Tecnológico de Monterrey - Campus Monterrey
Escuela de Ingeniería y Ciencias
Ingeniería en Tecnologías Computacionales
Interconexión de Dispositivos

Reto - Fase 2: Diseño Físico y Lógico de la Red

Group #304

Santiago Quintana Moreno A01571222
Ian Fernando León Hernández A01785078
Santiago Borbolla Regato A01660035
Miguel Ángel Gavito González A00839096
Manuel Arias Alcocer A01571655

Ing. Joel Hiram Chávez Verástegui
Ing. Mario Jesús Gárate Vélez

Monterrey, Nuevo León a 27 de mayo del 2025

SECCIÓN I - DESCRIPCIÓN DEL ESCENARIO ANÁLISIS

INTRODUCCIÓN:

- **Empresa**: AztechTech S.A. de C.V.
- **Matriz / Oficina Central:** San Pedro Garza García, Nuevo León.
- **Oficina Secundaria:** Polanco, Ciudad de México.
- **POS / Tiendas:** 30 en la República Mexicana.
- **Empleados:** 250 totales
    - 35, San Pedro Garza García, Nuevo León.
    - 35, Polanco, Ciudad de México.
    - 5, en cada sucursal / POS.

AztechTech S.A. de C.V., una empresa de tecnología (smartphones, audífonos, cargadores, computadoras, bocinas, etc.) y servicios de comunicación con sede en San Pedro Garza García y una oficina secundaria en Polanco, opera una red de 30 puntos de venta a lo largo de la República Mexicana. Se estima que sus ventas mensuales, impulsadas por su presencia a nivel nacional, rondan los $5 millones de pesos, acumulados en línea y en storefront. Una posible fortaleza radica en su extensa red de puntos de venta, facilitando el acceso a sus productos o servicios. Sin embargo, una debilidad podría ser la gestión y coordinación de un equipo distribuido en diferentes ubicaciones, lo que podría impactar en la eficiencia operativa.

Gracias al aumento de sus ventas a nivel nacional, tanto en línea como físicamente en sus sucursales, la empresa ha evolucionado de sus servicios básicos de comunicación y de tecnología contratados reactivamente, a necesitar de una renovación de dichos servicios para una operación continua y eficiente con mínimo tiempo de baja.

Por otra parte, las tendencias del mercado mexicano refuerzan la urgencia de actualizar la infraestructura. El consumo de productos tecnológicos y electrónicos sigue en auge: en 2024 el comercio electrónico minorista creció un 20% hasta alcanzar los $789,700 millones de pesos (Rodríguez, 2025), representando ya cerca del 16% de las ventas minoristas del país (Rodríguez, 2025). Se estima que un 84% de los internautas en México ya realizan compras en línea (Ortega, 2024), reflejo de nuevos hábitos de compra más digitalizados y de la preferencia por experiencias omnicanal por parte de los clientes (Ortega, 2024). En este contexto, expertos advierten que alrededor del 90% de las PyMEs que no adopten la digitalización podrían fracasar en los próximos años (Storecheck & Storecheck, 2025b). Por ello, adoptar una infraestructura de red de última generación no es solo una mejora técnica, sino una necesidad estratégica para asegurar la competitividad y la continuidad del negocio.

ANTECEDENTES:

AztechTech S.A. de C.V. se encuentra actualmente operando bajo una infraestructura de red y conectividad ampliamente superada por las demandas actuales del negocio. Esta infraestructura presenta una serie de deficiencias críticas tanto a nivel físico; hardware, lógico; software y servicios como de conectividad externa; servicios de Internet, lo que ha afectado directamente la continuidad operativa, la seguridad de la información y la eficiencia de los procesos internos.

En primer lugar, los equipos de red en uso, principalmente switches no administrables, routers básicos y cableado desorganizado o de categorías antiguas no ofrecen ningún nivel de segmentación, monitoreo ni control de tráfico. La inexistencia de VLANs o políticas de calidad de servicio (QoS) impide la separación lógica entre áreas sensibles como punto de venta (POS), administración, cámaras de vigilancia e inventario, lo que facilita la propagación de amenazas internas y genera competencia innecesaria por ancho de banda. Esta arquitectura de red "plana" no cumple con estándares modernos de seguridad ni escalabilidad. Las latencias elevadas, las caídas recurrentes en el servicio y la imposibilidad de priorizar tráfico crítico se han vuelto síntomas frecuentes que impactan directamente la experiencia del cliente, las transacciones en caja y la coordinación logística entre sedes.

