

A white computer keyboard is depicted within a dashed white rectangular border on the left side of the title banner. A yellow ribbon-like graphic flows behind the banner.

## **CONFIGURACIÓN DE DISPOSITIVOS**

ACTIVOS PARA SERVICIOS  
DE RED CON IPV6

**MATERIAL DE FORMACIÓN 2**  
**CONFIGURACIÓN DE DISPOSITIVOS**  
**ACTIVOS Y SERVICIOS PARA IPV6**



## Configuración de dispositivos activos y servicios para IPV6

# MATERIAL DE FORMACIÓN 2

---

### contenidos

### Pag.

INTRODUCCIÓN .....	2
MAPA CONCEPTUAL .....	3
SERVICIOS DE RED IPV6 .....	4
EQUIPOS ACTIVOS DE RED .....	10
SOFTWARE DE SIMULACION REDES PACKET TRACER .....	11
Glosario .....	13
BIBLIOGRAFÍA .....	14
CREATIVE COMMONS .....	15
CRÉDITOS DEL PROGRAMA .....	16



## INTRODUCCIÓN

La configuración del protocolo IPV6 es un poco más extensa y compleja, cuenta con 128 bits y un encabezado diferente al conocido IPV4, el IPV6 permite mayor conectividad en comparación con IPV4.

El protocolo IPV6 ha cobrado mayor relevancia entre el gremio que aborda la temática a través de redes y telecomunicaciones, lo anterior obedece a la gran demanda de conectividad a las redes que en la actualidad permite y facilita la comunicación de extremo a extremo desde cualquier parte del mundo.

IPV6 está inmerso en conceptos como: ciudades inteligentes, Internet de las cosas, conectividad avanzada y redes académicas de última tecnología.





Mapa  
Conceptual

**CONFIGURAR LOS DISPOSITIVOS ACTIVOS DE INTERCONEXIÓN EN LA RED QUE CUMPLAN LAS CONDICIONES DE TRANSMISIÓN E INTERCAMBIO DE INFORMACIÓN REQUERIDA PARA LA SOLUCIÓN.**

Servicios de  
red IPV6

Equipos activos de red

Software de simulación  
Packet Tracer

**CONFIGURAR LOS DISPOSITIVOS ACTIVOS Y SERVICIOS DE RED PARA IPV6 DE ACUERDO CON LOS REQUERIMIENTOS DE LA EMPRESA.**

## SERVICIOS DE RED IPV6

### Dirección unicast global de IPV6

IPv6 posee un formato de direcciones que permite la agrupación ascendente hasta llegar finalmente al ISP. Las direcciones unicast globales normalmente están compuestas por un prefijo de enrutamiento global de 48 bits y un ID de subred de 16 bits. Las organizaciones individuales pueden utilizar un campo de subred de 16 bits para crear su propia jerarquía de direccionamiento local. Este campo permite a la organización utilizar hasta 65.535 subredes individuales.

La dirección unicast global actual asignada por IANA utiliza el rango de direcciones que comienzan con el valor binario 001 (2000::/3), que es 1/8 del espacio de la dirección IPv6 y es el bloque más grande de direcciones asignadas. IANA está asignando espacio de direcciones IPv6 en los rangos de 2001::/16 a los cinco registros RIR (ARIN, RIPE, APNIC, LACNIC y AfriNIC).

### Direcciones reservadas

IETF reserva una parte del espacio de direcciones de IPv6 para diferentes usos, tanto presentes como futuros.

Las direcciones reservadas representan 1 de 256 partes del espacio total de direcciones de IPv6. Algunos de los otros tipos de direcciones IPv6 provienen de este bloque.

### Direcciones privadas

Se separó un bloque de direcciones IPv6 para direcciones privadas, igual que lo que se hizo con IPv4. Estas direcciones privadas son locales solamente en un enlace o sitio en particular y por lo tanto, nunca se enrutan fuera de la red de una empresa particular. Las direcciones privadas tienen un primer valor de octeto de "FE" en la notación hexadecimal y el siguiente dígito hexadecimal es un valor de 8 a F.

Estas direcciones se subdividen en dos tipos, según su ámbito.

