INTRODUCCIÓN

En la actualidad las exigencias laborales hacen que los candidatos a diferentes puestos de trabajo deban tener una rigurosa preparación, no solo a nivel universitario y lingüístico sino también en especializaciones de diversos fabricantes. Estas especializaciones convalidan conocimientos, habilidades y requisitos propios de ese fabricante, que es lo que se denomina certificación.

Una persona en posesión de un título de grado académico puede completar su capacitación a través de una o varias certificaciones acordes a las tareas que desee desarrollar en su ámbito laboral. Por lo tanto, una certificación permite, por ejemplo, que un ingeniero que posee un abanico muy amplio de conocimientos pueda especializarse aún más, o que un técnico informático pueda reorientar su formación hacia otros aspectos de la vida laboral. Lo que es aun igual de importante es la posibilidad que brindan las certificaciones a todos aquellos que por diversas circunstancias no poseen títulos académicos y quieran especializarse. Estas personas que hasta ahora quedaban fuera del contexto de las especializaciones podrán obtener el conocimiento necesario que les permitirá entrar y ser parte de una carrera laboral especializada.

Una certificación es entonces una calificación obtenida por una persona a través de un organismo certificador que ha cumplido con los requisitos mínimos impuestos por dicha entidad. Las empresas o fabricantes utilizan estos organismos como herramientas para otorgar sus certificaciones a través de evaluaciones teórico-prácticas, no obstante estos no intervienen en la elaboración de los tópicos o temarios que son propios de cada fabricante.

Desde que Cisco Systems creó la carrera de certificaciones en el año 1998, estas se han ido ampliando y mejorando según las exigencias y evolución del mercado, empresas y profesionales.

Para obtener la certificación CCNP *Routing* y *Switching* será necesario estar en posesión de la certificación CCNA R&S.

A partir de 2015 la configuración de la certificación CCNP establece un mayor grado de especialización en cada una de las ramas que componen la carrera profesional de Cisco.

- CCNP Cloud
- CCNP Collaboration
- CCNP Data Center
- CCNP Routing and Switching
- CCNP Security
- CCNP Service Provider
- CCNP Voice
- CCNP Wireless

La certificación CCNP R&S se compone de tres exámenes con un alto nivel de exigencias teórico-prácticas. Dichos exámenes están disponibles hasta el momento únicamente en inglés y japonés y no importa el orden en que se presenten.

Los exámenes correspondientes a la certificación **CCNP Routing y Switching** son los siguientes:

- **300-101 ROUTE**, Implementing Cisco IP Routing
- **300-115 SWITCH**, Implementing Cisco IP Switched Networks
- **300-135 TSHOOT**, Troubleshooting and Maintaining Cisco IP Networks

El examen **ROUTE 300-101** es un examen de calificación válido para las certificaciones Cisco CCNP *Routing* y *Switching* y CCDP. Este examen valida los conocimientos avanzados de direccionamiento IP, enrutamiento, implantación de *routers* Cisco en redes escalables LAN, WAN e IPv6. Tanto para redes empresariales, como sucursales y trabajadores móviles. El examen tiene una duración de 120 minutos y entre 45-65 preguntas.

El examen **SWITCH 300-115** certifica los conocimientos y habilidades de los candidatos en conmutación. Este examen valida los conocimientos en la planificación, configuración, verificación e implementación de soluciones de conmutación en redes empresariales complejas que utilizan la arquitectura empresarial de Cisco. El examen tiene una duración de 120 minutos y entre 30-40 preguntas.

El examen **TSHOOT 300-135** certifica que el candidato posee los conocimientos y habilidades necesarios para planificar y realizar un mantenimiento regular de una red empresarial compleja a nivel de enrutamiento y de conmutación. El examen tiene una duración de 120 minutos y entre 15-25 preguntas.

Los autores han cuidado celosamente la manera de compilar todo el material en un solo volumen en español manteniendo la terminología técnica en inglés como se utiliza generalmente en los ambientes laborales y en los propios exámenes. De esta manera se consigue eliminar la barrera idiomática sin desvirtuar el verdadero sentido de la certificación.

Sobre los autores fluye una larga trayectoria en el ámbito técnico y educativo y una lista de certificaciones como CCAI, CCNP, CCIE, entre otras. Su experiencia en publicaciones anteriores aporta y reafirma la calidad del material de este libro filtrando lo innecesario, valorando lo fundamental para volcarlo de manera racional sobre el papel.

Requisitos para la certificación CCNP

Para aquellos que persiguen la certificación CCNP R&S, deben saber que para obtenerla además de los tres exámenes es necesario poseer la certificación CCNA R&S y que tanto una como la otra caducan a los tres años. Los técnicos que estén en posesión de la certificación CCNA R&S cuya fecha de caducidad esté próxima, podrán mantenerla vigente si presentan alguno de los tres exámenes del CCNP R&S antes de la prescripción del CCNA.

Una buena recomendación es comenzar la lectura de este libro con tiempo suficiente, efectuar las prácticas y los test necesarios y, por qué no, realizar los cuestionarios en inglés.

Para los técnicos CCNP que deban recertificarse o solo necesitan material de consulta, todo el contenido del libro ha sido revisado y actualizado de tal manera que no habrá obstáculos de entendimientos técnicos o idiomáticos y será sin duda un beneficio añadido para la resolución de incidencias o nuevas configuraciones.

