Campus

Resumen de diseño

Abril de 2014

CISCO VALIDATED DESIGN

Contenido

Prefacio 1

Introducción 2

Resumen de diseño de la red LAN cableada del campus 3

- Modelo de diseño jerárquico 3
- Capa de acceso 5
  - Plataformas de capa de acceso 6
- Capa de distribución 6
  - Diseño de dos capas 6
  - Diseño de tres capas 8
  - Plataformas de capa de distribución 8
- Capa de núcleo central 9
  - Plataformas de capa de núcleo central 10
- Calidad de servicio (QoS) 10

Diseño de LAN por cable adicionales 11

- Administración de dispositivos con Cisco Secure ACS 11
- Cisco Network Analysis Module 11
  - Diseño de switch para distribución de bloque de servicios 12
  - Diseño de dispositivo para bloque de aplicaciones 12
  - Diseño de dispositivo para centro de datos 12
  - Diseño para sitio remoto 13
  - Supervisión de aplicaciones en tiempo real e histórica 13
  - Prestación de servicios y aplicaciones con inteligencia de desempeño de las aplicaciones 13
  - Detección y resolución simplificadas de problemas 13
  - Funcionalidades de exportación y fuentes de datos de Cisco Prime NAM 13
- Cisco Prime Infrastructure 14
  - Centro de trabajo de dispositivos 15
  - Tareas y plantillas de configuración 15
  - Alarmas, eventos y mensajes de syslog 15
  - Generación de informes 15
  - Compatibilidad con CleanAir 16
  - Compatibilidad con Network Analysis Module 16

Resumen de diseño de la red LAN inalámbrica del campus 17
Cisco Wireless LAN Controllers 19
Puntos de acceso ligero Cisco 20
Modelos para diseño inalámbrico 21
Modelo de diseño para modo local 21
Modelo de diseño con Cisco FlexConnect 22
Alta disponibilidad 24
Soporte de multidifusión 24
Selección de banda 25
ClientLink 26
Rendimiento de ancho de banda de 802.11ac 27
Planificación del canal 802.11ac 28
Red inalámbrica para usuarios temporales 29
Diseños de LAN inalámbrica adicionales 32
CleanAir inalámbrica del campus 32
Tecnología Cisco CleanAir 32
Infraestructura Cisco Prime con tecnología Cisco CleanAir 32
Cisco OfficeExtend 33
Controladores WAN inalámbricos Cisco 33
Puntos de acceso Cisco OfficeExtend 34
Modelos de diseño 34

Prefacio

Cisco Validated Designs (CVD) brindan un marco al diseño de sistemas en función de los casos de uso comunes o las prioridades actuales del sistema de ingeniería. Incorporan un amplio grupo de tecnologías, funciones y aplicaciones para abordar las necesidades de los clientes. Los ingenieros de Cisco han probado exhaustivamente y documentado cada CVD a fin de garantizar una implementación más rápida, confiable y predecible.

En este resumen de diseño se ofrece información sobre los casos de uso que se cubren en una serie o conjunto de guías de CVD relacionadas y se sintetiza sobre los productos y las tecnologías Cisco que resuelven los desafíos presentados por los casos de uso.

Comentarios y preguntas

Si desea hacer algún comentario sobre una guía o hacer preguntas, use el formulario de comentarios.

Para acceder a las guías más recientes de CVD, visite el siguiente sitio:

http://www.cisco.com/go/cvd/campus

Introducción

Existe una tendencia a menospreciar la red rebajándola a un mero conjunto de tuberías, a pensar que todo lo que se debe tener en cuenta es el tamaño de los tubos o las velocidades y la alimentación de las conexiones, con lo cual el resto no reviste de importancia. Así como las tuberías para un gran estadio o en un terreno elevado deben diseñarse teniendo en cuenta la escala, los fines, la redundancia y la protección contra alteraciones o fallas en el funcionamiento, y la capacidad para resistir picos de cargas, la red necesita consideraciones parecidas. Dado que los usuarios dependen de la red para acceder a la mayor parte de la información que necesitan para hacer sus trabajos y para transportar voz o video con confiabilidad, la red debe brindar un transporte inteligente y flexible.

Incluso con la gran cantidad de ancho de banda disponible para los enlaces troncales de LAN, existen aplicaciones sensibles al rendimiento que se ven afectadas por fluctuaciones, demoras y pérdida de paquetes. La función de la base de la red es proporcionar un transporte eficiente y tolerante a fallas que pueda diferenciar el tráfico de aplicaciones para tomar decisiones inteligentes sobre el uso compartido de cargas cuando la red está temporalmente congestionada. Independientemente de que el acceso a la red de un usuario sea por cable o inalámbrico, en la sede central o en un sitio remoto, la red debe ofrecer priorización inteligente y colas de tráfico junto con las rutas más eficientes posibles.

Cisco Validated Designs para el campus incorpora conectividad inalámbrica y por cable para tener una solución de acceso a la red completa. En este documento se explica lo siguiente:

- El diseño de la base LAN cableada del campus.
- La manera en que la LAN inalámbrica amplía el acceso seguro a la red para la fuerza laboral móvil.
- La manera en que la LAN inalámbrica puede ofrecer acceso de usuarios temporales para contratistas y personas que visten las instalaciones.

Puede encontrar todas las guías de CVD a las que se hace referencia en este resumen de diseño en:

www.cisco.com/go/cvd/campus

Resumen de diseño de la red LAN cableada del campus

LAN es la infraestructura de redes (interconexión) que proporciona acceso a los servicios de comunicación de red y recursos para usuarios finales y dispositivos que se encuentran en un piso individual o en un edificio. La red del campus se crea mediante la interconexión de un grupo de redes LAN dispuestas en una pequeña área geográfica. Los conceptos de diseño de red de campus son redes pequeñas inclusivas que usan desde un solo switch LAN hasta grandes redes con miles de conexiones.

La Guía de diseño para la tecnología LAN cableada en campus habilita la comunicación entre dispositivos en un edificio o entre un grupo de edificios, así como también la interconexión a la red WAN y módulos del perímetro de Internet en la red principal.

Específicamente, este diseño proporciona una base de red y servicios que hacen posible lo siguiente:

- Conectividad LAN en capas
- Acceso a la red por cable para los empleados
- Multidifusión IP para una distribución eficaz de los datos
- Infraestructura cableada lista para servicios multimedia

Modelo de diseño jerárquico

La Guía de diseño para la tecnología LAN cableada en campus usa un modelo de diseño jerárquico para desglosarlo en grupos modulares o capas. Este desglose del diseño en capas permite a cada capa implementar funciones específicas, lo que simplifica el diseño de red y, por lo tanto, la implementación y administración de la red.

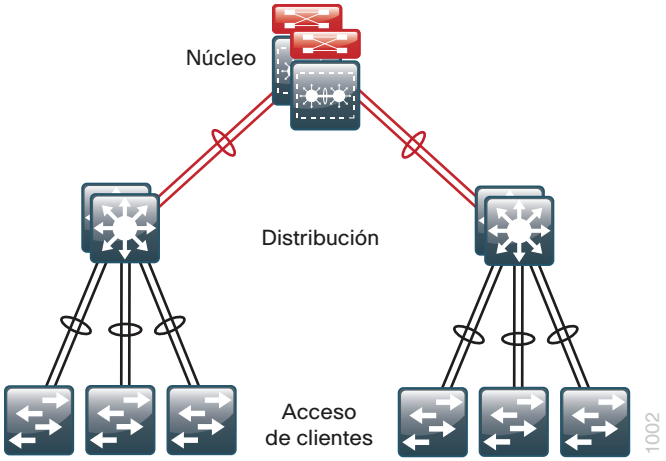
La modularidad en el diseño de red permite crear elementos de diseño que pueden replicarse en toda la red. La replicación ofrece una manera sencilla de ampliar la red, así como también un método de implementación homogéneo.

En arquitecturas de red mallada o plana, los cambios tienden a afectar a una gran cantidad de sistemas. El diseño jerárquico permite restringir los cambios operativos a un subgrupo de la red, lo que facilita la administración y mejora la recuperabilidad. La estructuración modular de la red en elementos pequeños y fáciles de comprender también facilita la recuperabilidad mediante aislamiento de fallas mejorado.

Un diseño de red LAN jerárquico incluye las siguientes tres capas:

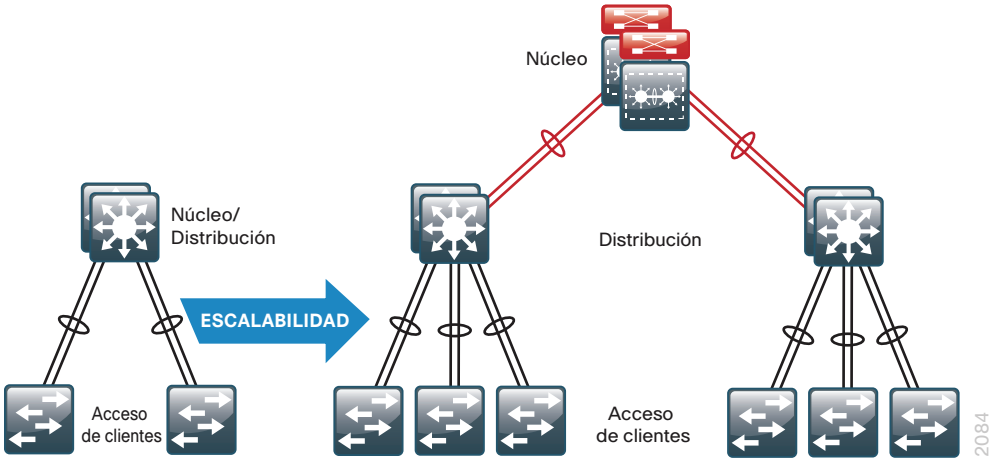
- **Capa de acceso:** ofrece a los terminales y usuarios acceso directo a la red.
- **Capa de distribución:** une las capas de acceso y ofrece conectividad a los servicios.
- **Capa central:** ofrece conectividad entre las capas de distribución para entornos de LAN grandes.

Figura 1 - Diseño jerárquico de LAN



Cada capa ofrece una funcionalidad diferente y funcionalidad para la red. Según las características del sitio de implementación, es posible que necesite una, dos o las tres capas. Por ejemplo, un sitio que ocupa un solo edificio puede necesitar solamente las capas de acceso y distribución. Pero si la organización es lo suficientemente grande, es posible que su red necesite las capas de acceso, distribución y central, a pesar de encontrarse todo en un solo edificio. Un campus de varios edificios probablemente necesitará las tres capas.

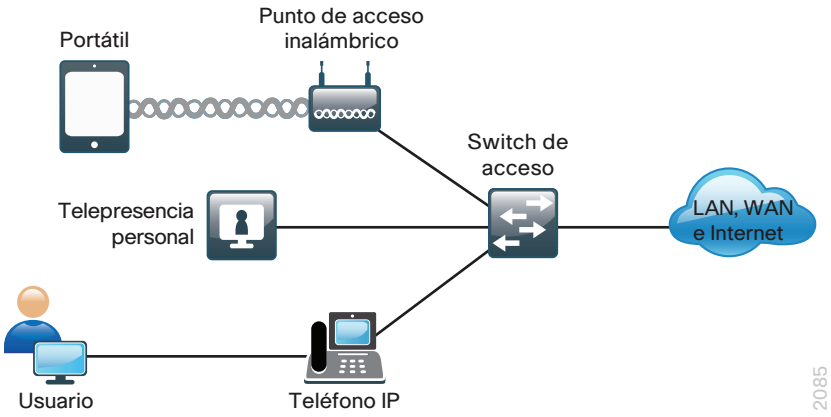
Figura 2 - Escalabilidad con un diseño modular



Capa de acceso

La capa de acceso es por donde los dispositivos controlados por el usuario, dispositivos accesibles al usuario y otros dispositivos terminales se conectan a la red. La capa de acceso ofrece conectividad tanto inalámbrica como por cable y contiene características y servicios para garantizar seguridad y recuperabilidad para toda la red.

Figura 3 - Conectividad de la capa de acceso



- **Conectividad de dispositivos:** la capa de acceso ofrece conectividad de dispositivos con ancho de banda de alta velocidad. A fin de hacer de la red una pieza transparente del trabajo diario del usuario final, la capa de acceso debe poder admitir ráfagas de tráfico de ancho de banda de alta velocidad cuando los usuarios realizan tareas de rutina, como enviar correos electrónicos pesados o abrir un archivo desde una página web interna.

  Debido a que muchos tipos de dispositivos de los usuarios finales se conectan a la capa de acceso (equipos personales, teléfonos IP, puntos de acceso inalámbricos, y cámaras de videovigilancia mediante IP), la capa de acceso puede admitir muchas redes lógicas, con lo cual ofrece los beneficios de rendimiento, administración y seguridad.
- **Servicios de seguridad y recuperabilidad:** el diseño de la capa de acceso debe garantizar que la red esté disponible para todos los usuarios que la necesitan, cuando la necesitan. Como punto de conexión entre la red y los dispositivos clientes, la capa de acceso debe ayudar a proteger la red contra errores humanos y ataques maliciosos. Esta protección incluye garantizar que los usuarios tengan acceso solamente a servicios autorizados, con lo cual se evita que los dispositivos de usuario final se apoderen del rol de otros dispositivos en la red y, cuando es posible, se verifica que todos los dispositivos de usuario final están permitidos en la red.
- **Funcionalidades de tecnología avanzada:** la capa de acceso ofrece un conjunto de servicios de red que admiten tecnologías avanzadas, como voz y video. La capa de acceso debe ofrecer acceso especializado para los dispositivos mediante el uso de tecnologías avanzadas, para garantizar que el tráfico de estos dispositivos no se vea afectado por el tráfico de otros dispositivos y, además, para garantizar la distribución eficiente del tráfico que necesitan muchos dispositivos en la red.

