Zona de diseño para el campus

Arquitectura de campus 3.0 empresarial: Información general y el Framework

Tabla de contenido

Arquitectura de campus 3.0 empresarial: Información general y Framework

Nota Este documento es la primera parte de un diseño general de sistemas de guía. Este documento se convertirá en capítulo 1 de la Guía de diseño general cuando se completen los restantes capítulos.

Contenido

Arquitectura de campus empresarial e introducción de diseño

Esta sección introductoria incluye las siguientes secciones de alto nivel para presentar la cobertura de contenido proporcionada en este documento:

- Audiencia
- Objetivos del documento
- Introducción
- El campus de Enterprise

Audiencia

Este documento está destinada a los planificadores de la red, ingenieros y administradores para clientes de empresas de construcción o que la intención de construir una red de campus a gran escala y requieren una comprensión de los requisitos generales de diseño.

Objetivos del documento

Este documento presenta un panorama general de la arquitectura de red del campus y incluye descripciones de diversas consideraciones de diseño, topologías, tecnologías, las directrices de diseño de configuración y otras consideraciones pertinentes para el diseño del campus de servicios completos de alta disponibilidad y tejido de conmutación. También se pretende servir de guía para dirigir a los lectores más específicas campus diseño mejores prácticas y ejemplos de configuración para cada una de las opciones de diseño específico.

Introducción

En los últimos 50 años, las empresas han logrado mejorar los niveles de productividad y una ventaja competitiva mediante el uso de la comunicación y tecnología informática. La red del campus de la empresa ha evolucionado a lo largo de los últimos 20 años para convertirse en un elemento clave en esta infraestructura informática y comunicación de negocio. No está ralentizando la evolución están relacionados entre sí de la tecnología de negocios y las comunicaciones y el medio ambiente está actualmente en otra etapa de esa evolución. La nueva *Red humana*, como que se ha denominado por los medios de comunicación, se muestra un cambio importante en la percepción de y los requisitos y exigencias en la red del campus. *La red de humana*colaboración, interactivo y centrado en las comunicaciones en tiempo real del usuario final, quien que el usuario puede ser un trabajador, un cliente, un socio, cualquier persona. La experiencia del usuario en la red ha convertido en el factor determinante del éxito o fracaso de los sistemas de tecnología, ya sea en la vida privada o profesional.

Web 2.0, aplicaciones de colaboración, combinaciones de datos etc. son refleja todo un conjunto de cambios de negocio y la tecnología que están cambiando los requisitos de nuestros sistemas de redes. Un mayor deseo de movilidad, la unidad para una mayor seguridad y la necesidad de identificar con precisión y de segmentar los usuarios, los dispositivos y redes están todos están impulsadas por los cambios en el socio de negocios de forma y trabajar con otras organizaciones. La lista de requisitos y retos que deben abordar la generación actual del campus de redes es muy diversa y incluye lo siguiente:

- Disponibilidad de la empresa global.
  - Comunicaciones unificadas, financieras, médicas y otros sistemas críticos están impulsando el requerimiento para la disponibilidad de las cinco nueves (99999) y una mejora de la convergencia veces necesarios para aplicaciones interactivas en tiempo real.
  - Migración hacia menos repositorios de datos centralizada aumenta la necesidad de disponibilidad de la red para todos los procesos de negocio.
  - Ventanas de cambio de red se están reduciendo o ser eliminada, negocios operaciones ajustan a la globalización y operan 7 x 24 x 365.
- Colaboración y comunicación en tiempo real es cada vez mayor uso de aplicaciones.
  - La experiencia del usuario se está convirtiendo en una prioridad para los sistemas de comunicación de negocio.
  - Como las comunicaciones unificadas implementaciones de aumentan, el tiempo de actividad se vuelve aún más crítica.
- Continua evolución de las amenazas de seguridad.
  - Las amenazas de seguridad continúan creciendo en número y la complejidad.
  - Distribuido y entornos de aplicaciones dinámicas están pasando por alto chokepoints de seguridad tradicionales.
- La necesidad de adaptación al cambio sin actualizaciones de carretilla.
  - TI compra la cara más tiempo en el servicio y debe ser capaz de adaptarse a adaptarse a futuros, así como los requisitos de negocio actuales.
  - Tiempo y recursos para implementar nuevas aplicaciones de negocios están disminuyendo.
  - Empiezan a aparecer nuevos protocolos de red y características (Microsoft va a presentar IPv6 en la red de la empresa).
- Las expectativas y requisitos para cualquier lugar; en cualquier momento el acceso a la red están creciendo.
  - La necesidad de acceso de socio y invitado aumenta a medida que las asociaciones empresariales están evolucionando.
  - Aumento del uso de dispositivos portátiles (portátiles y PDA) está impulsando la demanda de servicios de movilidad completa destacados y seguro.
  - Una creciente necesidad de apoyar a múltiples tipos de dispositivos en diversas ubicaciones.
- Próxima generación aplicaciones están impulsando mayores requerimientos de capacidad.
  - Medios enriquecidos incrustados en documentos.
  - Interactiva alta definición vídeo.
- Redes son cada vez más complejos.
  - Hágalo usted mismo integración puede retrasar la implementación de la red y aumentar los costos generales.
  - Reducción de riesgos de negocio requiere diseños de sistemas validadas.
  - Adopción de tecnologías avanzadas (voz, segmentación, seguridad, inalámbrica) todos introducir requisitos específicos y cambios a la base de diseño y capacidades de conmutación.

Este documento es la primera parte de una guía de diseño de sistemas generales que aborda las arquitecturas de campus de la empresa utilizando las últimas tecnologías de servicios avanzados de Cisco y se basa en principios de diseño de mejores prácticas que han sido probados en un entorno empresarial de sistemas. Introduce los principales componentes de la arquitectura y servicios que sean necesarios para implementar una red de campus altamente disponible, seguro y ricos en servicio. También define un marco de diseño de referencia que proporciona el contexto de cada uno de los capítulos de diseño específico: ayudar a comprender cómo específicas de diseño el ingeniero de red temas encajan en la arquitectura general.

El campus de Enterprise

El campus de la empresa generalmente se entiende como parte de la infraestructura informática que proporciona acceso a servicios de comunicación de red y recursos a los usuarios finales y dispositivos repartidos en una única ubicación geográfica. Podría abarcar un solo piso, edificio o incluso un gran grupo de edificios repartidos en una zona geográfica ampliada. Algunas redes tendrá un solo campus que también actúa como el núcleo o la columna vertebral de la red y proporcionar la interconectividad entre otras partes de la red global. El núcleo de campus a menudo puede interconectar el acceso de campus, el centro de datos y WAN partes de la red. En las empresas más grandes, puede haber varios sitios de campus distribuidos en todo el mundo con cada uno con el acceso de usuario final y la conectividad de red troncal local. De una técnica o de ingeniería de la red perspectiva, también se ha entendido el concepto de un campus en el sentido de la capa 2 y Ethernet Layer-3 partes de la red de conmutación fuera de los centros de datos a alta velocidad. Mientras que todas estas definiciones o conceptos de lo que una red de campus es aún son válidas, ya no completamente describen el conjunto de capacidades y servicios que componen la red del campus de hoy.

La red del campus, tal como se define a los efectos de las guías de diseño de la empresa, se compone de los elementos integrados que componen el conjunto de servicios utilizados por un grupo de usuarios y dispositivos de la estación final que todos compartimos a la misma estructura de comunicaciones conmutación a alta velocidad. Estos incluyen los servicios de paquetes-transporte (tanto cableadas e inalámbricas), la identificación de tráfico y el control (optimización de la seguridad y la aplicación), el tráfico de supervisión y administración y administración de sistemas generales y aprovisionamiento. Estas funciones básicas se implementan de manera como para proporcionar y apoyo directamente los servicios de alto nivel proporcionados por la organización de TI para uso por la comunidad de usuarios finales. Estas funciones incluyen:

- Sin-parar alta disponibilidad de servicios
- Acceso y servicios de movilidad
- Optimización de las aplicaciones y servicios de protección
- Servicios de virtualización
- Servicios de seguridad
- Operacionales y de servicios de gestión

En las secciones posteriores de este documento, se discute una visión general de cada uno de estos servicios y una descripción de cómo interoperan en una red del campus. Antes de analizar los seis servicios con más detalle, es útil entender los criterios de diseño principales y los principios de diseño que dan forma a la arquitectura de campus de la empresa. El diseño puede verse desde muchos aspectos a partir de la planta de cableado físico, escalando mediante el diseño de la topología de campus y finalmente hacer frente a la aplicación de los servicios del campus. El pedido o la manera en que todas estas cosas están vinculados a juntos para formar un todo coherente está determinado por el uso de un conjunto de la línea de base de principios de diseño que, cuando se aplica correctamente, prever una base sólida y un marco en el que se pueden implementar eficientemente los servicios de nivel superior.

Arquitectura de campus y principios de diseño

Cualquier sistema o arquitectura éxito se basa en una base de teoría del diseño sólido y principios. Diseñar una red de campus no es diferente a diseñar cualquier sistema de grande y complejo, como una pieza de software o incluso algo tan sofisticados como el transbordador espacial. El uso de un conjunto rector de los principios fundamentales de la ingeniería sirve para garantizar que el diseño de campus proporciona para el equilibrio de disponibilidad, seguridad, flexibilidad y facilidad de uso necesaria para responder a necesidades actuales y futuros empresariales y tecnológico necesita. El resto de esta visión general de diseño de campus y documentos relacionados aprovechará un conjunto común de principios de arquitectura e ingeniería: *jerarquía*, *modularidad*, *resistencia* y *flexibilidad*. Cada uno de estos principios se resume en breves las secciones siguientes:

- Jerarquía
- Modularidad
- Resiliencia
- Flexibilidad

Estos no son principios independientes. El éxito de diseño e implementación de una red de campus empresarial requiere un conocimiento de cómo cada uno se aplica a los generales de diseño y cómo se ajusta cada principio en el contexto de los demás.

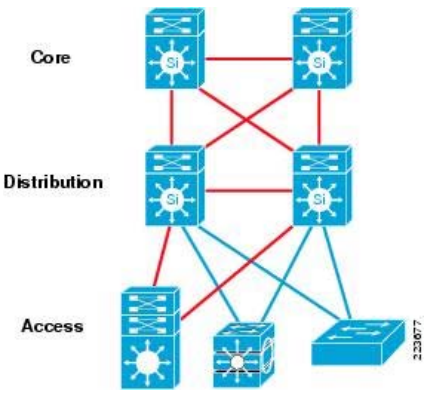
Jerarquía

Un factor crítico para la implementación exitosa de cualquier diseño de red del campus es seguir buenas directrices estructuradas de ingeniería. Un sistema estructurado se basa en dos principios complementarios: *jerarquía* y *modularidad*. Cualquier gran complejo sistema debe generarse utilizando un conjunto de componentes modular que se pueden ensamblar de forma estructurada y jerárquica. Dividir cualquier tarea o el sistema en componentes proporciona una serie de beneficios inmediatos. Cada uno de los componentes o módulos puede diseñarse con cierta independencia desde el diseño general y todos los módulos pueden funcionar como elementos semi-independent prevén el general mayor disponibilidad del sistema, así como para las operaciones y administración más sencilla. Programadores de computadoras han aprovechado este principio de la jerarquía y modularidad durante muchos años. En los primeros días del desarrollo de software, los programadores construyeron *código espagueti* sistemas. Estos primeros programas fueron altamente optimizado y muy eficaz. A medida que los programas se convirtió en más grandes y tuvieron que ser modificado o ser modificado, diseñadores de software muy rápidamente aprendieron que la falta de aislamiento entre diversas partes del programa o sistema significa que no se pueden hacer cualquier cambio pequeño sin afectar a todo el sistema. Principios de equipo basado en LAN de redes a menudo se desarrollaron después de un enfoque similar. Todos ellos comenzaron como simples optimizadas conexiones entre un pequeño número de ordenadores, impresoras y servidores. Como estas redes de área local creció y se convirtió en interconectados — que forman la primera generación de redes de campus universitarios: los mismos desafíos que enfrentan los desarrolladores del software se hizo evidentes a los ingenieros de red. Problemas en un área de la red muy a menudo habían afectado toda la red. Sencillo agregar y mover cambios en una zona tuvieron que ser cuidadosamente planeadas o puedan afectar a otras partes de la red. Del mismo modo, un error en una parte del campus bastante afectados a menudo la red del campus completo.

En el mundo del desarrollo de software, este tipo de problemas de crecimiento y la complejidad del sistema de conducir al desarrollo de diseño de programación estructurada usando sistemas modular o basada en la subrutina. Cada función individual o módulo de software ha sido escrito en tal forma que ésta podría ser modificada sin tener que cambiar todo el programa a la vez. El diseño de redes de campus universitarios ha seguido el mismo enfoque ingeniería básico como el usado por ingenieros de software. Al dividir el sistema del campus en subsistemas — o bloques de construcción, y les ensamblar en un pedido claro, que lograr un mayor grado de estabilidad, flexibilidad y capacidad de administración para las piezas individuales del campus y el campus en su conjunto.

En mirar cómo estructurado diseño deberían aplicarse las reglas para el campus, resulta útil estudiar el problema desde dos perspectivas. En primer lugar, ¿cuál es la estructura jerárquica en general del campus y qué características y funciones deberían aplicarse en cada nivel de la jerarquía? En segundo lugar, ¿cuáles son los módulos claves o la creación de bloques y cómo relacionan entre sí y trabajar en la jerarquía general? A partir de los conceptos básicos, el campus tradicionalmente se define como un modelo jerárquico de tres niveles que comprende las capas de *núcleo*, *distribución* y el *acceso* como se muestra en la figura 1 .

Figura 1 Las capas de la jerarquía del campus



Es importante tener en cuenta que si bien los niveles tienen funciones específicas en el diseño, no hay absolutas reglas para cómo físicamente se ha creado una red del campus. Si bien es cierto que muchas de las redes de campus se construyen con tres niveles físicos de conmutadores, esto no es un requisito estricto. En un campus más pequeño, la red puede tener dos niveles de conmutadores en el que los elementos básicos y la distribución se combinan en un switch físico, una distribución contraído y el núcleo. Por otra parte, una red puede tener cuatro o más niveles físicos de conmutadores porque la escala, la planta de cableado y la geografía física de la red pueden requerir que se amplíe el núcleo. Lo importante es esto: mientras que la jerarquía de la red a menudo define la topología física de los conmutadores, no son exactamente lo mismo. El principio clave del diseño jerárquico es que cada elemento en la jerarquía tiene un conjunto específico de funciones y servicios que ofrece y una función específica que desempeñar en cada uno del diseño.

Acceso

La capa de acceso es el primer nivel o el borde del campus. Es el lugar donde conexión dispositivos finales (ordenadores, impresoras, cámaras etc.) a la red cableada parte de la red del campus. También es el lugar donde se adjuntan los dispositivos que ampliación la red a un nivel más: teléfonos IP y los puntos de acceso inalámbrico (AP) están los ejemplos de clave de dos primos de dispositivos que amplían la conectividad espera una capa más desde el conmutador de acceso campus real. La amplia variedad de tipos posibles de dispositivos que pueden conectarse y los diversos servicios y mecanismos de configuración dinámica que son necesarias, hacer la capa de acceso a una de las partes más rico de la red del campus. La tabla 1 se muestran ejemplos de los tipos de servicios y funcionalidades que necesitan ser definido y apoyado en la capa de acceso de la red.

Tabla 1*Ejemplos de los tipos de servicio y capacidades*

Requisitos del servicio	Características del servicio
Descubrimiento y servicios de configuración	802.1AF, CDP, LLDP, LLDP-MED
Servicios de seguridad	IBNS (802.1X), (CISF): seguridad, DHCP espionaje, DAI, IPSG de puerto
Identidad de la red y acceso	802.1X, MAB, Web-Auth
Servicios de reconocimiento de aplicaciones	QoS marcado, policía, cola, inspección de paquetes profunda NBAR, etc..
Servicios de control de red inteligente	PVST +, Rapid PVST +, EIGRP, OSPF, AUTOEDICIÓN, PAgP/LACP, UDLD, FlexLink, Portfast, UplinkFast, BackboneFast, LoopGuard, BPDUGuard, Port Security, RootGuard
Servicios de infraestructura física	Power over Ethernet

La capa de acceso a proporciona la demarcación inteligente entre la infraestructura de red y los dispositivos informáticos que aprovechan esa infraestructura. Como tal constituye un límite de confianza política, seguridad y QoS. Es la primera capa de defensa en la arquitectura de seguridad de red y el primer punto de negociación entre dispositivos finales y la infraestructura de red. Cuando se mira el diseño general del campus, el modificador de acceso proporciona la mayoría de estos servicios de la capa de acceso y es un elemento clave para permitir que varios servicios del campus.

Distribución

La capa de distribución en el diseño de campus tiene un papel único en que actúa como un límite de servicios y el control entre el acceso y el núcleo. Tanto el acceso como núcleo son esencialmente de propósito especial dedicado capas. La capa de acceso está dedicada a cumplir las funciones de conectividad de dispositivos de final y la capa de núcleo se dedica a proporcionar conectividad sin interrupciones a través de la red de campus completo. La capa de distribución por otro lado sirve para varios propósitos. Es un punto de agregación para todos los conmutadores de acceso y actúa como parte integral del bloque de acceso de distribución de prestación de servicios de conectividad y política para flujos de tráfico dentro del bloque de distribución de acceso. También es un elemento en el núcleo de la red y participa en el diseño de enrutamiento del núcleo. Su tercera función consiste en proporcionar la agregación, punto de demarcación de política de control y el aislamiento entre el bloque de creación de la distribución de campus y el resto de la red. Volviendo a la analogía del software, la capa de distribución define los datos de entrada y salida entre la subrutina (bloque de distribución) y el línea principal (núcleo) del programa. Define un límite de resumen para los protocolos de plano de control de red (EIGRP, OSPF, Spanning Tree) y sirve como el límite de política entre los dispositivos y flujos de datos dentro del bloque de distribución de acceso y el resto de la red. En el suministro de todas estas funciones la distribución capa participa en el bloque de distribución de acceso y el núcleo. Como resultado, las opciones de configuración para las características de la capa de distribución a menudo se determinan por los requisitos de la capa de acceso o la capa de núcleo, o por la necesidad de actuar como una interfaz para ambos.

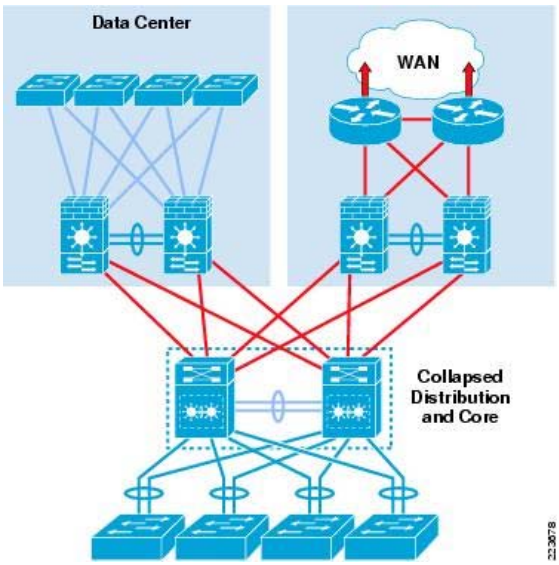
La función de la capa de distribución se explica con más detalle en la descripción del bloque de distribución de acceso y las secciones de diseño asociado.

Núcleo

El núcleo de campus es en cierta forma la parte más sencilla pero más crítica del campus. Proporciona un conjunto muy limitado de servicios y está diseñado para ser altamente disponible y operar en un *siempre en* modo. En el mundo de los negocios modernos, el núcleo de la red debe funcionar como un servicio de non-stop 7 x 24 x 365. Los objetivos clave de diseño para el núcleo de campus se basan en lo que ofrece el nivel apropiado de redundancia para permitir la recuperación de flujo de datos inmediata casi en caso de cualquier componente (conmutador, supervisor, tarjeta de línea o fibra) falla. El diseño de la red también debe permitir el ocasional, pero es necesario, hardware y software de actualización/cambio sin interrumpir las aplicaciones de red. El núcleo de la red no debe implementar servicios de cualquier política compleja, ni tampoco debería cualquier conexión de usuario/servidor con conexión directa. El núcleo también debe tener la configuración del plano de control mínimo junto con sistemas altamente disponibles configurados con la cantidad correcta de redundancia física para proporcionar a esta capacidad de servicio sin interrupciones.