Los exámenes constan de diferentes tipos y modalidades de preguntas:

- Respuesta única a partir de opciones múltiples.
- Respuestas múltiples a partir de opciones múltiples.
- Respuestas tipo *drag and drop*.
- Completar los espacios en blanco.
- Configuración de *routers* y *switches* con simulador.

Para mayor información sobre localización de centros de certificación autorizados, requisitos, horarios, precios u otro tipo de información puede consultarse la web de Pearson-Vue: *http://www.vue.com*.

Los estudiantes que deseen presentarse al examen de certificación CCNP deben cumplir las políticas de privacidad de Cisco Systems:

- Las personas de entre 13 y 17 años pueden presentarse al examen de certificación con el consentimiento de los padres o tutores.
- Las personas mayores de 18 años pueden presentarse sin ningún tipo de restricción.
- Los menores de 13 años no pueden presentarse al examen.

Los candidatos deben asumir el compromiso de integridad y confidencialidad de Cisco prohibiendo acciones que describan cualquier información acerca del examen de certificación.

http://www.cisco.com/web/learning/downloads/certificationNDA.pdf

Para mayor información respecto a duración de los exámenes, idiomas disponibles o cualquier otro tipo de duda sobre la certificación CCNP es posible consultar la web de Cisco:

http://www.cisco.com/web/learning/le3/le2/le37/le10/learning_certification_type_home.html

Acerca de los autores

Ernesto Ariganello es ingeniero en telecomunicaciones, instructor certificado de Cisco Networking Academy, imparte cursos relacionados con redes y comunicaciones. Especialista en electrónica de hardware de alta complejidad, posee varias certificaciones entre ellas el CCNP. Es, además, consultor especializado en comunicaciones de datos para varias empresas de la Unión Europea. Su trabajo en educación y formación es sumamente valorado en Europa y Latinoamérica, fundamentado en clases claras, dinámicas y muy prácticas por donde han pasado más de 800 alumnos en diferentes centros de formación y empresas.

Enrique Barrientos Sevilla comenzó su carrera técnico-profesional en el año 2003. Desde entonces ha compaginado su labor en las telecomunicaciones con la formación en nuevas tecnologías, impartiendo cursos en varias especialidades tales como Cisco y Microsoft.

Ha trabajado en proyectos de grandes magnitudes para varias de las más importantes empresas españolas, irlandesas y norteamericanas del sector. Posee varias certificaciones de diversos fabricantes entre las que destaca el CCIE #23973 en la especialidad de *Routing* y *Switching*.

Actualmente es un referente dentro del grupo de Arquitectura de Red de un importante ISP en Estados Unidos. Su pasión por la formación ha sido, sin duda, un aporte fundamental para la creación de este libro.

Agradecimientos de Ernesto

Este libro ha significado un trabajo enormemente agotador, incalculables horas dedicadas a que todo encaje perfectamente para que el material sea lo más fidedigno posible. Sin embargo, una vez que está en mis manos es sumamente reconfortante saber que servirá a muchos en su afán de aprender y crecer profesionalmente. Son ellos y su esfuerzo de superación lo que inspira y justifica tanto trabajo.

Por supuesto como siempre a todos los que de alguna manera hacen posible directa e indirectamente esta nueva edición, mi familia, amigos, alumnos, y compañeros de trabajo.

No puedo olvidarme de Enrique Barrientos Sevilla, mi compañero de batalla con quien he compartido, a más 8.500 kilómetros de distancia, el desarrollo de esta edición.

Para todos ellos mis agradecimientos.

Ernesto Ariganello

Agradecimientos de Enrique

Gracias a Gen, Olaya e Ivy, por convertir cada día en una nueva aventura llena de sorpresas increíbles.

Enrique Barrientos Sevilla

Convenciones sobre sintaxis de comandos

Las convenciones que se utilizan para representar la sintaxis de comandos en este libro son las mismas que se utilizan en **Cisco IOS Command Reference**. Los autores han preferido conservar los argumentos en idioma inglés tal como aparecerían tras ejecutar un comando de ayuda.

- La **negrita** representa comandos y palabras clave que se escriben tal y como se muestra.
- La *cursiva* indica argumentos para los que hay que suministrar valores.
- Los corchetes [ ] indican elementos opcionales.
- Las llaves { } contienen una elección de palabras clave necesarias.
- Las barras verticales | separan elementos alternativos y exclusivos entre sí.
- Las llaves y las barras verticales entre corchetes, por ejemplo [x {y | z}] indican una opción necesaria en un elemento opcional. No es necesario introducir lo que hay entre los corchetes, pero si lo hace, tendrá algunas opciones necesarias en los corchetes.

Advertencia

Se ha realizado el máximo esfuerzo para hacer de este libro una obra tan completa y precisa como sea posible, pero no se ofrece ninguna garantía implícita de adecuación a un fin en particular. La información se suministra "tal como está". Los autores no serán responsables ante cualquier persona o entidad con respecto a cualquier pérdida, daño o perjuicio que pudieran resultar emergentes de la información contenida en este libro.

Todos los términos mencionados en este libro que, según consta, pertenecen a marcas comerciales o marcas de servicios, se utilizan únicamente con fines educativos. No debe considerarse que la utilización de un término en este libro afecte a la validez de cualquier marca comercial o de servicio.