Plataformas de capa de acceso

La Guía de diseño para la tecnología LAN por cable en campus es compatible con los siguientes switches de Cisco como plataformas de capa de acceso:

- Switches Cisco Catalyst de la serie 2960-S
- Switches Cisco Catalyst de la serie 2960-X
- Switches Cisco Catalyst de la serie 3560-X
- Switches Cisco Catalyst de la serie 3750-X
- Switches Cisco Catalyst de la serie 3650
- Switches Cisco Catalyst de la serie 3850
- Switches Cisco Catalyst de la serie 4500E

Capa de distribución

La capa de distribución admite muchos servicios importantes. En una red donde la conectividad debe atravesar la LAN completa, ya sea entre distintos dispositivos de la capa de acceso o desde un dispositivo de la capa de acceso a la WAN, la capa de distribución hace posible esta conectividad.

- **Escalabilidad:** en cualquier sitio con más de dos o tres dispositivos de capa de acceso, no resulta práctico interconectar todos los switches de acceso. La capa de distribución sirve como un punto de agregación para múltiples switches de la capa de acceso.

  La capa de distribución puede reducir los gastos operativos haciendo que la red sea más eficiente, exigiendo menos cantidad de memoria, creando dominios de falla que compartimenten las fallas o los cambios en la red y procesando los recursos para dispositivos en cualquier otro lado en la red. La capa de distribución también aumenta la disponibilidad de red gracias a que contiene las fallas en dominios más pequeños.

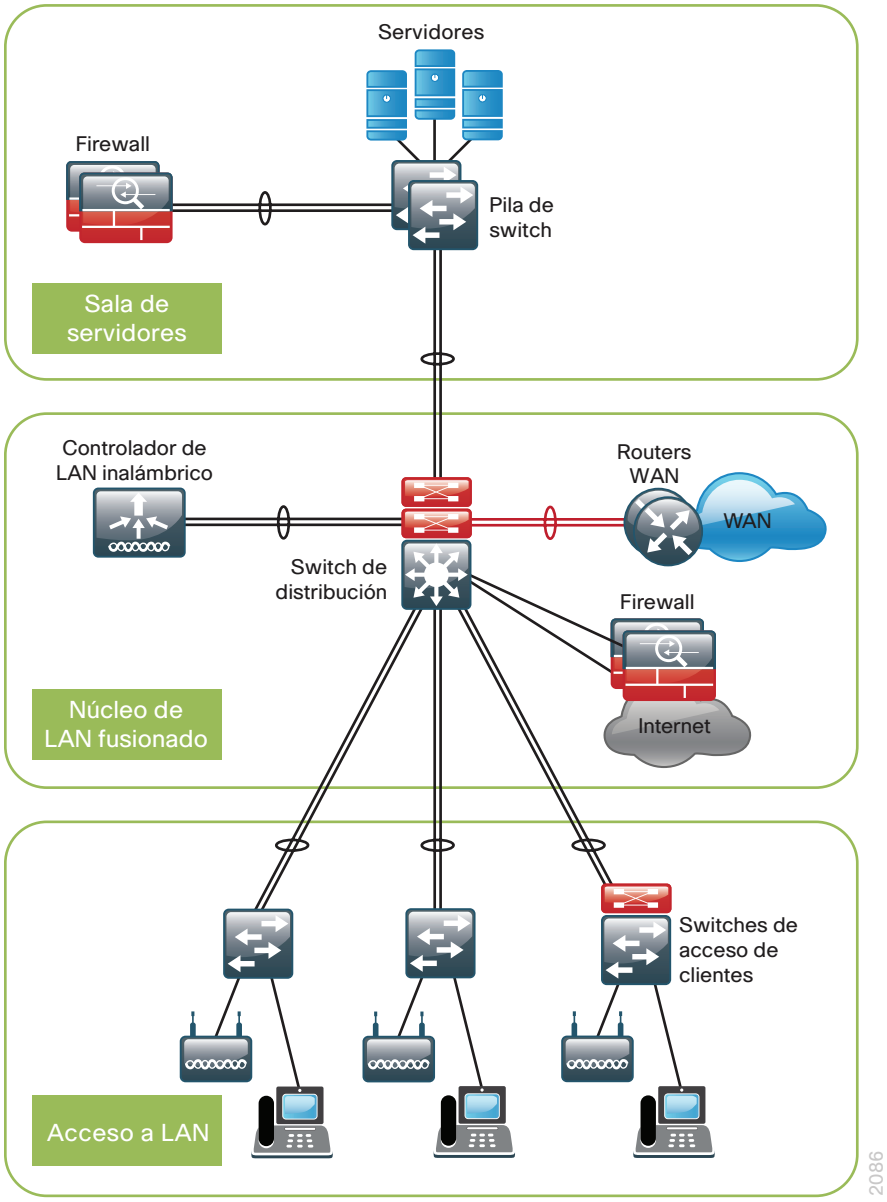
- **Reducción de la complejidad y aumento de la recuperabilidad:** la Guía de diseño para la tecnología LAN cableada en campus usa una capa de distribución simplificada, en la cual un nodo de la capa de distribución se compone de una entidad lógica individual que puede implementarse usando un par de switches físicamente separados que funcionan como un dispositivo, o bien usando una pila física de switches que funcionan como un dispositivo. La recuperabilidad la aportan los componentes físicamente redundantes, como fuentes de alimentación, supervisores y módulos, así como también la conmutación activa para los planos de control lógico redundantes.

  Este enfoque reduce la complejidad que supone configurar y operar la capa de distribución porque se requiere menor cantidad de protocolos. Se necesita muy poco o nada de ajuste para proporcionar convergencia en una fracción de segundo en torno a las fallas o interrupciones

Diseño de dos capas

La capa de distribución ofrece conectividad para los servicios basados en la red para la WAN y para el perímetro de Internet. Los servicios basados en la red pueden incluir y no se limitan a los Servicios de aplicaciones de área amplia (WAAS) y a los controladores LAN inalámbricos. Según las dimensiones de la LAN, estos servicios y la interconexión a WAN y al perímetro de Internet pueden residir en un switch de la capa de distribución que también agrega la conectividad de la capa de acceso LAN. Esto también se conoce núcleo fusionado, porque la distribución sirve como la capa de agregación de capa 3 para todos los dispositivos.

Figura 4 - Diseño de dos capas: la capa de distribución funciona como núcleo fusionado



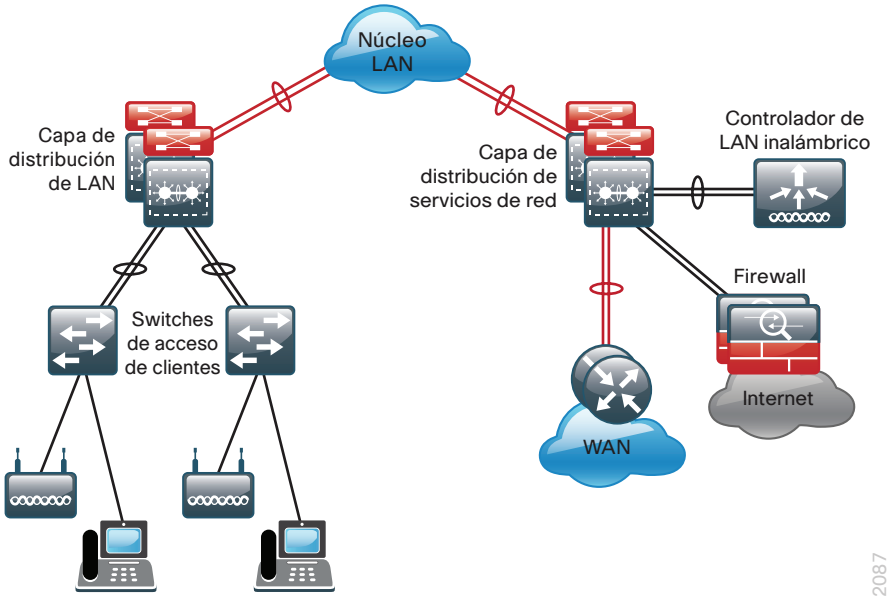
Diseño de tres capas

Los diseños de LAN más grandes requieren una capa de distribución exclusiva para los servicios basados en la red frente a la necesidad de compartir la conectividad con los dispositivos de la capa de acceso. A medida que la densidad de los routers WAN, los controladores WAAS, los dispositivos del perímetro de Internet y los controladores LAN inalámbricos crece, la capacidad de conectarse a un solo switch de la capa de distribución se hace difícil de administrar. Existe una cantidad de factores que impulsan el diseño de red LAN con diversos módulos de capa de distribución:

- La cantidad de puertos y ancho de banda del puerto que la plataforma de la capa de distribución puede proporcionar afecta el rendimiento y desempeño de la red.
- La capacidad de recuperación de la red es un factor cuando todos los servicios LAN y basados en la red dependen de una única plataforma; independientemente del diseño de dicha plataforma, puede presentar un punto de falla único o un gran e inaceptable dominio de fallas.
- La frecuencia y el control de cambios afectan a la capacidad de recuperación. Cuando todas las LAN, WAN y demás servicios de red se consolidan en una sola capa de distribución, los errores de configuración u operativos pueden afectar a todo el funcionamiento de la red.
- La dispersión geográfica de los switches de acceso LAN entre distintos edificios en un campus más grande exigiría más interconexiones de fibra óptica a un núcleo fusionado único.

Al igual que la capa de acceso, la capa de distribución también ofrece calidad de servicio (QoS) para flujos de aplicaciones a fin de garantizar que las aplicaciones críticas y las aplicaciones multimedia se desempeñen tal como se diseñaron.

Figura 5 - Diseño de tres capas con una capa de distribución de servicios de red



Plataformas de capa de distribución

La Guía de diseño para la tecnología LAN por cable en campus es compatible con los siguientes switches de Cisco como plataformas de capa de distribución:

- Switches Cisco Catalyst de la serie 6500 con Supervisor Engine 2T
- Switches Cisco Catalyst de la serie 6880-X
- Switches Cisco Catalyst de la serie 4500-X
- Switches Cisco Catalyst de la serie 4507R+E
- Switches Cisco Catalyst de la serie 3750-X

Capa de núcleo central

En un entorno de LAN grande con frecuencia surge la necesidad de contar con varios switches de capa de distribución. Uno de los motivos es que cuando los switches de la capa de acceso se ubican en varios edificios geográficamente dispersos, puede ahorrarse la instalación de fibra óptica –potencialmente costosa– entre los edificios mediante la colocación de un switch de capa de distribución en cada uno de esos edificios. Dado que las redes crecen más allá de las tres capas de distribución en una sola ubicación, las organizaciones deberían usar una capa de núcleo central para optimizar el diseño.

Otro motivo para usar varios switches de capa de distribución es cuando la cantidad de switches de capa de acceso que se conectan a una sola capa de distribución excede los objetivos de rendimiento del diseñador de redes. En un diseño modular y escalable, puede colocar capas de distribución para el centro de datos, conectividad WAN o servicios periféricos de Internet.

En entornos en los que existen varios switches de capa de distribución próximos entre sí y en los que la fibra óptica ofrece capacidad de interconexión de ancho de banda de alta velocidad, la capa de núcleo central reduce la complejidad de la red, tal como se muestra en las dos siguientes figuras.

Figura 6 - Topología LAN con una capa de núcleo central

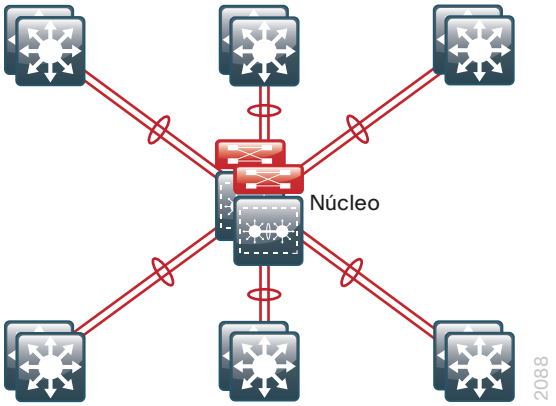
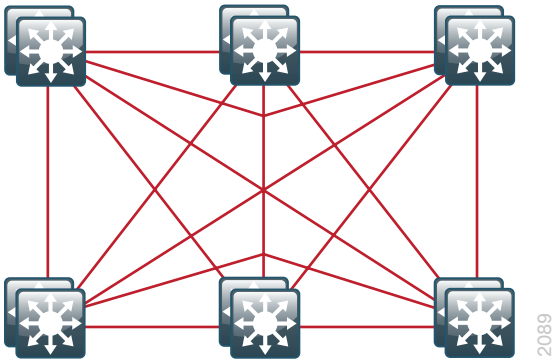


Figura 7 - Topología LAN sin una capa de núcleo central



La capa de núcleo central de la LAN es una pieza fundamental de la red escalable y, aun así, es una de las más simples de diseñar. La capa de distribución aporta los dominios de control y fallas, y el núcleo central representa la conectividad ininterrumpida, 24 horas al día, los 7 días de la semana todos los días del año, entre ellos; las organizaciones deben contar con esto en entornos comerciales modernos en los que la conectividad a los recursos para realizar negocios sea crucial.

Cuando se usan los switches Cisco Catalyst de la serie 6800 o de la serie 6500, la alternativa preferida es un diseño con núcleo central Catalyst VSS de Capa 3, que generalmente usa dos plataformas administradas y configuradas de forma independiente. La conectividad hacia y desde el núcleo es solo de Capa 3, lo que fomenta mejor estabilidad y recuperabilidad.

Plataformas de capa de núcleo central

La Guía de diseño para la tecnología LAN por cable en campus es compatible con los siguientes switches de Cisco como plataformas para la capa de núcleo central:

- Switches Cisco Catalyst de la serie 6807-XL con Cisco Catalyst 6500 Supervisor Engine 2T
- Switches Cisco Catalyst de la serie 6500 con Cisco Catalyst 6500 Supervisor Engine 2T

Calidad de servicio (QoS)

Debido a que el tráfico de comunicación en tiempo real es muy sensible a las demoras y caídas, la red debe garantizar que este tipo de tráfico se administre con prioridad, de manera tal que el flujo de audio o video no se vea interrumpido. Calidad de servicio (QoS) es la tecnología que responde a esta necesidad.

