aruba
a Hewlett Packard Enterprise company

Un proyecto de red para el espacio de trabajo digital

Autores: Dean Zaremba y Erin O'Reilly de Free Space, en alianza con Aruba, una empresa de Hewlett Packard Enterprise

UN PROYECTO DE RED PARA EL ESPACIO DE TRABAJO DIGITAL

El aumento de los dispositivos digitales

Los empleados digitales de la próxima generación usan dispositivos móviles en formas que van más allá de lo convencional. Los dispositivos en un mundo donde la movilidad viene primero ya no están relegados al entretenimiento personal o al correo electrónico laboral. Cada vez más se transforman en un componente central de cada aspecto de la productividad diaria.

Para el uso personal, las aplicaciones y los dispositivos móviles brindan entretenimiento, redes sociales, compras, navegación y administración financiera. En el ámbito laboral, brindan comunicación por voz, archivos compartidos, videoconferencias, CRM, colaboración unificada, informes de gastos, calendarios compartidos, soporte mediante mesa de ayuda y seguimiento de proyectos. Las líneas entre nuestras vidas laborales y sociales se vuelven más difusas cada día, como muestran los resultados de la más reciente encuesta del sector, realizada por la Economist Intelligence Unit (EIU):

- 30 % de los encuestados afirmaron que nunca trabajarían para una empresa que no les permitiera usar sus propios dispositivos móviles en el trabajo.
- La capacidad de trabajar en cualquier momento y en cualquier lugar se ve como el único impacto importante en la productividad de los empleados. El 49 % cree que el trabajo remoto y flexible fue el responsable del aumento en la productividad.
- 31% de las empresas encuestadas usan aplicaciones de comunicaciones móviles para mejorar la eficiencia de los empleados.

De la misma forma, la Internet de las Cosas (IoT) crea nuevas oportunidades y consideraciones para los empleados digitales que tienen la movilidad como su principal prioridad, a medida en que estos dispositivos "acéfalos" se conectan a un ritmo acelerado. Entre los dispositivos se incluyen iluminación, control de temperatura, control de sonido, electrónicos, candados, vehículos, equipo médico, maquinaria de fabricación, medidores de servicios públicos, cámaras de vigilancia, etc.

Los dispositivos móviles y la IoT obligan a los equipos de TI y las infraestructuras de red a adaptarse y responder a un conjunto completamente nuevo de requisitos y desafíos.

DESAFÍOS PARA LAS ORGANIZACIONES DE TI A LA HORA DE RESPALDAR EL ESPACIO DE TRABAJO DIGITAL

1. Brindar acceso a una red que satisfaga las demandas de los dispositivos digitales
2. Supervisar y resolver los nuevos problemas de la red creados por los dispositivos digitales
3. Proteger la red con respecto a los nuevos desafíos que representa la tendencia BYOD (el uso de los dispositivos personales en el trabajo), la IoT y el acceso de invitados
4. Mejorar el tiempo de actividad y el acceso a las aplicaciones de las nubes privadas y públicas desde cualquier dispositivo y en cualquier lugar
5. Relacionarse con los clientes y los empleados en los dispositivos móviles para mejorar las operaciones y el servicio al cliente

Sin duda, se trata de desafíos importantes. Pero con cada desafío, viene una gran oportunidad. Creemos que las organizaciones que pueden enfrentar estos desafíos y adaptarse al espacio laboral digital más rápido que sus competidores pueden y van a obtener beneficios considerables.

SOLUCIONES A ESOS DESAFÍOS

1. Acceso estable a la red, cableado y mediante Wi-Fi

Considere un escenario del mundo real en el que dos usuarios realizan las mismas tareas en una red Wi-Fi, pero uno tiene una experiencia de usuario de primer nivel y el otro no. Este escenario es muy común en las redes heredadas que no satisfacen las demandas de un espacio de trabajo digital. Pero, ¿por qué ocurre esto? Y, lo que es más importante, ¿cómo se puede enfrentar?

Para responder a esta pregunta, necesitamos ver el tipo de dispositivo: el smartphone, la tablet o la enorme variedad de electrónicos que se espera que respalde la red Wi-Fi. Cada uno de estos tipos de dispositivos tiene su propia radio de RF, su propio sistema operativo, su propio firmware de controlador de red Wi-Fi y sus propias enmiendas de 802.11. Como resultado, cada tipo de dispositivo funciona de forma muy diferente dentro de la misma red de RF.

Además, no se espera que todos los dispositivos admitan todas las aplicaciones de la empresa. Aunque muchas empresas están implementando con éxito VoIP y video en los dispositivos corporativos o en ciertos modelos de smartphones, la perspectiva de brindar estas aplicaciones de forma impecable a todos los dispositivos posibles en un entorno de BYOD resulta abrumadora.

Hay un doble desafío que enfrentar con los diversos tipos de dispositivos. Primero, hay que clasificar los dispositivos por caso de uso. Por ejemplo, ¿el dispositivo en cuestión se destina a servicios de ubicación, comunicación por voz, colaboración, acceso a aplicaciones de negocios o IoT? Luego, dentro de cada clasificación, cada dispositivo debe probarse y el entorno de RF debe estar diseñado para admitir cada caso de uso.

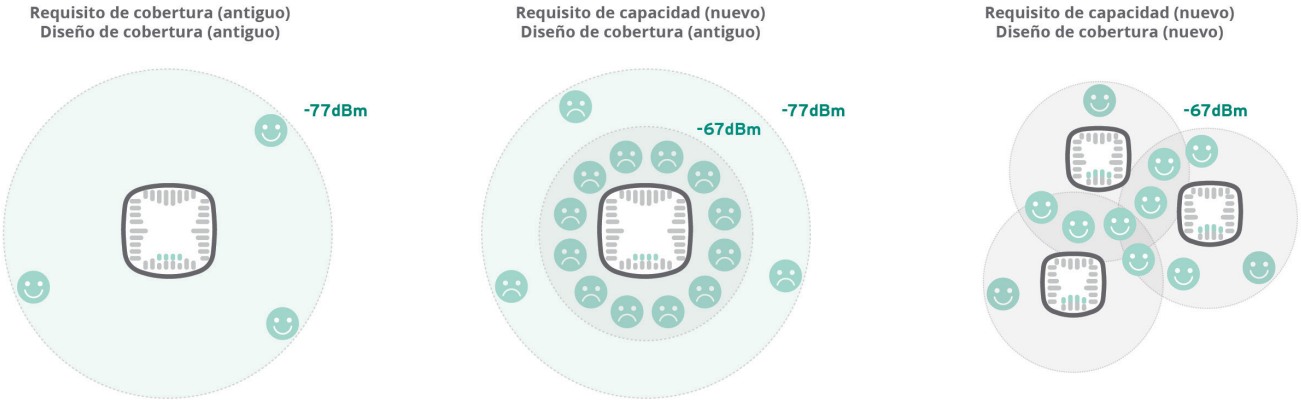
La nueva normalidad en la conectividad de la red con los dispositivos móviles y de IoT