Los conceptos, opiniones y gráficos expresados en este libro por los autores no son necesariamente los mismos que los de Cisco Systems, Inc.

Los iconos y topologías mostradas en este libro se ofrecen con fines de ejemplo y no representan necesariamente un modelo de diseño para redes.

Las configuraciones y salidas de los *routers*, *switches* y/o cualquier otro dispositivo se han tomado de equipos reales y/o simuladores y se ha verificado su correcto funcionamiento. No obstante, cualquier error en la transcripción es absolutamente involuntario.

1

DISEÑO DE REDES

1.1 REDES DE CAMPUS

Una red de campus consiste en un conjunto de redes LAN en uno o varios edificios, esas LAN pueden utilizar diferentes tecnologías y suelen estar situadas normalmente en la misma área geográfica.

En el diseño de las redes de campus resulta fundamental conocer el flujo de tráfico para poder realizar ese diseño lo más eficientemente posible. En el diseño de redes de campus existen diversos modelos según el tipo y necesidad de diseño:

- **Red compartida**
- **Segmentación de LAN**
- **Tráfico de red**
- **Red predecible**
- **Red jerárquica**

1.1.1 Modelo de red compartida

En este modelo la disponibilidad y el rendimiento son inversamente proporcionales al número de *hosts* que estén en él, puede utilizar tecnologías que utilicen metodologías de máximo esfuerzo, como Ethernet o deterministas como Token Ring. También se debe tener en cuenta que en sistemas de máximo esfuerzo las colisiones pueden ocurrir, y de hecho ocurren, sin embargo en las tecnologías de *token* como Token Ring esto no ocurre porque la ocupación del medio va por turnos o *tokens* de manera ordenada y precisa.

Para solucionar el problema del rendimiento en la red compartida se puede optar por dividir la red en distintos dominios de colisión, mediante *bridges* o *switches*.

En el caso del *broadcast* y del *multicast* se produce una inundación por el total de puertos y en el caso del *broadcast* las tramas son leídas y procesadas por todos los *hosts* del segmento, a diferencia del tráfico de *multicast* que solo es procesado por los *hosts* del segmento que están suscritos al grupo de *multicast* en concreto.

Si se analiza el tráfico de una red compartida se podrá ver la relación directa que existe entre el número de *hosts* y el número de tramas de *broadcast*, ya que son muchos los protocolos que utilizan *broadcast* en capa 2, como por ejemplo DHCP, GNS, ARP, etc.

En este modelo hay que destacar que existe el problema añadido de que los dispositivos de capa 2 permiten pasar los *broadcast* y *multicast*, así que el rendimiento de la red mejorará, pero extendiendo los *broadcast* de capa 2 más allá de los límites establecidos por los *switches* y *bridges* de capa 2.

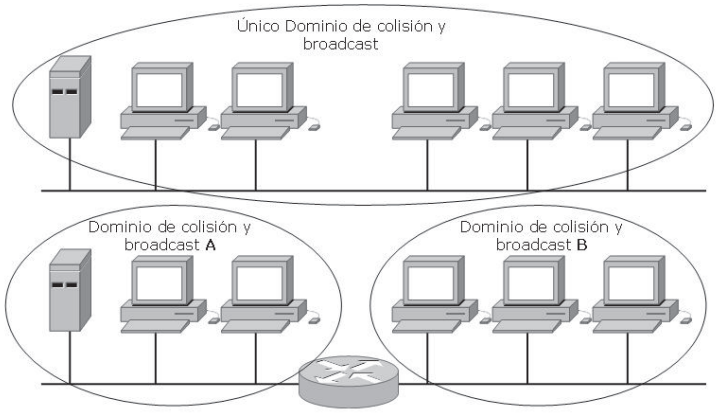
1.1.2 Modelo de segmentación de LAN

El modelo de segmentación de LAN va más allá que el modelo de red compartida porque no se permite que los *broadcast* de capa 2 se extiendan más allá de los límites establecidos, esto se hace dividiendo la red en varias LAN o VLAN. Para ello se establecen los límites de los segmentos utilizando dispositivos de capa 3, de esta forma se limitarán los *broadcast* de capa 3.

Los dispositivos de nivel 3 que se pueden utilizar en este modelo son *routers* o *switches* de capa 3, los cuales proporcionan todas las ventajas de los dispositivos de capa 2, pero además añaden una segmentación al nivel lógico establecido en la capa 3, con lo que el rendimiento mejora también en el caso de disponer de *broadcast* de capa 2.

La segmentación se puede realizar dividiendo en LAN o en VLAN, la diferencia básica reside en que la LAN utilizará todo el medio para ella sola, mientras que la VLAN utilizará un etiquetado o encapsulado que permitirá diferenciar el tráfico de una VLAN con el de otra, de esta forma el tráfico no se mezclará pudiendo disponer de una segmentación lógica que permitirá una flexibilidad mucho más grande.