Las direcciones locales de un sitio son direcciones similares a la asignación de direcciones para Internet privadas de RFC 1918 en IPv4. El ámbito de estas direcciones es un sitio o una organización completa. Sin embargo, el uso de direcciones locales de un sitio es problemático y RFC 3879 lo desaprueba desde 2003. En notación hexadecimal, las direcciones locales de un sitio

comienzan con "FE" y el tercer dígito hexadecimal está entre "C" y "F". Es así como estas direcciones empiezan así: "FEC", "FED", "FEE" o "FEF".

Las direcciones unicast de enlace local son nuevas dentro del concepto de direccionamiento con IP en la capa de red. Estas direcciones tienen un ámbito más pequeño que las direcciones locales de un sitio, ya que hacen referencia solamente a un enlace físico en particular (red física). Los *routers* directamente no reenvían datagramas con direcciones link-local, ni siquiera dentro de la organización. Solo se utilizan para comunicaciones en un segmento en particular de la red física. Se utilizan para comunicaciones de enlace, por ejemplo: configuración automática de direcciones, detección de vecinos y detección de *routers*. Muchos protocolos de enrutamiento IPv6 también utilizan direcciones link-local. En notación hexadecimal, las direcciones link-local comienzan con "FE" y el tercer dígito hexadecimal es un valor entre "8" y "B".

Así es como estas direcciones comienzan con: "FE8", "FE9", "FEA" o "FEB".

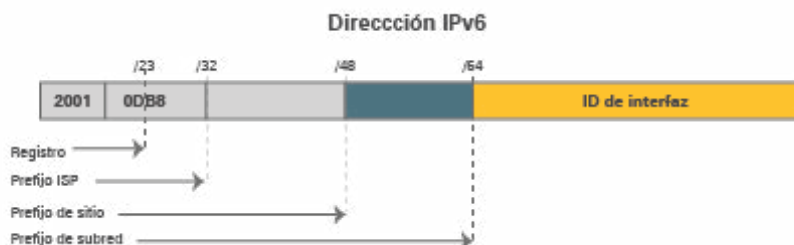
## Dirección de loopback

Igual que en IPv4, se hizo una reserva de una dirección especial de *loopback* IPv6 para hacer pruebas: los datagramas que se envían a esta dirección regresan al dispositivo emisor y forman así un bucle de retorno o '*loopback*'. Sin embargo, en IPv6 hay sólo una dirección y no todo un bloque para esta función. La dirección de *loopback* es 0:0:0:0:0:0:0:1, que normalmente se expresa mediante la compresión de ceros como "::1".

## Dirección no especificada

En IPv4, una dirección IP compuesta únicamente por ceros tiene un significado especial: hace referencia al mismo *host* y se utiliza cuando un dispositivo no conoce su propia dirección. En IPv6, este concepto se formalizó y la dirección compuesta únicamente por ceros (0:0:0:0:0:0:0:0) se denomina dirección 'no especificada'. Normalmente se utiliza en el campo de origen de un datagrama que envía un dispositivo que desea configurar su dirección IP. Es posible aplicar compresión de direcciones en esta dirección, lo que la convierte simplemente en "::".

Figura 1. Dirección unicast global IPv6



Fuente: (Cisco CCNA exploration, 2016)

## Administración IPv6

Las direcciones IPv6 utilizan identificadores de interfaz para identificar las interfaces de un enlace. Considérelas como la porción de *host* de una dirección IPv6. Los identificadores de la interfaz deben ser únicos en un vínculo específico. Los identificadores de la interfaz siempre tienen 64 bits y se pueden derivar dinámicamente de una dirección de Capa 2 (MAC).