Consideremos otro escenario del mundo real en el que a un usuario le va muy bien con Wi-Fi gigabit 802.11ac para todas sus necesidades. No obstante, algunas veces por semana, su rendimiento se degrada considerablemente, incluso cuando su dispositivo indica que la señal es fuerte y tiene conectividad de "4 barras". Tras investigar un poco, determina que el bajo rendimiento siempre ocurre cuando se usa una gran sala de conferencias que queda cerca. Este es un ejemplo clásico de una red de Wi-Fi que se diseñó para los requisitos de cobertura heredados y no para los requisitos de capacidad actuales.

Históricamente, el diseño de la red Wi-Fi se ha centrado en la fortaleza de la señal. Se determinaba la fortaleza de la señal necesaria para una aplicación y, siempre y cuando toda el área de cobertura mantuviera esa fortaleza, la red funcionaba como se deseaba. Las cosas cambiaron y el aumento en la densidad de los usuarios y los dispositivos, junto con el uso de aplicaciones con ancho de banda en tiempo real, como la voz y el video, han hecho que sea insuficiente concentrarse solo en la fortaleza de la señal.

Cuando se diseña una red para los dispositivos móviles y la IoT, se deben considerar la cantidad de dispositivos, los tipos de aplicaciones y los requisitos de principio a fin necesarios dentro del área de cobertura. Antes, un solo punto de acceso (AP) podía brindar cobertura adecuada. Actualmente, se necesitan varios AP para responder a los nuevos requisitos de capacidad de la red. En resumen, es **esencial** examinar la necesidad de capacidad y de cobertura en un diseño de Wi-Fi para el espacio laboral digital.

LOS NUEVOS REQUISITOS DE CAPACIDAD EXIGEN UN NUEVO DISEÑO

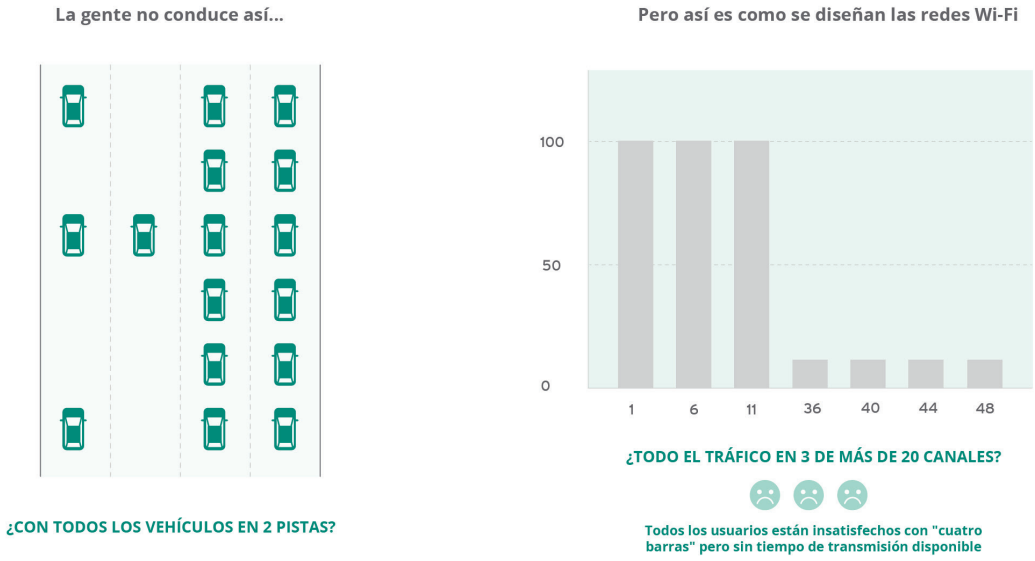


Después de pensar bien en el diseño de la red en torno de los dispositivos que respaldará, la ubicación de los usuarios y las aplicaciones que se usarán, es hora de analizar el uso del canal y el tiempo de transmisión.

La FCC solo permite suficiente radiofrecuencia (RF) para usar en una red de Wi-Fi. Por lo tanto, esta RF debe usarse con la mayor eficiencia e inteligencia posibles. Hay tantos trucos, consejos y factores en juego en un diseño de RF que no sería suficiente un informe completo solo para referirse al tema. Haremos nuestro mejor esfuerzo por mencionar los puntos más importantes.

Con frecuencia, las radios de los dispositivos usan el espectro de 2,4 GHz, aunque el mayor ancho de banda se encuentra dentro del espectro de los 5,0 GHz. Si se utiliza principalmente el espectro de los 2,4 GHz y se ignora el ancho de banda abierto y no utilizado disponible en el espectro de los 5,0 GHz puede producirse un “congestionamiento” innecesario para los usuarios. Aunque cada vez más redes están empezando a usar el espectro de los 5,0 GHz, hay una cantidad sorprendente de redes Wi-Fi heredadas, diseñadas con una mayoría de sus clientes en los 2,4 GHz. El resultado final es una red que parece una carretera donde una parte del tráfico está saturado mientras otras vías están inexplicablemente vacías.

LA UTILIZACIÓN DEL TIEMPO DE TRANSMISIÓN (CANAL) LO ES TODO



Imaginemos ahora un escenario diferente en el que el equipo de TI ha estudiado con cuidado los tipos de dispositivos que necesitan respaldar, así como sus requisitos de densidad ycapacidad.