El siguiente ejemplo ilustra un modelo de segmentación con un *router*:



1.1.3 Modelo de tráfico de red

Este modelo se basa en el movimiento de información dentro de la red. En redes corporativas estándar se puede aplicar el modelo del 80/20, es decir, el 80% del tráfico se queda en el segmento local y solo el 20% del tráfico atraviesa el *core* de la red. Esta situación puede parecer la más normal, pero habrá que tener en cuenta que existen redes en las cuales el tráfico mayoritariamente atraviesa el *core* de la red, por ejemplo, una red de una empresa de *hosting* en la que la mayoría del tráfico no es interno sino que es tráfico que va a salir a Internet y que atravesará el *core* o núcleo de la red.

El modelo del 80/20 puede ser uno de los modelos más comunes utilizados, pero implica que los servidores de aplicación se encuentran más cerca del usuario y no se dispone de servicios centralizados masivos.

Este modelo tiene una serie de requisitos importantes:

- Los recursos más utilizados tienen que estar lo más próximos al usuario como sea posible.
- Las aplicaciones tienen que estar distribuidas de forma que el tráfico se quede siempre que sea posible en el segmento local.
- Los usuarios con idénticos requisitos tienen que estar lo más próximos posible, ya sea proximidad física en el caso de LAN o proximidad lógica en el caso de VLAN.

Este modelo puede sin embargo ser complejo para el administrador de la red y puede no ser viable si la utilización de aplicaciones cliente-servidor es muy extensa.

En el caso de disponer de una red en la que la arquitectura cliente-servidor sea la predominante, entonces lo conveniente es el entorno 20/80, en el cual la mayoría del tráfico atravesará el *core* de la red; por supuesto esta otra visión requerirá que el diseño de la red sea totalmente diferente y adaptado a esas necesidades. Este modelo se describe a continuación.

1.1.4 Modelo de red predecible

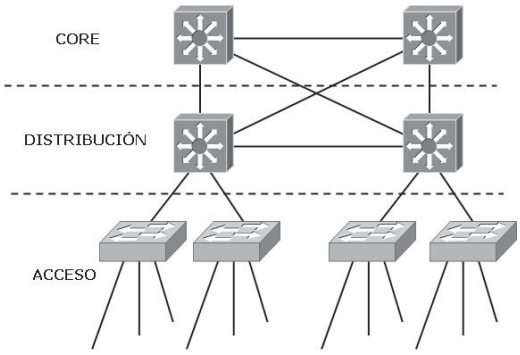
El modelo predecible tiene que ser el modelo que permita adaptar la topología de la red a los requisitos del tráfico y que haga posible el menor mantenimiento. Este modelo afrontará el desafío del entorno 20/80 y deberá estar basado en varias capas, las cuales serán acceso, distribución y *core*, que se describen posteriormente.

1.2 MODELO DE RED JERÁRQUICO

Este modelo es el modelo más conocido de Cisco y se basa en dividir la red de forma lógica en tres niveles o capas:

- **Acceso**
- **Distribución**
- **Core**

Cada uno de estos niveles realizará una función bien diferenciada y permitirá que el tráfico pueda ser tratado de forma independiente según el lugar de la red en que se encuentre. El resultado es una topología escalable, fácilmente modificable y aislable que permite un trabajo óptimo, lamentablemente no todas las redes de empresas tienen suficiente estructura como para poder montar claramente un modelo jerárquico, sin embargo para redes de tamaño considerable esta opción termina por ser la única viable.



1.2.1 Nivel de acceso

El nivel de acceso es el más próximo al usuario y donde se conectan los *hosts*. En este nivel comúnmente se dispone de *switches* de capa 2 con una gran densidad de puertos, con dispositivos de bajo coste. En este nivel también hay que tener en cuenta que es donde se concentra el tráfico de usuario que tiene que ir al nivel superior, con lo que es necesario tener en cuenta que los *switches* de acceso tendrán que disponer de puertos de *uplink* que típicamente soportarán varias VLAN.

Es en este nivel donde se aplican los primeros filtros al tráfico, se definen VLAN y se comienza a aplicar **QoS** (Calidad de Servicio).

1.2.2 Nivel de distribución

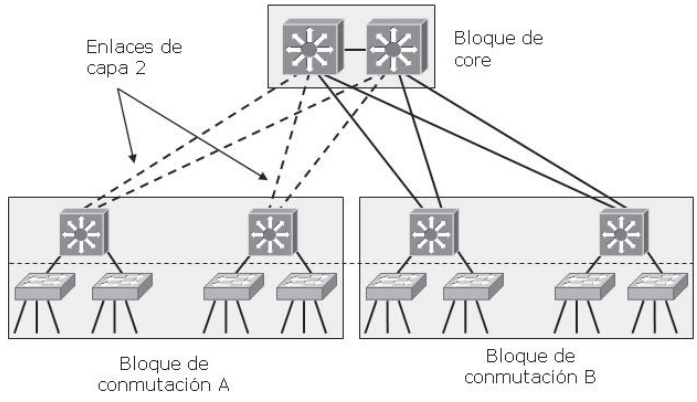
Este nivel es el encargado de comunicar la capa de acceso con la de *core* y de interconectar varios niveles de acceso diferentes. Es en este nivel donde se agregará el tráfico proveniente de las capas inferiores y el primer lugar donde se comenzará a utilizar *switching* de capa 3 para poder hacer la interconexión entre redes. En este nivel es muy importante que los equipos dispongan de puertos de alta velocidad, donde la QoS tiene una presencia más persistente. Al ser el primer nivel en implementar la capa 3 será hasta aquí donde lleguen los *broadcast* de las capas inferiores y donde se implementarán políticas de filtrados (ACL).

