

MANUAL DE MANTENIMIENTO
CONTRATO DE OBRA No. 12-OBR009 DE 2024

OBJETO: “CONTRATAR A NOMBRE DE LA NACIÓN - CONSEJO SUPERIOR DE LA JUDICATURA DIRECCIÓN EJECUTIVA DE ADMINISTRACIÓN JUDICIAL SECCIONAL NEIVA, LA ADECUACIÓN Y REMODELACIÓN DE LA INFRAESTRUCTURA FÍSICA DE LOS PISOS QUINTO Y SEXTO DE LA SEDE JUDICIAL EDIFICIO "RODRIGO LARA BONILLA" PALACIO DE JUSTICIA DE NEIVA”

ENTIDAD CONTRATANTE: LA NACIÓN - CONSEJO SUPERIOR DE LA JUDICATURA- DIRECCIÓN EJECUTIVA SECCIONAL DE ADMINISTRACIÓN JUDICIAL DE NEIVA

CONTRATISTA: CONSORCIO CARVI

INTERVENTOR: CONSORCIO JR

JUNIO
2025

Contenido

1. GENERALIDADES.....	4
2. INTRODUCCIÓN	4
3. OBJETIVO	4
4. ALCANCE	4
5. RESPONSABLES.....	5
6. DEFINICIONES.....	5
7. INSTRUCCIONES DE USO Y MANTENIMIENTO	7
7.1. VIDRIO TEMPLADO Y PUERTAS	8
7.2. CARPINTERÍA EN MADERA.....	11
7.3. PINTURAS	14
7.4. REDES ELÉCTRICAS Y CONECTIVIDAD	20
7.4.1. INTERRUPTORES, TOMACORRIENTES, RED REGULADA, RED NORMAL, PUNTOS DE VOZ Y DATOS, ACOMETIDAS DE AIRE ACONDICIONADO Y LUMINARIAS.	20
7.4.2. TABLEROS ELÉCTRICOS.....	22
7.4.3. RACKS	24
7.4.4. UPS	27
7.4.5. SWITCHES ARUBA DE 24 PUERTOS	30
7.5. MUROS EN DRYWALL	32
7.6. REVESTIMIENTOS DE PISOS Y PAREDES DE BAÑO EN TABLETA CERÁMICA	35
7.7. MESÓN LAVAMANOS EN GRANITO SAN GABRIEL.....	39
7.8. SANITARIOS Y ORINALES	41
7.9. GRIFERÍA ANTIVANDÁLICA PARA LAVAMANOS	44
7.10. VENTANERÍA EN ALUMINIO	47
7.11. DIVISIONES DE BAÑOS EN ACERO INOXIDABLE.....	49
8. ANEXOS.....	53
8.1. FORMATO DE REALIZACIÓN DE MANTENIMIENTO.	53

8.2. MANUAL DE MANTENIMIENTO UPS.....	54
8.3. MANUAL DEL USUARIO SWITCHES - ARUBA	55
8.4. MANUAL DEL USUARIO SANITARIOS Y ORINALES	56
8.5. MANUAL DEL USUARIO GRIFERÍA DE LAVAMANOS	57

1. GENERALIDADES

NOMBRE FIRMA CONSTRUCTORA	CONSORCIO CARVI.
NIT	901895769-1
CORREO ELECTRÓNICO	consorciocarvi@yahoo.com
NOMBRE FIRMA INTERVENTORA	CONSORCIO JR.
CONTRATO DE OBRA N° 12-OB009 DE 2024 SUSCRITO ENTRE LA RAMA JUDICIAL Y EL CONSORCIO CARVI. NEIVA - HUILA	

2. INTRODUCCIÓN

El presente documento es una guía que permite a los usuarios del proyecto que tiene por objeto **“CONTRATAR A NOMBRE DE LA NACIÓN - CONSEJO SUPERIOR DE LA JUDICATURA DIRECCIÓN EJECUTIVA DE ADMINISTRACIÓN JUDICIAL SECCIONAL NEIVA, LA ADECUACIÓN Y REMODELACIÓN DE LA INFRAESTRUCTURA FÍSICA DE LOS PISOS QUINTO Y SEXTO DE LA SEDE JUDICIAL EDIFICIO “RODRIGO LARA BONILLA” PALACIO DE JUSTICIA DE NEIVA”** contar con una referencia de las buenas prácticas de mantenimiento para garantizar la vida útil proyectada del mantenimiento, mejoras y mantenimiento del inmueble..

Este manual de mantenimiento es el cuidado que se debe tener en cuenta para conservar todos los elementos arquitectónicos con sus características, equipos técnicos de la adecuación y remodelación de los pisos quinto y sexto del Palacio de Justicia de la Ciudad de Neiva. No habría otra forma distinta para conservarlos a través del tiempo sino por medio de su correcto uso, respetando todas sus características originales y protegiéndolos de factores y agentes externos que puedan deteriorarlos.

