

Diseño de redes Corporativas

Jhon Jairo Padilla Aguilar, PhD.

Objetivo

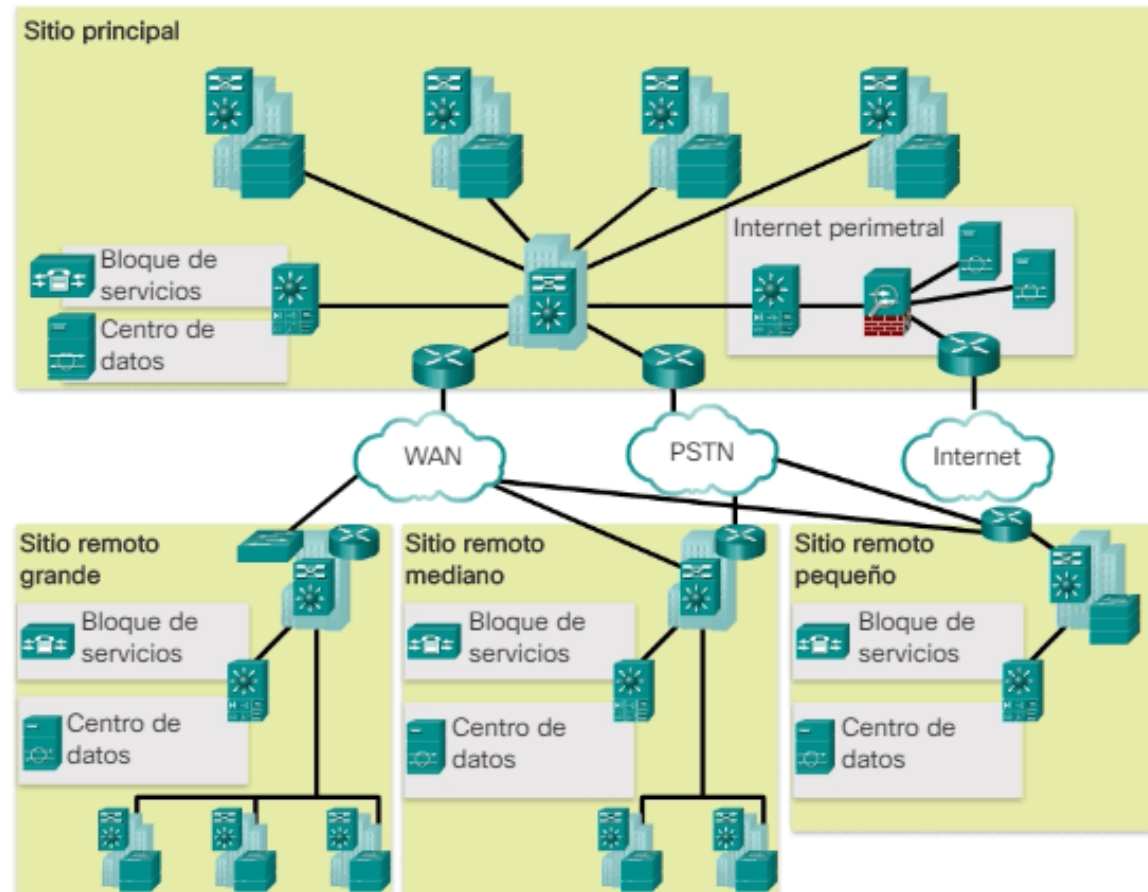
- A continuación se presentan los conceptos, los principios, los modelos y las arquitecturas del diseño de red.
- Se abarcan los beneficios que se obtienen mediante un enfoque de diseño sistemático.
- También se analizan las tendencias tecnológicas emergentes que afectan la evolución de las redes.
- Estos principios forman parte de las recomendaciones del curso CCNA 4 de Cisco.

Diseño Jerárquico de la red

- Cuando se analiza el diseño de red, es útil categorizar las redes según la cantidad de dispositivos que se atienden:
 - **Red pequeña:** proporciona servicios para hasta 200 dispositivos.
 - **Red mediana:** proporciona servicios para 200 a 1000 dispositivos.
 - **Red grande:** proporciona servicios para más de 1000 dispositivos.
- Los diseños de red varían según el tamaño y las necesidades de las organizaciones.
- Para cumplir con estos objetivos fundamentales del diseño, la red se debe armar sobre la base de una **arquitectura de red jerárquica** que permita la flexibilidad y el crecimiento.

Requisitos de la red

- Existen muchas variables para tener en cuenta al diseñar una red.
- Ejemplo de una red empresarial grande:



Principios de Ingeniería Estructurada

- Independientemente del tamaño o los requisitos de la red, un factor fundamental para la correcta implementación de cualquier diseño de red es seguir buenos principios de ingeniería estructurada:
 - **Jerarquía:** un modelo de red jerárquico es una herramienta útil de alto nivel para diseñar una infraestructura de red confiable. *Divide el problema complejo del diseño de red en áreas más pequeñas y más fáciles de administrar.*
 - **Modularidad:** al separar en módulos las diversas funciones que existen en una red, esta es más fácil diseñar.
 - Cisco identificó varios módulos: el campus empresarial, el bloque de servicios, el centro de datos e Internet perimetral.

Principios de Ingeniería Estructurada

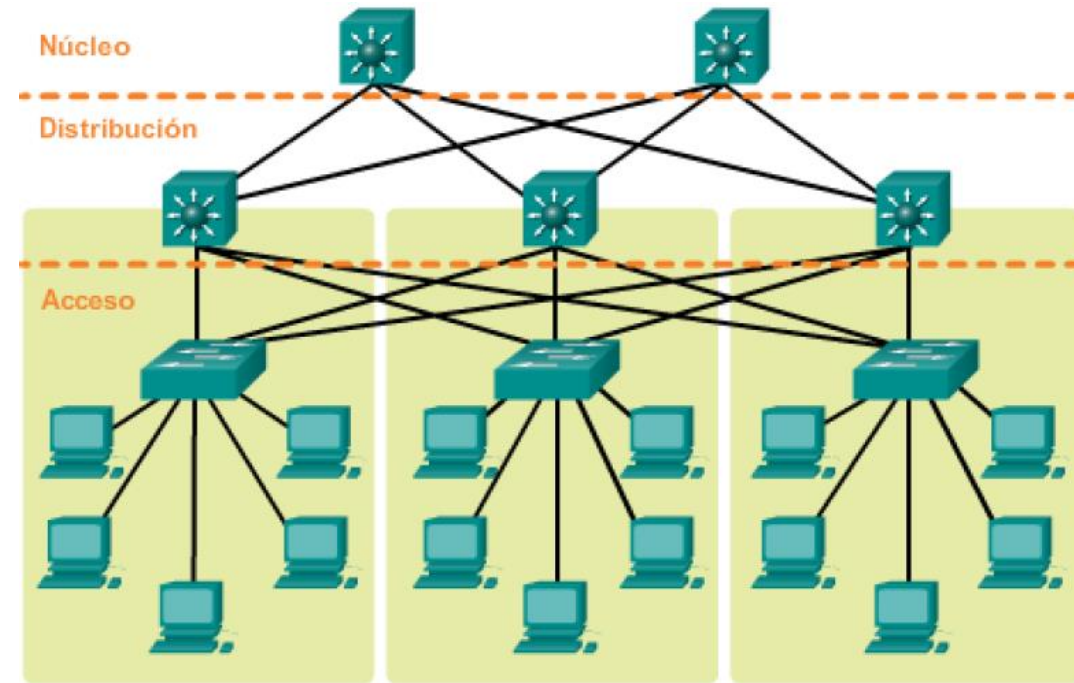
- **Resistencia:** la red debe estar disponible para que se pueda utilizar tanto en condiciones normales (períodos de mantenimiento) como anormales (fallas de hardware o de software).
- **Flexibilidad:** la capacidad de modificar partes de la red, agregar nuevos servicios o aumentar la capacidad sin necesidad de realizar actualizaciones de gran importancia (es decir, reemplazar los principales dispositivos de hardware).

Jerarquía de red

- En la tecnología de redes, un diseño jerárquico implica **dividir la red en capas independientes**. Cada capa (o nivel) en la jerarquía proporciona funciones específicas que definen su función dentro de la red general.
- Esto ayuda al diseñador y al arquitecto de red a optimizar y seleccionar las características, el hardware y el software de red adecuados para llevar a cabo las funciones específicas de esa capa de red. Los modelos jerárquicos se aplican al diseño de LAN y WAN.

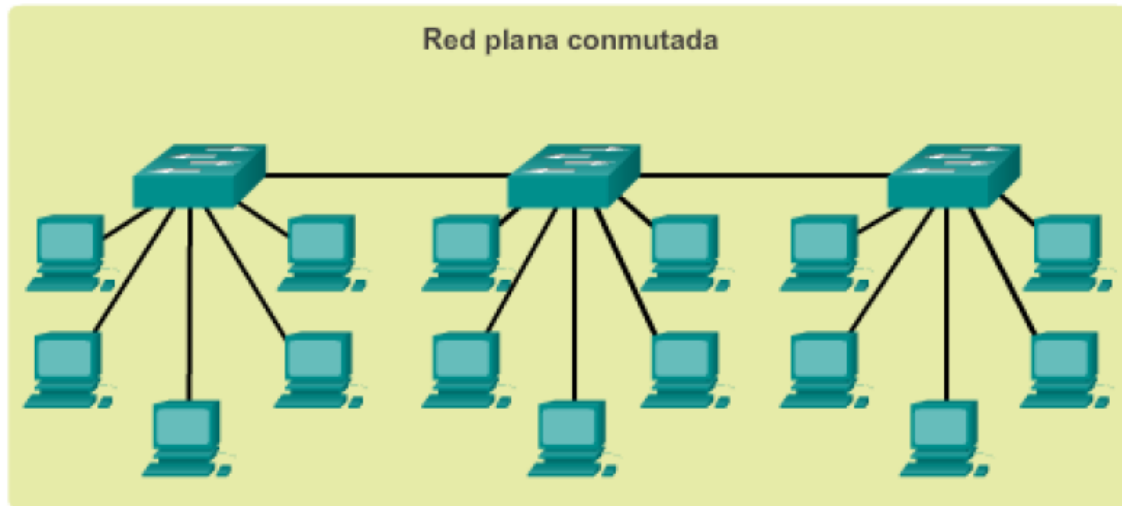
Jerarquía de Red

- Un diseño típico de red LAN jerárquica de campus empresarial incluye las siguientes tres capas:
 - **Capa de acceso:** proporciona acceso a la red para los grupos de trabajo y los usuarios.
 - **Capa de distribución:** proporciona una conectividad basada en políticas y controla el límite entre las capas de acceso y de núcleo.
 - **Capa de núcleo:** proporciona un transporte rápido entre los switches de distribución dentro del campus empresarial.

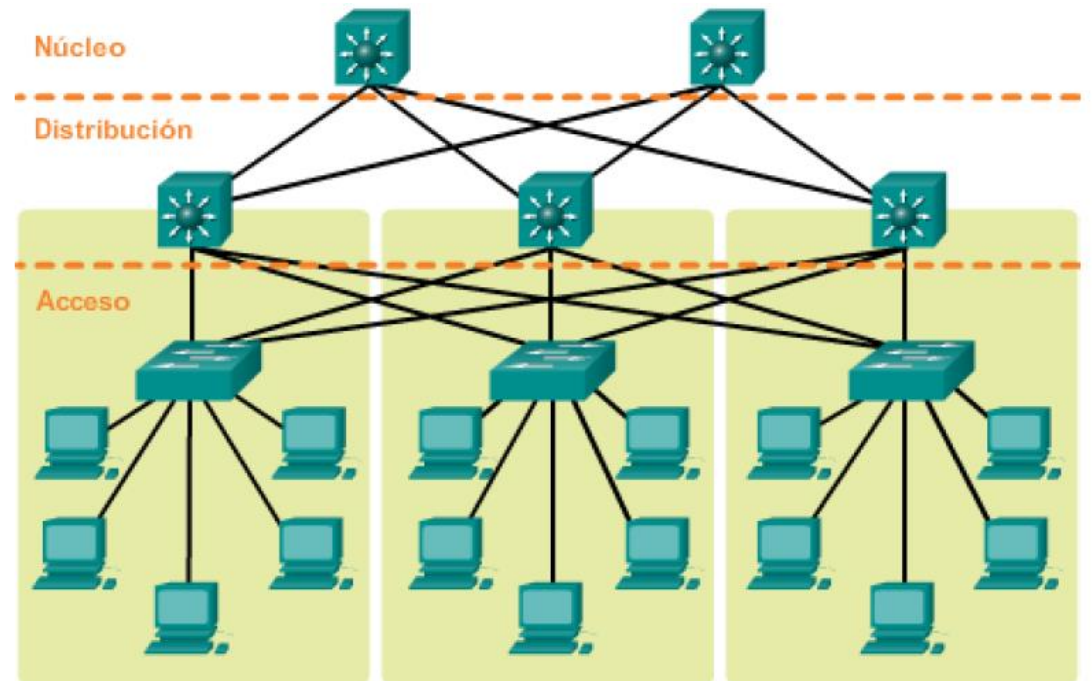


Red Jerárquica vs. Red Plana

Red Plana Conmutada



Red Jerárquica Conmutada

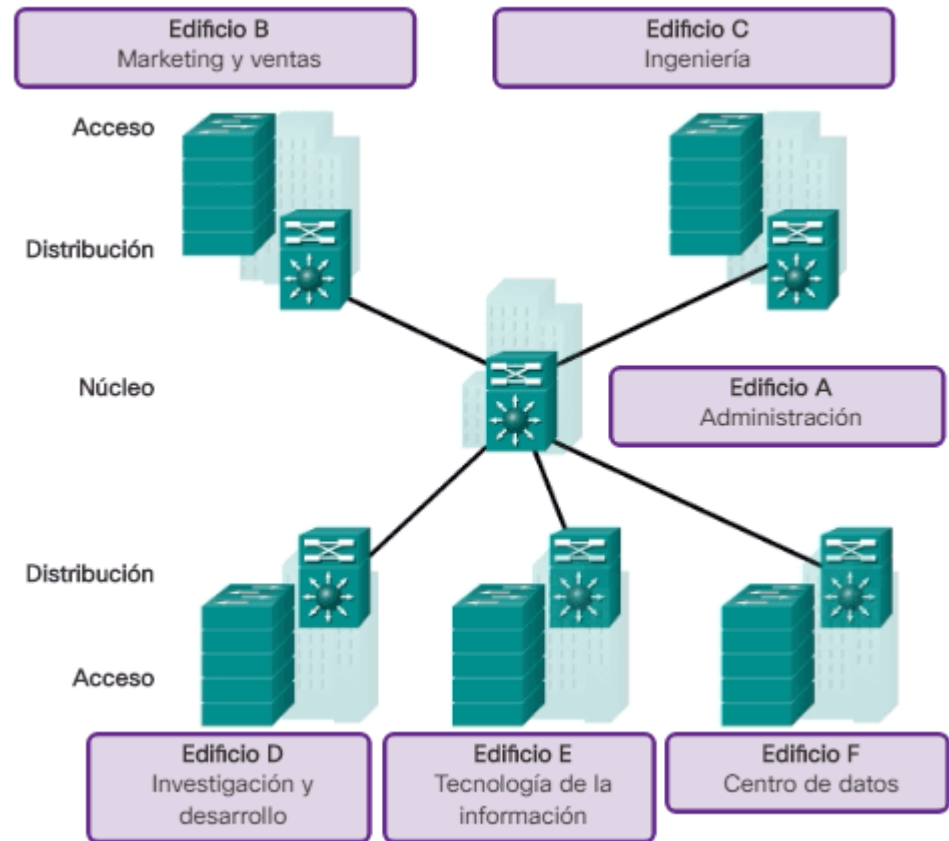


Beneficios de una red Jerárquica

- El beneficio de dividir una red plana en bloques más pequeños y fáciles de administrar es que el tráfico local sigue siendo local, mientras que sólo el tráfico destinado a otras redes se traslada a una capa superior.
- Los dispositivos de Capa 2 en una red plana brindan pocas oportunidades de controlar broadcasts o filtrar tráfico no deseado. A medida que se agregan más dispositivos y aplicaciones a una red plana, los tiempos de respuesta se degradan hasta que la red queda inutilizable.