1.2.3 Switch de capa 2 en distribución

Como se ha dicho anteriormente es posible utilizar *switches* de capa 2 en capa de distribución, pero este diseño tiene sus problemas, aunque puede ser recomendado en el caso de que no se disponga de suficientes recursos como para utilizar dispositivos de capa 3 en la capa de distribución de los diferentes bloques.

Aunque esta práctica tiene varios problemas hay que tener en cuenta los principales que están relacionados con la extensión y contención de VLAN y la utilización de Spanning Tree.

En cuanto a las VLAN, la utilización de *switches* de capa 2 en distribución provocará que todo el tráfico de las VLAN escale hasta el *core*, pasando los *broadcast* y todo el tráfico no necesario, redundando en una utilización poco óptima de enlaces de *uplink*.



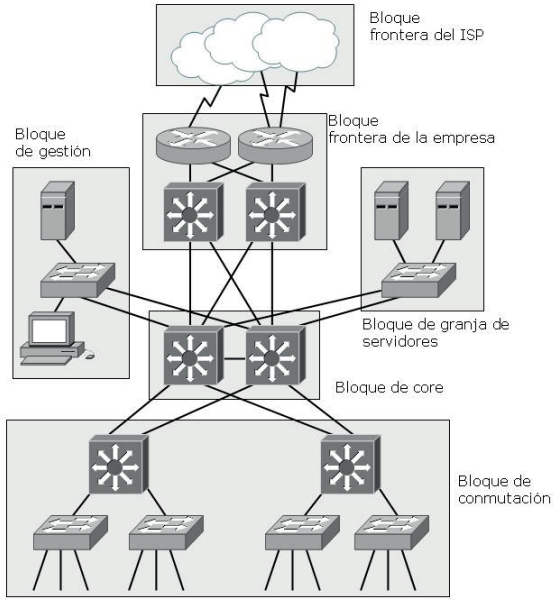
La redundancia de nivel 3 entre distribución y *core* no podrá ser posible debido a que no existen protocolos de enrutamiento para realizar el balanceo de tráfico, así que la mala utilización de los *uplinks* por la extensión de las VLAN se verá drásticamente empeorada por la imposibilidad de balancear el tráfico con STP estándar.

1.2.4 Nivel de core

Este nivel tiene una única y principal función que es mover el tráfico lo más rápidamente posible suministrando comunicación hacia el exterior sin realizar ninguna tarea más que no sea imprescindible.

1.3 DISEÑO MODULAR DE RED

Aunque en párrafos anteriores se haya descrito el diseño de red por capas también es posible definir este diseño mediante lo que se llama bloques. Estos bloques son unidades lógicas funcionales de equipos que ofrecen un servicio determinado.



Los bloques en los cuales se puede definir una red de campus son los siguientes:

- **Bloque de conmutación**: *switches* de acceso junto con sus *switches* de distribución.
- **Bloque de core**: el *backbone* de la red.
- **Bloque de granja de servidores**: conjunto de servidores con sus *switches* de acceso y distribución.
- **Bloque de gestión**: recursos de gestión de red con sus *switches* de acceso y distribución.
- **Bloque de frontera de la empresa**: recursos necesarios para conectar la empresa al exterior con sus *switches* de acceso y distribución.
- **Bloque de frontera del ISP**: servicios externos del ISP contratados por la empresa con sus interfaces al bloque de frontera de la empresa.

1.3.1 Bloque de conmutación

El bloque de conmutación contiene dispositivos de conmutación del nivel de acceso y distribución. Hay que tener en cuenta que todos los bloques tienen que estar conectados al bloque de *core* para proporcionar conectividad extremo a extremo en toda la red. El bloque de conmutación por un lado tendrá los *switches* de capa 2 de acceso y por otro lado tendrá *switches* de capa 3 de distribución, es decir, en este nivel hay funcionalidades tanto de capa 2 como de capa 3.

En este bloque los usuarios finales se conectan al *switch* de acceso mediante un puerto dedicado, los *switches* de acceso se conectan a los *switches* de distribución de la misma forma y los de distribución a su vez conectarán el bloque con el bloque de *core*. Este bloque proporciona, además, un blindaje en cuanto al tráfico, ya que los *broadcast* no deben ir más allá del bloque y por supuesto el protocolo Spanning Tree también queda confinado en el bloque. En este tipo de bloque es muy importante que las VLAN se queden en el mismo y que no salgan de ahí, ya que es conveniente que el tráfico de *broadcast* no circule por el *core*. La forma de evitar esto es limitando los dominios de difusión.

1.3.2 Dimensionamiento del bloque de conmutación

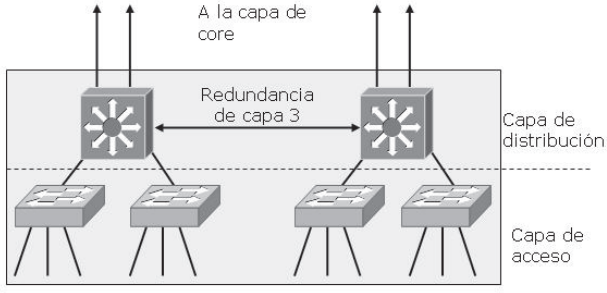
Los bloques de conmutación no pueden ser tan grandes como usuarios haya en la organización, muchas veces es necesario dividirlos, pero teniendo en cuenta una serie de factores que afectan al diseño.