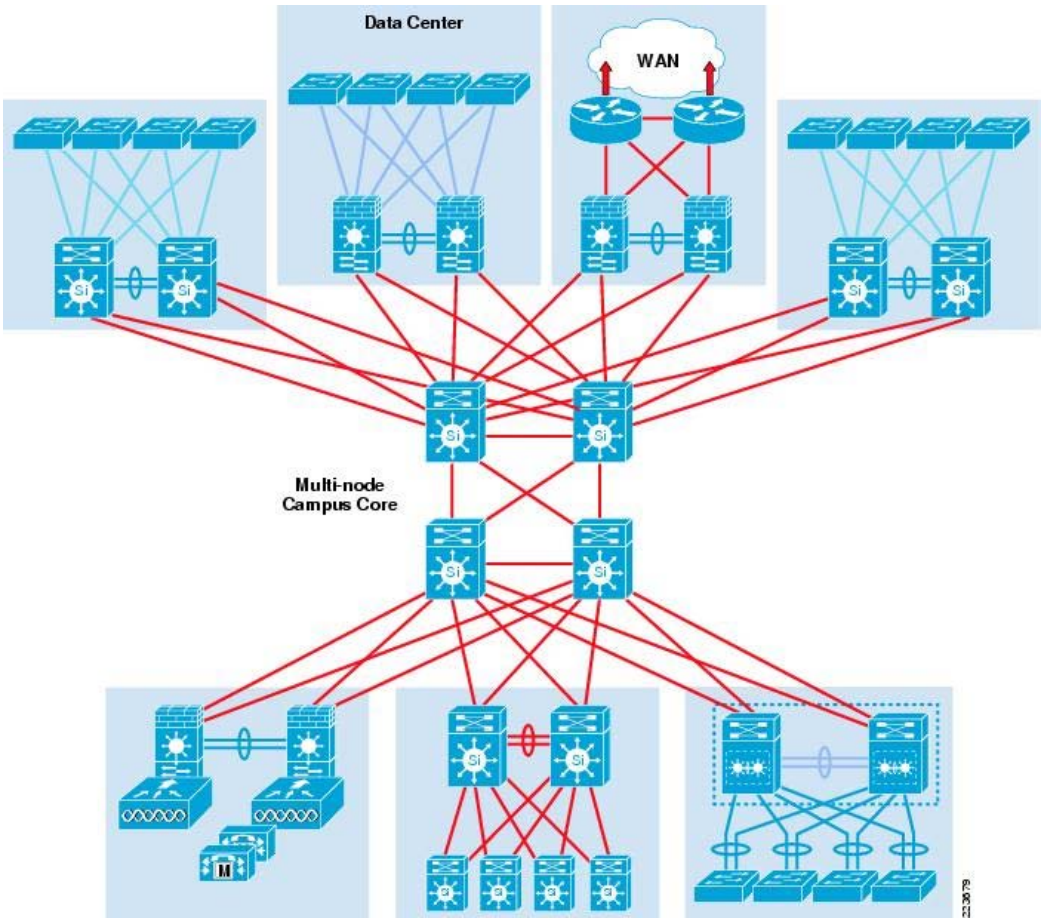
El campus principal es la columna vertebral que encola juntos todos los elementos de la arquitectura del campus. Es parte de la red que proporciona para la conectividad entre dispositivos finales, informática y servicios de almacenamiento de datos situados en el centro de datos — y otras áreas y servicios dentro de la red. Sirve como el agregador para todo el campus de otro bloquea y une el campus con el resto de la red. ¿Una pregunta que debe ser respondida al desarrollo de un diseño de campus es esto: es una capa de núcleo distintos necesaria? En esos entornos donde figura el campus dentro de un edificio único — o varios edificios adyacentes con la cantidad adecuada de fibra: es posible contraer el núcleo en los modificadores de la distribución de dos como se muestra enLa figura 2.

La figura 2 Distribución contraída y Core Campus



Es importante tener en cuenta que en cualquier campus diseño incluso aquellos que se puede integrar físicamente con un núcleo de distribución contraído que el propósito principal de la principal es proporcionar conectividad de red troncal y aislamiento de fallas. Aislar la distribución y el núcleo en dos módulos independientes crea una delimitación limpio para el control de cambio entre las actividades que afectan a estaciones finales (portátiles, teléfonos y las impresoras) y los que afectan a los datos del centro, WAN o de otras partes de la red. Una capa de núcleo también proporciona flexibilidad para adaptar el diseño de campus para satisfacer el cableado físico y los desafíos geográficos. Por ejemplo, en un campus edificios diseño que se muestra en figura 3, tener una capa independiente núcleo permite para que soluciones de diseño para cableado u otras limitaciones externas a desarrollarse sin comprometer el diseño de los bloques de distribución individuales. Si es necesario, una capa de núcleo independientes puede utilizar la tecnología de transporte, protocolos de enrutamiento, conmutación o hardware que el resto del campus, proporcionando para las opciones de diseño más flexibles cuando sea necesario.

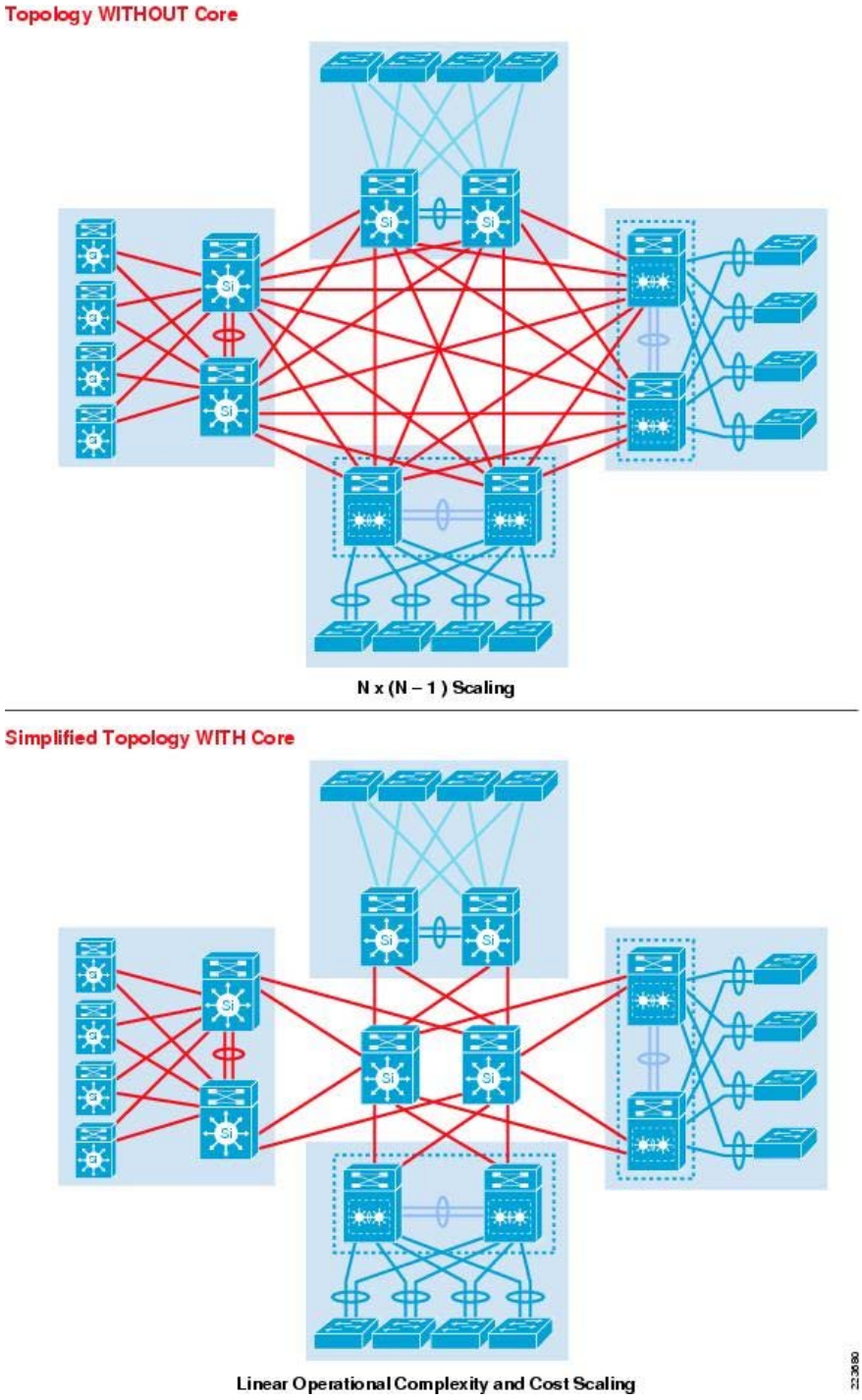
Figura 3 Multi Building Campus



Implementación de un núcleo independiente para la red del campus también proporciona una ventaja adicional de específica a medida que crece la red: un núcleo independiente ofrece la posibilidad de escalar el tamaño de la red del campus de manera estructurada que minimiza la complejidad de la general. También tiende a ser la solución más rentable.

Como se muestra en la figura 4 , como el tamaño de la red crece y crece el número de interconexiones necesarios para unir el campus, agregar una capa de núcleo reduce significativamente la complejidad del diseño general. Tenga en cuenta en figura 4, se recomienda el diseño de la parte inferior, no en la parte superior.

Figura 4 Uso de la capa de núcleo de campus para reducir la escala de la complejidad de red



El hecho de disponer de una capa de núcleo dedicado permite el campus dar cabida a este crecimiento sin comprometer el diseño de los bloques de distribución, el centro de datos y el resto de la red. Esto es especialmente importante como el tamaño del campus crece en número de bloques de distribución, área geográfica o complejidad. En un campus más grande, más complejo, el núcleo proporciona la capacidad y la capacidad para el campus en su conjunto de escalamiento.

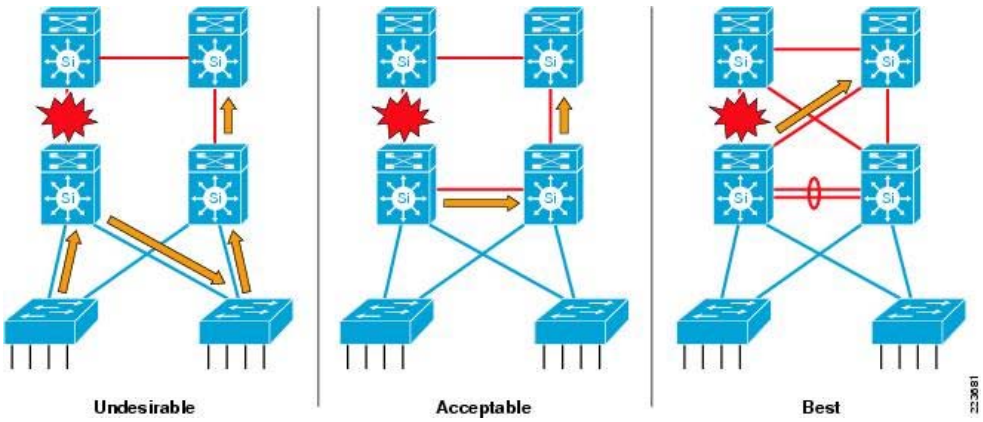
La cuestión de cuando es necesario un núcleo físico separado depende de varios factores. La capacidad de un núcleo distinto para permitir el campus resolver los desafíos de diseño físico es importante. Sin embargo, hay que recordar que un objetivo clave de tener un núcleo de distintos campus es proporcionar escalabilidad y minimizar el riesgo de movimientos (y simplificar), agrega y cambios en el campus. En general, una red que requiere cambios de configuración de rutina a los dispositivos de núcleo todavía no tiene el grado apropiado de diseño modular de diseño. A

medida que aumenta la red en tamaño o complejidad y cambios comienzan a afectar a los dispositivos de núcleo, a menudo señala razones de diseño para separar físicamente las funciones básicas y distribución en diferentes dispositivos físicos.

El control y el plano de datos de asignación a la jerarquía de la física

Implementación de jerarquía en la red del campus no es sólo cuestión de diseño físico. A fin de lograr el nivel deseado de fallas y cambiar el aislamiento, el diseño del plano de control lógico y el diseño de flujo de datos también deben seguir los principios de diseño jerárquico. Lo más importante, asignación de los tres elementos: conectividad física, plano de control lógico y flujos de datos: juntos en el mismo modelo jerárquico es necesaria para producir una implementación óptima de la red. Desde el punto de vista físico, la capa de distribución proporciona el límite entre el bloque de distribución de acceso y el núcleo de la red. Proporciona la demarcación física entre la infraestructura básica y los bloques de distribución de acceso. También debe ser el punto de demarcación y resumen entre el plano de control de núcleos y el plano de control de acceso de distribución de bloque. Tener una visión resumida de la conectividad y plano de control dentro del bloque de distribución de acceso permite el núcleo y el resto de la red se administren y cambiado sin tener en cuenta constantemente los detalles específicos de internos del bloque de distribución de acceso. El tercer aspecto del diseño jerárquico: cómo los flujos de tráfico de datos a través del campus, está configurado en la red, pero es una propiedad deseable o el objetivo del diseño. Como se muestra en la figura 5 , el mismo falla en el enlace en tres configuraciones de switch diferente puede resultar en tres rutas de recuperación de tráfico diferentes que van desde el mejor de los casos — donde aguas arriba tráfico que entra recupera a otra ruta ascendente: al peor de los casos, en el que tráfico debe fluir a una capa inferior de la jerarquía para restablecer la conectividad de red.

La figura 5 Recuperación de tráfico en un diseño jerárquico



Una de las ventajas del diseño jerárquica es que podemos lograr un grado de especialización en cada una de las capas, pero esta especialización supone cierto comportamiento de la red. Una de las hipótesis o los requisitos que permite que esta especialización es que el tráfico va siempre a fluir en el misma flujo de entrada o salida jerárquica moda (acceso a la distribución al núcleo). Cuando sabemos que la ruta alternativa para cualquier flujo de tráfico siga el mismo patrón jerárquico que la ruta original, podemos evitar tomar ciertas decisiones de diseño — tales como garantizar el acceso capa puede admitir cargas de tráfico adicional. Asimismo, sabiendo que el tráfico siempre fluye de la capa de acceso a través de una capa de distribución y, a continuación, el núcleo, es más fácil de implementar mecanismos de política consistente en cada capa. Reduce las complicaciones de diseño cuando no es necesario considerar la posibilidad de tráfico que fluye alrededor o a través de una capa de la política de dos veces. Diseñar la jerarquía de la red para apoyar la coherencia de los datos flujo comportamiento también tiene el efecto de mejorar la hora de convergencia de la red en caso de un fracaso. Igualdad costo Multi-Path (ECMP) diseña y otras configuraciones totalmente redundantes garantizar estos datos jerárquicos flujos además para tiempos de convergencia rápida y determinista con proporcionan no plenamente malla diseños, como se muestra en el caso *lo mejor* de figura 5.

Modularidad

El segundo de los dos principios de diseño estructurado es *modularidad*. Los módulos del sistema son los pilares que se ensamblan en el campus de la más grande. La ventaja del enfoque modular es en gran medida debido al aislamiento que puede proporcionar. Errores que se producen dentro de un módulo pueden ser aislados del resto de la red, proporcionando para la detección de problemas más simple y una mayor disponibilidad del sistema general. La introducción de nuevos servicios, mejoras o cambios en la red puede hacerse de forma controlada y por fases, lo que permite una mayor flexibilidad en el mantenimiento y operación de la red del campus. Cuando un módulo específico ya no tiene una capacidad suficiente o falta una nueva función o servicio, puede ser actualizado o sustituido por otro módulo que tiene el mismo papel estructural en el diseño general jerárquico. La arquitectura de red del campus se basa en el uso de dos bloques básicos o módulos que están conectados entre sí mediante el núcleo de la red:

- Bloque de distribución de acceso
- Bloque de servicios

Las secciones siguientes presentan los pilares de campus subyacente. Para obtener instrucciones de diseño detallado, consulte cada uno del documento de diseño adecuado que enfrenta cada módulo específico.

Bloque de acceso-distribución

El bloque de acceso-distribución (también contemplado como el bloque de distribución) es probablemente el elemento más conocido de la arquitectura del campus. Es el componente fundamental de un diseño de campus. Diseñar correctamente el bloque de distribución va un largo camino para garantizar el éxito y la estabilidad de la arquitectura general. El bloque de acceso-distribución consta de dos de los tres niveles jerárquicos dentro de la arquitectura multicapa campus: las capas de acceso y distribución. Si bien cada una de estas capas tiene servicio específico y los requisitos de la función, es las opciones de diseño de plano de control topología de red — como enrutamiento y que abarcan los protocolos de árbol, que son fundamentales para determinar cómo el bloque de distribución encola juntos y se ajusta a la arquitectura general. Actualmente hay tres opciones de diseño básico para la configuración del bloque de distribución de acceso y el plano de control asociado:

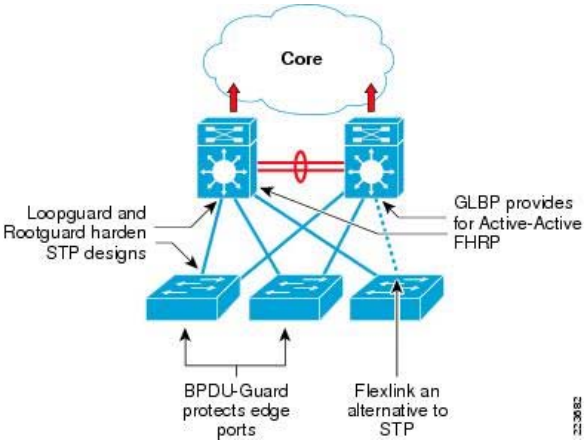
- Multi-Tier
- Acceso enrutado
- Switch virtual

Mientras que los tres de estos diseños utilizan el mismo básica topología física y el cableado de la planta de son las diferencias en donde existen los límites de nivel-2 y Layer-3, cómo se implementa la redundancia de topología de red y cómo funciona el equilibrio de carga, junto con una serie de otras diferencias principales entre cada una de las opciones de diseño. Si bien se puede encontrar una descripción de completar la configuración de cada modelo de distribución de acceso de bloque dentro de los documentos de diseño detallado, el siguiente proporciona una breve descripción de cada opción de diseño.

Bloque de acceso-distribución multi-nivel

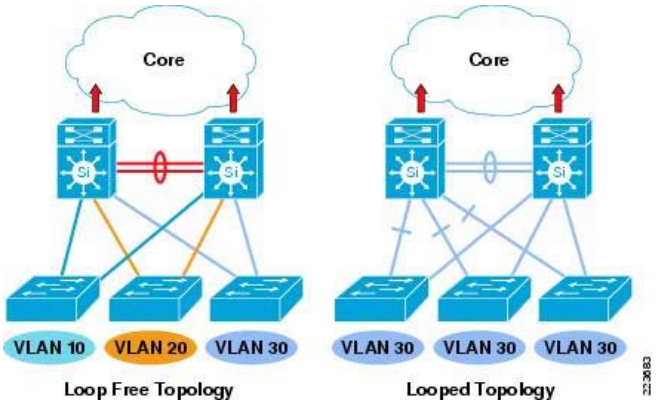
El modelo de múltiples niveles de acceso-distribución se ilustra en la figura 6 es el diseño de bloques de acceso-distribución de campus tradicionales. Todos los conmutadores de acceso están configurados para funcionar en modo de reenvío de capa 2 y la distribución de conmutadores están configurados para ejecutar el reenvío de capa 2 tanto Layer-3. Basado en VLAN troncos se utilizan para ampliar las subredes de los conmutadores de distribución hasta la capa de acceso. Un protocolo de puerta de enlace predeterminada — como HSRP o GLBP — se ejecuta en los distribución de los conmutadores de capa junto con un protocolo de enrutamiento para proporcionar enrutamiento ascendente al núcleo del campus. Una versión de árbol y el uso de la spanning tree endurecimiento características (como Loopguard, Rootguard y BPDUGuard) se configuran en los puertos de acceso y el conmutador y switch vínculos que corresponda.

La figura 6 Bloque de distribución Multi-Tier Campus acceso a



El diseño de varios niveles tiene dos variaciones básicas, como se muestra en la figura 7 , que principalmente sólo difieren en la forma en que se definen VLAN. En el diseño de un bucle, uno a muchos VLAN están configuradas para abarcar varios conmutadores de acceso. Como resultado, cada uno de estas VLAN *distribuido* tiene un spanning tree o capa 2 desdoblarse topología. La otra alternativa: laDiseño *V* o *libre de bucle*: sigue las instrucciones actual de prácticas recomendadas para el diseño de varios niveles y define VLAN únicas para cada conmutador de acceso. La eliminación de bucles en la topología proporciona una serie de beneficios, incluyendo por dispositivo de enlace ascendente balanceo de carga con el uso de GLBP, una menor dependencia que abarcan el árbol para proporcionar para la recuperación de la red, reducción del riesgo de difusión de las tormentas y la capacidad para evitar las inundaciones de unidifusión (y desafíos de diseño similar asociados con topologías no-simétricas de reenvío de nivel-2 y Layer-3).

La figura 7 Bloque de dos grandes variaciones de la distribución Multi-Tier

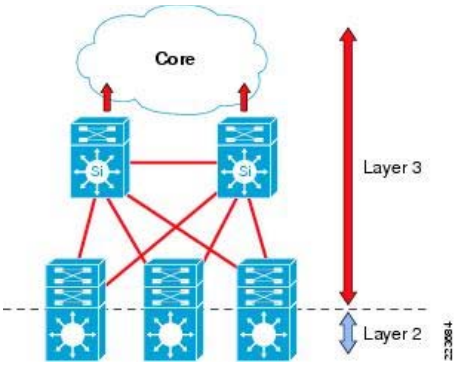


Las instrucciones de diseño detallado para el diseño de bloques de distribución de enrutado acceso pueden encontrarse en la sección de campus de la CCO SRND sitio http://www.cisco.com/go/srnd.