Se puede asignar un ID de dirección IPv6 de manera estática o dinámica:

- Asignación estática con un ID de interfaz manual
- Asignación estática con un ID de interfaz EUI-64
- Autoconfiguración sin estado
- DHCP para IPv6 (DHCPv6)

## Asignación de ID de interfaz manual

Una forma de asignar estáticamente una dirección IPv6 a un dispositivo consiste en asignar manualmente tanto el prefijo (red) como la porción del ID de la interfaz (*host*) de la dirección IPv6. Para configurar una dirección IPv6 en una interfaz de un *router* Cisco, use el comando `IPv6 address IPv6-address/prefix-length` en el modo de configuración de la interfaz. El siguiente ejemplo muestra la asignación de una dirección IPv6 a la interfaz de un *router* Cisco:

```
RouterX(config-if)#ipv6 address 2001:DB8:2222:7272::72/64
```



Figura 2. Asignación IPv6

Asignación estática	Asignación dinámica
<ul style="list-style-type: none"><li>• Asignación manual de ID de interfaz</li><li>• Asignación de ID de interfaz EUI-64</li></ul>	<ul style="list-style-type: none"><li>• Autoconfiguración sin estado</li><li>• DHCPv6 (con estado)</li></ul>

Fuente: (Cisco CCNA exploration, 2016)

### Asignación de ID de interfaz EUI-6

Una distinta forma de asignar una dirección IPv6 consiste en configurar la porción del prefijo (red) de la dirección IPv6 y derivar la porción del ID de la interfaz (*host*) de la dirección MAC de Capa 2 del dispositivo, que se conoce como ID de la interfaz EUI-64.

El estándar EUI-64 explica cómo extender las direcciones MAC de 48 a 64 bits mediante la inserción de la porción 0xFFFE de 16 bits en el medio en el bit 24 de la dirección MAC para crear un identificador de interfaz único de 64 bits.

Para configurar una dirección IPv6 en una interfaz de un *router* Cisco y habilitar el procesamiento de IPv6 con EUI-64 en esa interfaz, use el comando `IPv6 address ipv6-prefix/prefix-length eui-64` en el modo de configuración de la interfaz.

FIGURA 3. Identificador de interfaz EUI-64



Fuente: (Cisco CCNA exploration, 2016)

El siguiente ejemplo muestra la asignación de una dirección EUI-64 a la interfaz de un *router* Cisco:

```
RouterX(config-if)#ipv6 address 2001:DB8:2222:7272::/64 eui-64
```

### Configuración automática sin estado

La configuración automática, como su nombre lo indica, configura automáticamente la dirección IPv6. En IPv6 se supone que los dispositivos que no son PC, así como las terminales de computadoras, están conectados a la red. El mecanismo de configuración automática se introdujo para permitir networking plug-and-play de estos dispositivos, a fin de lograr la reducción de los gastos administrativos.

### DHCPv6 (con estado)

DHCPv6 permite que los servidores de DHCP pasen parámetros de configuración, por ejemplo, direcciones de red IPv6, a nodos IPv6. Ofrece la capacidad de asignación automática de direcciones de red reutilizables y mayor flexibilidad de configuración. Este protocolo es una contraparte con estado de la configuración automática sin estado de direcciones IPv6 (RFC 2462) y se puede utilizar por separado o de manera concurrente con la configuración automática de direcciones IPv6 sin estado para obtener parámetros de configuración.

### Estrategias de migración a IPv6

La transición de IPv4 no requiere que las actualizaciones de todos los nodos sean simultáneas. Hay muchos mecanismos

de transición que permiten una integración fluida de IPv4 e IPv6. Hay otros mecanismos que permiten que los nodos IPv4 se comuniquen con nodos IPv6. Para diferentes situaciones se requieren diferentes estrategias. La figura muestra la riqueza de las estrategias de transición disponibles.

Recuerde el consejo: “Use *stack* doble cuando pueda y *tunneling* cuando no tenga otra opción”. Estos dos métodos son las técnicas más comunes de transición de IPv4 a IPv6.

### Stack doble

El método de *stack* doble es un método de integración en el que un nodo tiene implementación y conectividad para redes IPv4 e IPv6. Es la opción recomendada y requiere que se ejecuten IPv4 e IPv6 simultáneamente. El *router* y los *switches* se configuran para admitir ambos protocolos; el protocolo preferido es IPv6.

### Tunneling

La segunda técnica de transición más importante es el tunneling. Existen varias técnicas de tunneling, entre las que se encuentran:

**Tunneling manual de IPv6 sobre IPv4:** un paquete de IPv6 se encapsula dentro del protocolo IPv4. Este método requiere *routers* de stack doble.