Para poder dimensionar adecuadamente el bloque de conmutación se debe tener en cuenta los patrones de tráfico, la capacidad de conmutación de capa 3 en la capa de distribución, números de usuarios, límites de las VLAN o incluso el tamaño de los dominios de Spanning Tree. Lamentablemente el análisis de estos requerimientos a priori se encuentra fuera del ámbito del CCNP, pero lo que sí está dentro del ámbito es detectar el momento en el que ese bloque de conmutación se queda pequeño, esto sucede cuando:

- Los *routers* de capa 3 de la capa de distribución son un cuello de botella y los recursos de CPU aumentan demasiado.
- Los *broadcast* y *multicast* provocan lentitud en los *switches* del bloque.

Para diseñar correctamente el bloque de conmutación es necesario proporcionar a los *switches* de acceso enlaces redundantes a los *switches* de distribución, y estos últimos pueden balancear el tráfico a los equipos de *core* ya que al ejecutar protocolos de enrutamiento de capa 3 es posible realizar este tipo

de configuración. Para proporcionar una redundancia adecuada los dos *uplinks* de los *switches* de acceso tienen que estar conectados a dos *switches* de distribución, proporcionando redundancia uno del otro.



Aunque el tema de la virtualización queda también fuera del temario del CCNP e incluso también fuera del CCIE, existen ya técnicas para proporcionar redundancia en capa 2 como es el uso de la tecnología VSS de Cisco Systems y utilizando EtherChannels y eliminando el uso de Spanning Tree entre los *switches* de acceso y los de distribución, o incluso sin tener virtualización se puede proporcionar una redundancia mediante MSTP (tema que se explicará más adelante) balanceando unas VLAN por un *trunk* y otras VLAN por otro *trunk*, de esta manera se proporciona un balanceo de tráfico entre los dispositivos de capa 2 de acceso y distribución. Por supuesto también existen otras posibilidades similares utilizando virtualización en otros fabricantes, actualmente en Juniper y Nortel, además de Cisco. Posibilidades de balanceo existen en capa 2, pero estas mejoras no han estado disponibles hasta finales de 2008 y solo en la gama 6500 de Cisco, así que esa es la razón por la que este tema no se incluye en el CCNP, al menos de momento.

1.3.3 Bloque de core

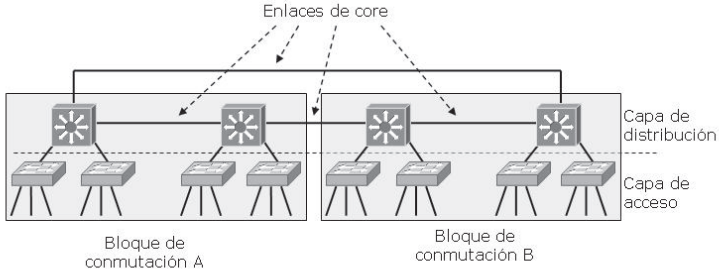
Para conectar al menos 2 bloques de conmutación es necesaria la existencia del bloque de *core* en la red. El bloque de *core* puede funcionar con prácticamente cualquier tecnología, aunque este libro se va a centrar en enlaces gigabit ethernet y 10 gigabit ethernet.

Su función principal, como se ha explicado anteriormente, es mover los datos de la forma más rápida posible, esa es la razón por la que antiguamente este bloque funcionase únicamente en capa 2, pero actualmente los precios de los *switches* de capa 3 ya no son los mismos y hoy en día este bloque se construye sobre *switches* multicapa.

Para el diseño de este bloque existen dos posibilidades principales:

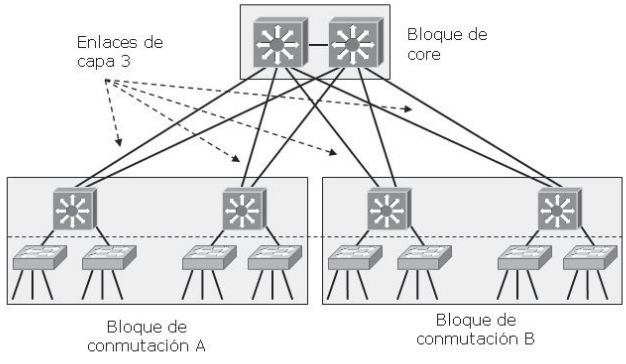
- **Bloque colapsado**, es aquel en el que la jerarquía del bloque de *core* está colapsada con el nivel de distribución de los otros bloques, es decir, el bloque de acceso se divide en acceso y distribución, el nivel de acceso se queda en el bloque de conmutación y el bloque de distribución pasa al bloque de *core*.

  De esta forma se ahorran equipos en los bloques de conmutación, pero los *broadcast* de nivel 3 y las VLAN llegan hasta el *core*, lo cual podría afectar al rendimiento. Este tipo de *core* solo podría tener sentido en redes pequeñas.



  Hay que tener en cuenta que este modelo no es escalable ya que no puede extenderse demasiado.