Dirige el bloque de distribución de acceso a

Como configuración alternativo a la distribución de varios niveles tradicional modelo de bloque es uno en que el modificador de acceso actúa como un completo Layer-3 enrutamiento nodo (proporciona tanto nivel-2 y conmutación Layer-3) y el acceso a la distribución de capa 2 enlace ascendente troncos se reemplazan con enlaces enrutado de punto a punto de Layer-3. Esta configuración alternativa, en el que se mueve la demarcación de la capa-2/3 interruptor de la distribución al conmutador acceso parece ser un cambio importante en el diseño, pero es realmente simplemente una extensión del diseño de la mejor práctica varios niveles. Consulte la figura de 8.

Figura 8 Enrutado diseño de bloques de distribución de acceso



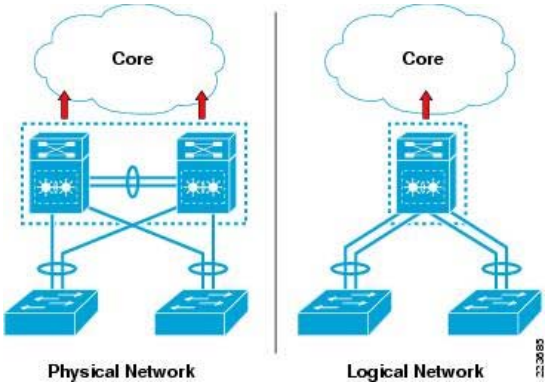
En el mejor diseño de acceso a múltiples niveles y enrutado práctica, cada conmutador de acceso está configurado con voz única, datos, y cualquier otro requiere VLAN. En el diseño de enrutado de acceso, el puente de puerta de enlace y raíz predeterminado para estos VLAN simplemente se mueve desde el conmutador de distribución para el modificador de acceso. Abordar para poner fin a todas las estaciones y para el valor predeterminado gateway sigue siendo la misma. VLAN y restos de configuración de puerto específico sin cambios en el conmutador de acceso. Interfaz de configuración del enrutador, listas de acceso, **auxiliar de ip** y cualquier otras configuraciones para cada VLAN siguen siendo idénticos. Sin embargo, estos ya están configurados en la VLAN Switched Virtual Interface (SVI) definidos en el conmutador de acceso, en lugar de en los conmutadores de distribución. Hay cambios de configuración notable asociados con el traslado de la interfaz Layer-3 hasta el modificador de acceso. Ya no es necesario configurar una dirección de la puerta de enlace virtual HSRP o GLBP, como las interfaces de enrutador para todas las VLAN ahora son locales. Asimismo, con un enrutador de multidifusión único para cada VLAN no es necesario para ajustar los intervalos de consulta PIM o para garantizar que el enrutador designado está sincronizado con la puerta de enlace HSRP activo.

El diseño de bloques de distribución de enrutado acceso tiene una serie de ventajas sobre el diseño de varios niveles con su uso del acceso de capa 2 a los enlaces ascendentes de distribución. Ofrece herramientas (como ping y traceroute) de solución de problemas de end-to-end común, que se utiliza un protocolo de control único (EIGRP o OSPF) y elimina la necesidad de características tales como HSRP. Si bien es el diseño apropiado para muchos entornos, no es adecuado para todos los entornos, ya que requiere que no VLAN abarcan varios conmutadores de acceso. Las instrucciones de diseño detallado para el diseño de bloques de distribución de enrutado acceso pueden encontrarse en la sección de campus del sitio SRND CCO, http://www.cisco.com/go/srnd.

Conmutador virtual

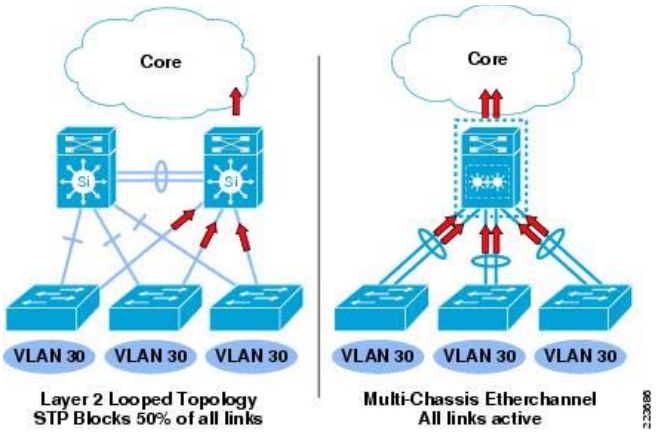
El diseño de bloques de distribución de sistema de cambio virtual (VSS) es el cambio radical de los acceso enrutado o diseños varios niveles. La introducción de la Cisco Catalyst 6500 VSS y Stackwise/Stackwise-Plus en el Cisco Catalyst 3750/3750E ofrece la oportunidad de realizar un cambio significativo en el interruptor y redundancia de vínculo puede realizarse. En el pasado, varios conmutadores de acceso se conectaron a dos conmutadores de distribución redundantes y la configuración de los protocolos de control de red (como HSRP, 802.1D spanning tree y EIGRP) determina la forma en que los modificadores reenvían el tráfico sobre cada uno de los enlaces ascendentes y la red recuperado en caso de una conmutador o falla del enlace. Con la introducción del concepto switch virtual, el par de conmutador de distribución ahora puede configurarse para que se ejecute como un solo conmutador lógico tal como se muestra en la figura 9 . Al convertir los modificadores de la distribución física redundantes en una única lógica modificador, se realiza un cambio significativo a la topología de la red. En lugar de un conmutador de acceso configurado con dos enlaces ascendentes a dos de distribución de conmutadores — y que necesitan un protocolo de control para determinar cuál de los enlaces ascendentes a utilizar: ahora el modificador de acceso tiene un único multi-chassis EtherChannel (MEC) enlace ascendente conectado a un conmutador de distribución única.

La figura 9 virtual conmutador físicos y lógicos



El cambio de dos enlaces ascendentes independientes a un único ascendentes de EtherChannel multi-chassis tiene una serie de ventajas. Véase la figura de , 10. Equilibrio de carga de tráfico y la recuperación de errores de enlace ascendente ahora aprovechar las capacidades de EtherChannel. El tráfico es el equilibrio de carga por flujo, en lugar de por cliente o por subred. En el caso de que se produce un error en uno de los enlaces ascendentes, la EtherChannel redistribuye automáticamente todo el tráfico a los vínculos restantes en el paquete de enlace ascendente en lugar de esperar que abarcan el árbol, HSRP, así como otro protocolo convergen. La capacidad de eliminar los bucles de capa 2 físicos de la topología — y que ya no depende de que abarcan el árbol de prever la topología de mantenimiento y vínculo redundancia: resulta en un diseño de bloques de distribución que permite subredes y VLAN para ser distribuidos a través de varios modificadores de acceso (sin los desafíos tradicionales y las limitaciones de un diseño de capa 2 spanning basado en el árbol).

La figura 10 Virtual switch frente a la expansión de la topología de árbol

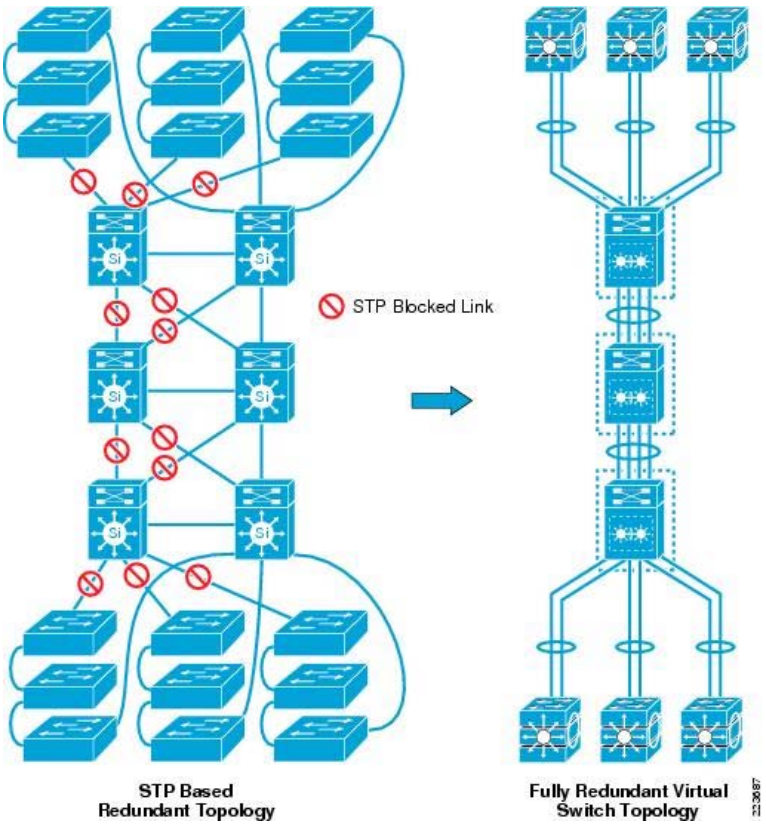


La capacidad para eliminar los bucles físicos de la topología y ya no puede depender de que abarcan el árbol, es una de las ventajas significativas del diseño switch virtual. Sin embargo, no es la única diferencia. El diseño de switch virtual permite una serie de cambios fundamentales a la configuración y el funcionamiento del bloque de distribución. Mediante la simplificación de la topología de red para usar un modificador único distribución virtual, muchos otros aspectos del diseño de la red son bien simplificados en gran medida o, en algunos casos, ya no es necesarios. Características como HSRP o GLBP ya no son necesarias porque ambos conmutadores actúan como una puerta de enlace predeterminada lógico. Listas de configuración para tanto por subred o VLAN características tales como el acceso, ip-auxiliar y otros deben sólo una vez hecho, no replica y mantener sincronizados entre dos conmutadores independientes. Asimismo, cualquier configuración del conmutador debe hacerse una sola vez y está sincronizado a través de los supervisores redundantes.

Nota Mientras que el diseño de switch virtual eliminar la dependencia de que abarcan el árbol para el mantenimiento de la topología activa, que abarcan árbol debe no desactivar. Spanning tree debe seguir siendo configurado como un mecanismo de resiliencia copia de seguridad.

El switch virtual no se limita a la distribución del campus. Un switch virtual puede utilizarse en cualquier ubicación en el diseño de campus donde es deseable para reemplazar la redundancia de hardware y plano de control actual con la topología simplificada ofrecida por el uso de un switch virtual. El switch virtual simplifica la topología de red mediante la reducción del número de dispositivos como vistos por el spanning tree o Protocolo de enrutamiento. Un switch virtual que existían dos o más nodos con varios vínculos independiente conectar la topología, puede reemplazar partes de la red con un único nodo lógico con menos de enlaces. Figura 11 se muestra un caso extremo en el que una topología-to-end, nivel-2 se va a migrar desde una topología de basado en el árbol spanning totalmente redundante a una red virtual basada en el conmutador de end-to-end. Aquí, la topología es tanto drásticamente simplificación y ahora todos los enlaces están activamente reenvío con no spanning bucles de árbol.

La figura 11 Uso del diseño virtual switch en una topología de capa 2-to-end



Mientras que el uso de un switch para simplificar la topología de campus virtual puede ayudar a enfrentar muchos desafíos de diseño, el diseño general deben seguir los principios de diseño jerárquica. El uso apropiado de nivel-2 y Layer-3 Resumen, seguridad y límites de QoS todos aplicar en un entorno de switch virtual. Mayoría de los entornos de campus adquirirán las grandes ventajas de un switch virtual en la capa de distribución.

Para obtener más información sobre el diseño de la distribución de conmutación virtual bloque vea el diseño de bloques de distribución de próximas switch virtual, http://www.cisco.com/go/srnd.

Comparación de diseño de bloques de distribución

Mientras que cada uno de los tres diseños de bloque de acceso-distribución ofrece un método viable, hay ventajas al conmutador virtual y diseños de enrutado acceso sobre el enfoque tradicional de varios niveles. Una configuración más sencilla de red global y la operación, por el equilibrio de carga ascendente y descendente de flujo y la convergencia más rápido son algunas de las diferencias entre estas opciones de diseño más recientes y el enfoque tradicional de varios niveles. La selección de una opción de diseño específico para una red de campus dado es una decisión importante en la planificación de un diseño de campus. Tabla 2 proporciona una visión general comparación de las tres opciones de diseño. Antes de hacer que una decisión de diseño final, revise las descripciones de diseño detallado proporcionadas por Cisco para garantizar que se consideran todos los factores pertinentes a su entorno.

Tabla 2 Comparación de modelos de diseño de bloques de distribución

	Acceso multi-nivel	Enrutado Access	Conmutador virtual
Protocolos de plano de control de distribución de acceso	Spanning Tree (PVST +, Rapid-PVST + o MST)	EIGRP o OSPF	PAgP, LACP
Spanning Tree	STP para redundancia de red y para evitar que los bucles de nivel 2	No[1]	No [2]
Mecanismos de recuperación de red	Spanning Tree y FHRP (HSRP, GLBP, VRRP)	EIGRP o OSPF	EtherChannel multi-Chassis (MEC)
Armarios de cableado spanning VLAN	Admite (requiere L2 spanning bucles de árbol)	N	Admite
Demarcación de capa 2/3	Distribución	Acceso	Distribución [3]
Primer Protocolo de redundancia de salto	HSRP, GLBP, VRRP necesario	No requiere	No requiere
Acceso a la distribución por el equilibrio de carga de flujo	N	Sí - ECMP	Sí - MEC
Convergencia	900 MS 50 segundos (Dependen de la topología de STP y ajuste FHRP)	50 a 600 MS	50 a 600 MS [4]
Control de cambios	Distribución dual conmutador diseño requiere configuración manual de sincronización, pero permite cambios y actualizaciones del código independiente	Distribución dual conmutador diseño requiere configuración manual de sincronización, pero permite cambios y actualizaciones del código independiente	Switch virtual única auto-sincroniza la configuración entre hardware redundante, pero no se permite no actualmente actualizaciones del código independiente para los conmutadores de miembros individuales

[1]Ni el acceso distribuido ni switch virtual diseños requieren STP configurado para conservar la topología de red. Es todavía recomendar y necesarias para permitir el uso de características tales como la guardia BPDU en puertos de acceso.
[2]Lo mismo como notas al pie de página 1.
[3]Con un diseño switch virtual, es posible configurar una capa de acceso a enrutado, pero esto afectará la capacidad para abarcar VLAN armarios de cableado.
[4]Pruebas iniciales indica veces convergencia comparable a la MS acceso enrutado 50 a 600. Consulte la próxima *Guía de diseño de conmutador virtual* para valores finales.

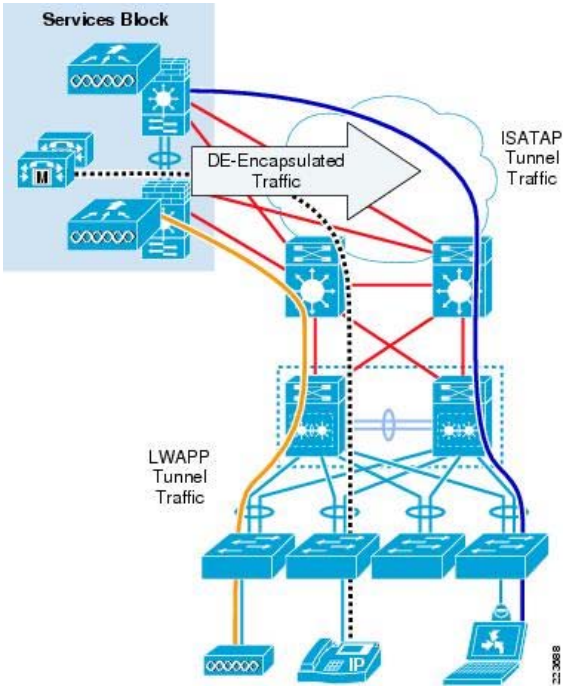
Bloque de servicios

El bloque de servicios es un elemento relativamente nuevo en el diseño de campus. Consulte la figura de 12. En cuanto los planificadores de la red de campus comienzan a considerar la migración a entornos de doble pila IPv4/IPv6, migrar a entornos de WLAN basada en el controlador y continuar integrar los servicios de comunicaciones unificadas más sofisticados, una serie de retos sentar por delante. Será imprescindible para integrar estos servicios en el campus sin problemas, mientras que prevén el grado apropiado de aislamiento de administración y fallas de cambio operacional y continua mantener un diseño flexible y escalable. Como ejemplo, se pueden implementar servicios IPv6 a través de una superposición ISATAP provisional que permite que los dispositivos túnel IPv6 sobre porciones del campus, que no todavía IPv6 nativo habilitado. Este enfoque provisional permite una rápida introducción de nuevos servicios sin necesidad de un toda la red, hot traslado.

Algunos ejemplos de funciones recomendadas que se encuentra en un bloque de servicios:

- Controladores inalámbricos LWAPP centralizados
- Terminación del túnel de ISATAP de IPv6
- Local borde de Internet
- Servicios de comunicaciones unificadas (Cisco Unified Communications Manager, puertas de enlace, MTP etc.)
- Política de puertas de enlace

La figura 12 Bloque de servicios de campus



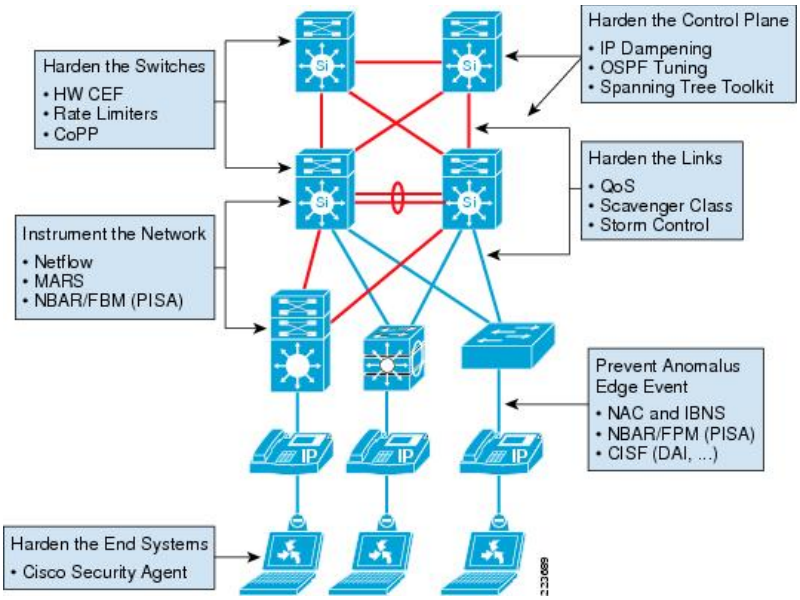
El bloque de servicios no es necesariamente una sola entidad. Puede haber varios bloques de servicios en función de la escala de la red, el nivel de redundancia geográfica necesaria y otros factores físicos y operacionales. El bloque de servicios sirve para un propósito central en el diseño de campus; aísla o separa funciones específicas en lo que permite limpiadores procesos operacionales y administración de la configuración de conmutadores de servicios dedicados.

Resiliencia

Si bien los principios de diseño estructurado y el uso de la modularidad y jerarquía son esenciales para el diseño de redes de campus universitarios son *no* es *suficiente* para crear una infraestructura de red escalable y sostenible. Considere la analogía de desarrollo de software. En el mundo del software, ya no es suficiente para que los programas simplemente generar la salida correcta dada la entrada correcta. En la misma manera, no es suficiente que una red del campus se consideran completa únicamente porque pasa datos desde un punto a otro correctamente. Como se muestra por las numerosas vulnerabilidades de seguridad que se exponen en sistemas operativos de software y programas en los últimos años, diseñadores de software están aprendiendo que para ser *correcta* ya no es suficiente. También se diseñarán sistemas para resistir el fracaso en condiciones inusuales o anormales. Una de las formas más sencillas para romper cualquier sistema es empujar las condiciones de límite: para buscar los bordes del diseño del sistema y buscar vulnerabilidades. Si estás intentando romper una pieza de software que acepta una gama de entrada de valores de uno a diez, intenta darle insumos de diez mil, diez millones de habitantes, etc., para determinar cuándo y cómo se romperá. Si estás intentando romper una red, siga un enfoque similar. Introducir un volumen de tráfico, número de los flujos de tráfico o otra condición anómala para encontrar las vulnerabilidades. Ingenieros de software se han convertido en muy conscientes del problema y han adoptado diversos enfoques para resolverlo, incluido el uso de comprobación de enlaces, hacer valer las comprobaciones y diseño modular mayor. Ingenieros de red frente a un desafío de diseño fundamentales similar también deben adaptarse a las estrategias de diseño de red para producir una arquitectura más resistente.

¿Qué significa para crear un diseño resistente en el contexto de la red del campus? Una característica básica de resiliencia es la capacidad para que el sistema permanecen disponibles para su uso en condiciones normales y anormales. Las condiciones normales incluyan tales eventos como cambiar ventanas y flujos de tráfico normal o esperado y patrones de tráfico. Condiciones anormales incluyen fallas de hardware o software, cargas de tráfico extrema, patrones de tráfico inusuales, eventos de denegación de servicio (DoS) si voluntaria o involuntariamente y cualquier otro evento imprevisto. Como ilustrado en figura 13, hay una serie de enfoques de proporcionar resiliencia incluyendo endurecimiento de los componentes individuales, conmutadores y vínculos de la red, agregar Acelerador o capacidades de funciones de software y hardware, proporciona controles explícitos sobre el comportamiento de los dispositivos de borde, de limitación de velocidad y los equipos de la utilización de instrumentos y herramientas de administración para proporcionar comentarios a las operaciones de red.