Ejemplo 2: Red Jerárquica más compleja

- Cada edificio utiliza el mismo modelo de red jerárquico que incluye las capas de acceso, de distribución y de núcleo.

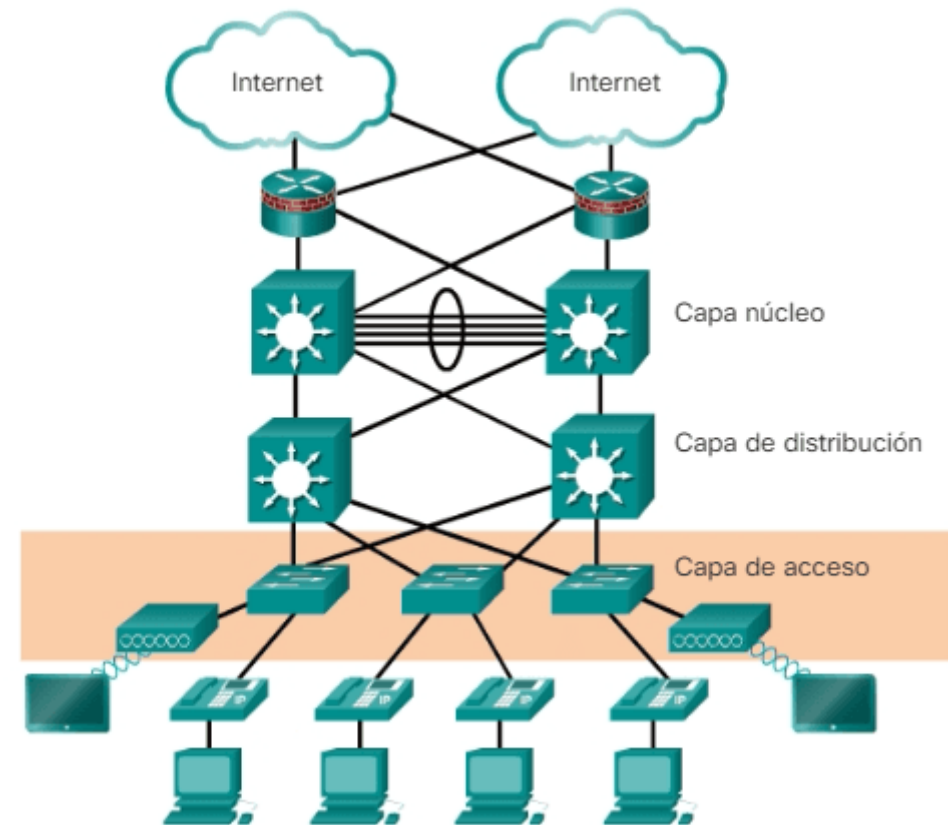


Capa de Acceso

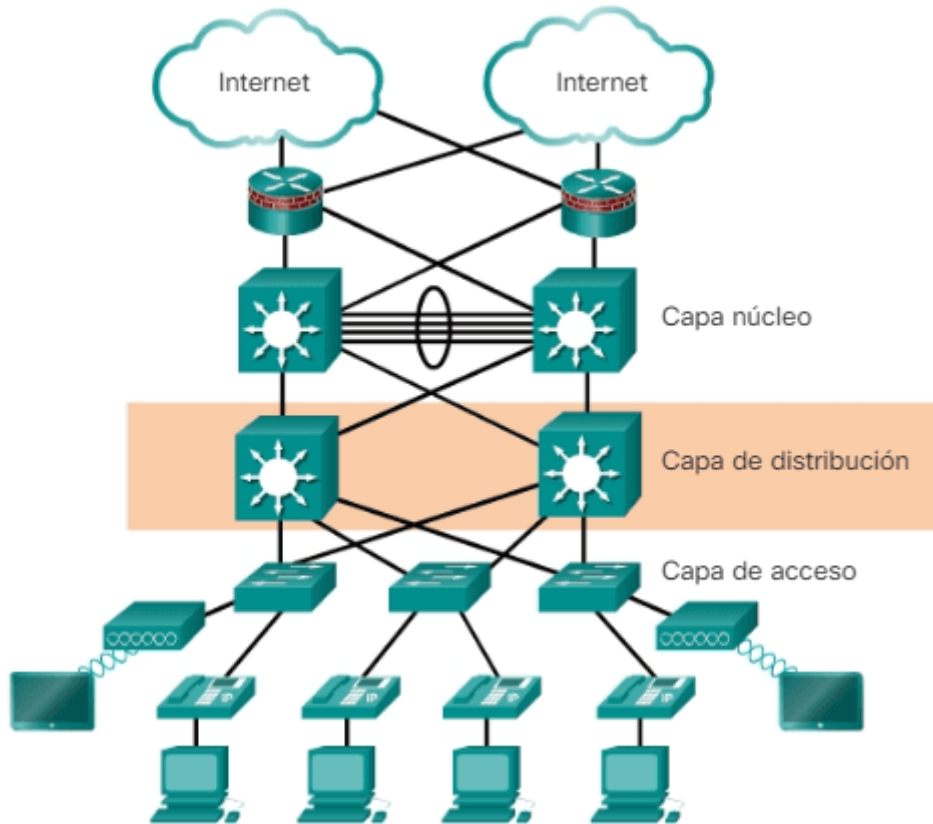
- En un entorno LAN, la capa de acceso otorga acceso a la red para las terminales.
- En el entorno WAN, puede proporcionar acceso a la red empresarial para los trabajadores a distancia o los sitios remotos a través de conexiones WAN.
- La capa de acceso para la red de una pequeña empresa, por lo general, incorpora switches de capa 2 y puntos de acceso que proporcionan conectividad entre las estaciones de trabajo y los servidores.

Funciones de la Capa de Acceso

- Switching de capa 2
- Alta disponibilidad
- Seguridad del puerto
- Clasificación y marcación de QoS, y límites de confianza
- Inspección del protocolo de resolución de direcciones (ARP)
- Listas de control de acceso virtual (VACL)
- Árbol de expansión
- Alimentación por Ethernet y VLAN auxiliares para VoIP



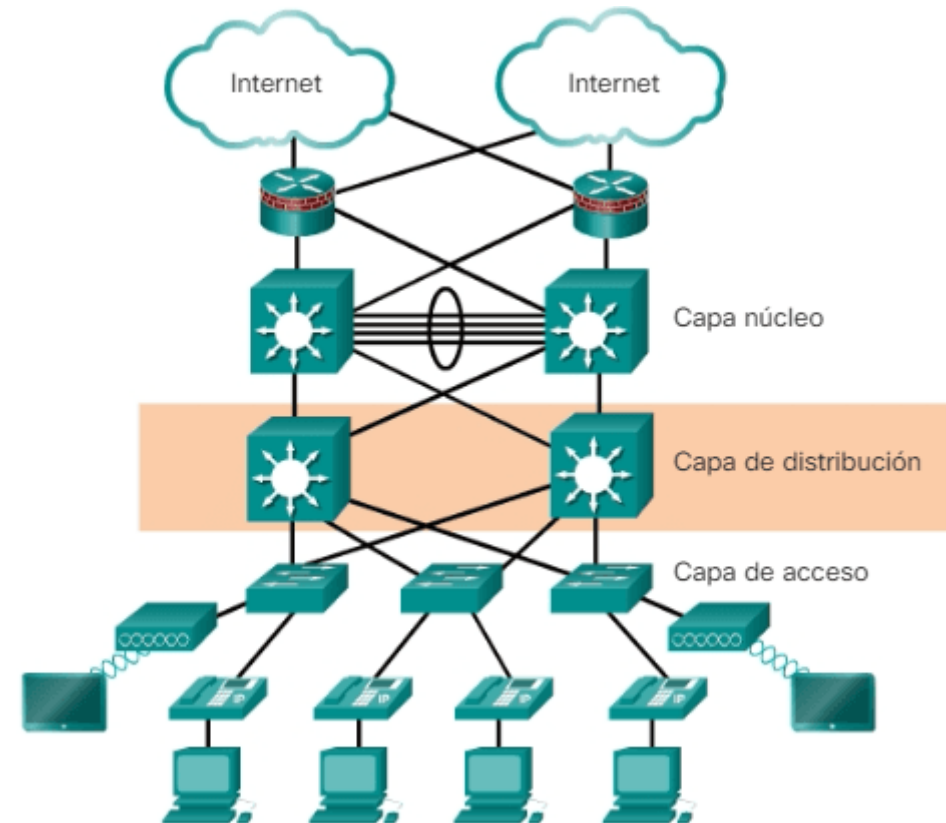
Capa de Distribución



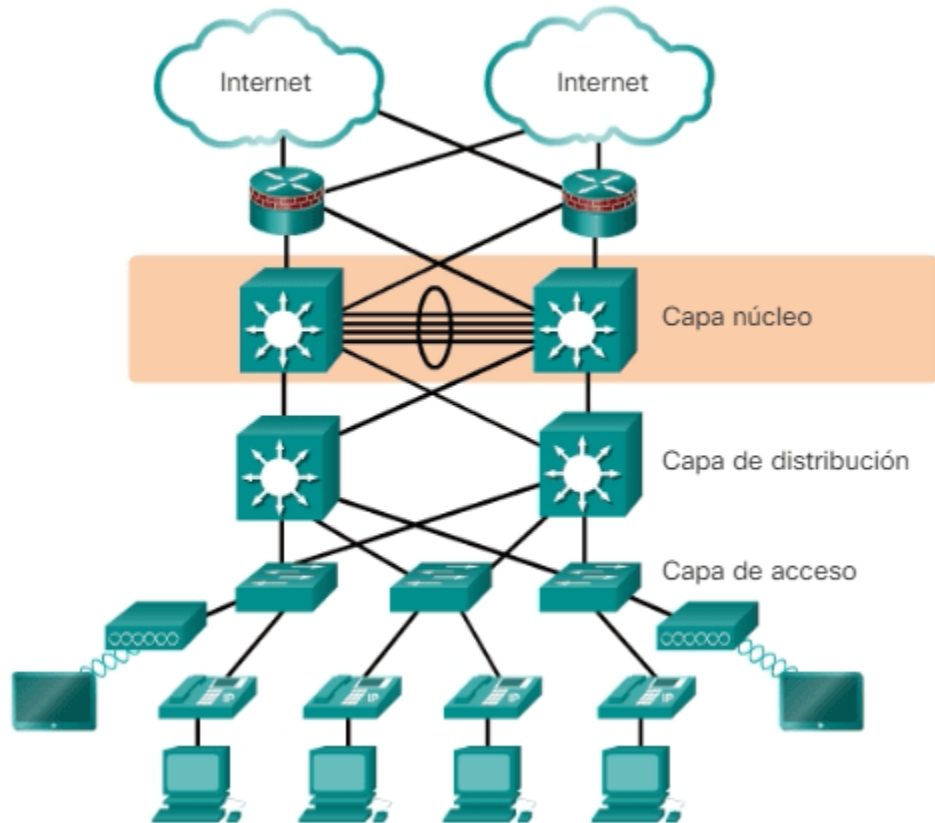
- La capa de distribución agrega el tráfico de los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final.
- La ubicación de la capa de distribución es el centro en los armarios de cableado.
- Para segmentar los grupos de trabajo y aislar los problemas de la red en un entorno de campus, se utiliza un router o un *switch multicapa*.

Funciones de la capa de Distribución

- Agregación de enlaces LAN o WAN.
- Seguridad basada en políticas en forma de listas de control de acceso (ACL) y filtrado.
- Servicios de routing entre redes LAN y VLAN, y entre dominios de routing (p. ej., EIGRP a OSPF).
- Redundancia y balanceo de carga.
- Un límite para la agregación de rutas que se configura en las interfaces hacia la capa de núcleo.
- Control del dominio de difusión, ya que ni los routers ni los switches multicapa reenvían difusiones. El dispositivo funciona como punto de demarcación entre los dominios de difusión.

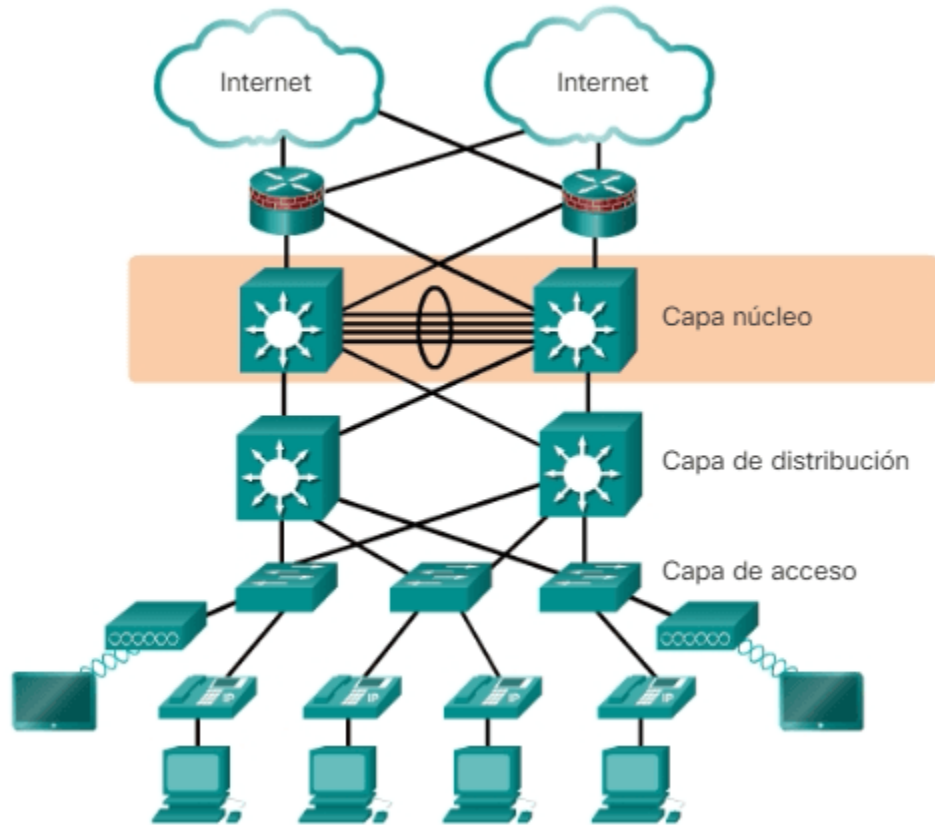


Capa de Núcleo



- La capa de núcleo también se conoce como “backbone de red”. La capa de núcleo consta de dispositivos de red de alta velocidad, como los switches Cisco Catalyst 6500 o 6800. Estos están diseñados para conmutar paquetes lo más rápido posible e interconectar varios componentes de campus, como módulos de distribución, módulos de servicio, el centro de datos y el perímetro de la WAN.

