acceso dentro de una organización, por ejemplo, dentro de una biblioteca? Las antenas



Medios guiados

Son aquellos que necesitan un medio físico. Ejemplo: fibra óptica para la transmisión de las señales.

de tecnología móvil se comunican entre sí por enlaces concatenados de microondas o mediante cables. Ahora, los puntos de acceso en una red informática dentro de una biblioteca se interconectan con medios guiados RJ45.

En la figura veremos un punto de acceso UniFi AP-Outdoor+ (UAP-Outdoor+) que ofrece wifi con una tecnología MIMO 802.11n para un rendimiento superior en las bandas de 2,4 o 5 GHz y alcanza hasta 600 pies.



Figura 10.

Fuente: https://dl.ubnt.com/datasheets/unifi/UniFi_AP_DS.pdf

Dispositivos multipropósito

Muchas veces el usuario desea encontrar dispositivos que le permitan realizar o integrar todas las funciones en un solo dispositivo. Hoy, en el mercado podemos encontrar dispositivos multipropósitos, esto se evidencia en el sector hogar, en donde el usuario prefiere tener dispositivos multipropósito con cada una de las funciones que realizan un *switch*, un punto de acceso inalámbrico y un *router*.

En la siguiente figura se puede visualizar el "Linksys WAP300N". En el *link* pueden apreciar que es un dispositivo multipropósito que cuenta con cuatro modos de uso en su forma de operar: el primero es modo punto de acceso (por defecto), después nos encontramos con el modo *wireless media connector* (conector de medios inalámbricos), seguido a este nos encontramos con el modo *wireless range extender* (amplificador de rango inalámbrico) y, por último, opera en el modo *wireless bridge* (puente inalámbrico).



Figura 11.

Fuente: <http://www.linksys.com/co/support-article?articleNum=136121>

Factores de forma del switch

Uno de los temas que determinan un buen diseño y una posterior configuración de redes informáticas es la correcta elección de los elementos o dispositivos. En este apartado nos enfocaremos en los factores de forma del *switch*. Este término lo podemos asociar como un patrón de medida a la hora de la elección de estos, dado que, dependiendo de la forma, el tamaño, la posterior ubicación en el *rack*, la configuración, ya sea fija, modular, apilable o no apilable, se puede determinar cuál *switch* es el adecuado en nuestras redes.

Analicemos el comportamiento de los *switches*, según su configuración:

- **Switches de configuración fija:** estos se basan en la configuración y las características que vienen preestablecidas por parte del fabricante, con lo cual podemos determinar que no se permite implementar cambios. Ejemplo: al tener en nuestra red un *switch* que contempla N números de puertos es imposible agregar más puertos a nuestro *switch*.

Ejemplo de un *switch* de configuración fija es el EX2200 de Juniper. En la siguiente figura se puede apreciar y en el *link* se encuentra la descripción.



Figura 12.

Fuente: <http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000307-en.pdf>

- **Switches de configuración modular:** pueden llegar a tener más de 1000 puertos en su fisionomía, dado que en su chasis pueden presentar módulos para la inserción de nuevas tarjetas con un determinado número de puertos. Estos *switches* los utilizan las grandes compañías y los ISP. Debido a estas configuraciones podemos decir que estos conmutadores modulares se pueden amoldar a las necesidades futuras de las diferentes redes informáticas dentro de las organizaciones. En las empresas donde el número de clientes crece considerablemente en el tiempo esta característica se conoce como escalabilidad.

Un ejemplo de un *switch* de configuración modular es el Conmutador HPE FlexFabric Serie 12900. En la siguiente figura se puede apreciar y en el *link* se encuentra la descripción.



Figura 13.

Fuente: <https://www.hpe.com/lamerica/es/productcatalog/networking/networking-switches/pip.hpe-flexfabric-12900-switch-series.5443167.html>

- **Switches de configuración apilable:** poseen un cable en la parte trasera que se denomina *backplane*, el cual tiene la característica de interconectar varios *switches*. De esta manera, facilita la obtención de un número mayor de puertos al unir los diferentes *switches*, lo cual es determinante al momento de ahorrar recursos dentro de las organizaciones, permite un manejo práctico en cuanto al rendimiento (ancho de banda) y posibilita la escalabilidad.

Un ejemplo de un *switch* de configuración apilable es el ERS 5000. En la siguiente figura se puede apreciar y en el *link* se encuentra la descripción.



Figura 14.