Figura 13 Ejemplos de las características de resiliencia campus



Diseño resistente no es una característica tampoco hay una cosa específica que hace para lograrlo. Como con la jerarquía y modularidad, resiliencia es un principio básico que se hace real mediante el uso de muchas funciones relacionadas y opciones de diseño. El uso coordinado de varias funciones y el uso de características para servir a múltiples propósitos son aspectos del diseño resistente. Un ejemplo que ilustra este principio es la forma en que se utiliza una función de puerto de acceso, como la seguridad del puerto. Lo que permite la seguridad de puerto en el conmutador de acceso permite restringir qué fotogramas se permiten entrante desde el cliente en un puerto de acceso basado en la dirección MAC en el marco de origen. Cuando está habilitado, puede resolver varios problemas: como evitar ciertos man-in-the-middle y DoS ataques de inundaciones, así como para mitigar contra bucles de capa 2 (spanning tree) que afectan a los puertos de acceso. Implementación de seguridad de puerto proporciona una comprobación de límites explícita sobre el número de dispositivos de final que debería ser conectada a un puerto de final. Cada red está diseñado para soportar un número específico de dispositivos en un puerto de borde. Mediante la implementación de una regla explícita que aplica ese comportamiento esperado, el diseño de la red logra un mayor grado de resistencia global al prevenir todos los posibles problemas que podrían ocurrir si miles de direcciones MAC de repente aparecieron en un puerto de borde. Por la ingeniería de la red para ambos lo que usted desea para hacer y le impiden hacer lo que no desea hacer, disminuye la probabilidad de algún evento inesperado de romper o interrumpir la red.

Como se ilustra en el ejemplo de seguridad del puerto, hay muchos casos donde las características de seguridad tradicionales y las características de calidad de servicio (QoS) pueden y deben utilizarse para la seguridad de la dirección y requisitos de QoS, sino también para mejorar la disponibilidad de la infraestructura de campus en su conjunto. El principio de la resistencia se extiende a la configuración de los protocolos de plano de control (tales como EIGRP, Rapid-PVTS + y UDLD), así como los mecanismos utilizados para proporcionar resiliencia nivel conmutador o dispositivo. La implementación específica de enrutamiento de Protocolo de resumen y el Kit de herramientas de árbol spanning (como Loopguard y Rootguard) son ejemplos de controles explícitos que pueden utilizarse para el control de las redes de campus de la manera de comportan en virtud de las operaciones normales y reaccionan ante eventos inesperados y esperados.

Resiliencia es el tercero de cuatro principios de diseño de campus fundacional. Igual que la forma en que implementamos jerarquía y modularidad son interdependientes mutuamente, la manera de lograr y aplicar resiliencia es también estrechamente asociada para el diseño general. Resiliencia agregar al diseño puede requerir el uso de nuevas características, pero a menudo es sólo cuestión de cómo elegimos implementar nuestra jerarquía y cómo nos configurar el nivel básico-2 y topologías Layer-3.

Flexibilidad

En la mayoría de los entornos de negocio de empresa, redes de campus universitarios ya no son nuevas adiciones a la red. En general, redes de campus universitarios han evolucionado a través de la generación de primera y segunda generación - ciclos y el ciclo de vida esperado para campus redes han aumentado considerablemente, de tres a cinco y en algunos casos, siete años. Al mismo tiempo, estas redes han convertido en más grandes y complejas, mientras que el entorno empresarial y sus requerimientos subyacentes de la comunicación continúan evolucionando. El resultado es que un creciente grado de adaptabilidad o flexibilidad debe permite diseños de red. La capacidad de modificar partes de la red, agregar nuevos servicios o aumentar la capacidad sin pasar por una actualización importante *elevadoras* son consideraciones clave para los diseños del campus de eficacia.

El diseño de jerárquico estructurado intrínsecamente proporciona un alto grado de flexibilidad ya que permite cambios por fases o graduales para cada módulo en la red bastante independientemente de los demás. Cambios en el núcleo de transporte pueden realizarse independientemente de los bloques de distribución. Cambios en el diseño o la capacidad de la capa de distribución pueden implementarse de forma gradual o incremental. Además, como parte del diseño general jerárquica, la introducción del módulo de bloque de servicios en la arquitectura está específicamente destinada para hacer frente a la necesidad de implementar servicios de forma controlada. Este diseño modular del diseño general también se aplica a la selección de dispositivos para rellenar cada una de las funciones en la arquitectura general. Como la esperanza de vida de un núcleo, distribución o aumentos de conmutador de acceso, es necesario tener en cuenta cómo cada uno será apoyar y permitir la evolución constante de las funciones necesarias para soportar los requerimientos cambiantes del negocio sin escala todo de sustitución de hardware.

Hay una serie de áreas clave donde es muy probable que redes evolucionará en los próximos años y los diseños existentes deben adaptarse a incorporar el grado apropiado de flexibilidad en sus diseños para adaptarse a estos cambios potenciales. Áreas clave para tener en cuenta las siguientes:

- *Flexibilidad de plano de control*: la capacidad para apoyar y permitir la migración entre enrutamiento múltiples, que abarcan el árbol y otros protocolos de control.
- *Reenvío de plano flexibilidad*: la capacidad para apoyar la introducción y el uso de IPv6 como requisito paralelo a lo largo del lado IPv4.
- *Flexibilidad de grupo de usuario*: la capacidad de virtualizar la red de reenvío de capacidades y los servicios dentro de la estructura de campus para apoyar los cambios en la estructura administrativa de la empresa. Esto podría implicar la adquisición, asociación, o la externalización de funciones del negocio.
- *Administración de tráfico y la flexibilidad de control*, comunicaciones unificadas, enfoques de negocios colaborativos y modelos de software continúan evolucionando — junto con una tendencia hacia un mayor crecimiento en los flujos de tráfico de peer-to-peer. Estos cambios fundamentales requieren diseños de campus que permiten la implementación de la seguridad, supervisión y solución de problemas de herramientas disponibles para apoyar estos nuevos patrones de tráfico.

- *Arquitectura de seguridad flexible*: la alta probabilidad de cambiar los patrones de tráfico y un continuo aumento de las amenazas de seguridad como desarrollan nuevos patrones de aplicaciones y comunicaciones requerirá una arquitectura de seguridad que pueda adaptarse a estas condiciones cambiantes.

La capacidad de realizar modificaciones evolutivas en cualquier campus es una negocio práctica y la necesidad operacional. Lo que asegura que la arquitectura general dará el grado óptimo de flexibilidad posible se asegurará de que futuras del negocio y requisitos de la tecnología será más fácil y más rentable para poner en práctica.

Servicios de campus

La arquitectura general del campus es más que el diseño jerárquico fundamental debatido en la arquitectura de campus y principios de diseño. Mientras que los principios jerárquicos son fundamentales para *Cómo* diseñar un campus no responden a las preguntas de underling acerca de lo que hace una red del campus. ¿Qué servicios deben proporciona a los usuarios finales y dispositivos? ¿Cuáles son los parámetros de esos servicios y las expectativas? ¿Qué funcionalidad deberá diseñarse en cada uno de los niveles jerárquicos? ¿Qué debe hacer una red del campus a fin de cumplir los requisitos técnicos y del negocio de la empresa? Un campus de lo que hace o debe proporcionar puede clasificarse en seis grupos:

- Alta disponibilidad sin-parar
- Acceso y servicios de movilidad
- Optimización de las aplicaciones y servicios de protección
- Servicios de virtualización
- Servicios de seguridad
- Operacionales y de servicios de gestión

En las secciones siguientes, se introduce cada uno de estos servicios o requerimientos de nivel de servicio. Explicaciones más detalladas sobre cada tema estará disponibles en los capítulos de diseño de campus específicos.

Alta disponibilidad sin-parar

En muchos casos, el requisito de servicio de principio de la red del campus es la disponibilidad de la red. La capacidad para conectar los dispositivos y para las aplicaciones funcionar depende de la disponibilidad del campus. Disponibilidad no es un requisito de nuevo y históricamente ha sido el requisito principal de servicio para la mayoría de campus de diseños. Las métricas de qué disponibilidad significa y los requisitos para cómo *disponible* la red han cambiado por el crecimiento en comunicaciones unificadas, vídeo de alta definición y la creciente dependencia general de la red para todos los procesos de negocio.

Disponibilidad de medición

Disponibilidad tradicionalmente se mide a través de una gran cantidad de métricas, incluyendo el porcentaje de tiempo de la red está disponible o el *número de nueves* — como cinco nueves — de disponibilidad. El cálculo de disponibilidad se basa en una función del *tiempo medio entre fallos* (MTBF) de los componentes de la red y el *tiempo promedio de reparación* (MTTR) — o cuánto tarda en recuperarse de un error. Vea la figura de 14.

La figura 14 Cálculo de disponibilidad

$$\text{Availability} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

MTBF = Mean Time Between Failure
MTTR = Mean Time To Repair

mejorar la disponibilidad se logra incrementando el MTBF (reducir la probabilidad de que algo romper) o disminuyendo el tiempo medio de reparación (reduce el tiempo para recuperarse de un error) o ambos. ¿En una red con un único dispositivo, esto es todo lo que necesitamos para examinar: cómo confiable es el dispositivo? Y ¿cuán rápido podemos nosotros arreglarlo si se rompe? En una red de más de un dispositivo, hay otros factores que influyen en la disponibilidad general y nuestras opciones de diseño.

Una red de campus generalmente se compone de varios dispositivos, conmutadores, y se calcula la probabilidad de que la red en su defecto (MTBF) de la red basada en el tiempo medio entre fallos de cada dispositivo y son redundantes si o no. En una red de tres conmutadores conectados en serie, con no redundancia, la red se romperá si cambia de cualquiera de los tres saltos. La red global MTBF es una función de la probabilidad es que se producirá un error en uno de los tres. En una red con switches redundantes o conmutadores en paralelo, la red sólo se romperá si ambos de los conmutadores redundantes fallan. Los cálculos para el sistema de tiempo medio entre fallos se basan en la probabilidad de que un interruptor en una red (serie) no redundante de saltos (figura 15), o ambos conmutadores en un salto de diseño (paralela) redundante (figura 16).

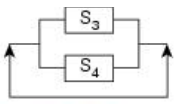
Figura 15 MTBF cálculo con conmutadores de serie

S_1, S_2 - Series Components

System is available when both components are available:

$$A_{series} = A_1 \times A_2$$

Figura 16 MTBF cálculo con conmutadores paralelos



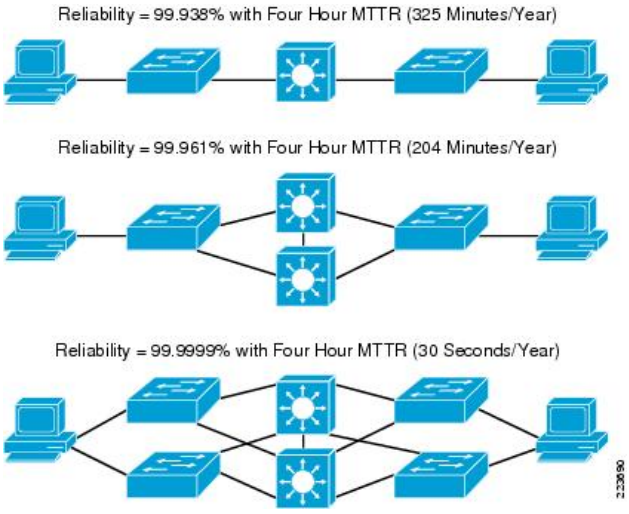
S_3, S_4 - Parallel Components

System is unavailable when both components are unavailable:

$$A_{parallel} = 1 - (1 - A_1) \times (1 - A_2)$$

Además de cambiar los cálculos de tiempo medio entre fallos, redundancia y cómo se utiliza redundancia en un diseño también afecta el tiempo medio de reparación para la red. Consulte figura 17. El tiempo para restaurar el servicio, flujos de datos, en la red se basa en el tiempo necesario para el dispositivo ha fallado que se va a reemplazar o la red recuperar los flujos de datos a través de una ruta redundante. El tiempo que toma cualquier equipo de operaciones para sustituir un dispositivo generalmente se mide en horas o días en lugar de en minutos o segundos y el impacto sobre la disponibilidad de la red puede ser importante si el grado apropiado de redundancia de dispositivo no está presente en el diseño.

La figura 17 Impacto de redundancia de la red sobre la confiabilidad de campus global



El otro comúnmente usa métrica para medir la disponibilidad es *defectos por millones* (DPM). Mientras que la probabilidad de falla de una red de medición y establecer el acuerdo de nivel de servicio (SLA) que es capaz de lograr un diseño específico son una herramienta útil, DPM adopta un enfoque diferente. Mide el impacto de defectos en el servicio desde la perspectiva del usuario final. A menudo es una mejor métrica para determinar la disponibilidad de la red porque refleja mejor la experiencia del usuario relativa a los efectos del evento. DPM se calcula en función de tener la total *minutos de usuario afectado* para cada evento, totales de los usuarios afectados y la duración del evento, en comparación con el número total de minutos de servicio durante el período de que se trate. Puede divide la suma de minutos de tiempo de inactividad de servicio por minutos de servicio total y multiplica por 1.000.000. Véase la figura de , 18.

Figura 18 Defectos por millón de cálculo

$$DPM = \frac{\Sigma(\#ofUsers\_Affected \times Outage\_Minutes)}{(\#Total\_Users \times Total\_Service\_Minutes)} \times 10^6$$

233827

DPM es útil, ya que es una medida de la disponibilidad observada y considera el impacto para el usuario final, así como la propia red. Agregar este elemento de la experiencia de usuario a la cuestión de la disponibilidad de campus es muy importante comprender y se está convirtiendo en una parte más importante de la cuestión de lo que hace que una red del campus o de alta disponibilidad sin interrupciones. Una red de *cinco nueves*, que ha sido considerada como el sello de diseño de la red de empresa excelente durante muchos años, se permite hasta cinco (5) minutos de interrupción o el tiempo de inactividad al año. Consulte la tabla de 3.

Tabla 3 Disponibilidad, DPM y tiempo de inactividad

Disponibilidad (porcentaje)	**DPM**	**El tiempo de inactividad/año (24 x 7 x 365)**		
99.000	10.000	3 Días	15 Horas	36 Minutos
99.500	5.000	1 Día	19 Horas	48 Minutos
99.900	1.000		8 Horas	46 Minutos
99.950	500		4 Horas	23 Minutos
99.990	100			53 Minutos
99,999	**10**			**5 Minutos**
99.9999	1			0,5 Minutos

Desde una perspectiva de las operaciones de red, alcanzar un máximo de cinco minutos de inactividad durante el año es un objetivo importante. Sin embargo, como una métrica única, no es suficiente caracterizar una red que cumplen los requisitos de disponibilidad de la corriente y la evolución de entornos empresariales. DPM toma en consideración la medición de la disponibilidad de la red desde la perspectiva del usuario (o aplicación) y es la herramienta valiosa para determinar si o no está cumpliendo el acuerdo de nivel de servicio de red. Sin embargo, no es una métrica suficiente bien. La métrica de tercera a considerar en el diseño de campus es la *máxima interrupción* que cualquier aplicación o secuencia de datos experimentarán durante un fallo de la red. Tiempo de recuperación de la red desde la perspectiva del usuario (o aplicación) es la tercera métrica de diseño críticas para tener en cuenta al diseñar una red del campus. Cinco minutos de interrupción experimentado en medio de un evento de críticos del negocio tiene un impacto significativo sobre la empresa.

Requisitos de comunicaciones unificadas

Prevén una alta disponibilidad en un diseño de campus requiere la consideración de los tres aspectos:

- ¿Qué SLA soporten el diseño (nueves cuántos)?

- ¿Es la red cumple el SLA (DPM)?
- ¿Cuál será el impacto de cualquier falla en las aplicaciones y la experiencia de usuario?

Los dos primeros son agregados métricas de la integridad operacional de una red del campus y se utilizan para determinar el nivel de fiabilidad de funcionamiento de la red. La tercera reflexión es una medida de interrupción del negocio: cómo perjudiciales para el negocio cualquier falla será. La elección de una métrica para los criterios de terceros ha cambiado con el tiempo como la naturaleza de las aplicaciones y la dependencia de la infraestructura de red ha cambiado.

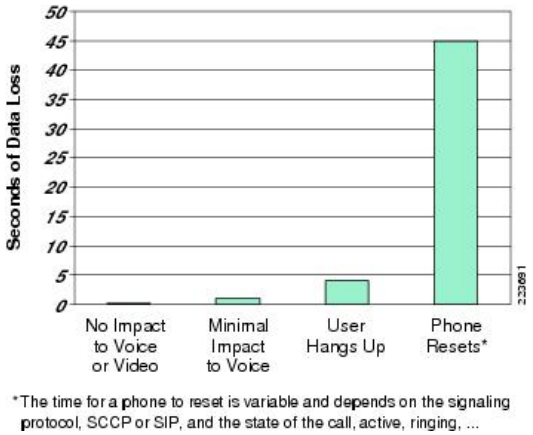
Como las empresas migran a VoIP y comunicaciones unificadas, lo que se considera aceptable disponibilidad debe también ser reevaluó. El límite superior para reconvergencia red aceptable, el tiempo medio de reparación, para una de las comunicaciones unificadas debe tener en cuenta varias métricas claves:

- ¿Con qué rapidez la red debe restaurar flujos de datos antes de la pérdida se convierte en disruptiva en una voz interactivo o un vídeo? ¿Cuándo se interrumpirá su conversación?
- ¿Con qué rapidez debe la red convergen y restaurar los flujos de datos antes de que alguien cuelga en una conversación activa debido a los muertos aire? ¿Cuánto tiempo alguien escuchará al teléfono si no oye nada? ¿Cuánto tiempo será antes de la red aparece rota?
- ¿Con qué rapidez debe convergen la red para evitar la llamada señalización fallas, pérdida de tono de marcado, restablecer desencadenados por la pérdida de conexión con el agente de llamada (como administrador de comunicaciones unificadas de Cisco, Cisco Unified SRST o Cisco Unified Communications Manager Express)?

Estas métricas contienen objetivo y elementos subjetivos. Además de definir cuando se producirá un error en las aplicaciones, también definir lo que es perjudicial para los empleados y los usuarios de la red, qué eventos interrumpirá su capacidad para realizar negocios y los eventos que significan un fracaso de la red. Como las comunicaciones basadas en la red se convierten en la norma para todos los aspectos de la vida personal y de negocio, la definición de métricas que describe una red *de trabajo* es cada vez más importante y más restrictiva.

Si bien las métricas para evaluar la evaluación subjetiva de fracaso son por definición subjetiva, tienen una base en los patrones comunes de patrones de comunicación humana. La cantidad de tiempo que una persona está dispuesta a escuchar al aire muertos antes de decidir que no la llamada (red), causando el usuario colgar — es variable, pero tiende a ser en el segundo intervalo de 3-a-6. La longitud de la pérdida de datos o portador de ruta en una secuencia RTP es mucho más estricta. Mientras que el oído humano puede detectar la pérdida de sonido en streaming de audio hasta 50 MS o menos, el intervalo promedio que resulte perjudicial para una conversación está más cerca de 200 MS. La capacidad para cubrir la pérdida de información fonética en una conversación y en el umbral para qué plazo de tiempo constituye una pausa en la intervención: señalización es turno para hablar de otra persona — son mucho más de lo que puede detectar el oído humano como sonido perdido. Pérdida de sonido para períodos de hasta un segundo se recuperan en el patrón de discurso normal relativamente fácil, pero más allá de se convierten en disruptivas para conversación y resultado en comunicación perdido o ha fallado. Véase figura 19.

Figura 19 Comparative medida de tiempo medio de reparación en comunicaciones unificadas



Un campus que puede restaurar secuencias multimedia RTP en menos tiempo que tarda en interrumpir una conversación de activos del negocio es tanto un objetivo de diseño en una empresa de comunicaciones unificadas habilitado como se reúne un destino de cinco nueves de disponibilidad.

Nota Voz y vídeo no son las únicas aplicaciones con requisitos estrictos de convergencia. Cotización de sistemas, la atención de la salud y otras aplicaciones en tiempo real podría tener como requerimientos estrictos o aún más estrictas para la velocidad de recuperación de la red. Voz se utiliza como una métrica para las guías de diseño de la empresa Cisco porque se está convirtiendo en una aplicación estándar en la mayoría de las redes empresariales y proporciona un objetivo común que deben cumplir todos los diseños como requisito mínimo.