QoS permite a una organización definir distintos tipos de tráfico y crear una gestión más determinista del tráfico en tiempo real. QoS es útil en particular para manejar congestiones, en donde un canal de comunicaciones completo puede impedir que flujos de voz o video sean inteligibles del lado receptor. La congestión es común cuando los enlaces tienen sobresuscripción por agregación de tráfico de una cantidad de dispositivos y, también, cuando el tráfico en un enlace a un dispositivo proviene de enlaces de carga con mayor ancho de banda. En lugar de crear ancho de banda, QoS toma ancho de banda de una clase y lo asigna a otra clase.

En la Guía de diseño para la tecnología de LAN cableada en campus, Cisco mantuvo los perfiles de QoS lo más simples posible y a la vez garantizó la compatibilidad para aplicaciones que necesitan una distribución especial. Este enfoque establece un marco de trabajo modular, escalable y sólido para implementar QoS en toda la red.

Los objetivos principales de implementar QoS en la red son los siguientes:

- Servicio de distribución de comunicaciones acelerado para aplicaciones compatibles en tiempo real.
- Continuidad de los negocios para aplicaciones cruciales para el negocio.
- Equidad entre el resto de las aplicaciones cuando ocurren congestiones.
- Quitar prioridad a aplicaciones que se ejecutan en segundo plano y a aplicaciones no comerciales orientadas al entretenimiento, de manera tal que no retrasen las aplicaciones interactivas o cruciales para el negocio.
- Un perímetro de confianza alrededor de la red para garantizar que los usuarios no puedan inyectar sus propios valores arbitrarios y para permitir que la organización confíe en el tráfico marcado a través de la red.

A fin de alcanzar estos objetivos, el diseño implementa QoS en toda la red, de la siguiente manera:

- Establece una cantidad limitada de clases de tráfico (es decir, de una a ocho clases) dentro de la red que necesitan administración especial (por ejemplo, voz en tiempo real, video en tiempo real, datos de alta prioridad, tráfico interactivo, tráfico por lotes y clases predeterminadas).
- Clasifica las aplicaciones en las clases de tráfico.
- Aplica administración especial a las clases de tráfico para lograr el comportamiento de red pretendido.

Diseño de LAN por cable adicionales

Otras guías de CVD, validadas en el entorno de la Guía de diseño para la tecnología de la LAN cableada, se encuentran disponibles; estas se enfocan en la supervisión y la administración de la red del campus.

Administración de dispositivos con Cisco Secure ACS

Sin un punto de aplicación de políticas de identidad y acceso centralizado, es difícil poder garantizar la confiabilidad de una red a medida que la cantidad de dispositivos y administradores crece.

Cisco Secure Access Control System (ACS) funciona como servidor de autenticación, autorización y administración (AAA o triple A) centralizado que combina autenticación de usuario, control de acceso del administrador y el usuario y control de políticas en una sola solución. Cisco Secure ACS usa un modelo de política basado en reglas que hace posibles políticas de seguridad que garantizan privilegios de acceso basado en diferentes características y condiciones, además de la identidad de un usuario.

Las funcionalidades de un servidor Cisco Secure ACS complementado con una configuración AAA en los dispositivos de red reduce los problemas administrativos en torno al hecho de tener información de cuenta local estática en cada dispositivo. Cisco Secure ACS puede proporcionar control de autenticación centralizado, lo que permite que la organización otorgue o revoque rápidamente el acceso para un usuario en cualquier dispositivo de red.

La asignación de usuarios basada en reglas a grupos de identidad puede realizarse según la información disponible en un directorio externo o un almacén de identidades, como Microsoft Active Directory. Los dispositivos de red pueden categorizarse en diversos grupos de dispositivos, los que pueden funcionar como una jerarquía según características tales como ubicación, fabricante, o rol en la red. La combinación de identidad y grupos de dispositivos le permite crear fácilmente reglas de autorización que definen los administradores de redes que pueden autenticar determinados dispositivos.

Estas mismas reglas de autorización dan lugar a una autorización de nivel de privilegio que puede usarse para dar acceso limitado a los comandos de un dispositivo. Por ejemplo, una regla puede dar a los administradores de redes acceso completo a todos los comandos o limitar a los usuarios de mesa de ayuda a los comandos de supervisión.

La Guía de diseño para administración de dispositivos con la tecnología Cisco Secure ACS se encuentra disponible en:

www.cisco.com/go/cvd/campus

Cisco Network Analysis Module

Las empresas confían en que las aplicaciones corporativas les permitan garantizar operaciones eficientes y obtener ventajas competitivas. Al mismo tiempo, TI se encuentra ante el desafío de administrar la distribución de aplicaciones en un entorno dinámico y distribuido. Debido a las nuevas demandas comerciales, es crucial que los negocios cuenten con visibilidad integral de la red y las aplicaciones para lograr una mejor eficacia operativa y administración exitosa de la experiencia general del usuario final.

Puede usar el producto Cisco Prime Network Analysis Module (NAM) para mantener y mejorar la eficacia operativa. Cisco Prime NAM incluye características fundamentales que le permiten analizar y solucionar los problemas de desempeño de las aplicaciones de voz, detectar paquetes continuamente y ver las tareas previas y posteriores a la optimización de WAN.

Cisco Prime NAM, parte de la solución general de Cisco Prime, es un producto que:

- Ofrece instrumentación de red avanzada en la capa de servicios de usuario para admitir servicios de datos, voz y video.
- Permite a los administradores, gerentes e ingenieros de red obtener visibilidad de la capa de servicios de usuario con un enfoque simple de flujo de trabajo; desde la supervisión del estado general de la red al análisis de una variedad de métricas detalladas y la solución de problemas con detalles a nivel de paquete.
- Es compatible con las capas de servicios de red, como optimización de aplicaciones.
- Ofrece una combinación versátil de análisis de tráfico en tiempo real, análisis históricos, funcionalidades de detección de paquetes y la capacidad de medir demoras percibidas por el usuario en la red WAN.
- Ofrece una capa uniforme de instrumentación que recopila datos a partir de varias fuentes y, luego, analiza y presenta la información. Esta información está disponible a través de una interfaz gráfica de usuario en línea y también puede exportarla a aplicaciones externas.

La Guía de diseño para la tecnología de Network Analysis Module ofrece opciones de diseño para la implementación de Cisco NAM en su red del campus.

Diseño de switch para distribución de bloque de servicios

El módulo de análisis de red Cisco Catalyst de la serie 6500 (NAM-3) se implementa en el switch Cisco Catalyst de la serie 6500 que se encuentra en la distribución del bloque de servicios en el campus. El módulo NAM-3 aprovecha la integración de la placa de circuito mediante simplificación de la capacidad de administración y reducción del costo total de propiedad, del espacio físico de la red y del espacio en rack. Cisco NAM-3 supervisa el tráfico en el switch Cisco Catalyst 6500 mediante dos puertos de datos internos de 10 Gigabit.

El diseño de switch de distribución del bloque de servicios usa el módulo Cisco NAM-3 para lo siguiente:

- Calidad de voz y vídeo en el campus.
- Uso de tráfico y desempeño de aplicaciones entre el campus y el centro de datos y entre el campus y el sitio remoto.
- Detección de paquetes para solución de problemas.
- Supervisión de URL para políticas de filtrado en línea, calidad de servicio (QoS) para aplicación de políticas de QoS.
- Análisis de aplicaciones y de host, por ejemplo, todo el tráfico en una interfaz o en una VLAN.

Diseño de dispositivo para bloque de aplicaciones

En este diseño, el dispositivo Cisco Prime NAM 2320 se implementa en la distribución del bloque de servicios conectado a los switches Cisco Catalyst de la serie 6500. Cisco Prime NAM 2320 cuenta con la flexibilidad para conectarse a cualquier plataforma (incluidas las plataformas de las series Catalyst y Nexus) que sea compatible con los analizadores de puertos SPAN/RSPAN/ERSPAN para visibilidad del switch local. El dispositivo Cisco Prime NAM 2320 supervisa el tráfico en switches mediante dos interfaces de puerto de datos de 10 Gigabit.

Diseño de dispositivo para centro de datos

El diseño de dispositivo para centro de datos usa el dispositivo Cisco Prime NAM 2320 para lo siguiente:

- Uso de tráfico y desempeño de las aplicaciones entre el centro de datos y el campus, y entre el centro de datos y el sitio remoto.
- Análisis de optimización de WAN y solución de problemas.
- Detección de paquetes para solución de problemas.
- QoS para aplicación de políticas de QoS.
- Análisis de aplicaciones y de host, por ejemplo, todo el tráfico en una interfaz o en una VLAN.

Diseño para sitio remoto

Cisco Prime NAM en Cisco Services Ready Engine (SRE) de la serie 710 o 910 como parte de los routers de servicios integrados de segunda generación (ISR G2) se implementa en el sitio remoto, lo que le permite supervisar, medir e informar sobre el estado de la red al nivel del sitio remoto.

El diseño para sitio remoto usa Cisco Prime NAM SRE para lo siguiente:

- Calidad de voz y video en el sitio remoto.
- Uso de tráfico y rendimiento de las aplicaciones entre el sitio remoto y el centro de datos, entre el sitio remoto y el campus y entre sitio remoto y sitio remoto.
- Detección de paquetes para solución de problemas.
- Supervisión de URL para políticas de filtrado en línea, QoS para aplicación de políticas QoS.
- Análisis de aplicaciones y de host, por ejemplo, todo el tráfico en una interfaz o en una VLAN.

Supervisión de aplicaciones en tiempo real e histórica

El módulo Cisco Prime NAM supervisa el tráfico en tiempo real y ofrece una variedad de análisis. Ofrece análisis históricos a pedido de los datos recopilados. Esta categoría de supervisión incluye el reconocimiento de aplicaciones, análisis de principales conversaciones, hosts, protocolos, puntos de código de servicio diferenciados y redes VLAN.

Prestación de servicios y aplicaciones con inteligencia de desempeño de las aplicaciones

A fin de evaluar con precisión la experiencia del usuario final, el módulo Cisco Prime NAM ofrece mediciones de inteligencia de desempeño de las aplicaciones (API). Estas mediciones analizan las solicitudes y los reconocimientos de cliente/servidor por TCP para proporcionar estadísticas de tiempo de respuesta sensibles a las transacciones, como la demora de cliente, demora del servidor, demora de la red, tiempos de transacción y estado de conexión Estos datos pueden ayudarlo a aislar los problemas de las aplicaciones de la red o del servidor. También puede ayudarlo a diagnosticar rápidamente la causa de la demora y solucionar el problema, a la vez que se minimiza el impacto sobre el usuario final.

Las mediciones de API pueden ayudar al personal sobrecargado de TI a resolver problemas de desempeño de las aplicaciones; a analizar y estimar tendencias en el comportamiento de las aplicaciones; a identificar oportunidades de consolidación de las aplicaciones; a definir y garantizar los niveles de servicio; y a ejecutar supervisiones previas y posteriores a la implementación sobre la optimización de las aplicaciones y los servicios de aceleración.

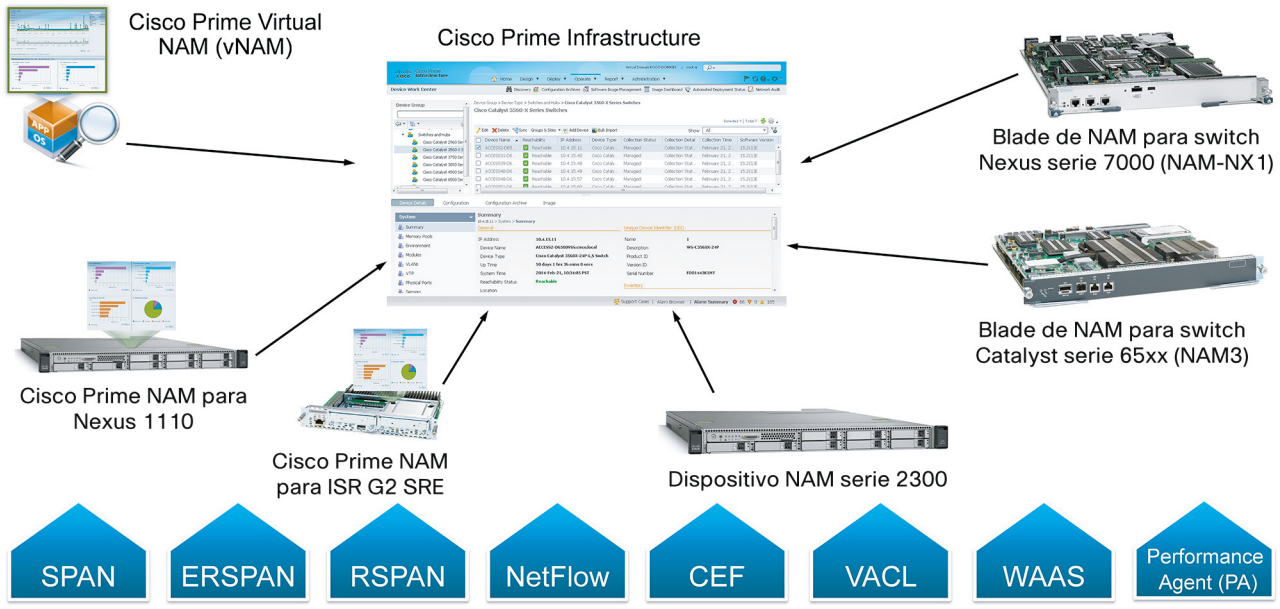
Detección y resolución simplificadas de problemas

Con Cisco Prime NAM puede establecer umbrales y alarmas para varios parámetros de red (p. ej.: aumento en el uso, severas demoras en la respuesta de las aplicaciones, degradación de la calidad de voz) y alertar sobre posibles problemas. Cuando se activan una o más alarmas, Cisco Prime NAM puede enviar una alerta por correo electrónico, generar un syslog o una notificación de SNMP y automáticamente detectar y decodificar el tráfico relevante para poder resolver el problema. Mediante el uso de un navegador, el administrador puede realizar manualmente detecciones y ver decodificaciones a través de la GUI del analizador de tráfico mientras los datos aún se están detectando. La funcionalidad de detección y decodificación de Cisco Prime NAM ofrece detalles e información sobre análisis de datos mediante el uso de detecciones basadas en la activación, filtros, decodificaciones, análisis de detección y un conjunto de herramientas de escaneo de errores para detectar y resolver rápidamente áreas de problemas.

