SNPP
SERVICIO NACIONAL DE PROMOCIÓN PROFESIONAL

LICITACIÓN POR CONCURSO DE OFERTAS
LCO N° 13/15

"SERVICIO ESTRUCTURADO DE VOZ Y DATOS, DATACENTER Y EQUIPOS DE REDES (LAN, WLAN) - AD REFERENDUM"

ID PORTAL N° 295.939

ADENDA 03

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

Asunción, 15 de junio de 2015

ADENDA Nº 03

El Servicio Nacional de Promoción Profesional emite la Adenda N° 03 que formará parte del llamado a Licitación por Concurso de Ofertas LCO N° 13/15 "SERVICIO ESTRUCTURADO DE VOZ Y DATOS, DATACENTER Y EQUIPOS DE REDES (LAN, WLAN) - AD REFERENDUM" con ID 295.939. A partir de esta adenda queda redactada de la siguiente forma:

Sección I. Datos de la Licitación (DDL)

	B. Contenido de los Documentos de la Licitación
IAO 7.1	Para **aclaraciones de las ofertas,** solamente, la dirección de la Convocante es: SERVICIO NACIONAL DE PROMOCIÓN PROFESIONAL Atención: **ABG.CARLOS MARIA RUÍZ GONZÁLEZ** Dirección: Molas López N° 480 e/ Tte. Cirilo Gill y Thomas Isasi. Ciudad: Asunción, Paraguay Teléfono: 021 605 490 int. 8195 Fax: 021 605 490 Dirección de correo electrónico: uocsnpp@gmail.com **La fecha y hora límites para realizar consultas es: 19 de junio de 2015 hasta las 08:00 hs.**
	D. Presentación y Apertura de Ofertas
IAO 23.1	**Para propósitos de la presentación de las ofertas**, la dirección de la Convocante es: SERVICIO NACIONAL DE PROMOCIÓN PROFESIONAL Atención: ABG. CARLOS MARÍA RUÍZ GONZÁLEZ Dirección: Molas López N° 480 e/ Tte. Cirilo Gill y Thomas Isasi. Número del Piso/Oficina: 1er. Piso, Oficina de la UOC. Ciudad: ASUNCION, Paraguay La fecha límite para presentar las ofertas es: Fecha: **29 de junio de 2015** Hora: **08:00 a.m.**
IAO 26.1	**La apertura de las ofertas tendrá lugar en**: SERVICIO NACIONAL DE PROMOCION PROFESIONAL Dirección: Molas López N° 480 e/ Tte. Cirilo Gill y Thomas Isasi. Número de Piso/Oficina Primer piso oficina UOC. Ciudad: Asunción, Paraguay Fecha: **29 de junio de 2015** Hora: **08:10 a.m.**

Sección III. Suministros Requeridos

1. ESPECIFICACIONES TECNICAS

Objetivo: solución integral de instalación de cableado estructurado cat 6 Y provisión y configuración de equipos activos de (lan, wlan)

CONSIDERACIONES GENERALES.

El alcance de estas especificaciones tiene como objetivo ilustrar a todos los Oferentes sobre los criterios que deberán ser respetados para la cotización y posterior realización del proyecto de referencia, para el **SNPP CENTRO TECNOLOGICO DE AVANZADA PARAGUAY COREA**, Ubicado en Mcal. Estigarribia km 10/2 San Lorenzo, en lo que a Cableado del Sistema de Voz y Datos se refiere, así también del suministro de los equipos activos de red, las descripciones de los mismos y accesorios necesarios para su implementación.

Será entera responsabilidad del proveedor por los trabajos de Elaboración del Proyecto, Provisión de materiales, ejecución del proyecto y puesta en marcha, certificación de los puntos de red y verificación técnica para la entrega final por parte del fabricante de los productos proveídos. ***TODOS ESTO EN MODALIDAD LLAVE EN MANO***, o sea incluyendo todos los accesorios e insumos, trasmisión de conocimiento técnico a los funcionarios designados por la Dirección de Tecnología de Información y Comunicación sobre los equipos activos proveídos por el oferente, y los equipamientos necesarios para garantizar las mejores prácticas acorde a las normas internacionales de cableado estructurado de la EIA y TIA o similares como así también las certificaciones de los productos utilizados por ETL y UL (laboratorios mundiales de certificación de productos) o similares.

Los bienes y servicios ofertados deberán ser presupuestados atendiendo siempre a estas especificaciones técnicas y que cada oferente lo analizará entendiendo que será el marco mínimo a ser respetado tanto en la cotización como en la realización si fuere posteriormente adjudicado. Todo trabajo incluido en estas especificaciones deberá cumplir con las leyes, códigos y reglas aquí mencionadas así como a las reglas del buen arte inherentes a la realización de los diversos trabajos a ser realizados.

NORMAS GENERALES.

Cableado Estructurado.

El Sistema de Cableado Estructurado de voz y datos para el cableado debe cumplir con las especificaciones de CATEGORIA 6A (ANSI/TIA-568-C.2 o ISO/IEC 11801)

Las normas y recomendaciones consignadas en esta infraestructura serán los siguientes estándares y adendas.

ANSI/TIA/EIA–568C Comercial Building Wiring Standard, que permite la planeación e instalación de un sistema de Cableado Estructurado que soporta independientemente del proveedor y sin conocimiento previo, los servicios y dispositivos de telecomunicaciones que serán instalados durante la vida útil del edificio.
EIA/TIA-568-C.0 (Cableado Genérico de Telecomunicaciones para establecimientos de clientes)
EIA/TIA-568-C.1 (Estándar de cableado de Telecomunicaciones para construcciones comerciales)
EIA/TIA-568-C.2 (Estándar para componentes y cableado de par trenzado compensado)
EIA/TIA-568-C.3 (Estándar para componentes de cableado de fibra óptica)
ANSI/TIA 569C (Aprobado: 3 Mayo 2012) Commercial Building Standard for Telecomunications Pathways and Spaces, que estandariza prácticas de diseño y construcción dentro y entre edificios, que son hechas en soporte de medios y/o equipos de telecomunicaciones tales como canaletas y guías, facilidades de entrada al edificio, armarios y/o closet de comunicaciones y cuarto de equipos.
ANSI/TIA 606B (Rev. TIA-606-A – Aprobado 22 Junio 2012). Administration Standard for the Telecomunications Commercial Building dura of Comercial Buildings, que da las guías para marcar y administrar los componentes de un sistema de Cableado Estructurado.
TIA-607-B: Requisitos para telecomunicaciones de empalme y puesta a tierra de edificios comercialesCommercial Building Grounding (Earthing) and Bonding Requeriments for Telecomunications, que describe los métodos estándares para distribuir las señales de tierra a través de un edificio.
TIA-1152: Pautas sobre la prueba de cobre
UL-1449 "Underwriters Laboratories (3ra Edición de UL 1449)"

ESPECIFICACIONES PARA CABLEADO UTP Y FIBRA OPTICA

Cableado Estructurado Horizontal

Para la solución UTP, el canal completo categoría 6 deberá cumplir con las pruebas de rendimiento y desempeño de la ANSI/TIA-568-C.2 o ISO/IEC 11801 con Cables Categoría 6A para 90 metros de cable UTP, 10 metros de patch cords y cuatro (4) conectores en el canal. Para esto, el postor deberá adjuntar el reporte de certificación de un laboratorio independiente de prestigio (no fabricantes) como UL o ETL.
Todos los componentes del cableado estructurado deberán ser del mismo fabricante tales como patch cords, cable UTP, Jacks RJ45, patch panel, ordenador horizontal y faceplate.

Cable UTP:
El cable UTP es el usado para el tendido del cableado horizontal, no debe exceder de 90 metros desde el Outlet al Patch Panel por cada enlace
Cable de cobre Unshield Twisted Pair de 4 pares trenzados, 23-24 AWG, 100 Ohm, en presentación de cajas selladas.

Avda. Molás López N°480
Asunción - Paraguay
Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

Debe cumplir o superar las especificaciones de la norma ANSI/TIA-568-C.2 o ISO/IEC 11801 con Cables Categoría 6A Transmission Performance Specifications for 4 Par 100 Ω Category 6 Cabling y los requisitos de cable categoría 6 (clase E) de la norma ISO/IEC 11801.
El cable debe tener aislante de polietileno y la chaqueta del cable UTP debe ser del tipo CMR.
Debe contar con certificado UL o ETL en conjunto con los conectores ofertados.
El cable debe tener un separador de pares del tipo cruz y debe ser retardante a la flama.

Line Cords:

El Line Cord es el cable utilizado para conectar el equipo periférico (PC, Servidor, Impresora, o similar) con la toma para datos conformada por el Jack y el Face Plate.
El Line Cord debe estar conformado solamente por cable de cobre multifilar Unshield Twisted Pair de 4 pares trenzados 24 AWG, y con un plug RJ45 Categoría-6 de 8 posiciones en cada extremo. Debe estar confeccionado integralmente por el fabricante en configuración según el esquema T568.
Debe cumplir con las pruebas de performance de la ANSI/TIA-568-C.2 o ISO/IEC 11801 con Cables Categoría 6A , certificados por Laboratorios independientes: UL o ETL.
Los Line Cords deberán ser ensamblados y certificados de fábrica.
Debido a que es UTP no deberán contar con ningún blindaje o malla eléctrica alrededor el plug.
Debe tener una variedad de 8 colores para poder identificar el servicio según la TIA/EIA 606A.
Los Plug RJ45 de cada Line Cord deben tener un sistema anti enredo o capuchas como parte del Plug RJ45 para evitar atascos durante movimientos o reordenamiento y no deberán tener algún accesorio que amplíe sus dimensiones laterales.
La longitud del Line Cord debe ser no mayor a 3 metros.

Patch Cords:

El Path Cord es el cable utilizado para conectar el Patch Panel con el equipo activo de red (switch, hub o similar) en configuración directa o en configuración cross-connect.
El Patch Cord Categoría-6 debe estar conformado solamente por cable de cobre multifilar Unshield Twisted Pair de 4 pares trenzados 24 AWG y con un plug RJ45 Categoría-6 de 8 posiciones en cada extremo. Debe estar confeccionado integralmente por el fabricante en configuración según el esquema T568.
Los Patch Cords deberán ser ensamblados y certificados de fábrica.
Debe tener una variedad de 8 colores para poder identificar el servicio según la TIA/EIA 606A.
Debido a que es UTP no deberán contar con ningún blindaje o malla eléctrica alrededor el plug.
Los Plug RJ45 de cada Parch Cord deben tener un sistema anti enredo o capuchas como parte del Plug RJ45 para evitar atascos durante movimientos o reordenamiento y no deberán tener algún accesorio que amplié sus dimensiones laterales.
Debe cumplir con las pruebas de performance de la ANSI/TIA-568-C.2 o ISO/IEC 11801 Categoría-6, certificado por Laboratorios independientes: UL o ETL.
La chaqueta del cable UTP debe ser de PVC, tipo No Plenum.
La longitud del Patch Cord debe ser de 1.5 metros para los gabinetes. Garantizando un correcto ordenamiento de cables con los ordenadores solicitados para el patch panel y gabinete.

Avda. Molás López N°480
Asunción - Paraguay
Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

Patch Panel:

Debe permitir la inserción de al menos 24 jacks de categoría 6 o 24 jacks de categoría 6A UTP o 24 acopladores LC duplex, a fin de garantizar upgrades futuros.

Deben ser modulares y permitir la instalación de diferentes conectores: UTP categoría 6, Coaxial, Tipo F de audio, RCA, fibra óptica: ST, SC, LC y MTRJ, etc. a fin de asegurar la inversión a futuro respecto a las tendencias en tecnologías.

Cada jack del patch panel debe cumplir con las pruebas de performance de la ANSI/TIA-568-C.2 o ISO/IEC 11801 Categoría-6, certificado por laboratorios independientes: UL o ETL.

Deben ser modulares puerto por puerto de tal forma que pueda ser posible cambiar un jack individualmente en caso de fallas y no se requiera tener que adquirir un bloque o módulo de 04 o 06 jacks ni tener que cambiar todo el Patch Panel.

Los conectores RJ45 ofertados para los patch panels deben permitir trabajar con el mapa de cables T568A o el T568B.

Cada puerto frontal RJ45 debe soportar como mínimo 750 inserciones de Plug RJ45 de 8 posiciones La máscara el patch panel debe ser de material metálico.

Debe tener 19 pulgadas de ancho para ser instalados en los racks o gabinetes.

Deben permitir la conexión total de las salidas de información de todas las aplicaciones (datos, voz,, etc.), perfectamente identificados en el panel, y con todos los requerimientos para facilitar la administración y manejo de la red, de acuerdo con la norma ANSI/TIA/EIA 606A.

Deben contar con una protección plástica transparente que impida el contacto directo de las manos u otros objetos con las etiquetas garantizando con ello su longevidad de acuerdo a la ANSI/TIA/EIA 606A.

Los Patch Panels deben permitir la instalación de los jacks ofertados.

Se deberán colocar modulo individuales / tapas de color negro en todos los puertos no utilizados del Patch Panel.

Deben contar con Certificación ISO 9001.

TOMA PARA PARA RED CON CATEGORIA 6 (285 doscientos ochenta y cinco puntos) puntos detallados en el plano y más 01 en caseta de GUARDIA, ESTA CANTIDAD INCLUYE LAS CONEXIONES DE DATOS PARA PC, WLAN, TELEFONIA IP Y LAS CONEXIONES PARA CAMARAS IP), TAMBIEN DEBE CONTEMPLAR LA PROVICION DE CABLES ADICIONAL PARA CAMARAS PTZ EN 05 PUNTOS A SER CONFIRMADOS POR EL CONVOCANTE.

LOS PUNTOS ESTÁN DISTRIBUIDOS EN 3 BLOQUES DE EDIFICIOS DE LA SIGUIENTE MANERA:
BLOQUE A: PLANTA BAJA C/DATACENTER INTERMEDIO 45 PUNTOS, PRIMER PISO 22 PUNTOS
BLOQUE BC: PLANTA BAJA 09 PUNTOS
BLOQUE D: PLANTA BAJA AREA EDUCATIVA TIC 140 PUNTOS,
PRIMER PISO AREA EDUCATIVA MECATRONICA 25 PUNTOS,
SEGUNDO PISO AREA EDUCATIVA DISEÑO DE MODAS Y DATACENTER PRINCIPAL 42 PUNTOS,
CASETA DE GUARDIA 02 PUNTOS *Deberá (llegar los cables de datos, telefonía ip , cámara ip)*
Enlace entre Datacenter Principal (Bloque D) y Datacenter Secundario (Bloque A) a 10GB
Patch Cords: 30 unidades adicionales para los teléfonos IP

Patch Cords: para PCs en su totalidad en bases a la cantidad de Puntos en referencia.
Conexión de Teléfonos IP debe estar Disponible en los puntos de red en las oficinas administrativas del bloque A, BC, D y caseta de guardia todos con conexión POE según como defina el convocante.
LOS PUNTOS DE ACCESOS INALAMBIRCOS DEBEN ESTAR DISTRIBUIDOS EN EL EDIFICIO COMO SIGUE:

BLOQUE A PB: 03
BLOQUE A PP: 02
BLOQUE BC PB: 02
BLOQUE D PB: 02
BLOQUE D PP: 02
BLOQUE D SP: 02
a confirmar: 02

Fibra Óptica Tipo OM3 o superior – Multimodo, 50 / 125 uM con 12(doce) fibras internas para instalación en ducto subterráneo con protección tipo lámina metálica anti Roedores y protección contra humedad.
2(dos) Distribuidores Internos Ópticos (DIO) del Tipo Rackeable de 1U – 300mm de profundidad con al menos 16(dieciséis) Conectores tipo LC-LC conectorizado y con prueba de funcionamiento con la Fibra Óptica solicitada.
El DIO Proveído debe poseer bandeja deslizable para fácil acceso a la fibra óptica. Además debe poseer Charola porta empalmes y sujetador de exceso de cable.
4(cuatro) Cables de Interconexión Óptica Tipo OM4 con conectores tipo LC-LC, Multimodo 50 / 125 uM Instalación con todos los accesorios y partes necesarios para su funcionamiento a cargo del proveedor.

EL ASEGURAMIENTO DE PROVISION DEL SISTEMA ELECTRICO CON LOS ESTANDARES REQUERIDOS PARA LOS EQUIPOS ACTIVOS DE LA RED ES RESPONSABILIDAD DEL PROVEEDOR.
Deberán instalarse cajas externas dobles por área de trabajo, la salida no utilizada deberá ir con tapa ciega.
Deberá permitir la inserción de un icono de identificación sobre cada salida RJ45 para identificar si el servicio es de telefonía o datos.
Debe permitir la inserción de: jacks de categoría 6 o jacks de categoría 6A UTP o acopladores LC duplex, a fin de garantizar upgrades futuros.
Debe incluir sus tornillos de sujeción y etiquetas de identificación para cada puerto, con cobertor transparente.

Jacks RJ45 Categoría 6
Deben ser de categoría 6 de acuerdo a la ANSI/TIA-568-C.2 o ISO/IEC 11801 Debe ser de 8 posiciones tipo IDC, para conectorización sin herramienta de impacto.
Debe permitir la conectorización tipo T568A o T568B contando con una etiqueta que indique el método para ello.
Deberán contar con una certificación component compliance emitida por algún laboratorio neutral de pruebas tipo UL o ETL.
Deben asegurar la no desconexión del cable UTP sólido al ser expuesto a jalones, contando para ello con una tapa o seguro sobre las conexiones del cable UTP y las conexiones IDC.
Debe permitir la inserción de iconos plásticos.

Avda. Molás López N°480
Asunción - Paraguay
Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

El fabricante debe contar con al menos 8 colores distintos (TIA/EIA 606A) a fin de facilitar la administración.
Debe cumplir con los requerimientos de IEC60603-7 de acuerdo a la TIA/EIA 568B.
Debe poder ser instalado en los faceplates como en los patch panels suministrados.
Debe permitir la inserción de patch cord de 2 y 4 pares sin degradarse.
Deben contar con Certificación ISO9001.

Ordenador Horizontal de Cables

Tipo frontal con tapas para proteger a los cables de golpes o aplastamientos.
El área de sección frontal debe permitir alojar 48 cables sin que estos resulten presionados contra las paredes.