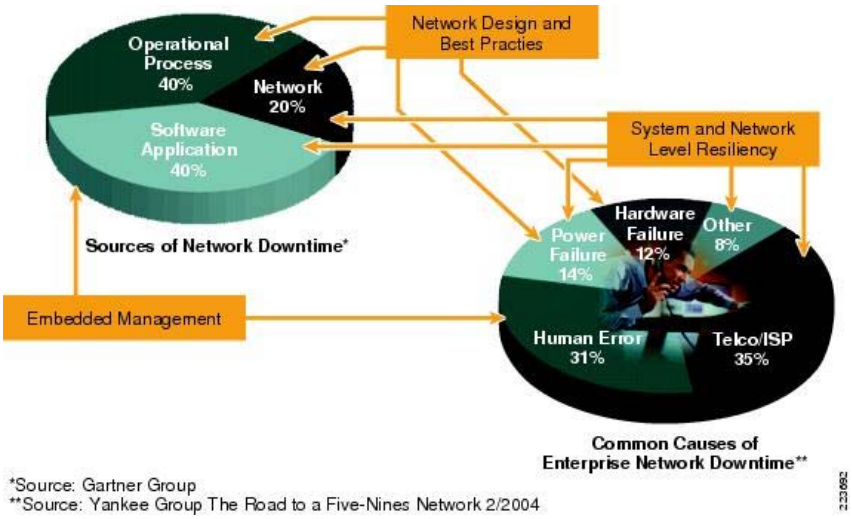
Herramientas y enfoques para alta disponibilidad de campus

El enfoque adoptado en la Guía de diseño de ESE campus para resolver los problemas de garantizar la cinco nueves de disponibilidad y ofrecer a los tiempos de recuperación requeridos por un campus habilitados para comunicaciones unificadas se basa en abordando el problema de servicio de alta disponibilidad desde tres perspectivas:

- Red resiliencia
- Dispositivo resiliencia
- Resiliencia operacional

Este enfoque se basa en un análisis de los principales factores que contribuyen de inactividad de la red (como se muestra en la figura 20) y mediante el uso de los principios de la jerarquía, resiliencia y modularidad, combinada con las capacidades de la conmutación de la familia de Catalyst de Cisco para definir un conjunto de recomendaciones de diseño.

Figura 20 Causas comunes de red tiempo de inactividad



Las secciones siguientes proporcionan breves descripciones de las funciones claves necesarias y consideraciones de diseño al abordar cada uno de estos requisitos de tres resiliencia.

Red resiliencia

Red resiliencia preocupa en gran medida con cómo el diseño general implementa topología redundancia, vínculos redundantes y dispositivos, y cómo los protocolos de plano de control (como EIGRP, OSPF, PIM y STP) configurados para operar en ese diseño. El uso de redundancia física es una parte esencial de asegurar la disponibilidad de la red global. En caso de un componente falla, tener un componente redundante significa que la red global puede seguir funcionando. Las capacidades de control de plano del campus de proporcionan la capacidad de administrar la forma en que se aprovecha la redundancia física, la carga de red equilibra el tráfico, la red converge y opera la red. Las recomendaciones detalladas de cómo configurar de manera óptima los diversos protocolos plano de control están cubiertas en la Guía de diseño de campus específicos, pero se pueden aplicar los siguientes principios básicos en todas las situaciones:

- Siempre que sea posible, aprovechar la capacidad del hardware conmutador para proporcionar el mecanismo principal de detección y recuperación de errores en la red (por ejemplo, uso EtherChannel Multi-Chassis, Equal Cost multi-path recuperación para la recuperación de errores). Esto garantiza un rápido y una recuperación de errores más determinista.
- Aplicar un enfoque de *defensa en profundidad* a los mecanismos de detección y recuperación de fracaso. Un ejemplo de esto está configurando el Protocolo de detección de vínculo unidireccional (UDLD) que utiliza una capa 2 keep-alive para probar que los vínculos de conmutador al switch están conectados y operando correctamente y actúa como una copia de seguridad de las capacidades de detección de vínculo unidireccional de capa-1 nativas había proporcionada por 3z y 802.3ae las normas.
- Asegúrese de que el diseño es self-stabilizing. Utilizar una combinación de diseño modular de plano de control (como ruta resumen) y software para que se aíslan errores en su impacto y ese plano de control impide que las condiciones de inundación o thrashing derivados de regulación (como la atenuación de la interfaz IP).

Estos principios se pretenden ser una parte complementaria de la general estructurado diseño modular enfoque a la arquitectura de campus y servir principalmente para reforzar las prácticas de buen diseño resistente.

Dispositivo resiliencia

Mientras que una topología de red redundantes, con vínculos redundantes y conmutadores, puede ayudar a enfrentar muchos desafíos de disponibilidad de campus global, proporciona redundancia de por sí sola no comprende una solución completa. Cada diseño de campus tendrá puntos únicos de falla y la disponibilidad general de la red podría depender de la disponibilidad de un solo dispositivo. Un buen ejemplo de ello es la capa de acceso. Cada modificador de acceso representa un punto único de fallo para todos los dispositivos conectados. Asegurar la disponibilidad de los servicios de red depende a menudo la resistencia de los dispositivos individuales.

Dispositivo resiliencia, como ocurre con la resistencia de la red, se logra a través de una combinación del nivel adecuado de redundancia física, endurecimiento de dispositivo y el apoyo a funciones de software. Los estudios indican que los errores más comunes en las redes de campus están asociados con fallas de la capa-1 - de componentes como los vínculos de poder, ventiladores y fibra. El uso de fibra diversas rutas con vínculos redundantes y tarjetas de línea en combinación con fuentes de alimentación totalmente redundante y circuitos de potencia, son los aspectos más críticos de la resiliencia de dispositivo. El uso de fuentes de alimentación redundantes se vuelve aún más crítico en los conmutadores de acceso con la introducción de Power over Ethernet (PoE) dispositivos tales como teléfonos IP. Varios dispositivos dependen ahora de la disponibilidad del modificador de acceso y su capacidad para mantener el nivel de potencia para todos los dispositivos conectados final. Después de fallas en físicas, la causa más común de interrupción en el dispositivo está a menudo relacionada con el fracaso de supervisor hardware o software. Las interrupciones de la red debido a la pérdida o el restablecimiento de un dispositivo debido a un fallo de supervisor pueden resolverse mediante el uso de redundancia de supervisor. Los switches Cisco Catalyst proporciona dos mecanismos para alcanzar este nivel de redundancia adicional:

- Con estado de cambio y el reenvío de non-stop (NSF/SSO) de Cisco Catalyst 4500 y Cisco Catalyst 6500
- Stackwise y Stackwise-Plus de Cisco Catalyst 3750 y Cisco Catalyst 3750E

Ambos de estos mecanismos proporcionan para una copia de seguridad activa caliente para el plano de tejido y control de conmutación: asegurar que tanto el reenvío de datos y red plano de control (con protocolos como EIGRP, OSPF y STP) sin problemas recuperan (pérdida de tráfico de fracciones de segundos) durante cualquier forma de bloqueo de hardware software o supervisor.

Nota Para obtener información adicional sobre la mejora de la resistencia de dispositivo en el diseño de campus consulte el capítulo de campus redundante de supervisor de diseño.

Además de garantizar que cada uno de los conmutadores en el campus tiene el nivel necesario de redundancia de software y hardware físicos, también es importante proporcionar la protección adecuada para el plano de control de conmutadores. Las velocidades de varios gigabits de las redes modernas de conmutación pueden sobrecargar la capacidad de cualquier CPU. Si bien se reenvía la mayor parte del tráfico en la red del campus en el hardware y la CPU debe sólo deba plano de control de proceso y otro tráfico de administración de sistemas, existe la posibilidad bajo ciertas condiciones de error (o en caso de un ataque DoS malintencionado) para el volumen y tipo de tráfico reenviado a abrumar a la CPU. En tal caso, a menos que la arquitectura de hardware de conmutador adecuado y los controles en el lugar, la red en su conjunto puede fallar debido a la CPU no poder procesar plano críticos de control (por ejemplo, EIGRP y STP) y el tráfico de administración (como Telnet y SSH). El diseño de campus ocupa de este tipo de problema a través de los tres enfoques:

- Limitar el plano de control de la línea de base y la carga de CPU en cada conmutador a través del diseño modular, así como para proporcionar control plano aislamiento entre los módulos en el caso de incumplimiento se produce.
- Reducir la probabilidad de un evento de las inundaciones a través de la reducción en el ámbito de la topología de capa 2 y el uso de las características de kit de herramientas de árbol spanning para endurecer el diseño de árbol spanning.
- Aproveche las características de protección de plano de control (CoPP) de los conmutadores Catalyst para limitar y priorizar el tráfico reenviado a cada conmutador CPU y mecanismos de protección de hardware de CPU.

La combinación de los tres elementos (física redundancia fallas física dirección capa-1, supervisor de redundancia para prever un plano de non-stop reenvío (datos) y el endurecimiento de la placa de control a través de la combinación de buenas capacidades de protección de CPU de diseño y hardware) son los elementos clave para garantizar la disponibilidad de los modificadores de sí mismos y tiempo de actividad óptima para el campus en su conjunto.

Resiliencia operacional

El diseño de la red para recuperarse de los sucesos de error es sólo un aspecto de la arquitectura de non-stop de campus global. Entornos de negocios continúan avanzar hacia la necesidad de 7 x 24 x 365 disponibilidad.

Es cada vez más creciente difícil encontrar una *ventana de cambiar*, o una hora cuando la red puede ser apagada para el mantenimiento con la globalización de las empresas, el deseo de*siempre en* las comunicaciones y el movimiento de los sistemas de aplicación monolítica basada en mainframe para web y sistemas basados en comunicaciones unificadas.

El campus — que podrían formar o ser parte de la columna vertebral de la red de la empresa: debe ser diseñado para permitir procesos operacionales estándar, cambios de configuración, actualizaciones de software y hardware sin interrumpir los servicios de red.

La capacidad de hacer cambios, actualizar el software y reemplazar o actualización de hardware en la producción es posible debido a la aplicación de redundancia de red y del dispositivo. Al tener dos rutas activas a través de conmutadores redundantes diseñados para convergen en plazos de fracciones de segundos, es posible programar una cita de interrupción en uno de los elementos de la red y le permiten ser actualizado y, a continuación, traído en servicio con una interrupción mínima de la red como un todo. La posibilidad de actualizar los dispositivos individuales sin tomarlos fuera de servicio se basan asimismo en la existencia de redundancia de los componentes internos (como con las fuentes de alimentación y supervisores) complementado con las capacidades de software de sistema. Existen dos mecanismos principales para actualizar el software en el lugar en el campus:

- Imagen completa docente software upgrade (ISSU) sobre el Cisco Catalyst 4500 aprovecha dos supervisores para permitir un completo, en el lugar Cisco IOS actualizar. Pasar de 12.2 (37) SG1 a 12,2 (40) SG, como un ejemplo. Esto aprovecha las capacidades de NSF/SSO del conmutador y proporciona por menos de 200 MS de pérdida de tráfico durante un lleno de Cisco IOS actualizar.
- Subsistema de ISSU sobre el Cisco Catalyst 6500 aprovecha Cisco IOS modularidad y la capacidad de proporciona para reemplazar los componentes individuales de Cisco IOS (como los protocolos de enrutamiento) sin afectar el reenvío de tráfico u otros componentes en el sistema.

Tener la capacidad de operar el campus como un sistema de non-stop depende de las capacidades adecuadas está diseñado en desde el principio. Redundancia nivel de red y del dispositivo, junto con los mecanismos de control de software necesario, garantizan la recuperación rápida y controlada de todos los flujos de datos tras cualquier fallo de la red, ofreciendo al mismo tiempo la capacidad de administrar de manera proactiva la infraestructura de non-stop.

Acceso y servicios de movilidad

De todos los factores que influyen en cambio en la arquitectura del campus, la expectativa creciente dentro de la comunidad empresarial para un entorno de trabajo flexibles: proporcionar en cualquier momento y en cualquier lugar conectividad de red: es uno de los más visibles. Este requisito de mayor movilidad y flexibilidad no es nuevo, pero se está convirtiendo en una prioridad más alta que requiere una reevaluación de cómo el acceso a la red y servicios de acceso de red están diseñados a la arquitectura general del campus. El crecimiento de la demanda de mayor movilidad — tanto cableadas e inalámbricas: puede ser caracterizada por observar tres escasamente relacionados con las tendencias:

- El crecimiento en el ordenador portátil y otros dispositivos portátiles como el negocio principal herramienta en lugar de equipos de sobremesa.
- El crecimiento del número de socios en el sitio, contratistas y otros invitados mediante los servicios del campus. Estos usuarios aprovechará más a menudo una combinación de su propio equipo informático: su empresa prestados normalmente portátil — y equipos, teléfonos, impresoras y similares proporcionados por la empresa de host.
- El crecimiento del número y tipo de dispositivos conectados a la red del campus, tales como teléfonos VoIP, cámaras de vídeo de escritorio y cámaras de seguridad.

El único subproceso que reúne todos los requisitos es la necesidad de mover dispositivos dentro de las instalaciones y tenerlas asociados con las políticas de red correcto y servicios, dondequiera que estén conectados de manera rentable. Para lograr este nivel de la movilidad de acceso, la red del campus deberá garantizar que los siguientes servicios de acceso se integren en la arquitectura de campus global:

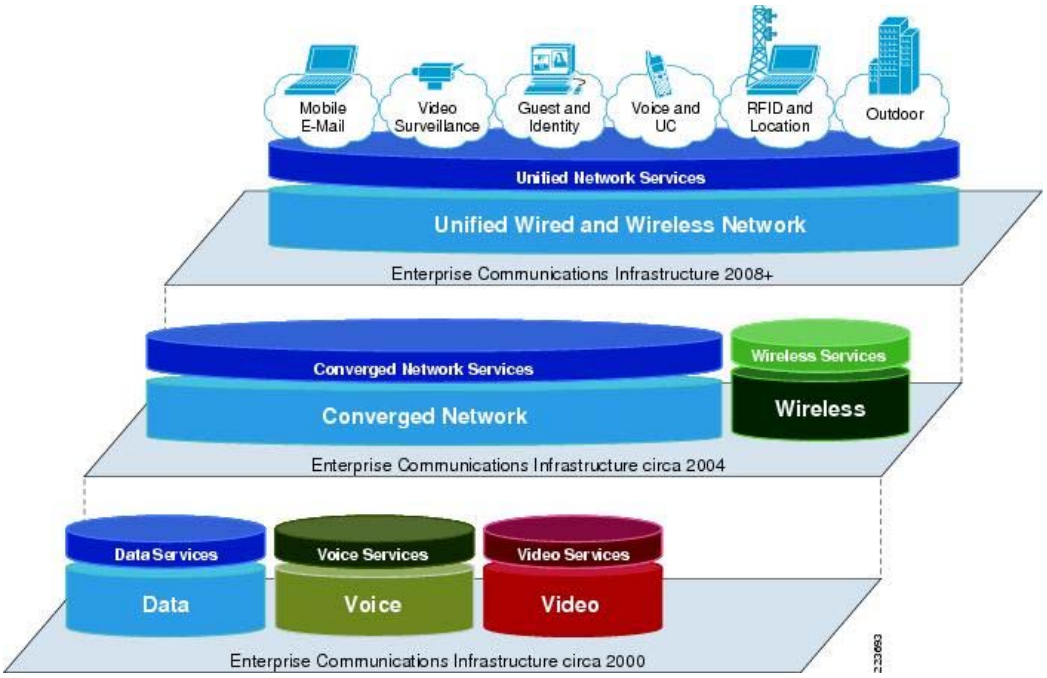
- Capacidad de adjuntar a la red y estar asociada con, físicamente o negociar los servicios de red correctos capa-1 y capa 2 — PoE, vincular la velocidad y dúplex, subred (VLAN o SSID)
- Capacidad de proporcionar identificación del dispositivo y, cuando sea necesario, realizar la autenticación de acceso de red
- Capacidad para la red aplicar las directivas de QoS para el flujo de tráfico, dispositivo o usuario específico (como secuencias de RTP)
- Capacidad para la red aplicar las políticas de seguridad deseado para el usuario específico o un dispositivo
- Capacidad para la red y el dispositivo para determinar y, a continuación, registrar la ubicación del dispositivo adjuntar
- Capacidad para el dispositivo negociar y registrar los parámetros de estación final correcta (tales como DHCP), así como para registrarse para cualquier otro servicio de red necesaria (como el registro para los servicios de comunicaciones unificadas presencia y llamada agente)

El desafío para el arquitecto del campus consiste en determinar cómo implementar un diseño que satisface esta amplia variedad de requisitos, la necesidad de diversos niveles de movilidad, la necesidad de un entorno de las operaciones rentables y flexibles, sin dejar de ser capaz de proporcionar el equilibrio adecuado de seguridad y disponibilidad espera que en los entornos más tradicionales, fijo-configuración.

Diseño de campus con cable y Wireless convergentes

Un enfoque que se utiliza para tratar esta creciente necesidad de acceso a la red más dinámico y flexible es la introducción de funciones inalámbricas 802.11 en el campus. Mientras que 802.11 pueden y ofrece para los móviles más fácil y puede proporcionar un método eficaz para mejorar el acceso a la red, la aplicación de tecnología inalámbrica debe integrarse en una arquitectura de campus general a fin de un conjunto coherente de los servicios y facilidad de movimiento para dispositivos inalámbricos móviles y dispositivos de red cableados altamente disponibles. La integración de métodos de acceso cableadas e inalámbricas en una arquitectura de campus común es sólo la última fase de la convergencia de la red. Como ilustrado en figura 21 (movimiento desde la parte inferior a la parte superior) la red de la empresa ha pasado por varias fases de integración o de convergencia.

Figura 21 Evolución de las redes convergentes campus



Hay dos factores clave de motivación que ha sido impulsando el proceso de convergencia de la red. La primera es la capacidad para una red convergente reducir los costes operativos de la general de la empresa mediante el aprovechamiento común sistemas (lo que es más importante) una común equipos de apoyo operacional y procesos. El segundo, y igualmente importante, controlador de convergencia es la ventaja de negocio cuando adquirida anteriormente aislados los procesos del negocio pueden ser más estrechamente integrados. La convergencia de las redes de voz, vídeo y datos (como ejemplo) ha permitido el desarrollo de sistemas de comunicaciones unificadas que están permitiendo a las empresas más eficientemente aprovechan todas las herramientas de comunicación interpersonales diferentes. Esta próxima fase de integración, combinadas con cable y wireless en un campus convergente, está motivada por las mismas razones. Sistemas inalámbricos que se pueden inicialmente han implementado como soluciones de casos aisladas o especiales ahora están siendo más estrechamente integradas en la arquitectura de campus global en muchos casos para proporcionar a los ahorros de costos operacionales. Aprovechar los sistemas de back-end de autenticación común, los clientes de escritorio, servicios de seguridad comunes y similares, junto con el uso de procesos comunes de apoyo: puede resultar en un entorno operativo más eficiente y eficaz. Justo como lo que es importante, la capacidad de proporcionar la eficiencia del negocio por poder mover sin problemas un dispositivo entre entornos cableadas e inalámbricas y para proporcionar para la colaboración y servicios comunes entre dispositivos independientes de tipo de conectividad de acceso físico subyacente es un requisito clave para esta próxima fase de diseño convergente.

Como una parte del proceso de desarrollo de la general converge con cable y arquitectura de acceso inalámbrico, es importante comprender que la unidad para proporcionar mayor movilidad debe ser equilibrada con la necesidad de apoyar las aplicaciones de misión crítica. Actualmente, todavía hay diferencias en las propiedades y capacidades de acceso de los cableadas e inalámbrica tecnologías que deben analizarse al decidir los dispositivos que debe utilizar con cable, que debe utilizar inalámbrica, y que necesitan la capacidad de mover hacia atrás y hacia adelante basándose en los requerimientos cambiantes. La matriz de decisión que se utiliza para determinar cuando un dispositivo debe configurarse para utilizar el acceso a red cableada versus acceso inalámbrico tiene una serie de factores específicos, pero transforma esencialmente hacia abajo en conjunto una cuestión de donde se sienta un dispositivo y sus requisitos de aplicación en un espectro de requerimiento de nivel de servicio estricta frente a la facilidad-de-movilidad. Consulte figura 22.

La figura 22 Wired frente a claves de la decisión de Wireless

Una de las principales diferencias entre los entornos con cables e inalámbricos es principalmente una función de las diferencias entre los medios de comunicación compartido y dedicado. El puerto de acceso por cable es un recurso de dúplex completo conmutado con recursos de hardware dedicado proporcionar los servicios de acceso (QoS, seguridad) para cada cliente. Los medios de comunicación inalámbrica son un recurso compartido que aprovecha los protocolos de arbitraje para asignar uso justo de los medios de comunicación compartida. El resultado de esta diferencia básica es que mientras que proporciona acceso inalámbrico para un entorno altamente flexible que permite transparente móviles en todo el campus sufre el riesgo de que el servicio de red se degradará bajo condiciones extremas y no siempre será capaz de garantizar los requerimientos de nivel de servicio de red. Puertos de red cableadas proporcionan garantías mucho más fiables para QoS (vibración, latencia), paquete confiabilidad (multidifusión) y ofrecen mucho mayor capacidad y fundamentalmente más aislamiento para problemas de la capa-1 y nivel-2. Sin embargo, un puerto de red cableado es un recurso de ubicación fija. Tabla 4 proporciona un desglose de algunos criterios que se pueden utilizar para evaluar el equilibrio entre red cableadas frente a acceso inalámbrico de decisión.