Funcionalidades de exportación y fuentes de datos de Cisco Prime NAM

En el contexto del módulo Cisco Prime NAM, un recurso de datos se refiere a una fuente de tráfico para la cual todo el flujo o resúmenes de datos de ese flujo se envían a Cisco Prime NAM para supervisión. Cisco Prime NAM puede supervisar una variedad de fuentes de datos y computar las métricas correspondientes. En la siguiente figura se muestra una instantánea de todas las posibles fuentes de datos y, también, de los distintos mecanismos de exportación que admite el módulo.

Figura 8 - Fuentes de datos para Cisco Prime NAM



En esta figura se muestra el rol de Cisco Prime NAM como herramienta de la capa de mediación: recopila y analiza los datos de red a partir de diversas fuentes y muestra los resultados en una consola de informes y administración integrada, por ejemplo, una GUI en línea de NAM; también ofrece datos a Cisco Prime Infrastructure mediante la interfaz de transferencia de estado representacional (REST)/XML.

Debido a que Cisco Prime NAM combina un analizador de tráfico (distintos factores de forma) y una consola de generación de informes, el usuario puede aprovechar el módulo NAM como una solución para rendimiento de las aplicaciones de red independiente. Si se implementan varios módulos NAM en la red, por ejemplo, NAM en el centro de datos, en el campus y en sitios remotos, entonces Cisco Prime Infrastructure ofrece una solución que permite al usuario detectar, configurar y administrar los módulos NAM. Entre los ejemplos de Prime Infrastructure como administración multi-NAM se incluyen la configuración centralizada de protocolo de tiempo de red (NTP), configuración del Sistema de nombres de dominio (DNS) e ID de aplicaciones, administración centralizada de la imagen de NAM, detección de paquetes centralizada con activaciones de alarmas, y un único tablero para la consolidación de toda la información de tráfico de NAM.

La Guía de diseño para la tecnología de Network Analysis Module se encuentra disponible en:

www.cisco.com/go/cvd/campus

Cisco Prime Infrastructure

A medida que las redes y la cantidad de servicios que admiten siguen progresando, las responsabilidades de los administradores de redes para mantener y mejorar su eficacia y productividad también crecen. El uso de una solución para administración de redes puede hacer posible y mejorar la eficacia operativa de los administradores de redes.

Cisco Prime Infrastructure es una sofisticada herramienta administrativa que permite dar soporte a la administración integral de elementos para tecnologías y servicios de red que son fundamentales para el funcionamiento de una organización. Esta herramienta combina la funcionalidad de administración de redes con la forma en que los administradores de redes hacen su trabajo. Cisco Prime Infrastructure proporciona una GUI en línea intuitiva a la que puede accederse desde cualquier lugar de la red y le ofrece una vista completa del uso y el desempeño de la red.

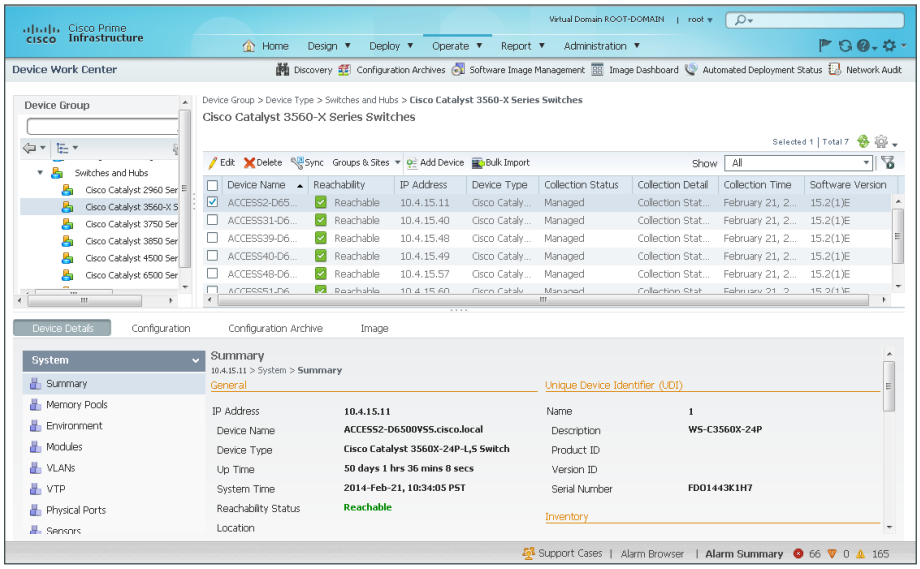
Gracias a la red de campus y los servicios que admite, Cisco Prime Infrastructure puede jugar un rol fundamental en las operaciones de red del día a día.

Centro de trabajo de dispositivos

La Infraestructura Cisco Prime incluye el centro de trabajo de dispositivos. Entre algunas de las características que aporta este Centro de trabajo de dispositivos se destacan las siguientes:

- **Detección:** crea y mantiene un inventario actualizado de los dispositivos administrados, incluso información de imagen de software y detalles de la configuración del dispositivo.
- **Archivos de configuración:** mantiene un archivo activo de diversas iteraciones de archivos de configuración para cada dispositivo administrado.
- **Administración de imagen de software:** habilita un administrador de red para importar imágenes de software desde Cisco.com, dispositivos administrados, URL, o sistemas de archivo, y luego las distribuye a un solo dispositivo o a un grupo de dispositivos.

Figura 9 - Centro de trabajo de dispositivos



Tareas y plantillas de configuración

Con el uso de la función Tareas de configuración para aplicar plantillas de configuración a varios dispositivos, los administradores pueden ahorrarse muchas horas de trabajo. Cisco Prime Infrastructure ofrece un conjunto de plantillas lista para usar, con las que puede crear una tarea de configuración, proporcionando valores específicos del dispositivo según sea necesario. Para otras necesidades de configuración, Cisco Prime Infrastructure le permite definir sus propias plantillas.

Alarmas, eventos y mensajes de syslog

Cisco Prime Infrastructure ofrece una función de alarmas y eventos, una pantalla unificada con diagnósticos detallados. La función proporciona información procesable y la capacidad de abrir automáticamente solicitudes de servicio en Cisco Technical Assistance Center (TAC).

Generación de informes

Cisco Prime Infrastructure le ofrece un único punto de lanzamiento para todos los informes que puede configurar, programar y ver. La página Report Launch Pad le da acceso a más de 100 informes; puede personalizar cada uno según sea necesario.

Compatibilidad con CleanAir

Cisco Prime Infrastructure admite los puntos de acceso inalámbricos compatibles con CleanAir, lo que permite que los administradores vean eventos de interferencia. Para obtener más información sobre CleanAir, consulte la sección CleanAir inalámbrica en el campus.

Compatibilidad con Network Analysis Module

Cisco Prime Infrastructure es compatible con las funcionalidades de administración y generación de informes para los productos Módulo de análisis de redes de Cisco (Cisco NAM). Para obtener más información sobre los productos Cisco NAM, consulte la sección Cisco Network Analysis Module.

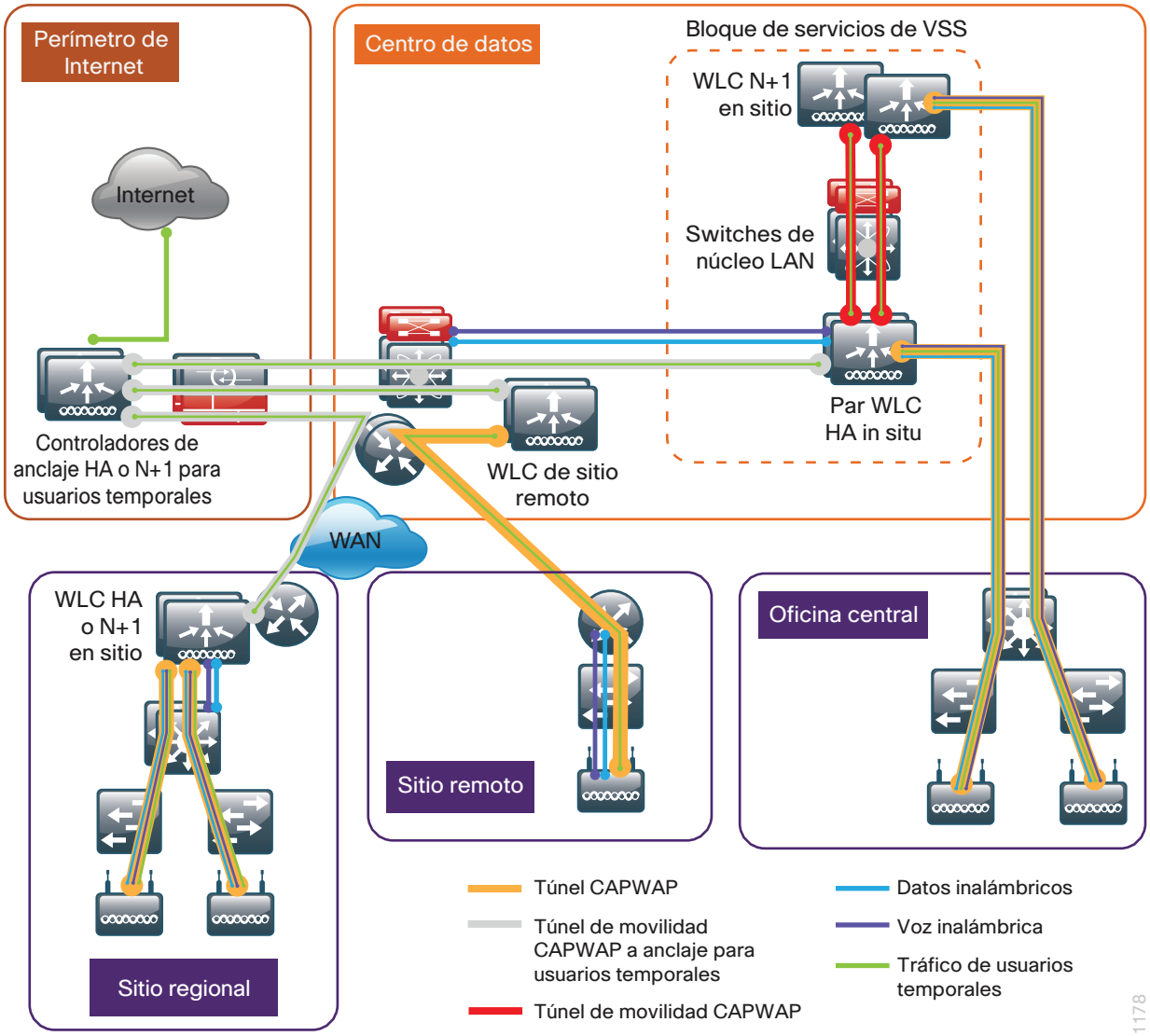
Resumen de diseño de la red LAN inalámbrica del campus

La Guía de diseño para la tecnología LAN inalámbrica del campus ofrece conectividad de voz y datos ubicua para empleados y proporciona acceso a Internet inalámbrica para usuarios temporales. Independientemente de su ubicación dentro de la organización (en campus grandes o en sitios remotos), los usuarios de la red inalámbrica tendrán la misma experiencia cuando se conecten a servicios de voz, video y datos.

Entre los beneficios de la Guía de diseño para la tecnología LAN inalámbrica del campus se incluyen:

- **Mayor productividad mediante acceso a la red seguro e independiente de la ubicación:** mejoras medibles en la productividad y comunicación.
- **Flexibilidad de red adicional:** ubicaciones difíciles de conectar por cable se conectan de manera inalámbrica, sin construcciones costosas.
- **Implementación rentable:** adopción de tecnologías virtualizadas dentro del diseño inalámbrico general.
- **Fácil administración y operación:** control centralizado de un entorno inalámbrico distribuido, desde un panel de interfaz único.
- **Implementación plug-and-play:** aprovisionamiento automático cuando se conecta un punto de acceso a la red cableada de soporte.
- **Diseño tolerante a fallas y flexible:** conectividad inalámbrica confiable en entornos críticos, y administración completa del espectro RF.
- **Soporte para usuarios inalámbricos:** modelos de diseño del tipo BYOD (Bring Your Own Device).
- **Transmisión eficiente del tráfico de multidifusión:** soporte para diversas aplicaciones de comunicación en grupo, como vídeo y función de pulsar para hablar.

Figura 10 - Descripción general de la red inalámbrica



La Guía de diseño para la tecnología de LAN inalámbrica del campus se basa en dos componentes principales:

- Controladores LAN inalámbricos Cisco
- Puntos de acceso ligero Cisco

Cisco Wireless LAN Controllers

La Guía de diseño para la tecnología de LAN inalámbrica del campus es un diseño inalámbrico basado en controladores, que simplifica la administración de redes gracias al uso de controladores LAN inalámbricos Cisco (WLC) para centralizar la configuración y el control de los puntos de acceso inalámbricos. Este enfoque permite que la red LAN inalámbrica (WLAN) funcione como una red de información inteligente y que admita servicios avanzados. A continuación le presentamos algunos de los beneficios de este diseño basado en controladores:

- **Menores gastos operativos:** habilita configuraciones automatizadas para puntos de acceso ligeros; fácil diseño del canal y configuraciones de alimentación y administración en tiempo real, incluso la identificación de vacíos de RF para optimizar el entorno de RF; movilidad transparente entre diversos puntos de acceso dentro del grupo de movilidad; una vista integral de la red que da soporte a las decisiones sobre escala, seguridad y operaciones en general.
- **Mejor retorno de la inversión:** habilita instancias virtualizadas del controlador LAN inalámbrico, lo que reduce el costo total de propiedad gracias a que aprovecha su inversión en virtualización.
- **Escalamiento más simple con diseño óptimo:** permite que la red escale bien, ya que admite un diseño de modo local para entornos del campus y un diseño de Cisco FlexConnect para sitios remotos eficientes.
- **Conmutación activa con alta disponibilidad:** hace posible la conectividad sin interrupciones a dispositivos cliente inalámbricos durante una falla en el controlador LAN inalámbrico.