- **Core dual**, este tipo de *core* contacta de forma redundante dos o más bloques de conmutación y en él está totalmente diferenciado el nivel de distribución con nivel 3, que se queda en cada uno de los bloques de conmutación, y el nivel de *core*, con lo que el tráfico de *broadcast* de nivel 3 se queda en cada uno de los bloques de conmutación y no llega hasta el bloque de *core*.



La ventaja fundamental del bloque de *core* funcionando como *dual core* es que es posible utilizar *uplinks* de cada uno de los bloques de conmutación de forma paralela y balanceada. Esto es posible gracias a los protocolos de enrutamiento de capa 3, que permiten balancear el tráfico de esta manera, gracias a que los *switches* de distribución de los bloques de conmutación y los *switches* del *core* son *switches* de capa 3.

1.3.4 Tamaño del core en una red de campus

Una consideración muy importante e interesante a tener en cuenta es relativa al tamaño del *core* en una red de campus.

El tamaño es totalmente dependiente del número de bloques que existan por debajo del bloque de *core*, se ha de tener en cuenta que cada bloque tendrá dos *uplinks* hacia el *core* que deben ser *non-blocking*, es decir, los *switches* de *core* tienen que tener la capacidad de aceptar que las interfaces puedan estar al 100% de capacidad.

Otro factor a tener en cuenta en cuanto al tamaño es el o los protocolos de enrutamiento a utilizar. Ya se ha dicho que se ejecutará un protocolo de enrutamiento entre los bloques para poder ofrecer redundancia y balanceo entre los *uplinks* de los bloques de conmutación hacia el bloque de *core*, cuanto más grande sea la red más actualizaciones de enrutamiento serán necesarias y esto puede afectar al rendimiento. Estas limitaciones son las responsables de determinar si son necesarios más equipos o más grandes y potentes en el bloque de *core*.

1.4 PROTOCOLOS DE DESCUBRIMIENTO

1.4.1 CDP

El protocolo **CDP** (*Cisco Discovery Protocol*) se utiliza para obtener información de *routers* y *switches* que están conectados localmente. El CDP es un protocolo propietario de Cisco, destinado al descubrimiento de vecinos y es independiente de los medios y del protocolo de enrutamiento. Aunque el CDP solamente mostrará información sobre los vecinos conectados de forma directa, constituye una herramienta de gran utilidad.

El Protocolo de Descubrimiento de Cisco (CDP) es un protocolo de capa 2 que conecta los medios físicos inferiores con los protocolos de red de las capas superiores. CDP viene habilitado por defecto en los dispositivos Cisco, los dispositivos de otras

marcas serán transparentes para el protocolo. CDP envía actualizaciones por defecto cada 60 segundos y un tiempo de espera antes de dar por caído al vecino (*holdtime*) de 180 segundos.

1.4.1.1 Configuración

Como se explicó anteriormente CDP viene habilitado por defecto, sin embargo si fuera necesario configurarlo se ejecuta desde el modo global:

Router(config)#cHay dos formas de deshabilitar CDP, una es en una interfaz específica para que no funcione particularmente con las conexiones locales y la otra de forma general para que no funcione completamente en ninguna interfaz. Las sintaxis muestran los respectivos comandos desde una interfaz y de modo total.

```
Router#configure terminal
Router(config)# tipo y número de interfaz
Router(config-if)#no cdp enable

Router(config)#no cdp run
```

El ajuste de los temporizadores se realiza con los siguientes comandos.

```
Router(config)#cdp timer segundos
Router(config)#cdp holdtime segundos
```

1.4.1.2 Verificación

Mediante el comando **show cdp neighbors** se obtiene información sobre los dispositivos directamente conectados, pero con una visión muy reducida:

```
Switch-B# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
Switch-A Gig 1/1 105 S I WS-C3550-4Gig 0/1
Switch-C Gig 2/1 139 S I WS-C3550-4Gig 0/1
Router Gig 3/1 120 R Cisco 2610Fas 0/0
```

Existe también la opción de ampliar la información con el comando **show cdp neighbors detail**:

```
Switch-# show cdp neighbors detail
-------------------------
Device ID: Switch-B
Entry address(es): 192.168.254.17
Platform: cisco WS-C4506, Capabilities: Router Switch IGMP
Interface: GigabitEthernet0/1, Port ID (outgoing port): GigabitEthernet1/1
Holdtime : 134 sec
Version :
```

```
Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-I9S-M), Version 12.2(18)
EW, EARLY
DEPLOYMENT RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright 1986-2004 by cisco Systems, Inc.
Compiled Fri 30-Jan-04 02:04 by hqluong
advertisement version: 2
VTP Management Domain: ''
Duplex: full
Management address(es):
```

La lectura del comando **show cdp neighbors detail** es idéntica al **show cdp entry *** e incluye la siguiente información bien detallada:

- Dirección IP del *router* vecino.
- Información del protocolo.
- Plataforma.
- Capacidad.
- ID del puerto.
- Tiempo de espera.
- La ID del dispositivo vecino.
- La interfaz local.
- Los siguientes datos se agregan en el CDPv2:
- Administración de nombres de dominio VTP.
- VLAN nativas.
- *Full* o *half-duplex*.