Deben ser de 2 unidades de rack (2 RU), color negro y de 19" de ancho
Deberán contar con un sistema que garantice el radio de giro de los Patch Cords en su ingreso y salida del Ordenador.
Deberán contar con elementos de fijación que soporten a los cables y eviten que estos se caigan al ser retiradas las tapas o en todo caso deberán contar con tapas abisagradas.
Deberá contar con una dimensión mínima frontal de (75 x 75) mm (alto x profundidad)
Se instalarán cada 02 Patch Panels y cada Patch Panel será de 24 puertos RJ45 de tal forma que el ordenador de 2RU tendrá un Patch Panel de 24 puertos encima y otro debajo.
Opcionalmente podrán incluir accesorios que protegen el radio de giro en a la entrada y salida del ordenador.
Deberán contar con por lo menos 02 accesos para el paso de los cables de la parte frontal a la parte posterior del Ordenador.
Deben contar con Certificación ISO 9001.

RACK PARA DATACENTER PRINCIPAL E INTERMEDIO

Deberán contar Cada uno como mínimo conforme a las especificaciones técnicas.

- Bastidor de 19" estándar;
- Altura de 42 a 45U;

RACK DE COMUNICACION

Los Rack de 9U mínimo del tipo pivotante para los equipos de accesos conforme a las especificaciones técnicas.
Si existiera por alguna razón en caso excepcional también se podría usar rack de piso de 12 U 19" estándar, todo cerrado con llave de seguridad incorporado

IDENTIFICACIÓN, SEÑALIZACIÓN Y ORDENAMIENTO

Todos los elementos del Sistema de Cableado Estructurado incluyendo: Cables, Punto de la estación de trabajo, Patch Panel, Racks, Sala Técnica y Datacenter principal e intermedio, deberán contar con una identificación única de acuerdo a lo indicado por la ANSI/TIA 606B (Rev. TIA-606-A – Aprobado 22 Junio 2012).

Todas las identificaciones deberán ser impresas con impresora láser o de transferencia térmica, no se aceptarán impresiones en impresora de tinta, matricial o a mano.

En todos los casos la identificación deberá ser fácilmente visible y deberá estar basada en etiquetas adhesivas siendo necesaria que adicionalmente cuenten con alguna protección plástica que impida el contacto directo de las manos con la impresión. Las etiquetas para cables y tubos podrán ser auto laminables.

El Fabricante de las etiquetas, y los elementos de soporte de las etiquetas debe contar con Certificación ISO 9001.

Todos los cables deberán agruparse por zonas usando cintas (cintas tipo velcro) los mismos que deberán incluso colocarse dentro de los Ordenadores de Cables Verticales antes del ingreso de cables a los Ordenadores Horizontales, no se permitirá el uso de cintillos plásticos para esta labor.
Se deberá adjuntar una planilla de identificación de infraestructura de enlaces según 5.5.1 Sistema de Administración Clase I - ANSI/TIA 606B (Rev. TIA-606-A – Aprobado 22 Junio 2012).

GARANTIAS CABLEADO ESTRUCTURADO

La garantía de instalación que deberá presentar el postor adjudicado debe ser emitida por el Fabricante de la solución de cableado estructurado por un tiempo mínimo de 3 años, en la que se especifique una garantía de fabricación de los componentes, performance, aplicaciones y mano de obra por un tiempo de mínimo de 3 años.

La garantía por mano de obra por parte del fabricante significa que en caso de que algún producto con falla de fábrica aplicación presente o futura que se desarrolle para trabajar sobre la categoría solicitada, no cumpla con lo solicitado tenga que ser cambiada, el fabricante se comprometerá a cubrir con el total de costos (mano de obra por re-instalación, viáticos, pasajes, etc, los gastos que fueran necesarios) que demande dichos cambios adicionalmente al cambio de productos, independientemente si es que el postor existiera o no a la fecha de presentado el problema, sin perjuicio alguno para el centro asistencial.
La garantía deberá contemplar el cambio de componentes incluyendo el servicio ante el incumplimiento por falla de origen de los componentes, por falla de los parámetros de performance solicitados y por falla de las aplicaciones garantizadas. Estos cambios se realizarán a solicitud de la entidad y con la comprobación del postor o fabricante del producto.

El fabricante debe contar con oficinas o representante legalmente constituidas en el Paraguay y una persona de soporte para el trámite de garantías.

Se debe incluir junto con la garantía la relación de aplicaciones soportadas por el fabricante para la solución de cableado estructurado requerida en las bases.
Se debe incluir un informe impreso y electrónico de verificación por cada punto de los parámetros de performance según la TIA/EIA-568C según la Categoría requerida para el presente proceso, esto se realizará con un equipo certificador para medir estos parámetros de performance.

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

Todos los elementos de cableado estructurado que conformaran el canal de comunicación deberán ser de una única MARCA, elaborados por un único FABRICANTE, no se aceptaran productos con diferente marca así pertenezcan al mismo grupo económico de manera que se asegure la total compatibilidad electrónica entre los elementos de cableado y se prevengan degradaciones en el desempeño de la red.

Debe adjuntarse a la propuesta todos los certificados y especificaciones técnicas de los productos ofrecidos de modo a garantizar la calidad de los productos y que cumplan con lo solicitado.

LA GARANTÍA DE MANTENIMIENTO UN MÍNIMO DE 3 AÑOS

PLANOS.

El SNPP entregará los planos del edificio con la ubicación de la Sala Técnica, Rack Principal y Racks Intermediarios y Ubicación de los puntos de manera a que los oferentes puedan realizar el proyecto técnico acorde a las normas de cableado estructurado internacional (EIA- TIA)

LOS PLANOS EN PDF Y AUTOCAD EN FORMATO DIGITAL PODRÁN SER RETIRADOS POR LOS POTENCIALES OFERENTES, DEL DEPARTAMENTO CENTRO TECNOLÓGICO DE AVANZADA CTA DEL SNPP CENTRAL, TERCER BLOQUE, EN AVDA. MOLAS LÓPEZ N° 480 E/ TTE. CIRILO GILL Y THOMAS ISASI; EN HORARIO DE 07:00 A 12:00 HS.

SOBRE EL PERSONAL QUE PRESTARA LOS SERVICIOS

La firma contratada deberá presentar certificados de entrenamiento internacional del personal; en las áreas de Cobre, Fibra Óptica, Datacenter y Diseño.

La firma contratada es responsable del desempeño, responsabilidad, experiencia e instrucción para el cumplimiento del servicio contratado, así como también del comportamiento y trato con el personal de la institución.

CERTIFICACIÓN Y ACEPTACIÓN DEFINITIVA.

Para la aceptación definitiva del cableado estructurado de Datos, el contratista deberá presentar como mínimo, la siguiente documentación debidamente certificada por los fiscales:

Plano físico actualizado (as built) del proyecto final, en archivo informático, indicando claramente el tendido de los cables (indicando tipos de cables, cantidades y todos materiales utilizados)

Plano lógico del cableado que coincida perfectamente con las etiquetas del cableado (cables, Patch Panel, cajas, etc.).

Documentación de todo lo instalado en cada rack. Una copia deberá quedar en cada rack.

Cualquier otra documentación relativa al proyecto que pueda ser requerida por los fiscales.

Presentación dela documentación del resultado de las mediciones de cada punto del cableado de la RED de Datos, Telefonía efectuados con los equipos de Testeo (Certificación para cables de categoría 6).

DOCUMENTACION ADICIONAL

Se deberá adicionar a la documentación a presentar información de detalle de montajes y estadísticas de instalación donde figuren fotos de los racks terminados, de los puestos de usuarios y de puntos especiales como cruces de tuberías, acometidas, etc

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

Adicionalmente se entregará en formato electrónico la documentación reseñada:
• Se permite tanto Soporte CD-ROM como DVD-R (2 copias).
La documentación se entregará en idioma castellano y debidamente identificado no así los resultados técnicos, con indicación de la fecha de realización de la instalación. Los formatos informáticos para la documentación presentada son los siguientes:
• Ficheros de texto: La Memoria final de la Instalación se deberá suministrar
En los siguientes formatos: MICROSOFT WORD (*.DOC)
DOCUMENT FORMAT (*.PDF)
•Diagramas: Se deberán proporcionar en los formatos AUTOCAD (*.DWG),
PORTABLE DOCUMENT FORMAT (*.PDF) y VISIO (*.VSD)

CRONOGRAMA DE IMPLEMENTACIÓN DE LA RED:
El oferente deberá presentar un cronograma de implementación de trabajos siendo el plazo máximo de 30 días calendario.

ALCANCE DEL PROYECTO.
El Oferente deberá instalar y terminar la red pasiva y activa incluyendo todos los accesorios y materiales necesarios, como lo indica esta especificación técnica.
En este proyecto cada oferente es responsable de contemplar en sus propuestas todos los elementos que hagan falta para la correcta implementación del cableado estructurado para Datos.

EQUIPOS ACTIVOS PARA EL CABLEADO ESTRUCTURADO

LA INSTACION, CONFIGURACION Y LA PUESTA EN MARCHA "MODALIDAD LLAVE EN MANO", SE DEBE INSTALAR UN SISTEMA DE MONITOREO CENTRALIZADO DE LOS EQUIPOS, ADEMAS EL PROVEEDOR ADJUDICADO DEBE PROPORCIONAR EL ENTRENAMIENTO TECNICO DE USO COMO MINIMO DE TRES PERSONAS DECIGNADO POR EL SNPP PARA LA ADMINISTRACION DE LOS EQUIPOS DE LA RED.

Los Conmutadores Centrales y de Acceso así como el Controlador Wireless deberán ser de la misma marca para garantizar al oferente la compatibilidad plena del sistema y facilitar la Configuración y Administración del mismo desde la consola de un solo fabricante.
El Firewall podrá ser de una marca diferente o del mismo fabricante siempre que se ajuste a las especificaciones técnicas requeridas.

PARTIDA	DESCRIPCIÓN
	CONMUTADORES DE DATOS
	UNIDAD DE CONMUTACION DE DATOS TIPO BACKBONE (NODOS CENTRALES)
CANT: 1	El equipo será el responsable de crear el *backbone* de de transporte de la LAN en redes pequeñas y/o medianas o será responsable de proporcionar puertos de acceso para redes empresariales basadas en la tecnología de Ethernet, FastEthernet, GigabitEthernet y tener soporte de alta densidad de 10 Gigabit y deberá cumplir con las siguientes especificaciones técnicas.

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

ESPECIFICACIONES TECNICAS

SOBRE LA UNIDAD

El *Switch* de *Backbone* se refiere a un conmutador de datos tipo chasis de 6 ranuras de interfaces. Soporte de conmutación (switcheo) y enrutamiento (routing) de paquetes en capa 2 Ethernet, capa 3 (IPv4 e IPV6) y capa 4 (TCP y UDP) como mínimo. Deberá tener funciones avanzadas de capa 4 y estar listo para transportar aplicaciones de voz sobre IP.

El Switch de Backbone debe estar basado en una arquitectura de switcheo CrossBar. No se aceptarán switches con backplane de ancho de banda compartido.

Para la unidad *Switch* de *Backbone* , el equipo deberá tener una capacidad de *backplane* pasivo de 520 Gbps y hasta 390 Mpps de throughput como minimo.

El equipo deberá ser provisto con redundancia en fuentes de poder y en controladoras.

La unidad deberá tener una arquitectura basada en chasis modular. No se aceptarán arquitecturas de switcheo distribuidas o similares.

Todos los módulos deberán tener características de inserción "en caliente", Hot-Swap, que permita introducir o remover componentes estando la unidad en plena operación, como lo son módulos de puertos de servicio, procesadora, fuentes de poder y ventiladores.

Soporte IEEE 802.3az Energy Efficient Ethernet: baja consumo de potencia en periodos de enlace fuera de servicio.

Soporte IEEE 802.3af Power over Ethernet (PoE).

Soporte IEEE 802.3at Power Over Ethernet Plus

Soporte Prestandard PoE: Compatibilidad con dispositivos que soportan prestandard PoE.

Se requiere de funcionalidades de redundancia que cumplan con lo siguiente:

- Virtual Router Redundancy Protocol: VRRP permite que grupos de dos routers se respalden entre sí dinámicamente para crear entornos enrutados de alta disponibilidad.
- Protocolo Spanning Tree IEEE 802.1s de múltiples instancias: proporciona alta disponibilidad de enlaces en varios entornos de VLAN al permitir múltiples Spanning Trees; engloba el protocolo Spanning Tree IEEE 802.1D y el protocolo Spanning Tree rápido IEEE 802.1w.
- Agregación IEEE 802.3ad Link Aggregation Control Protocol (LACP): admite hasta 60 trunks, con hasta 8 enlaces (puertos) cada uno; es posible establecer trunks desde diferentes módulos.
- Agregación distribuida de enlaces para evitar tener puntos únicos de falla.

La unidad deberá poder montarse en un rack de 19 pulgadas.

CARACTERISTICAS SWITCHING L2

VLAN Tagging: Soporte de 2048 IEEE 802.1Q standard simúltaneamente.

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	Soporte standard IEEE 802.1v VLANs por protocolo. VLANs basadas en MAC. Soporte GARP protocol de registro de VLAN o equivalentes, misma o mejor funcionalidad Soporte de IEEE 802.1ad Q-in-Q para conexión de múltiples LANs en un campus de alta velocidad o red metro. LLDP-MED (Media Endpoint Discovery): extensión del estandar LLDP que almacena valores de parámetros como QoS y VLAN para automaticamente configurar dispositivosde red como teléfonos IP.
	CARACTERISTICAS SWITCHING L3 Enrutamiento IP estático para IPv4 e IPv6. Soporte del protocol de enrutamiento dinámico Routing Information Protocol (RIP): RIPv1 y RIPv2. Soporte de protocol de enrutamiento dinámico OSPF: OSPFv2 para IPv4 y OSPFv3 para IPv6. Soporte PBR Policy-based routing usa clasificador para seleccionar el tráfico que será enviado basado en la política definida por el administrador de la red. Soporte protocolo de enrutamiento dinámico BGP4 para IPv4 Border Gateway routing protocol. IP multicast routing : PIM Sparse y PIM Dense mode para enrutar tráfico IP multicast. IP multicast snooping (data-driven IGMP): automaticamente previene flooding de tráfico IP multicast.
	SEGURIDAD Access control lists (ACLs): Basadas en campo dirección IP origen/destino, dirección/subred IP, Puerto de origen/destino TCP/UDP por VLAN o por puerto. DHCP protection: bloqueo paquetes DHCP de servers DHCP no autorizados, previniendo ataques DoS . Administración Segura: SSHv2, SSL, y/o SNMPv3. Switch CPU protection: prove protección automatic contra tráfico de red malicioso tratando de hacer shut down al switch. ICMP throttling: defiende contra ataques DoS de ICMP. Identity-driven ACL: enables implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user.

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

STP BPDU port protection.

Dynamic IP lockdown: trabaja con la protección de DHCP para bloquear el tráfico desde hosts no autorizados, previniendo spoofing de dirección IP de origen.

Dynamic ARP protection.

STP Root Guard.

Detección de ataques maliciosos: monitorea 10 tipos de tráfico de red y envía un warning cuando una anomalía que potencialmente puede ser causada por un ataque malicioso es detectada.

Port security: allows access only to specified MAC addresses, which can be learned or specified by the administrator.

MAC address lockout: previene que direcciones MAC configuradas se conecten a la red.

Source-port filtering: allows only specified ports to communicate with each other

Seguridad en Switch login: puede usar RADIUS o TACACS+ para autenticación para logon seguro en la interfaz CLI del switch.

Security banner: despliega un mensaje de política de seguridad personaliazado cuando los usuarios se conectan al login del switch.

Multiples metodos de autenticación:

IEEE 802.1X: provee autenticación de múltiples usuarios IEEE 802.1X por puerto; previene "piggybacking" de usuario sobre la autenticación IEEE 802.1X de otro usuario.

Autenticación basada en Web: autenticación desde browser Web para clientes que no soportan supplicant IEEE 802.1X.

Autenticación basada en MAC: el cliente es autenticado basado en servidor RADIUS con las direcciones MAC de los clientes.

Esquemas de autenticación concurrentes IEEE 802.1X, Web, y MAC por puerto: el puerto del switch aceptará hasta 32 sesiones de autenticación IEEE 802.1X, Web y dirección MAC.