Este equipo también configuró su red para reducir las ineficiencias en su utilización del tiempo de transmisión y seleccionó con cuidado el ancho de canal adecuado entre 20 y 40 MHz (los 80 y 160 MHz solo tienen un pequeño caso de uso en el mundo de los SOHO y, aún allí, por lo general no se recomienda).

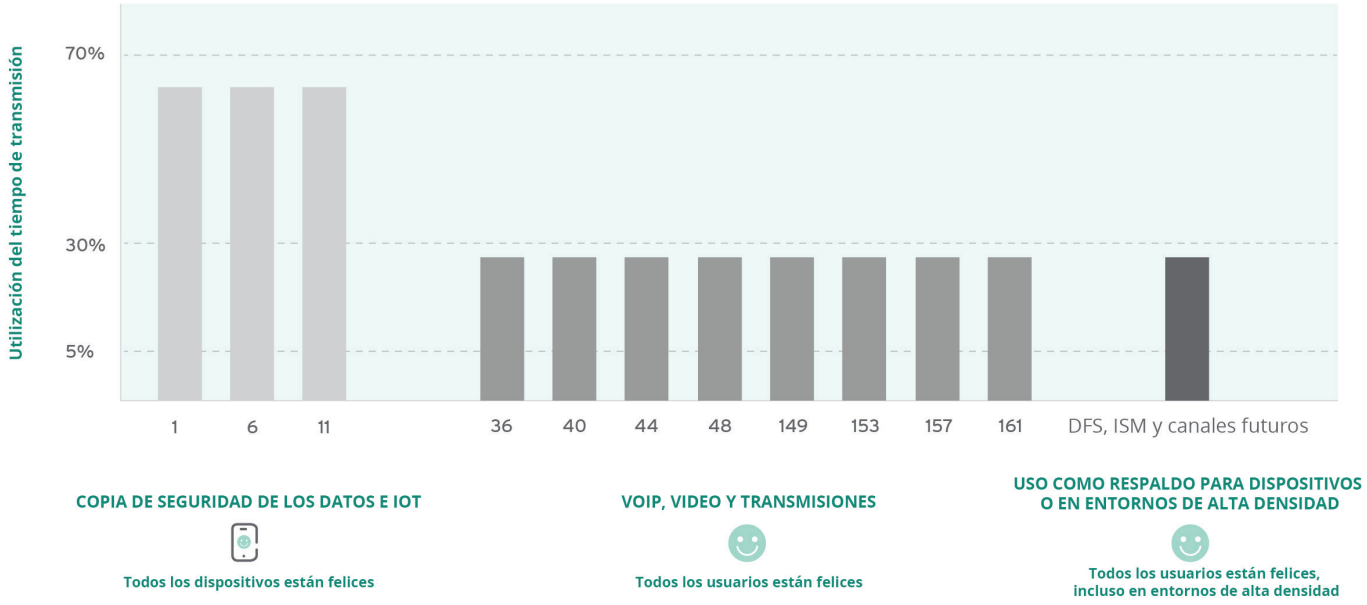
Redujeron los datos generales excesivos (el tráfico que no es de carga) al disminuir la cantidad de SSID, eliminar las bajas velocidades de datos, reducir la interferencia del canal conjunto y los reintentos de la red y eliminar los AP no autorizados. Implementaron una política de calidad de servicio (QoS) para optimizar el rendimiento de aplicaciones en tiempo real como VoIP y video. Usan herramientas de red para supervisar la equidad del tiempo de transmisión y asegurar que unos cuantos usuarios más lentos no afecten el rendimiento general.

Además, el equipo ha estudiado cuidadosamente el uso de canales de selección de frecuencia dinámica (DFS) que ofrecen ancho de banda considerable pero tienen dos riesgos. El primero es que no todos los dispositivos admiten este tipo de canales, especialmente los dispositivos de IoT. El segundo es que las normas gubernamentales prohíben el uso de estas frecuencias durante eventos de radar, por lo que bloquean temporalmente el Wi-Fi en estos canales. El equipo de TI decidió mejorar la capacidad en sus áreas de alta densidad al implementar el uso de canales de DFS y, a la vez, superpusieron al menos un canal que no es de DFS en las áreas de alta densidad para mitigar ambos riesgos.

Finalmente, supervisaron con cuidado su utilización de canal y tiempo de transmisión máximos para que los gastos generales no superaran los 5 % en ningún canal, los canales de datos no superaran el 70 % de utilización y los canales de VoIP / video no superaran el 30 % de utilización. El resultado final de las medidas combinadas en este escenario es una red de Wi-Fi capaz de responder a las nuevas demandas de los dispositivos digitales.

UNA RED BIEN DISEÑADA MAXIMIZA TODO EL ESPECTRO

RED WI-FI LIBRE = RENDIMIENTO MÁXIMO



De la misma forma que adaptamos el diseño de la red de Wi-Fi para responder a las necesidades del espacio laboral digital, el perímetro cableado también debe adaptarse. El aumento de los dispositivos digitales Wi-Fi conlleva un declinio en el uso de equipos de desktop y teléfonos VoIP cableados. Con este cambio, ya no necesitamos dimensionar nuestro perímetro con la expectativa de dos o tres conexiones de cable por oficina o cubículo. Esto permite reasignar partes del presupuesto de TI para satisfazer las demandas de los dispositivos digitales.

Aunque es de suma importancia que el perímetro de acceso cableado actualmente respalde los AP

necesarios para conectar dispositivos digitales inalámbricos, la necesidad de respaldar también dispositivos digitales cableados no ha desaparecido. También hay dispositivos heredados como los equipos de desktop, las impresoras, las televisiones inteligentes, el equipo de fabricación heredado y las máquinas de MRI que necesitan un puerto de Ethernet cableado. Por ello, la red actual tendrá que seguir respaldando estos dispositivos con un enfoque unificado de la configuración y la administración de opciones cableadas e inalámbricas.

Con capacidad de programación e inteligencia en el nivel del núcleo, lo que elimina la necesidad del uso extensivo de soluciones "off-box", una red compleja que incluya opciones cableadas e inalámbricas (heredadas y de punta) se vuelve mucho más sencilla y económica de administrar.