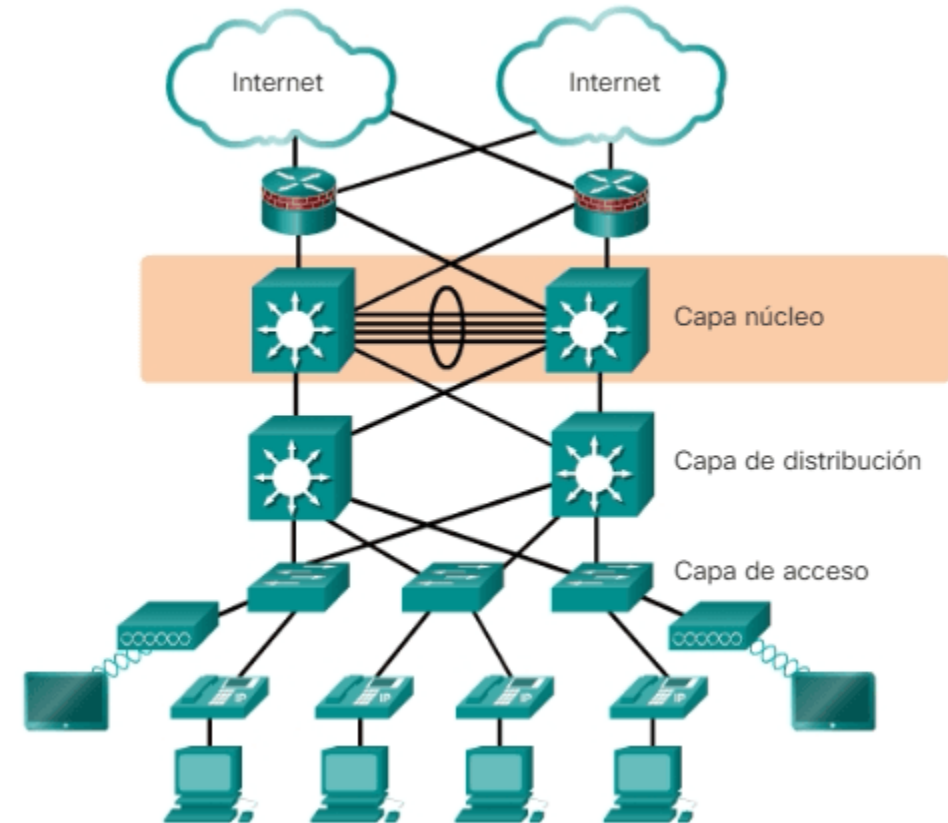
Capa de Núcleo



- Interconecta el bloque de distribución al perímetro de la WAN y de Internet.
- El núcleo debe tener una alta disponibilidad y debe ser redundante.
- El núcleo agrega el tráfico de todos los dispositivos de la capa de distribución, por lo tanto debe poder enviar grandes cantidades de datos rápidamente.

Características de la capa de Núcleo

- Debe proporcionar switching de alta velocidad (es decir, un transporte rápido).
- Debe proporcionar confiabilidad y tolerancia a fallas.
- Debe lograr la escalabilidad mediante equipos más rápidos, no con más equipos.
- Debe evitar la manipulación de paquetes que implica una gran exigencia para la CPU a causa de la seguridad, la inspección, la clasificación de la calidad de servicio (QoS) u otros procesos.

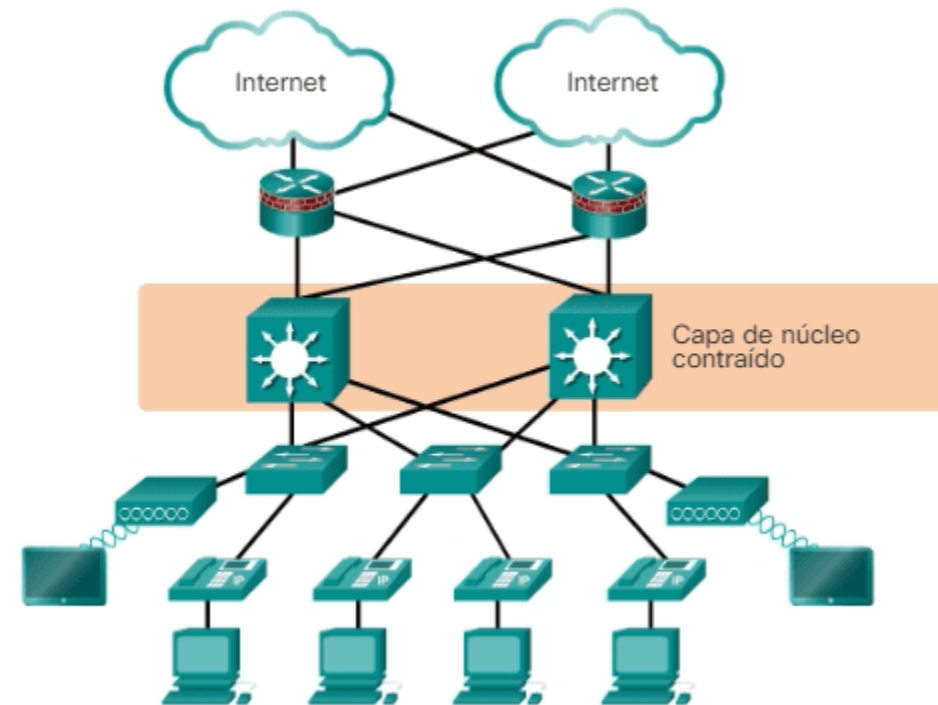


Diseño de Núcleo contraído de 2 niveles

- No existen reglas absolutas sobre la forma en que se debe armar físicamente una red de campus. Si bien es cierto que muchas redes de campus se construyen con tres niveles físicos de switches, no es un requisito estricto.
- En un campus más pequeño, la red puede tener dos niveles de switches en los que los elementos de núcleo y de distribución se combinan en un switch físico. Esto se denomina “diseño de núcleo contraído”.

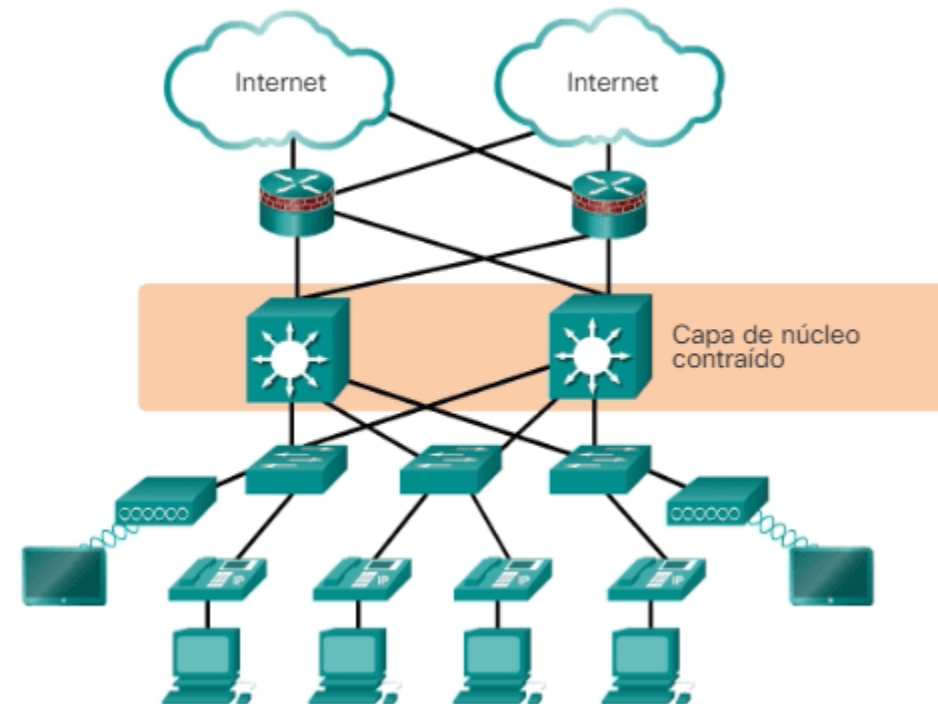
Diseño de Núcleo contraído de 2 niveles

- Hay muchas redes de pequeñas empresas que no crecen mucho con el tiempo.
- Por lo tanto, un diseño jerárquico de dos niveles en el que las capas de núcleo y de distribución se combinan en una sola capa suele ser más práctico.
- Existe un “núcleo contraído” cuando las funciones de la capa de distribución y de la capa de núcleo se implementan mediante un único dispositivo.
- La principal motivación para elegir el diseño de núcleo contraído es la **reducción de costos de la red**, a la vez que se mantiene la mayoría de los beneficios del modelo jerárquico de tres niveles.



Diseño de Núcleo contraído de 2 niveles

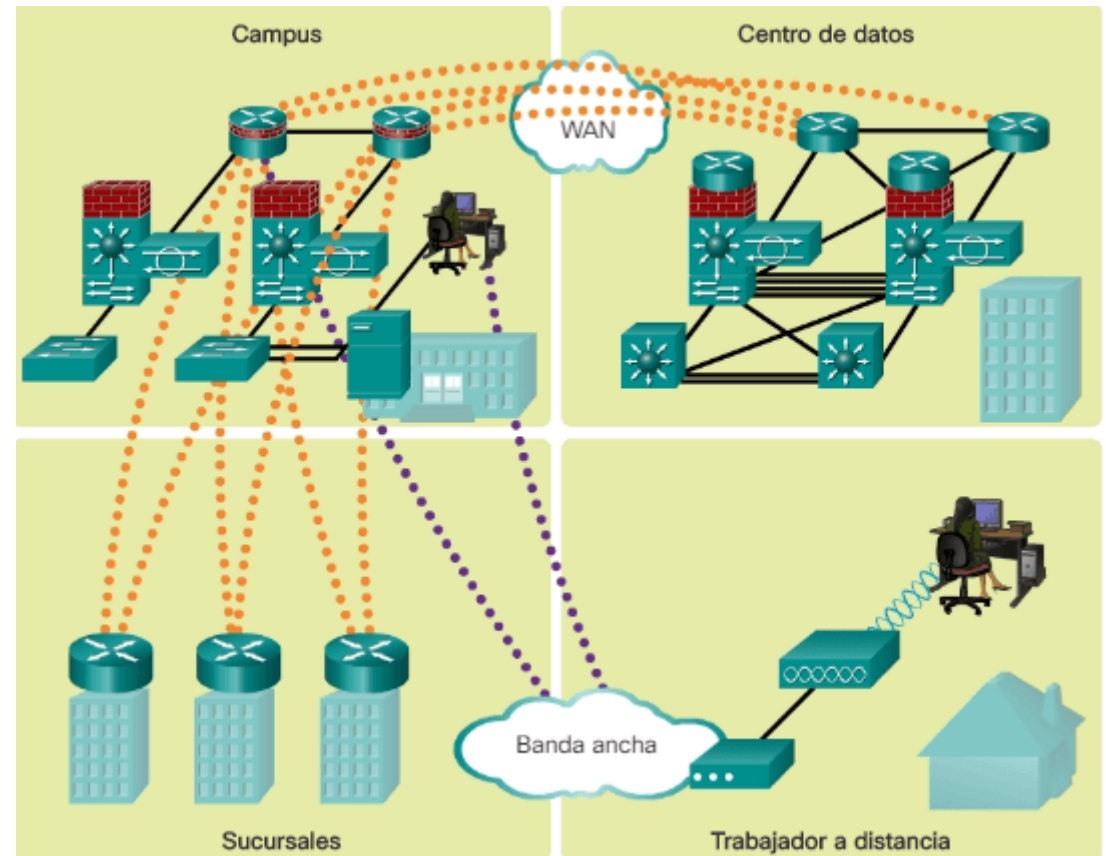
- En esta red se contrajo la funcionalidad de la capa de distribución y la capa de núcleo en dispositivos de switch multicapa.



Arquitectura Empresarial de Cisco

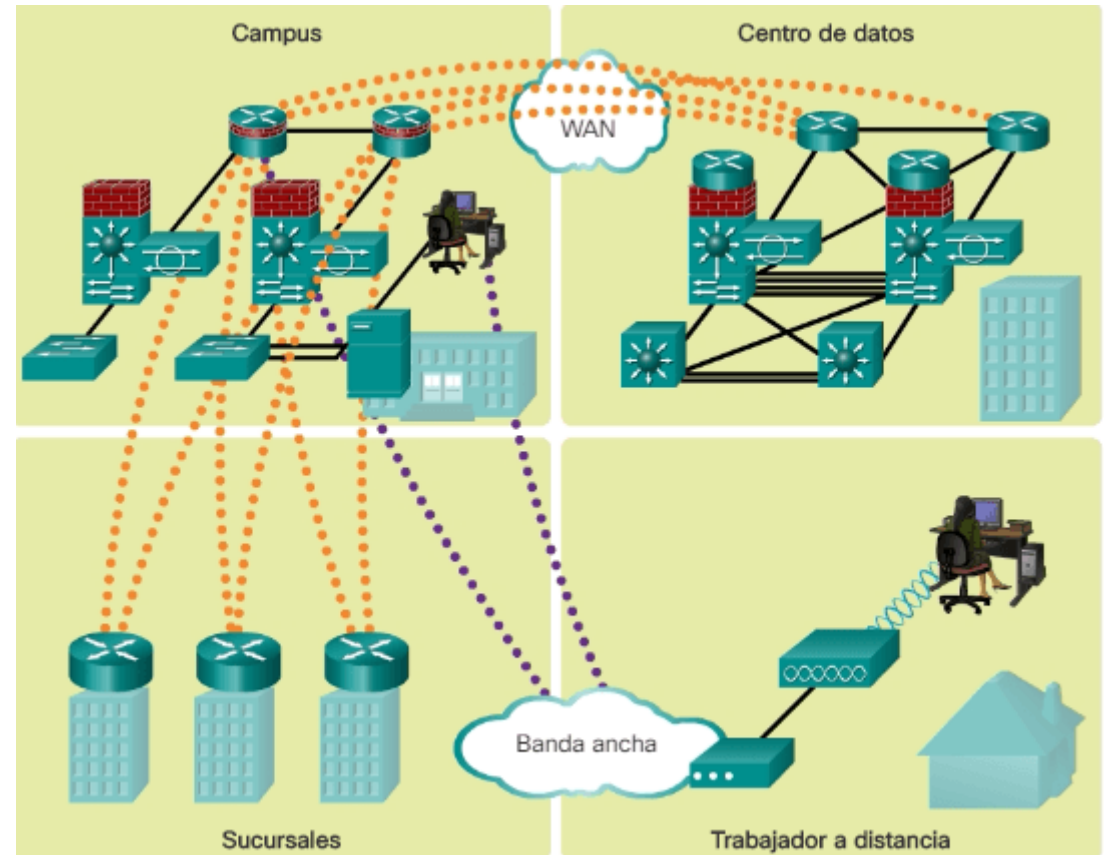
Diseño de red Modular

- Si bien el diseño de red jerárquico funciona bien dentro de la infraestructura del campus, las redes se expandieron más allá de estas fronteras. Como se muestra en la Imagen, las redes se volvieron más sofisticadas y complejas, y algunas requieren conexiones a centros de datos dedicados, que por lo general son externos.