Los controladores LAN inalámbricos Cisco son los encargados de las funciones WLAN en todo el sistema, como políticas de seguridad, prevención de intrusiones, administración de RF, QoS y movilidad Trabajan en conjunto con los puntos de acceso ligeros Cisco para admitir aplicaciones inalámbricas cruciales para el negocio. Desde servicios de voz y datos hasta localización de ubicaciones, los controladores LAN inalámbricos Cisco proporcionan el control, la escalabilidad, la seguridad y la confiabilidad que los administradores de redes necesitan para crear redes inalámbricas escalables y seguras.

Si bien un controlador autónomo puede admitir puntos de acceso ligeros en varios pisos y edificios al mismo tiempo, debe implementar los controladores en pares para tener recuperabilidad. Existen distintas formas de configurar la recuperabilidad de un controlador; la más simple es usar un modelo primario/secundario en el que todos los puntos de acceso en el sitio prefieren unirse al controlador primario y solo se unen al secundario durante una falla.

Los siguientes controladores se incluyen en la Guía de diseño de la tecnología LAN inalámbrica del campus:

- Controlador LAN inalámbrico Cisco de la serie 2500
- Controlador LAN inalámbrico Cisco de la serie 5500
- Cisco Wireless Services Module 2 (WiSM2)
- Controlador LAN inalámbrico Cisco de la serie 5760
- Controlador LAN inalámbrico virtual Cisco
- Controlador de la nube Cisco Flex de la serie 7500

Dado que la flexibilidad de licencias del software le permite agregar puntos de acceso adicionales a medida que los requisitos de su empresa cambian, puede elegir los controladores que darán soporte a sus necesidades a largo plazo, pero comprará licencias para puntos de acceso incrementales solo cuando las necesite.

Puntos de acceso ligero Cisco

En la arquitectura de red inalámbrica unificada de Cisco, los puntos de acceso son *ligeros*. Es decir que no pueden actuar independientemente de un controlador LAN inalámbrico. A medida que el punto de acceso se comunica con el controlador LAN inalámbrico, descarga su configuración y sincroniza su software o imagen de firmware.

Los puntos de acceso ligeros Cisco trabajan en conjunto con el controlador LAN inalámbrico Cisco para conectar dispositivos inalámbricos a la red LAN y, al mismo tiempo, admiten el reenvío simultáneo de datos y funciones de supervisión en el aire. La Guía de diseño de la tecnología LAN inalámbrica del campus está basada en puntos de acceso inalámbricos Cisco de segunda generación, que ofrecen cobertura resistente con hasta nueve veces más desempeño que las redes 802.11a/b/g. Los siguientes puntos de acceso se incluyen en la Guía de diseño de la tecnología LAN inalámbrica del campus:

- Puntos de acceso Cisco Aironet de la serie 1600
- Puntos de acceso Cisco Aironet de la serie 2600
- Puntos de acceso Cisco Aironet de la serie 3600
- Puntos de acceso Cisco Aironet de la serie 3700

La compatibilidad con dos tecnologías clave diferencia a los puntos de acceso incluidos en la Guía de diseño de la tecnología LAN inalámbrica de Cisco:

- **Tecnología Cisco CleanAir:** proporciona a los administradores de TI visibilidad del espectro inalámbrico para que puedan manejar la interferencia de RF y evitar tiempos de inactividad inesperados. Cisco CleanAir brinda protección de rendimiento para las redes 802.11n. Esta inteligencia a nivel del chip crea una red inalámbrica con capacidad de autorreparación y autooptimización que mitiga el impacto de la interferencia inalámbrica. Para obtener más información sobre Cisco CleanAir, consulte la sección CleanAir inalámbrica en el campus.
- **802.11ac:** la especificación IEEE 802.11ac Wave 1 aporta importantes mejoras al rendimiento de la red inalámbrica. Para obtener más información sobre el estándar 802.11ac, consulte las secciones Rendimiento de ancho de banda con 802.11ac y Planificación de canal con 802.11ac.

Tabla 1 - Compatibilidad de puntos de acceso con Cisco CleanAir y IEEE 802.11ac

Puntos de acceso Cisco Aironet	Compatible con Cisco CleanAir	Compatible con 802.11ac
1600	No[1]	No
2600	Sí	No
3600	Sí	Sí[2]
3700	Sí	Sí

[1]Los puntos de acceso Cisco Aironet de la serie 1600 son compatibles con CleanAir Express, que no se incluye en la Guía de diseño de la tecnología LAN inalámbrica del campus.

[2]Los puntos de acceso Cisco Aironet de la serie 3600 son compatibles con el estándar 802.11ac si está instalado el módulo de radio adaptable para 802.11ac Wave 1.

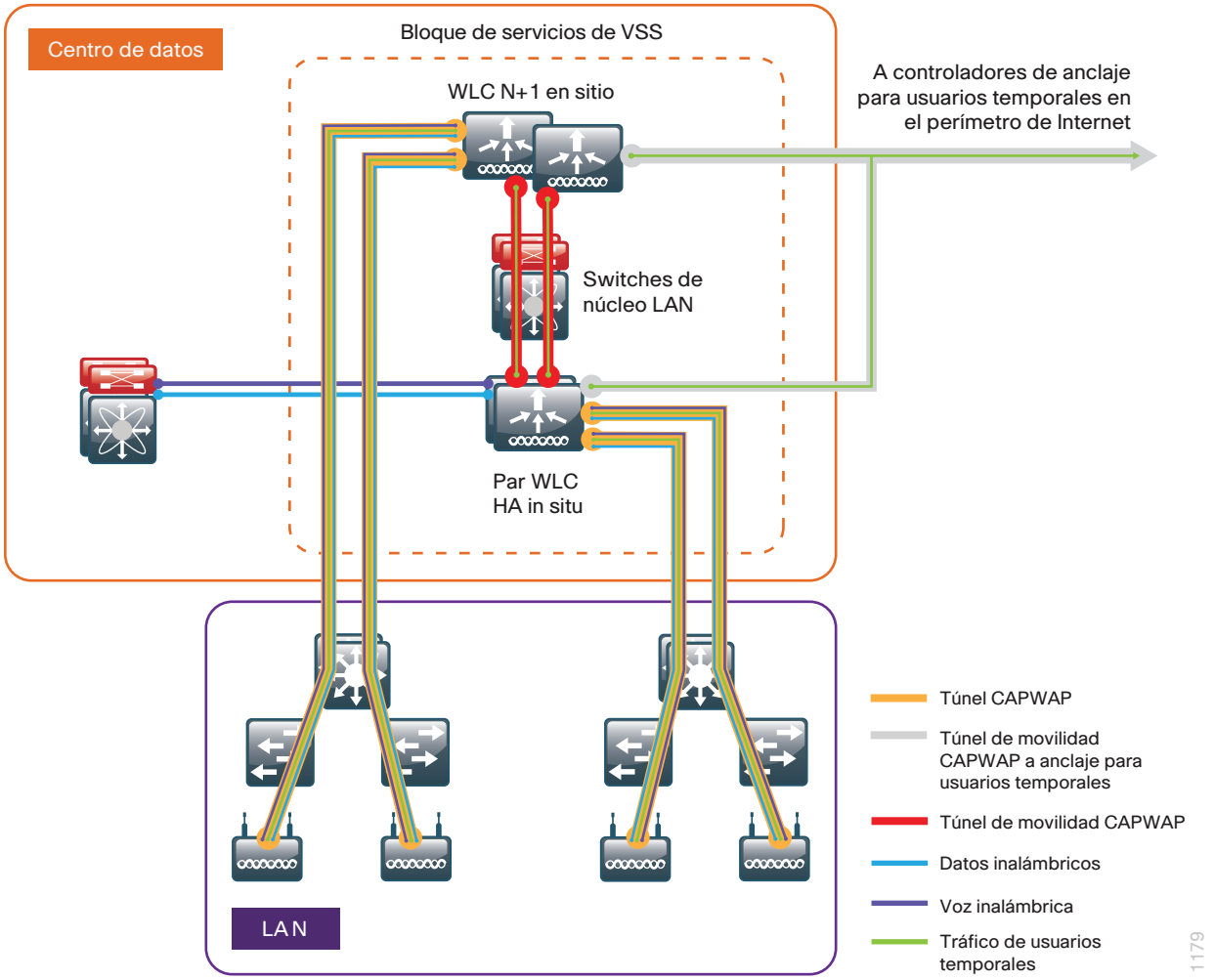
Modelos para diseño inalámbrico

Las redes inalámbricas unificadas de Cisco admiten dos modelos de diseño para el campus: modo local y Cisco FlexConnect.

Modelo de diseño para modo local

En este modelo de diseño, el controlador LAN inalámbrico y los puntos de acceso están ubicados conjuntamente. El controlador LAN inalámbrico puede estar conectado a un bloque de servicios del centro de datos o puede estar conectado a una capa de distribución LAN. Se crea un túnel para el tráfico inalámbrico entre los clientes de LAN inalámbrica y la LAN mediante el uso del protocolo de control y aprovisionamiento de puntos de acceso inalámbricos (CAPWAP) entre el controlador y el punto de acceso.

Figura 11 - Modelo de diseño para modo local



La arquitectura del modo local usa el controlador como punto único para la administración de las políticas de red inalámbrica y seguridad de capa 2. También permite que los servicios se apliquen al tráfico por cable e inalámbrico de manera homogénea y coordinada.

Además de brindar los beneficios tradicionales de un enfoque de red inalámbrica unificada de Cisco, el modelo de diseño para modo local satisface las siguientes demandas del cliente:

- **Movilidad transparente:** permite roaming rápido en el campus, para que los usuarios sigan conectados a su sesión incluso cuando se mueven entre varios pisos o edificios adyacentes con subredes distintas.
- **Capacidad de dar soporte a multimedia interactiva:** mejora la resistencia de la voz con control de admisión de llamadas (CAC) y de multidifusión con la tecnología Cisco VideoStream.
- **Política centralizada:** permite la inspección inteligente mediante el uso de firewalls, así como también inspección de aplicaciones, control de acceso a la red, aplicación de políticas y clasificación precisa del tráfico.

Si **cualquiera** de las siguientes situaciones se da en un sitio, debería implementar un controlador localmente en el sitio:

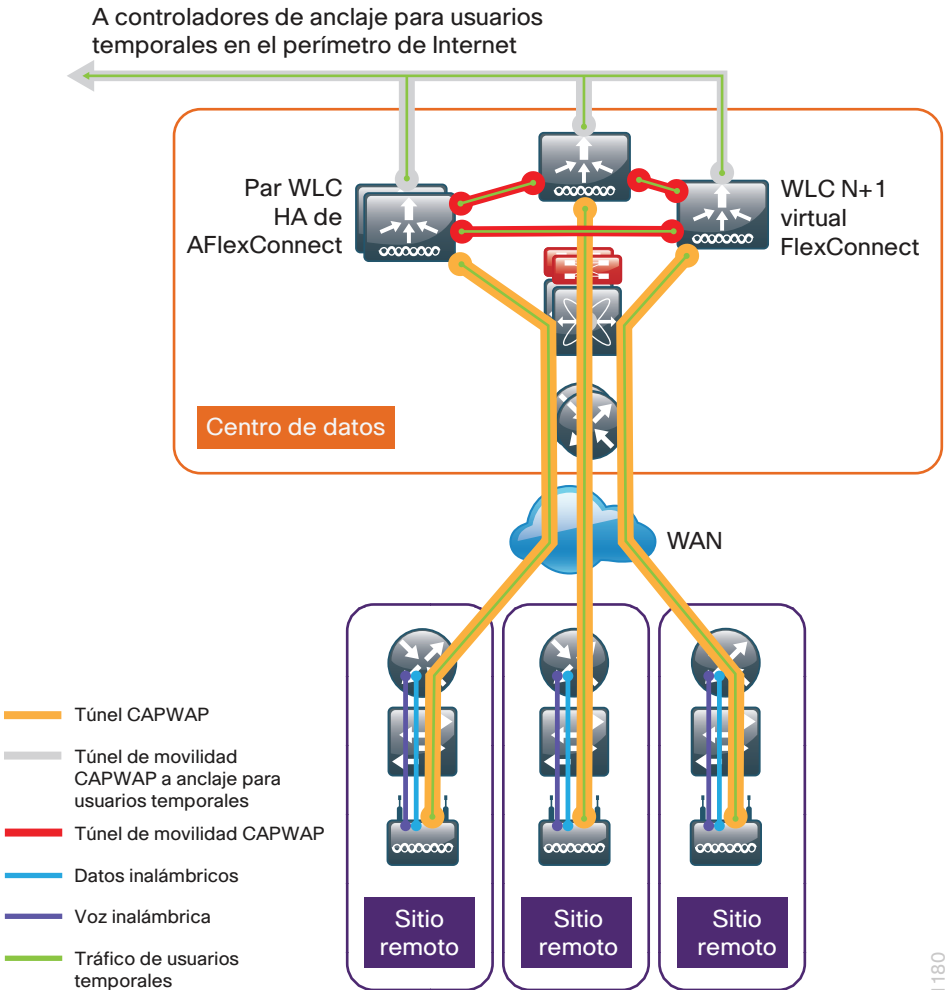
- El sitio tiene un centro de datos.
- El sitio tiene una capa de distribución LAN.
- El sitio tiene más de 50 puntos de acceso.
- El sitio tiene una latencia WAN mayor a los 100 ms de ida y vuelta a un controlador compartido propuesto.

En una implementación de estas características, use un controlador LAN inalámbrico Cisco de las series 2500, 5500 y 5700 o Cisco WiSM2. A efectos de recuperabilidad, la Guía de diseño de la tecnología LAN inalámbrica del campus usa dos o más controladores LAN inalámbricos para el campus. Se pueden agregar controladores LAN inalámbricos adicionales para proporcionar capacidad y recuperabilidad adicionales al diseño.