Fuente: <https://www.avaya.com/es/documents/ethernet-routing-switch-serie-5000-de-avaya-dn5098sp.pdf?t=0>

¿Qué son las redes conmutadas?

Hace años surgió la arquitectura LAN más común: Ethernet 802.3. Esta tecnología de conmutación se caracterizaba por enviar datos dentro de la red a los



LAN

(Local area network): son redes de área local utilizadas por los administradores en la mayoría de las organizaciones.

diferentes dispositivos. Se basaba en topologías bus, las cuales advierten muchos inconvenientes al momento de implementarlas. Ejemplos de estos inconvenientes son:

- Después de 500 m es necesario utilizar repetidores, debido a que la señal se debilita. A esto se le suman los factores atmosféricos.
- La implementación de los recursos es elevada.
- Al momento de presentarse una caída de uno de los **hosts** se interrumpe la comunicación en toda la red.
- Se debe compartir el ancho de banda (10 Mbps), por lo cual se producen muchas colisiones y retardos en la red.

Al incorporar dispositivos de capa 2, como los conmutadores, no ocurren inconvenientes como los expresados; por ejemplo: "Al momento de presentarse una caída en uno de los **hosts** se interrumpe la comunicación en toda la red", debido a que los conmutadores tienen la capacidad de aprender las direcciones MAC ubicadas en las tramas transmitidas. Gracias a esta característica, toman decisiones acerca del reenvío de mensajes, lo cual alivia las colisiones dentro de la red. Los conmutadores envían mensajes de difusión a los dispositivos que forman parte de la red,

produciendo un bajo rendimiento de esta. Al sumar dispositivos de capa 3, los **routers**, estos cumplen un papel fundamental a la hora de escoger el mejor camino de envío y recepción de los mensajes. Con los **routers** no se manejan tráficos por difusión, lo cual aumenta el rendimiento de las redes LAN.

Los administradores de red implementan en su diseño dispositivos de interconexión en las diferentes capas del modelo OSI (física-enlace de datos-red). Esto se hace partiendo de las prioridades en las redes LAN. En su desarrollo, las LAN empezaron a sufrir congestión y retardos en sus actividades, debido al gran consumo de ancho de banda en los servicios que se manejaban dentro de estas: telefonía convencional, PC de escritorio, impresoras, escáner, portátiles, tabletas, transferencia de archivos, transacciones, videos, mensajería, etc. Por esta razón, hoy tenemos tecnologías más avanzadas como las LAN conmutadas, que permiten un mayor ancho de banda dentro de las organizaciones, lo cual mejora el tráfico y da un mayor rendimiento a las LAN. Esto se logra con la utilización del ancho de banda por cada usuario sin interferir con el resto de la red. Se puede decir que se tiene un ancho de banda dedicado a los diferentes usuarios.

Características de las LAN conmutadas

- Los dispositivos de las LAN conmutadas deben tener la propiedad de convivir con tecnologías existentes y, además, de acoplarse a los cambios que se presentan a diario en la tecnología (por ejemplo, VOIP). Para entrar en contexto, la telefonía analógica debe ser aceptada y propiciada en las redes conmutadas.

- Se maneja calidad del servicio (QoS).
- Al manejar cantidades de información, es importante garantizar que dicha información sea protegida. Esto implica tener un alto grado de seguridad en las redes LAN dentro de las organizaciones.
- Las redes conmutadas tienen como principio converger tecnológicamente. Esto va de la mano con lo que se conoce hoy en día como redes convergentes.



QoS

Del inglés quality of service, hace referencia a la calidad del servicio; por ejemplo, al administrar el ancho de banda dentro de una organización debemos dar prioridad a servicios como las llamadas telefónicas y la transferencia de archivos; y una reducida parte del ancho de banda al video, dado que este consume mucho.

Redes convergentes

La mejor manera de interpretar las redes convergentes es comprender la necesidad que tienen los diferentes organismos de llevar cada uno de los servicios, como voz, datos y video, por un solo medio. Un ejemplo son los operadores que tenemos en Colombia, como Claro, los cuales nos entregan por un mismo medio tecnología coaxial, HFC (híbrido de fibra y coaxial) o fibra óptica, servicios de TV, telefonía e internet, con la particularidad de un “reuso” de la señal. Esto indica que, en horas esenciales para el descanso del colombiano, puede ser a las 8:00 p. m., hay una lentitud al acceso de la red, debido a que la tecnología, en este caso de fibra, sale de la estación principal y llega a los diferentes nodos y de ahí se redistribuye la señal a los abonados vinculados a dicho nodo.