Antes, a un puerto perimetral de Ethernet se le asignaba una VLAN y una configuración que no se alteraba, porque los dispositivos raramente se movían. Con la llegada de la movilidad, el equipo de la red ahora requiere una forma mejor de configurar los puertos de acceso de Ethernet. Una opción es asignar de forma dinámica una configuración a cada puerto tan pronto se clasifica el dispositivo después de su conexión. En este modelo, los equipos de operaciones de la red no tienen que gastar horas configurando puertos individuales o rastreando cuál puerto se asignó a qué uso.

El aumento continuo en la congestión del tráfico dentro de la capa de acceso de la red cableada requiere la implementación de políticas de QoS en la red troncal cableada. Las aplicaciones críticas de los negocios, como VoIP o las cámaras de seguridad con transmisión en vivo, necesitan clasificarse y priorizarse para garantizar niveles más bajos de latencia y una mayor velocidad de operación para los procesos de negocios.

Otra consideración importante con relación a los puertos de Ethernet en el perímetro es que por lo general admitían solo uno o dos dispositivos a la vez y una velocidad de 1 Gbps era suficiente. No obstante, un AP respaldará muchos dispositivos a la vez, lo que genera la preocupación de que 1 Gbps genere un embotellamiento. Hay cierto debate con relación a la capacidad de un AP de superar actualmente el umbral de rendimiento de 1 Gbps, pero hay consenso en que eso sucederá pronto. En consecuencia, los puertos cableados con varios gigabytes en el perímetro deben ser un componente de las compras actuales de infraestructura cableada.

LISTA DE VERIFICACIÓN 1 SOBRE LAS RECOMENDACIONES

1. Documente la mezcla de dispositivos y aplicaciones de misión crítica
2. Planifique la cobertura y la capacidad
3. Reduzca la cantidad de SSID y deshabilite los índices más bajos siempre que sea posible en las radios Wi-Fi
4. Use canales de DFS para superponer canales de otro tipo con el fin de aumentar el rendimiento de Wi-Fi
5. Haga cumplir las políticas de QoS en redes cableadas y Wi-Fi para mejorar el rendimiento de las aplicaciones en tiempo real
6. Clasifique de forma dinámica cada dispositivo en las partes cableadas y Wi-Fi de la red
7. Rastree la utilización del canal y habilite la equidad del tiempo de transmisión en las radios Wi-Fi
8. Implemente puertos 802.3at PoE+ y cableados de varios gigabits para prepararse para el futuro

2. Más visibilidad, resolución de problemas más inteligente, automatización de tareas

Las fuerzas del mercado continuamente desafían a las empresas para que sean más ágiles y respondan a los cambios a un ritmo alucinante. A medida que las empresas confían en su TI para sus operaciones cotidianas, la infraestructura de TI tiene que hacer lo mismo. Como lo hemos comentado varias veces, la cantidad de dispositivos digitales en la red está creciendo exponencialmente, así como la cantidad de aplicaciones que están en uso. Muchas organizaciones están migrando sus redes de un modelo de cliente/servidor a uno de nube privada/pública. Además, cada vez más tráfico de la red corresponde a voz y video, lo que exige entrega en tiempo real. Todo esto aumenta la necesidad urgente de recursos inteligentes de supervisión y resolución de problemas. Los conmutadores del núcleo y la agregación en la actualidad definitivamente deben ser capaces de satisfacer esta necesidad. Asimismo, cuando las herramientas de solución de problemas, supervisión y análisis están incorporadas en el conmutador, la capacidad del núcleo de la red está a la altura de su importancia y los beneficios en términos de eficiencia y costo son enormes.

Aunque el núcleo aún tiene que respaldar protocolos L2/L3, HA, VSF y seguridad confiable, ya no tiene por qué basarse en un sistema cerrado. En vez de ello,

debe brindar una integración fácil mediante la API. Para mejorar el tiempo de actividad y la resiliencia, el núcleo de la generación digital tiene que permitir que la configuración cambie en un entorno virtualizado con la posibilidad de volver a los valores anteriores fácilmente.

Supervisar y resolver esta nueva dinámica en redes heredadas con herramientas heredadas puede ser muy lento y consumir mucho tiempo. La visibilidad actual consiste en flujos de red, registros y herramientas de terceros. Muchos problemas de la red no se capturan en los registros y los que sí lo hacen a veces son difíciles de solucionar a partir de los datos del registro.

Los datos basados en reglas son esenciales para optimizar la solución de problemas. Por ejemplo, si la calidad de la VoIP se deteriora, se podría usar una regla para recopilar y entregar información de la cola de QoS, la utilización de la CPU y la última vez que ocurrió un cambio en la configuración. Esta resolución de problemas se puede hacer mediante la red antes incluso de que un humano sepa que hay una falla. Si se quiere ir más allá, una corrección basada en políticas se puede implementar automáticamente o con un solo clic.

La programación (y la resolución de problemas) de la CLI del equipo de la red puede consumir mucho tiempo y está propensa a errores humanos. La explosión de dispositivos digitales, combinada con la reducción de los presupuestos de la red, empeora esta preocupación. Cada nuevo tipo de dispositivo o aplicación podría necesitar una nueva VLAN, política de QoS, SSID o VRF. Los ingenieros de red necesitan la capacidad de automatizar este tipo de programación, de modo que puedan concentrase en los problemas del panorama general.

Una mejor visibilidad y una resolución de problemas más inteligente no solo son necesarias en el núcleo, sino en la red Wi-Fi. Antes, explicamos cómo identificar y entender los tipos de dispositivos, la cobertura frente a la planificación de la capacidad, y la utilización del tiempo de transmisión: todo tiene un efecto directo en la experiencia del usuario de Wi-Fi. Esto nos lleva a cuestionarnos lo siguiente:

- ¿Cómo supervisamos estas mediciones críticas?
- ¿Cómo conocemos los umbrales que indican que la experiencia del usuario es deficiente?
- Además de Wi-Fi, ¿qué otros factores podrían perjudicar la experiencia del usuario?
- ¿Cómo hacemos para, además de recopilar los datos, reparar el problema antes incluso de que el usuario sepa que existió?

Para brindar la mejor experiencia de usuario posible, los departamentos de TI deben ser capaces de predecir, en vez de reaccionar. La recopilación de mediciones de RF clave, como los niveles de interferencia, la cantidad de dispositivos, los principales consumidores, las tasas de reintentos y la fortaleza de la señal, puede ayudar en buena medida a hacer tales predicciones.