3. OBJETIVO

Indicar las actividades de mantenimiento y periodicidad de estas a ser aplicadas con el fin de asegurar la vida útil de los elementos de la infraestructura, en conformidad con las actividades ejecutadas dentro del alcance del contrato.

4. ALCANCE

Este Manual de Mantenimiento es aplicable a todas las adecuaciones y remodelaciones ejecutadas por la firma constructora CONSORCIO CARVI, en el marco del contrato de obra 12-OB009 DE 2024, en el Palacio de Justicia “Rodrigo Lara Bonilla” de la ciudad de Neiva.

5. RESPONSABLES

El responsable por la aplicación del presente Manual de mantenimiento será el Consejo Superior de la Judicatura Dirección Ejecutiva Seccional de Administración Judicial de la ciudad de Neiva., quien a su vez gestionará la aplicación de mantenimientos preventivos y/o correctivos para asegurar la vida útil de cada una de las mejoras y adecuaciones realizadas, a partir del recibido de la obra a conformidad de las partes involucradas.

6. DEFINICIONES

CONSERVACIÓN

La conservación, en el ámbito del presente Manual, está dedicada a la preservación para los usuarios futuros de las condiciones físicas de la infraestructura de la oficina en sus materiales, estructura, espacialidad o volumetría, entre otros. Implementando un conjunto de operaciones periódicas necesarias para mantener en condiciones óptimas de servicio y funcionamiento la infraestructura, equipos e instalaciones. Las actividades de conservación incluyen el análisis, documentación, tratamiento y el cuidado.

CONSERVACIÓN PREVENTIVA

Todas aquellas medidas y acciones que tengan como objetivo evitar o minimizar futuros deterioros o pérdidas. Se realizan sobre el contexto o el área circundante al bien, o más frecuentemente un grupo de bienes, sin tener en cuenta su edad o condición. Estas medidas y acciones son indirectas - no interfieren con los materiales y las estructuras de los bienes. No modifican su apariencia. Algunos ejemplos de conservación preventiva incluyen las medidas y acciones necesarias para el registro, control de las condiciones ambientales (luz, humedad, contaminación atmosférica e insectos), planificación de emergencia, educación del personal, sensibilización del público, aprobación legal.

DETERIORO

Entendido como el desgaste ocasionado sobre los elementos componentes de la infraestructura, producido por el uso normal, falta de mantenimiento, desgaste natural, accidentes, uso inadecuado o factores ambientales.

TIPOS DE DETERIORO DE LA INFRAESTRUCTURA

DETERIORO POR EL USO NORMAL.

Es el que se presenta en la infraestructura por la actividad cotidiana de uso.

DETERIORO POR FALTA DE MANTENIMIENTO (RECURRENTE, PREVENTIVO Y PREDICTIVO).

Es el que se presenta en la infraestructura por la falta de acciones para el sostenimiento adecuado en un nivel aceptable de la infraestructura; la omisión de estos procedimientos regularmente origina mantenimientos correctivos de mayor costo y dimensión.

DETERIORO POR DESGASTE NATURAL.

Causado por uso normal, generalmente se presenta en recubrimientos y elementos móviles, como puertas, ventanas, dotaciones por cambio de tecnologías, cumplimiento de ciclos de uso.

DETERIORO POR ACCIDENTES.

Causado por terceros donde en un evento fuera de control se generan daños a la infraestructura.

DETERIORO POR USO INADECUADO DE LA INFRAESTRUCTURA.

Dentro del uso normal de la infraestructura se presentan situaciones de mal uso por parte de los usuarios causadas por desconocimiento del funcionamiento, acciones malintencionadas o vandalismo. Deterioro por factores ambientales.

EL DETERIORO POR FACTORES AMBIENTALES

Es recurrente por lluvia, efectos nocivos de los rayos del sol, altas humedades y efectos abrasivos por zonas desérticas o salinidad en zonas costeras. Este deterioro depende específicamente de las zonas geográficas donde están ubicados los establecimientos educativos

MANTENIMIENTO

Conjunto de acciones periódicas y sistemáticas realizadas con el propósito de asegurar, garantizar o extender la vida útil de la infraestructura, necesarias para conservar las condiciones originales de funcionamiento normal y adecuado, su seguridad, productividad, confort, imagen corporativa, salubridad e higiene.

TIPOS DE MANTENIMIENTO

RUTINARIO

Comprende este las labores de revisión, observación y limpieza realizadas en forma diaria y dentro de períodos de tiempo cercanos. Este proceso da como resultado la realización o ejecución de reparaciones menores.