**Tunneling dinámico 6to4:** establece automáticamente la

conexión de islas de IPv6 a través de la red IPv4, normalmente Internet. Aplica dinámicamente un prefijo IPv6 válido y único a cada isla de IPv6, lo que posibilita la implementación rápida de IPv6 en una red corporativa sin recuperación de direcciones de los ISP o los registros. (Exploration, 2016)

Otras técnicas de tunneling menos utilizadas y que están más allá del ámbito de este curso incluyen:

**Tunneling del protocolo de direccionamiento automático de túnel dentro de un sitio (ISATAP, Intra-Site Automatic Tunnel Addressing Protocol):** mecanismo de tunneling de capa superior automática que utiliza la red IPv4 subyacente como capa de enlace para IPv6. Los túneles del ISATAP permiten que los *hosts* de stack doble individuales IPv4 o IPv6 de un sitio se comuniquen con otros *hosts* similares a través de un enlace virtual y creen así una red IPv6 mediante la infraestructura IPv4. (Exploration, 2016)

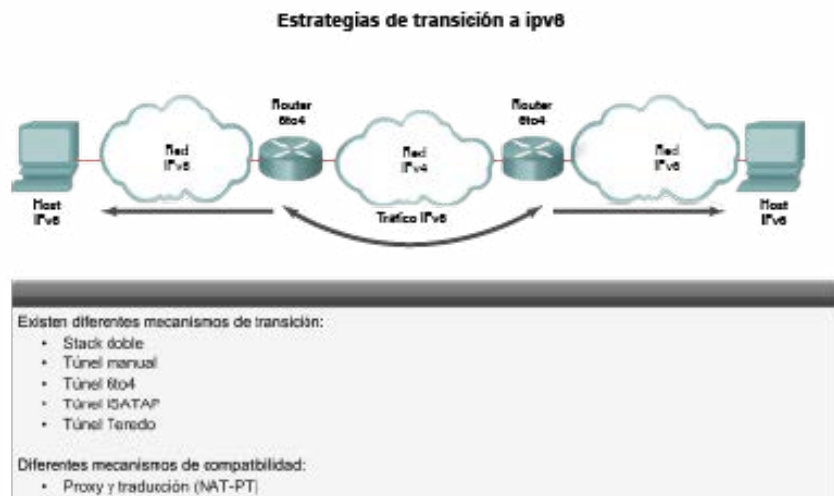
**Tunneling Teredo:** tecnología de transición a IPv6 que proporciona tunneling automático de *host* a *host* en lugar de tunneling de gateway. Este enfoque transmite tráfico IPv6 unicast si hay hosts de stack doble (hosts que ejecutan tanto IPv6 como IPv4) detrás de una o varias NAT IPv4. (Exploration, 2016)

**Traducción de protocolos NAT (NAT-Protocol Translation, NAT-PT)**

Esta traducción permite la comunicación directa entre hosts que utilizan versiones diferentes del protocolo IP. Estas traducciones son más complejas que IPv4 NAT.



Figura 4. ESTRATEGIAS DE MIGRACION IPV6



Fuente: (cisco CCNA exploration,2016)