Tabla 4 comparación de Wired frente a Wireless soporte de los requerimientos de aplicación de

	Con cable	Tecnología inalámbrica
Disponibilidad	Ethernet conmutada prevé inherente de la capa 1 fallas aislamiento y cuando se felicitó por capacidades en los conmutadores Catalyst actualmente proporciona capa de aislamiento de fallas y protección de los DoS 2. [1]	Los 5 GHz WLAN sistemas modernos con administración centralizada de radio proporcionan varias capas de protección contra interferencias de radio. Aunque todos los medios de comunicación inalámbricas es susceptibles a voluntaria o involuntariamente DoS eventos (radio

		interferencia, interferencia de RF) el uso de diseños de WLAN de gestión centralizada de radio ofrece soluciones para enfrentar estos desafíos [1].
QoS	Ethernet conmutada proporciona varias colas de hardware dedicado, incluyendo una cola de prioridad estricta para cada puerto proporcionar la capacidad de soportar garantizan las directivas de QoS. Adicionales por puerto por VLAN características como policiers proporcionar tráfico granular marcado y el control de tráfico y la protección contra misbehaving clientes.	Mejoras para QoS WLAN definidos por el 802.11e normas proporcionan la capacidad para las estaciones de habilitados para QoS tener la capacidad para solicitar los parámetros de transmisión específicos requeridos para satisfacer los estrictos requisitos de política de QoS (velocidad de datos, vibraciones, etc.). Actualmente la mayoría de las implementaciones de WLAN no admiten una 802.11e completa aplicación y pueden sufrir de la degradación de QoS bajo cargas de tráfico muy alto.
Multidifusión	Los precios de error de bit (BER) extremadamente bajo de fibra y cobre enlaces combinado con colas de hardware dedicado garantizar una probabilidad muy baja de descartar el tráfico de multidifusión y, por lo tanto, una muy alta probabilidad de entrega garantizada para que el tráfico de multidifusión. (Tráfico de multidifusión es UDP base y no tiene capacidades inherentes re-transmission. La capacidad de forma fiable garantiza la entrega de datos de multidifusión es dependiente de la capacidad de la red para prevenir caídas de paquetes).	Entornos de LAN inalámbricas experimentan una tasa BER superior a una red cableada comparable y no prevén la entrega reconocida de multidifusión datos entre el punto de acceso y el cliente. Mientras que los entornos de WLAN admiten la transmisión de tráfico de multidifusión no pueden satisfacer las necesidades de alto volumen pérdida sensible multidifusión aplicaciones (Nota: tráfico de unidifusión 802.11 utiliza las transmisiones reconocidas para lograr una confiabilidad similar para el tráfico de unidifusión con redes cableadas incluso con la mayor BER inherente.)
Control de tráfico de peer to Peer	Sí, por puerto de ACL y capacidades de aislamiento de PVLAN permiten segmentación de tráfico a nivel de dispositivo	Sí, se puede bloquear el tráfico de peer to peer por el sistema WLAN, en el nivel de dispositivo.
Autenticación	Autenticación de cliente (802.1X x) se admite en un entorno conmutado pero tiende a ser una tecnología de complemento a un previamente existente madurar entorno y puede resultar de tener un más complicado implementación que en un entorno inalámbrico equivalente.	Protocolos de autenticación de cliente están integrados en las normas WLAN y incorporados a los clientes existentes de estación final. Políticas de autenticación de cliente consistente son la norma para diseños inalámbricas.
Ubicación	Ubicación según los servicios son una tecnología de complemento a un entorno maduro previamente existente.	Ubicación basa servicios integrados en los sistemas actuales de WLAN.

[1] Capa 3 DoS protección es común a ambos entornos, como se trata de una propiedad de la infraestructura conmutada compartida

Es razonable suponer que la mayoría de los entornos campus empresa seguirá tienen variaciones en los requerimientos de aplicación del negocio y necesitará una combinación de acceso tanto cableada e inalámbrica en los próximos años. Entornos ni inalámbricas como cableadas será únicamente suficientes para hacer frente a todos los requisitos de negocio. El desafío para el Diseñador de la red es implementar una solución de campus integrada que proporciona los requisitos de servicio óptimo para todos los dispositivos basados en los principios de la red convergente, mientras que todavía proporcionar un conjunto común de la línea de base de los servicios de red y lo que permite operaciones unificadas y gestión.

Servicios de acceso campus

La capacidad de negociar los parámetros de configuración y la configuración de dispositivos de borde y la infraestructura de red es una central de la propiedad de la capa de acceso del campus. Tradicionalmente, diseños, campus o centro de datos de conmutación, todo parecía fundamentalmente similar. Consistió en conectividad Ethernet básica con el número adecuado de los puertos de acceso y la capacidad general de la red. Como han evolucionado tanto en el centro de datos y en los entornos de campus, los diseños y requisitos del sistema se han convertido en más especializados y divergentes. Es un área donde es más evidente en la capa de acceso. La capa de acceso a los campus soporta múltiples tipos de dispositivos, incluyendo teléfonos, AP, las cámaras de vídeo y portátiles, con cada uno que requieren servicios específicos y políticas. Se trata de un ajuste totalmente diferente desde el centro de datos — con sus servidores blade alta densidad, clústeres y sistemas de servidor virtual. PoE, autenticación de cliente, QoS dinámico y servicios de seguridad para apoyar una fuerza cada vez más móvil obras son requisitos en la capa de acceso a los campus que distinguen de ambos legado de conmutación entornos y las necesidades específicas de los centros de datos.

Mira cómo este conjunto de servicios de acceso evolucionado y sigue evolucionando, resulta útil entender cómo está cambiando la naturaleza de la capa de acceso. DHCP fue el primer mecanismo para proporcionar la configuración de red de dispositivos de borde dinámico y facilitar la circulación de dispositivos físicos a lo largo de la red. Negociación dinámica de los movimientos de configuración aliviado de pila IP correctos agrega y cambia de ordenadores, impresoras y otros dispositivos. La migración a VoIP y la capacidad de teléfonos negociar dinámicamente requerimientos de servicio con la red prevista otro importante paso en este movimiento a la movilidad del usuario mayor. Además de aprovechar la IP dinámica dispositivos VoIP de configuración también aprovechan mecanismos de registro de servicio dinámico (SCCP registro con Cisco Unified Communications Manager), así como la negociación de servicios de red dinámica. La capacidad de los teléfonos para negociar los requisitos de energía, PoE, así como parámetros de QoS, topología y seguridad del puerto de borde previstas una capacidad de plug-and-play bastante sofisticada. Protocolo de descubrimiento de Cisco (CDP) proporciona la capacidad para el dispositivo de final, tal un teléfono IP, para identificarse a sí mismo a la red y para la red y el teléfono para negociar los parámetros de configuración. Un teléfono IP identifica (a través de CDP) la VLAN es necesario utilizar para que el tráfico de voz y cómo observación el CoS bits en el tráfico recibido desde el PC conectado. Asimismo el conmutador identificará los requisitos específicos de energía, así como el ajustado correctamente la configuración del puerto QoS basada en la presencia de un teléfono en el puerto de borde. Las recientes mejoras a este proceso de negociación dinámico — que requieren que un teléfono negociar los parámetros PoE y CDP correctos antes de que se asigne a la voz VLAN — son mejoras adicionales de proporcionar un mayor grado de confianza y seguridad a este proceso de negociación dinámico.

Otra tendencia que se deben tener en cuenta es que la detección de red y capacidades de configuración de CDP se que se complementan con la adición de la IEEE LLDP y protocolos LLDP-MED. LLDP y LLDP-MED complementan y superponen la funcionalidad proporcionada por CDP, pero con una serie de diferencias. LLDP no prevea CDP v2 características, tales como la negociación de poder bidireccional entre el dispositivo de final y el conmutador necesario que se puede utilizar para reducir el total de energía asignación y el consumo en entornos de PoE. En la mayoría de las redes de campus, es razonable esperar que las capacidades de CDP y LLDP/LLDP-MED tendrá que ser activada y compatible con todos los puertos de conmutador de acceso. El propósito de CDP y LLDP es facilitar el funcionamiento y configuración desafíos asociados con el traslado de dispositivos. A medida que la comunidad de usuarios finales se vuelve cada vez más móvil, será necesario para algunos prolongado período de tiempo para garantizar que cualquier dispositivo pueda asociar a cualquier puerto en el campus y recibir la configuración de red apropiada de acceso y servicios: si un dispositivo admite CDP, LLDP o ambos.

La introducción de 802.1 X como un método de autenticación para usuarios y dispositivos es una parte de la siguiente fase de aprovisionamiento de dinámicas de acceso. Además de proporcionar autenticación fuerte, 802.1 X también puede utilizarse como un medio para configurar aún más los servicios de red, VLAN asignación, QoS y las políticas ACL del puerto. La asignación de directiva X 802.1 ya no sólo se basa en valores predeterminados globales para cada tipo de dispositivo, como en el caso de un teléfono IP, sino en los requerimientos específicos de dispositivo o usuario. Inicial de las implementaciones de 802.1 X en el campus a menudo resultó difícil debido principalmente a los desafíos en la integración de un 20-plus año legado de dispositivos y sistemas operativos que existen en el entorno de red cableado. La mayoría legado redes cableada nunca había sido diseñado o implementado con autenticación de red en mente. Las características más recientes, como derivación de autenticación de MAC (MAB), autenticación Web y las capacidades de autenticación abierta introducidas en los conmutadores Catalyst de Cisco proporcionará la capacidad para enfrentar estos desafíos. Con el tiempo, un sistema de autenticación para ambos con cable y wireless común — y más importante aún dispositivos mover entre dominios de acceso con cable e inalámbricos, se convertirá en el modelo de implementación común. Esta unificación de las capacidades cableadas e inalámbricas continuará como cableada acceso comienza la adopción de normas 802.1ae y 802.1af, que proporcionará la autenticación y cifrado entre el punto final y el puerto de acceso: apoyo a la misma, por lo tanto, los servicios como disponible con 802. 11i inalámbrica hoy.

El uso de servicios de localización unificado es otro aspecto de la tendencia de integración de servicios de red inalámbrica y con cables. Servicios de localización resolvían una serie de desafíos asociados con entornos de red dinámicos. La capacidad de ubicar un dispositivo para ayudar en la resolución del problema es más importante cuando el dispositivo tiene la capacidad de moverse a lo largo de la red con ningún proceso de control de cambio asociada. Como puntos finales habilitados para comunicaciones unificadas mover a la red, el proceso de determinar qué políticas de control de admisión de llamada para aplicar y qué códec, puerta de enlace, o recursos del plan de mediano plazo para utilizar pueden llegar a ser extremadamente difícil de administrar sin algún tipo de información de ubicación dinámica reemplazando la configuración de recurso estático.

Optimización de las aplicaciones y servicios de protección

La red del campus, por lo general, proporciona la máxima capacidad y la menor latencia de cualquier parte de la red de la empresa. Determinar si o no los mecanismos de QoS — y la asignación de prioridades de tráfico y la protección que proporcionan — son necesarias en el campus a menudo ha sido un tema de debate para red planers. Experiencias con problemas inesperados, como gusanos de Internet y otros eventos similares sin embargo han convencido a mayoría ingenieros de red que no es seguro asumir que las aplicaciones de misión crítica siempre recibirá el servicio que requieren sin las capacidades de QoS correctas en el lugar, incluso con toda la capacidad en el mundo.

Un número de otros factores también está afectando la capacidad de redes para soportar los requerimientos del negocio de empresa:

- La introducción de 10 Gigabit enlaces y más avanzados algoritmos de control de flujo TCP están creando mayores ráfagas de tráfico y discrepancias de velocidad potencial aún mayores entre los dispositivos de acceso y el núcleo de la red: impulsan la necesidad de las colas más grandes.
- El aumento de la peer-to-peer tráfico y la sobrecarga de los puertos conocidos con varios tipos de tráfico y la aplicación agregaron otro conjunto de desafíos. Las aplicaciones de enmascaramiento como web tráfico y múltiples aplicaciones con requerimientos de servicio diferentes utilizando todos los puertos HTTP mismos son ejemplos de puerto de sobrecarga.
- Flujos de tráfico dentro de las instalaciones son cada vez más compleja y diversa. La capacidad de predecir la ubicación de los puntos de congestión se vuelve más difícil como patrones de flujo de datos son capaces de migrar mientras dinámicas sesiones peer-to-peer ir y venir de la red.
- La capacidad de identificar la crítica frente a tráfico no crítico en función de un número de puerto TCP o UDP es casi imposible cuando un gran número de procesos de negocios comparte común aplicación web front-end. Se convierte en aún más difícil encontrar aplicaciones no deseadas o desconocidas cuando esas aplicaciones se utiliza una variedad de números de puerto se han escrito y son capaces de enmascararse como tráfico HTTP en el puerto TCP 80 mientras buscaba dinámicamente el acceso a través de los cortafuegos corporativos.

Todo esto está ocurriendo simultáneamente como acelera la migración a las comunicaciones unificadas y más voz y interactivo de alta definición vídeo se añaden a las redes de la empresa.

Principios de diseño de QoS Campus de

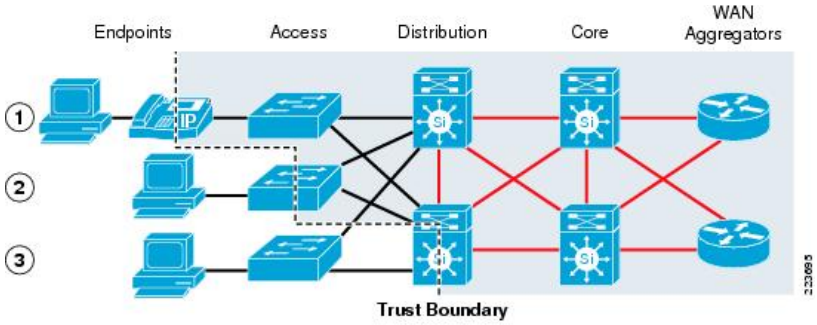
Al considerar los requisitos para la optimización y la protección de las aplicaciones y flujos de tráfico en el campus, es esencial para comprender qué herramientas de QoS están disponibles y cómo utilizar. Además de la cola es necesarios en todos cambie enlaces en todo el campus, clasificación, marcado y policiales son importantes funciones de QoS que se realizan de forma óptima en la red del campus en la capa de acceso.

Tres principios de diseño de QoS son importantes al implementar las directivas de QoS campus:

- Clasificar y marcar las aplicaciones como cerca de sus fuentes como sea posible desde el punto de vista técnico y administrativo. Este principio promueve end-to-end diferenciados Services/per-Hop comportamientos.
- Flujos de tráfico no deseado de la policía lo más cerca de sus fuentes como sea posible. Esto sucede especialmente cuando el tráfico no deseado es el resultado de DoS o los ataques del gusano.
- Siempre realizar funciones de QoS en hardware, en lugar de software cuando existe una opción.

Lo que permite la clasificación, el marcado y capacidades en el acceso o el borde de la red de vigilancia establece un límite de confianza de QoS. El límite de confianza es el punto de la red donde todo el tráfico más allá de ese punto ha sido correctamente identificado y marcados con la clase correcta de servicio (CoS) / diferenciada servicios código apunta marcas (DSCP). Define la parte de la red en la que fluye de aplicación está protegidos y las partes en el que no sean. Define el límite de confianza lo más cerca de la periferia de la red como sea posible significa *todos* de los flujos de aplicación: llamadas de voz incluso persona a persona entre colegas en la misma zona están protegidas. Ver la figura 23.

Figura 23 Campus QoS Fiduciario límite recomendaciones

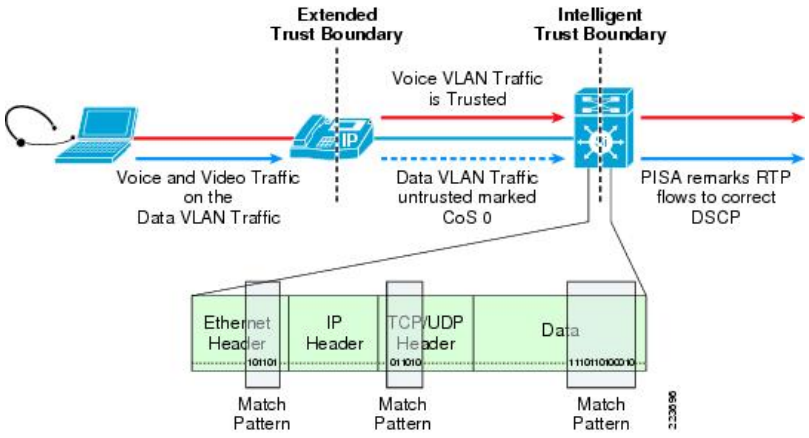


1. Optimal Trust Boundary: Trusted Endpoint
2. Optimal Trust Boundary: Untrusted Endpoint
3. Suboptimal Trust Boundary

En el campus actual diseño QoS, los puertos de acceso de cada uno de los conmutadores están configurados para no confiar en las marcas de QoS de cualquier tráfico que llega en ese puerto, a menos que se encuentra en el auxiliar o voz VLAN y el conmutador ha detectado que hay un teléfono (dispositivo de confianza) en la que VLAN. La decisión de confiar o no confiar en el tráfico de los extremos es binaria; o bien el tráfico es desde el teléfono y de confianza o de cualquier otro dispositivo y no de confianza. Este modelo funciona bien en un entorno con teléfonos dedicados, pero como las tendencias en comunicaciones unificadas continuar y las aplicaciones de voz y vídeo comienzan a combinar con otras aplicaciones de PC, la necesidad de forma selectiva e inteligente confiar en determinados flujos de aplicación de la *que no son de confianza* PC es cada vez es necesario. El uso de por VLAN y por policers de tráfico del puerto es un mecanismo que se utiliza para confiar selectivamente en ciertos intervalos de puertos y en ciertos tipos de datos de tráfico. Cada puerto arista puede configurarse para detectar el tráfico dentro de un intervalo de puerto específico y, para todo el tráfico que es inferior a una tasa definida *normal*, marcar ese tráfico con los valores correctos de DSCP. Se elimina todo el tráfico de esta tasa, que proporciona un mecanismo de seguridad para proteger contra una aplicación enmascaramiento como otro más de misión crítica uno (mediante el uso de números de puerto de la aplicación más importante para la comunicación). Si bien este enfoque basado en policer ha demostrado que funcionan bien y todavía es válida para ciertos entornos, la lista cada vez más compleja de aplicaciones que comparten los números de puerto y que podría ser secuestren otras aplicaciones de confianza de intervalos de puertos requiere que consideramos un enfoque más sofisticado.

Inspección profunda de paquetes (ppp) o la capacidad de examinar la carga de datos de un paquete IP y el uso no sólo la cabecera IP y TCP/UDP para determinar qué tipo de tráfico el paquete contiene, proporciona una herramienta para abordar este problema. Un conmutador equipado con hardware de red basado en aplicaciones reconocimiento (NBAR) es capaz de determinar si un flujo UDP es verdaderamente una secuencia RTP o algunos otros basados en aplicaciones mediante el examen de la cabecera RTP contenida dentro de la carga del paquete. Consulte figura 24.

La figura 24 Uso de Deep Packet Inspection para proporcionar un límite de QoS Fiduciario inteligente



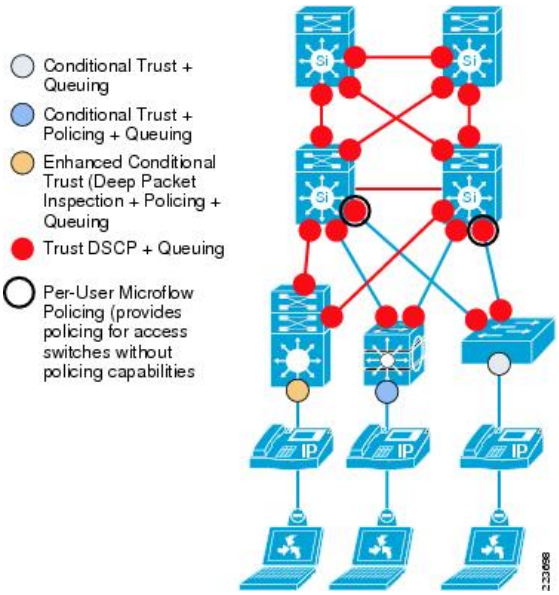
La capacidad para detectar y marque adecuadamente los flujos de aplicación específica en el borde de la red ofrece para un límite de confianza de QoS más detallado y preciso.

Hasta hace poco, se recomienda que los propios no debe ser considerado como dispositivos de final de confianza a menos que se administraban estrictamente por el grupo de operaciones de TI. Siempre ha sido posible para un usuario configurar la NIC en su PC para marcar todas su tráfico a cualquier clasificación. Lo que marcan todo el tráfico de EF DSCP que podrían secuestrar eficazmente los recursos de red reservados para aplicaciones de tiempo real (como VoIP), con lo cual arruinar la calidad de servicio de VoIP en toda la empresa. Control de la clasificación de QoS centralizado de la introducción de capacidades en el agente de seguridad de Cisco (CSA) y en vista de Microsoft para prever y marcado de los flujos de tráfico de aplicación es otro enfoque que debería permitir una política de confianza más granular de QoS. Es importante tener en cuenta al considerar el campus global diseño QoS que las capacidades de los clientes de vista y CSA no prevén policiales y otras capacidades de control de tráfico ofrecidos por los modificadores. Todavía se recomienda que, en el campus de entornos de aprovechar la CSA y vista marcado capacidades, la propia red diseñarse para proporcionar el tráfico adecuado controles de identificación y la policía.