Los AP de producción o los monitores dedicados pueden recopilar estas mediciones y normalmente se ven en un panel de controladora Wi-Fi o en software de supervisión. Los monitores pueden recopilar más datos en más canales en un periodo más corto que los AP de producción, lo que es esencial para ser proactivo y no reactivo. Aunque estos datos se pueden usar para rastrear el estado general de su entorno de Wi-Fi, para obtener una imagen verdadera de la experiencia del usuario, se necesita mucho más que eso.

Supervisión básica del estado de los clientes y los puntos de acceso

Aquí es donde entra en juego la recopilación de datos en el nivel de la aplicación. Es importante tener una comprensión completa de las aplicaciones utilizadas conmúnmente y el tráfico web en una red, en la medida en que son indicadores vitales de los patrones de consumo general. A partir de ahí, podemos definir las aplicaciones de misión crítica, crear políticas de QoS, supervisar las etiquetas de QoS, configurar las colas de QoS y, en última instancia, garantizar que todas las aplicaciones de misión crítica obtengan el ancho de banda y el acceso prioritario que se necesitan en una experiencia de usuario impecable.

La clase de aplicaciones más asociadas con los dispositivos móviles son las de comunicación unificada y colaboración (UCC) y, de acuerdo con ello, merecen una nota aparte. Las aplicaciones de UCC permiten las comunicaciones de voz y video, así como la

colaboración y la opción de compartir documentos, y son esenciales para aumentar la productividad en un espacio de trabajo donde la movilidad es la prioridad. Debido a que las aplicaciones de UCC funcionan en tiempo real y requieren calidad de video, representan la mayor carga para la red. Una organización que puede brindar a sus empleados una aplicación de UCC en sus dispositivos móviles cumple con éxito los estándares de un verdadero espacio de trabajo donde la movilidad es una prioridad.

La visibilidad de la calidad de las aplicaciones móviles, incluidas las comunicaciones unificadas

La compilación de mediciones de red en tablas, hojas de cálculo o bases de datos es cosa del pasado. Los equipos de TI actuales exigen mapas visuales fáciles de interpretar, donde se puedan ver todos los datos relevantes en una sola pantalla. Ser proactivo y no reactivo significa ser capaz de ver una imagen en tiempo real de todo el entorno de RF, así como de la red cableada subyacente, la ubicación de los usuarios, su estado y el rendimiento de la aplicación en esos lugares, además de cualquier intrusión o dispositivo no autorizado.

La supervisión en vivo del consumo de aplicaciones, la densidad del dispositivo y la calidad del aire

Para analizar la verdadera experiencia de usuario integral, debemos ver el tiempo que tarda el usuario en recibir el primer paquete de datos después de que se conecta y de cada evento de itinerancia. Lo más importante es el tiempo total necesario para asociarse a una red inalámbrica, autenticarse en un servidor Radius, obtener una IP con DHCP, resolver los nombres del host mediante DNS y transmitir un primer paquete de datos. Si no podemos capturar y seguir cada paso de este proceso, es como si ignoráramos el eslabón más delgado de una cadena y después nos preguntáramos porque se rompe todo el tiempo. Por eso, la próxima generación de herramientas de supervisión debe ayudar a evaluar este rendimiento de principio a fin. Además, si se descubren problemas, esas herramientas de supervisión deben permitirnos usar nuestros AP como clientes para ejecutar pruebas sintéticas bajo pedido en toda la experiencia del usuario.

Análisis predictivo de la experiencia del usuario de principio a fin en la red

El componente final de ser proactivo y no reactivo corresponde a la notificación. Una vez que podemos revisar fácilmente las mediciones y definir lo que es aceptable para el usuario y el espacio de trabajo, necesitamos la capacidad de definir umbrales y crear alarmas que notifiquen al equipo de TI antes de alcanzar esos límites. En un mundo realmente digital, los administradores de la TI son tan móviles como los usuarios, por lo que las notificaciones deben ir directamente a los dispositivos móviles y activar una respuesta antes incluso de que el usuario se dé cuenta de que hubo un problema.

Los mismos procesos que nos permitirán resolver de forma proactiva los fallos de la red también brindarán beneficios cuando un departamento de TI tenga que reaccionar a un problema. Con la amplia cantidad de datos que podemos recopilar, podemos enviar los problemas al soporte de la mesa de ayuda de Nivel 1 en vez de recurrir a equipos de solución de mayor nivel y con un costo más alto. Y, en las raras situaciones en que se necesite un soporte de un nivel más alto, la amplitud de mediciones nos permitirá darle a ese equipo un buen punto de partida.

LISTA DE VERIFICACIÓN 2 SOBRE LAS RECOMENDACIONES

1. Implemente conmutadores de núcleo y agregación diseñados desde el principio para respaldar las necesidades heredadas y las avanzadas.

2. Utilice un motor de análisis de la red para brindar mejor visibilidad y una solución de problemas más rápida
3. Automatice la implementación de las tareas de configuración para reducir el tiempo de CLI de diseño
4. Recopile información sobre el rendimiento de la aplicación, además de las mediciones básicas de Wi-Fi
5. Habilite análisis forenses y de tendencias para obtener una visibilidad más amplia de la experiencia integral del usuario
6. Tenga un método para simular de forma sintética el rendimiento de la red y las pruebas de conectividad
7. Defina las mediciones del umbral y las alertas asociadas para una respuesta proactiva
8. Cree un proceso para utilizar la mesa de ayuda de Nivel 1 cuando se requiere una respuesta reactiva

3. Respalde con seguridad los diversos casos de la tendencia BYOD, los invitados y IoT

Hemos analizado cómo diseñar una red confiable, la importancia de una supervisión proactiva de la red y la necesidad de reaccionar con eficiencia cuando surgen los problemas. Los siguientes pasos para garantizar una experiencia de usuario positiva tienen que ver con la protección de la red. Esto requiere tres pasos básicos:

- Elaborar con cuidado políticas y reglas
- Inspeccionar todas las solicitudes para brindar acceso de acuerdo con las políticas
- Negar o autorizar permisos en función de ellas

Con una amplia gama de tipos de dispositivos, tipos de usuarios y aplicaciones, debe diseñarse el control de acceso a la red (NAC) caso a caso. A continuación se presentan los elementos clave para proteger el espacio laboral digital donde la movilidad es prioritaria.

