# ANEXO 1

| CARACTERISTICAS | | | |
|---|---|---|---|
| Item | SWITCH DE RED CORE | Requisitos mínimos | Descripcion Solucion |
| 1 | Marca | | |
| 2 | Modelo | Debe ser catalogado en el fabricante como Familia: Small Business | |
| 3 | Número de Switch Core incluidos en la solución | 2 | |
| 4 | numero de puertos solicitados | 48 GE | |
| 5 | capacidad de enrutamiento capa 3 | Si | |
| 6 | ¿Es rackeable? | SI | |
| 7 | Memoria de CPU ARM de 800 MH | 256 MB | |
| 8 | Memoria flash | 32 MB | |
| 9 | Buffer de paquetes | 2*10 Mb | |
| 10 | Certificación | UL (UL 60950), CSA (CSA 22.2), marcación CE, FCC Parte 15 (CFR 47) Clase A | |
| 11 | tiempo medio entre fallas | 166 790 hras | |
| 12 | Puertos Uplink de enlaces | 4 x 10 GE (4 XG SFP+ (dos ranuras SFP combinadas de 5G)) | |
| 13 | Capacidad de conmutación y velocidad de transferencia. Todos los conmutadores son de velocidad de cable y no bloqueantes | Capacity in mpps (64-byte packets): 130<br>Switching Capacity (Gbps): 170 | |
| 14 | Spanning Tree Protocol | Standard 802.1d Spanning Tree Support<br>Fast convergence using 802.1w (Rapid Spanning Tree [RSTP]), enabled by default<br>Multiple spanning tree instances using 802.1s (MSTP). 16 instances are supported | |
| 15 | Port grouping/link aggregation | Support for IEEE 802.3ad Link Aggregation Control Protocol (LACP)<br>• Up to 32 groups<br>• Up to 8 ports per group with 16 candidate ports for each (dynamic) 802.3ad LAG | |
| 16 | Agregación de enlaces/agrupación de puertos | Compatibilidad con protocolo de control de agregación de enlaces (LACP) versión IEEE 802.3ad<br>• Hasta 32 grupos<br>• Hasta 8 puertos por grupo con 16 posibles puertos por cada agregación (dinámica) de enlaces<br>802.3ad | |
| 17 | VLAN | Admite un máximo de 4096 VLAN simultáneas: VLAN basadas en puerto, en etiquetas 802.1Q y en MAC<br>VLAN de administración<br>Perímetro de red VLAN privada (PVE), también conocido como puerto protegido, con varios uplinks<br>VLAN para usuarios temporales, VLAN sin autenticación, VLAN basada en protocolo, CPE VLAN<br>Asignación de VLAN dinámica por medio del servidor Radius junto con autenticación de cliente 802.1x | |

| | | | |
|---|---|---|---|
| 18 | VLAN de voz | El tráfico de voz se asigna automáticamente a una VLAN específica de voz y se trata con los niveles apropiados de QoS. Las capacidades de voz automáticas proporcionan implementación sin intervención, en toda la red, de los terminales de voz y dispositivos de control de llamadas. | |
| 19 | VLAN de multidifusión TV | VLAN de multidifusión TV permite compartir una VLAN de multidifusión única mientras los suscriptores permanecen en VLAN separadas. Esta característica también se conoce como registro de VLAN de multidifusión (MVR). | |
| 20 | Q-in-Q | Las VLAN cruzan de manera transparente una red de proveedor de servicios mientras aíslan el tráfico entre los clientes. | |
| 21 | GVRP/GARP | El protocolo genérico de registro de VLAN (GVRP) y el protocolo genérico de registro de atributos (GARP) permiten la propagación automática y la configuración de las redes VLAN en un dominio en puente. | |
| 22 | Detección de enlace unidireccional (UDLD) | UDLD supervisa la conexión física para detectar enlaces unidireccionales que surgen a causa de cableado incorrecto o fallas en los puertos, para prevenir bucles de reenvío y agujeros negros de tráfico en las redes conmutadas. | |
| 23 | Retransmisión DHCP en capa 2 | Retransmisión de tráfico DHCP a servidor DHCP en otra VLAN. Funciona con la opción 82 de DHCP | |