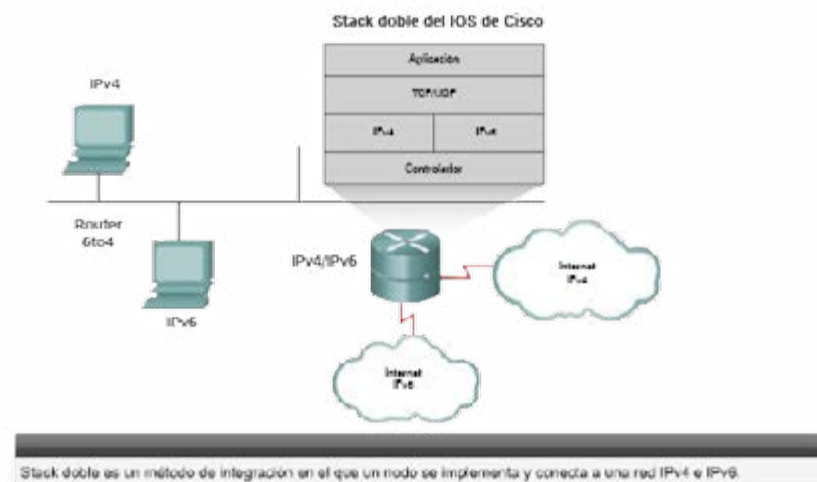
### Stack doble del IOS de Cisco

El método de stack doble es un método de integración que permite que un nodo tenga conectividad con redes IPv4 e IPv6 de manera simultánea. Cada nodo tiene dos stacks de protocolos con la configuración en la misma interfaz o en varias interfaces.

El enfoque de stack doble para la integración de IPv6, en el que los nodos tienen stacks de IPv4 e IPv6, será uno de los métodos de integración más comúnmente utilizados. Un nodo de stack doble elige qué stack utilizar en función de la dirección de destino del paquete. Un nodo de stack doble debe preferir utilizar IPv6 cuando esté disponible. Las aplicaciones antiguas que sólo admiten IPv4 siguen funcionando igual que antes. Las aplicaciones nuevas y las modificadas aprovechan las dos capas IP.

Se ha definido una nueva interfaz de programación de aplicaciones API (Application Programming Interface) para admitir direcciones y solicitudes DNS de IPv4 e IPv6. Una API facilita el intercambio de mensajes o datos entre dos o más aplicaciones de software diferentes. Un ejemplo de API es la interfaz virtual entre dos funciones de software, por ejemplo, un procesador de textos y una hoja de cálculo. La API se integra en las aplicaciones de software para traducir IPv4 a IPv6 y viceversa mediante la aplicación del mecanismo de conversión IP. Las aplicaciones nuevas pueden utilizar tanto IPv4 como IPv6.

Figura 5. STACK DOBLE



Fuente: (Cisco CCNA exploration,2016)

En la conversión de aplicaciones IPv4 a IPv6 sugiere que para la mayoría de las aplicaciones hay un cambio mínimo en algunos lugares puntuales del código fuente. Esta

técnica es conocida y se ha aplicado en el pasado para otras transiciones de protocolo. Permite la actualización gradual de las aplicaciones, una por una, a IPv6. (Exploration, 2016)

El uso de IPv6 en un *router* IOS de Cisco requiere el uso del comando de configuración global IPv6 unicast-routing. Este comando habilita el reenvío de datagramas IPv6.

Se debe configurar todas las interfaces que reenvían tráfico IPv6 con una dirección IPv6 mediante el comando de interfaz `ipv6 address IPv6-address [/prefix length]`

Figura 6. CONFIGURACION STACK DOBLE



Fuente: (cisco CCNA exploration, 2016)

## Tunneling IPv6

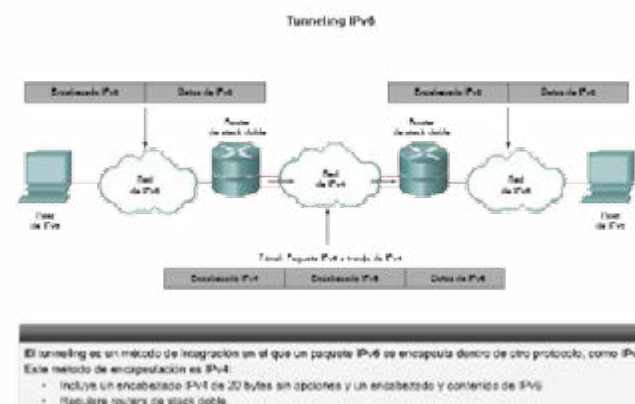
El tunneling es un método de integración en el que un paquete IPv6 se encapsula dentro de otro protocolo, por ejemplo, IPv4. Este método permite la conexión de islas de IPv6 sin

necesidad de convertir las redes intermediarias a IPv6. Cuando se utiliza IPv4 para encapsular el paquete IPv6, se especifica el tipo de protocolo 41 en el encabezado de IPv4 y el paquete incluye un encabezado de IPv4 de 20 bytes sin opciones y un encabezado y contenido de IPv6. También requiere *routers* de stack doble.