Empecemos con el caso de uso más común que es el otorgamiento de acceso a la red a los empleados que usan un dispositivo brindado por la empresa o de propiedad personal (BYO). La meta es proporcionar acceso a la red cableada, inalámbrica o VPN con la mayor facilidad y simplicidad posible, sin varios métodos de acceso, credenciales o pantallas de inicio de sesión.

Para habilitarlo, una sola plataforma de NAC con autenticación basada en 802.1X-se está volviendo la opción estándar. La metodología más segura es el uso de certificados en EAP-TLS. Con frecuencia, la autenticación se basa en un nombre de usuario y una contraseña y se asocia a almacenes de usuario existentes como un Directorio activo o LDAP. Para obtener más seguridad, algunas empresas están implementando autenticación con varios factores: una pregunta secreta, huellas digitales, reconocimiento de voz, fotografía o ubicación física.

Además del usuario, el propio dispositivo se puede incluir como parte de la política de acceso a la red. En el caso de los dispositivos corporativos, la política de seguridad podría basarse simplemente en una dirección MAC o puede incluir la presencia de un agente de software de administración de dispositivos móviles (MDM) instalado en el dispositivo. En el caso de los dispositivos propios en el trabajo, podría basarse en las versiones del SO, el modelo de dispositivo y/o la presencia de una solución de administración de aplicaciones móviles (MAM). Las soluciones de administración de aplicaciones y dispositivos móviles pueden segmentar los datos personales a partir de las aplicaciones y los datos corporativos con el fin de mantener la red segura, o se pueden usar para hacer cumplir las listas negras con relación a ciertas aplicaciones o dispositivos "inadecuados".

Empleados, invitados, contratistas

Otro escenario de caso de uso común es el acceso a la red que se solicita para un invitado que busca servicios de Internet, impresión y de otro tipo. Estos "no empleados" pueden ser visitantes, clientes, contratistas, socios de negocios, compradores, etc.

El acceso a estos usuarios invitados se debe brindar de forma segura y eficiente. Las opciones de registro suelen incluir soluciones basadas en el portal, como el responsable del empleado o el registro propio, que reducen el peso de la administración de TI. Una vez registrados, los usuarios suelen obtener credenciales por correo electrónico o texto y pueden obtener acceso a una VLAN segura que les da acceso limitado a la red.

Otro ejemplo de un caso de uso de acceso de invitado sería una instalación de alta capacidad como un aeropuerto, un espacio deportivo o un centro comercial. En este caso, podría usarse una simple cuenta de "aceptación de uso" o, como alternativa, podría solicitarse un inicio de sesión en una red social. En algunos casos, la autenticación abierta también podría ser una opción. En estas situaciones, la WLAN para invitados debe ser 100 % segura a partir de la red corporativa, por lo general, mediante el uso de políticas basadas en roles, de cumplimiento obligatorio mediante seguridad de firewall incorporada en la infraestructura de red.

Portales web personalizados y fáciles de usar para ayudar a los usuarios a incorporar sus dispositivos a la red

La necesidad de acceso a la red a "no empleados" se ve aumentada por el crecimiento de la IoT. Aunque estos dispositivos son "acéfalos", es decir que no son manejados por humanos, también requieren acceso a la red. Las organizaciones deben desarrollar políticas basadas en roles para la IoT, que sean diferentes de las políticas para sus empleados y los usuarios invitados. Incluso pueden necesitar varias políticas para enfrentar la amplia gama de dispositivos de IoT que se conectan a la red.

La elaboración de perfiles de dispositivos y el uso de huellas digitales que ya eran importantes para la seguridad de la red se han vuelto esenciales con la IoT. Cada vez que un dispositivo trata de conectarse a la red, se elabora un perfil automáticamente. Esto significa saber qué tipo de dispositivo es y qué función realiza en su empresa, lo que permite aplicar la política de seguridad correcta. Si la red encuentra un dispositivo al que no se le puede aplicar un perfil automáticamente, el dispositivo se coloca en cuarentena hasta obtener más información.

Clasificación automatizada de los dispositivos en la red

Los problemas de seguridad relacionados con el NAC no son los únicos que hay que considerar en la red. Esa lista la encabezan las intrusiones. Juntos, un sistema inalámbrico de detección de intrusiones (WIDS) y un sistema inalámbrico de protección contra intrusiones (WIPS) ayudan a identificar amenazas potenciales a la infraestructura de AP o los clientes asociados.

Una solución de WIDS/WIPS sofisticada y eficaz, aunque fácil de administrar, debe proprocionarle al administrador de la red los medios para identificar, evaluar y defenderse de ataques y, a la vez, mantener una experiencia segura y sin interrupciones. Lo que es más: los WIDS/WIPS deben poder personalizarse en la medida en que los requisitos y las normas que corresponden a cada red pueden variar mucho en función de que se trate de un lugar para conferencias, una institución financiera o una agencia gubernamental.

Otra preocupación de seguridad imperante en las redes es el malware en varias fases o los ataques persistentes. Son amenazas que permiten que, una vez que una persona obtiene el acceso a la red, pueda mantenerse en ella durante mucho tiempo y lanzar varios ataques, por lo general para robar los datos en vez de hacer fallar la red. Los firewalls y el software antivirus heredados no son suficientes para este tipo de ataque. La solución es la protección de la próxima generación con integración impecable entre múltiples productos que realizan la detección, la mitigación y la prevención. Esta protección debe aplicarse en la capa de la aplicación, en la medida en que la seguridad basada en puertos es insuficiente.

Los nuevos sistemas de seguridad deben integrarse con las plataformas de política de acceso a la red para obligar su cumplimiento en la red cableada y Wi-Fi, en caso de que se identifiquen ataques internos y/o externos. Mientras las soluciones tradicionales de NAC solo se preocupaban por la corrección inicial de los dispositivos cableados y de Wi-Fi, las soluciones de administración de políticas de la próxima generación orientan sus acciones contra el riesgo creciente que representan los dispositivos conectados a medida que se identifican las actividades maliciosas.