Modelo de diseño con Cisco FlexConnect

Cisco FlexConnect es una solución de redes inalámbricas para implementaciones de sitio remoto. Permite a las organizaciones configurar y controlar puntos de acceso de sitio remoto desde las oficinas centrales a través de la WAN sin implementar un controlador en cada sitio remoto. El punto de acceso Cisco FlexConnect puede conmutar tráfico de datos de cliente fuera de su interfaz cableada local y usar enlaces troncales 802.1Q para segmentar varias WLAN. La VLAN nativa del enlace troncal se usa para toda la comunicación CAPWAP entre el punto de acceso y el controlador. Este modo de operación se conoce como switching local de FlexConnect y es el modo de operación que se describe en esta guía.

Figura 12 - Modelo de diseño con Cisco FlexConnect



Cisco FlexConnect también puede crear un túnel de tráfico de vuelta al controlador centralizado, que se usa específicamente para el acceso inalámbrico de usuarios temporales.

Puede usar un par controlador compartido o un par controlador exclusivo para implementar Cisco FlexConnect.

En un modelo de controlador compartido, tanto los puntos de acceso configurados para modo local como los de FlexConnect comparten un controlador común. Una arquitectura de controlador compartida necesita que el controlador LAN inalámbrico sea compatible con el switching FlexConnect local y con el modo local. Los controladores LAN inalámbricos que admiten ambas opciones en esta guía CVD son los controladores inalámbricos Cisco de las series 5500 y 2500, y Cisco WiSM2. Si tiene un par controlador de modo local en el mismo sitio que su agregación WAN y si su par controlador cuenta con capacidad adicional suficiente para admitir los puntos de acceso Cisco FlexConnect, puede usar una implementación compartida.

Si no reúne los requisitos para un controlador compartido, puede implementar un par controlador de alta disponibilidad exclusivo usando un controlador de la nube Cisco Flex de la serie 7500, o controladores Cisco de las series 5500 o Cisco WiSM2. Los controladores flexibles duales configurados en un modelo de redundancia N+1 pueden emplearse usando un controlador LAN inalámbrico Cisco de la serie 2500 o el controlador LAN inalámbrico virtual Cisco. El controlador debe residir en el centro de datos.

Si **todas** las siguientes condiciones se dan en un sitio, implemente Cisco FlexConnect en el sitio:

- La LAN del sitio es un switch de capa de acceso individual o una pila de switch.
- El sitio tiene menos de 50 puntos de acceso.
- El sitio tiene una latencia WAN menor a los 100 ms de ida y vuelta a un controlador compartido propuesto.

Alta disponibilidad

A medida que la movilidad ejerce cada vez más influencia en todos los aspectos de nuestras vidas a nivel personal y profesional, la disponibilidad sigue siendo una inquietud prioritaria. La Guía de diseño de la tecnología LAN inalámbrica del campus admite alta disponibilidad mediante el uso de controladores flexibles dentro de un grupo de movilidad común.

Cisco AireOS admite conmutación activa del punto de acceso y conmutación activa de cliente. Estas dos funciones se conocen colectivamente como conmutación activa de alta disponibilidad (HA SSO). Con el uso del rentable modelo de licencia de HA SSO, las implementaciones de red inalámbrica de Cisco pueden mejorar la disponibilidad de la red inalámbrica con tiempos de recuperación del controlador inferiores al segundo durante una interrupción del controlador LAN inalámbrico. Además, HA SSO permite que el controlador LAN inalámbrico flexible ofrezca una licencia rentable como controlador flexible en modo de espera, y hereda automáticamente su recuento de licencia de punto de acceso a partir de su controlador LAN inalámbrico primario. Esto se logra mediante la compra de un controlador flexible en modo de espera usando la SKU de HA disponible para los controladores LAN inalámbricos Cisco de las series 5500 y 7500, y Cisco WiSM2. La compatibilidad para HA SSO dentro de la familia de controladores WiSM2 exige que ambos controladores LAN inalámbricos WiSM2 se implementen de una de las siguientes maneras:

- Dentro de un par de switch Cisco Catalyst de la serie 6500 configurado para operación de sistema de switching virtual (VSS).
- Dentro del mismo chasis del switch Cisco Catalyst de la serie 6500.
- Dentro de un chasis del switch Cisco Catalyst de la serie 6500 distinto cuando la VLAN con redundancia de capa 2 se extiende.

La configuración y las actualizaciones de software del controlador LAN inalámbrico primario se sincronizan automáticamente con el controlador LAN inalámbrico en modo de espera.

En la siguiente tabla se muestran los controladores compatibles con la función HA SSO.

Tabla 2 - Compatibilidad con la función de alta disponibilidad

Modelos de WLC de Cisco	HA SSO	Redundancia N+1	Grupo de agregación de enlaces (LAG)
vWLC	No	Sí	Sí (mediante VMWare)
2500	No	Sí	Sí
5500	Sí	Sí	Sí
WiSM2	Sí	Sí	N/D
5760	Sí[1]	Sí	Sí
7500 Flex	Sí	Sí	Sí

[1]El controlador LAN inalámbrico Cisco de la serie 5760 admite conmutación activa del punto de acceso (AP SSO) por medio de un cable de apilamiento.

Soporte de multidifusión

Las aplicaciones de voz y video siguen creciendo a medida que se agregan smartphones, tablets y equipos personales a las redes inalámbricas, en todos los aspectos de nuestra vida diaria. En cada uno de los modelos de diseño inalámbrico, el soporte de multidifusión al que los usuarios están acostumbrados en una red por cable se encuentra disponible en la red inalámbrica. A fin de permitir una distribución eficiente de ciertas aplicaciones con relación una a muchas (p. ej.: comunicaciones por video y por grupos de pulsar para hablar) se necesita contar con multidifusión. Con la ampliación del soporte de multidifusión más allá del que tienen el centro de datos y el campus, los usuarios móviles ahora pueden usar aplicaciones basadas en multidifusión.

La Guía de diseño de la tecnología LAN inalámbrica del campus admite la transmisión de multidifusión para el controlador in situ mediante el uso del modo multidifusión-multidifusión, que usa una dirección IP de multidifusión para comunicar de manera más efectiva flujos de multidifusión con puntos de acceso que hacen que los usuarios inalámbricos se suscriban a un grupo de multidifusión particular. El modo multidifusión-multidifusión se admite en esta CVD mediante el uso de los controladores LAN inalámbricos Cisco de las series 2500, 5500 y 5760, y Cisco WiSM2.

Los sitios remotos que usan el controlador de nube Cisco Flex de la serie 7500 o Cisco xWLC con Cisco FlexConnect en modo de switching local también pueden beneficiarse con el uso de aplicaciones basadas en multidifusión. La multidifusión en sitios remotos aprovecha el soporte subyacente de LAN y WAN del tráfico de multidifusión. Cuando se combinan con puntos de acceso en el modo FlexConnect con switching local, los suscriptores a los flujos de multidifusión reciben el servicio directamente por la red WAN o LAN sin que se coloque una sobrecarga adicional en el controlador LAN inalámbrico.

Selección de banda

Con la aparición de dispositivos de consumo que funcionan en la banda industrial, científica y médica de 2,4 GHz, ha crecido considerablemente el nivel de ruido que da como resultado interferencia. Asimismo, muchos de los dispositivos inalámbricos disponibles hoy son de doble banda y pueden funcionar en la banda de 2,4 GHz o de 5 GHz.

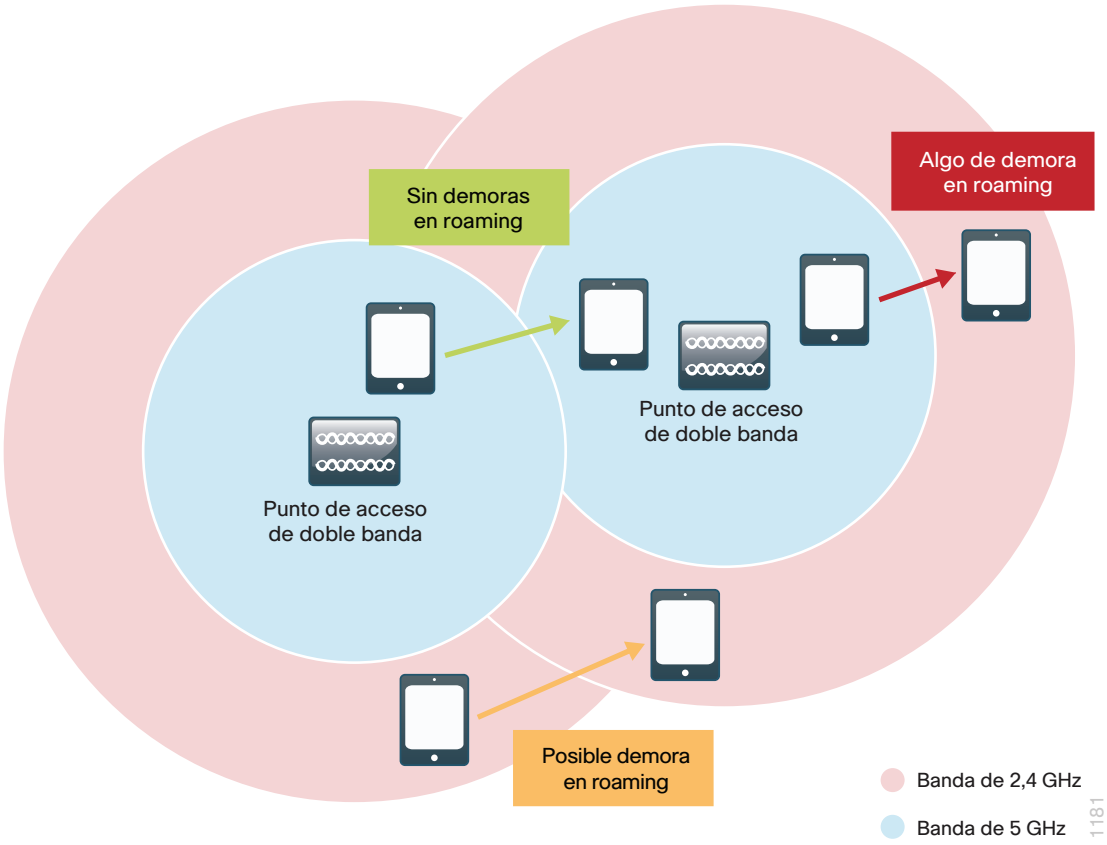
En el caso de los dispositivos de clase empresarial críticos, sería muy ventajoso influenciarlos para que usen la banda de 5 GHz, a fin de que se reduzca en gran medida la interferencia y se obtenga, en consecuencia, una mejor experiencia del usuario.

Cuando los dispositivos inalámbricos de doble banda buscan un punto de acceso, por lo general primero envían una solicitud de sonda a la banda de 2,4 GHz y luego otra a la banda de 5 GHz, unos milisegundos después. Como generalmente la respuesta de la sonda de 2,4 GHz se recibe primera, muchos dispositivos se conectan usando la banda de 2,4 Hz a pesar de que el punto de acceso de 5 GHz está disponible.

La selección de bandas, demora la respuesta a la sonda de 2,4 GHz unos cientos de milisegundos, lo que permite que el punto de acceso determine si el dispositivo inalámbrico es de doble banda. Un dispositivo inalámbrico de doble banda se detecta cuando se recibe una prueba de 2,4 GHz y de 5 GHz del mismo dispositivo. Al demorar la respuesta de prueba de 2,4 GHz y dar prioridad a la respuesta de prueba de 5 GHZ sobre la de 2,4 GHz, es posible influenciar al cliente inalámbrico para que se conecte a la banda preferida de 5 GHz.

No se recomienda el uso de selección de banda para dispositivos de voz y video porque introduce demoras en las respuestas a solicitudes de sonda en la banda de 2,4 GHz. Para los dispositivos de transmisión en tiempo real que pasan de un área de 5 GHz a un área cubierta por 2,4 GHZ, o para clientes que están haciendo roaming entre puntos de acceso de 2,4 GHz, esta demora podría provocar una interrupción momentánea de la conectividad. Con los flujos de tráfico de solo datos, esta demora es insignificante y generalmente no afecta el acceso a las aplicaciones.

Figura 13 - Selección de banda - Efectos en aplicaciones de tiempo real



ClientLink

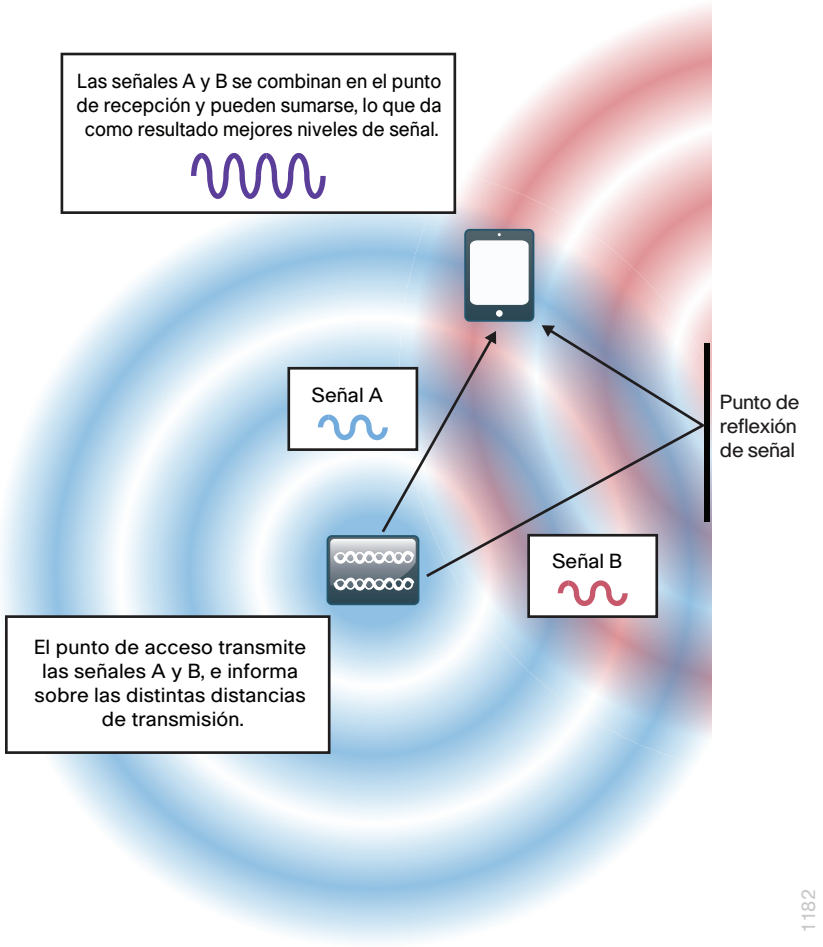
La tecnología de red inalámbrica Cisco ClientLink usa formación de haces para mejorar la relación señal-ruido (SNR) para todos los clientes inalámbricos y no se limita solo a aquellos que admiten el estándar 802.11n. ClientLink hace posible un mejor rendimiento entre el punto de acceso y el cliente ya que reduce las retransmisiones y facilita mayores velocidades de datos. Y gracias a la reducción del tiempo de uso de canal RF para cualquier cliente inalámbrico, el rendimiento general de la red inalámbrica mejora.