Nota Microsoft ha implementado una serie de mecanismos de control de flujo en la pila IP de vista que pretenden proporcionar para funciones de administración del tráfico mejorada. En el momento en que este documento fue escrito, Cisco todavía estaba en colaboración con Microsoft para determinar la efectividad y mejores prácticas para el uso de estas nuevas herramientas de QoS. Actualmente la mejor práctica todavía se recomienda implementar un modelo de límite de confianza tradicional complementado por el DIP.

La presencia del límite de la confianza en el campus de diseño de QoS proporciona la base para la arquitectura general. Al garantizar que en la red de tráfico correctamente es clasificado y marcado, sólo es necesario proporcionar la cola apropiado en el resto del campus (véase figura 25).

Figura 25 Clasificación de QoS Campus, marcadores, Queue Server y seguridad



Red resiliencia y QoS

El uso de QoS en el campus generalmente se pretende proteger determinados flujos de tráfico de aplicación de períodos de congestión. En un entorno de campus con aplicaciones de misión crítica, el uso de herramientas de QoS y principios de diseño proporciona mayor resistencia o disponibilidad para las aplicaciones de misión que explícitamente están protegidos según sus CoS / marcas DSCP. Mejorando el campus de la línea de base diseño de QoS para incluir mecanismos tales como una cola de *análisis* combinado con DPI y el perímetro de la policía, también es capaz de proporcionar un grado de protección para todas las aplicaciones de esfuerzo mejores restantes.

Los principios de la utilización de la clasificación de análisis son bastante simples. Hay ciertos flujos de tráfico en cualquier red que debería recibir lo que se denomina menos-que-mejor servicio *posible*. Las aplicaciones que no es necesario llevar a cabo en un momento específico, como algunos tipos de copias de seguridad o son no esenciales a los procesos de negocio, pueden considerarse como tráfico de análisis. Puede utilizar cualquier red recursos quedan después de todo el resto de aplicaciones han sido atendidas. Una vez que un flujo de tráfico específicos se determina que entran en esta categoría, todos sus paquetes están marcadas con valor DSCP CS1 para indicar que están clasificados como tráfico de análisis. Colas específicas con una probabilidad alta de la caída, a continuación, se asignan para el tráfico de análisis que proporcionan un mecanismo de límite en el caso de que el tráfico de depurador comienza a competir con los flujos de mejor esfuerzo.

Una vez que se ha definido una clase de análisis, proporciona una valiosa herramienta para hacer frente a cualquier tráfico no deseado o inusual en la red. Mediante el uso de NBAR (inspección profunda de paquetes), es posible determinar que existen aplicaciones no deseadas en la red y bien colocar ese tráfico o marca como análisis — en función del tipo de tráfico y la Directiva de la red. Mediante la implementación de un policer de ingreso en los puertos de acceso en el campus, también es posible determinar si cualquier dispositivo o aplicación comienza a transmitir a velocidades de datos anormalmente alta. También se puede clasificar como análisis tráfico que supera un umbral normal o aprobado durante un período prolongado de tiempo.

Tener una política que identifica tráfico inoportuno o inusual como tráfico de análisis proporciona protección adicional sobre el acceso equitativo a los recursos de red para todo el tráfico y QoS diseño — incluso que marcó el mejor esfuerzo. Proporciona un control más explícita sobre lo que es la normal o comportamiento esperado para el tráfico de campus fluye y es un componente importante del enfoque general resistente al diseño de campus.

Nota Para obtener más detalles sobre el uso de QoS de análisis y el campus global diseño QoS, vea el capítulo de diseño de QoS campus de la *empresa QoS soluciones referencia Network Design guía versión 3.3* que se encuentra en el sitio SRND CCO, http://www.cisco.com/go/srnd.

Servicios de virtualización

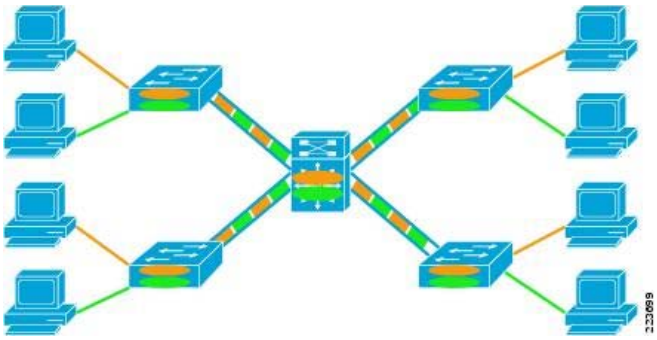
Muchas empresas ofrecen servicios de red para redes departamentales o unidades de negocio, hospedados proveedores, socios, huéspedes. Cada uno de estos diversos grupos puede requerir un conjunto de políticas especializados y acceso a los diversos recursos y servicios informáticos controlado. También es a menudo el caso de que ciertas restricciones reglamentarias o cumplimiento de mandatos de control de acceso específicos, aislamiento de tráfico o control de la ruta de tráfico para determinados grupos. Algunos de estos grupos pueden existir en la red durante largos períodos de tiempo, como socios, y otros sólo pueden requerir acceso para la vida de un proyecto específico, como contratistas. Una red también podría encontrarse a tener que soportar un número creciente de los usuarios invitados itinerante. Los cambios corporativos como adquisiciones, desinversiones y subcontratación también afectan a la infraestructura informática. La manera en que las comunicaciones e informática están entrelazados en los procesos de negocio de la empresa significa que cualquier cambio en la estructura de la organización inmediatamente se refleja en las necesidades del campus y de la red como un todo. La exigencia de una red de campus responder rápidamente a estos cambios repentinos en las políticas del negocio exige un diseño con un alto grado de flexibilidad inherente.

Virtualización: la capacidad de asignar recursos físicos de manera lógica (uno dispositivo físico compartido entre varios grupos o varios dispositivos operada como un único dispositivo lógico) — proporciona la capacidad de diseñar en un alto grado de flexibilidad en la arquitectura del campus. Diseño de la capacidad de reasignar recursos e implementar servicios para grupos específicos de los usuarios sin necesidad de reestructurar la infraestructura física a la arquitectura general del campus proporciona un importante potencial para reducir los costos operacionales y de capital global sobre la vida útil de la red.

Mecanismos de virtualización de campus

Capacidades de virtualización no son nuevas para la arquitectura del campus. La introducción de LAN virtual (VLAN) proporciona las capacidades de virtualización primeras en el campus. Consulte figura 26. La capacidad de tener un dispositivo, de un conmutador, reemplazar múltiples concentradores y puentes mientras proporcionando reenvío distintos planos para cada grupo de usuarios era un importante cambian en el diseño de campus.

Figura 26 Virtual LAN (Campus virtualización)

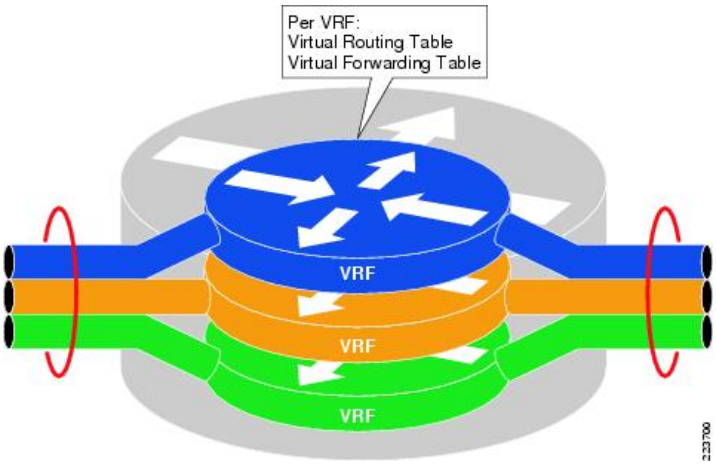


El uso de un diseño basado en VLAN conmutado ha proporcionado para una serie de ventajas, la mayor capacidad, el aislamiento y la capacidad de administración. Sin embargo, es la flexibilidad que VLAN ofrecen que ha tenido el mayor impacto en el diseño de campus. La capacidad de reconfigurar dinámicamente la red, agregar nuevas subredes o grupos empresariales, sin tener que reemplazar físicamente la red proporciona enormes costos y beneficios operacionales. Entorno de red de campus modernas de hoy en día existe en gran medida debido a las capacidades que proporciona la virtualización VLAN.

Si bien VLAN proporcionan cierta flexibilidad en la segmentación dinámicamente de grupos de dispositivos, VLAN tienen algunas limitaciones. Como una técnica de virtualización de capa 2, VLAN están obligadas por las reglas de diseño de red de capa 2. En el diseño de campus jerárquica estructurado no tienen la flexibilidad necesaria para abarcar grandes dominios. El uso de virtualización de enrutamiento y reenvío (VRF) con GRE, 802.1q y MPLS etiquetado para crear Virtual Private Networks (VPN) en el campus proporciona un enfoque a la ampliación de la flexibilidad de configuración que ofrece VLAN en el campus todo y si es necesario a través de toda la red. Consulte figura 27.

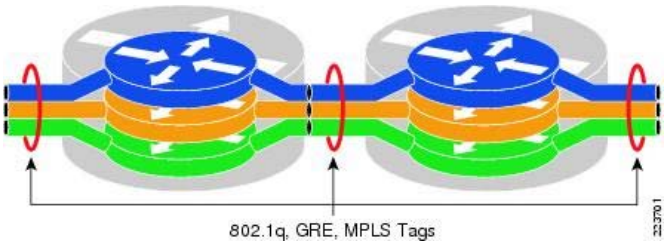
VRFs ofrecen la posibilidad de que el enrutamiento independiente y reenvío instancias dentro de un conmutador física. Cada VRF tiene su propia tabla de reenvío Layer-3. Cualquier dispositivo en un VRF específico puede ser cambiado directamente Layer-3 (en otras palabras, enrutado) a otro dispositivo en el mismo VRF, pero no puede llegar directamente a uno en otro VRF. Esto es similar a la forma en que cada VLAN en cada uno tiene su propia capa 2 reenvío y las inundaciones de dominio. Cualquier dispositivo en una VLAN puede llegar directamente a otro dispositivo en el nivel-2 en la misma VLAN, pero no un dispositivo en otro VLAN a menos que se reenvía por un enrutador Layer-3.

Figura 27 Virtual de enrutamiento y reenvío (VRF)



Al igual que con una red VLAN basada mediante 802.1q troncos para ampliar la VLAN entre conmutadores, un VRF en función de troncos de usos 802.1q de diseño, túneles GRE o etiquetas MPLS para ampliar y unir los VRFs. Consulte figura 28.

Figura 28 Opciones de virtualización de vínculo



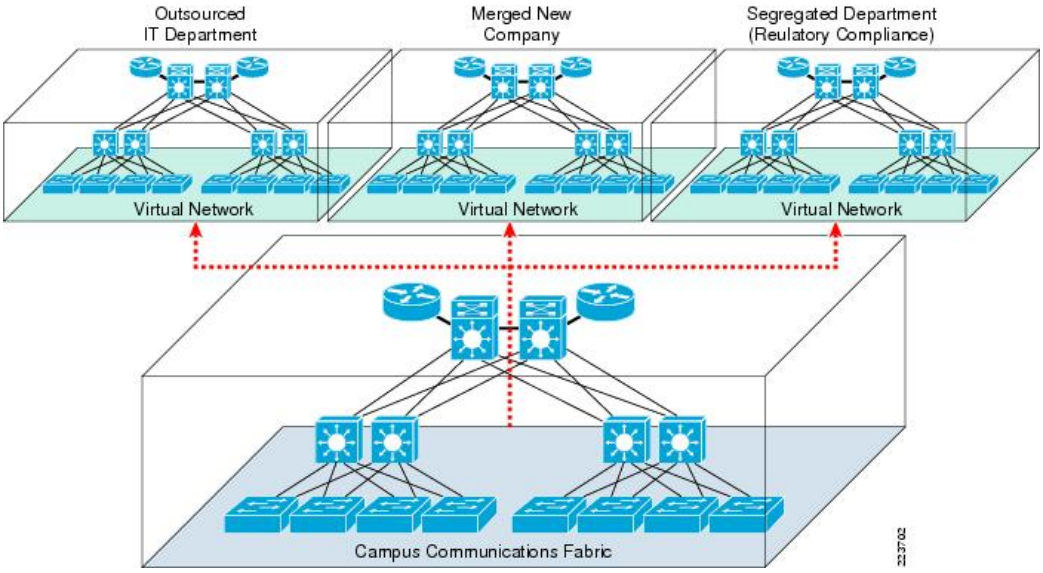
Todas o cualquiera de estos mecanismos de virtualización de tres vínculo puede utilizarse en la virtualización de reenvío basado en VRF Layer-3 en el diseño to-end. La decisión sobre qué combinación de estas técnicas para utilizar depende principalmente en la escala del diseño y los tipos de los flujos de tráfico (peer-to-peer o concentrador y radio).

Virtualización de red

Virtualización de red es como la capacidad de aprovechar una única infraestructura física y ofrecen varias redes virtuales cada con un conjunto distinto de las directivas de acceso y todavía compatible con todos de la seguridad, QoS, servicios de comunicaciones unificadas disponibles en una red física dedicada. Teniendo las capacidades de virtualización básica del campus combinada con la posibilidad de asignar los usuarios y los dispositivos a grupos de directivas específicas a través de 802.1 X proporciona flexibilidad en la arquitectura general del campus. Como ilustrado

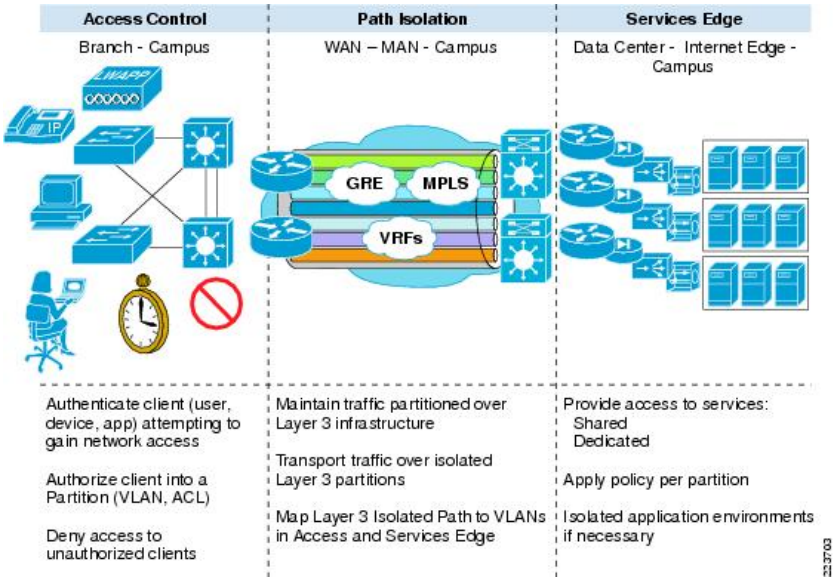
en figura 29, puede permitir un solo campus físico para la asignación de varias redes lógicas separados cuando construida con las capacidades necesarias.

Ejemplo de figura 29 De los varios-to-One asignación de virtual a redes físicas



El problema de diseñar el campus para habilitar la compatibilidad de las redes virtualizados mejor se entiende por romper el problema en tres partes funcionales: acceso control; aislamiento de la ruta de acceso; y capacidades de borde de servicios como se muestra en la figura 30 . Cada una de estas tres partes a su vez se ha creado con muchas características individuales, todas diseñadas para interoperar y producir la solución de red virtualizada-to-end.

Figura 30 Elementos funcionales necesarios en redes de Campus virtuales



La habilitación de control de acceso requiere que se realice algún tipo de asignación de política y de grupo en el borde de la red. Esto puede hacerse dinámicamente a través de 802.1X, MAB, Web-Auth o el dispositivo de NAC. Estos que todas pueden ser utilizadas para asignar un usuario particular o un dispositivo a una VLAN específica. También se puede lograr estática a través de la configuración manual que asigna puertos específicos a VLAN específicas (y redes virtuales específicas). Aislamiento de la ruta de acceso puede llevar a cabo mediante cualquier combinación de los mecanismos de enlace y reenvío virtual. Un ejemplo es VRF-Lite utilizando VRFs combinada con 802.1q troncos, como se describe en la descripción anterior. En el centro de datos o en redes de mayor tamaño localmente en el módulo de bloque de servicios de campus, se pueden implementar las políticas de borde de servicios.

Nota Para obtener información detallada sobre cómo cada una de estas tres áreas funcionales se implementan en un diseño de campus, consulte la sección de virtualización de red en la página de SRND en http://www.cisco.com/go/srnd.

Servicios de seguridad

Servicios de seguridad son parte integral de cualquier diseño de red. La interconexión de redes, el aumento del uso de dispositivos móviles y el cambio de la mentalidad de la comunidad de hackers — de uno donde orgullo técnica motivado la mayoría de los ataques a uno donde los intereses financieros son un factor de motivación principal — tienen todos sido responsable de la continua aumentan en los riesgos de seguridad asociados con nuestras infraestructuras de red.

Muchas de las características de *seguridad* de campus ya han sido examinadas en alguna forma en las diversas secciones anteriores. Ya no es un complemento de la red de seguridad pero está totalmente integrado en el diseño de campus todo y muchas de las capacidades de la red del campus que abordan una vulnerabilidad de seguridad también sirven para resolver los problemas fundamentales de la disponibilidad o ayuda en la dinámica provisión de servicios de red.

Dentro del entorno de red en la actualidad, hay una gran variedad de tipos y vectores de ataque, que van desde los simples datos rastreos a sofisticadosentornos *botnet* aprovechar los sistemas de control distribuido complejo. Todos estos diversos ataques de seguridad se clasifican dentro de seis clases fundamentales de las amenazas de seguridad que debe considerar el diseño de campus:

- Ataques de reconocimiento
- Denegación de servicio y distribuidos ataques de denegación de servicio
- Ataques de la intervención de línea telefónica
- Daños colaterales
- Ataques de acceso no autorizado
- Utilización no autorizada de información, recursos o activos

Hacer frente a estas amenazas requiere un enfoque que aprovecha la prevención y detección de técnicas para abordar la raíz causar vectores de ataque o vulnerabilidades que seguridad ataques uso —, así como proporcionar para una rápida respuesta en caso de un brote o ataque. La combinación de herramientas dentro de la estructura de conmutación con capacidades de prevención y control externo será necesaria para abordar el problema global.

La arquitectura de seguridad para el campus puede dividirse en tres partes básicas: infraestructura; seguridad perimetral y extremo; y protección. Estos se abordan en las secciones siguientes.

Infraestructura de seguridad

Hay dos consideraciones de seguridad general al diseñar un campus red infraestructura. En primer lugar, es necesario proteger a la infraestructura de ataque intencional o accidental: garantizar la disponibilidad de la red y servicios de red. En segundo lugar, la infraestructura debe proporcionar información sobre el estado de la red a fin de ayudar en la detección de un ataque constante.

Protección de infraestructura

El diseño de seguridad debe proporcionar protección para los tres elementos básicos de la infraestructura: dispositivos (interruptores); enlaces; y, el plano de control.

Protección de los dispositivos de red

Protección de los conmutadores de campus comienza con el uso del control de gestión y el cambio seguro para todos los dispositivos. El uso de alguna forma de AAA para el control de acceso debe combinarse con las comunicaciones cifradas (como SSH) para la administración y configuración del dispositivo de todos. Los métodos de AAA preferidos son RADIUS o TACACS +; estas deben configurarse para apoyar la autorización de comando y contabilidad completa. Como un paso adicional, cada uno de los dispositivos debe configurarse para minimizar la posibilidad de que cualquier atacante acceder o comprometer al propio conmutador. Esta protección se logra mediante la función de Cisco IOS AutoSecure. AutoSecure es una macro de sistema de Cisco IOS que actualiza la configuración de seguridad de cada uno de los conmutadores para ponerla en línea con las mejores prácticas de seguridad recomendadas de Cisco. Aunque el uso de la función AutoSecure puede facilitar enormemente el proceso de protección de todos los dispositivos en la red, se recomienda que se desarrolle una política de seguridad de red y que se aplique un proceso de auditorías periódicas para garantizar el cumplimiento de todos los dispositivos de red.

Proteger los enlaces

Protección de los vínculos entre switches de amenazas de seguridad en gran medida se logra mediante la aplicación del campus diseño QoS discutido en la optimización de aplicaciones y servicios de protección. Con el límite de confianza adecuadas y las políticas de cola, complementado con el uso de herramientas de análisis en el diseño general — ayudará en la protección de la capacidad de enlace en el marco de la zona de confianza (dentro del límite de la confianza de QoS) de la red de ataque directo. Áreas fuera de la calidad de servicio de confianza límite requerirá mecanismos adicionales, tales como la guardia de DDoS Cisco, implementan para abordar los problemas de saturación de enlace por ataque malintencionado.