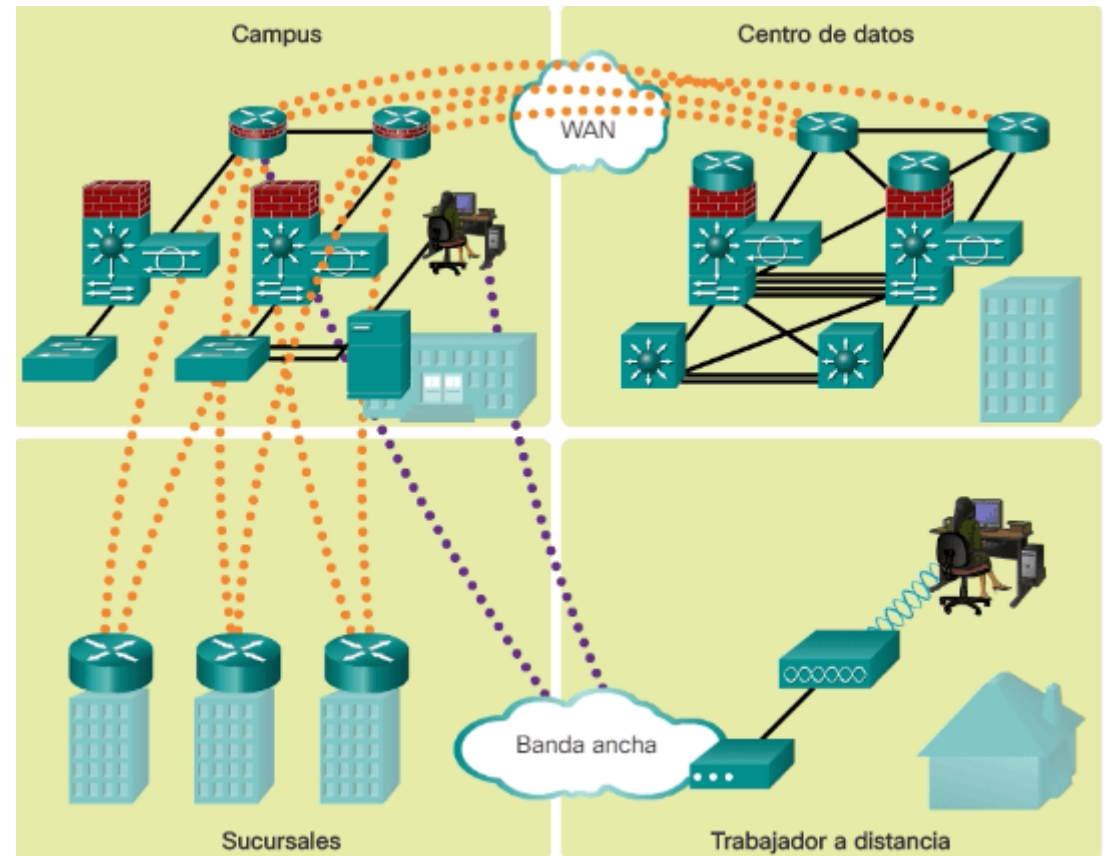
Diseño de red Modular

- Un diseño de red modular separa la red en varios módulos de red funcionales, y cada uno de estos apunta a un lugar o un propósito específico en la red.
- Los módulos representan áreas que tienen una conectividad física o lógica diferente. Se encargan de designar dónde se llevan a cabo las diferentes funciones en la red.



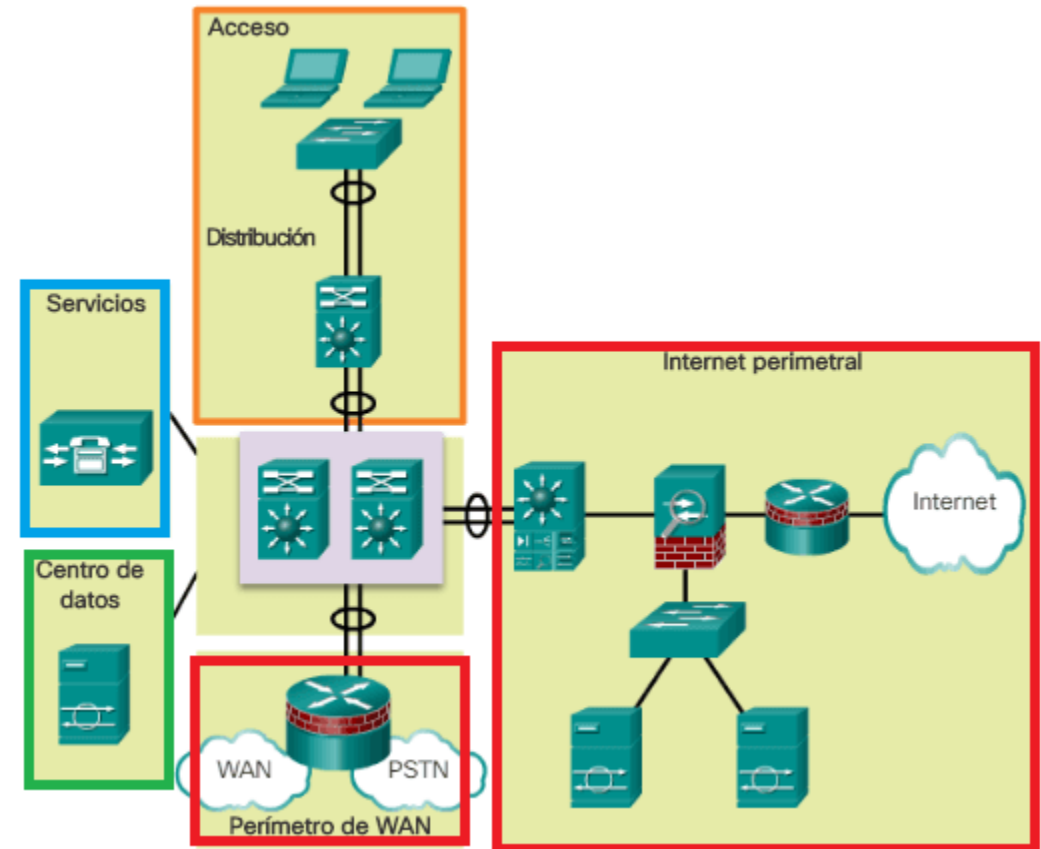
Beneficios del diseño Modular

- Las fallas que ocurren dentro de un módulo se pueden aislar del resto de la red, lo que permite una detección de problemas más sencilla.
- Los cambios, las actualizaciones o la introducción de nuevos servicios de redes se pueden realizar de forma controlada y gradual, lo que permite una mayor flexibilidad en el mantenimiento y el funcionamiento de la red del campus.
- Cuando un módulo específico ya no posee la capacidad suficiente o no tiene una función o un servicio nuevos, se puede actualizar o reemplazar con otro módulo que tenga la misma función estructural en el diseño jerárquico general.
- Se puede implementar seguridad de forma modular.



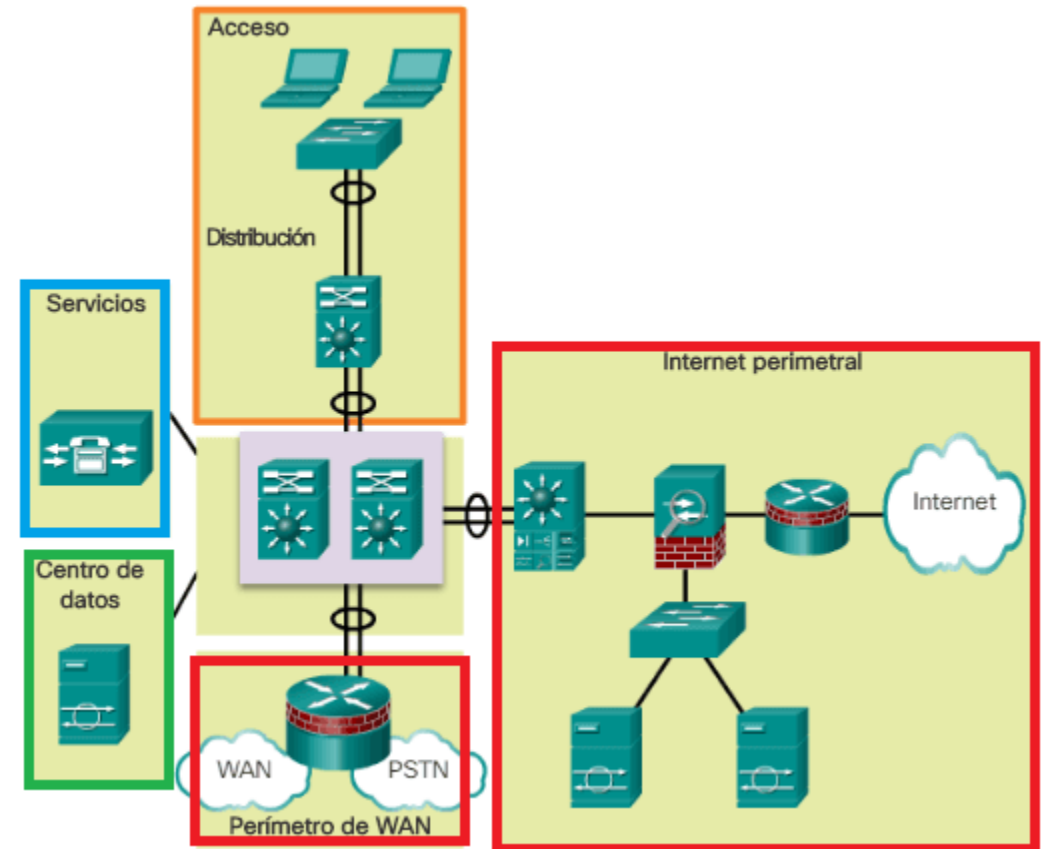
Diseño Modular

- El enfoque modular aplicado al diseño de red divide aún más el diseño jerárquico de tres capas, ya que elimina bloques específicos o áreas modulares.
- Estos módulos básicos están conectados entre sí a través del núcleo de la red.

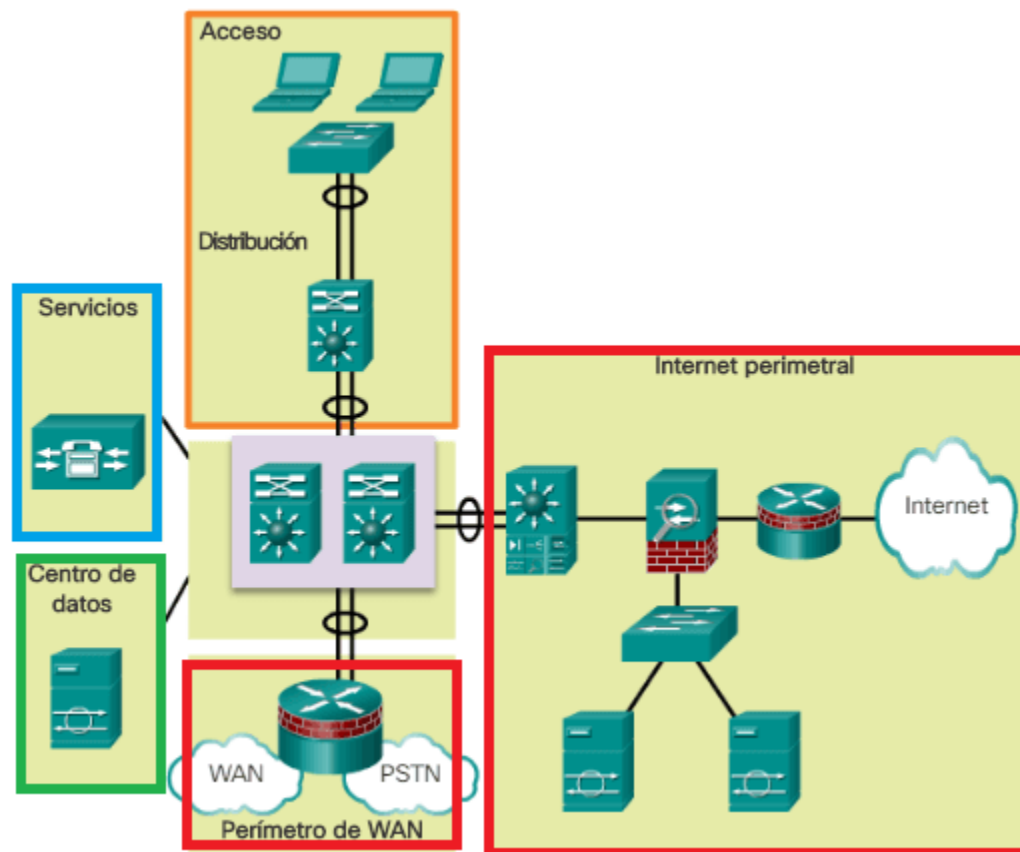


Módulos y su función

- **Acceso y distribución:** también denominado “bloque de distribución”, (recuadro naranja). A este módulo se conectan los usuarios de la red.
- **Servicios:** este es un bloque genérico que se utiliza para identificar servicios como los controladores inalámbricos centralizados del protocolo de punto de acceso ligero (LWAPP), los servicios de comunicaciones unificadas, los gateways de políticas, entre otros (recuadro celeste).
- **Centro de datos:** este es un bloque genérico que se utiliza para identificar servicios como los controladores inalámbricos centralizados del protocolo de punto de acceso ligero (LWAPP), los servicios de comunicaciones unificadas, los gateways de políticas, entre otros (recuadro verde).



Módulos y su función



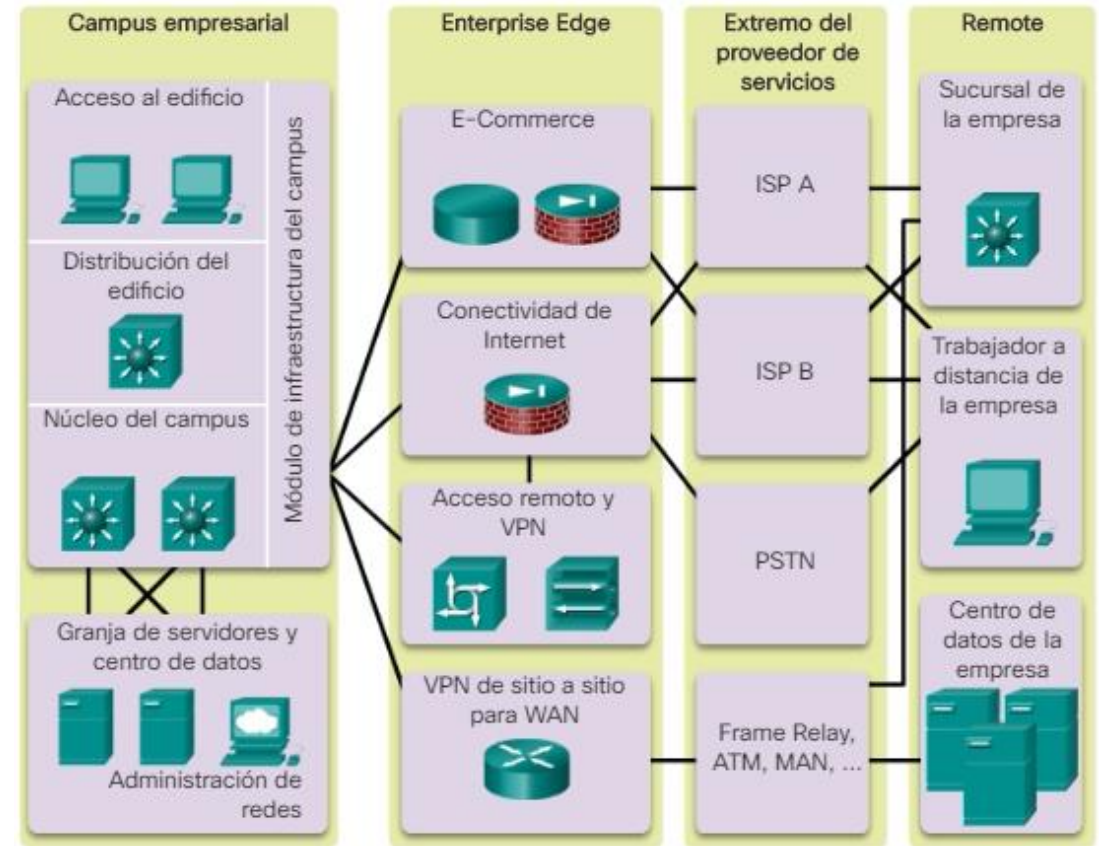
- **Centro de datos:** originalmente, se denominaba “granja de servidores”. Este bloque es responsable de administrar y mantener muchos sistemas de datos que son fundamentales para las operaciones comerciales modernas. Los empleados, los socios y los clientes confían en los datos y los recursos del centro de datos para crear, colaborar e interactuar de manera eficaz (recuadro verde).
- **Perímetro empresarial:** consta de Internet perimetral y del perímetro de WAN. Estos bloques ofrecen conectividad a servicios de voz, de video y de datos fuera de la empresa (recuadro rojo).

Modelo de arquitectura empresarial de CISCO

- Para satisfacer la necesidad de modularidad en el diseño de red, Cisco desarrolló el modelo de arquitectura empresarial de Cisco. Este modelo proporciona todos los beneficios del diseño de red jerárquico en la infraestructura del campus y facilita el diseño de redes más grandes y escalables.
- El modelo de arquitectura empresarial de Cisco separa la red empresarial en áreas funcionales que se conocen como “módulos”. La modularidad que se incorpora a la arquitectura permite que haya flexibilidad en el diseño de red y facilita su implementación y la resolución de problemas.

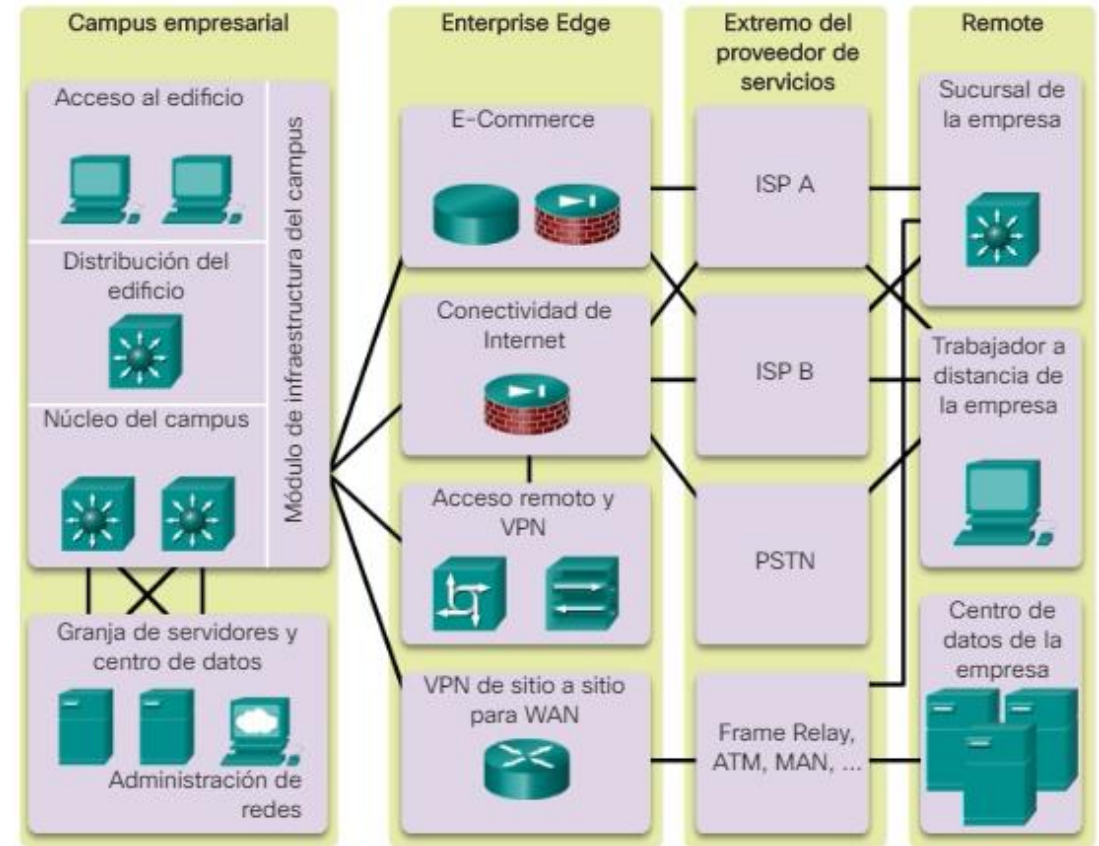
Módulos de la arquitectura empresarial de Cisco

- Los siguientes son los módulos principales de la arquitectura empresarial de Cisco:
 - Campus empresarial
 - Enterprise Edge
 - Extremo del proveedor de servicios
- Existen módulos adicionales conectados al perímetro del proveedor de servicios:
 - Centro de datos de la empresa
 - Sucursal de la empresa
 - Trabajador a distancia de la empresa



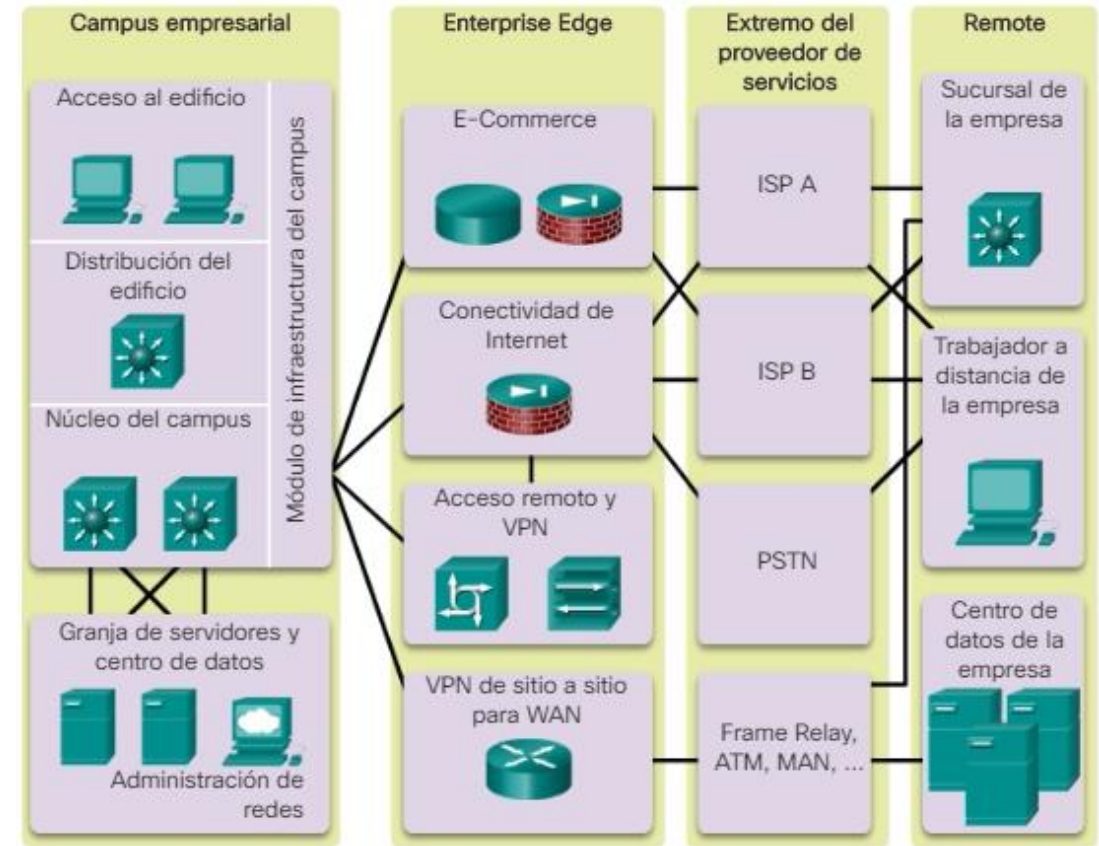
Campus empresarial

- Una red de campus es un edificio o un grupo de edificios conectados a una red empresarial que consta de muchas LAN.
- Por lo general, un campus se limita a un área geográfica fija, pero puede abarcar varios edificios vecinos, por ejemplo, un complejo industrial o el entorno de un parque industrial.
- El módulo de campus empresarial describe los métodos recomendados para crear una red escalable, a la vez que aborda las necesidades de las operaciones comerciales del tipo de campus.
- La arquitectura es modular y se puede expandir fácilmente para incluir edificios o pisos de campus adicionales a medida que la empresa crece.



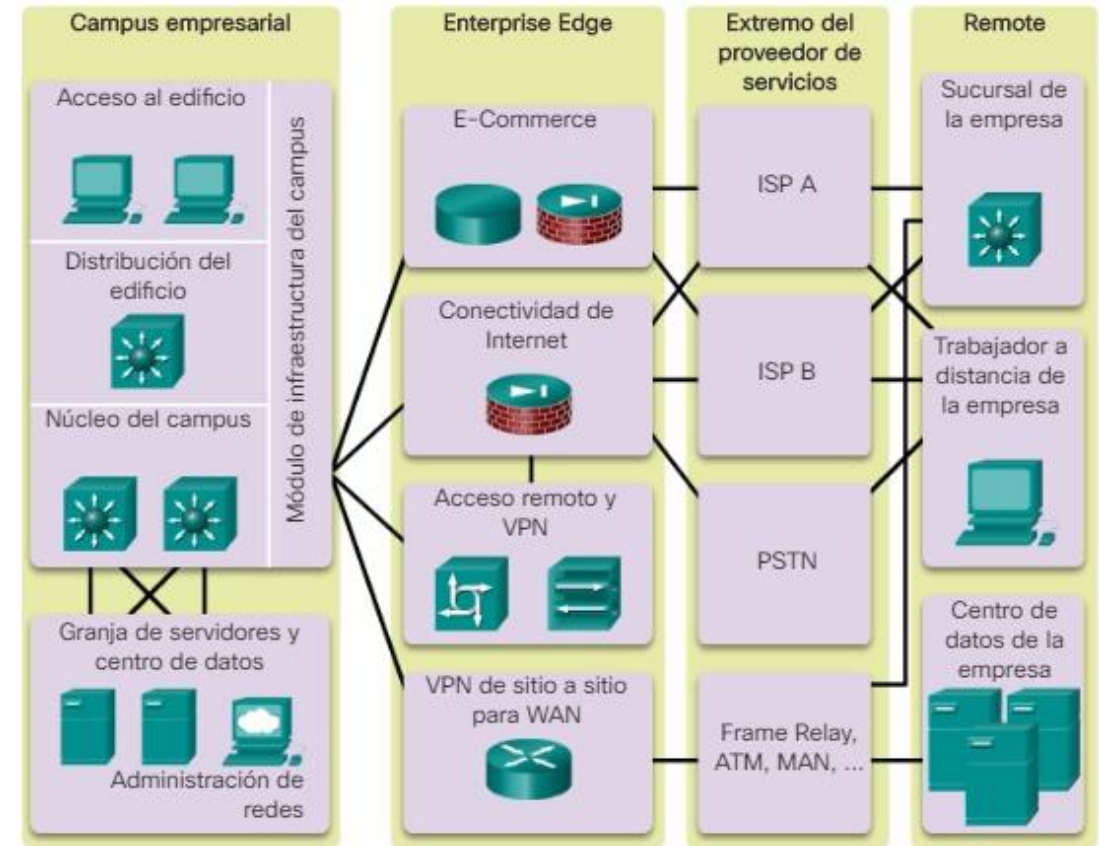
Submódulos del Campus Empresarial

- El módulo de campus empresarial consta de los siguientes submódulos:
 - Acceso al edificio
 - Distribución del edificio
 - Núcleo del campus
 - Centro de datos



Submódulos del campus empresarial

- Juntos, estos submódulos realizan lo siguiente:
 - Proporcionan una alta disponibilidad mediante un diseño de red jerárquico resistente.
 - Integran las comunicaciones IP, la movilidad y la seguridad avanzada.
 - Utilizan el tráfico de multidifusión y QoS para optimizar el tráfico de la red.
 - Proporcionan una mayor seguridad y flexibilidad mediante la administración del acceso, las VLAN y las VPN con IPsec.



Beneficios del campus empresarial

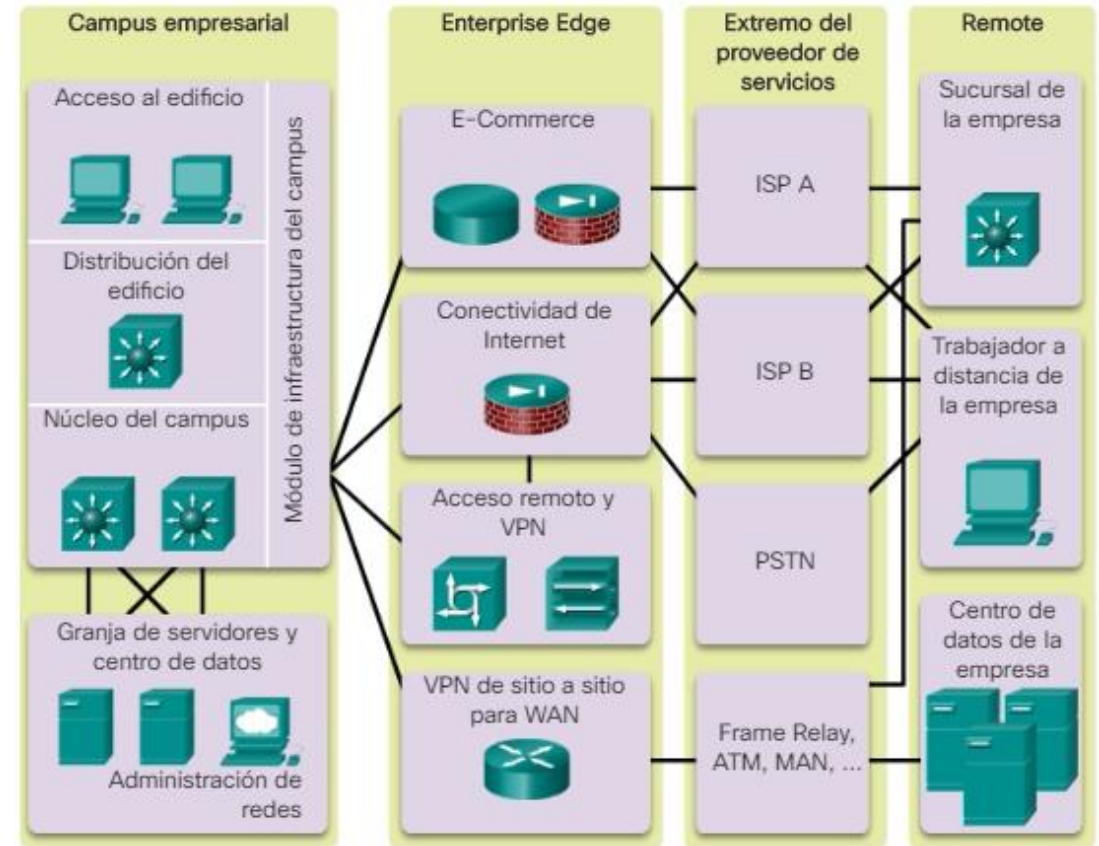
- La arquitectura del módulo de campus empresarial proporciona a la empresa una **alta disponibilidad** a través de un **diseño multicapa resistente**, características de hardware y software redundante, y procedimientos automáticos para volver a configurar las rutas de la red cuando ocurren fallas.
- La **seguridad integrada** protege contra el impacto de gusanos, virus y otros ataques a la red, además de mitigarlo, incluso en el nivel del puerto del switch.
- El submódulo de centro de datos normalmente contiene servidores de correo electrónico y corporativos internos que proporcionan servicios de aplicación, de archivo, de impresión, de correo electrónico y de sistema de nombres de dominios (DNS) a los usuarios internos.

Perímetro Empresarial de Cisco

- El módulo de perímetro empresarial proporciona conectividad para los servicios de voz, video y datos fuera de la empresa.
- A menudo, este módulo funciona como vínculo entre el módulo de campus empresarial y los otros módulos.
- El módulo de perímetro empresarial consta de los siguientes submódulos:
 - Redes y servidores de comercio electrónico
 - Conectividad a Internet y zona perimetral (DMZ)
 - Acceso remoto y VPN
 - WAN

Submódulos del perímetro Empresarial

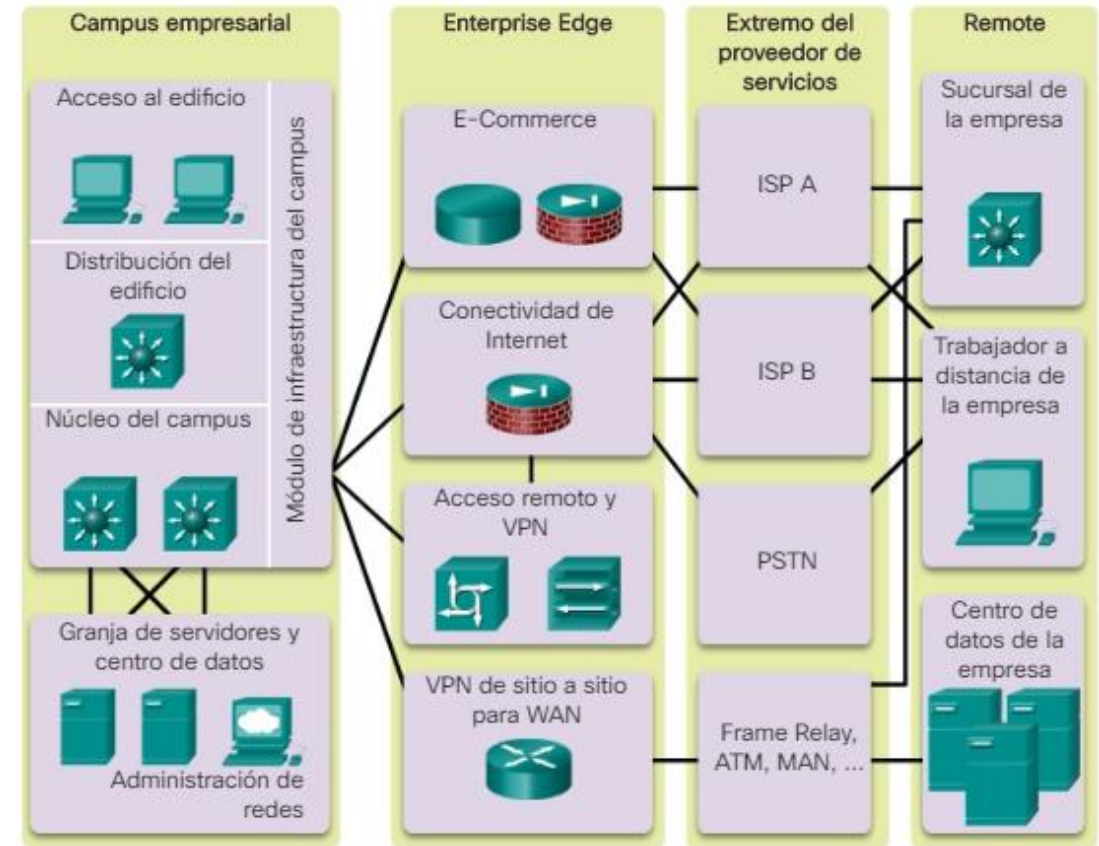
- **Redes y servidores de comercio electrónico:**
 - El submódulo de comercio electrónico permite que las empresas admitan aplicaciones de comercio electrónico a través de Internet.
 - Incluyen los servidores web, de aplicaciones y de bases de datos, el firewall y los routers de firewall, y los sistemas de prevención de intrusiones (IPS) en la red.



Submódulos del perímetro Empresarial

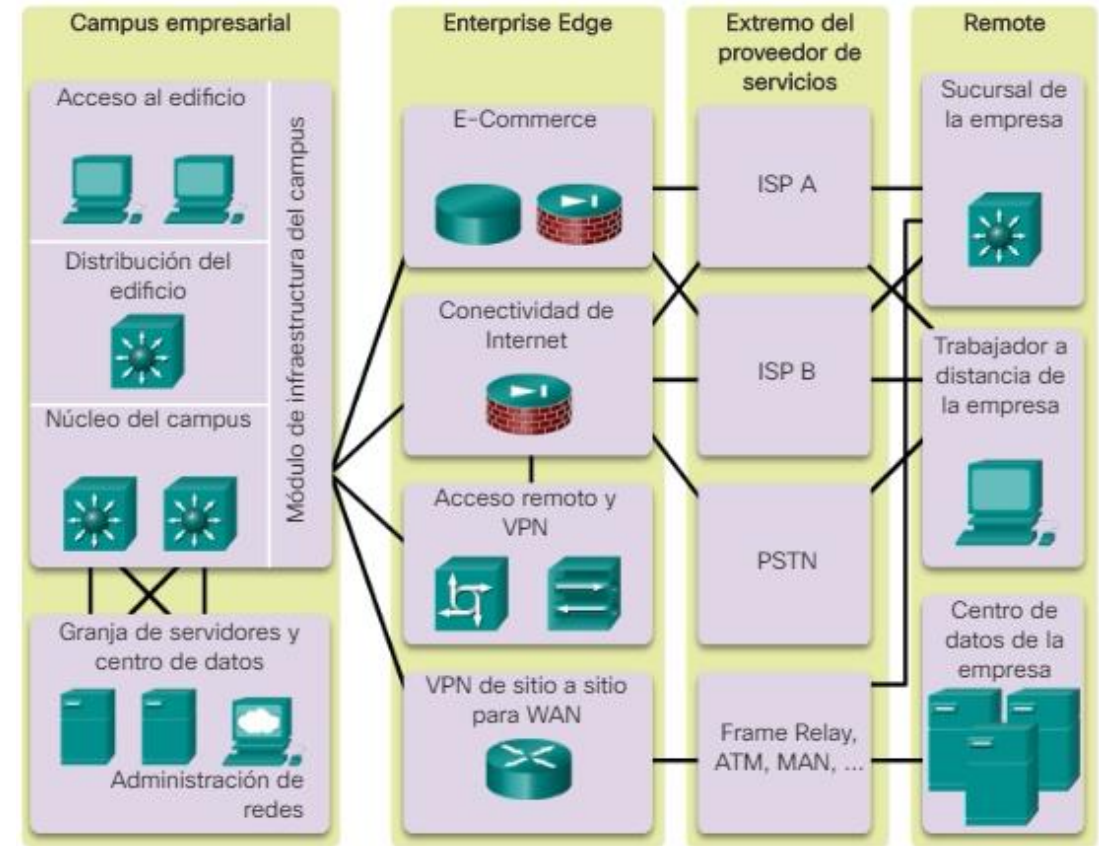
- **Conectividad a Internet y zona perimetral (DMZ):**

- El submódulo de Internet del perímetro empresarial proporciona a los usuarios internos una conectividad segura a los servicios de Internet, como los servidores públicos, el correo electrónico y DNS.
- También se proporciona la conectividad a uno o varios proveedores de servicios de Internet (ISP).
- Incluyen el firewall y los routers de firewall, los routers perimetrales de Internet, los servidores FTP y HTTP, los servidores de retransmisión de SMTP y los servidores DNS.



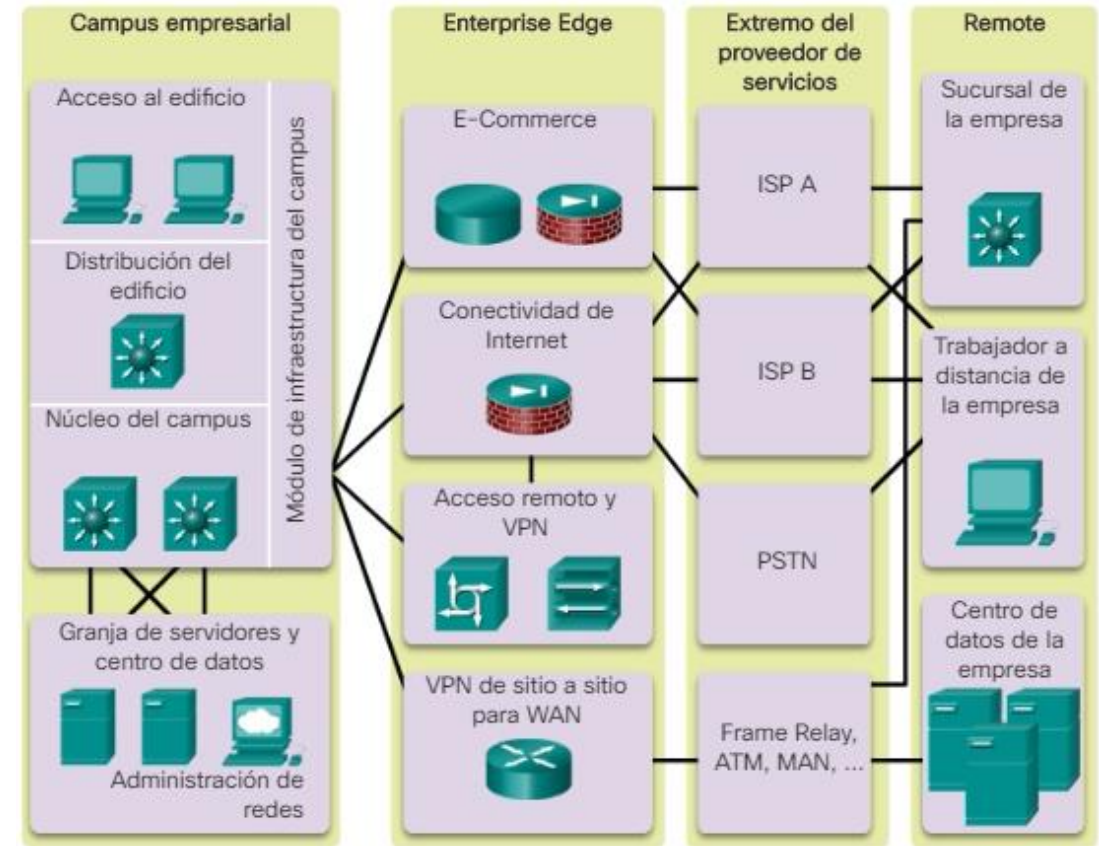
Submódulos del perímetro Empresarial

- **Acceso remoto y VPN:** el submódulo de acceso remoto y VPN del perímetro empresarial proporciona servicios de terminación de acceso remoto, incluida la autenticación para usuarios y sitios remotos.
- Incluyen los firewalls, los concentradores de acceso telefónico, los dispositivos de seguridad adaptables (ASA) de Cisco y las aplicaciones de sistema de prevención de intrusiones (IPS) en la red.



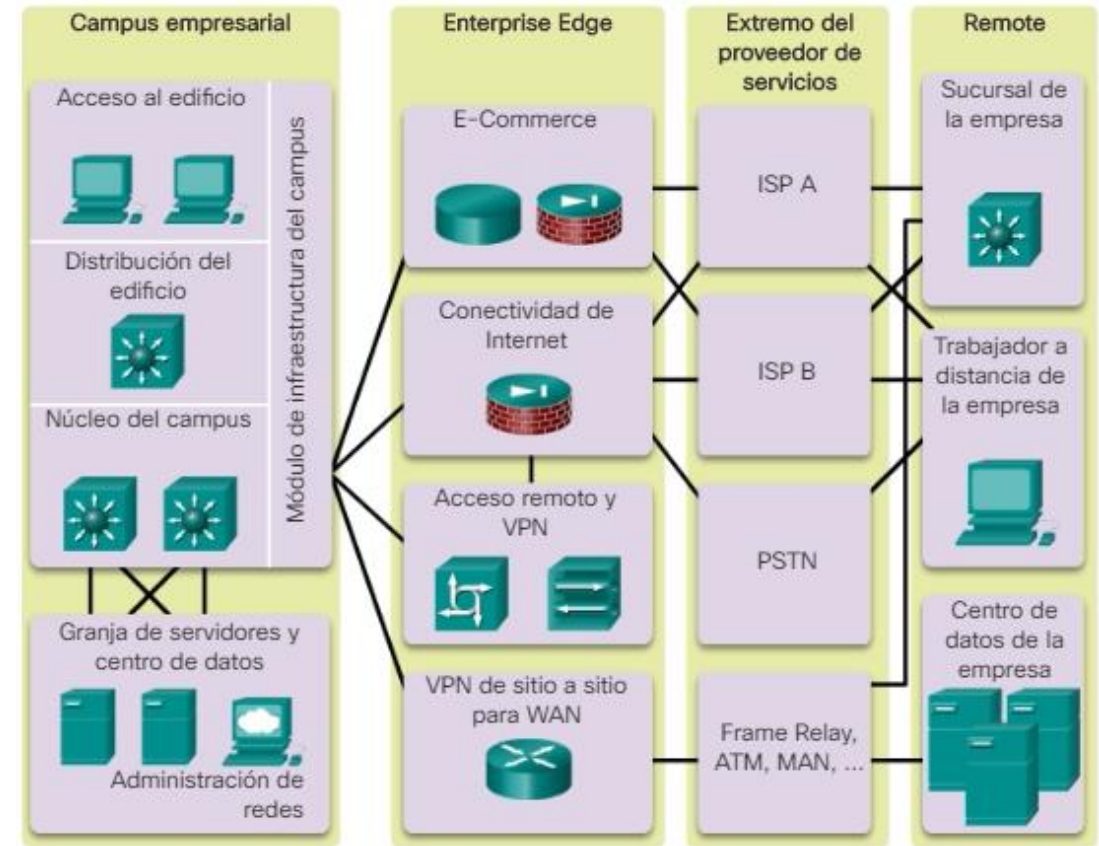
Submódulos del perímetro Empresarial

- **WAN:** el submódulo WAN utiliza diversas tecnologías WAN para enrutar el tráfico entre los sitios remotos y el sitio central.
- Incluyen tecnologías como la conmutación de etiquetas multiprotocolo (MPLS), Ethernet metropolitana, las líneas arrendadas, la red óptica síncrona (SONET) y la jerarquía digital síncrona (SDH), PPP, Frame Relay, ATM, el cable, la línea de suscriptor digital (DSL) y la tecnología inalámbrica.



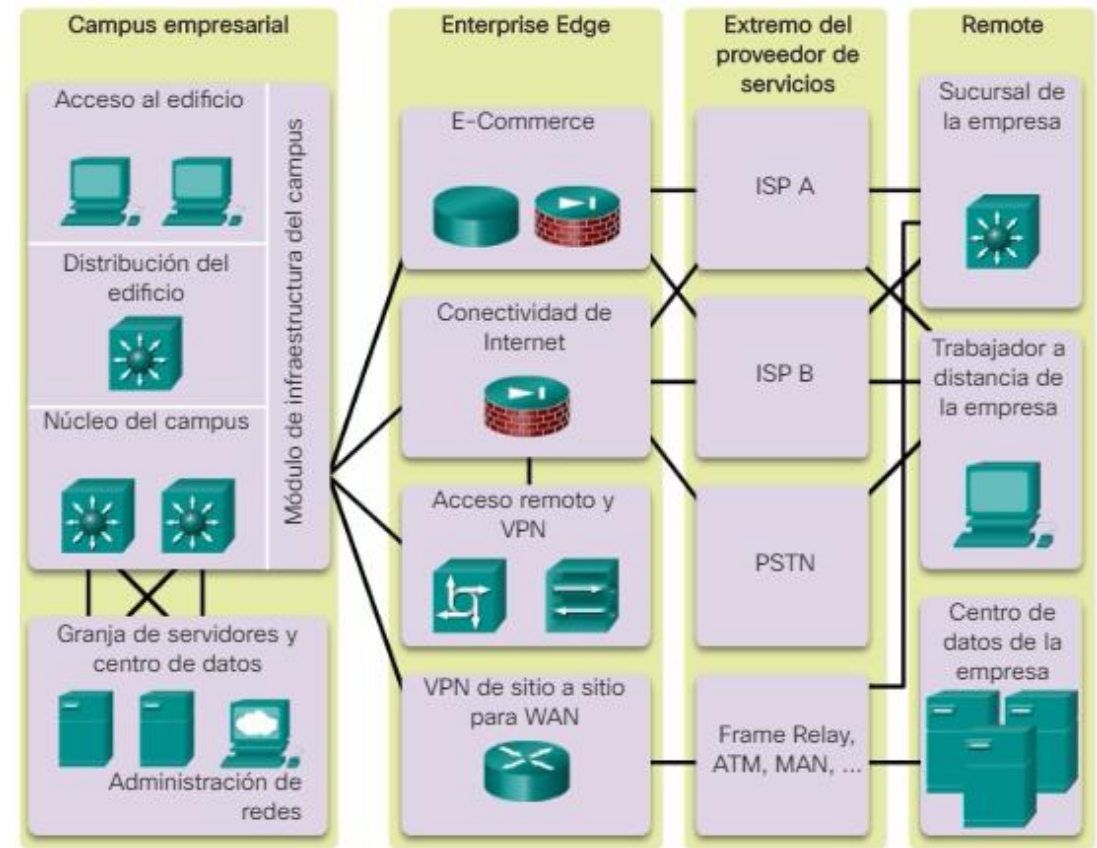
Extremo del Proveedor de Servicios

- Las empresas utilizan proveedores de servicios (SP) para enlazarse con otros sitios.
- El módulo de perímetro del SP puede incluir lo siguiente:
 - Proveedores de servicios de Internet (ISP)
 - Servicios WAN, como Frame Relay, ATM y MAN
 - Servicios de red pública de telefonía conmutada (PSTN)
- El perímetro del SP proporciona conectividad entre el módulo de campus empresarial y los módulos remotos de centro de datos, de sucursales y de trabajadores a distancia de la empresa.

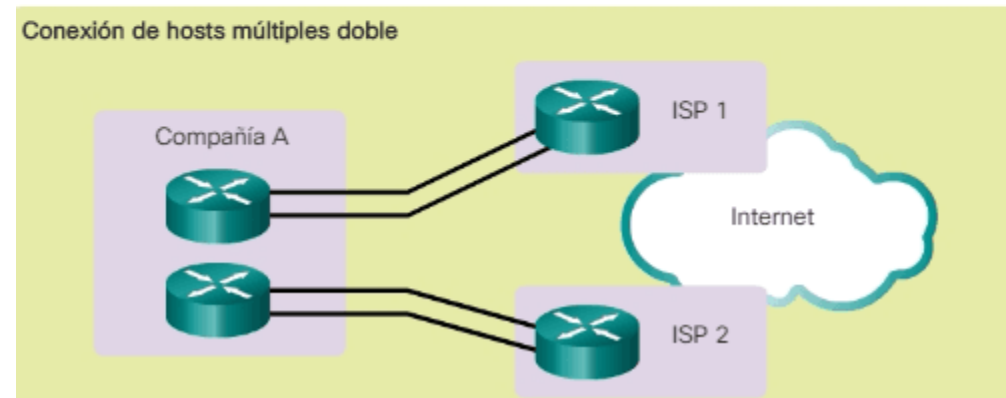
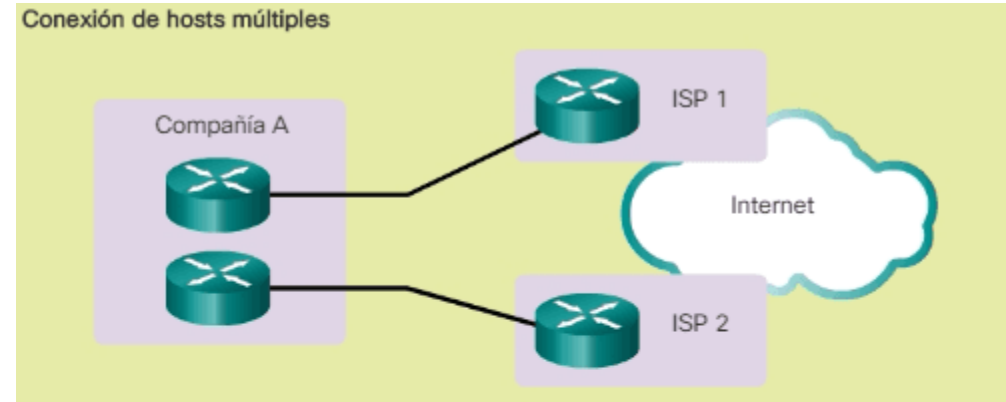
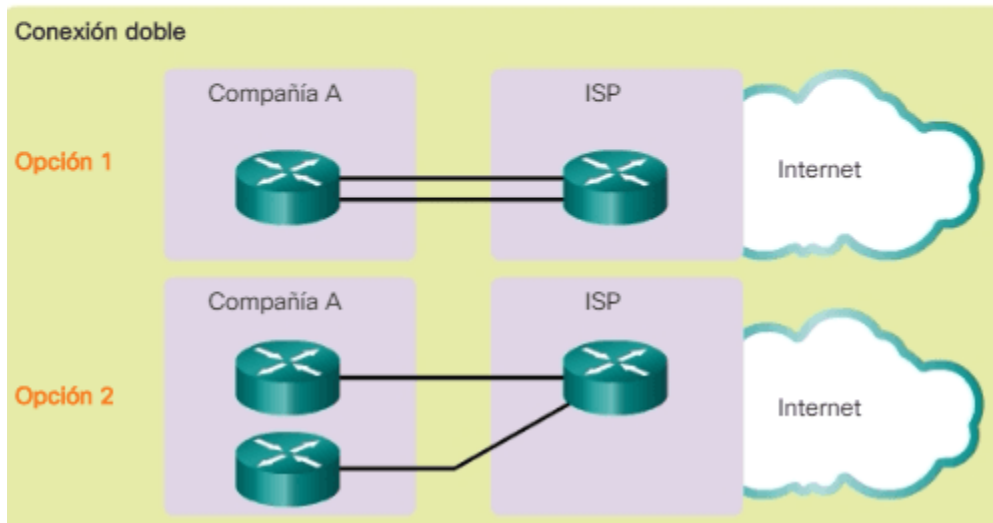
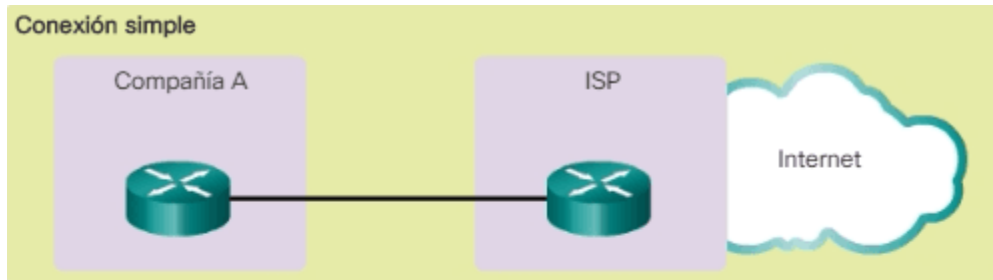


Extremo del Proveedor de Servicios

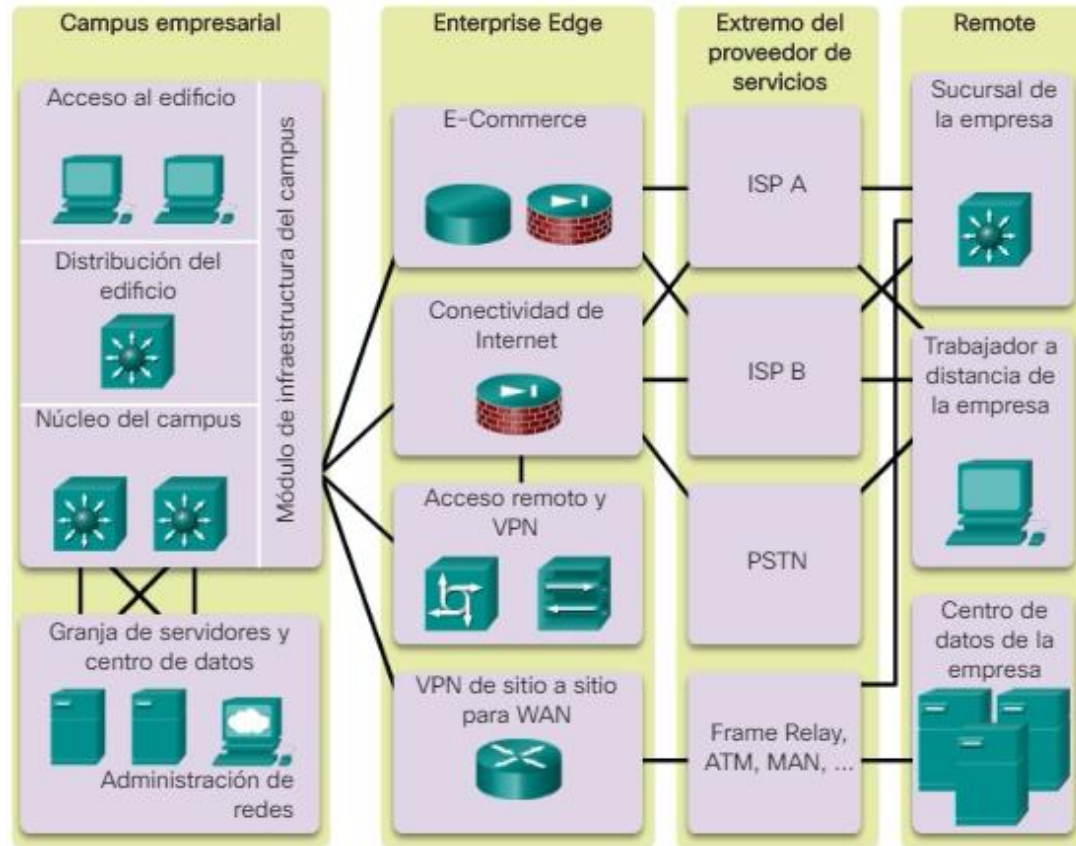
- El módulo de perímetro del SP presenta las siguientes características:
 - Abarca amplias áreas geográficas de manera rentable.
 - Converge los servicios de voz, video y datos a través de una única red de comunicaciones IP.
 - Admite QoS y acuerdos del nivel de servicio.
 - Admite seguridad mediante VPN (IPsec y MPLS) a través de las WAN de capa 2 y capa 3.



Conexiones simples y redundantes a un ISP



Área Funcional Remota



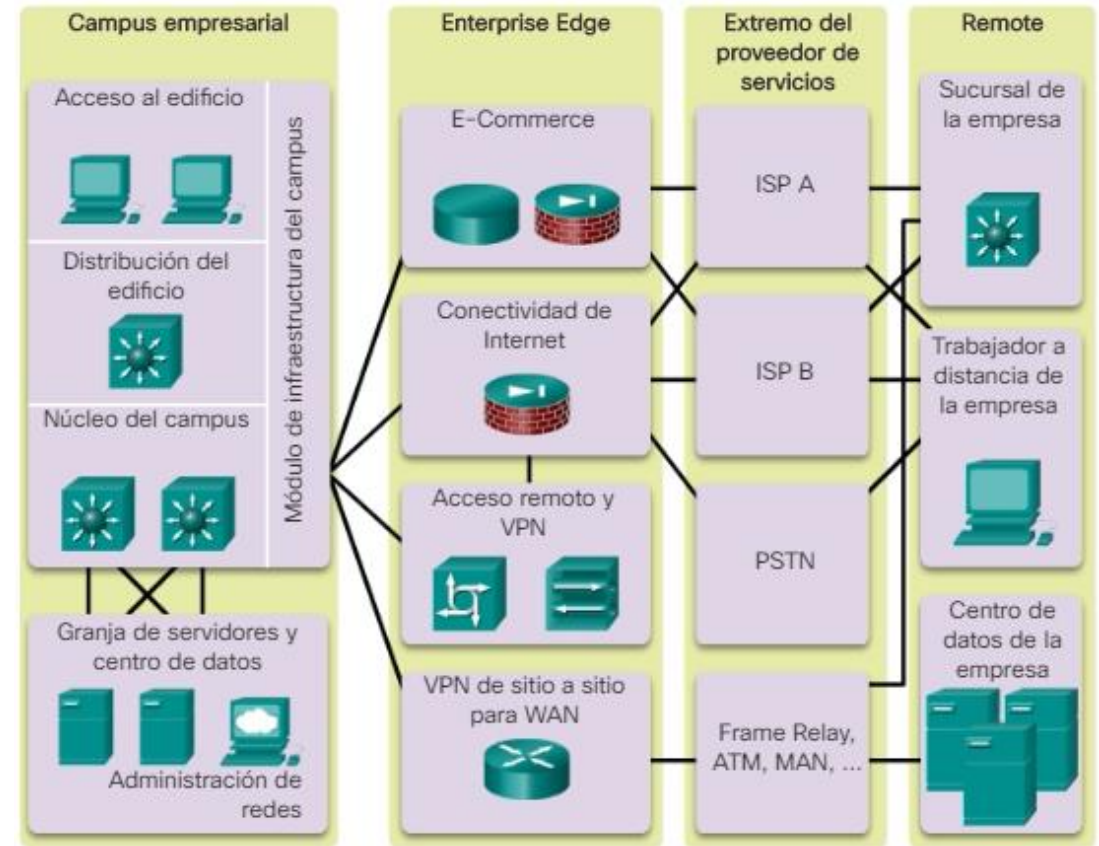
- El área funcional remota es responsable de las opciones de conectividad remota e incluye varios módulos:
 - Sucursal de la empresa
 - Trabajador a Distancia de la empresa
 - Centro de Datos de la empresa

Sucursales de la empresa

- Por lo general, estas ubicaciones son las que proporcionan opciones de seguridad, telefonía y movilidad a los empleados, así como conectividad general a la red del campus y a los distintos componentes ubicados dentro del campus empresarial.
- El módulo de sucursales de la empresa permite que las empresas extiendan las aplicaciones y los servicios de la oficina central, como la seguridad, las Comunicaciones unificadas de Cisco y el rendimiento de las aplicaciones avanzadas, hasta las sucursales remotas.
- El dispositivo perimetral que conecta el sitio remoto al sitio central varía según las necesidades y el tamaño del sitio.
- Los sitios remotos grandes pueden utilizar switches Cisco Catalyst de tecnología avanzada, mientras que los sitios más pequeños pueden usar un router ISR G2.
- Estos sitios remotos dependen del perímetro del SP para proporcionar los servicios y las aplicaciones del sitio principal.