En un controlador LAN inalámbrico dado, ClientLink se habilita en toda la banda de radio (como 802.11b o 802.11a) o por punto de acceso.

Tabla 3 - Configuración predeterminada y compatibilidad de ClientLink

Versión de ClientLink	Compatibilidad con puntos de acceso	Configuración predeterminada de ClientLink
3.0	Routers de acceso multiservicio Cisco Aironet de la serie 3700	Habilitado
2.0	Cisco Aironet de las series 1600, 2600 y 3600	Habilitado
1.0	Cisco Aironet de las series 1140, 3500, 1250 y 1260	Deshabilitado

Figura 14 - Optimización de ClientLink



Rendimiento de ancho de banda de 802.11ac

En ningún otro momento de la evolución de la tecnología inalámbrica basada en Wi-Fi se han visto mejoras tan importantes en el rendimiento que con la introducción de 802.11ac. La presentación en 1997 del original estándar 802.11 abrió el paso a un rendimiento de la capa física teórica (PHY) de 2 Mbps. En la actualidad, con la introducción del estándar 802.11ac Wave 1 con tres flujos espaciales (3SS), el rendimiento máximo teórico de la PHY salta a los 1,3 Gbps.

Tabla 4 - Rendimiento de ancho de banda de 802.11ac

Año	Tecnología	Rendimiento teórico de la PHY	Rendimiento esperado del usuario
1997	802.11	2 Mbps	1 Mbps
1999	802.11b	11 Mbps	6 Mbps
1999	802.11a	54 Mbps	25 Mbps
2003	802.11g	54 Mbps	25 Mbps
2003	802.11a/g	54 Mbps	13-25 Mbps
2007	802.11n	450 Mbps c/ 3SS	180-220 Mbps
2013	802.11ac Wave 1	1,3 Gbps c/ 3SS	hasta 750 Mbps
Futuro	802.11ac Wave 2	Rendimiento de 2,4-3,5 Gbps	Por determinar

El rendimiento inalámbrico real es función de una cantidad de variables, como distancia, adaptador inalámbrico, y el entorno general de RF. Además, las celdas mixtas adyacentes que usan el estándar 802.11ac pueden dar como resultado un uso más prolongado del canal debido a la menor velocidad de trasmisión. Cuando se implementa 802.11a/n adyacente con enlace de 40 MHz junto con un canal primario desajustado, no se aprovechan los beneficios del mecanismo Clear Carrier Assessment (Evaluación clara de la portadora).

La especificación 802.11ac Wave 1 incluye numerosas tecnologías, según se detalla a continuación, que son las responsables de esta significativa mejora en el rendimiento.

- 802.11ac se implementa únicamente en la banda más silenciosa y menos cargada de 5 GHz.
- 802.11ac usa a modulación de amplitud en cuadratura 256 (QAM), que habilita 8 bits por símbolo y un aumento cuatro veces mayor en rendimiento. En palabras más sencillas, QAM es una técnica de modulación que usa una fase de formas de onda y amplitud para codificar datos. Con QAM 256 hay 256 símbolos que dan como resultado mayor rendimiento.
- 802.11ac amplía los anchos del canal, para hacer posibles anchos de 20, 40 y 80 MHz en Wave 1; y anchos de 20, 40, 80, 80+80 y 160 MHz en Wave 2.
- La formación de haces, mejorada en 802.11ac Wave 1 e incluida en la tecnología de red inalámbrica Cisco ClientLink, permite que el punto de acceso *conduzca el haz* o dirija una concentración de señales en el receptor que se combinan para aumentar la calidad y el nivel de señal en el receptor. En Wave 2, la formación de haces para varios usuarios permite que un solo punto de acceso transmita a 4 clientes inalámbricos al mismo tiempo y en la misma frecuencia, lo que permite que cada cliente tenga su propia corriente espacial exclusiva.

Planificación del canal 802.11ac

La asignación de canales al usar administración de recursos de radio (RRM) y asignación dinámica de canales (DCA) es mucho más simple que en la época del estándar 802.11. Sin embargo, existen ciertos puntos que se deben tener en cuenta antes de tomar la decisión de enlazar canales. Si bien la Guía de diseño de la tecnología LAN inalámbrica del campus supone una implementación en un entorno nuevo, es posible que los administradores de redes de entornos inalámbricos existentes deseen moverse con más precaución y asegurarse de que se aborden las consideraciones sobre planificación de canales.

Si su entorno se limita a los canales estándar de 20 MHz de amplitud, Cisco sugiere un enfoque en etapas para switching a canales de 80 MHz de amplitud. El paso inicial es habilitar un conjunto de canales de selección dinámica de frecuencias (DFS). El uso de canales DFS requiere que el punto de acceso examine el uso del radar. Si se detecta el radar, el punto de acceso se traslada a otro canal o reduce la potencia de transmisión. Los canales DFS hacen posible un rango más amplio de espectro de RF, sujeto a su dominio regulador. A su vez esto habilita más opciones de entrelazado de canales por DCA.

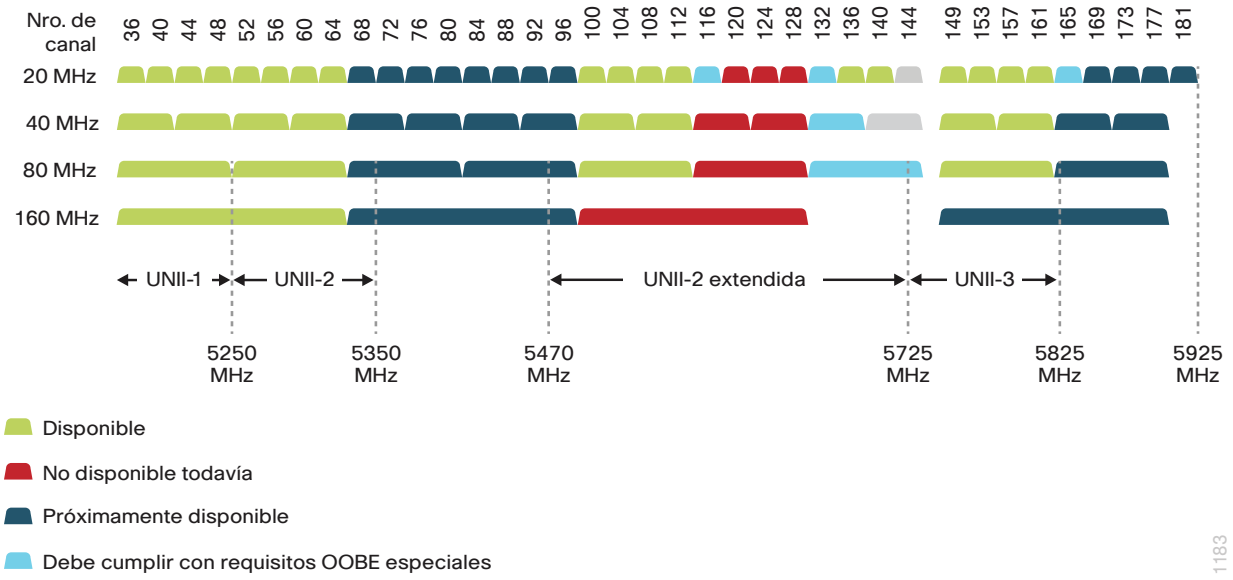
Con los canales DFS habilitados, hay cuatro canales de 80 MHz y ocho canales de 40 MHz disponibles en EE. UU.

Tabla 5 - Disponibilidad de canal de 5 GHz a nivel mundial

Cantidad de canales disponibles	EE. UU.	Unión Europea	China	India	Japón	Rusia
Canales de 20 MHz	18	16	5	13	19	16
Canales de 40 Mhz	8	8	2	6	9	8
Canales de 80 Mhz	4	4	1	3	4	4

Con la aparición de canales de 80 MHz de amplitud en el estándar 802.11ac Wave 1, y los canales de 160 MHz de amplitud en Wave 2 de inminente aparición, hay ciertos puntos que se deben tener en cuenta en cuanto a la planificación de canales. La cantidad de canales de 20 MHz en la banda de 5 GHz es abundante, pero esto puede cambiar rápidamente a medida que se implementan los de 80 MHz y de 160 MHz (Wave 2) dentro de la empresa. En la figura 15 se explican los efectos de las selecciones de canales de 40 MHz y de 80 MHz.

Figura 15 - Uso de canales en EE. UU.



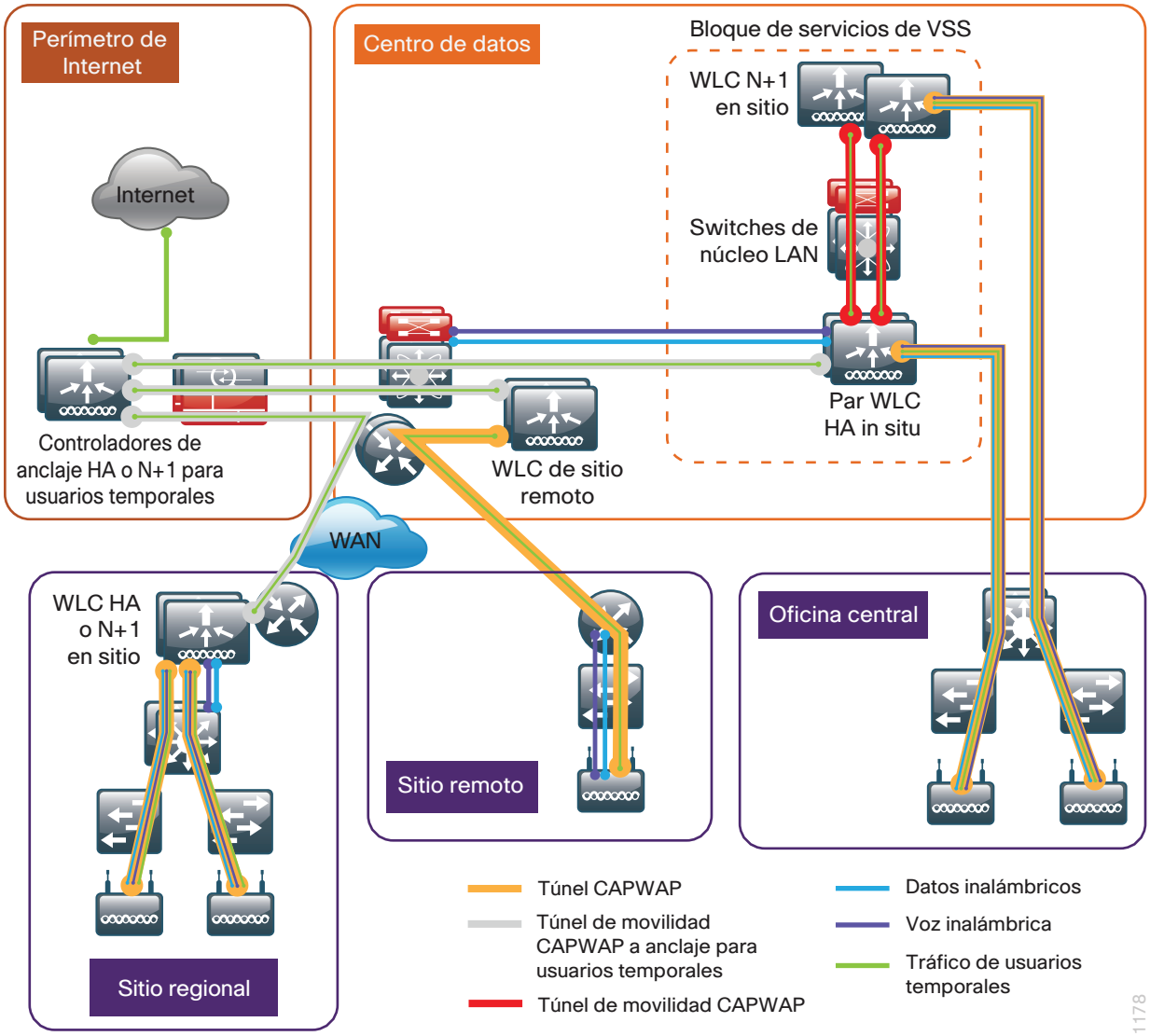
Con RRM, control de potencia de transmisión (TPC) y DCA, el proceso de selección de canales puede automatizarse y optimizarse.

Red inalámbrica para usuarios temporales

El uso de la red LAN cableada existente del campus para acceso de usuarios temporales proporciona una manera rentable y conveniente de ofrecer acceso a Internet para contratistas y visitantes. La red inalámbrica para usuarios temporales brinda la siguiente funcionalidad:

- Ofrece acceso a Internet a los usuarios temporales mediante un identificador SSID abierto e inalámbrico con control de acceso en línea.
- Admite la creación de credenciales de autenticación temporales para cada usuario mediante un usuario interno autorizado.
- Mantiene el tráfico en la red de usuarios temporales separado de la red interna para poder prevenir que un usuario temporal acceda a los recursos de red internos.
- Admite los modelos de diseño para modo local y Cisco FlexConnect.

Figura 16 - Descripción general de la arquitectura inalámbrica



Tanto los modelos de implementación de par controlador exclusivo y de par controlador compartido dentro de la zona perimetral (DMZ) de Internet son compatibles para los servicios inalámbricos para usuarios temporales en esta guía CVD.