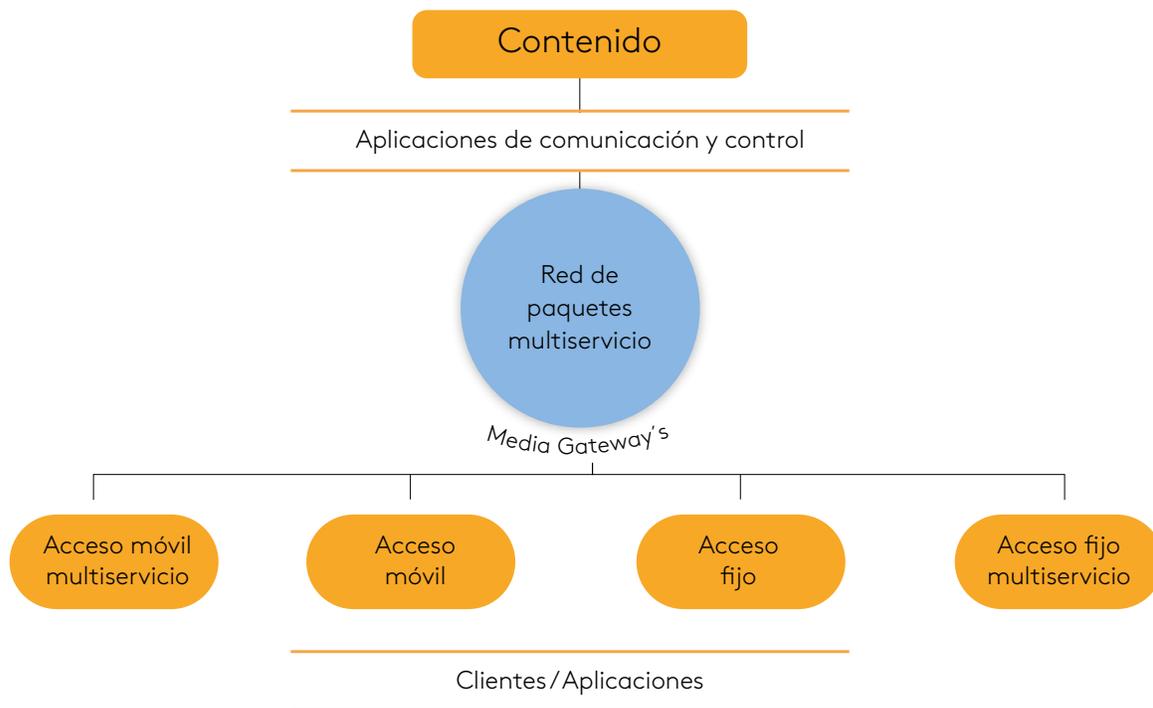


Figura 15.

Fuente: https://www.crcm.gov.co/recursos_user/Actividades%20Regulatorias/regulacion_redes/Unicauca.pdf

Características

- Las redes convergentes implementan en su configuración y diseño una única red física indispensable para garantizar eficacia al momento de administrar las redes informáticas.
- La implementación del protocolo IP dentro de cada uno de los servicios que se prestan en las redes: voz, datos y video, idealizando una red donde el tráfico y el transporte confluyen sobre una red que converge. Con este uso de IP en las redes convergentes se obtiene lo siguiente:
 - Los administradores de red tendrán un manejo apropiado en la administración de la red.
 - Una mejor distribución del ancho de banda dentro de las organizaciones para optimizar recursos.
 - Capacidad de adoptar nuevas aplicaciones dentro de las empresas.
- En las organizaciones podemos encontrar tecnologías que permiten un manejo práctico de las llamadas. Un ejemplo de esto es la posibilidad de tener oficinas con teléfonos IP, los cuales brindan opciones como: si usted no se encuentra en su punto de trabajo y entra una llamada, el teléfono inmediatamente identifica la llamada y puede transferirla. Además, si estamos ocupados cuando entra la llamada, podemos usar la llamada en espera; asimismo, frente a una reunión con socios o clientes, podemos realizar una teleconferencia.

- A través de las redes convergentes podemos implementar la mensajería, mediante voz o datos, incluyendo multimedia.
- Con el advenimiento de los *smartphones* podemos establecer una comunicación en tiempo real a cualquier hora del día y en cualquier lugar del planeta.