| 24 | Detección IGMP (versiones 1, 2 y 3) | El protocolo de administración de grupos de Internet (IGMP) limita el tráfico de multidifusión con uso intensivo del ancho de banda solo para los solicitantes; respalda 1000 (1024) y 4000 grupos de multidifusión (también admite multidifusión específica del origen). | |
| 25 | Función de consulta de IGMP | La función de consulta de IGMP sirve para admitir un dominio de multidifusión de capa 2 de switches de detección ante la falta de un router de multidifusión. | |
| 26 | Tramas gigantes | Tramas hasta de 9000 (9216) bytes de longitud. | |
| 27 | Routing IPv4 | Routing de paquetes IPv4 a velocidad de cable<br>Hasta 2000 (2048) rutas estáticas y hasta 256 interfaces IP | |
| 28 | Routing estático IPv6 a velocidad de cable | Hasta 2000 (2048) rutas estáticas y hasta 128 interfaces IPv6 | |
| 29 | Interfaz de capa 3 | Configuración de la interfaz de capa 3 en el puerto físico, LAG, interfaz de VLAN o interfaz de bucle invertido | |
| 30 | CIDR | Admite routing entre dominios sin clase | |
| 31 | RIP v2 | Compatible con el protocolo de información de routing versión 2, para routing dinámico | |
| 32 | VRRP | El protocolo de redundancia de router virtual (VRRP) brinda disponibilidad mejorada en una red de capa 3, pues ofrece redundancia de los hosts de servicio de la gateway predeterminada en la red.<br>Compatible con las versiones 2 y 3 de VRRP. Admite hasta 255 routers virtuales | |
| 33 | Servidor DHCP | El switch funciona como un servidor DHCP IPv4 que presta servicio a las direcciones IP para varios conjuntos/ámbitos de DHCP<br>Compatible con opciones de DHCP | |
| 34 | Retransmisión DHCP en capa 3 | Retransmisión de tráfico DHCP en dominios IP | |
| 35 | Retransmisión de protocolo UDP | Retransmisión de información de difusión en dominios de capa 3 para la detección de aplicaciones o la retransmisión de paquetes BootP/DHCP | |

| | | | |
|---|---|---|---|
| 36 | Apilamento de switch<br>Pila de hardware | Hasta 8 unidades en una pila Hasta 416 puertos administrados como un solo sistema, con conmutación<br>por falla del hardware | |
| 37 | Alta disponibilidad | La rápida conmutación por falla de la pila ofrece mínima pérdida de tráfico. | |
| 38 | Configuración/administración Plug-and-play de apilamiento | Copia de seguridad/maestra para control y recuperación de la pila<br>Numeración automática.<br>Intercambio con el sistema activo de unidades en la pila<br>Opciones de apilamiento en cadena y anillo Velocidad del puerto de apilamiento automática Opciones<br>de puerto de apilamiento flexibles | |
| 39 | Interconexiones de pila de alta velocidad | Interfaces 5G de cobre y 10G de alta velocidad de cobre y fibra | |
| 40 | SSH | SSH es un reemplazo seguro del tráfico de Telnet. SCP también utiliza SSH. Compatible con versiones<br>1 y 2 de SSH | |
| 41 | SSL | La capa de sockets seguros (SSL) cifra todo el tráfico HTTPS, lo que permite un acceso seguro a la<br>GUI de administración basada en navegador en el switch. | |
| 42 | IEEE 802.1X (función de autenticador) | Autenticación y administración de RADIUS, algoritmo hash MD5;<br>VLAN para usuarios temporales;<br>VLAN no autenticada, modo host único/múltiple y sesiones únicas/múltiples<br>Admite la asignación de red VLAN dinámica con 802.1X basada en tiempo. | |
| 43 | Autenticación web | La autenticación web proporciona control de admisión de redes mediante el navegador web para todos<br>los sistemas operativos y dispositivos de host. | |