El tunneling presenta estos dos problemas. La unidad máxima de transmisión MTU (Maximum Transmission Unit) se reduce 20 octetos si el encabezado de IPv4 no contiene ningún campo opcional. Además, los problemas de las redes que utilizan tunneling normalmente son difíciles de resolver. (Exploration, 2016)

El tunneling es una técnica de integración y transición intermedia y no debe considerarse como una solución definitiva. El objetivo final debe ser una arquitectura IPv6 nativa.

Figura 7. TUNNELING IPV6

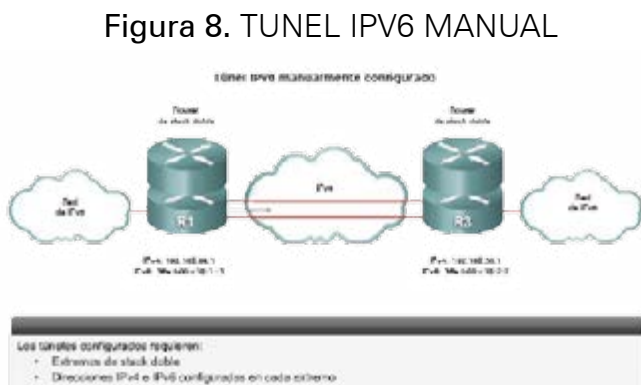


Fuente: (cisco CCNA exploration, 2016)

## Túnel IPv6 configurado manualmente

Un túnel configurado en forma manual equivale a un enlace permanente entre dos dominios IPv6 sobre un enlace troncal IPv4. El uso principal es para conexiones estables que requieren comunicación segura periódica entre dos *routers* de borde, entre un sistema final y un *router* de borde o para conexión con redes IPv6 remotas. Los *routers* de borde deben ser de stack doble y la configuración no puede cambiar dinámicamente a medida que cambian las necesidades de la red y de enrutamiento.

Los administradores configuran una dirección IPv6 estática de manera manual en una interfaz de túnel y asignan las direcciones IPv4 estáticas configuradas manualmente al origen y al destino del túnel. El *host* o el *router* de cada extremo de un túnel configurado debe admitir stacks de protocolos IPv4 e IPv6. Los túneles configurados manualmente pueden establecerse entre dos *routers* de borde o entre un *router* de borde y un *host*. (Exploration, 2016)



Fuente: (cisco CCNA exploration, 2016)

## EQUIPOS ACTIVOS DE RED

Son aquellos dispositivos como: *switch*, *router*, access point, firewall, ect, los cuales se interconectan con segmentos de cable a las computadoras y servidores, con el fin de pasar datos y comunicar internamente o externamente a las personas de una compañía. Estos tienen la posibilidad de ser administrables, con lo cual se brinda mayor control y confiabilidad a la red. (Exploration, 2016)

Figura 9. Dispositivos Activos de red



Fuente: SENA

**SWITCH:** Dispositivo de transmisión de datos con características administrables y de alto rendimiento.

**ROUTER:** Dispositivo que permite la interconexión de varias redes.

**BRIDGE:** Dispositivo que une dos tipos de redes y con la posibilidad de creación de subredes; permite ampliar la extensión de la red.

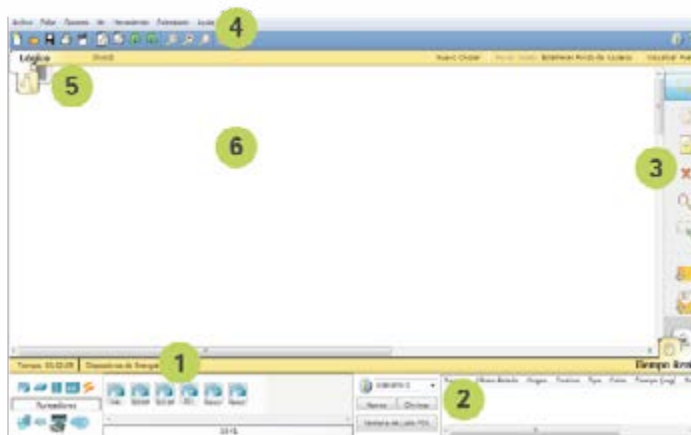
**Access Point (AP):** Dispositivo que permite la interconexión inalámbrica a la red.

## SOFTWARE DE SIMULACION REDES PACKET TRACER

PT (Packet Tracer), es una herramienta de aprendizaje y simulación de redes interactiva. Esta herramienta permite crear tipologías de red, simular una red con múltiples representaciones visuales, principalmente es una herramienta de apoyo didáctico.

Permite a los estudiantes crear redes con un número casi ilimitado de dispositivos y experiencias de solución de problemas sin tener que comprar *routers* o *switches* reales. Así mismo, les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Packet Tracer se enfoca en apoyar mejor los protocolos de redes que se enseñan en el currículum de la certificación cisco.

Figura 10. Esquema packet tracer



Fuente: (Programa Packet Tracer, 2016)

En este programa se crea la topología física de la red simplemente arrastrando los dispositivos a la pantalla. En este programa se puede ingresar a sus consolas de configuración; allí están soportados todos los comandos del Cisco IOS e incluso funciona el 'intérprete de línea de comandos'. Una vez completada la configuración física y lógica, también se puede hacer simulaciones de conectividad (pings "Buscador o rastreador de paquetes en redes, 'traceroutes' consola de diagnóstico de redes de Linux, entre otros).

Todo ello desde la misma aplicación simulando las consolas. De acuerdo al gráfico, se indican las secciones por su numeral

1. Aquí se indican los equipos de redes (*routers*, *switches*, *hubs*, *pc*, entre otros) y también se encuentran los conectores (es el ícono del rayo), es decir, los cables para que los equipos se puedan conectar (cable derecho, cruzado, serial, etc).
2. En esta parte, se encuentran los escenarios donde muestra información de los PDU enviados.
3. Se observan herramientas para poder modificar la topología. Se tiene el cuadrado punteado con una flecha que sirve para arrastrar equipos, cambiar la interfaz a la cual se conectar los cables y muchas cosas más. Se cuenta también con el ícono de la mano, el cual sirve para mover la topología completa, está el ícono del papel que sirve para poner anotaciones o colocar notas, es decir, si se tiene una topología bastante amplia, lo que se puede hacer con esta herramienta es agregar información que sea útil para no caer en errores de equipos, direcciones IP, etc. La cruz roja sirve para eliminar equipos y cables y por último los sobres. Hay dos el primer sobre (ícono de sobre cerrado) sirve para mandar un pdu simple y el otro cumple la misma función solamente que en este último

se le puede configurar el TTL, TOS. Se recomienda que cuando quiera mandar un PDU use el simple (ícono de sobre cerrado).

4. La ya conocida barra de menú, se puede hacer lo mismo que se hace con cualquier programa, guardar, salir, abrir, entre otras opciones.
5. En la imagen hay 2 espacios de trabajo, uno lógico y otro físico. El espacio lógico es donde se arma la topología, ya sea grande, chica, mediana y se tiene todo ahí. En cambio en el espacio físico, como es un programa que simula redes, se puede armar conexiones entre distintas zonas y lo que muestra es como sería en la vida real la red que se está armando, básicamente se muestra eso. Generalmente se trabaja en el espacio lógico.
6. En esta parte es donde va a crear su propio diseño o topología.





# Glosario

**DHCP (Dynamic Host Configuration Protocol):** Un protocolo de configuración con estado 'stateful' que proporciona direcciones IP y otros parámetros de configuración para conexión a una red IP.

**Dirección anycast:** Es una dirección del rango reservado para las direcciones unicast que identifica múltiples interfaces y es empleada para la entrega de uno a uno-entre-varios. Con un rutado apropiado, los datagramas dirigidos a una dirección de tipo anycast serán entregados en un único interfaz, el más cercano.

**Dirección anycast de router de subred:** Dirección anycast (prefijo de 64 bits::) que se asigna a las interfaces de los routers.