Por otra parte, en el plano del software, se detectó una convivencia de múltiples versiones obsoletas del sistema operativo en servidores dentro de cada oficina central como en los POS, muchas de ellas fuera de soporte oficial y sin actualizaciones de seguridad. Esta diversidad impide aplicar políticas centralizadas de gestión, control de parches y seguridad, además de representar un riesgo elevado de vulnerabilidades conocidas y explotables. Tampoco existe una estructura de dominio con Active Directory, lo cual obliga a una administración manual y descentralizada de usuarios, accesos, y dispositivos en cada punto de venta o sede. Los servicios críticos como ERP, nómina, inventario y CRM residen en servidores locales sin virtualización, sin respaldo en la nube, y sin replicación entre sedes, lo cual reduce considerablemente la disponibilidad y confiabilidad del sistema.

Finalmente, desde la perspectiva de conectividad externa (capa 3), se observó que la empresa depende en gran medida de servicios residenciales o comerciales básicos contratados con ISPs sin garantías empresariales (SLA), ni enlaces dedicados. Las conexiones entre sedes se realizan mediante túneles VPN sobre enlaces asimétricos sin redundancia ni respaldo físico, lo cual genera una alta tasa de pérdida de paquetes, desconexiones frecuentes y problemas serios de sincronización entre los servicios centrales y los puntos de venta. La ausencia de enlaces MPLS o fibra óptica dedicada ha creado un escenario de único punto de fallo (SPOF), donde cualquier falla en la conexión principal puede paralizar operaciones completas. Este esquema, si bien aparentemente más económico en corto plazo, ha generado mayores pérdidas operativas, aumento de incidencias, y un costo oculto por improductividad y atención a contingencias.

En resumen, la empresa opera actualmente con una arquitectura tecnológica reactiva, no estandarizada, vulnerable y carente de escalabilidad. Esta situación no solo frena el crecimiento operativo y la expansión comercial de la empresa, sino que expone sus activos informáticos a riesgos significativos de seguridad y pérdida de información. Estos antecedentes justifican una intervención integral orientada a modernizar la infraestructura de red, implementar controles unificados de software, estandarizar el entorno operativo y profesionalizar la conectividad entre sedes, todo con el objetivo de garantizar continuidad, eficiencia y seguridad en la operación.

DIAGNÓSTICO Y DICTAMEN:

CAUSA RAÍZ	EFECTO VISIBLE	SOLUCIÓN PROPUESTA
Uso de switches no administrables, hubs o routers obsoletos.	Alta latencia, interrupciones frecuentes, cuellos de botella.	Reemplazo por switches administrables capa 3, implementación de topología jerárquica, cableado estructurado Cat 6A.
Equipos de red sin segmentación (red plana sin VLANs).	Riesgo de propagación de malware, tráfico no controlado, fallos generalizados.	Creación de VLANs por función (POS, administración, cámaras, visitantes), políticas de QoS, enrutamiento con OSPF.
Diversidad de versiones de sistema operativo obsoletas.	Incompatibilidades, brechas de seguridad, dificultad en administración.	Estandarización a Windows 11 Enterprise o server edition, dominio con Active Directory, políticas de grupo y control de parches con WSUS o Intune.
Conectividad entre sedes por VPNs residenciales o enlaces asimétricos.	Caídas frecuentes, pérdida de sincronización entre ERP, nómina e inventario.	Migración a fibra óptica dedicada (DIA), enlaces MPLS con SLA empresarial, redundancia de ISP y balanceo de carga.
Ausencia de firewalls de nueva generación.	Exposición a amenazas externas, falta de control sobre el tráfico.	Implementación de NGFW con IDS/IPS, VPN IPsec, filtrado web y segmentación perimetral
Gestión manual de inventario y falta de visibilidad en tiempo real.	Errores en stock, desabasto en sucursales, decisiones lentas.	Implementación de sensores RFID e integración con Azure IoT Hub y Power BI para visibilidad en tiempo real y análisis predictivo
Ausencia de redundancia de conectividad e infraestructura crítica (SPOF).	Interrupciones operativas completas ante fallos ISP o de energía.	Dual WAN con failover, energía redundante (UPS) y enlaces duales en sitios críticos.
Mala gestión de IPs, sin subredes claras ni escalabilidad	Conflictos de red, dificultad de administración, límites de crecimiento.	Planificación con subredes /24 por función o ubicación, integración de DHCP centralizado y DNS empresarial.