| 44 | Protección BPDU STP | Un mecanismo de seguridad para proteger la red de configuraciones no válidas. Un puerto habilitado<br>para protección de la unidad de datos de protocolo puente (BPDU) se apaga si se recibe un mensaje<br>BPDU en ese puerto. Esta acción evita bucles de topología accidentales. | |
| 45 | Protección de raíz de STP | Esto evita que dispositivos perimetrales que no están bajo el control del administrador de la red se<br>conviertan en nodos de raíz del protocolo de árbol de extensión. | |
| 46 | Detección de DHCP | Filtra los mensajes DHCP con direcciones IP no registradas o de interfaces inesperadas o no<br>confiables. Esto evita que los dispositivos dudosos se comporten como un servidor DHCP | |
| 47 | Protección de IP de origen (IPSG) | Cuando se activa la protección de IP de origen en un puerto, el switch filtra los paquetes IP recibidos<br>desde el puerto si las direcciones IP de origen de los paquetes no se han configurado en forma estática<br>o no se han detectado dinámicamente desde la detección de DHCP. Esto evita la suplantación de<br>identidad en direcciones IP. | |
| 48 | Inspección ARP dinámica (DAI) | El switch desecha los paquetes ARP de un puerto si no hay enlaces estáticos o dinámicos IP/MAC o si<br>hay discrepancias entre las direcciones origen y destino en el paquete ARP. Esto evita los ataques con<br>intermediario | |

| | | | |
|---|---|---|---|
| 49 | Enlace de puertos IP/Mac (IPMB) | Las funciones (detección DHCP, protección de IP de origen e inspección ARP dinámica) mencionadas funcionan en conjunto para evitar ataques de DoS en la red y, de este modo, aumentan la disponibilidad de red. | |
| 50 | Secure Core Technology (SCT) | Garantiza que el switch reciba y procese el tráfico de administración y protocolo sin importar cuánto tráfico reciba. | |
| 51 | Datos confidenciales seguros (SSD) | Un mecanismo para administrar datos confidenciales (como contraseñas, claves, etc.) de manera segura en el switch, que completa estos datos en otros dispositivos y asegura la configuración automática. Se brinda acceso a una visualización de datos confidenciales como texto simple o cifrado según el nivel de acceso configurado para el usuario y el método de acceso del usuario. | |
| 52 | Aislamiento de capa 2 (PVE) con VLAN comunitaria | El perímetro de red VLAN privada ofrece seguridad y aislamiento entre los puertos del switch y, de esa manera, impide que los usuarios espíen el tráfico de otros; admite múltiples uplinks. | |
| 53 | Seguridad de puertos | Capacidad de bloquear direcciones MAC de origen a los puertos y limitar la cantidad de direcciones MAC detectadas. | |
| 54 | RADIUS/TACACS+ | Admite la autenticación de RADIUS y TACACS. Funciones de switch como cliente | |
| 55 | Administración de RADIUS | Las funciones de administración de RADIUS permiten que los datos se envíen al inicio y finalización de los servicios, e indican la cantidad de recursos (como tiempo, paquetes, bytes, etc.) que se utilizaron durante la sesión | |
| 56 | Control de tormentas | Difusión, multidifusión y unidifusión desconocida | |
| 57 | Prevención de denegación de servicio (DoS) | Prevención de ataques de denegación de servicio (DoS). | |
| 58 | Diversos niveles de privilegio para usuario en CLI | Niveles 1, 7 y 15 de niveles de privilegio | |
| 59 | Listas de control de acceso (ACL) | Admite hasta 3000.<br>Limite de velocidad o descarte en función de la dirección MAC de origen y destino, la ID de VLAN o la dirección IP, el protocolo, el puerto, el punto de código de servicios diferenciados (DSCP)/la precedencia IP, los puertos de origen y destino TCP/ UDP, la prioridad 802.1p, el tipo de Ethernet, los paquetes de protocolo de administración de grupos de Internet (IGMP), el indicador TCP<br>Admite ACL basadas en tiempo. | |