LISTA DE VERIFICACIÓN 3 SOBRE LAS RECOMENDACIONES

1. Cree políticas de acceso a la red con un contexto completo de tipos de dispositivos, estado, usuario, hora y lugar
2. Use perfiles de dispositivos para incorporar dispositivos de IoT a la red y ponerlos en cuarentena si es necesario
3. Implemente una sola plataforma para lidiar con el control de acceso a la red cableada, inalámbrica y VPN
4. En el caso de los empleados, use 802.1X EAP-TLS junto con la autenticación de varios factores
5. Para el acceso seguro de invitados, haga cumplir las políticas de firewall dentro de la red
6. Implemente detección inalámbrica de intrusiones y/o políticas, procedimientos y soluciones de prevención
7. Integre protección de amenazas de la próxima generación con la plataforma de administración de políticas

4. Brinde aplicaciones de nube y colaboración en todo lugar

La última pieza en la experiencia integral del usuario es la propia aplicación. Claro que no hay redes ni organizaciones con las mismas necesidades de aplicación. Pero hay elementos fundamentales que corresponden a la mayoría de los escenarios.

La arquitectura tradicional de cliente/servidor ya no es adecuada para la red donde la movilidad es prioridad. Este modelo se diseñó para entregar archivos e información desde un solo servidor a una PC conectada a la misma LAN u, ocasionalmente, a la WAN. Aunque la PC sea suficiententemente robusta para admitir el almacenamiento local de aplicaciones grandes, esto ya no es viable con los dispositivos móviles. Por eso exigimos una entrega de aplicaciones optimizada y centralizada.

Además, los usuarios con frecuencia no trabajan en la misma LAN que el servidor. En un día de trabajo cualquiera, un usuario puede trabajar desde su casa y necesita acceder a una aplicación en una tablet con una conexión a Internet por cable. Al día siguiente, el mismo usuario puede estar viajando o visitando clientes y necesita acceder a esa aplicación en un smartphone con el servicio celular de 4G. Y, un día después, este usuario puede estar revisando operaciones en varias oficinas remotas y necesita usar la WAN corporativa para conectarse con seguridad a las aplicaciones.

Aunque cada uno de esos escenarios requiere su propio diseño de infraestructura de red particular, el usuario necesita que su experiencia sea uniforme en todas las combinaciones posibles de métodos de acceso, tipos de dispositivos o lugares. Satisfacer esa exigencia implica migrar las aplicaciones a una ubicación centralizada y usar servidores virtualizados, un concepto suficientemente sencillo que aporta muchas ventajas a la red donde la movilidad es prioridad.

"Las aplicaciones entregadas desde una ubicación centralizada" es el camino natural de las aplicaciones de la nube. Las aplicaciones de la nube son posibles gracias a centros de datos y granjas de servidores virtualizados que se pueden entregar mediante la nube pública o la privada. Las aplicaciones de la nube privada se manejan desde un centro de datos de propiedad y administración internas, y solo los usuarios que han obtenido acceso a la red pueden usar esas aplicaciones. La ventaja evidente de usar un centro de datos privado es la capacidad de mantener los protocolos de seguridad y QoS del cliente en los servidores de la aplicación. El beneficio diferenciado de las aplicaciones en la nube pública es la rentabilidad y la facilidad de acceso. Con todas estas opciones disponibles, cada organización debe decidir cuál combinación de aplicaciones en nubes públicas y privadas es la mejor para sus necesidades específicas y su presupuesto.

Cuando las organizaciones quieren explorar nuevas geografías para sus negocios, cuanto más rápido migran a sus nuevos lugares y se vuelven a conectar a los recursos corporativos, más rápido obtienen el RoI. La infraestructura de red no debe limitar la forma de hacer negocios en lugares remotos.

LISTA DE VERIFICACIÓN 4 SOBRE LAS RECOMENDACIONES

1. Diseñe un modelo de red para la conectividad de oficinas domésticas, pequeñas y sucursales
2. Implemente un sistema de fácil uso para la conectividad de quien pasa fuera de la oficina en puntos de acceso 4G, LTE y Wi-Fi
3. Cree una lista de las aplicaciones que se entregarán a los usuarios remotos mediante nubes públicas y privadas
4. Defina claramente mediciones de red que satisfagan las expectativas del usuario y supervíselas en tiempo real
5. Implemente QoS integral para sus aplicaciones de nube privadas, principalmente para las comunicaciones unificadas
6. Negocie con cuidado y entienda los acuerdos de nivel de servicio (SLA) de las aplicaciones de nube pública

5. Aproveche Bluetooth Low Energy (BLE) en los servicos de ubicación

Los servicios basados en la ubicación y la adhesión a aplicaciones móviles son aspectos cada vez más importantes de la experiencia digital. La capacidad de relacionarse con los clientes y los usuarios de forma contextual, mediante recursos como las notificaciones push dirigidas o las instrucciones paso a paso, brinda una amplia gama de ventajas para la experiencia del usuario y el resultado de la organización.

Bluetooth Low Energy (BLE) es la tecnología ideal para los servicios en interiores basados en la ubicación. Las balizas de BLE funcionan en la frecuencia de 2,4 GHz, tienen un rango típico de cerca de 61 metros (200 pies) y pueden brindar precisión de 30,5 cm (un pie) en la ubicación. Cuando se combinan con una aplicación móvil bien diseñada, se puede usar una tablet o un smartphone como dispositivo del lado del cliente en la red de baliza de BLE. El valor de la información basada en la ubicación se volverá prácticamente ilimitado a medida que crece la interacción entre los smartphones y la IoT.

La BLE no se usa solo para la ubicación humana. También es una tecnología excelente para el rastreo de activos. Una etiqueta pequeña y económica de BLE se puede colocar en cualquier activo, independientemente de que sea una máquina de MRI móvil en un hospital, una cama nido en un hotel, o una herramienta valiosa en una planta de fabricación; y ese activo se puede rastrear y ubicar mediante una aplicación en un dispositivo móvil. Este tipo de rastreo de activos ahorra tiempo y dinero.