Virus throttling: detecta patrones de tráfico típicos de WORM y acelera o previene que el virus sea diseminado a través de VLANs enrutadas or bridged interfaces, sin requerir

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	appliances externos.
	SOBRE LA ADMINISTRACION LOCAL La unidad deberá poder configurarse por medio de un solo puerto de consola con interface RS-232 (DB-9). Funcionalidades equivalentes a RMON, XRMON y sFlow v5: ofrecen funcionalidades avanzadas de monitorización y notificación de estadísticas, históricas, alarmas y eventos. Acceso seguro a la gestión: todos los métodos de acceso —interfaz de línea de comandos, GUI o MIB— están cifrados de forma segura a través de SSHv2, SSL y/o SNMPv3. Soporte SNMP v1, v2c y v3. Despliegue de estadísticas rápidas de ACL (listas de acceso) y QoS, interfaces IP Bitácoras del sistema Bitácora de Syslog La unidad deberá contar con indicadores luminosos tipo LED, para monitoreo local a fin de supervisar el estatus del chasis encendido, fallo en la alimentación de una fuente de poder; en puertos de servicio indicar el estado de los enlaces, actividad del puerto y fallo del puerto. El software del sistema y el de los módulos de servicio deberá poder ser migrado a nuevas versiones de manera remota y local dentro de las instalaciones del cliente. Port Mirroring Remoto: duplica el tráfico seleccionado de entrada/salida basado en listas de control de acceso, puerto, dirección MAC o VLAN hacia un conmutador remoto o local en cualquier lugar de la red. El equipo deberá de tener administración jerárquica y protección de passwords para la interface de administración El equipo deberá ser capaz de guardar una bitácora de eventos El equipo deberá de tener herramientas de ping y traceroute tanto para IPv4 como para IPv6 El equipo deberá tener la capacidad de generar y filtrar alarmas detalladas y jerárquicas e información de debug del equipo Capacidad de salvar y restaurar la configuración total del equipo. Soporte de múltiples archivos de configuración almacenados en flash para restaurarlos cuando sea necesario. Soporte de dos versiones de sistema operativo para que se pueda tener la contingencia en caso de actualización del sistema operativo y poder hacer el respectivo roll back. Soporte de TFTP y Secure FTP. El sistema deberá de contar con una herramienta de administración gráfica

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	Autoejecucion segura USB: Configura, diagnostica y actualiza el conmutador desde la unidad flash USB; funciona con credenciales seguras para evitar la manipulación.
	SOBRE LAS FUNCIONALIDADES Y COMPATIBILIDADES La unidad deberá tener funciones de Conmutación de Paquetes de Capa 2, 3 y 4 según el modelo de referencia OSI. **Gestión de dispositivos** RFC 1591 DNS (cliente) HTML y gestión telnet **Protocolos generales** IEEE 802.1ad Q-in-Q (Licencia Premium) Puentes MAC IEEE 802.1D Prioridad IEEE 802.1p VLANs IEEE 802.1Q Varios Spanning Trees IEEE 802.1s Clasificación de IEEE 802.1v VLAN por protocolo y por puerto Reconfiguración rápida de Spanning Tree IEEE 802.1w IEEE 802.3ad Link Aggregation Control Protocol (LACP) Power over Ethernet IEEE 802.3af Control de flujo IEEE 802.3x RFC 768 UDP Protocolo RFC 783 TFTP (revisión 2) RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 854 TELNET RFC 868 Time Protocol RFC 951 BOOTP RFC 1058 RIPv1 Protocolo RFC 1350 TFTP (revisión 2) CIDR RFC 1519 Extensiones BOOTP RFC 1542 Simple Network Time Protocol (protocolo sencillo de tiempo en red) v4 RFC 2030 RFC 2131 DHCP RFC 2453 RIPv2 RFC 2548 (MS-RAS-sólo proveedor) Opción de información de agente de relé DHCP RFC 3046 RFC 3576 Ext to RADIUS (sólo CoA) VRRP RFC 3768 (Licencia Premium) VLAN y prioridad RFC 4675 RADIUS **IP multicast** PIM de modo disperso RFC 2362 (Licencia Premium) RFC 3376 IGMPv3 (sólo joins de host) PIM de modo denso RFC 3973 (Licencia Premium) **IPv6** RFC 1981 IPv6 Path MTU Discovery (Detección de MTU de ruta IPv6, RFC 1981)

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	RFC 2460 IPv6 Specification (Especificación RFC 2460 IPv6) RFC 2461 IPv6 Neighbor Discovery (Detección de IPv6 vecino, RFC 2461) RFC 2462 IPv6 Stateless Address Auto-configuration (Configuración automática de dirección sin estado IPv6) RFC 2462 RFC 2463 ICMPv6 RFC 2710 Multicast Listener Discovery (MLD) (Detección de oyente multicast para RFC 2710) para IPv6 Operaciones remotas 2925 MIB (sólo Ping) MIB MLDv1 RFC 3019 RFC 3315 DHCPv6 (sólo cliente) RFC 3513 IPv6 Addressing Architecture (Arquitectura de direcciones IPv6, RFC 3513) RFC 3596 DNS Extension for IPv6 (Extensión para IPv6, RFC 3596 DNS) RFC 3810 MLDv2 (sólo joins de host) MIB para TCP RFC 4022 MIB para UDP RFC 4113 Arquitectura SSHv6, RFC 4251 Autenticación SSHv6, RFC 4252 Capa de transporte SSHv6, RFC 4253 Conexión SSHv6, RFC 4254 MIB para IP, RFC 4293 Intercambio de claves para SSH, RFC 4419 Switch Snooping IGMP & MLD, RFC 4541 **MIBs** RFC 1213 MIB II MIB de bridge RFC 1493 RFC 1724 RIPv2 MIB RFC 1850 OSPFv2 MIB RFC 2021 RMONv2 MIB RFC 2096 MIB de tabla de reenvío IP RFC 2613 SMON MIB MIB de cliente RFC 2618 RADIUS MIB de administración RADIUS RFC 2620 RFC 2665 Ethernet-Like-MIB RFC 2668 802.3 MAU MIB MIB de bridge RFC 2674 802.1p e IEEE 802.1Q MIB de entidad RFC 2737 (Versión 2) MIB de VRRP RFC 2787 RFC 2863 The Interfaces Group MIB MIB de ping RFC 2925 **Gestión de redes** IEEE 802.1AB Link Layer Discovery Protocol (LLDP) Cuatro grupos de RFC 2819 RMON: 1 (estadísticas), 2 (historial), 3 (alarmas) y 9 (incidencias) sFlow RFC 3176 ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED) SNMPv1/v2c/v3

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	XRMON **OSPF** RFC 2328 OSPFv2 (Licencia Premium) RFC 3101 OSPF NSSA **Calidad del servicio/Clase de servicio** DiffServ Precedence RFC 2474, incluidos 8 puertos/colas RFC 2597 DiffServ Assured Forwarding (AF) RFC 2598 DiffServ Expedited Forwarding (EF) **Seguridad** Control de acceso de red basado en puerto IEEE 802.1X RFC 1492 TACACS+ RFC 2865 RADIUS (sólo cliente) RFC 2866 administración de RADIUS Secure Sockets Layer (SSL) SSHv1/SSHv2 Secure Shell
	CONEXIONES Y DENSIDAD DE PUERTOS
	SOBRE LA DENSIDAD DE PUERTOS POR UNIDAD La unidad deberá soportar las densidades máximas y características en puertos que se describen a continuación: 08 Puertos 10 Gigabit Ethernet (Se deberán proveer los SFP+ para cada puerto 10GbE) 24 puertos 10/100/1000 Gig-T PoE+. 24 puertos 10/100/1000 Gig-T. Para puertos de 1 Gbps la sobresuscripción al backplane del equipo deber ser menor a 1:1 Para puertos de 10 Gbps la sobresuscripción al backplane del equipo deber ser menor a 4:1
	SOBRE LA ESCALABILIDAD DEL EQUIPO El equipo debe ser un equipo preparado para soportar alta densidad de puertos 10 Gigabit ethernet manteniendo el rendimiento y arquitectura non-blocking.
	GARANTIA 3(tres) años. Mano de Obra, Partes, Repuesto en las oficinas de la Convocante sin cargo. Nivel de Soporte Mínimo Requerido: Modalidad 8x5 – Atención Telefónica, Reemplazo al siguiente día laboral de Hardware.

PARTIDA	DESCRIPCIÓN
	CONMUTADORES DE DATOS
	UNIDAD DE CONMUTACION DE DATOS TIPO ACCESO (NODOS CENTRALES) con ALIMENTACION SOBRE ETHERNET (PoE)

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

CANT: 1(uno)	El equipo será el responsable de proporcionar el acceso a la LAN para estaciones terminales o servidores departamentales basadas en la tecnología de Ethernet, FastEthernet, GigabitEthernet y tener soporte de puertos de 10 Gigabit y deberá cumplir con las siguientes especificaciones técnicas.
	ESPECIFICACIONES TECNICAS
	SOBRE LA UNIDAD El *Switch* de *acceso* se refiere a un conmutador de datos de 24 puertos. Soporte de conmutación (switcheo) y enrutamiento (routing) de paquetes en capa 2 Ethernet, capa 3 con enrutamiento estático, RIPv1, RIPv2 (IPv4 e IPV6). Soporte POE+. Deberá estar listo para transportar aplicaciones de voz sobre IP. Para la unidad *Switch* de *Acceso*, el equipo deberá tener una capacidad de *tráfico de conmutación* no menor a 128 Gbps y no menos a 95 Mpps de throughput. Asimismo, el equipo deberá contar con la capacidad de soportar redundancia en fuentes de poder. Se requiere de funcionalidades de redundancia que cumplan con lo siguiente: • Protocolo Spanning Tree IEEE 802.1s de múltiples instancias: proporciona alta disponibilidad de enlaces en varios entornos de VLAN al permitir múltiples Spanning Trees; engloba el protocolo Spanning Tree IEEE 802.1D y el protocolo Spanning Tree rápido IEEE 802.1w. • Agregación IEEE 802.3ad Link Aggregation Control Protocol (LACP): admite hasta 24 trunks, con hasta 8 enlaces (puertos) cada uno. Soporte IEEE 802.3af Power over Ethernet (PoE). Soporte IEEE 802.3at Power Over Ethernet Plus Soporte Prestandard PoE: Compatibilidad con dispositivos que soportan prestandard PoE. Soporte administración con una dirección IP para stack virtual hasta de 16 switches. Auto MDIX. La unidad deberá poder montarse en un rack de 19 pulgadas.
	CARACTERISTICAS SWITCHING L2 VLAN Tagging: Soporte de 256 IEEE 802.1Q standard simúltaneamente (soporte de 4094 Vlan IDs). Soporte standard IEEE 802.1v VLANs por protocolo. Soporte GARP protocol de registro de VLAN. o equivalentes, misma o mejor funcionalidad

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	LLDP-MED (Media Endpoint Discovery): extensión del estandar LLDP que almacena valores de parámetros como QoS y VLAN para automaticamente configurar dispositivosde red como teléfonos IP. Soporte IEEE 802.1AB LLDP.
	CARACTERISTICAS SWITCHING L3 Enrutamiento IP estático para IPv4. Soporte del protocolo de enrutamiento dinámico Routing Information Protocol (RIP): RIPv1 y RIPv2. IP multicast snooping (data-driven IGMP): automaticamente previene flooding de tráfico IP multicast.
	SEGURIDAD Access control lists (ACLs): Basadas en campo dirección IP origen/destino, dirección/subred IP, Puerto de origen/destino TCP/UDP por VLAN o peor puerto. DHCP protection: bloqueo paquetes DHCP de servers DHCP no autorizados, previniendo ataques DoS . Administración Segura: SSHv2, SSL, y/o SNMPv3. Identity-driven ACL: enables implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user. STP BPDU port protection. Dynamic ARP protection. STP Root Guard. Detección de ataques maliciosos: monitorea 10 tipos de tráfico de red y envía un warning cuando una anomalía que potencialmente puede ser causada por un ataque malicioso es detectada. Port security: allows access only to specified MAC addresses, which can be learned or specified by the administrator. MAC address lockout: previene que direcciones MAC configuradas se conecten a la red.

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	Source-port filtering: allows only specified ports to communicate with each other Seguridad en Switch login: puede usar RADIUS o TACACS+ para autenticación para logon seguro en la interfaz CLI del switch. Banner customizable: despliega un mensaje de política de seguridad customizado cuando los usuarios se conectan al login del switch. Múltiples métodos de autenticación: IEEE 802.1X: provee autenticación de hasta 8 usuarios IEEE 802.1X por puerto; previene "piggybacking" de usuario sobre la autenticación IEEE 802.1X de otro usuario. Autenticación basada en Web: autenticación desde browser Web para clientes que no soportan supplicant IEEE 802.1X. Autenticación basada en MAC: el cliente es autenticado basado en servidor RADIUS con las direcciones MAC de los clientes. Esquemas de autenticación concurrentes IEEE 802.1X y Web o MAC por puerto. Per port broadcast throttling: Selectivamente configura control de broadcast en puertos de uplink de alto tráfico.
	SOBRE LA ADMINISTRACION LOCAL La unidad deberá poder configurarse por medio de un puerto de consola con interface RS-232 (RJ45). Funcionalidades equivalentes a RMON, XRMON y sFlow v5: ofrecen funcionalidades avanzadas de monitorización y notificación de estadísticas, históricas, alarmas y eventos. Acceso seguro a la gestión: todos los métodos de acceso —interfaz de línea de comandos, GUI o MIB— están cifrados de forma segura a través de SSHv2, SSL y/o SNMPv3. Soporte SNMP v1, v2c y v3. Despliegue de estadísticas rápidas de ACL (listas de acceso) y QoS, interfaces IP Bitácoras del sistema Soporte eventos a Syslog server Soporte de debug La unidad deberá contar con indicadores luminosos tipo LED, para monitoreo local a fin de supervisar el estatus del switch encendido, en puertos de servicio indicar el estado de los enlaces, actividad del puerto y fallo del puerto. El equipo deberá de tener administración jerárquica y protección de passwords para la interface de

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	administración El equipo deberá ser capaz de guardar una bitácora de eventos. El equipo deberá de tener herramientas de ping y traceroute tanto para IPv4 como para IPv6. Capacidad de salvar y restaurar la configuración total del equipo. Soporte de múltiples archivos de configuración almacenados en flash para restaurarlos cuando sea necesario. Soporte de dos versiones de sistema operativo para que se pueda tener la contingencia en caso de actualización del sistema operativo y poder hacer el respectivo roll back. Capacidad de TFTP y SFTP El sistema deberá de contar con una herramienta de administración gráfica.
	SOBRE LAS FUNCIONALIDADES Y COMPATIBILIDADES La unidad deberá tener funciones de Conmutación de Paquetes de Capa 2, 3 y 4 según el modelo de referencia OSI. **Gestión de dispositivos** RFC 1591 DNS (cliente) HTML y gestión telnet **Protocolos generales** IEEE 802.1D MAC Bridges IEEE 802.1p Priority IEEE 802.1Q VLANs IEEE 802.1s Multiple Spanning Trees IEEE 802.1v VLAN classification by Protocol and Port IEEE 802.1w Rapid Reconfiguration of Spanning Tree IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.3af Power over Ethernet IEEE 802.3at PoE+ IEEE 802.3x Flow Control RFC 768 UDP RFC 783 TFTP Protocol (revision 2) RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 854 TELNET RFC 868 Time Protocol RFC 951 BOOTP RFC 1058 RIPv1 RFC 1350 TFTP Protocol (revision 2) RFC 2030 Simple Network Time Protocol (SNTP) v4 RFC 2131 DHCP RFC 2453 RIPv2 RFC 2548 (MS-RAS-Vendor only)

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

RFC 3046 DHCP Relay Agent Information Option

IP multicast
RFC 3376 IGMPv3 (host joins only)

IPv6
RFC 1981 IPv6 Path MTU Discovery
RFC 2460 IPv6 Specification
RFC 2710 Multicast Listener Discovery (MLD) for IPv6
RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (Ping only)
RFC 3019 MLDv1 MIB
RFC 3315 DHCPv6 (client and relay)
RFC 3513 IPv6 Addressing Architecture
RFC 3596 DNS Extension for IPv6
RFC 3810 MLDv2 (host joins only)
RFC 4022 MIB for TCP
RFC 4113 MIB for UDP
RFC 4251 SSHv6 Architecture
RFC 4252 SSHv6 Authentication
RFC 4253 SSHv6 Transport Layer
RFC 4254 SSHv6 Connection
RFC 4293 MIB for IP
RFC 4419 Key Exchange for SSH
RFC 4443 ICMPv6
RFC 4541 IGMP & MLD Snooping Switch
RFC 4861 IPv6 Neighbor Discovery
RFC 4862 IPv6 Stateless Address Auto-configuration

MIBs
RFC 1213 MIB II
MIB de bridge RFC 1493
RFC 1724 RIPv2 MIB
RFC 2021 RMONv2 MIB
RFC 2613 SMON MIB
MIB de cliente RFC 2618 RADIUS
MIB de administración RADIUS RFC 2620
RFC 2665 Ethernet-Like-MIB
RFC 2668 802.3 MAU MIB
MIB de bridge RFC 2674 802.1p e IEEE 802.1Q
MIB de entidad RFC 2737 (Versión 2)
RFC 2863 The Interfaces Group MIB
MIB de ping RFC 2925
Gestión de redes
IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
Cuatro grupos de RFC 2819 RMON: 1 (estadísticas), 2 (historial), 3 (alarmas) y 9 (incidencias)
sFlow RFC 3176
ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED)
SNMPv1/v2c/v3
XRMON

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	Calidad del servicio/Clase de servicio DiffServ Precedence RFC 2474, incluidos 8 puertos/colas RFC 2597 DiffServ Assured Forwarding (AF) RFC 2598 DiffServ Expedited Forwarding (EF) **Seguridad** Control de acceso de red basado en puerto IEEE 802.1X RFC 1492 TACACS+ RFC 2138 RADIUS Authentication RFC 2866 RADIUS Accounting Secure Sockets Layer (SSL)
	CONEXIONES Y DENSIDAD DE PUERTOS
	SOBRE LA DENSIDAD DE PUERTOS POR UNIDAD La unidad deberá soportar las densidades máximas y características en puertos que se describen a continuación: 4 Puertos Gigabit Ethernet para Fibra Óptica en combo con 4 puertos UTP 24 Puertos 10/100/1000 UTP 2 Puertos de 10 GbE incluido los 2(dos) Transceivers SFP+ LC SR 2 Cables de F.O. 2m Multi-mode OM4 LC/LC Capacidad para 4 Puertos 10 Gigabit Ethernet con módulos adicionales Módulo de Stack (La Solucion debe permitir hasta 4 Switches en modalidad de stack capacidad de Stack 40 Gbps half-duplex o Full-Duplex).
	GARANTIA 3(tres) años. Mano de Obra, Partes, Repuesto en las oficinas de la Convocante sin cargo. Nivel de Soporte Mínimo Requerido: Modalidad 8x5 – Atención Telefónica, Reemplazo al siguiente día laboral de Hardware.

PARTIDA	DESCRIPCIÓN
	CONMUTADORES DE DATOS
	UNIDAD DE CONMUTACION DE DATOS TIPO ACCESO (NODOS CENTRALES) con ALIMENTACION SOBRE ETHERNET (PoE)
CANT: 1(uno)	El equipo será el responsable de proporcionar el acceso a la LAN para estaciones terminales o servidores departamentales basadas en la tecnología de Ethernet, FastEthernet, GigabitEthernet y tener soporte de puertos de 10 Gigabit y deberá cumplir con las siguientes especificaciones técnicas.
	ESPECIFICACIONES TECNICAS
	SOBRE LA UNIDAD El *Switch* de *acceso* se refiere a un conmutador de datos de 48 puertos. Soporte de conmutación (switcheo) y enrutamiento (routing) de paquetes en capa 2 Ethernet, capa 3 con enrutamiento estático, RIPv1, RIPv2 (IPv4 e IPV6). Soporte POE+. Deberá estar listo para transportar aplicaciones de voz sobre IP. Para la unidad *Switch* de *Acceso*, el equipo deberá tener una capacidad de *tráfico de conmutación* no menor a 175 Gbps y no menos a 128 Mpps de throughput. Asimismo, el equipo deberá contar con la capacidad de soportar redundancia en fuentes de poder.

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	Se requiere de funcionalidades de redundancia que cumplan con lo siguiente: • Protocolo Spanning Tree IEEE 802.1s de múltiples instancias: proporciona alta disponibilidad de enlaces en varios entornos de VLAN al permitir múltiples Spanning Trees; engloba el protocolo Spanning Tree IEEE 802.1D y el protocolo Spanning Tree rápido IEEE 802.1w. • Agregación IEEE 802.3ad Link Aggregation Control Protocol (LACP): admite hasta 24 trunks, con hasta 8 enlaces (puertos) cada uno. Soporte IEEE 802.3af Power over Ethernet (PoE). Soporte IEEE 802.3at Power Over Ethernet Plus Soporte Prestandard PoE: Compatibilidad con dispositivos que soportan prestandard PoE. Soporte administración con una dirección IP para stack virtual hasta de 16 switches. Auto MDIX. La unidad deberá poder montarse en un rack de 19 pulgadas.
	CARACTERISTICAS SWITCHING L2 VLAN Tagging: Soporte de 256 IEEE 802.1Q standard simúltaneamente (soporte de 4094 Vlan IDs). Soporte standard IEEE 802.1v VLANs por protocolo. Soporte GARP protocol de registro de VLAN. o equivalentes, misma o mejor funcionalidad LLDP-MED (Media Endpoint Discovery): extensión del estandar LLDP que almacena valores de parámetros como QoS y VLAN para automaticamente configurar dispositivosde red como teléfonos IP. Soporte IEEE 802.1AB LLDP.
	CARACTERISTICAS SWITCHING L3 Enrutamiento IP estático para IPv4. Soporte del protocolo de enrutamiento dinámico Routing Information Protocol (RIP): RIPv1 y RIPv2. IP multicast snooping (data-driven IGMP): automaticamente previene flooding de tráfico IP multicast.
	SEGURIDAD

Access control lists (ACLs): Basadas en campo dirección IP origen/destino, dirección/subred IP, Puerto de origen/destino TCP/UDP por VLAN o peor puerto.

DHCP protection: bloqueo paquetes DHCP de servers DHCP no autorizados, previniendo ataques DoS .

Administración Segura: SSHv2, SSL, y/o SNMPv3.

Identity-driven ACL: enables implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user.

STP BPDU port protection.

Dynamic ARP protection.

STP Root Guard.

Detección de ataques maliciosos: debe monitorear 10 tipos de tráfico de red y envía un warning cuando una anomalía que potencialmente puede ser causada por un ataque malicioso es detectada.

Port security: allows access only to specified MAC addresses, which can be learned or specified by the administrator.

MAC address lockout: previene que direcciones MAC configuradas se conecten a la red.

Source-port filtering: allows only specified ports to communicate with each other

Seguridad en Switch login: puede usar RADIUS o TACACS+ para autenticación para logon seguro en la interfaz CLI del switch.

Banner customizable: despliega un mensaje de política de seguridad customizado cuando los usuarios se conectan al login del switch.

Múltiples métodos de autenticación:

IEEE 802.1X: provee autenticación de hasta 8 usuarios IEEE 802.1X por puerto; previene "piggybacking" de usuario sobre la autenticación IEEE 802.1X de otro usuario.

Autenticación basada en Web: autenticación desde browser Web para clientes que no soportan supplicant IEEE 802.1X.

Autenticación basada en MAC: el cliente es autenticado basado en servidor RADIUS con las

Avda. Molás López N°480
Asunción - Paraguay
Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	direcciones MAC de los clientes. Esquemas de autenticación concurrentes IEEE 802.1X y Web o MAC por puerto. Per port broadcast throttling: Selectivamente configura control de broadcast en puertos de uplink de alto tráfico.
	SOBRE LA ADMINISTRACION LOCAL La unidad deberá poder configurarse por medio de un puerto de consola con interface RS-232 (RJ45). Funcionalidades equivalentes a RMON, XRMON y sFlow v5: ofrecen funcionalidades avanzadas de monitorización y notificación de estadísticas, históricas, alarmas y eventos. Acceso seguro a la gestión: todos los métodos de acceso —interfaz de línea de comandos, GUI o MIB— están cifrados de forma segura a través de SSHv2, SSL y/o SNMPv3. Soporte SNMP v1, v2c y v3. Despliegue de estadísticas rápidas de ACL (listas de acceso) y QoS, interfaces IP Bitácoras del sistema Soporte eventos a Syslog server Soporte de debug La unidad deberá contar con indicadores luminosos tipo LED, para monitoreo local a fin de supervisar el estatus del switch encendido, en puertos de servicio indicar el estado de los enlaces, actividad del puerto y fallo del puerto. El equipo deberá de tener administración jerárquica y protección de passwords para la interface de administración El equipo deberá ser capaz de guardar una bitácora de eventos. El equipo deberá de tener herramientas de ping y traceroute tanto para IPv4 como para IPv6. Capacidad de salvar y restaurar la configuración total del equipo. Soporte de múltiples archivos de configuración almacenados en flash para restaurarlos cuando sea necesario. Soporte de dos versiones de sistema operativo para que se pueda tener la contingencia en caso de actualización del sistema operativo y poder hacer el respectivo roll back. Capacidad de TFTP y SFTP El sistema deberá de contar con una herramienta de administración gráfica.
	SOBRE LAS FUNCIONALIDADES Y COMPATIBILIDADES

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	La unidad deberá tener funciones de Conmutación de Paquetes de Capa 2, 3 y 4 según el modelo de referencia OSI. **Gestión de dispositivos** RFC 1591 DNS (cliente) HTML y gestión telnet **Protocolos generales** IEEE 802.1D MAC Bridges IEEE 802.1p Priority IEEE 802.1Q VLANs IEEE 802.1s Multiple Spanning Trees IEEE 802.1v VLAN classification by Protocol and Port IEEE 802.1w Rapid Reconfiguration of Spanning Tree IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.3af Power over Ethernet IEEE 802.3at PoE+ IEEE 802.3x Flow Control RFC 768 UDP RFC 783 TFTP Protocol (revision 2) RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 854 TELNET RFC 868 Time Protocol RFC 951 BOOTP RFC 1058 RIPv1 RFC 1350 TFTP Protocol (revision 2) RFC 2030 Simple Network Time Protocol (SNTP) v4 RFC 2131 DHCP RFC 2453 RIPv2 RFC 2548 (MS-RAS-Vendor only) RFC 3046 DHCP Relay Agent Information Option **IP multicast** RFC 3376 IGMPv3 (host joins only) **IPv6** RFC 1981 IPv6 Path MTU Discovery RFC 2460 IPv6 Specification RFC 2710 Multicast Listener Discovery (MLD) for IPv6 RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (Ping only) RFC 3019 MLDv1 MIB RFC 3315 DHCPv6 (client and relay) RFC 3513 IPv6 Addressing Architecture RFC 3596 DNS Extension for IPv6 RFC 3810 MLDv2 (host joins only) RFC 4022 MIB for TCP RFC 4113 MIB for UDP RFC 4251 SSHv6 Architecture RFC 4252 SSHv6 Authentication

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

RFC 4253 SSHv6 Transport Layer
RFC 4254 SSHv6 Connection
RFC 4293 MIB for IP
RFC 4419 Key Exchange for SSH
RFC 4443 ICMPv6
RFC 4541 IGMP & MLD Snooping Switch
RFC 4861 IPv6 Neighbor Discovery
RFC 4862 IPv6 Stateless Address Auto-configuration

MIBs
RFC 1213 MIB II
MIB de bridge RFC 1493
RFC 1724 RIPv2 MIB
RFC 2021 RMONv2 MIB
RFC 2613 SMON MIB
MIB de cliente RFC 2618 RADIUS
MIB de administración RADIUS RFC 2620
RFC 2665 Ethernet-Like-MIB
RFC 2668 802.3 MAU MIB
MIB de bridge RFC 2674 802.1p e IEEE 802.1Q
MIB de entidad RFC 2737 (Versión 2)
RFC 2863 The Interfaces Group MIB
MIB de ping RFC 2925

Gestión de redes
IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
Cuatro grupos de RFC 2819 RMON: 1 (estadísticas), 2 (historial), 3 (alarmas) y 9 (incidencias)
sFlow RFC 3176
ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED)
SNMPv1/v2c/v3
XRMON

Calidad del servicio/Clase de servicio
DiffServ Precedence RFC 2474, incluidos 8 puertos/colas
RFC 2597 DiffServ Assured Forwarding (AF)
RFC 2598 DiffServ Expedited Forwarding (EF)

Seguridad
Control de acceso de red basado en puerto IEEE 802.1X
RFC 1492 TACACS+
RFC 2138 RADIUS Authentication
RFC 2866 RADIUS Accounting
Secure Sockets Layer (SSL)

CONEXIONES Y DENSIDAD DE PUERTOS

SOBRE LA DENSIDAD DE PUERTOS POR UNIDAD
La unidad deberá soportar las densidades máximas y características en puertos que se describen a continuación:

4 Puertos Gigabit Ethernet para Fibra Óptica en combo con 4 puertos UTP

Avda. Molás López N°480
Asunción - Paraguay
Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	48 Puertos 10/100/1000 UTP 2 Puertos de 10 GbE incluido los 2(dos) Transceivers SFP+ LC SR 2 Cables de F.O. 2m Multi-mode OM4 LC/LC Capacidad para 4 Puertos 10 Gigabit Ethernet con módulos adicionales Módulo de Stack (La Solucion debe permitir hasta 4 Switches en modalidad de stack capacidad de Stack 40 Gbps half-duplex o Full-Duplex).
	GARANTIA 3(tres) años. Mano de Obra, Partes, Repuesto en las oficinas de la Convocante sin cargo. Nivel de Soporte Mínimo Requerido: Modalidad 8x5 – Atención Telefónica, Reemplazo al siguiente día laboral de Hardware.

PARTIDA	DESCRIPCIÓN
	CONMUTADORES DE DATOS
	UNIDAD DE CONMUTACION DE DATOS TIPO ACCESO (NODOS CENTRALES) con ALIMENTACION SOBRE ETHERNET (PoE)
CANT: 3(tres)	El equipo será el responsable de proporcionar el acceso a la LAN para estaciones terminales o servidores departamentales basadas en la tecnología de Ethernet, FastEthernet, GigabitEthernet y tener soporte de puertos de 10 Gigabit y deberá cumplir con las siguientes especificaciones técnicas.
	ESPECIFICACIONES TECNICAS
	SOBRE LA UNIDAD El *Switch* de *acceso* se refiere a un conmutador de datos de 24 puertos. Soporte de conmutación (switcheo) y enrutamiento (routing) de paquetes en capa 2 Ethernet, capa 3 con enrutamiento estático, RIPv1, RIPv2 (IPv4 e IPV6). Soporte POE+. Deberá estar listo para transportar aplicaciones de voz sobre IP. Para la unidad *Switch* de *Acceso*, el equipo deberá tener una capacidad de *tráfico de conmutación* no menor a 128 Gbps y no menos a 95 Mpps de throughput. Asimismo, el equipo deberá contar con la capacidad de soportar redundancia en fuentes de poder. Se requiere de funcionalidades de redundancia que cumplan con lo siguiente: • Protocolo Spanning Tree IEEE 802.1s de múltiples instancias: proporciona alta disponibilidad de enlaces en varios entornos de VLAN al permitir múltiples Spanning Trees; engloba el protocolo Spanning Tree IEEE 802.1D y el protocolo Spanning Tree rápido IEEE 802.1w. • Agregación IEEE 802.3ad Link Aggregation Control Protocol (LACP): admite hasta 24 trunks, con hasta 8 enlaces (puertos) cada uno. Soporte IEEE 802.3af Power over Ethernet (PoE). Soporte IEEE 802.3at Power Over Ethernet Plus Soporte Prestandard PoE: Compatibilidad con dispositivos que soportan prestandard PoE.

Avda. Molás López N°480
Asunción - Paraguay
Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	Soporte administración con una dirección IP para stack virtual hasta de 16 switches. Auto MDIX. La unidad deberá poder montarse en un rack de 19 pulgadas.
	CARACTERISTICAS SWITCHING L2 VLAN Tagging: Soporte de 256 IEEE 802.1Q standard simúltaneamente (soporte de 4094 Vlan IDs). Soporte standard IEEE 802.1v VLANs por protocolo. Soporte GARP protocol de registro de VLAN. o equivalentes, misma o mejor funcionalidad LLDP-MED (Media Endpoint Discovery): extensión del estandar LLDP que almacena valores de parámetros como QoS y VLAN para automaticamente configurar dispositivosde red como teléfonos IP. Soporte IEEE 802.1AB LLDP.
	CARACTERISTICAS SWITCHING L3 Enrutamiento IP estático para IPv4. Soporte del protocolo de enrutamiento dinámico Routing Information Protocol (RIP): RIPv1 y RIPv2. IP multicast snooping (data-driven IGMP): automaticamente previene flooding de tráfico IP multicast.
	SEGURIDAD Access control lists (ACLs): Basadas en campo dirección IP origen/destino, dirección/subred IP, Puerto de origen/destino TCP/UDP por VLAN o peor puerto. DHCP protection: bloqueo paquetes DHCP de servers DHCP no autorizados, previniendo ataques DoS . Administración Segura: SSHv2, SSL, y/o SNMPv3. Identity-driven ACL: enables implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user. STP BPDU port protection. Dynamic ARP protection. STP Root Guard. Detección de ataques maliciosos: monitorea 10 tipos de tráfico de red y envía un warning cuando una anomalía que potencialmente puede ser causada por un ataque malicioso es detectada. Port security: allows access only to specified MAC addresses, which can be learned or specified by the administrator. MAC address lockout: previene que direcciones MAC configuradas se conecten a la red. Source-port filtering: allows only specified ports to communicate with each other Seguridad en Switch login: puede usar RADIUS o TACACS+ para autenticación para logon

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	seguro en la interfaz CLI del switch. Banner customizable: despliega un mensaje de política de seguridad customizado cuando los usuarios se conectan al login del switch. Múltiples métodos de autenticación: IEEE 802.1X: provee autenticación de hasta 8 usuarios IEEE 802.1X por puerto; previene "piggybacking" de usuario sobre la autenticación IEEE 802.1X de otro usuario. Autenticación basada en Web: autenticación desde browser Web para clientes que no soportan supplicant IEEE 802.1X. Autenticación basada en MAC: el cliente es autenticado basado en servidor RADIUS con las direcciones MAC de los clientes. Esquemas de autenticación concurrentes IEEE 802.1X y Web o MAC por puerto. Per port broadcast throttling: Selectivamente configura control de broadcast en puertos de uplink de alto tráfico.
	SOBRE LA ADMINISTRACION LOCAL La unidad deberá poder configurarse por medio de un puerto de consola con interface RS-232 (RJ45). Funcionalidades equivalentes a RMON, XRMON y sFlow v5: ofrecen funcionalidades avanzadas de monitorización y notificación de estadísticas, históricas, alarmas y eventos. Acceso seguro a la gestión: todos los métodos de acceso —interfaz de línea de comandos, GUI o MIB— están cifrados de forma segura a través de SSHv2, SSL y/o SNMPv3. Soporte SNMP v1, v2c y v3. Despliegue de estadísticas rápidas de ACL (listas de acceso) y QoS, interfaces IP Bitácoras del sistema Soporte eventos a Syslog server Soporte de debug La unidad deberá contar con indicadores luminosos tipo LED, para monitoreo local a fin de supervisar el estatus del switch encendido, en puertos de servicio indicar el estado de los enlaces, actividad del puerto y fallo del puerto. El equipo deberá de tener administración jerárquica y protección de passwords para la interface de administración El equipo deberá ser capaz de guardar una bitácora de eventos. El equipo deberá de tener herramientas de ping y traceroute tanto para IPv4 como para IPv6. Capacidad de salvar y restaurar la configuración total del equipo. Soporte de múltiples archivos de configuración almacenados en flash para restaurarlos cuando sea necesario. Soporte de dos versiones de sistema operativo para que se pueda tener la contingencia en caso de actualización del sistema operativo y poder hacer el respectivo roll back. Capacidad de TFTP y SFTP El sistema deberá de contar con una herramienta de administración gráfica.
	SOBRE LAS FUNCIONALIDADES Y COMPATIBILIDADES La unidad deberá tener funciones de Conmutación de Paquetes de Capa 2, 3 y 4 según el modelo de referencia OSI. **Gestión de dispositivos** RFC 1591 DNS (cliente) HTML y gestión telnet

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

Protocolos generales
IEEE 802.1D MAC Bridges
IEEE 802.1p Priority
IEEE 802.1Q VLANs
IEEE 802.1s Multiple Spanning Trees
IEEE 802.1v VLAN classification by Protocol and Port
IEEE 802.1w Rapid Reconfiguration of Spanning Tree
IEEE 802.3ad Link Aggregation Control Protocol (LACP)
IEEE 802.3af Power over Ethernet
IEEE 802.3at PoE+
IEEE 802.3x Flow Control
RFC 768 UDP
RFC 783 TFTP Protocol (revision 2)
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 TELNET
RFC 868 Time Protocol
RFC 951 BOOTP
RFC 1058 RIPv1
RFC 1350 TFTP Protocol (revision 2)
RFC 2030 Simple Network Time Protocol (SNTP) v4
RFC 2131 DHCP
RFC 2453 RIPv2
RFC 2548 (MS-RAS-Vendor only)
RFC 3046 DHCP Relay Agent Information Option

IP multicast
RFC 3376 IGMPv3 (host joins only)

IPv6
RFC 1981 IPv6 Path MTU Discovery
RFC 2460 IPv6 Specification
RFC 2710 Multicast Listener Discovery (MLD) for IPv6
RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (Ping only)
RFC 3019 MLDv1 MIB
RFC 3315 DHCPv6 (client and relay)
RFC 3513 IPv6 Addressing Architecture
RFC 3596 DNS Extension for IPv6
RFC 3810 MLDv2 (host joins only)
RFC 4022 MIB for TCP
RFC 4113 MIB for UDP
RFC 4251 SSHv6 Architecture
RFC 4252 SSHv6 Authentication
RFC 4253 SSHv6 Transport Layer
RFC 4254 SSHv6 Connection
RFC 4293 MIB for IP
RFC 4419 Key Exchange for SSH
RFC 4443 ICMPv6
RFC 4541 IGMP & MLD Snooping Switch
RFC 4861 IPv6 Neighbor Discovery

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	RFC 4862 IPv6 Stateless Address Auto-configuration **MIBs** RFC 1213 MIB II MIB de bridge RFC 1493 RFC 1724 RIPv2 MIB RFC 2021 RMONv2 MIB RFC 2613 SMON MIB MIB de cliente RFC 2618 RADIUS MIB de administración RADIUS RFC 2620 RFC 2665 Ethernet-Like-MIB RFC 2668 802.3 MAU MIB MIB de bridge RFC 2674 802.1p e IEEE 802.1Q MIB de entidad RFC 2737 (Versión 2) RFC 2863 The Interfaces Group MIB MIB de ping RFC 2925 **Gestión de redes** IEEE 802.1AB Link Layer Discovery Protocol (LLDP) Cuatro grupos de RFC 2819 RMON: 1 (estadísticas), 2 (historial), 3 (alarmas) y 9 (incidencias) sFlow RFC 3176 ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED) SNMPv1/v2c/v3 XRMON **Calidad del servicio/Clase de servicio** DiffServ Precedence RFC 2474, incluidos 8 puertos/colas RFC 2597 DiffServ Assured Forwarding (AF) RFC 2598 DiffServ Expedited Forwarding (EF) **Seguridad** Control de acceso de red basado en puerto IEEE 802.1X RFC 1492 TACACS+ RFC 2138 RADIUS Authentication RFC 2866 RADIUS Accounting Secure Sockets Layer (SSL)
	CONEXIONES Y DENSIDAD DE PUERTOS
	SOBRE LA DENSIDAD DE PUERTOS POR UNIDAD La unidad deberá soportar las densidades máximas y características en puertos que se describen a continuación: 4 Puertos Gigabit Ethernet para Fibra Óptica en combo con 4 puertos UTP 24 Puertos 10/100/1000 UTP Capacidad para 4 Puertos 10 Gigabit Ethernet con módulos adicionales Módulo de Stack (La Solucion debe permitir hasta 4 Switches en modalidad de stack capacidad de Stack 40 Gbps half-duplex o Full-Duplex).

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	GARANTIA 3(tres) años. Mano de Obra, Partes, Repuesto en las oficinas de la Convocante sin cargo. Nivel de Soporte Mínimo Requerido: Modalidad 8x5 – Atención Telefónica, Reemplazo al siguiente día laboral de Hardware.

PARTIDA	DESCRIPCIÓN
	CONMUTADORES DE DATOS
	UNIDAD DE CONMUTACION DE DATOS TIPO ACCESO (NODOS CENTRALES) con ALIMENTACION SOBRE ETHERNET (PoE)
CANT: 1(uno)	El equipo será el responsable de proporcionar el acceso a la LAN para estaciones terminales o servidores departamentales basadas en la tecnología de Ethernet, FastEthernet, GigabitEthernet y tener soporte de puertos de 10 Gigabit y deberá cumplir con las siguientes especificaciones técnicas.
	ESPECIFICACIONES TECNICAS
	SOBRE LA UNIDAD El *Switch* de *acceso* se refiere a un conmutador de datos de 48 puertos. Soporte de conmutación (switcheo) y enrutamiento (routing) de paquetes en capa 2 Ethernet, capa 3 con enrutamiento estático, RIPv1, RIPv2 (IPv4 e IPV6). Soporte POE+. Deberá estar listo para transportar aplicaciones de voz sobre IP. Para la unidad *Switch* de *Acceso*, el equipo deberá tener una capacidad de *tráfico de conmutación* no menor a 175 Gbps y no menos a 128 Mpps de throughput. Asimismo, el equipo deberá contar con la capacidad de soportar redundancia en fuentes de poder. Se requiere de funcionalidades de redundancia que cumplan con lo siguiente: • Protocolo Spanning Tree IEEE 802.1s de múltiples instancias: proporciona alta disponibilidad de enlaces en varios entornos de VLAN al permitir múltiples Spanning Trees; engloba el protocolo Spanning Tree IEEE 802.1D y el protocolo Spanning Tree rápido IEEE 802.1w. • Agregación IEEE 802.3ad Link Aggregation Control Protocol (LACP): admite hasta 24 trunks, con hasta 8 enlaces (puertos) cada uno. Soporte IEEE 802.3af Power over Ethernet (PoE). Soporte IEEE 802.3at Power Over Ethernet Plus Soporte Prestandard PoE: Compatibilidad con dispositivos que soportan prestandard PoE. Soporte administración con una dirección IP para stack virtual hasta de 16 switches. Auto MDIX. La unidad deberá poder montarse en un rack de 19 pulgadas.
	CARACTERISTICAS SWITCHING L2 VLAN Tagging: Soporte de 256 IEEE 802.1Q standard simúltaneamente (soporte de 4094

Avda. Molás López N°480
Asunción - Paraguay
Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	Vlan IDs). Soporte standard IEEE 802.1v VLANs por protocolo. Soporte GARP protocol de registro de VLAN. o equivalentes, misma o mejor funcionalidad LLDP-MED (Media Endpoint Discovery): extensión del estandar LLDP que almacena valores de parámetros como QoS y VLAN para automaticamente configurar dispositivosde red como teléfonos IP. Soporte IEEE 802.1AB LLDP.
	CARACTERISTICAS SWITCHING L3 Enrutamiento IP estático para IPv4. Soporte del protocolo de enrutamiento dinámico Routing Information Protocol (RIP): RIPv1 y RIPv2. IP multicast snooping (data-driven IGMP): automaticamente previene flooding de tráfico IP multicast.
	SEGURIDAD Access control lists (ACLs): Basadas en campo dirección IP origen/destino, dirección/subred IP, Puerto de origen/destino TCP/UDP por VLAN o peor puerto. DHCP protection: bloqueo paquetes DHCP de servers DHCP no autorizados, previniendo ataques DoS . Administración Segura: SSHv2, SSL, y/o SNMPv3. Identity-driven ACL: enables implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user. STP BPDU port protection. Dynamic ARP protection. STP Root Guard. Detección de ataques maliciosos: monitorea 10 tipos de tráfico de red y envía un warning cuando una anomalía que potencialmente puede ser causada por un ataque malicioso es detectada. Port security: allows access only to specified MAC addresses, which can be learned or specified by the administrator. MAC address lockout: previene que direcciones MAC configuradas se conecten a la red. Source-port filtering: allows only specified ports to communicate with each other Seguridad en Switch login: puede usar RADIUS o TACACS+ para autenticación para logon seguro en la interfaz CLI del switch. Banner customizable: despliega un mensaje de política de seguridad customizado cuando los usuarios se conectan al login del switch. Múltiples métodos de autenticación: IEEE 802.1X: provee autenticación de hasta 8 usuarios IEEE 802.1X por puerto; previene "piggybacking" de usuario sobre la autenticación IEEE 802.1X de otro usuario. Autenticación basada en Web: autenticación desde browser Web para clientes que no soportan supplicant IEEE 802.1X.

Avda. Molás López N°480
Asunción - Paraguay
Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	Autenticación basada en MAC: el cliente es autenticado basado en servidor RADIUS con las direcciones MAC de los clientes. Esquemas de autenticación concurrentes IEEE 802.1X y Web o MAC por puerto. Per port broadcast throttling: Selectivamente configura control de broadcast en puertos de uplink de alto tráfico.
	SOBRE LA ADMINISTRACION LOCAL La unidad deberá poder configurarse por medio de un puerto de consola con interface RS-232 (RJ45). Funcionalidades equivalentes a RMON, XRMON y sFlow v5: ofrecen funcionalidades avanzadas de monitorización y notificación de estadísticas, históricas, alarmas y eventos. Acceso seguro a la gestión: todos los métodos de acceso —interfaz de línea de comandos, GUI o MIB— están cifrados de forma segura a través de SSHv2, SSL y/o SNMPv3. Soporte SNMP v1, v2c y v3. Despliegue de estadísticas rápidas de ACL (listas de acceso) y QoS, interfaces IP Bitácoras del sistema Soporte eventos a Syslog server Soporte de debug La unidad deberá contar con indicadores luminosos tipo LED, para monitoreo local a fin de supervisar el estatus del switch encendido, en puertos de servicio indicar el estado de los enlaces, actividad del puerto y fallo del puerto. El equipo deberá de tener administración jerárquica y protección de passwords para la interface de administración El equipo deberá ser capaz de guardar una bitácora de eventos. El equipo deberá de tener herramientas de ping y traceroute tanto para IPv4 como para IPv6. Capacidad de salvar y restaurar la configuración total del equipo. Soporte de múltiples archivos de configuración almacenados en flash para restaurarlos cuando sea necesario. Soporte de dos versiones de sistema operativo para que se pueda tener la contingencia en caso de actualización del sistema operativo y poder hacer el respectivo roll back. Capacidad de TFTP y SFTP El sistema deberá de contar con una herramienta de administración gráfica.
	SOBRE LAS FUNCIONALIDADES Y COMPATIBILIDADES La unidad deberá tener funciones de Conmutación de Paquetes de Capa 2, 3 y 4 según el modelo de referencia OSI. **Gestión de dispositivos** RFC 1591 DNS (cliente) HTML y gestión telnet **Protocolos generales** IEEE 802.1D MAC Bridges IEEE 802.1p Priority IEEE 802.1Q VLANs IEEE 802.1s Multiple Spanning Trees IEEE 802.1v VLAN classification by Protocol and Port IEEE 802.1w Rapid Reconfiguration of Spanning Tree

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.3af Power over Ethernet IEEE 802.3at PoE+ IEEE 802.3x Flow Control RFC 768 UDP RFC 783 TFTP Protocol (revision 2) RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 854 TELNET RFC 868 Time Protocol RFC 951 BOOTP RFC 1058 RIPv1 RFC 1350 TFTP Protocol (revision 2) RFC 2030 Simple Network Time Protocol (SNTP) v4 RFC 2131 DHCP RFC 2453 RIPv2 RFC 2548 (MS-RAS-Vendor only) RFC 3046 DHCP Relay Agent Information Option **IP multicast** RFC 3376 IGMPv3 (host joins only) **IPv6** RFC 1981 IPv6 Path MTU Discovery RFC 2460 IPv6 Specification RFC 2710 Multicast Listener Discovery (MLD) for IPv6 RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (Ping only) RFC 3019 MLDv1 MIB RFC 3315 DHCPv6 (client and relay) RFC 3513 IPv6 Addressing Architecture RFC 3596 DNS Extension for IPv6 RFC 3810 MLDv2 (host joins only) RFC 4022 MIB for TCP RFC 4113 MIB for UDP RFC 4251 SSHv6 Architecture RFC 4252 SSHv6 Authentication RFC 4253 SSHv6 Transport Layer RFC 4254 SSHv6 Connection RFC 4293 MIB for IP RFC 4419 Key Exchange for SSH RFC 4443 ICMPv6 RFC 4541 IGMP & MLD Snooping Switch RFC 4861 IPv6 Neighbor Discovery RFC 4862 IPv6 Stateless Address Auto-configuration **MIBs** RFC 1213 MIB II MIB de bridge RFC 1493 RFC 1724 RIPv2 MIB RFC 2021 RMONv2 MIB

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	RFC 2613 SMON MIB MIB de cliente RFC 2618 RADIUS MIB de administración RADIUS RFC 2620 RFC 2665 Ethernet-Like-MIB RFC 2668 802.3 MAU MIB MIB de bridge RFC 2674 802.1p e IEEE 802.1Q MIB de entidad RFC 2737 (Versión 2) RFC 2863 The Interfaces Group MIB MIB de ping RFC 2925 **Gestión de redes** IEEE 802.1AB Link Layer Discovery Protocol (LLDP) Cuatro grupos de RFC 2819 RMON: 1 (estadísticas), 2 (historial), 3 (alarmas) y 9 (incidencias) sFlow RFC 3176 ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED) SNMPv1/v2c/v3 XRMON **Calidad del servicio/Clase de servicio** DiffServ Precedence RFC 2474, incluidos 8 puertos/colas RFC 2597 DiffServ Assured Forwarding (AF) RFC 2598 DiffServ Expedited Forwarding (EF) **Seguridad** Control de acceso de red basado en puerto IEEE 802.1X RFC 1492 TACACS+ RFC 2138 RADIUS Authentication RFC 2866 RADIUS Accounting Secure Sockets Layer (SSL)
	CONEXIONES Y DENSIDAD DE PUERTOS

	SOBRE LA DENSIDAD DE PUERTOS POR UNIDAD La unidad deberá soportar las densidades máximas y características en puertos que se describen a continuación: 4 Puertos Gigabit Ethernet para Fibra Óptica en combo con 4 puertos UTP 48 Puertos 10/100/1000 UTP Capacidad para 4 Puertos 10 Gigabit Ethernet con módulos adicionales Módulo de Stack (La Solucion debe permitir hasta 4 Switches en modalidad de stack capacidad de Stack 40 Gbps half-duplex o Full-Duplex).
	GARANTIA 3(tres) años. Mano de Obra, Partes, Repuesto en las oficinas de la Convocante sin cargo. Nivel de Soporte Mínimo Requerido: Modalidad 8x5 – Atención Telefónica, Reemplazo al siguiente día laboral de Hardware.

PARTIDA	DESCRIPCIÓN
	CONMUTADORES DE DATOS

Avda. Molás López N°480
Asunción - Paraguay
Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	UNIDAD DE CONMUTACION DE DATOS TIPO ACCESO (NODOS CENTRALES)
CANT: 5(cinco)	El equipo será el responsable de proporcionar el acceso a la LAN para estaciones terminales o servidores departamentales basadas en la tecnología de Ethernet, FastEthernet, GigabitEthernet y tener soporte de puertos de 10 Gigabit y deberá cumplir con las siguientes especificaciones técnicas.
	ESPECIFICACIONES TECNICAS
	SOBRE LA UNIDAD El *Switch* de *acceso* se refiere a un conmutador de datos de 24 puertos. Soporte de conmutación (switcheo) y enrutamiento (routing) de paquetes en capa 2 Ethernet, capa 3 con enrutamiento estático, RIPv1, RIPv2 (IPv4 e IPV6). Deberá estar listo para transportar aplicaciones de voz sobre IP. Para la unidad *Switch* de *Acceso*, el equipo deberá tener una capacidad de *tráfico de conmutación* no menor a 128 Gbps y no menos a 95 Mpps de throughput. Asimismo, el equipo deberá contar con la capacidad de soportar redundancia en fuentes de poder. Se requiere de funcionalidades de redundancia que cumplan con lo siguiente: • Protocolo Spanning Tree IEEE 802.1s de múltiples instancias: proporciona alta disponibilidad de enlaces en varios entornos de VLAN al permitir múltiples Spanning Trees; engloba el protocolo Spanning Tree IEEE 802.1D y el protocolo Spanning Tree rápido IEEE 802.1w. • Agregación IEEE 802.3ad Link Aggregation Control Protocol (LACP): admite hasta 24 trunks, con hasta 8 enlaces (puertos) cada uno. Soporte administración con una dirección IP para stack virtual hasta de 16 switches. Auto MDIX. La unidad deberá poder montarse en un rack de 19 pulgadas.
	CARACTERISTICAS SWITCHING L2 VLAN Tagging: Soporte de 256 IEEE 802.1Q standard simúltaneamente (soporte de 4094 Vlan IDs). Soporte standard IEEE 802.1v VLANs por protocolo. Soporte GARP protocol de registro de VLAN. o equivalentes, misma o mejor funcionalidad LLDP-MED (Media Endpoint Discovery): extensión del estandar LLDP que almacena valores de parámetros como QoS y VLAN para automaticamente configurar dispositivosde red como teléfonos IP. Soporte IEEE 802.1AB LLDP.

	CARACTERISTICAS SWITCHING L3 Enrutamiento IP estático para IPv4. Soporte del protocolo de enrutamiento dinámico Routing Information Protocol (RIP): RIPv1 y RIPv2. IP multicast snooping (data-driven IGMP): automaticamente previene flooding de tráfico IP multicast.
	SEGURIDAD Access control lists (ACLs): Basadas en campo dirección IP origen/destino, dirección/subred IP, Puerto de origen/destino TCP/UDP por VLAN o por puerto. DHCP protection: bloqueo paquetes DHCP de servers DHCP no autorizados, previniendo ataques DoS . Administración Segura: SSHv2, SSL, y/o SNMPv3. Identity-driven ACL: enables implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user. STP BPDU port protection. Dynamic ARP protection. STP Root Guard. Detección de ataques maliciosos: monitorea 10 tipos de tráfico de red y envía un warning cuando una anomalía que potencialmente puede ser causada por un ataque malicioso es detectada. Port security: allows access only to specified MAC addresses, which can be learned or specified by the administrator. MAC address lockout: previene que direcciones MAC configuradas se conecten a la red. Source-port filtering: allows only specified ports to communicate with each other Seguridad en Switch login: puede usar RADIUS o TACACS+ para autenticación para logon seguro en la interfaz CLI del switch. Banner customizable: despliega un mensaje de política de seguridad customizado cuando los usuarios se conectan al login del switch.

	Múltiples métodos de autenticación: IEEE 802.1X: provee autenticación de hasta 8 usuarios IEEE 802.1X por puerto; previene "piggybacking" de usuario sobre la autenticación IEEE 802.1X de otro usuario. Autenticación basada en Web: autenticación desde browser Web para clientes que no soportan supplicant IEEE 802.1X. Autenticación basada en MAC: el cliente es autenticado basado en servidor RADIUS con las direcciones MAC de los clientes. Esquemas de autenticación concurrentes IEEE 802.1X y Web o MAC por puerto. Per port broadcast throttling: Selectivamente configura control de broadcast en puertos de uplink de alto tráfico.
	SOBRE LA ADMINISTRACION LOCAL La unidad deberá poder configurarse por medio de un puerto de consola con interface RS-232 (RJ45). Funcionalidades equivalentes a RMON, XRMON y sFlow v5: ofrecen funcionalidades avanzadas de monitorización y notificación de estadísticas, históricas, alarmas y eventos. Acceso seguro a la gestión: todos los métodos de acceso —interfaz de línea de comandos, GUI o MIB— están cifrados de forma segura a través de SSHv2, SSL y/o SNMPv3. Soporte SNMP v1, v2c y v3. Despliegue de estadísticas rápidas de ACL (listas de acceso) y QoS, interfaces IP Bitácoras del sistema Soporte eventos a Syslog server Soporte de debug La unidad deberá contar con indicadores luminosos tipo LED, para monitoreo local a fin de supervisar el estatus del switch encendido, en puertos de servicio indicar el estado de los enlaces, actividad del puerto y fallo del puerto. El equipo deberá de tener administración jerárquica y protección de passwords para la interface de administración El equipo deberá ser capaz de guardar una bitácora de eventos. El equipo deberá de tener herramientas de ping y traceroute tanto para IPv4 como para IPv6.

	Capacidad de salvar y restaurar la configuración total del equipo. Soporte de múltiples archivos de configuración almacenados en flash para restaurarlos cuando sea necesario. Soporte de dos versiones de sistema operativo para que se pueda tener la contingencia en caso de actualización del sistema operativo y poder hacer el respectivo roll back. Capacidad de TFTP y SFTP El sistema deberá de contar con una herramienta de administración gráfica.

	SOBRE LAS FUNCIONALIDADES Y COMPATIBILIDADES La unidad deberá tener funciones de Conmutación de Paquetes de Capa 2, 3 y 4 según el modelo de referencia OSI. **Gestión de dispositivos** RFC 1591 DNS (cliente) HTML y gestión telnet **Protocolos generales** IEEE 802.1D MAC Bridges IEEE 802.1p Priority IEEE 802.1Q VLANs IEEE 802.1s Multiple Spanning Trees IEEE 802.1v VLAN classification by Protocol and Port IEEE 802.1w Rapid Reconfiguration of Spanning Tree IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.3x Flow Control RFC 768 UDP RFC 783 TFTP Protocol (revision 2) RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 854 TELNET RFC 868 Time Protocol RFC 951 BOOTP RFC 1058 RIPv1 RFC 1350 TFTP Protocol (revision 2) RFC 2030 Simple Network Time Protocol (SNTP) v4 RFC 2131 DHCP RFC 2453 RIPv2 RFC 2548 (MS-RAS-Vendor only) RFC 3046 DHCP Relay Agent Information Option **IP multicast** RFC 3376 IGMPv3 (host joins only) **IPv6**

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

RFC 1981 IPv6 Path MTU Discovery
RFC 2460 IPv6 Specification
RFC 2710 Multicast Listener Discovery (MLD) for IPv6
RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (Ping only)
RFC 3019 MLDv1 MIB
RFC 3315 DHCPv6 (client and relay)
RFC 3513 IPv6 Addressing Architecture
RFC 3596 DNS Extension for IPv6
RFC 3810 MLDv2 (host joins only)
RFC 4022 MIB for TCP
RFC 4113 MIB for UDP
RFC 4251 SSHv6 Architecture
RFC 4252 SSHv6 Authentication
RFC 4253 SSHv6 Transport Layer
RFC 4254 SSHv6 Connection
RFC 4293 MIB for IP
RFC 4419 Key Exchange for SSH
RFC 4443 ICMPv6
RFC 4541 IGMP & MLD Snooping Switch
RFC 4861 IPv6 Neighbor Discovery
RFC 4862 IPv6 Stateless Address Auto-configuration

MIBs
RFC 1213 MIB II
MIB de bridge RFC 1493
RFC 1724 RIPv2 MIB
RFC 2021 RMONv2 MIB
RFC 2613 SMON MIB
MIB de cliente RFC 2618 RADIUS
MIB de administración RADIUS RFC 2620
RFC 2665 Ethernet-Like-MIB
RFC 2668 802.3 MAU MIB
MIB de bridge RFC 2674 802.1p e IEEE 802.1Q
MIB de entidad RFC 2737 (Versión 2)
RFC 2863 The Interfaces Group MIB
MIB de ping RFC 2925

Gestión de redes
IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
Cuatro grupos de RFC 2819 RMON: 1 (estadísticas), 2 (historial), 3 (alarmas) y 9 (incidencias)
sFlow RFC 3176
ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED)
SNMPv1/v2c/v3
XRMON

Calidad del servicio/Clase de servicio
DiffServ Precedence RFC 2474, incluidos 8 puertos/colas
RFC 2597 DiffServ Assured Forwarding (AF)
RFC 2598 DiffServ Expedited Forwarding (EF)

Avda. Molás López N°480
Asunción - Paraguay
Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	Seguridad Control de acceso de red basado en puerto IEEE 802.1X RFC 1492 TACACS+ RFC 2138 RADIUS Authentication RFC 2866 RADIUS Accounting Secure Sockets Layer (SSL)

	CONEXIONES Y DENSIDAD DE PUERTOS
	SOBRE LA DENSIDAD DE PUERTOS POR UNIDAD La unidad deberá soportar las densidades máximas y características en puertos que se describen a continuación: 4 Puertos Gigabit Ethernet para Fibra Óptica en combo con 4 puertos UTP 24 Puertos 10/100/1000 UTP Capacidad para 4 Puertos 10 Gigabit Ethernet con módulos adicionales Módulo de Stack (La Solucion debe permitir hasta 4 Switches en modalidad de stack capacidad de Stack 40 Gbps half-duplex o Full-Duplex)
	GARANTIA 3(tres) años. Mano de Obra, Partes, Repuesto en las oficinas de la Convocante sin cargo. Nivel de Soporte Mínimo Requerido: Modalidad 8x5 – Atención Telefónica, Reemplazo al siguiente día laboral de Hardware.

PARTIDA	DESCRIPCIÓN
	CONMUTADORES DE DATOS
	UNIDAD DE CONMUTACION DE DATOS TIPO ACCESO (NODOS CENTRALES)
CANT: 1(uno)	El equipo será el responsable de proporcionar el acceso a la LAN para estaciones terminales o servidores departamentales basadas en la tecnología de Ethernet, FastEthernet, GigabitEthernet y tener soporte de puertos de 10 Gigabit y deberá cumplir con las siguientes especificaciones técnicas.
	ESPECIFICACIONES TECNICAS
	SOBRE LA UNIDAD El *Switch* de *acceso* se refiere a un conmutador de datos de 48 puertos. Soporte de conmutación (switcheo) y enrutamiento (routing) de paquetes en capa 2 Ethernet, capa 3 con enrutamiento estático, RIPv1, RIPv2 (IPv4 e IPV6). Deberá estar listo para transportar aplicaciones de voz sobre IP. Para la unidad *Switch* de *Acceso*, el equipo deberá tener una capacidad de *tráfico de conmutación* no menor a 175 Gbps y no menos a 128 Mpps de throughput. Asimismo, el equipo deberá contar con la capacidad de soportar redundancia en fuentes de poder. Se requiere de funcionalidades de redundancia que cumplan con lo siguiente:

Avda. Molás López N°480
Asunción - Paraguay
Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	• Protocolo Spanning Tree IEEE 802.1s de múltiples instancias: proporciona alta disponibilidad de enlaces en varios entornos de VLAN al permitir múltiples Spanning Trees; engloba el protocolo Spanning Tree IEEE 802.1D y el protocolo Spanning Tree rápido IEEE 802.1w. • Agregación IEEE 802.3ad Link Aggregation Control Protocol (LACP): admite hasta 24 trunks, con hasta 8 enlaces (puertos) cada uno. Soporte administración con una dirección IP para stack virtual hasta de 16 switches. Auto MDIX. La unidad deberá poder montarse en un rack de 19 pulgadas.
	CARACTERISTICAS SWITCHING L2 VLAN Tagging: Soporte de 256 IEEE 802.1Q standard simúltaneamente (soporte de 4094 Vlan IDs). Soporte standard IEEE 802.1v VLANs por protocolo. Soporte GARP protocol de registro de VLAN. o equivalentes, misma o mejor funcionalidad LLDP-MED (Media Endpoint Discovery): extensión del estandar LLDP que almacena valores de parámetros como QoS y VLAN para automaticamente configurar dispositivosde red como teléfonos IP. Soporte IEEE 802.1AB LLDP.
	CARACTERISTICAS SWITCHING L3 Enrutamiento IP estático para IPv4. Soporte del protocolo de enrutamiento dinámico Routing Information Protocol (RIP): RIPv1 y RIPv2. IP multicast snooping (data-driven IGMP): automaticamente previene flooding de tráfico IP multicast.
	SEGURIDAD Access control lists (ACLs): Basadas en campo dirección IP origen/destino, dirección/subred IP, Puerto de origen/destino TCP/UDP por VLAN o por puerto. DHCP protection: bloqueo paquetes DHCP de servers DHCP no autorizados, previniendo ataques DoS .

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

Administración Segura: SSHv2, SSL, y/o SNMPv3.

Identity-driven ACL: enables implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user.

STP BPDU port protection.

Dynamic ARP protection.

STP Root Guard.

Detección de ataques maliciosos: monitorea 10 tipos de tráfico de red y envía un warning cuando una anomalía que potencialmente puede ser causada por un ataque malicioso es detectada.

Port security: allows access only to specified MAC addresses, which can be learned or specified by the administrator.

MAC address lockout: previene que direcciones MAC configuradas se conecten a la red.

Source-port filtering: allows only specified ports to communicate with each other

Seguridad en Switch login: puede usar RADIUS o TACACS+ para autenticación para logon seguro en la interfaz CLI del switch.

Banner customizable: despliega un mensaje de política de seguridad customizado cuando los usuarios se conectan al login del switch.

Múltiples métodos de autenticación:

IEEE 802.1X: provee autenticación de hasta 8 usuarios IEEE 802.1X por puerto; previene "piggybacking" de usuario sobre la autenticación IEEE 802.1X de otro usuario.

Autenticación basada en Web: autenticación desde browser Web para clientes que no soportan supplicant IEEE 802.1X.

Autenticación basada en MAC: el cliente es autenticado basado en servidor RADIUS con las direcciones MAC de los clientes.

Esquemas de autenticación concurrentes IEEE 802.1X y Web o MAC por puerto.

Per port broadcast throttling: Selectivamente configura control de broadcast en puertos de uplink de alto tráfico.

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	SOBRE LA ADMINISTRACION LOCAL La unidad deberá poder configurarse por medio de un puerto de consola con interface RS-232 (RJ45). Funcionalidades equivalentes a RMON, XRMON y sFlow v5: ofrecen funcionalidades avanzadas de monitorización y notificación de estadísticas, históricas, alarmas y eventos. Acceso seguro a la gestión: todos los métodos de acceso —interfaz de línea de comandos, GUI o MIB— están cifrados de forma segura a través de SSHv2, SSL y/o SNMPv3. Soporte SNMP v1, v2c y v3. Despliegue de estadísticas rápidas de ACL (listas de acceso) y QoS, interfaces IP Bitácoras del sistema Soporte eventos a Syslog server Soporte de debug La unidad deberá contar con indicadores luminosos tipo LED, para monitoreo local a fin de supervisar el estatus del switch encendido, en puertos de servicio indicar el estado de los enlaces, actividad del puerto y fallo del puerto. El equipo deberá de tener administración jerárquica y protección de passwords para la interface de administración El equipo deberá ser capaz de guardar una bitácora de eventos. El equipo deberá de tener herramientas de ping y traceroute tanto para IPv4 como para IPv6. Capacidad de salvar y restaurar la configuración total del equipo. Soporte de múltiples archivos de configuración almacenados en flash para restaurarlos cuando sea necesario. Soporte de dos versiones de sistema operativo para que se pueda tener la contingencia en caso de actualización del sistema operativo y poder hacer el respectivo roll back. Capacidad de TFTP y SFTP El sistema deberá de contar con una herramienta de administración gráfica.
	SOBRE LAS FUNCIONALIDADES Y COMPATIBILIDADES La unidad deberá tener funciones de Conmutación de Paquetes de Capa 2, 3 y 4 según el modelo de referencia OSI. **Gestión de dispositivos**

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	RFC 1591 DNS (cliente) HTML y gestión telnet **Protocolos generales** IEEE 802.1D MAC Bridges IEEE 802.1p Priority IEEE 802.1Q VLANs IEEE 802.1s Multiple Spanning Trees IEEE 802.1v VLAN classification by Protocol and Port IEEE 802.1w Rapid Reconfiguration of Spanning Tree IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.3x Flow Control RFC 768 UDP RFC 783 TFTP Protocol (revision 2) RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 854 TELNET RFC 868 Time Protocol RFC 951 BOOTP RFC 1058 RIPv1 RFC 1350 TFTP Protocol (revision 2) RFC 2030 Simple Network Time Protocol (SNTP) v4 RFC 2131 DHCP RFC 2453 RIPv2 RFC 2548 (MS-RAS-Vendor only) RFC 3046 DHCP Relay Agent Information Option **IP multicast** RFC 3376 IGMPv3 (host joins only) **IPv6** RFC 1981 IPv6 Path MTU Discovery RFC 2460 IPv6 Specification RFC 2710 Multicast Listener Discovery (MLD) for IPv6 RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (Ping only) RFC 3019 MLDv1 MIB RFC 3315 DHCPv6 (client and relay) RFC 3513 IPv6 Addressing Architecture RFC 3596 DNS Extension for IPv6 RFC 3810 MLDv2 (host joins only) RFC 4022 MIB for TCP RFC 4113 MIB for UDP RFC 4251 SSHv6 Architecture RFC 4252 SSHv6 Authentication RFC 4253 SSHv6 Transport Layer RFC 4254 SSHv6 Connection RFC 4293 MIB for IP RFC 4419 Key Exchange for SSH RFC 4443 ICMPv6 RFC 4541 IGMP & MLD Snooping Switch

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

RFC 4861 IPv6 Neighbor Discovery
RFC 4862 IPv6 Stateless Address Auto-configuration

MIBs
RFC 1213 MIB II
MIB de bridge RFC 1493
RFC 1724 RIPv2 MIB
RFC 2021 RMONv2 MIB
RFC 2613 SMON MIB
MIB de cliente RFC 2618 RADIUS
MIB de administración RADIUS RFC 2620
RFC 2665 Ethernet-Like-MIB
RFC 2668 802.3 MAU MIB
MIB de bridge RFC 2674 802.1p e IEEE 802.1Q
MIB de entidad RFC 2737 (Versión 2)
RFC 2863 The Interfaces Group MIB
MIB de ping RFC 2925

Gestión de redes
IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
Cuatro grupos de RFC 2819 RMON: 1 (estadísticas), 2 (historial), 3 (alarmas) y 9 (incidencias)
sFlow RFC 3176
ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED)
SNMPv1/v2c/v3
XRMON

Calidad del servicio/Clase de servicio
DiffServ Precedence RFC 2474, incluidos 8 puertos/colas
RFC 2597 DiffServ Assured Forwarding (AF)
RFC 2598 DiffServ Expedited Forwarding (EF)

Seguridad
Control de acceso de red basado en puerto IEEE 802.1X
RFC 1492 TACACS+
RFC 2138 RADIUS Authentication
RFC 2866 RADIUS Accounting
Secure Sockets Layer (SSL)

CONEXIONES Y DENSIDAD DE PUERTOS

SOBRE LA DENSIDAD DE PUERTOS POR UNIDAD

La unidad deberá soportar las densidades máximas y características en puertos que se describen a continuación:

4 Puertos Gigabit Ethernet para Fibra Óptica en combo con 4 puertos UTP
48 Puertos 10/100/1000 UTP
Capacidad para 4 Puertos 10 Gigabit Ethernet con módulos adicionales
Módulo de Stack (La Solucion debe permitir hasta 4 Switches en modalidad de stack capacidad de Stack 40 Gbps half-duplex o Full-Duplex).

Avda. Molás López N°480
Asunción - Paraguay
Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	GARANTIA 3(tres) años. Mano de Obra, Partes, Repuesto en las oficinas de la Convocante sin cargo. Nivel de Soporte Mínimo Requerido: Modalidad 8x5 – Atención Telefónica, Reemplazo al siguiente día laboral de Hardware.

PARTIDA	DESCRIPCIÓN
	Controlador de Acceso Inalámbrico a la Red
CANT: 1(Uno)	**UNIDAD DE CONTROL CENTRALIZADO DE ANTENAS PARA ACCESO INALAMBRICO (ACCESS POINTS)**
Característica	**Descripción**
Descripción General	Controlador para manejo centralizado de antenas (Access Point) Wi-Fi. El controlador debe apoyar despliegue de red inalámbrica Wi-Fi tanto de tráfico distribuido a través de la red como de tráfico centralizado donde todo el tráfico pasa a través del controlador. Capacidad del controlador para manejar la interferencia de-canal y proporcionar ajuste de potencia automáticamente. Controlador debe poder manejar hasta 40 AP.
Puertos	• Al menos (4) puertos 10/100/1000 UTP RJ45 Auto MDI/MDIX • (2) puertos SFP Doble Personalidad-10/100/1000 cobre • Como mínimo 1 puertos consola serial RJ45
Funcionalidades Servicio Inalámbrico	• Capacidad de Proveer Portal Cautivo • Capacidad de Proveer Manejo de Usuarios Guest • Capacidad para proveer y apoyar "Real-Time Location Services" (RTLS) • Soporte Funcionalidad Band Steering 5G • Capacidad avanzada transparente "roaming" entre redes capa-3 Soporte para Access Points 802.11a/b/g/n
Memoria	• 256 KB Flash • 1G DDR2
Tamaño y Rackeo	No debe exceder de 2 RU Debe tener una estructura tal que permita ser colocado en un bastidor (rack) estándar de 19 pulgadas
Temperatura	• Deberá poder operar a una temperatura de 5° hasta 45°C
Fuente de Poder	Deberá operar de manera continua con fuente de poder de 100-240 VAC, 50/60Hz
Cantidad Access Points	Capacidad para manejar hasta 40 AP
Niveles de Ejecución	Hasta 8.9 millones pps (paquetes por segundo)
Cantidad Sesiones Concurrentes	250 usuarios concurrentes
SSID	Hasta 64 SSID/Virtual Profiles Debe soportar asignación Vlan Dinámicas.
Funcionalidades Generales/Calidad de Servicio	Capacidad de proveer Calidad de Servicio • Calidad de Servicio basado en Wi-Fi Multimedia (WMM) estándar con 4 queues • 802.1p estándar para clasificación de trafico • Capacidad para aplicar calidad de servicio independiente por SSID/Virtual Profile • Proveer capacidad para hasta 64 Virtual Profiles/SSID • Capacidad para clasificación de trafico estándar Diffserv

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	• Capacidad para clasificación de trafico estándar ToS • Capacidad para manejar trafico VoIP y trafico multicast • Capacidad avanzada automática para Optimización y Manejo de Frecuencias • Capacidad automática Spectrum Analysis • Capacidad de Firewall • DHCP Relay Opcion 82
Seguridad y Autenticación	• Soportar la capacidad para encriptar tráfico de administración (CLI, GUI, MIB) utilizando SSH v2c, SSL and SNMv3 • Control para autenticar usuarios inalámbricos utilizando 802.1x, MS Active Directory y RADIUS • Capacidad integrada para "Intrusion Detection System (IDS)" en el tráfico de usuarios en la red inalámbrica. Capacidad de detección, clasificación y detección de ataques automático. • Capacidad y cumplimiento disposiciones PCI DSS
Apilamiento	Capacidad de proveer arquitectura con alta disponibilidad. Soporte para arquitectura Activo/Pasivo y Activo/Activo en alta disponibilidad para la totalidad de los Access Point Wi-Fi
Gestión	• Debe controlar y permitir el acceso de administración vía Web Browser, Telnet, CLI, SOAP y SNMP • Debe soportar administración mediante IPv6, con soporte de Telnet, DNS, SNMP, DHCP y syslog. • Soporte SSL y/o SSH • Soporte de gestión a través de login por Radius o Tacacs+ • SNMP: Soporte de SNMPv1, SNMPv2 y SNMPv3. • RMON 4 Grupos – (Statistics, History, Alarms, Events). • Soporte de sFlow •
Protocolos y Funcionalidades Requeridas	• RFC 768 UDP • ▯ RFC 791 IP • ▯ RFC 792 ICMP • ▯ RFC 793 TCP • ▯ RFC 826 ARP • RFC 1122 Requirements for Internet Hosts • ▯ RFC 1519 CIDR • ▯ RFC 2131 DHCP (server, client & relay) • ▯ RFC 3176 (sFlow) • ▯ IEEE 802.3 (type 10BASE-T) (except MSM765 zl)) • ▯ IEEE 802.3ab (1000BASE-T) (except MSM765 zl) • ▯ IEEE 802.3af (PoE-PD, powered device) (MSM710 only) • ▯ IEEE 802.3x (Flow control) • ▯ IEEE 802.1AB (LLDP) • ▯ IEEE 802.1D (MAC bridges) • ▯ IEEE 802.1p (priority) • ▯ IEEE 802.1Q (VLANs) • ▯ WPA • ▯ IEEE 802.11i (WPA2, RSN) • ▯ RFC 1321 MD5 Message-Digest Algorithm • ▯ RFC 1851 The ESP Triple DES Transform • ▯ RFC 2104 HMAC: Keyed Hashing for message Authentication

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	• RFC 2246 TLS Protocol Version 1.0 • RFC 2401 Security Architecture for the Internet Protocol • RFC 2403 HMAC-MD5-96 within ESP and AH • RFC 2404 HMAC-SHA-1-96 within ESP and AH • RFC 2406 IPsec • RFC 2407 Interpretation for ISAKMP • RFC 2408 ISAKMP • RFC 2409 IKE • RFC 2451 ESP CBC-Mode Cipher Algorithm • RFC 3280 Internet X.509 PKI Certificate and CRL Profile • RFC 3602 The AES-CBC Cipher Algorithm and its use with IPsec • RFC 3686 Using AES Counter Mode with IPsec ESP • SSL and TLS; RC4 128-bit and RSA 1024- and 2048-bit • AES: CCM, CCMP • IPsec: 3DES, AES-CBC • IEEE 802.1X • RFC 2548 Microsoft Vendor-Specific RADIUS attributes • RFC 2716 PPP EAP-TLS • RFC 2865 RADIUS Authentication • RFC 2866 RADIUS Accounting • RFC 3579 RADIUS Support for EAP • RFC 3580 IEEE 802.1X RADIUS Guidelines • RFC 3748 Extensible Authentication Protocol • Web-based Authentication • SNMP v1, v2c, v3
	GARANTIA 3(tres) años. Mano de Obra, Partes, Repuesto en las oficinas de la Convocante sin cargo. Nivel de Soporte Mínimo Requerido: Modalidad 8x5 – Atención Telefónica, Reemplazo al siguiente día laboral de Hardware.

Wireless Access Point:

PARTIDA	DESCRIPCIÓN
	Transmisor de Red Inalámbrica 802.11x
CANT: 15(QUINCE)	**UNIDAD DE ACCESO INALAMBRICO (ACCESS POINTS) CONTROLADO CENTRALMENTE**
Característica	**Descripción**
Descripción General	Access Point con soporte para estándares IEEE 802.11a/b/g/n. Certificado para uso interior (certificado plenum) y capacidad para manejar aplicaciones "high-throughput"
Puertos	• Al menos (1) puerto 10/100/1000 UTP RJ45 Auto MDI/MDIX • 1 puertos consola serial RJ45
Funcionalidades Servicio Inalámbrico	• Capacidad de proveer funcionalidad "Intrusion Prevention System IDS" integrado Capacidad de proveer Optimización Automática Recursos Radio Frecuencia

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	• Ajuste automático en la potencia transmisión del radio • Balanceo automático usuarios inalámbricos • Selección automática canales WiFi • Capacidad para proveer y apoyar "Real-Time Location Services" (RTLS)
Modo Operación	• Capacidad para manejo centralizado a través de Controladora WLAN • Capacidad para operar en modo autónomo en el caso pierda contacto con la Controladora WLAN.
Modo Operación Radios	• Capacidad para manejar usuarios/clientes inalámbricos • Capacidad para manejar enlaces "wireless mesh" • Capacidad para captura de paquetes en modo "Intrusion Detection"
Temperatura	• Deberá poder operar a una temperatura de 0° hasta 50°C
Cantidad de Radios	• Dual Radio (a/b/g/n) / Arreglo MIMO 3x3 / 2 Spatial Streams
Cantidad Antenas	• (3) 5dBi 2.4 GHz y (3) 7dBi 5 GHz antenas internas omnidireccionales
Fuente de Poder	Operación "Full Power" utilizando IEEE 802.3af PoE para puerto Gigabit Ethernet.
Niveles de Ejecución	300Mbps throughput
SSID	Hasta 16 SSID/Virtual Profiles, Cada uno con una unica MAC address Debe soportar asignación Vlan Dinámicas.
Funcionalidades Generales/Calidad de Servicio	Capacidad de proveer Calidad de Servicio • Capacidad 802.1p estándar para clasificación de trafico • Capacidad para manejar trafico multimedia 802.11e EDCF • Capacidad para aplicar calidad de servicio independiente por SSID/Virtual Profile • Capacidad para clasificación de trafico estándar Diffserv • Capacidad para manejar trafico VoIP y trafico multicast
Seguridad y Autenticación	• Capacidad proveer encripción TKIP/WEP • Capacidad autenticación 802.1x utilizando EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP • Capacidad autenticación por MAC address • Capacidad de proveer Aislación Layer 2 clientes inalámbricos • Capacidad integrada para "Intrusion Detection System (IDS)" en el tráfico de usuarios en la red inalámbrica. Capacidad de detección, clasificación y detección de ataques • Capacidad de proveer funcionalidades 802.11i, WPA, WPA2
Gestión	• Debe controlar y permitir el acceso de administración vía Web Browser, Telnet, CLI, SOAP y SNMP • SNMP: Soporte de SNMPv1, SNMPv2 y SNMPv3.
Protocolos y Funcionalidades Requeridas	• EEE 802.11a High Speed Physical Layer in the 5 GHz Band • IEEE 802.11b Higher-Speed Physical Layer Extension in the 2.4 GHz Band • IEEE 802.11d Global Harmonization • EEE 802.11g Further Higher Data Rate Extension in the 2.4 GHz Band • IEEE 802.11i Medium Access Control (MAC) Security Enhancements • IEEE 802.11n WLAN Enhancements for Higher Throughput • SNMP v1, v2c, v3 • FCC Part 15.247 • UL 2043UL 60950-1IEC • 60950-1EN • 60950-1CAN/CSA-C22.2 No. 60950-1

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

	• EN60601-1-2
	GARANTIA 3(tres) años. Mano de Obra, Partes, Repuesto en las oficinas de la Convocante sin cargo. Nivel de Soporte Mínimo Requerido: Modalidad 8x5 – Atención Telefónica, Reemplazo al siguiente día laboral de Hardware.
	OTROS *Para todos los equipos solicitados en la presente oferta, la marca de los equipos propuestos por el licitante deberá ser la misma debido a que se requiere de una sola plataforma de administración y monitoreo de la red.* Se deberán entregar todos los manuales para la completa operación del equipo. Se deberá prever la Instalación, Configuración y Puesta en Marcha de los Equipos con todos los detalles necesarios sin cargo para la Convocante. Se deberá prever la Transferencia de Conocimiento en cuanto al Manejo y Configuración de los Equipos entregados. El mismo consiste en la Capacitación de al menos 3(tres) Técnico que designe la Convocante.

ROUTER/FIREWALL

Cantidad: 1(uno)

Adquisición de un sistema de seguridad informática perimetral que sea del tipo Administración Unificada de Amenazas (UTM por sus siglas en inglés), donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que se detallan en el presente documento.

El dispositivo debe ser un equipo de propósito específico.

Capaz de brindar una solución de "Complete Content Protection". Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.

ITEM	CARACTERISTICAS		MINIMO EXIGIDO	PROPUESTA DEL OFERENTE	
				CUMPLE SI/NO	EXPLICAR COMO CUMPLE
1.	RENDIMIENTO Y CAPACIDAD	Performance Firewall Troughput en paquetes de 64 bytes	1500 Mbps		
2.		VPN IPSEC Troughput	1000 Mbps		
3.		Sesiones Concurrentes soportadas	498.000		
4.		Nuevas sesiones por segundo	3.990		
5.		Cantidad de Políticas de Seguridad	5.000		
6.		Cantidad de Usuarios Concurrentes.	Ilimitado		
7.	CONECTIVIDAD DE RED	Cantidad de puertos 10/100/1000Base-T – Configurables como WAN	2		

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

8.		Cantidad de puertos 10/100/1000Base-T – Configurables como LAN o DMZ	6		
9.		Cantidad de puertos 10/100/1000Base-T – Configurables como DMZ	1		
10.		Puertos USB 2.0	1		
11.	**ROUTING**	BGP	EXIGIDO		
12.		OSPF	EXIGIDO		
13.		RIP v1/v2	EXIGIDO		
14.		Soporte a ruteo de multicast	EXIGIDO		
15.		Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas	EXIGIDO		
16.		Soporte a políticas de ruteo (policy routing)	EXIGIDO		
17.		Soporte a ruteo dinámico RIPng, OSPFv3	EXIGIDO		
18.		Soporte de ECMP (Equal Cost Multi-Path)	EXIGIDO		
19.	**AUTENTICACION DE USUARIOS Y CONTROL DE ACCESO**	Capacidad de integrarse con Servidores de Autenticación RADIUS	EXIGIDO		
20.		Capacidad nativa de integrarse con directorios LDAP	EXIGIDO		
21.		Soporte a inclusión en autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) y mediante archivos.	EXIGIDO		
22.	**TRADUCCION DE DIRECCIONES**	NAT	EXIGIDO		
23.		PAT	EXIGIDO		
24.		NAT estatico	EXIGIDO		
25.		NAT con PAT	EXIGIDO		
26.	**ASIGNACION DE DIRECCIONES IP**	Cliente DHCP	EXIGIDO		
27.		Servidor DHCP	EXIGIDO		
28.		DHCP Relay	EXIGIDO		
29.	**CONMUTACION EN LAYER 2**	Soporte de VLAN 802.1Q	4000		
30.		Soporte de Link Aggregation Group (802.3ad) con un mínimo de 4 interfaces por grupo	EXIGIDO		
31.		Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs	EXIGIDO		
32.	**ADMINISTRACION DE TRAFICO Y CALIDAD DE SERVICIO (QoS)**	Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall	EXIGIDO		
33.		Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo	EXIGIDO		
34.		Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo	EXIGIDO		
35.		Capacidad para definir prioridad de tráfico, en al menos tres niveles de importancia	EXIGIDO		
36.		Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión	EXIGIDO		
37.		Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.	EXIGIDO		
38.	**ALTA DISPONIBILIDAD**	Soporte de Alta Disponibilidad en modo transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle.	EXIGIDO		
39.		Soporte de Alta Disponibilidad en modo Activo-Activo	EXIGIDO		

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

40.		Soporte de Alta Disponibilidad en modo Activo-Pasivo	EXIGIDO		
41.		Posibilidad de definir al menos dos interfaces para sincronía para Alta Disponibilidad de forma a evitar el uso de Multicast en la red	EXIGIDO		
42.	**CONTROL DE APLICACIONES**	El equipo deberá poseer prestaciones de Control de Aplicaciones.	EXIGIDO		
43.		Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo	EXIGIDO		
44.		La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico	EXIGIDO		
45.		Las solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante	EXIGIDO		
46.		El listado de aplicaciones debe actualizarse periódicamente	EXIGIDO		
47.		Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log	EXIGIDO		
48.		Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log	EXIGIDO		
49.		Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping	EXIGIDO		
50.		Preferentemente deben soportar mayor granularidad en las acciones	EXIGIDO		
51.	**INSPECCION DE CONTENIDO – IDS/IPS**	El equipo deberá poseer prestaciones de IDS/IPS	EXIGIDO		
52.		Performance Inspeccion IPS	200 Mbps		
53.		El Detector y preventor de intrusos deberá de estar orientado para la protección de redes	EXIGIDO		
54.		El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de linea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror.	EXIGIDO		
55.	**INSPECCION DE CONTENIDO – IDS/IPS**	El detector y preventor de intrusos podrá implementarse en linea y fuera de linea en forma simultánea para distintos segmentos.	EXIGIDO		
56.		El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad sin necesidad de instalar un servidor o equipo externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos.	EXIGIDO		
57.		Deberá soportar captar ataques por Anomalía (Anomaly detection).	EXIGIDO		
58.		Deberá soportar captar ataques basado en análisis de firmas en el flujo de datos en la red (signature based / misuse detection).	EXIGIDO		
59.		Deberá permitir configurar firmas nuevas para cualquier protocolo.	EXIGIDO		

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

60.		Deberá poseer una tecnología de detección tipo Stateful basada en Firmas (signatures).	EXIGIDO		
61.		Deberá soportar la actualización automática de firmas para el detector de intrusos (por 3 años)	EXIGIDO		
62.		El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios	EXIGIDO		
63.		Deberá contar con mecanismos de deteccion de ataques basados en Reconocimiento de patrones y Análisis de protocolos.	EXIGIDO		
64.		Deberá contar con mecanismos de deteccion de ataques basados en Detección de anomalías.	EXIGIDO		
65.		Deberá contar con mecanismos de deteccion de ataques basados en Detección de ataques de RPC (Remote procedure call)	EXIGIDO		
66.		Deberá contar con mecanismos de Protección contra ataques de Windows o NetBios	EXIGIDO		
67.		Deberá contar con mecanismos de Protección contra ataques de SMTP, IMAP o POP.	EXIGIDO		
68.		Deberá contar con mecanismos de Protección contra ataques DNS.	EXIGIDO		
69.		Deberá contar con mecanismos de Protección contra ataques a FTP, SSH y Telnet.	EXIGIDO		
70.		Deberá contar con mecanismos de Protección contra ataques de ICMP.	EXIGIDO		
71.		Deberá contar con Alarmas mostradas en la consola de administración del equipo.	EXIGIDO		
72.		Deberá contar con la capacidad de cuarentena. La misma debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto	EXIGIDO		
73.	**INSPECCION DE CONTENIDO – FILTRADO DE URL**	El equipo poseer prestaciones de Filtrado de Páginas Web (URL Filtering).	EXIGIDO		
74.		El equipo deberá poseer la capacidad de trabajar como un Proxy Cache	EXIGIDO		
75.		Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 39 millones de sitios web en la base de datos.	EXIGIDO		

76.	**INSPECCION DE CONTENIDO – FILTRADO DE URL**	Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad sin necesidad de instalar un servidor o equipo externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.	EXIGIDO		
77.		Configurable directamente desde la interfaz de administración del dispositivo. Con capacidad para permitir esta protección por política de control de acceso.	EXIGIDO		
78.		Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo	EXIGIDO		

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

		establecida			
79.		Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables.	EXIGIDO		
80.		Capacidad de filtrado de scripts en páginas web (JAVA/Active X).	EXIGIDO		
81.	**INSPECCION DE CONTENIDO – ANTISPAM**	El equipo poseer prestaciones de Antispam.	EXIGIDO		
82.		La capacidad antispam incluída deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.	EXIGIDO		
83.		La capacidad AntiSpam incluída deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address)	EXIGIDO		
84.		La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como mecanismos para detección de SPAM	EXIGIDO		
85.		En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.	EXIGIDO		
86.	**ADMINISTRACION**	Soporte de Interfaz CLI	EXIGIDO		
87.		Soporte de Interfaz WEB (HTTP y HTTPS)	EXIGIDO		
88.		Puerto serial dedicado para administración.	EXIGIDO		
89.		Comunicación cifrada y autenticada con username y password, tanto como para la interfase gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet)	EXIGIDO		
90.		Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.	EXIGIDO		
91.		El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet,http o HTTPS.	EXIGIDO		
92.		El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser	EXIGIDO		

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

		(Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningun software adicional.			
93.		Soporte de SNMP versión 2	EXIGIDO		
94.		Soporte de servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos	EXIGIDO		
95.	**ALIMENTACION ELECTRICA Y DIMENSIONES**	Tensión de operación	Alterna, 220VCA		
96.		Montaje en rack de 19"	EXIGIDO		
97.					
98.	**IMPLEMENTACION**	INSTALACION, CONFIGURACION Y PUESTA EN MARCHA, ADEMAS DE LA CAPACITACION A 03 PERSONAS COMO MINIMO CONTROL ANCHO DE BANDA POR VLAN CONTROL DE ANCHO DE BANDA PARA LA RED WLAN SEGMENTADOS POR CATEGORIAS CONTROL DE ANCHO DE BANDA INDEPENDIENTE PARA LOS SERVIDORES SEPARADOS POR SERVICIOS DEBE CONTAR CON REGLAS DE ACCESOS POR CATEGORIAS Y OTRAS FUNCIONES REFERENTE A LA SEGURIDAD.	EXIGIDO		
99.	**GARANTIA**	3(tres) años. Mano de Obra, Partes, Repuesto en las oficinas de la Convocante sin cargo. Nivel de Soporte Mínimo Requerido: Modalidad 8x5 – Atención Telefónica, Reemplazo al siguiente día laboral de Hardware.			
100.					

ESPECIFICACIONES RACK CERRADO 42U COMO MÍNIMO:

1(Un) Gabinete estándar para aplicaciones de integración en red y servidores de baja o media densidad de 42U de altura mínima:

Incluye:

- Piezas de anexión
- CD de documentación
- Puertas y paneles laterales con llave única
- Patas niveladoras
- Piezas para montaje
- Ruedas preinstaladas

INFORMACION DE DIMENSIONES Y PESO

Peso neto: 125.09 KG
Alto: 1991.00 mm
Ancho: 600.00 mm
Fondo: 1070.00 mm
Capacidad de peso (carga estática): 1363.64 KG
Capacidad de peso (carga dinámica): 1022.73 KG
Altura del rack: 42U mínimo
Color: Negro
Garantía: 2(dos) años.

Especificaciones PDU de 32A:

2(dos) Rack PDU, Basic, Zero U, 32A, 230V, (20) C13 & (4) C19; IEC C20
APC Basic Rack PDU , Entrada: 200V, 208V, 230V , Tipo de enchufe: IEC-320 C20 , Longitud del cable: 10 Pies (3.05 metros) , Salida: 230V , Conexiones de salida: IEC 320 C13,IEC 320 C19
Incluye: Guía de instalación, Brackets para Rack-mount, Juego de montaje sin herramientas
Fuente de potencia de entrada única
Proporcione energía desde un whip (látigo) de derivación a múltiples equipos, de modo de alimentar equipos de montaje en rack de la manera más conveniente. Ahorrará tiempo y dinero durante la instalación al emplear un whip de derivación y conexiones estándares.
Amplia gama de conexiones de entrada y de salida.
230V entre tomas de salida múltiples. Contar con diversas entradas y salidas le permite al usuario adaptarse a requisitos de potencia cambiantes. APC ofrece unidades que alcanzan 5,7kW con un sólo whip (látigo) de derivación.

Salida	
Tensión de salida nominal	230V
Total máximo de corriente extraída	16ª
(20) IEC 320 C13	
(4) IEC 320 C19	

Entrada	
Entrada de voltaje	200V,208V,230V
Frecuencia de entrada	50/60 Hz
Tipo de enchufe	IEC-320 C20
Longitud del cable	3.05 metros

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

Misión: *Desarrollar y promover la formación profesional y favorecer las condiciones de inserción laboral, a través de la capacitación, asistencia técnica, consultoría, incorporación y difusión de Innovaciones tecnológicas pertinentes de calidad, aumentando la competitividad de los segmentos de la producción y contribuyendo al desarrollo humano integral y sustentable del país.*

Cantidad de cables de alimentación	1
Corriente de entrada máxima por fase	16ª
Capacidad de carga	3680 VA
Físico	
Peso neto	4.86 KG
Dimensiones de altura máxima	1619.00 mm
Dimensiones de anchura máxima	56.00 mm
Dimensiones de profundidad máxima	44.00 mm
Peso de embarque	5.77 KG
Altura de envío	2134.00 mm
Anchura de envío	152.00 mm
Profundidad de envío	127.00 mm
Color	Negro
Conformidad	
Reparación o reemplazo por 2 años	
Cumplimiento de normas ambientales	

Garantía: 2(dos) Años.

RACK DE COMUNICACION

Los Rack de 9U mínimo del tipo pivotante para los equipos de accesos conforme a las especificaciones técnicas.

Rack de pared de 9U
Construido 100% en acero laminado en frio de espesor de 1,5mm
Puerta frontal con visor de vidrio templado y cerradura con llave
Puerta frontal con abertura 180°
Puerta frontal desmontable y reversible
Tapas laterales en hoja metálica desmontables
Paneles frontales y laterales ventilados
Techo con capacidad para instalación de dos mini ventiladores
Línea de corte para entrada de cables por base y techo - 4 entradas en cada lado
4 (cuatro) parantes de fijación regulables
Sistema de fijación a la pared por medio de soporte desmontable
Acabado en pintura de superficie texturado. Pintura Electroestática color negro

Deberá incluir cuarenta tornillos con tuercas enjauladas
Tapa ciega de goma para orificios de entrada de cable.
Deberá incluir 1(un) Supresor de Picos del Tipo Rackeable de 19" de al menos 8(ocho) Tomas.
Dimensiones:
Alto exterior: 50 cm
Profundidad exterior: 60 cm
Profundidad Interna útil: Hasta 50 cm
Garantía: 2(dos) Años o Superior.
Certificados: ANSI/EIA RS310-D; IEC60297-2

Garantía: 2(dos) Años.

2(dos) x UPS de 3kVA, Doble Conversión, On-Line, AVR, Onda Senoidal, autonomía expandible, Rackeable, Tarjeta de Monitoreo SNMP/WEB, 2 años de garantía. Para Datacenter	
Generalidades	Autodiagnóstico de forma automática, Apagado automático, Regulación automática de tensión, Desvío automático incorporado, Puesta en marcha en frío, Notificación de alerta avanzada de problemas, Indicador LED de destellos, Compatible con generador, Baterías intercambiables en funcionamiento, Corrección del factor de alimentación de entrada, Manejo inteligente de la batería, Protección contra relámpagos y sobrecargas, Medidor de carga, Tensiones de salida múltiples, Acondicionamiento de línea clasificado para redes, Capacidad de manejo de sobrecarga, Frecuencia programable, Rack Mount – (kit de montaje se adquiere por separado) Autonomía escalable, Salida de onda sinusoidal, Software, Carga de batería con compensación de temperatura, Cierre automático seguro y sin inconvenientes, Tiempo de transferencia cero

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

Misión: *Desarrollar y promover la formación profesional y favorecer las condiciones de inserción laboral, a través de la capacitación, asistencia técnica, consultoría, incorporación y difusión de Innovaciones tecnológicas pertinentes de calidad, aumentando la competitividad de los segmentos de la producción y contribuyendo al desarrollo humano integral y sustentable del país.*

Salida	
Capacidad de Potencia de Salida	2100 Vatios / 3000 VA
Tensión de salida nominal	230V
Nota de tensión de salida	Configurable para tensión de salida nominal para 220 : 230 o 240
Eficiencia con carga completa	92%
Distorsión de tensión de salida	menor a 3%
Frecuencia de salida (sincronizada a red eléctrica principal)	50/60 Hz +/- 3 Hz ajustable por el usuario +/- 0,1
Factor de cresta	3 : 1
Tipo de forma de onda	Onda senoidal
Conexiones de salida	(8) IEC 320 C13 y (2) IEC 320 C19
Desviación	Desviación interna (automática y manual)
Entrada	
Entrada de voltaje	230V
Frecuencia de Entrada	50/60 Hz +/- 5 Hz (autosensible)
Tipo de enchufe	IEC-320 C14
Variación de tensión de entrada para operaciones principales	160 - 280V
Variación de tensión de entrada adaptable para operaciones principales	100 - 280V
Otras tensiones de entrada	220, 240VAC
Baterías y Autonomía	
Tipo de Baterías	VLRA - Batería sellada de plomo sin necesidad de mantención con electrolito suspendido: a prueba de filtración
Tiempo típico de recarga	3 horas
Autonomía a media carga	33.9 minutos (1050 Vatios)
Comunicaciones y manejo	
Puerto de interfaz	DB-9 RS-232,SmartSlot
Cantidad de interfaces SmartSlot™	1 (La tarjeta de monitoreo remoto SNMP/WEB en este modelo es un opcional)
Panel de control	Visualizador de estatus LED con barras gráficas de carga y batería e indicadores de red: Batería activada: Cambiar Batería: Sobrecarga y derivación

Visión: *Institución Líder e Innovadora en formación y capacitación profesional en el país, y reconocida internacionalmente.*

Alarma audible	Alarma de batería encendida: alarma distintiva de carga de batería baja: alarma de sobrecarga de tono continuo
Interruptor de emergencia (EPO)	Sí
Protección contra picos y filtrado	
Clasificación de energía de sobrecarga (Joules)	420 Joules
Filtrado	Filtrado completo de ruidos multipolares: sobretensión tolerable de 0,3% IEEE: tiempo de respuesta de cierre cero: cumple con UL 1449
Físico	
Alto	432.00 mm
Ancho	130.00 mm
Fondo	660.00 mm
Altura del Rack	3U
Peso Neto	54.55 KG
Color	Negro
Ambiental	
Ambiente operativo	0 - 40 °C
Humedad relativa de operación	De 0 a 95% de humedad relativa, sin condensación
Elevación de operación	0 - 3000 metros
Ruido audible a 1 metro de la unidad	55.00 dBA
Disipación térmica en línea	609.00 BTU/hora
Conformidad	
Certificaciones	ISO9001:2008 e ISO14001:2004
Aprobaciones	C-tick, CE, EN 50091-1, EN 50091-2, EN 55022 Clase A, EN 60950, EN 61000-3-2, GOST, VDE
Garantía estándar	Reparación o reemplazo por 2 años.
Cumplimiento de normas ambientales	RoHS
Topología	
Topología	Doble Conversión ON LINE

UPS de 1500VA Interactiva para RACKS de COMUNICACIONES:

Potencia	1500 VA / 900 Watt
Tecnología	Interactiva
Formato	Torre

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

Entrada	
Voltaje nominal:	220V
Rango regulación:	165V AC ~ 275V AC
Frecuencia	50/60Hz ±10%
Salida	
Voltage:	220V ±10%
Frecuencia	50/60Hz ± 1%(Battery)
Factor de cresta	3:1
Transferencia	2-7 ms
Factor potencia	0.6
Conector salida	6 salidas tipo NEMA: 4 salidas sobre bateria; 2 salidas estabilizadas
Batería	
Tipo de batería	2×12V/8AH
Autonomía	5 ~10 minutos (dependiendo de la carga)
Tiempo recarga	8Hs con capacidad al 90%
Comunicación / Administración	
Software	Software de administración Incluir CD
Tipo de conexión	Puerto USB (incluye cable)

Otros	
Pantalla	LCD
Indicadores	Capacidad de Batería, Porcentaje de carga, Voltaje de salida, Voltaje y frecuencia de entrada, Alarma.
Ruido	<45db (1 metro)
Temperatura	0~40ºC
Humedad	0~90%
Estabilizador	AVR
Protección linea	RJ45 (Fax/Modem/Red)
Garantía	
Sobre UPS	2 años (en condiciones normales de uso)
Certificados	
ISO 9001:2008	
ISO 14001:2004	
GB/T 19001:2008	

Sección VII. Anexos

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

ANEXO N° I

DOCUMENTOS QUE COMPONEN LA OFERTA

I) Cualquier otro documento adicional requerido.		
• Autorización del Fabricante, Representante o Distribuidor		
• Balance General de los años (2011, 2012, 2013)		
• Certificado de Origen Nacional emitido por el MIC. La no presentación de la misma no será causal de descalificación.		
• Declaración Jurada de cumplimiento de normas laborales en general – Presentación de Planillas ante al el Ministerio de Trabajo, Empleo y Seguridad Social (MTESS) y de no adeudar al mismo en concepto de multas por incumplimientos en normas laborales.		
• Declaración Jurada de Garantía por tres (3) años de Mantenimiento de Cableado Estructurado		
• Declaración Jurada de Garantía por tres años (3) años de la **UNIDAD DE CONMUTACION DE DATOS TIPO BACKBONE (NODOS CENTRALES)** Mano de Obra, Partes, Repuesto en las oficinas de la Convocante sin cargo. Nivel de Soporte Mínimo Requerido: Modalidad 8x5 – Atención Telefónica, Reemplazo al siguiente día laboral de Hardware.		
• Declaración Jurada de Garantía por tres años (3) años de la **UNIDAD DE CONMUTACION DE DATOS TIPO ACCESO (NODOS CENTRALES) con ALIMENTACION SOBRE ETHERNET (PoE)** Mano de Obra, Partes, Repuesto en las oficinas de la Convocante sin cargo. Nivel de Soporte Mínimo Requerido: Modalidad 8x5 – Atención Telefónica, Reemplazo al siguiente día laboral de Hardware.		
• Declaración Jurada de Garantía por tres años (3) años de la **UNIDAD DE CONTROL CENTRALIZADO DE ANTENAS PARA ACCESO INALAMBRICO (ACCESS POINTS)** Mano de Obra, Partes, Repuesto en las oficinas de la Convocante sin cargo. Nivel de Soporte Mínimo Requerido: Modalidad 8x5 – Atención Telefónica, Reemplazo al siguiente día laboral de Hardware.		
• Declaración Jurada de Garantía por tres años (3) años de la **UNIDAD DE ACCESO INALAMBRICO (ACCESS POINTS) CONTROLADO CENTRALMENTE.** Mano de Obra, Partes, Repuesto en las oficinas de la Convocante sin cargo. Nivel de Soporte Mínimo Requerido: Modalidad 8x5 – Atención Telefónica, Reemplazo al siguiente día laboral de Hardware.		
• Declaración Jurada de prever la Instalación, Configuración, y Puesta en Marcha de los Equipos con todos los detalles necesarios sin cargo para la Convocante.		
• Declaración Jurada de prever la transferencia de Conocimiento en cuanto al manejo y configuración de los equipos entregados. Capacitación de al menos tres		

Avda. Molás López N°480
Asunción - Paraguay

Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

(3) técnicos que designe la Convocante		
• Declaración Jurada de Garantía por tres años (3) años de la **ROUTER/FIREWALL** Mano de Obra, Partes, Repuesto en las oficinas de la Convocante sin cargo. Nivel de Soporte Mínimo Requerico: Modalidad 8x5 – Atención Telefónica, Reemplazo al siguiente día laboral de Hardware.		
• Declaración Jurada de Garantía por dos años (2) años del RACK CERRADO 42U		
• Declaración Jurada de Garantía por dos años (2) años del PDU de 32A		
• Declaración Jurada de Garantía por dos años (2) años del UPS de 3 KVA, REPARACIÓN O REEMPLAZO		
• Declaración Jurada de Garantía por dos años (2) años sobre UPS		

ANEXO N° II

DOCUMENTOS A PRESENTAR PARA LA FIRMA DEL CONTRATO

3.Documentos. Personas Físicas / Jurídicas y/o Consorcios
a) Si la oferta adjudicada estuviera acompañada de documentos emitidos por autoridades extranjeras, el Oferente deberá acompañar los documentos debidamente legalizados por el Consulado Paraguayo del país de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay.
• La firma contratada deberá presentar certificados de entrenamiento internacional del personal; en las áreas de Cobre, Fibra Óptica, Datacenter y Diseño.
• Para la aceptación definitiva del cableado estructurado de Datos, el contratista deberá presentar como mínimo, la siguiente documentación debidamente certificada por los fiscales: - Plano físico actualizado (as built) del proyecto final, en archivo informático, indicando claramente el tendido de los cables (indicando tipos de cables, cantidades y todos materiales utilizados) - Plano lógico del cableado que coincida perfectamente con las etiquetas del cableado (cables, Patch Panel, cajas, etc.). - Documentación de todo lo instalado en cada rack. Una copia deberá quedar en cada rack. - Cualquier otra documentación relativa al proyecto que pueda ser requerida por los fiscales. - Presentación dela documentación del resultado de las mediciones de cada punto del cableado de la RED de Datos, Telefonía efectuados con los equipos de Testeo (Certificación para cables de categoría 6).
• Se deberá adicionar a la documentación a presentar información de detalle de montajes y estadísticas de instalación donde figuren fotos de los racks terminados, de los puestos de usuarios y de puntos especiales como cruces de tuberías, acometidas, etc

Avda. Molás López N°480
Asunción - Paraguay
Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py

Adicionalmente se entregará en formato electrónico la documentación reseñada: - Se permite tanto Soporte CD-ROM como DVD-R (2 copias). - La documentación se entregará en idioma castellano y debidamente identificado no así los resultados técnicos, con indicación de la fecha de realización de la instalación. Los formatos informáticos para la documentación presentada son los siguientes: - Ficheros de texto: La Memoria final de la Instalación se deberá suministrar En los siguientes formatos: MICROSOFT WORD (*.DOC) DOCUMENT FORMAT (*.PDF) - Diagramas: Se deberán proporcionar en los formatos AUTOCAD (*.DWG), PORTABLE DOCUMENT FORMAT (*.PDF) y VISIO (*.VSD)
• El sistema de cableado deberá estar respaldado por una Garantía de Rendimiento, por un periodo de al menos 3 (tres) años. La garantía de rendimiento será entregada por el Contratista adjudicado y se establecerá entre el Snpp y el fabricante del sistema de cableado.

TODAS LAS DEMAS CONDICIONES ESTABLECIDAS EN EL PLIEGO DE BASES Y CONDICIONES PERMANECEN INVARIABLES E INALTERABLES.----------

Abg. CARLOS MARÍA RUÍZ GONZÁLEZ
Director - U. O. C.
SERVICIO NACIONAL DE PROMOCIÓN PROFESIONAL

Avda. Molás López N°480
Asunción - Paraguay
Tel.: (595) 21 603-062
(595) 21 607-289
Pagina Web: www.snpp.edu.py
Email: snpp@snpp.edu.py