| 60 | Calidad de Servicio, Niveles de prioridad | 8 colas de hardware | |
| 61 | Programación | Prioridad estricta y operación por turnos ponderada (WRR) | |

| | | | |
|---|---|---|---|
| 62 | Clase de servicio | Basada en el puerto; basada en prioridad de VLAN 802.1p; basada en precedencia IP IPv4/v6/tipo de servicio (ToS)/DSCP; Servicios diferenciados (DiffServ); ACL de clasificación y remarcación, QoS de confianza Asignación de colas en base a punto de código de servicios diferenciados (DSCP) y clase de servicio (802.1p/CoS) | |
| 63 | Limitación de velocidad | Vigilante de tráfico entrante; modelado y control de tráfico saliente; por VLAN, por puerto y basado en el flujo | |
| 64 | Prevención de congestión | El algoritmo de prevención de congestión TCP sirve para minimizar y prevenir la sincronización global de pérdidas de TCP. | |
| 65 | Estándares | IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE- T Gigabit Ethernet, protocolo de control de agregación de enlaces IEEE 802.3ad, IEEE 802.3z Gigabit Ethernet, control de flujo IEEE 802.3x, IEEE 802.3 ad LACP, IEEE 802.1D (STP, GARP y GVRP), IEEE 802.1Q/p VLAN, STP rápido IEEE 802.1w, STP múltiple IEEE 802.1s, autenticación de acceso al puerto IEEE 802.1X, IEEE 802.3af, IEEE 802.3at, RFC 768, RFC 783, RFC 791, RFC 792, RFC 793, RFC 813, RFC 879, RFC 896, RFC 826, RFC 854, RFC 855, RFC 856, RFC 858, RFC 894, RFC 919, RFC 922, RFC 920, RFC 950, RFC 951, RFC 1042, RFC 1071, RFC 1123, RFC 1141, RFC 1155, RFC 1157, RFC 1350, RFC 1533, RFC 1541, RFC 1542, RFC 1624, RFC 1700, RFC 1867, RFC 2030, RFC 2616, RFC 2131, RFC 2132, RFC 3164, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 2576, RFC 4330, RFC 1213, RFC 1215, RFC 1286, RFC 1442, RFC 1451, RFC 1493, RFC 1573, RFC 1643, RFC 1757, RFC 1907, RFC 2011, RFC 2012, RFC 2013, RFC 2233, RFC 2618, RFC 2665, RFC 2666, RFC 2674, RFC 2737, RFC 2819, RFC 2863, RFC 1157, RFC 1493, RFC 1215, RFC 3416 | |
| 66 | IPv6 | Modo host IPv6 IPv6 por Ethernet pila doble IPv6/IPv4 Detección de router y enlaces vecinos (ND) IPv6 Configuración automática de dirección independiente del estado para IPv6 Detección de MTU de ruta Detección de dirección duplicada (DAD) ICMPv6 IPv6 por red IPv4 con respaldo para túnel ISATAP Certificaciones USGv6 y IPv6 Gold | |
| 67 | Calidad de servicio de IPv6 | Prioriza los paquetes IPv6 en el hardware | |
| 68 | ACL IPv6 | Límite de velocidad o descarte de paquetes IPv6 en el hardware | |
| 69 | Seguridad de primer salto en IPv6 | Protección de RA<br>Inspección de ND<br>Protección de DHCPv6<br>Tabla de enlaces vecinos (entradas estáticas y de falsificación)<br>Verificación de integridad de los enlaces vecinos | |
| 70 | Detección de Multicast Listener Discovery (MLD v1/2) | Entrega paquetes multidifusión IPv6 solo a los receptores requeridos | |

| | | | |
|---|---|---|---|
| 71 | Compatibilidad con IPv6<br>RFC | RFC 4443 (que vuelve obsoleto a RFC 2463) – ICMPv6<br>RFC 4291 (que vuelve obsoleto a RFC 3513) – Arquitectura de direcciones IPv6<br>RFC 4291 – Arquitectura de direcciones IP versión 6<br>RFC 2460 – Especificación de IPv6<br>RFC 4861 (que vuelve obsoleto a RFC 2461) – Detección de vecinos para IPv6<br>RFC 4862 (que vuelve obsoleto a RFC 2462) – Configuración automática de dirección independiente del estado para IPv6<br>RFC 1981 – Detección de MTU de ruta<br>RFC 4007 – Arquitectura de direcciones definidas IPv6<br>RFC 3484 – Mecanismo de selección de direcciones predeterminadas<br>RFC 5214 (que vuelve obsoleto a RFC 4214) – Túnel ISATAP RFC 4293 – MIB IPv6: Convenciones textuales y grupo general RFC 3595 – Convenciones textuales para etiqueta de flujo de IPv6 | |
| 72 | Administración Interfaz de usuario web | Utilidad de configuración de switch integrada para facilitar la configuración de dispositivos basada en navegador (HTTP/HTTPS). Admite configuración, tablero del sistema, mantenimiento del sistema y supervisión. | |
| 73 | SNMP | SNMP versiones 1, 2c y 3 compatibles con capturas y modelo de seguridad basado en el usuario (USM) para SNMP versión 3 | |
| 74 | MIB estándar | LLDP-MIB<br>lldpextdot1-MIB<br>lldpextdot3-MIB<br>lldpextmed-MIB<br>rfc2674-MIB<br>rfc2575-MIB<br>rfc2573-MIB<br>rfc2233-MIB<br>rfc2013-MIB<br>rfc2012-MIB<br>rfc2011-MIB<br>RFC-1212<br>RFC-1215<br>rfc2665-MIB<br>rfc2668-MIB<br>rfc2737-MIB<br>rfc3621-MIB<br>rfc4668-MIB<br>rfc4670-MIB<br>trunk-MIB<br>tunnel-MIB<br>udp-MIB<br>draft-ietf-bridge-8021x-MIB<br>draft-ietf-bridge-04-MIB<br>draft-ietf-hubmib-etherif-mib<br>SNMPv2-CONF<br>SNMPv2-TC | |
| 75 | RMON (supervisión remota) | El agente de software de RMON integrado admite 4 grupos de RMON (historial, estadísticas, alarmas y eventos) para una mejor administración, supervisión y análisis del tráfico | |

| | | | |
|---|---|---|---|
| 76 | Pila dual IPv4 e IPv6 | Coexistencia de ambas pilas de protocolos para facilitar la migración | |
| 77 | Actualización de firmware | • Actualización de navegador web (HTTP/HTTPS) y TFTP y SCP<br>• La actualización se puede iniciar también a través del puerto de la consola<br>• Imágenes dobles para actualizaciones con capacidad de recuperación de firmware | |
| 78 | Puertos reflejados | El tráfico de un puerto puede reflejarse en otro puerto para que lo analice un analizador de red o una sonda RMON. Se pueden reflejar hasta 8 puertos de origen en un puerto de destino | |
| 79 | Creación de reflejo de VLAN | El tráfico de una VLAN puede reflejarse en otro puerto para que lo analice un analizador de red o una sonda RMON. Se pueden reflejar hasta 8 VLAN de origen en un puerto de destino. | |
| 80 | DHCP | Las opciones de DHCP permiten realizar un control más riguroso desde un punto central (servidor DHCP) para obtener direcciones IP, configuración automática (con descarga de archivos de configuración), retransmisión DHCP y nombre de host | |
| 81 | Configuración automática con descarga de archivos con copia segura (SCP) | Permite la implementación masiva segura con protección de datos confidenciales. | |
| 82 | Configuraciones de texto editable | Los archivos de configuración pueden editarse con un editor de texto y descargarse en otro switch, lo que facilita aún más la implementación masiva. | |
| 83 | Smartports | Configuración simplificada de calidad de servicio (QoS) y capacidades de seguridad. | |
| 84 | Auto Smartports | Aplica la inteligencia que se proporciona a través de las funciones de Smartport automáticamente al puerto basada en los dispositivos detectados a través de CDP o LLDP-MED. Esto facilita las implementaciones sin intervención. | |
| 85 | Copia segura (SCP) | Permite transferir archivos de manera segura desde y hacia el switch. | |
| 86 | Textview CLI | CLI que permite ejecutar scripts. Admite CLI completa así como también CLI basada en el menú. | |
| 87 | Localización | Localización de GUI y documentación en varios idiomas. | |
| 88 | Anuncio de inicio de sesión | Anuncios diversos de inicio de sesión para web y CLI | |
| 89 | Operación de puerto basada en tiempo | Conexión y desconexión basadas en horarios definidos por el usuario (cuando el puerto está conectado administrativamente). | |

| | | | |
|---|---|---|---|
| 90 | Otras funciones administrativas | Traceroute; administración de IP única; HTTP/HTTPS; SSH; RADIUS; puertos reflejados; actualización de TFTP; cliente DHCP; BOOTP; protocolo simple de tiempo de red (SNTP); actualización de Xmodem; diagnósticos de cables; ping; syslog; cliente Telnet (admite SSH seguro); ajustes de tiempo automáticos desde la estación de administración. | |
| 91 | Detección de energía | Automáticamente corta la alimentación del puerto RJ-45 Gigabit Ethernet al detectar un enlace no disponible. El modo activo se reanuda sin pérdida de paquetes cuando el switch detecta que el enlace está nuevamente disponible | |
| 92 | Detección de longitud de cable | Ajusta la intensidad de la señal según la longitud del cable. Reduce el consumo de energía para cables de menos de 10 m. Compatible en todos los modelos Gigabit Ethernet | |
| 93 | Cumple con EEE (802.3az) | Admite IEEE 802.3az en todos los puertos Gigabit de cobre. | |
| 94 | Desactivar LED de los puertos | Los LED se pueden apagar manualmente para ahorrar energía. | |
| 95 | Tramas gigantes | Tramas hasta de 8000 bytes Compatible con interfaces 10/100 y Gigabit Ethernet La MTU predeterminada es 2000 | |
| 96 | Tabla de MAC | 16 000 (16384) direcciones MAC. | |
| 97 | Bonjour | El switch se anuncia mediante el protocolo Bonjour | |
| 98 | LLDP (802.1ab) con extensiones LLDP-MED | El protocolo de detección de capa de enlace (LLDP) permite al switch anunciar su identificación, configuración y funciones a dispositivos vecinos que guardan los datos en una MIB. LLDP-MED es una mejora de LLDP que agrega las extensiones requeridas para los teléfonos IP | |
| 99 | Discovery Protocol | El switch se anuncia mediante el protocolo CDP. También detecta el dispositivo conectado y sus características por medio de CDP. | |
| 100 | Consumo de energía (peor caso) | Disipación de calor (BTU/h):1570 | |
| Items | REQUERIMIENTOS FUNCIONALES | Requisitos mínimos | |
| 1 | ¿El switch de core permite realizar segmentacion de trafico en Layer 3? | Si | |
| 2 | Conectar sus usuarios a la red con capacidades integrales de Capa 2 y Capa 3 de conmutación, la movilidad, la seguridad, la visibilidad de las aplicaciones, segmentación y calidad de servicio | SI | |
| 3 | Gestionar de forma transparente LAN heterogéneos y distribuidos. | Si | |
| 4 | Escalar en la red para la expansión de los negocios con la Capa 3 avanzada. | Si | |
| 5 | Segmentar la red para la seguridad, el cumplimiento y los procesos de negocio complejos | Si | |
| 6 | Optimizar la utilización de la infraestructura de red. | Si | |
| Items | REQUERIMIENTOS INSTALACION | Requisitos mínimos | |

| | | | |
|---|---|---|---|
| 1 | El precio de la solución incluye la instalación y configuración | Si | |
| 2 | La solución incluye transferencia de conocimiento en la configuración de la solución | Si | |
| 3 | Quien instalará los equipos debe tener las certificaciones y experiencia en la instalación del producto con aval del fabricante, debe incluir certificación del ingeniero por parte del proveedor de la solución. | Si | |
| Item | GARANTIA | Requisitos mínimos | |
| 1 | Garantía ofrecida para todo el hardware | 3 años | |
| 2 | Modalidad de garantía / Tiempo de respuesta ante incidentes para todo el hardware | 8x5xNBD | |