La infraestructura de BLE se puede implementar como balizas de BLE autónomas, como AP aptos para BLE o como una combinación de ambos. Las balizas de BLE son fáciles de implementar y de usar, pero las implementaciones grandes pueden introducir desafíos operacionales en términos de la administración, como los cambios en la batería y los ajustes en los niveles de energía. Para superar estos desafíos y eliminar el tiempo y los costos de la administración manual, las organizaciones interesadas en las balizas de BLE deben buscar soluciones que incluyan sensores y otros recursos de administración remota.

Administración centralizada de balizas de BLE

En el caso de las organizaciones que no cuentan con los recursos para desarrollar sus propias aplicaciones móviles desde cero, hay una amplia gama de modelos que pueden usar. En el caso de las organizaciones que tienen una aplicación pero quieren agregarle servicios basados en la ubicación, hay complementos de SDK para funcionalidades como la navegación y el marketing sensible al contexto. Entre los casos de uso comunes para los servicios basados en ubicación se incluyen:

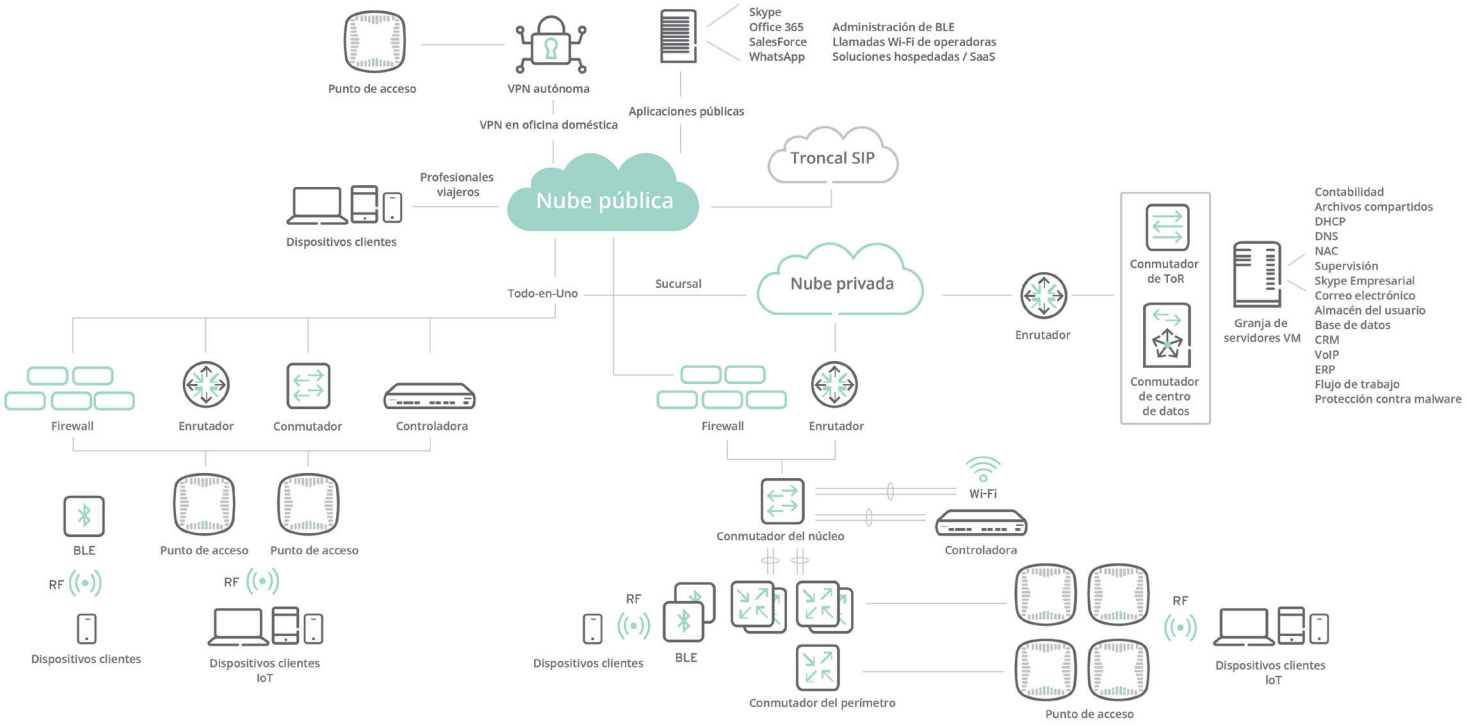
- Brindar una experiencia de “punto azul” en un mapa con el fin de ayudar a los usuarios a navegar en sus instalaciones con instrucciones paso a paso
- Permitir que los usuarios encuentren a amigos y colegas de forma rápida y fácil
- Rastrear activos valiosos con el uso de una etiqueta de BLE
- Permitir que los clientes encuentren fácilmente a los empleados cuando necesitan ayuda
- Entregar notificaciones push a los clientes basados en su ubicación actual y en sus hábitos de compra pasados
- Brindar facturación, acceso a la habitación y control de temperatura automatizados para los huéspedes de un hotel

- Encender y apagar automáticamente las luces y otros servicios cuando los empleados entran y salen de las salas

LISTA DE VERIFICACIÓN 5 SOBRE LAS RECOMENDACIONES

1. Defina con claridad los casos de uso de las balizas de BLE para posibilitar servicios basados en la ubicación
2. Empiece a trabajar con un socio de desarrollo de aplicaciones concentrado en mejorar la experiencia del usuario final
3. Cree un plan y una estrategia para la forma en que su aplicación móvil va a interactuar con los dispositivos de IoT
4. Use administración centralizada para las balizas de BLE con el fin de reducir los costos operacionales

¿Cómo se ve una red de dispositivos digitales?



CONCLUSIÓN

Independientemente del tipo de negocios que tenga (servicios financieros, gobierno, atención médica, educación, sector minorista, turismo o fabricación), los dispositivos digitales afectan la forma en que lleva su empresa y el tipo de infraestructura de red que necesita.

En este documento se describen algunos de los desafíos que los dispositivos digitales imponen a las organizaciones en todos los mercados verticales y se analizan algunas de las soluciones a esos problemas. Las empresas progresistas toman esa información y trabajan con especialistas en movilidad, arquitectos de red e ingenieros para encontrar enfoques detallados y personalizados para su caso de uso específico. Al hacerlo, disfrutarán de beneficios que van desde una mejor comunicación y colaboración hasta una mayor productividad y gastos reducidos de capital y operaciones.

aruba
a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM