DESCRIPCIÓN GENERAL

Nomenclatura	Significado
ID. General	Estándar Equipo Tecnológico CI-12-2024
CI-E47	Estándar de conmutador de distribución de capa de red
20240202	Fecha de actualización

Modelos de referencia

En febrero del 2024 se verificó este estándar frente a los siguientes equipos del mercado.

- ✓ Meraki MS390-24UX-HW

DESCRIPCIÓN TÉCNICA

A partir de este punto es la descripción técnica a utilizar en el proceso de compra correspondiente, copie a partir de este punto.

----------**Inicio de descripción técnica**----------

Referencia: CI- E47-20240202 (favor no remover o modificar esta referencia)

1. Características físicas

1.1. Contener 2 puertos de pila dedicados que permitan apilar al menos 8 unidades y proporcionen al menos 480Gbps de capacidad de apilamiento.

1.2. Debe contar con la capacidad de apilar y compartir las fuentes de poder de al menos 4 unidades permitiendo la continuidad de un miembro de la pila aun cuando ha perdido ambas fuentes de poder.

1.3. Conmutador con al menos 24 puertos 100M/1G/2.5G/5G/10G RJ45, con al menos 8 puertos 10 GigabitEthernet basados en SFP+ (Small Form-Factor Pluggeable) con el módulo MA-MOD-8X 10G

1.4. Puertos 100M/1G/2.5G/5G/10G BASE-T Ethernet (RJ45) con soporte de detección auto-MDIX crossover y auto negociación de velocidad.

1.5. 1 interfaz de administración dedicada

1.6. Debe contar con fuentes de poder de al menos 1100W de potencia para suministrar alimentación eléctrica a equipos directamente conectados en cualquiera de los 24 puertos.

1.7. Debe contar con ventiladores redundantes y reemplazables en caliente.

1.8. Debe tener la capacidad de soportar fuente de alimentación redundante reemplazable en caliente.

2. Característica de rendimiento

2.1. Priorización de tráfico vía Calidad de Servicio 802.1p, con hasta 8 colas de Clase de Servicio (CoS) por puerto

2.2. Etiquetado de hasta 4094 VLAN's soportando troncales 802.1q

2.3. Soporte de estándares Spanning Tree y Rapid Spanning Tree 802.1d y 802.1w

2.4. Manejo de control de tormentas de difusión (broadcast storm)

2.5. Soporte de Link Layer Discovery Protocol LLDP 802.1ab

2.6. Capacidad de agregación de hasta 8 puertos en un enlace lógico vía estándar LACP 802.3ad

2.7. Capacidad de espejeo de puertos para necesidades de monitoreo continuo de tráfico

2.8. Soporte de puertos espejo o SPAN

2.9. Soporte de IGMP snooping para filtrado de tráfico multicast

2.10. Soporte para control de flujo

2.11. Apilamiento físico de hasta 8 unidades con un ancho de banda de 480Gbps bidireccional

2.12. Los equipos deberán tener una fábrica de conmutación de segmentos ethernet sin bloqueos o sobresubscripción alguna (non-blocking).

2.13. Los equipos contarán con una latencia mínima de conmutación de 2.5 microsegundos

2.14. El equipamiento deberá soportar Jumbo Frames Ethernet de 9600 bytes

2.15. Se requieren 8 enlaces de uplink de 10Gbps dedicados que puedan usar fibra

2.16. La capacidad de conmutación del equipo deberá ser basado en una arquitectura sin bloqueos, y de al menos 480 Gbps

2.17. Capacidad de entrada de direcciones MAC: 24 puertos: 16.000

2.18. Tasa de conmutación (aplica a modelos PoE y no-PoE): 24 puertos: 476.19Mpps

2.19. Soporte de PoE (802.3af), PoE+ (802.3at), UPoE (802.3bt)

2.20. Compatilibidad PoE/PoE+: minimo 560W (con una fuente de poder) 1440W (Con dos fuentes de poder)

3. Características de seguridad

3.1. El equipo deberá permitir el acceso a la red mediante previa autorización a través del pro-tocolo 802.1x

3.2. El equipo deberá tener la capacidad de permitir el acceso al puerto físico del switch depen-diendo de la dirección MAC del dispositivo que busca el acceso.

3.3. El Equipo deberá soportar microsegmentación con etiquetas de grupos de seguridad. (SGT)

3.4. El equipo deberá tener la capacidad de evitar que BPDUs del protocolo spanning tree pue-dan ingresar por un puerto que está identificado como puerto de acceso. Cuando el equipo detecte que existe un intento de introducir un BPDU por un puerto de acceso, el puerto de acceso deberá inhabilitarse temporalmente.

3.5. El equipo deberá tener la capacidad de evitar que BPDUs del protocolo spanning tree, en una métrica superior, puedan ingresar por un puerto en estado “designado” y de tal forma modificar la topología indeseada. Cuando el equipo detecte que esto suceda, el puerto deberá inhabilitarse hasta que tales eventos cesen.

3.6. Los equipos podrán registrar vía direcciones IP los servidores legítimos DHCP que existan en la red para efectos de seguridad

3.7. Deberá contar con mecanismos para garantizar que el sistema operativo sea íntegro y consistente en todos los switches

3.8. El equipo deberá ser capaz mediante 802.1x de asignar la VLAN a la cual pertenece puerto del switch en donde se conecta el cliente en base a las credenciales que el usuario presen-ta ante la infraestructura de red

3.9. Soporte de listas de control de acceso

3.10. Bypass de autenticación basada en dirección MAC

3.11. Soporte de RADIUS COA y accounting

4. Características de administración

4.1. Gestión y control centralizados en la forma de una consola de administración basada en Web desde la cual se deberá poder acceder, configurar y monitorear todos los equipos de SD-WAN+UTM, Puntos de acceso Inalámbricos WiFi, switches LAN considerados en esta licitación.

4.2. Tal gestión y control puede ser un sistema basado en nube, como servicio del fabricante de los equipos propuestos.

4.3. La gestión deberá ser un sistema que contenga redundancia de hardware y geográfica en su implementación, y deberá ser capaz de administrar al menos 20,000 equipos.

4.4. El acceso a la consola central deberá ser por HTTPS y sus certificados de seguridad deberán ser emitidos por entidades reconocidas en Internet.

4.5. Capacidad de registrar y desplegar los equipos de forma automática, basado en su número serial u otro identificador, para otorgarles su configuración y versión de sistema operativo correspondientes.

4.6. La conectividad con los equipos gestionados deberá ser de una forma segura (encriptada) y con un ancho de banda que no exceda los 3kbps por equipo.

4.7. Durante la vida del contrato, los equipos propuestos deberán poder recibir sus parches y actualizaciones de software, empujados de forma centralizada y calendarizables conforme haga sentido.

4.8. Igualmente se espera que la consola central de gestión sea actualizada por el sistema en un máximo de 1 mes a partir que el fabricante haya anunciado parches y mejoras.

4.9. Los equipos propuestos deberán de seguir brindando servicios de conectividad incluso ante eventualidades de imposibilidad de estar conectados a su consola de gestión central.

4.10. Deberán existir mecanismos para agrupar lógicamente la administración de un número determinado de dispositivos SD-WAN+UTM, Puntos de acceso

Inalámbricos Wifi, switches LAN para propósitos de empujar cambios simultáneos en sus configuraciones y tener homogeneidad de estas

4.11. De igual manera, desde la misma consola de administración basada en Web, se deberán poder generar los reportes de utilización históricos, así como datos de su uso en tiempo real, correspondientes a todos los equipos de SD-WAN+UTM, Puntos de acceso Inalámbrico WiFi, switches LAN, objeto de esta licitación, ya sea individual o grupal

4.12. La consola deberá ser accesible desde cualquier equipo que cuente con conexión a Internet tanto al interior como al exterior de las instalaciones usando navegadores de Internet populares y en versiones aún soportadas por el mismo desarrollador

4.13. El acceso a la consola de administración deberá ser capaz de realizarse mediante un método de autenticación de dos factores (two-factor authentication), incluyendo, mas no limitado, a nombre de usuario y contraseña más una app de soft-token en dispositivos móviles

4.14. La consola deberá de tener controles que forcen a los administradores a: cambiar contraseña periódicamente, limitar el reuso de contraseñas pasadas, implementar contraseñas robustas, congelar sus cuentas en casos repetidos de ingreso incorrecto de contraseña y sacarlos de la consola en caso de inactividad

4.15. Deberá haber una bitácora de quién y a qué hora han intentado entrar al sistema de gestión, incluyendo dirección IP de proveniencia y locación estimada

4.16. Deberá haber una bitácora de quién, hora y qué cambios se hicieron a las configuraciones de los equipos gestionados por medio de tal plataforma

4.17. La consola de gestión debe tener la capacidad de limitar las peticiones de ingreso provenientes de direcciones IP especificadas

4.18. Deberá de haber un mecanismo para medir el ancho de banda entre los equipos y el sistema de gestión centralizado

4.19. Soporte de SAML para poder ingresar a la plataforma de gestión mediate uso de credenciales institucionales

4.20. La consola de administración deberá soportar la definición de cuentas de administrador basadas en roles y permisos diferenciados.

4.21. Deberá soportar la interacción programática mediate interfases de programación de aplica-tivos RESTful (RESTful APIs) que sean abiertas, utilizando HTTPS para transporte y JSON para serialización de objetos, con repositorios públicos demostrables de código reutilizable.

4.22. La consola central tendrá capacidad de ser fuente de información SNMPv3 consolidada de los dispositivos que gestiona.

4.23. La consola deberá mostrar un inventario de los dispositivos que gestiona, mostrando al menos el número serial, dirección MAC y si está desplegado o no.