**Dirección MAC:** Dirección de nivel de enlace de tecnologías típicas de redes locales como Ethernet, Token Ring y FDDI. También se la conoce como dirección física, dirección del hardware o dirección del adaptador de red.

**Dirección multicast:** Es una dirección que identifica múltiples interfaces y que se emplea en entregas de datos uno-a-muchos. Mediante la topología de rutado multicast apropiada, los paquetes dirigidos a una dirección multicast se entregarán a todas las interfaces identificadas por ella.

**Dirección unicast:** Dirección que identifica a una única interfaz y que permite comunicaciones punto a punto a nivel de red. El alcance o ámbito de utilización de esa dirección es precisamente aquél en el que esa dirección es única.

**Dirección de uso local:** Dirección unicast IPv6 que no es alcanzable en la Internet IPv6. Las direcciones de uso local incluyen direcciones locales del enlace y direcciones locales del sitio.

**DNS (Domain Name System):** Servidor de nombre de dominio.

**IANA (Internet Assigned Numbers Authority):** Es la entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet.

**IETF (Internet Engineering Task Force) (en español, Grupo de Trabajo de Ingeniería de Internet1):** Es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas como: transporte, encaminamiento, seguridad. Se creó en los Estados Unidos, en 1986.

**ISP:** Proveedor de servicios de Internet

**Máquina (host):** Un nodo que no puede reenviar datagramas no originados por sí mismo. Una máquina es típicamente el origen y destino del tráfico IPV6 y va a descartar discretamente el tráfico que no esté dirigido específicamente a él mismo.

**PDU (Unidad de datos del protocolo):** Conjunto de datos correspondiente a una capa concreta en una arquitectura de red en capas. La unidad de datos de la unidad n se convierte en la carga útil de la capa n-1 (la capa inferior).

**Subred:** En IPV6 uno o más enlaces que utilizan el mismo prefijo de 64 bits.





# Bibliografía

Cisco CCNA Exploration. (2016). *Cisco networking*. Consultado el 24 de noviembre de 2016, en <http://www.cisco.com/c/en/us/index.html>

Vallehermoso, J. (2016). *Dispositivos Pasivos y Activos (Redes)*. Consultado el 22 de noviembre de 2016, en <http://georgehard.blogspot.com.co>

Mbc. (2016). *Equipos Activos de Red*. Consultado el 24 de noviembre de 2016, en <http://www.mbcpro.com>

D-link. (2016). *Routers*. Consultado el 24 de noviembre de 2016, en <http://www.dlink.com/es/es>

Amazon. (2016). *Switch*. Consultado el 24 de noviembre de 2016, en <https://www.amazon.com>



# Creative Commons



ATRIBUCIÓN, NO COMERCIAL, COMPARTIR IGUAL

Este material puede ser distribuido, copiado y exhibido por terceros si se muestra en los créditos. No se puede obtener ningún beneficio comercial y las obras derivadas tienen que estar bajo los mismos términos de licencia que el trabajo original.





# Créditos

PROGRAMA	Configuración de dispositivos activos para servicios de red con IPV6
NOMBRE DEL OBJETO	Configuración de dispositivos activos y servicios para IPV6
EXPERTO TEMÁTICO	Fabio Enrique Combariza Nocua
DISEÑADORES GRÁFICOS	Caren Xiomara Carvajal Pérez Luis Guillermo Roberto Báez Luis Carlos Reyes Parada
GESTORAS DE REPOSITORIO	Nancy Astrid Barón López Milady Tatiana Villamil Castellanos
PROGRAMADORES	Nilda Inés Camargo Suescún Fredy Velandia Figueroa Wolfran Alirio Pinzón Murillo
GUIONISTA Y PRODUCTOR DE MEDIOS AUDIOVISUALES	Jheison Edimer Muñoz Ramírez
GUIONISTA	Adriana Carolina Acosta Caycedo
ASESORAS PEDAGÓGICAS	Kennia Andrea Peña Barrera Janet Lucia Villalba Triana
LÍDER DE LA LÍNEA DE PRODUCCIÓN	Zulma Yurany Vianchá Rodríguez