Si cuenta con un solo par controlador para toda la organización y ese par controlador está conectado al mismo switch de distribución que el firewall del perímetro de Internet, puede usar una implementación compartida.

En una implementación compartida, se crea una VLAN en el switch de distribución para conectar de manera lógica el tráfico de usuarios temporales desde los controladores LAN inalámbricos a la DMZ. La VLAN para usuarios temporales en DMZ no tendrá una interfaz de capa 3 asociada ni una interfaz virtual switch. Como tal, cada cliente inalámbrico en la red para usuarios temporales usará el firewall del perímetro de Internet como gateway predeterminada.

Si no cumple con los requisitos para una implementación compartida, puede usar los controladores LAN inalámbricos Cisco de la serie 5500 o de la serie 2500 para implementar un controlador de usuario temporal exclusivo. El controlador está directamente conectado con la DMZ de Internet y el tráfico de usuarios temporales de los demás controladores en la organización está tunelizado a este controlador. Otros controladores como los controladores LAN inalámbricos Cisco WiSM2 y Cisco de la serie 5760 pueden proporcionar servicios de anclaje para usuarios temporales tal como se describió, pero la mayoría de las organizaciones usará otros modelos de controlador LAN inalámbrico y, por lo tanto, estos modelos de implementación no se tratan en esta guía.

Tanto en los modelos de diseño inalámbrico compartidos como exclusivos para usuarios temporales, el firewall del perímetro de Internet restringe el acceso desde la red de usuarios temporales. La red para usuarios temporales solo puede alcanzar a Internet y a los servidores DNS y DHCP internos.

En esta guía se cubre el uso del controlador LAN inalámbrico Cisco de la serie 5760 como un controlador LAN inalámbrico del campus centralizado en el sitio. El controlador LAN inalámbrico de acceso unificado Cisco de la serie 5760 puede implementarse en diferentes modelos. Con la introducción del acceso convergente, también se han agregado diversas funciones nuevas, como Mobility Controller (MC), Mobility Agent (MA) y Mobility Oracle (MO).

El modelo de implementación usado en esta guía CVD para el controlador LAN inalámbrico Cisco de la serie 5760 es parecido al de Cisco AireOS, específicamente Cisco Unified Wireless Network (CUWN). En la arquitectura de CUWN, los controladores mantienen tanto las funciones MC como MA en el controlador. En versiones futuras se comenzarán a separar estas funciones para proporcionar funcionalidades de escalabilidad adicionales. Este enfoque es coherente con muchas implementaciones del controlador LAN inalámbrico Cisco de la serie 5760; tiene la intención de trasladar la función MA a los switches Cisco Catalyst de las series 3850/3650 a medida que los switches de la capa de acceso se actualicen.

Diseños de LAN inalámbrica adicionales

La Guía de diseño de la tecnología CleanAir inalámbrica del campus permite reducir la interferencia de RF en su LAN inalámbrica, mientras que la Guía de diseño de la tecnología Cisco OfficeExtend hace posible el éxito de los trabajadores remotos; ambas guías están validadas en el entorno de la Guía de diseño de la tecnología LAN inalámbrica del campus.

CleanAir inalámbrica del campus

Los usuarios de redes inalámbricas esperan tener acceso inalámbrico sin problemas y que ofrezca un rendimiento similar a un acceso por cable. Cuando la interferencia RF afecta al rendimiento inalámbrico, generalmente es temporal. A veces no es posible acceder inmediatamente a los ingenieros de TI que se especializan en la tecnología inalámbrica, y para cuando el problema logra informarse, generalmente ya se ha resuelto.

La tecnología Cisco CleanAir, ahora disponible en todos los puntos de acceso Cisco CleanAir, usa un análisis del espectro en tiempo real para identificar y ubicar las fuentes de interferencia. Cisco CleanAir también puede adoptar medidas en tiempo real para reducir los efectos de la interferencia y, en consecuencia, mejorar la experiencia de red de los usuarios de redes inalámbricas. Durante eventos de interferencia, Cisco CleanAir puede hacer que los puntos de acceso afectados cambien de canales para eludir la interferencia.

Los eventos de interferencia se registran automáticamente en el motor de servicios de movilidad para su posterior análisis. Sin tener en cuenta la ubicación del administrador de red, se encuentra disponible información avanzada histórica y en tiempo real del análisis del espectro.

La Guía de diseño de la tecnología CleanAir inalámbrica del campus incluye la instalación y el uso del software MetaGeek Chanalyzer, lo que permite al administrador de red obtener inteligencia de espectro de Cisco CleanAir en detalle y en tiempo real.

Tecnología Cisco CleanAir

La tecnología Cisco CleanAir es la integración de la inteligencia de espectro de RF histórica y en tiempo real que se obtiene a partir de los puntos de acceso Cisco CleanAir. Antes de que se presentara esta tecnología, los operadores debían deambular con un instrumento para detectar señales de interés y ubicar físicamente el dispositivo que las generaba. La tecnología Cisco CleanAir automatiza estas tareas gracias a que incorpora inteligencia sobre los analizadores de espectro independientes. Con el agregado del dispositivo virtual motor de servicios de movilidad de Cisco, los operadores de red pueden acceder a la información histórica de CleanAir. Este mayor reconocimiento situacional basado en RF y fuera de hora es ideal para entornos que requieren administración constante del espectro de RF, como hospitales y entornos de fabricación.

Los componentes de una solución Cisco CleanAir básica son el controlador LAN inalámbrico Cisco y los puntos de acceso Cisco Aironet de las series 2600, 3600 o 3700. Para aprovechar el conjunto completo de las funciones de CleanAir, la Infraestructura Cisco Prime puede mostrar en tiempo real los datos recuperados de CleanAir. Los puntos de acceso Cisco 3500 y 1550 también son capaces de proporcionar inteligencia de espectro de CleanAir, pero no se cubren en la Guía de diseño de la tecnología CleanAir inalámbrica del campus.

Infraestructura Cisco Prime con tecnología Cisco CleanAir

El poder real de la Infraestructura Cisco Prime con CleanAir, combinada con los puntos de acceso Cisco, es la capacidad de representar visualmente el estado del entorno de RF al administrador de red. Esto le permite al administrador gestionar mejor y solucionar problemas antes de que afecten a los usuarios de la red inalámbrica. Con el dispositivo virtual motor de servicios de movilidad de Cisco que se incluye en la solución, el administrador puede ver los problemas de RF que ocurrieron en el pasado. Generalmente este es el caso que se da, porque los usuarios con frecuencia no informan los problemas de inmediato y porque los equipos de soporte del primer nivel intentan solucionar el problema antes de pasarlo al soporte de segundo o tercer nivel.

Cisco Prime Infrastructure con la tecnología Cisco CleanAir permite a los administradores de redes ver el nivel de desempeño de la red inalámbrica, solucionar problemas de conectividad del cliente de manera remota, administrar los recursos de red inalámbrica, analizar los dispositivos que causan interferencia, y más. Para obtener más información sobre Cisco Prime Infrastructure, consulte la sección Cisco Prime Infrastructure.

La Guía de diseño de la tecnología Cisco CleanAir inalámbrica se encuentra disponible en:

www.cisco.com/go/cvd

Cisco OfficeExtend

Para quienes trabajan desde sus hogares, es fundamental que el acceso a los servicios empresariales sea confiable y homogéneo, con una experiencia similar a la de estar en el campus. Pero en la banda inalámbrica de 2,4 GHz que se usa comúnmente, los entornos residenciales y urbanos cuentan con diversas fuentes potenciales de congestión, como auriculares inalámbricos, smartphones, tablets y dispositivos de monitoreo de bebés. Para dar soporte a usuarios cuyas habilidades técnicas varían ampliamente, una solución para trabajadores remotos debe brindar una manera simplificada y optimizada para implementar dispositivos que permitan el acceso seguro al entorno corporativo.

Las operaciones de TI tienen un conjunto distinto de desafíos en lo que respecta a implementar una solución para trabajo remoto; entre ellos, administrar, mantener y asegurar adecuadamente el entorno del trabajador remoto desde una ubicación centralizada. Debido a que los gastos operativos son un tema que se tiene en cuenta constantemente, TI debe implementar una solución rentable que proteja la inversión de una organización sin sacrificar calidad o funcionalidad.

La Guía de diseño de la tecnología Cisco OfficeExtend cubre los requisitos de facilidad de uso, calidad de experiencia y gastos operativos. La solución Cisco OfficeExtend tiene dos componentes principales:

- Controlador LAN inalámbrico Cisco de la serie 2500 o de la serie 5500
- Punto de acceso OfficeExtend Cisco Aironet de la serie 600

Controladores WAN inalámbricos Cisco

Los controladores LAN inalámbricos Cisco funcionan junto con los puntos de acceso Cisco OfficeExtend para dar soporte a las aplicaciones inalámbricas cruciales del negocio para los trabajadores remotos. Los controladores LAN inalámbricos Cisco ofrecen el control, la escalabilidad, la seguridad y la confiabilidad que los administradores de redes necesitan para crear un entorno seguro y escalable para los trabajadores remotos.

Un controlador autónomo puede admitir hasta 500 sitios de Cisco OfficeExtend. Para tener una solución flexible, Cisco sugiere implementar los controladores en pares.

Los siguientes controladores se incluyen en la Guía de diseño de la tecnología Cisco OfficeExtend:

- Controlador LAN inalámbrico Cisco de la serie 2500
- Controlador LAN inalámbrico Cisco de la serie 5500

Gracias a que la flexibilidad de licencias de software le permite agregar puntos de acceso adicionales a medida que los requisitos del negocio cambian, puede escoger el controlador que dará soporte a sus necesidades a largo plazo, pero pagar únicamente por lo que necesita, cuando lo necesita.

A fin de permitir que los usuarios conecten sus dispositivos de terminales a la red inalámbrica en sitio de la organización o a las redes inalámbricas de trabajo remoto en sus hogares son configuración, la Guía de diseño de la tecnología Cisco OfficeExtend usa las mismas SSID inalámbricas en los hogares de los trabajadores remotos que aquellas que admiten datos y voz dentro de la organización.

Puntos de acceso Cisco OfficeExtend

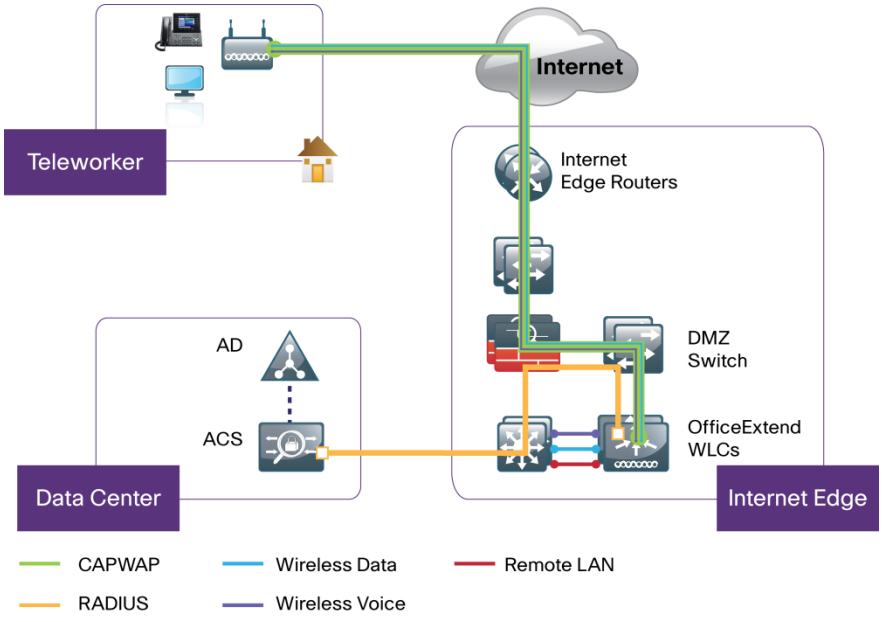
El punto de acceso OfficeExtend Cisco Aironet de la serie 600 es ligero, es decir, que no puede actuar independientemente de un controlador LAN inalámbrico. Para ofrecer conectividad WLAN remota usando el mismo perfil que en la oficina corporativa, el punto de acceso valida todo el tráfico en contraste con las políticas de seguridad centralizadas. Con el uso de controladores LAN inalámbricos para la centralización de políticas, Cisco OfficeExtend minimiza la sobrecarga de administración asociada con los firewalls basados en el hogar. Las comunicaciones entre el punto de acceso y el controlador LAN inalámbrico están protegidas por una conexión de seguridad de la capa de transporte de datagramas (DTLS).

Cisco OfficeExtend ofrece rendimiento inalámbrico total de la tecnología 802.11n y evita la congestión provocada por los dispositivos residenciales porque funciona simultáneamente en las bandas de radiofrecuencia de 2,4 GHz y 5 GHz. El punto de acceso además ofrece conectividad Ethernet por cable, además de la inalámbrica. El punto de acceso Cisco OfficeExtend proporciona segmentación inalámbrica y por cable del tráfico corporativo y en el hogar, lo que hace posible la conectividad de dispositivos en el hogar sin introducción de riesgos de seguridad para las políticas corporativas.

Modelos de diseño

Para una implementación más segura y flexible de la tecnología Cisco OfficeExtend, implemente un par controlador exclusivo para Cisco OfficeExtend usando los controladores LAN inalámbricos Cisco de la serie 5500 o 2500. En el modelo de diseño exclusivo, el controlador está conectado directamente a la DMZ de Internet y el tráfico de Internet termina en la red perimetral en contraste con la red interna, mientras que el tráfico de cliente sigue conectado directamente a la red interna.

Figura 17 - Modelo de diseño exclusivo con Cisco OfficeExtend



La Guía de diseño de la tecnología Cisco OfficeExtend se encuentra disponible en:

www.cisco.com/go/cvd/campus

Comentarios

Use el formulario de comentarios para enviar sus comentarios y sugerencias sobre esta guía.

Sede central en América
Cisco Systems, Inc.
San José CA

Sede Central en Asia-Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede Central en Europa
Cisco Systems International BV Amsterdam,
Holanda

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y los números de fax están disponibles en el sitio web de Cisco en www.cisco.com/go/offices.

B-0000225-1 04/14