Durante la intervención técnica realizada en la empresa de retail tecnológico con sede en Monterrey, se identificó una serie de deficiencias estructurales y operativas en la infraestructura de red que justifican una intervención urgente y profunda. El ecosistema tecnológico de la organización muestra síntomas severos de obsolescencia: equipos de red sin capacidad de administración, una red plana sin segmentación funcional, sistemas operativos desactualizados y sin parches, así como enlaces a internet residenciales sin respaldo ni contratos empresariales con SLA.

Esta falta de planeación ha traído como consecuencias interrupciones constantes en los servicios críticos como el ERP, las aplicaciones de nómina e inventario, además de vulnerabilidades de seguridad generalizadas que podrían facilitar desde ataques internos hasta ransomware. La conexión entre sedes se encuentra sustentada en túneles VPN poco confiables, sin enlaces dedicados ni mecanismos de failover, haciendo que cualquier falla en la conectividad provoque pérdida de sincronización de datos entre puntos de venta y oficinas principales.

Además, se observó una dependencia de procesos manuales en áreas clave como inventarios y POS, lo cual genera errores humanos, falta de visibilidad operativa y baja capacidad de reacción ante fluctuaciones de demanda. En consecuencia, se propone una modernización integral, que abarca desde la capa física (cableado, switching, enlaces dedicados) hasta la capa lógica (sistemas operativos, políticas de red, servicios cloud e IoT). Esta transformación no solo resolverá los problemas actuales, sino que dotará a la organización de una plataforma tecnológica moderna, segura, escalable y preparada para competir a nivel nacional e internacional en el sector de retail tecnológico.

SECCIÓN II - DISEÑO FÍSICO Y LÓGICO DE LA RED

LISTA DE COMPONENTES DE RED

Oficina Central: San Pedro Garza García		
DISPOSITIVO	**TIPO**	**CANTIDAD**
ISR 1100 8P Dual GE SFP WAN 8GB Router	Router	1
Catalyst 9200 48-port PoE+, Network Essentials	Switch	3
Catalyst 9115AX Series	Access Point	3
UCS C220 M7 Rack w/o CPU, mem, drives, 1U w NVMe Backplane	Server	3
Oficina Secundaria: Polanco, CDMX		
DISPOSITIVO	**TIPO**	**CANTIDAD**
ISR 1100 8P Dual GE SFP WAN 8GB Router	Router	1
Catalyst 9200 48-port PoE+, Network Essentials	Switch	3
Catalyst 9115AX Series	Access Point	3
UCS C220 M7 Rack w/o CPU, mem, drives, 1U w NVMe Backplane	Server	3
POS (Point of Sale)		
DISPOSITIVO	**TIPO**	**CANTIDAD**
ISR 1100 8P Dual GE SFP WAN 8GB Router	Router	1
Catalyst 9200 48-port PoE+, Network Essentials	Switch	1
Catalyst 9115AX Series	Access Point	1

Para mejorar la infraestructura de red en AztechTech S.A. de C.V., se seleccionaron una serie de componentes electrónicos cuyo propósito es mejorar el flujo de datos entre las oficinas centrales, oficinas secundarias, y puntos de venta (POS), de forma que la transmisión de información en la compañia sea más eficiente. De entre los componentes mencionados anteriormente, se escogieron los siguientes: ISR1100X Series Router (1 unidad), Catalyst 9200 Series Switch (3 unidades), Catalyst 9115AX Series Access Point (3 unidades), y UCS C220 M7 SFF Rack Server (3 unidades). El router seleccionado ofrece funciones esenciales para la interconexión entre sucursales y oficinas empresariales, tales como una red de área amplia (WAN), bajo consumo de energía eléctrica, alta velocidad y eficiencia en la concurrencia de servicios sin degradación del rendimiento (esto permite a los empleados acceder y/o enviar información en las plataformas de la empresa de forma simultánea y con mayor rapidez), protocolos failover (mecanismos para que un sistema o aplicación cambie automáticamente a un servidor o componente de respaldo en caso de que el principal deje de funcionar), y protección de datos mediante IPsec (high-speed IP Security), Estándares de Encriptación Avanzados (AES), y servicios de seguridad (Firewall Empresarial con Reconocimiento de Aplicaciones, Sistema de Detección de Intrusos, Filtración URL, Protección Avanzada de Malware,

Integración de Cisco Umbrella y del sistema SD-WAN). La versión de este router también ofrece 8 GB de memoria DRAM, lo cual permitirá una mayor velocidad para el acceso y transmisión de información entre las oficinas y sucursales. Sin duda alguna, el ISR1100X Series Router mejora el desempeño de la red considerablemente, sin embargo, cabe mencionar que este dispositivo se complementa con otros, de entre los cuales se encuentra Catalyst 9200 Series Switch. La versión de este componente contiene diversos beneficios, aparte de mejorar la conectividad de redes locales entre las sucursales y oficinas, de entre los cuales se encuentran: Cifrado MACse (protege la integridad de la información de la red a nivel de enlace de datos), ancho de banda de hasta 80 Gbps, capacidad de recuperación ante fallas del hardware o software, integración del Cisco Catalyst Center (permite la gestión y el monitoreo centralizados de la red, aprovechando la IA para optimizar operaciones), y capacidad de acceder a la capa 3 (admite protocolos como OSPF, EIGRP, ISIS, y RIP, expandiendo así, las facultades de enrutamiento).

El Catalyst 9115AX Series Access Point soporta el estándar de Wi-Fi 6, esto asegura que las distintas oficinas tengan una red inalámbrica con la mejor conectividad, rapidez y una alta tasa de estabilidad permitiendo la conexión de varios dispositivos sin presentar ningún efecto negativo en la conectividad a la red. Así mismo la implementación de este dispositivo nos permitirá la creación de VLANs, creando así, redes exclusivas para el tipo de persona que se encuentre en la oficina tanto por empleados como clientes todo esto sin ninguna diferencia en la velocidad y capacidad. Finalmente, la naturaleza de este dispositivo ayuda a que la implementación de estos sea escalable permitiendo aumentar la capacidad en caso de ser necesario. Para concluir con los dispositivos propuestos es importante mencionar el uso del dispositivo UCS C220 M7 Rack, este dispositivo es un servidor en rack permitiendo la escalabilidad de estos a medida que las necesidades de la compañía aumente. Dentro de los beneficios que este rack proporciona una de las cualidades clave es la asignación automática de direcciones IP así como el almacenamiento de datos, como lo son bases de datos, aplicaciones empresariales almacenamiento general, y correcta distribución de estas a los diferentes dispositivos que necesitan conectarse a la red. Debido a que ambas oficinas cuentan con un servidor esto permitirá que las oficinas mantengan sus servicios locales así como la redundancia entre ellas, además de esto al ser un servidor físico este se puede virtualizar permitiendo a las oficinas aprovechar de mejor manera los recursos disponibles así como reducir los costos operativos del hardware.

DISEÑO FÍSICO

Para el primer boceto del diseño físico y poder en buena fe determinar cuáles serían los dispositivos y la cantidad de los mismos necesarios para poder mejorar el funcionamiento de la red y tecnología en la compañía se realizó el siguiente análisis:

https://www.canva.com/design/DAGokBp0aRE/zkffM5qrvHxkphtKliAE7g/edit?utm_content=DAGokBp0aRE&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton

DISEÑO LÓGICO

Posterior al análisis físico de los dispositivos a emplearse, optamos por determinar la mejor forma de configurar los dispositivos siguiendo la normativa estandarizada por organismos internacionales e independientes, por ello, realizamos el siguiente análisis de diseño lógico, donde se estableció un boceto para cada uno de los corporativos y sus puntos de venta, estableciendo las IPs, máscaras de subred y las VLANs, por emplearse:

https://docs.google.com/spreadsheets/d/1iMzfkqS7B2JtOJZSi7BzAZnq0JhmgTJbdAoOHjskaCw/edit?usp=sharing

PRESUPUESTO DE LOS COMPONENTES ELECTRÓNICOS

Como primer plan para asegurar los dispositivos para el cliente, es necesario realizar un listado de los dispositivos con su valor de mercado para poder establecer un primer presupuestado y presentarlo al cliente.

https://docs.google.com/spreadsheets/d/1jWHf_ShhxsWxyHlSrl5-NLto7fBy067Cq6pyU_E6Pls/edit?usp=sharing