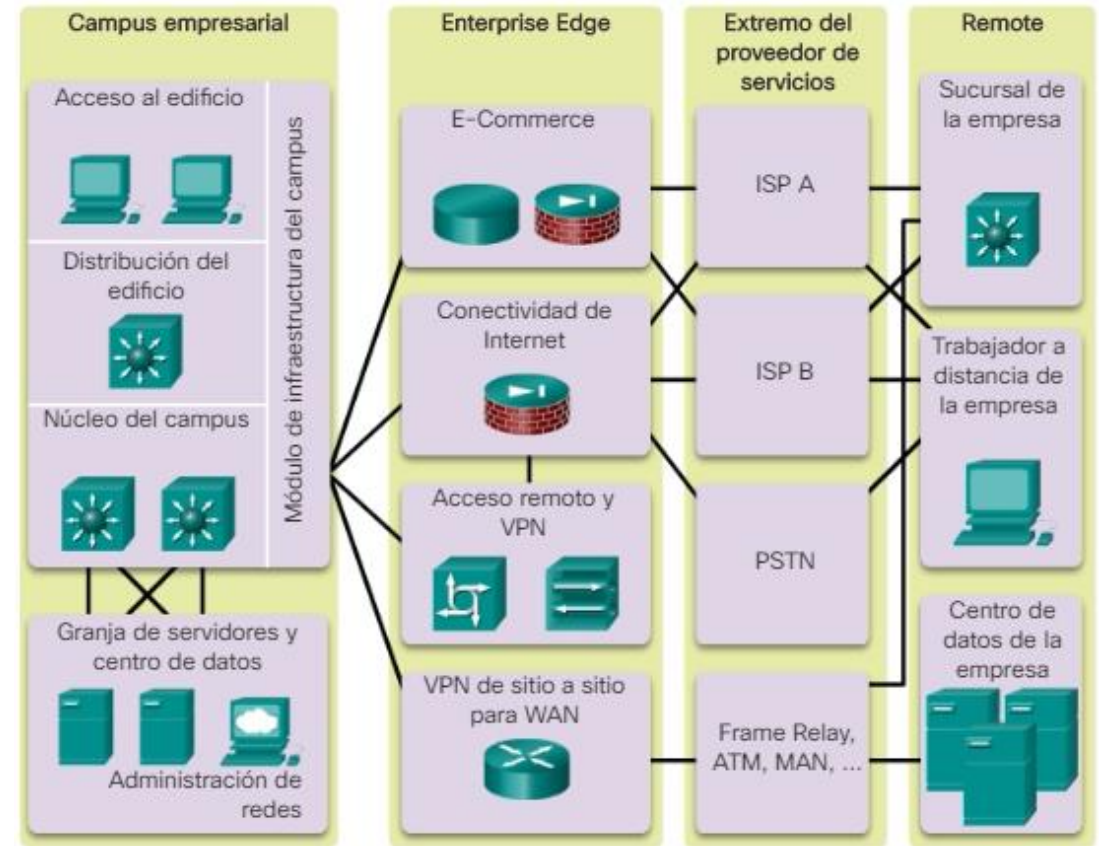
Sucursales de la empresa

- El módulo de sucursales de la empresa se conecta al campus empresarial principalmente mediante un enlace WAN; sin embargo, también cuenta con un enlace a Internet de respaldo. El enlace a Internet utiliza la tecnología VPN con IPsec de sitio a sitio para cifrar datos corporativos.



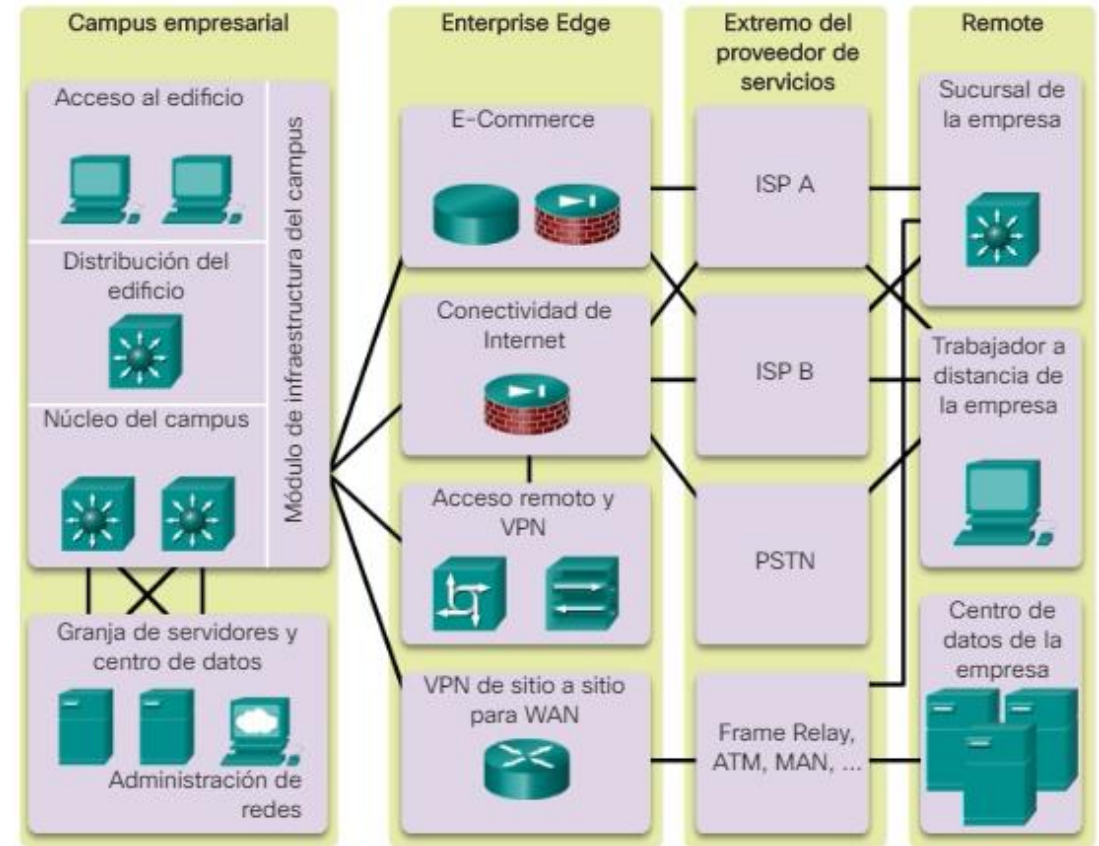
Trabajador a Distancia

- El módulo de trabajadores a distancia de la empresa se encarga de proporcionar conectividad a los empleados que trabajan desde diversas ubicaciones geográficamente dispersas, que incluyen las oficinas domésticas, los hoteles o los sitios de clientes.

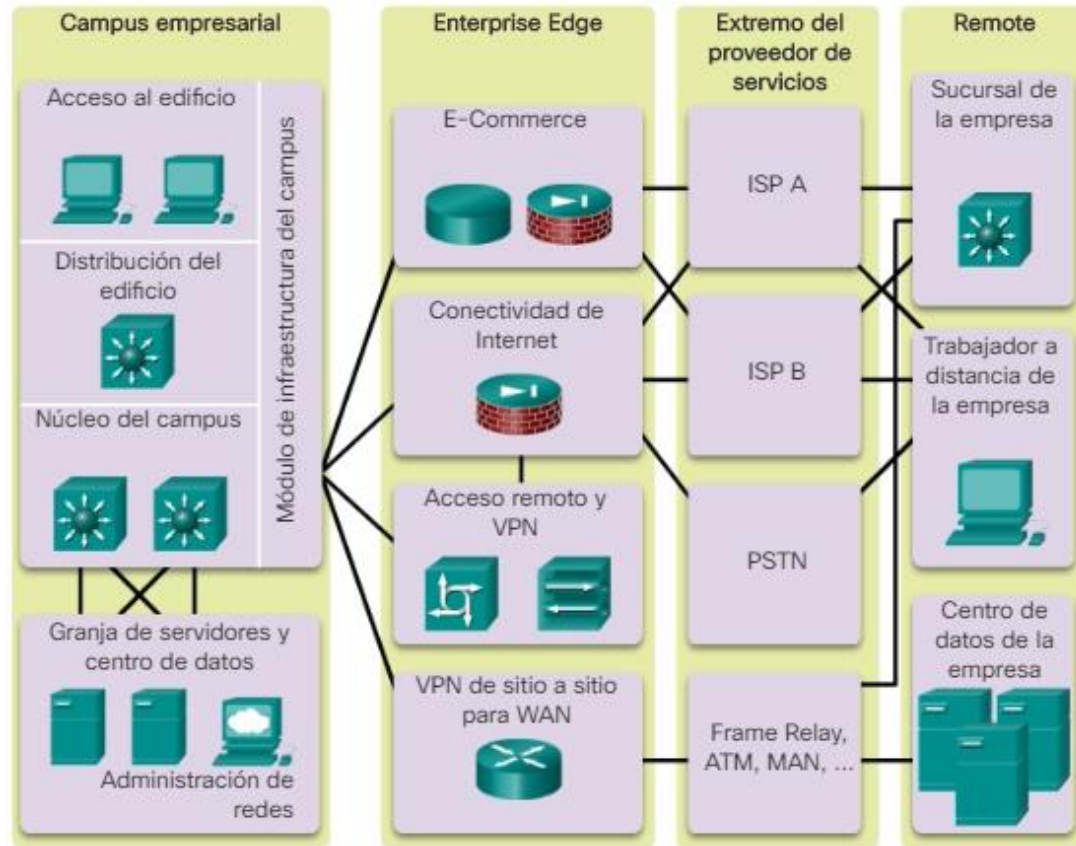


Trabajador a Distancia

- El módulo de trabajadores a distancia recomienda que los usuarios móviles se conecten a Internet mediante los servicios de un ISP local, como el cable módem o el módem DSL.
- Se pueden utilizar **servicios de VPN** para proteger las comunicaciones entre el trabajador móvil y el campus central.
- Los **servicios de red de seguridad integrada y basados en identidad** permiten que la empresa extienda las políticas de seguridad del campus al trabajador a distancia.
- El personal puede iniciar sesión en la red de manera segura a través de la VPN y acceder a las aplicaciones y los servicios autorizados desde una única plataforma rentable.

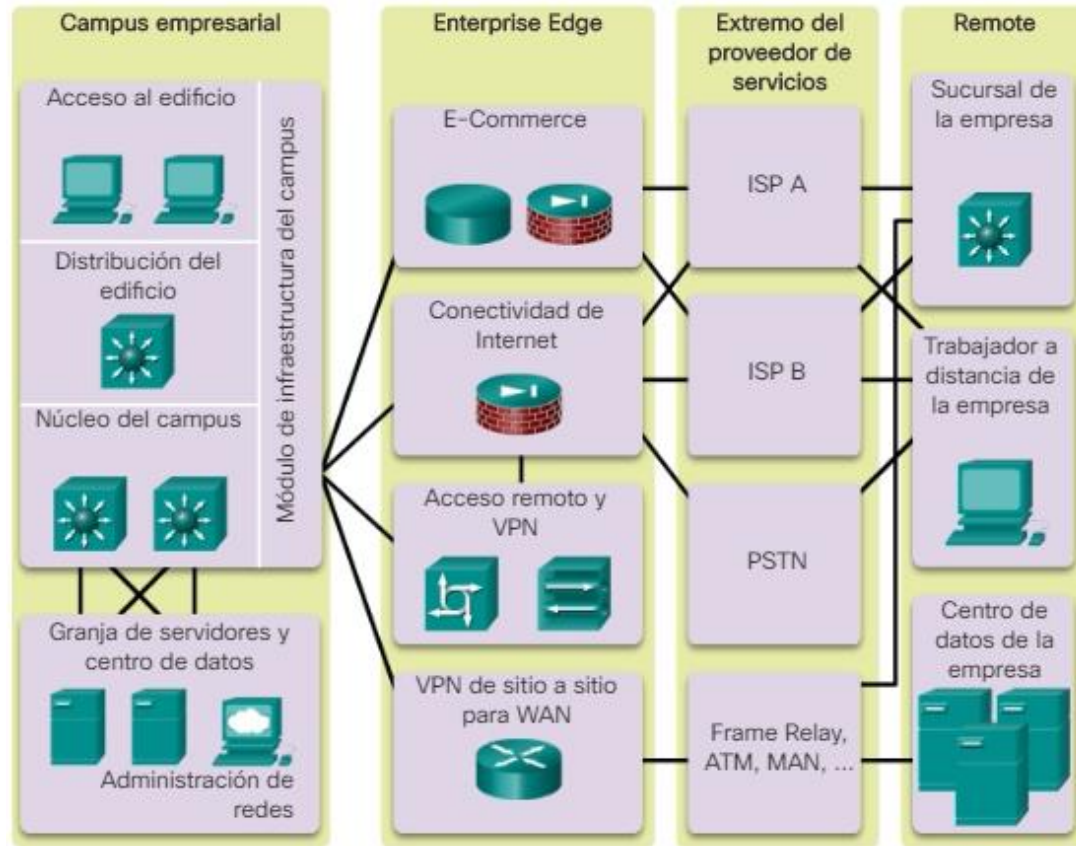


Centro de Datos de la empresa



- El módulo de centro de datos de la empresa es un centro de datos con las mismas opciones funcionales del centro de datos del campus, pero en una ubicación remota.

Centro de Datos de la empresa



- Esto proporciona una capa de seguridad adicional, dado que el centro de datos externo puede proporcionar a la empresa **servicios de recuperación tras un desastre y de continuidad empresarial**.
- Los switches de tecnología avanzada, como los switches de la serie Cisco Nexus, utilizan servicios WAN rápidos como **Ethernet metropolitana (MetroE)** para conectar el campus empresarial al centro de datos de la empresa remoto.
- Los centros de datos redundantes proporcionan respaldo mediante **la replicación síncrona y asíncrona de datos y aplicaciones**. Además, la red y los dispositivos ofrecen balanceo de carga de servidores y aplicaciones para maximizar el rendimiento. Esta solución permite que la empresa escale sin que se produzcan cambios importantes en la infraestructura.