Proteger el plano de control

Proteger el plano de control implica tanto la CPU del sistema de endurecimiento de las condiciones de sobrecarga y asegurar el control de protocolos de plano. El uso de autenticación basada en MD5 y desactivación explícitamente cualquier protocolo de control en cualquier interfaz donde no es específicamente requerido, en conjunto proporcionan el primer nivel de protección por asegurar el control de protocolos de plano. Una vez que estos riesgos se han cerrado, el siguiente problema es proteger CPU del conmutador de otras vulnerabilidades. Si la CPU del conmutador puede ser atacada y sobrecargada — ya sea intencionalmente o no: el plano de control también es vulnerable. Si el conmutador está no se puede procesar enrutamiento, que abarcan el árbol, o cualquier otros paquetes de control, la red es vulnerable y potencialmente se pone en peligro su disponibilidad. Como se describe en las herramientas y enfoques para alta disponibilidad de campus, este tipo de problema se dirige mejor con limitación de herramientas (limitadores de velocidad de hardware o algoritmos de colas de hardware) combinados con un mecanismo de control policial de plano (CoPP) inteligente de la velocidad de CPU. Seguridad, QoS y disponibilidad diseño superposición aquí como necesario utilizar herramientas de QoS para enfrentar un posible problema de seguridad dirigida directamente a la disponibilidad de la red.

Infraestructura de telemetría y monitoreo

Sin la capacidad para supervisar y observar lo que está ocurriendo en la red, puede ser muy difícil de detectar la presencia de dispositivos no autorizados o flujos de tráfico malintencionado. Los siguientes mecanismos pueden utilizarse para proporcionar los datos de telemetría necesario necesarios para detectar y observar cualquier actividad anómala o malintencionado:

- *NetFlow* — brinda la capacidad de realizar un seguimiento de cada flujo de datos que aparece en la red.
- *Hardware DPI (NBAR)* — proporciona la capacidad de detectar indeseables de la aplicación flujos de tráfico en la red tener acceso a capa y permitan control seleccionado (colocar o policía) de tráfico no deseado.
- *Syslog* — proporciona la capacidad de realizar un seguimiento de eventos del sistema.

Además de utilizar NetFlow y DIP para el control de tráfico distribuido, inserción de dispositivos IPS en puntos clave de retracción ofrece un nivel adicional de la capacidad de observación y mitigación. Aunque NetFlow proporciona un mecanismo muy escalable detectar y encontrar los flujos de tráfico anómalo, IPS junto con NBAR basa DPI puede proporcionar visibilidad del contenido de los paquetes individuales. Los tres de estos mecanismos de telemetría deben basarse en el backend adecuado sistemas de vigilancia. Herramientas, tales como el MARS Cisco, deben aprovecharse para proporcionar una visión consolidada de los datos recopilados para permitir una visión general más precisa de cualquier brote de seguridad.

Nota Un capítulo de diseño de campus próximos documentará las mejores prácticas detalladas para implementar la seguridad de la infraestructura de campus y endurecimiento descritas anteriormente.

Control de acceso de perímetro y seguridad perimetral

Sólo como un firewall o router de seguridad exterior proporciona seguridad y control de las políticas en el perímetro exterior de la red de la empresa, las funciones de la capa de acceso campus como un perímetro de la red interna. La red debe ser capaz de proporcionar la tranquilidad

de que el cliente se conecta en el perímetro interno, de hecho, es un cliente conocido y de confianza (o al menos cumple los requisitos mínimos para ser con seguridad puede conectarse en este punto de la red). Características de confianza y la identidad deben ser implementadas en estos internos perímetros en forma de mecanismos de autenticación como IBNS (802.1X) o control de admisión de red (NAC). Esto permite que la prevención de acceso no autorizado o la capacidad de introducir el cumplimiento de normas y gestión de riesgos en el momento de la conexión. Impedir el acceso no autorizado, también mitiga la amenaza de compromiso para activos adicionales en la red.

Además de garantizar la autenticación y el cumplimiento de los dispositivos adjuntar a la red, la capa de acceso a también se debe configurar para proporcionar protección contra un número de capa 2 *man-in-the-middle* ataques (MiM). Configurar la características de seguridad integrada de Cisco (CISF), el puerto de la seguridad, IP origen guardia, dinámica de ARP de inspección y supervisión DHCP en todos los puertos de acceso complementa la política de control de acceso de seguridad que ofrecen IBNS y NAC.

Seguridad extremo

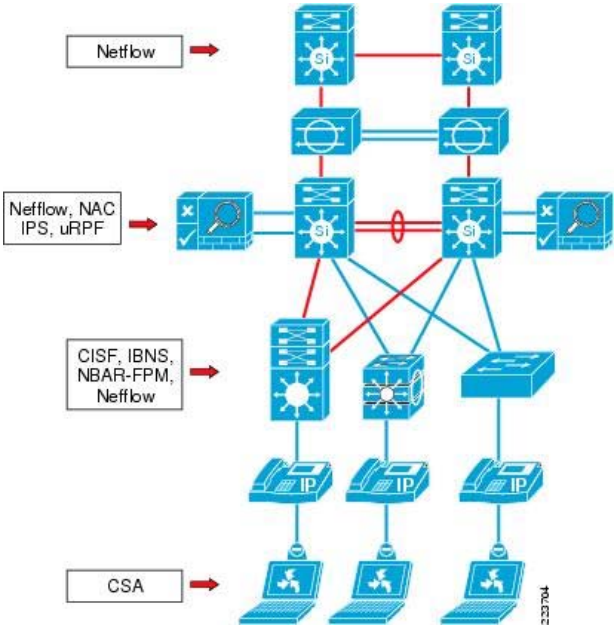
La arquitectura de seguridad de campus debería ampliarse para incluir al mismo cliente. Los extremos, como los portátiles, son los objetivos más vulnerables y más deseables de ataque. Contienen datos importantes y, cuando se pone en peligro, también pueden servir como un lanzamiento puntos para otros ataques contra la red interna. La creciente amenaza de *bots* es sólo el último de una larga línea de vulnerabilidades de extremo que puede amenazar el negocio de la empresa.

La instalación de aplicaciones de cliente, agente de seguridad tales como Cisco (CSA), es un paso importante para completar la arquitectura de seguridad to-end, junto con software de cliente NAC y IBNS en los extremos que participan con el resto de los elementos de seguridad de red integrada. Es una parte del esfuerzo para ayudar a las complejas operaciones de seguridad a nivel de aplicación mediante el aprovechamiento de los servicios de seguridad integrada de redes.

Distribuido seguridad: defensa en profundidad

Quizás el desafío de seguridad más grande que enfrenta la empresa de hoy es uno de escala. El problema de cómo detectar, prevenir y mitigar contra el creciente número de amenazas de seguridad requiere un enfoque que aprovecha un conjunto de herramientas de seguridad que escalar proporcionalmente con el tamaño de la red. Es un enfoque de este problema de escala distribuir los servicios de seguridad en el tejido de conmutación por sí mismo. Se muestra un ejemplo de este enfoque en figura 31. Los diversos telemetría y la política de aplicación de mecanismos de seguridad se distribuyen a través de todas las capas de la jerarquía del campus. A medida que crece la red en el modelo distribuido, los servicios de seguridad crecen proporcionalmente con la capacidad de conmutación.

La figura 31 Servicios de seguridad distribuida



Además de proporcionar un enfoque escalable de seguridad del campus, el modelo distribuido tiende a reforzar una posición de *profundidad-en-defensa*. Mediante la integración de funciones de seguridad en todos los niveles de la red, resulta más fácil prever mecanismos de vigilancia y control del cumplimiento de la seguridad redundantes.

Operacionales y de servicios de gestión

Garantizar la capacidad de forma rentable administrar el campus de la red es uno de los elementos más críticos del diseño general. Como se alarga el ciclo de inversión para redes de campus universitarios, están aumentando los costos operacionales de la red (OPEX) relativa a los gastos de capital originales (CAPEX). Dispositivos continúan en servicio más largo y está creciendo el porcentaje del costo total asociado con la operación a largo plazo de cada dispositivo relativo a su coste original de la capital. La capacidad de administrar, configurar y solucionar problemas de los dispositivos de ambos en la red y las aplicaciones que utilizan la red es un factor importante en el éxito del diseño de la red.

El marco FCAPS define cinco categorías de administración de red: error; configuración de Contabilidad, el rendimiento; y, la seguridad. Un debate completo de la administración de red y un examen exhaustivo de cada una de estas áreas es fuera del alcance de este documento; sin embargo, comprende los principios del campus de diseñar y capacidades de conmutador en el marco de la administración general es esencial. Cada una se describe brevemente en las secciones siguientes.

Administración de fallos

Uno de los objetivos principales del diseño de la global campus es minimizar el impacto de cualquier culpa de las aplicaciones de red y servicios. La redundancia y la resiliencia integrado en el diseño se pretenden evitar fallos (fallos) de afectar la disponibilidad del campus. Todavía se producirán errores sin embargo, y contar con las capacidades para detectar y reaccionar a las fallas, así como proporcionar información suficiente para llevar a cabo un post mortem análisis de los problemas son aspectos necesarios de sonido procesos operacionales. Proceso de administración de fallas puede dividirse en tres etapas o los aspectos, proactivos y reactivos y post mortem análisis.

Administración proactiva de error

Finalmente, cada red requiere la instalación de hardware nuevo, si desea agregar capacidad a la red existente, reemplazar un componente defectuoso o agregar funcionalidad a la red. La capacidad de probar este nuevo hardware en forma proactiva y asegurar que funciona correctamente antes de realizar la instalación puede ayudarle a evitar más interrupciones de servicio una vez que se instalan equipos en la red. Mientras que todos los proveedores, ampliamente, probar y certifican que los equipos está funcionando correctamente antes de se envía a un cliente, pueden ocurrir muchas cosas a una pieza del equipo antes de que finalmente se instale en la red de producción. Equipo puede ser dañado durante el envío o dañado durante la instalación (descarga estática puede dañar los componentes electrónicos si no están instalados sistemas mediante los procedimientos correctos). Si bien se tiene cuidado para garantizar que ninguno de estos eventos se producen, tener la capacidad de ejecutar una amplia diagnósticos para detectar cualquier errores componentes antes a cualquier producción traslado puede evitar posibles problemas de producción que se produzca más tarde.

El marco de diagnóstico online genérico de Catalyst (GOLD) está diseñado para proporcionar capacidades de gestión integrada de diagnóstico para mejorar las capacidades de detección de fallas proactivo de la red. GOLD proporciona un marco en el que se puede configurar diagnósticos de vigilancia de la salud de sistema de curso/tiempo de ejecución de prever Estado continua comprueba los modificadores de la red (como en banda activas pings que probar el funcionamiento correcto de la placa de reenvío). GOLD también proporciona la capacidad de ejecutar (o programar) potencialmente intrusivas diagnósticos bajo demanda. Estos diagnósticos pueden ayudar a solucionar problemas de hardware sospechosos y proporcionar la capacidad de manera proactiva probar nuevo hardware antes de cutovers de producción.

Nota Para obtener más información sobre GOLD, consulte la siguiente URL: http://www.cisco.com/en/US/partner/products/ps7081/products_white_paper0900aecd801e659f.shtml

Administración de fallas reactiva

Uno de los objetivos centrales para cualquier diseño de campus es garantizar que la red se recupera forma inteligente de cualquier evento de error. Los diversos protocolos de control (como EIGRP o OSPF) todos proporcionan la capacidad para configurar respuestas específicas a los sucesos de error. Sin embargo, en algunos casos las capacidades de Protocolo de control estándar no son suficientes y el diseño puede requerir un nivel de personalización adicional como parte del proceso de recuperación. Los enfoques tradicionales de agregar este comportamiento personalizado a menudo implican el uso de sistemas de control centralizados para capturar eventos y ejecutar secuencias de comandos para tomar una acción específica para cada tipo de evento. Proporcionar inteligencia distribuida adicional en el tejido conmutación puede complementar y/o simplificar estos procesos operacionales. Herramientas, tales como la Cisco IOS Embedded Event Manager (EEM), proporcionan la capacidad para distribuir las secuencias de comandos a los conmutadores en la red: en lugar de ejecución de todas las secuencias de comandos de manera centralizada en un único servidor. Distribución de la inteligencia secuencias de comandos en la propia red campus aprovecha la capacidad de procesamiento distribuido y supervisión de capacidades de los conmutadores de fallos directa. Las capacidades, tales como mejorada objeto seguimiento (EOT), también proporcionan un nivel adicional de inteligencia configurable para los mecanismos de recuperación de la red. La capacidad para cada conmutador de la red de ser programable de la manera en que reacciona a las fallas y tienen que programación personalizada y cambiado con el tiempo — puede mejorar las capacidades de reacción de la red a las condiciones de falla.

Post Mortem análisis capacidades

Es importante para la red a recuperarse del fracaso cuando se produce un error. También es importante en la unidad a mantener un alto nivel de disponibilidad general de la red que los equipos de las operaciones de poder comprender qué ha fallado. Tener un registro centralizado de eventos de red (a través de datos SNMP y syslog), proporciona para la primera vista de topología de red o nivel de información de diagnóstico post mortem. A fin de proporcionar una visión más detallada de eventos de error específico dentro de los dispositivos individuales, es necesario para los dispositivos de sí mismos para recopilar y almacenar datos de diagnóstico más detallados. Ya no pueden recopilar datos desde un dispositivo que ya no está en pleno funcionamiento (si es parte de la red hacia abajo puede no recopilar datos a través de la red) sistemas de gestión centralizada, es importante tener un almacén local de la información de eventos. Algunos mecanismos, tales como el Archive Catalyst de eventos System (SEA) — pueden almacenar un registro de todos los eventos del sistema local en almacenamiento no volátil rearranque. Más detallada de supervisión de fallos de nivel de componente a través de mecanismos, tales como la Catalyst incorporada error de registro (OBFL) — son necesarias para permitir para problemas de hardware de nivel. OBFL actúa como un grabador de caja negra con tarjetas de línea y conmutadores. Registra temperaturas de funcionamiento, el tiempo de actividad de hardware, interrupciones y otros eventos importantes y mensajes que pueden ayudar a diagnosticar problemas con hardware tarjetas (o módulos) instalado en un router Cisco o switch. Fallas en un gran complejo sistema — por ejemplo, una red de campus — son inevitables. Tener las capacidades diseñadas en la red para apoyar un post mortem proceso de análisis del problema es muy valiosa para cualquier empresa que busca un elevado *número de nueves* de disponibilidad.

Contabilidad y rendimiento

Contabilidad y el rendimiento son dos aspectos del modelo FCAPS que se refiere principalmente con la supervisión de la capacidad y la facturación para el uso de la red. Entornos empresariales no son generalmente como que se trate con los aspectos de Contabilidad del modelo FCAPS porque ellos generalmente no implementan uso complejo sistemas de facturación. Sin embargo, las empresas requieren la posibilidad de observar el impacto de la red sobre la aplicación final-sistemas de tráfico y rendimiento. El mismo conjunto de herramientas de de supervisión y telemetría como parte de la arquitectura de seguridad también puede proporcionar supervisión de aplicaciones. NetFlow y DIP basado en NBAR que se utilizan para detectar el tráfico no deseado o anómalo pueden utilizarse también para observar los flujos de tráfico de aplicación normal. Aumenta el volumen de tráfico de aplicación, o la detección de nuevos patrones de tráfico de aplicaciones que podrían requerir la actualización de red o cambios de diseño: se puede dar seguimiento a través de NetFlow. Generación de perfiles de aplicaciones detallada puede recopilarse a través de las estadísticas NBAR y capacidades de monitoreo.

Además de patrones de tráfico y el volumen de seguimiento, a menudo también es necesario realizar análisis más detallado de tráfico de red de aplicación. Herramientas de análisis de red distribuida (como, por ejemplo, captura de paquetes y RMON sondeos) a menudo son elementos muy útiles para incluir en el diseño de campus global. Estos proporcionan la capacidad de recopilar trazas de paquetes de forma remota y verlas en una consola de administración central. Analizadores de paquetes distribuidos son potentes herramientas, no siempre es posible conectar uno a cada interruptor en la red. Es útil complementar herramientas distribuidos con el tráfico que abarcan capacidades (la capacidad para enviar una copia de un paquete de un lugar en la red a otra para permitir una herramienta físicamente remota examinar el paquete). El puerto básico que abarcan la capacidad de cada uno de los conmutadores debería complementarse con el uso de sensibilidad remota (RSPAN) y la RSPAN encapsulado (ERSPAN) para proporcionar esta capacidad. Modificadores de acceso deben configurarse con capacidades ERSPAN para permitir la supervisión de los flujos de tráfico como cerca a los dispositivos de final como sea posible RSPAN o (preferiblemente). ERSPAN es la solución preferida porque permite para que el tráfico distribuido que se lleven a través de varios saltos de Layer-3, lo que permite la consolidación de herramientas de análisis de tráfico en menos ubicaciones.

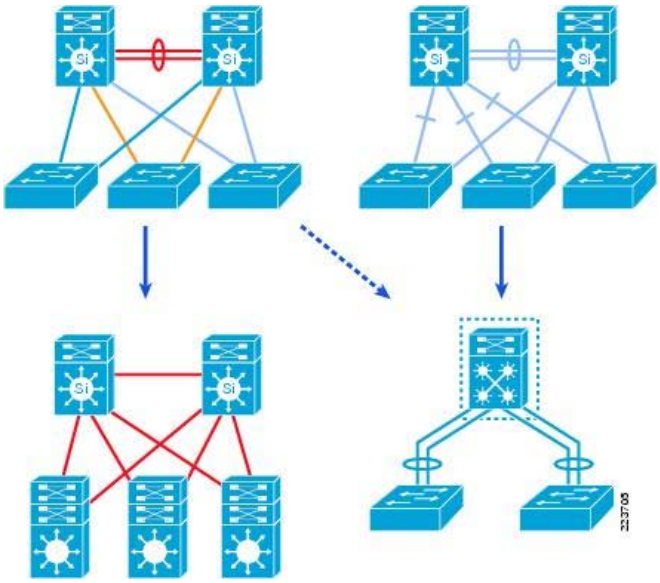
Configuración y seguridad

La configuración y la seguridad de los dispositivos de red se ha debatido anteriormente en la sección relativa a los servicios de seguridad. Las directrices de diseño que se describe allí están destinadas a satisfacer las necesidades del modelo FCAPS así como para proporcionar una seguridad más amplio de campus to-end. Consulte la sección "servicios de seguridad" para obtener más información.

Evolución de la arquitectura de campus

La arquitectura de red campus está evolucionando en respuesta a una combinación de los nuevos requerimientos del negocio, cambios tecnológicos y un creciente conjunto de las expectativas del usuario final. La migración del diseño de bloques de distribución de varios niveles de más de 10 años de edad a una de las opciones de diseño de bloque de enrutado distribución basada en el conmutador basado en el acceso o virtual más recientes se está produciendo en respuesta a los cambiantes requerimientos del negocio. Consulte figura 32. Mientras que el diseño de varios niveles tradicional todavía proporciona una opción viable para ciertos entornos de campus, se combina la mayor disponibilidad, más rápido convergencia, una mejor utilización de capacidad de la red y simplificados los requisitos operativos ofrecidos por los nuevos diseños para motivar a un cambio en arquitecturas fundacionales.

La figura 32 Evolución del diseño de bloques de distribución de campus



Se están produciendo cambios evolutivos dentro de la arquitectura del campus. Un ejemplo es la migración desde un tradicional diseño de red de acceso de capa 2 (con su requisito para abarcar VLAN y subredes varios conmutadores de acceso) a un diseño virtual basada en el conmutador. Otro es el movimiento de un diseño con subredes contenida dentro de un interruptor de acceso único para el diseño de enrutado-acceso.

Como se describe a lo largo de este documento, otro importante cambio evolutiva a la arquitectura de campus es la introducción de servicios adicionales, incluidos los siguientes:

- Servicios sin parar, alta disponibilidad
- Servicios de acceso y movilidad
- Servicios de optimización y la protección de la aplicación
- Servicios de virtualización
- Servicios de seguridad
- Funcionamiento y los servicios de administración

La motivación para la introducción de estas capacidades para el diseño de campus se han descrito a lo largo de este documento. El aumento de los riesgos de seguridad, la necesidad de contar con una infraestructura más flexible, cambiar en flujos de datos de aplicación, y todos los requisitos de SLA han impulsado la necesidad de una arquitectura más capaces. Sin embargo, la implementación del cada vez más complejo conjunto de capacidades impulsados por el negocio y servicios en la arquitectura de campus puede ser un desafío, si se hace de una manera de comida de la pieza. Tal como se describe en este documento, cualquier arquitectura éxito debe basarse en una base de teoría del diseño sólido y principios. Para cualquier negocio de empresas involucrada en el diseño y funcionamiento de una red de campus, se recomienda la adopción de un enfoque integrado: basados en sistemas sólidos principios de diseño. La *Guía de diseño de Cisco ESE campus*, que incluye esta discusión visión general y una serie de capítulos posteriores diseño detallado, está específicamente destinado a ayudar a la ingeniería y equipos de operaciones de desarrollan un diseño de campus basadas en sistemas que proporcionará el equilibrio de disponibilidad, seguridad, flexibilidad, y necesita de operabilidad necesario para responder a necesidades actuales y futuros empresariales y tecnológico.