PROPUESTAS DE SOLUCIÓN

Reemplazo de Switches Obsoletos y No Administrables

- Problemática Detectada:
    - Se utilizan hubs, routers residenciales y switches no administrables que impiden la gestión eficiente de la red.
    - No se puede monitorear ni aplicar políticas de red, lo que genera cuellos de botella y pérdida de conectividad.
    - Alta latencia en la transmisión de datos y fallas frecuentes en servicios críticos.
- Propuesta de Solución
    - Implementar switches administrables de capa 3 en todas las sucursales y en el corporativo, adoptando una topología jerárquica y cableado estructurado categoría 6A. Esta infraestructura permitirá segmentar el tráfico, aplicar políticas de QoS, y mejorar significativamente la eficiencia, estabilidad y escalabilidad de la red.
- Indicadores de Desempeño
    - Reducción del 35% en la latencia promedio de red.
    - Disminución del 50% en interrupciones no planificadas por fallos de red.
    - Mejora del 40% en la eficiencia de los sistemas POS y ERP.
    - Cumplimiento con estándares TIA/EIA-568-C para cableado.
    - Escalabilidad garantizada para duplicar nodos sin rediseño físic

Homologación del Sistema Operativo Empresarial

- Problemática Detectada
    - Existen múltiples versiones de sistemas operativos, incluyendo versiones obsoletas y sin soporte.
    - Se presentan incompatibilidades y vulnerabilidades de seguridad.
    - Dificultades en administración centralizada y gestión de actualizaciones.
- Propuesta de Solución
    - Estandarizar todos los equipos con Windows 11 Enterprise y servidores con Windows Server, integrando a todos al dominio mediante Active Directory, GPOs, WSUS o Microsoft Intune para una gestión unificada, segura y eficiente de todos los dispositivos.
- Indicadores de Desempeño
    - Reducción del 70% en incidencias relacionadas con software obsoleto.
    - Unificación del 100% del parque informático bajo políticas GPO.
    - Mejora del 45% en velocidad de despliegue de actualizaciones.
    - Reducción del 60% en vulnerabilidades críticas detectadas.

Implementación de Segmentación Lógica con VLANs

- Problemática Detectada:
    - La red actual es plana y sin segmentación, lo que permite tráfico no controlado entre todas las áreas.
    - Aumenta el riesgo de propagación de amenazas y congestión de tráfico.
    - No se pueden aplicar políticas de prioridad ni seguridad por función.
- Propuesta de Solución:
    - Diseñar e implementar VLANs funcionales (POS, administración, seguridad, invitados) con ruteo inter-VLAN gestionado por switches de capa 3 utilizando OSPF. Esta segmentación aumentará la seguridad, eficiencia y control sobre el tráfico, permitiendo aplicar políticas diferenciadas por área.
- Indicadores de Desempeño:
    - Reducción del 60% en tráfico innecesario entre áreas.
    - Incremento del 25% en velocidad de acceso a servicios internos clave.
    - Aislamiento lógico de amenazas con reducción de superficie de ataque.
    - Aplicación de políticas de acceso personalizadas por VLAN.
    - Monitoreo detallado

Conectividad Estable y Redundante entre Sedes

- Problemática Detectada
    - Las sucursales dependen de conexiones residenciales o VPNs inestables.
    - Frecuentes interrupciones afectan sistemas de nómina, ventas e inventario.
    - No hay mecanismos de respaldo ni balanceo automático.
- Propuesta de Solución
    - Migrar a enlaces empresariales con fibra dedicada (DIA) o redes MPLS con contratos SLA, integrando balanceo de carga y failover automático para mantener la operación continua incluso ante fallos de un proveedor.
- Indicadores de Desempeño
    - Reducción del 90% en caídas de conexión entre sedes.
    - Disponibilidad de red superior al 99.95% garantizada por SLA.
    - Tiempo de recuperación ante fallos reducido de horas a segundos.
    - Optimización del tráfico con balanceo inteligente (hasta 40% más eficiente).
    - Mayor confiabilidad en servicios críticos con respaldo automático.

Implementación de Firewalls de Nueva Generación

- Problemática Detectada
    - La seguridad perimetral es mínima o inexistente en muchas sedes.
    - La red está expuesta a ataques externos, malware y accesos no autorizados.
    - No hay herramientas de detección ni control granular del tráfico.
- Propuesta de Solución
    - Implementar firewalls de nueva generación (NGFW) con IDS/IPS, VPN IPsec, filtrado web, control de aplicaciones y registro de tráfico. Estos equipos permitirán proteger la red ante amenazas externas y tener visibilidad detallada del uso de la red.
- Indicadores de Desempeño
    - Disminución del 80% en incidentes de seguridad perimetral.
    - Detección temprana del 95% de amenazas conocidas con IDS/IPS.
    - Reducción del 70% en el tráfico no autorizado mediante filtrado web.
    - Aumento del 50% en cumplimiento de normativas de seguridad.
    - Mejora de la trazabilidad del tráfico con logs centralizados.

Redundancia ante Fallos Críticos (Eliminación de SPOFs)

- Problemática Detectada
    - La red y la energía presentan puntos únicos de falla (SPOFs).
    - Cualquier fallo desconecta completamente servicios clave.
    - No existen mecanismos de respaldo automático ni energía redundante.
- Propuesta de Solución
    - Incorporar conectividad Dual WAN con failover automático y sistemas UPS para energía continua en puntos críticos. Esto garantizará la disponibilidad continua de servicios ante fallos de red o energía.
- Indicadores de Desempeño
    - Reducción del 95% en tiempo de inactividad por fallos.
    - Recuperación automática de conectividad en menos de 10 segundos.
    - Aumento del 99.9% en uptime de servicios prioritarios.
    - Mitigación total de SPOFs en sedes principales y servidores.
    - Cumplimiento con políticas de continuidad operativa.

Reestructuración del Esquema de Direccionamiento IP

- Problemática Detectada
    - El direccionamiento IP es desordenado, sin separación funcional ni jerarquía.
    - Se generan conflictos de IP y dificultades para monitorear o crecer la red.
    - No existe asignación automática centralizada ni nombres consistentes.
- Propuesta de Solución
    - Diseñar un esquema de direccionamiento estructurado con subredes /24 por función (ventas, administración, seguridad, invitados) y asignación vía DHCP centralizado, con resolución DNS empresarial. Esto permitirá orden, escalabilidad y trazabilidad completa de dispositivos.
- Indicadores de Desempeño
    - Reducción del 100% en conflictos de IP por duplicidad.
    - Mejora del 45% en trazabilidad de dispositivos en la red.
    - Escalabilidad habilitada para duplicar áreas sin rediseño.
    - Reducción del 60% en tiempo de configuración de nuevos nodos.
    - Monitoreo automatizado de nodos por subred con herramientas SNMP.

REFERENCIAS

Ortega, R. (2024, November 28). *La Digitalización del Retail: Un Mercado de Crecimiento para los Canales en México*. eSemanal - Noticias Del Canal. https://esemanal.mx/2024/11/la-digitalizacion-del-retail-un-mercado-de-crecimiento-para-los-canales-en-mexico/

Rodríguez, E. M. (2025, March 14). Comercio electrónico en México creció 20% en 2024, alcanzó un valor de 789,000 millones de pesos. *El Economista*. https://www.eleconomista.com.mx/el-empresario/comercio-electronico-mexico-crecio-20-2024-alcanzo-valor-789-000-millones-pesos-20250312-750213.html

Storecheck, R., & Storecheck, R. (2025, January 22). *Recap del Retail 2024 en México: Adaptación y nuevas oportunidades*. Blog Storecheck. https://blog.storecheck.com.mx/retail-2024-en-mexico-adaptacion-y-nuevas-oportunidades/

Spec Sheet Cisco UCS C220 M7 SFF Rack Server. (n.d.). Retrieved May 27, 2025, from https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m7-sff-specsheet.pdf

Cisco Catalyst 9115AX Series Access Point Getting Started Guide. (2025, March). Cisco. https://www.cisco.com/c/en/us/td/docs/wireless/access_point/9115ax/quick/guide/ap9115ax-getstart.html#pgfId-95427

Cisco Catalyst 9200 Series Switches. (2024, July). Cisco. https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html#Productoverview

Cisco 1000 Series Integrated Services Routers. (2024, October). Cisco. https://www.cisco.com/c/en/us/products/collateral/routers/1000-series-integrated-services-routers-isr/datasheet-c78-742893.html?dtid=osscdc000283&linkclickid=srch