4.24. La consola deberá mostrar el estatus detallado de licenciamiento de cada dispositivo que gestiona.

4.25. Deberá mostrar una lista de los distintos sitios que tengan equipos, cantidad de éstos en línea y fuera de línea, así como un conteo de dispositivos usuarios y volumen de datos consumidos.

4.26. La herramienta de monitoreo será capaz de visualizar por sitio un perfilamiento de los dispositivos que hayan usado la red, mostrando al menos su nombre, sistema operativo, fabricante, direcciones MAC e IP y uso en volumen de datos, todo en hasta al menos 30 días.

4.27. La herramienta de monitoreo será capaz de visualizar las aplicaciones utilizadas por los dispositivos del punto anterior, proveyendo una lista con volumen de datos y cantidad de dispositivos que hayan hecho uso de tales aplicaciones en hasta al menos 30 días.

4.28. De los puntos anteriores, la herramienta deberá mostrar una gráfica de utilización de ancho de banda en hasta al menos 30 días que pueda ayudar para propósitos de planeación de capacidad.

4.29. Para propósitos del moldeado de una Política de uso Aceptable de la Red Institucional, la herramienta de gestión central permitirá entrar al detalle individual de cada dispositivo que ha usado la red para conocer a detalle su historial de

navegación.

4.30. Se podrán hacer capturas de paquetes directamente desde la herramienta de gestión, en cualquiera de los dispositivos gestionados y en cualquiera de sus interfases.

4.31. La solución de gestión / monitoreo deberá mostrar toda actividad de navegación que cruza la infraestructura gestionada, incluyendo aplicaciones usadas, con dominios visitados o direcciones IP de sitios, el protocolo usado, el volumen de datos en total dividido en enviado y recibido, la cantidad de flujos, tiempos activos, y su cantidad de usuarios, todo en hasta 30 días de uso.

4.32. Garantía:

4.32.1 Se contará con acceso ilimitado a actualizaciones de software, gestión centralizada y so-porte telefónico en español con servicio telefónico dentro de Costa Rica y América Latina durante 60 meses.

4.32.2 Los equipos deberán estar garantizados, el estar soportados por el fabricante al menos 5 años después del anuncio de fin de venta de estos.

4.32.3 Los equipos contar con una garantía que reemplazo del siguiente día hábil.

4.32.4 Soporte de fábrica 8x5xNBD a 60 meses.

4.33. Adicionalmente:

4.33.1 Los equipos deben ser 100% compatibles con la nube de gestión de telecomunicaciones Meraki que está vigente en la Universidad de Costa Rica.

4.33.2 El equipo debe ser compatible con los teléfonos IP y puntos de acceso inalámbricos marca Cisco utilizados en la plataforma de la Universidad de Costa Rica.

4.33.3 El equipo ofertado debe ser funcionalmente compatible a nivel de hardware y protocolos con los equipos cisco series 4500, 3800, Nexus 7000, Nexus 9000 y demás dispositivos de enrutamiento y conmutación existentes en el núcleo, distribución y acceso, de la Universidad de Costa Rica de forma que se garantice la interoperabilidad completa del sistema.

4.33.4 El equipo debe ser adquirido por medio de un canal certificado como DISTRIBUIDOR AUTORIZA-DO del fabricante, que asegure la efectiva "Garantía de Fábrica" del equipo ofrecido en Costa Rica.

4.33.5 Este canal debe aportar copia del certificado vigente de Cisco Gold Certified Partner para brindar servicio de soporte en Costa Rica. Esta certificación debe ser dirigida a la Universidad de Costa Rica e incluir la marca y el modelo del equipo que es ofrecido, con una antigüedad no mayor de 3 meses de emitida.

4.33.6 El equipo adquirido debe ser registrado ante el fabricante a nombre de la Universidad de Costa Rica.

----------**Fin de descripción técnica**----------

APARTADO DE ACCESORIOS Y EQUIPAMIENTO OPCIONAL A CONSIDERAR
Se excluye de la definición formal del estándar las características relacionadas con componentes y/o accesorios adicionales tales como:

a) n/a

Dado que los requerimientos de cada usuario varían de acuerdo a necesidades específicas, la unidad solicitante de la compra deberá determinar las características de los componentes y/o accesorios adicionales que se requieren. En caso de ser necesario, el Centro de Informática puede brindar la asesoría correspondiente.

RESPONSABLE Y REVISIONES:

Actividad	Rol
Elaboración	Xiomara Céspedes Jiménez, Colaboradora Unidad de Gestión de Adquisiciones (UGA) Rebeca Esquivel Flores , Coordinadora Área de Gestión de Comunicaciones (AGC)

Revisión y visto bueno	Cindy Arias Quiel, Coordinadora (UGA)
Aprobación	**Tatiana Bermúdez Páez, Subjefa CI**

UCR Firmado digitalmente