Otros comandos adicionales son:

- **show cdp traffic**. Para saber el tráfico de CDP en el *router*.
- **show cdp interface**. Muestra el estado de todas las interfaces que tienen activado CDP.
- **clear cdp counters**. Restaura los contadores a cero.
- **clear cdp table**. Borra la información contenida en la tabla de vecinos.

Los siguientes comandos pueden utilizarse para mostrar la versión, la información de actualización, las tablas y el tráfico:

- **show cdp traffic**
- **show debugging**
- **debug cdp adjacency**
- **debug cdp events**
- **debug cdp ip**
- **debug cdp packets**
- **cdp timer**
- **cdp holdtime**
- **show cdp**

NOTA:
Estos comandos únicamente sirven si todos los dispositivos de la red son Cisco y tienen el protocolo CDP habilitado.

1.4.2 LLDP

El protocolo **LLDP** (*Link Layer Discovery Protocol*) es similar a CDP pero se basa en el estándar IEEE 802.1ab. Como resultado LLDP funciona en redes de múltiples proveedores.

La información de los vecinos se anuncia mediante la agrupación de atributos en estructuras **TLV** (*Type-Length-Value*). Por ejemplo, un dispositivo puede anunciar su nombre de sistema con un TLV, su dirección de gestión en otro TLV, la descripción del puerto con otro TLV, sus requerimientos de energía en otro TLV, y así sucesivamente. Los anuncios LLDP se convierten en una cadena de varios TLV que pueden ser interpretados por el dispositivo receptor.

LLDP es compatible con los dispositivos que utilizan TLV adicionales tales como los teléfonos de VoIP, los **LLDP-MED** (*Media Endpoint Device*) proveen información más exacta acerca de las políticas de red, como número de VLAN, calidad de servicio necesaria para el tráfico de voz, administración de energía, gestión de inventarios y datos de localización física.

LLDP soporta por defecto LLDP MED TLV, pero no puede enviar simultáneamente la TLV básica y TLV-MED por un puerto del *switch*. LLDP envía solo los TLV básicos a los dispositivos conectados. Si un *switch* recibe un TLV-MED iniciará el envío de TLV-MED hacia el *switch* que inició el envío.

Por defecto el tiempo de actualización de los paquetes LLDP es de 30 segundos, el *holdtime* es de 120 segundos.

1.4.2.1 Configuración

Por defecto, LLDP está deshabilitado globalmente en un *switch* Catalyst. Para habilitarlo o deshabilitarlo utilice los siguientes comandos globales de configuración:

```
Switch(config)# lldp run
Switch(config)# end

Switch(config)# no lldp run
Switch(config)# end
```

Una vez LLDP está habilitado, los anuncios se envían y reciben en cada interfaz del *switch*. Es posible controlar el funcionamiento LLDP en una interfaz determinada con el siguiente comando:

```
Switch(config-if)# [ no ] lldp { receive | transmit }
```

1.4.2.2 Verificación

Para ver si se está ejecutando o no, utilice el comando **show lldp**.

```
Switch(config)# show lldp neighbors [ type member/module/number ] [ detail ]
```

Para obtener un resumen de los vecinos que han sido descubiertos:

```
Switch1# show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID Local Intf Hold-time Capability Port ID
Switch2 Gi1/0/24 113 B Gi2/0/24
APb838 Gi1/0/23 91 B,R Gi0
SEP2893FEA2E7F4 Gi1/0/22 180 B,T 2893FEA2E7F4:P1
Total entries displayed: 2
```

Para especificar un vecino descubierto por una interfaz determinada:

```
Switch1# show lldp neighbors gig1/0/22 detail
------------------------------------------------
Chassis id: 10.120.48.177
Port id: 2893FEA2E7F4:P1
Port Description: SW PORT
System Name: SEP2893FEA2E7F4.voice.uky.edu
System Description:
Cisco IP Phone 7942G,V6, SCCP42.9-3-1-1S
Time remaining: 124 seconds
System Capabilities: B,T
Enabled Capabilities: B,T
Management Addresses:
      IP: 10.120.48.177
Auto Negotiation - supported, enabled
Physical media capabilities:
      1000baseT(HD)
      1000baseX(FD)
      Symm, Asym Pause(FD)
      Symm Pause(FD)
Media Attachment Unit type: 16
Vlan ID: - not advertised

MED Information:
      MED Codes:
            (NP) Network Policy, (LI) Location Identification
            (PS) Power Source Entity, (PD) Power Device
            (IN) Inventory

H/W revision: 6
F/W revision: tnp42.8-3-1-21a.bin
S/W revision: SCCP42.9-3-1-1S
Serial number: FCH1414A0BA
Manufacturer: Cisco Systems, Inc.
Model: CP-7942G
Capabilities: NP, PD, IN
Device type: Endpoint Class III
Network Policy(Voice): VLAN 837, tagged, Layer-2 priority: 5, DSCP: 46
Network Policy(Voice Signal): VLAN 837, tagged, Layer-2 priority: 4, DSCP:
32
PD device, Power source: Unknown, Power Priority: Unknown, Wattage: 6.3
Location - not advertised
Total entries displayed: 1
```

NOTA:
Los *switches* que utilizan LLDP pueden recoger información detallada de los dispositivos a medida que se unen o dejan la red o cambian de ubicación, exportando la información a través de Cisco MSE (*Management Services Engine*).