¿Qué es Cisco Borderless Network?

Imaginemos el siguiente escenario: una red Campus que establece comunicación con sus dos sucursales dentro de la ciudad de Barranquilla. En cada una de ellas hay un servidor y servicios de voz y datos. Además, estas sucursales tienen acceso a internet, cuentan con la telefonía tradicional **PSTN** y acceso a internet inalámbrico. Para conseguir el correcto funcionamiento en las sucursales de la red convergente es fundamental la implementación de una arquitectura que se conoce como Cisco Borderless Network. Esta tecnología incluye en su puesta en marcha una inteligencia en torno a la aceptación de futuros usuarios en las sucursales, esta característica se denomina escalabilidad.



PSTN

Del inglés public switched telephone network (red de telefonía pública conmutada), es una red de telecomunicaciones en donde se dan las comunicaciones mediante líneas telefónicas en tiempo real.

Con Cisco Borderless Network tenemos redes sin fronteras. Analicemos esa frase: “redes sin fronteras”, inmediatamente se nos viene a la mente que no hay límites, que nos podemos comunicar, relacionarnos con determinado número de personas, organizaciones, etc., a cualquier hora del día independiente del lugar en que nos encontremos. Aún mejor, podemos lograr una interacción en los entornos donde nos

encontremos para propiciar la mejor manera de laborar y establecer negocios alrededor del mundo.

Las redes convergentes sin fronteras nos indican que los procesos deben realizarse con normas, lineamientos o doctrinas adecuados. Partiendo de este parámetro, las redes convergentes necesitan guiarse por un modelo en capas o diseño jerárquico que garantice un manejo apropiado de la información.

Modelo jerárquico de las redes convergentes

En la siguiente figura podemos apreciar el modelo jerárquico de las redes convergentes y sus capas.

Algunas características del modelo son:

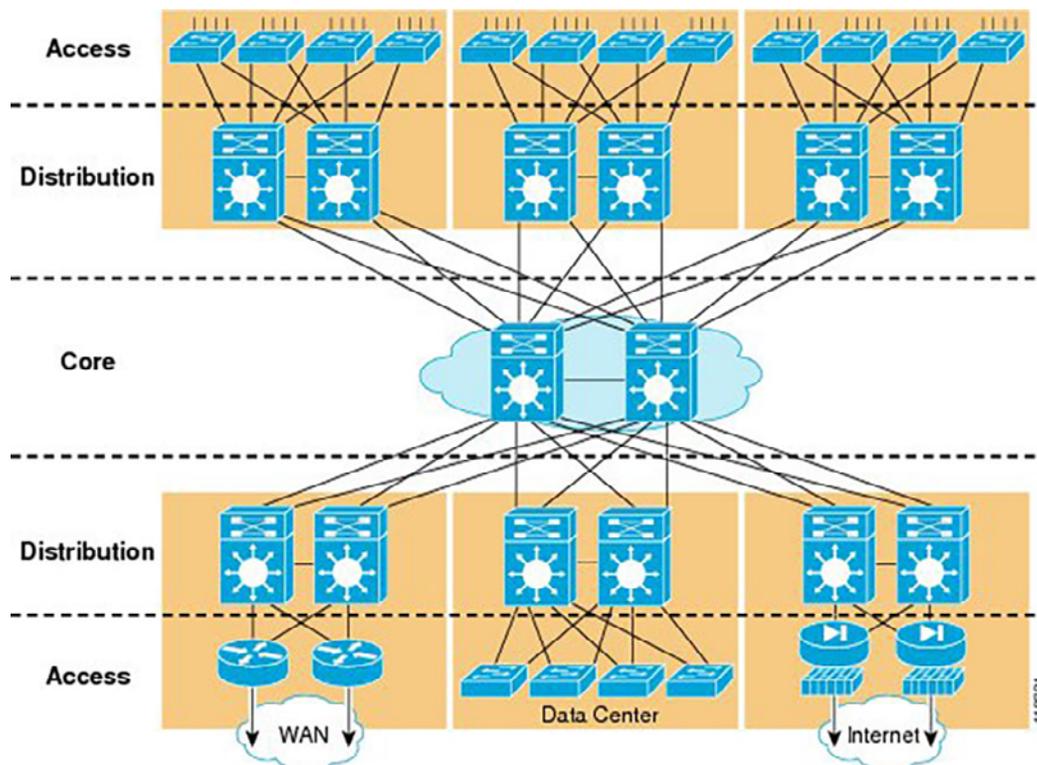


Figura 16.

Fuente: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/ha-campusdg.html?dtid=ossdc000283

- Brinda garantías en la confiabilidad al pensar en un diseño de redes conmutadas sin fronteras, basándose en establecer una jerarquía. Sin esta, no se podría identificar el rol de los diferentes elementos y dispositivos dentro de las redes.
- Un buen diseño debe aceptar evolución y crecimiento. Debe contemplar la idea de incorporar nuevos usuarios a las redes, lo cual se comprende como la capacidad de ser modular.
- Al presentarse alguna falla dentro de la red, esta debe ser inteligente para garantizar su funcionamiento. Esto se conoce como capacidad de recuperación.
- ¿Qué tan segura es nuestra red al brindar acceso a un socio en una reunión? Partiendo de la premisa de que la información es lo más importante para las organizaciones, debemos garantizar que nuestro socio tenga acceso a internet, pero con limitaciones. Si una persona no autorizada se conecta a nuestra red con intenciones maliciosas, debemos estar en capacidad de denegar este acceso por medio de políticas y bloquearla.

Capas del diseño jerárquico de redes

- 1. Capa de acceso:** facilita que los usuarios o dispositivos finales accedan a la red. Estos tienen la característica de estar conectados a *switches* de acceso que, a su vez están conectados a los *switches* de la capa de distribución. Ejemplo: los *switches* catalyst 2960 de Cisco. Hoy en día la eficiencia y la seguridad de estos *switches* facilitan la administración de las diferentes aplicaciones. Debido a la inteligencia que poseen estos dispositivos, en esta capa se pueden agregar más enlaces.
- 2. Capa de distribución:** favorece la interoperabilidad entre las capas de acceso y **core** del modelo jerárquico. Facilita enlaces redundantes para garantizar el funcionamiento de la red. Además, en su funcionamiento, implementa conmutadores de capa 3; por ejemplo: el *switch* catalyst 3750 de Cisco capa 3 maneja QoS.
- 3. Capa de núcleo o core:** es la capa central de la red. En esta se manejan muchas velocidades. Por la gran cantidad de información que se trata, se garantiza QoS. Esta capa implementa *switches* modulares; por ejemplo, el *switch* catalyst 6500 de Cisco.

Aznar López, A. (2005). *La red internet. El modelo TCP/IP*. Madrid, España: Grupo Abantos Formación y Consultoría.

Boronat Seguí, F. (2013). *Direccionamiento e interconexión de redes basadas en TCP/IP: IPv4/IPv6, DHCP, NAT, encaminamiento RIP y OSPF*. Valencia, España: Editorial de la Universidad Politécnica de Valencia.

Carceller Cheza, R. (2013). *Servicios en red*. Madrid, España: Macmillan Iberia S. A.

Castaño Ribes, R. J. (2013). *Redes locales*. Madrid, España: Macmillan Iberia S. A.

Hallberg, B. (2007). *Fundamentos de redes*. Madrid, España: McGraw-Hill Interamericana.

Hillar, G. C. (2004). *Redes: diseño, actualización y reparación*. Buenos Aires, Argentina: Editorial Hispano Americana S. A.

Íñigo Griera, J. (2008). *Estructura de redes de computadores*. Barcelona, España: Editorial UOC.

Jiménez Camacho, R. (2014). *Análisis del mercado de productos de comunicaciones (UF1869)*. Málaga, España: IC Editorial.

Martínez Yelmo, I. (2015). *IPv6-Lab: entorno de laboratorio para la adquisición de competencias relacionadas con IPv6*. Madrid, España: Universidad de Alcalá.

McGraw-Hill Interamericana. (2013). *Redes locales*. Madrid, España: McGraw-Hill.

Molina Robles, F. J. (2014). *Servicios de red e internet*. Madrid, España: RA-MA Editorial.

Moreno Pérez, J. C. (2014). *Sistemas informáticos y redes locales*. Madrid, España: RA-MA Editorial.

Quintero, E. B. (2014). *UF1879: equipos de interconexión y servicios de red*. Málaga, España: IC Editorial.

Santos González, M. (2014). *Diseño de redes telemáticas*. Madrid, España: RA-MA Editorial.

Velte, T. J. (2008). *Manual de Cisco®*. Madrid, España: McGraw-Hill Interamericana.