PREVENTIVO

Este tipo de mantenimiento está enfocado a la conservación de todas las zonas que conforman la adecuación y renovación del piso cinco y piso seis los elementos arquitectónicos, técnicos y de dotación. Se logra mediante el análisis de los registros de inspección.

CORRECTIVO

Es producto de la no aplicación del mantenimiento preventivo o rutinario se presenta por fallas en los materiales especificados e instalados, y/o por mal uso de estos.

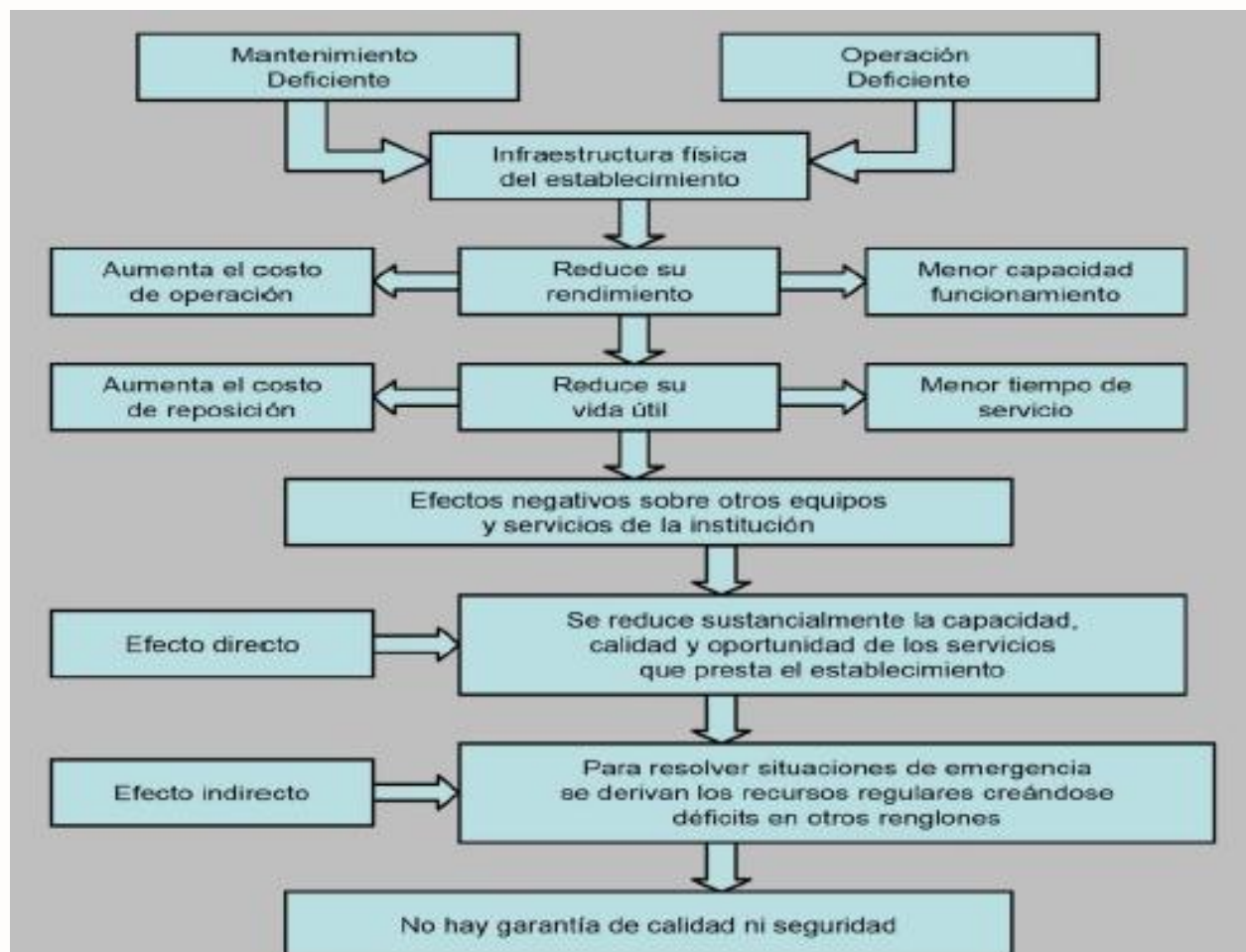
PREDICTIVO

Se aplica para equipos y maquinarias, con la sustitución parcial de piezas o partes integrantes que requieren ser reemplazadas para permitir la continuidad en el funcionamiento.

7. INSTRUCCIONES DE USO Y MANTENIMIENTO

Las instrucciones de uso son indicaciones dadas para conseguir el objetivo descrito, con el fin de asegurar la vida útil de los elementos de la infraestructura intervenida, en conformidad con las actividades ejecutadas dentro del alcance del contrato (mantenimiento).

Las instrucciones de mantenimiento van enfocadas a conocer el manejo que se dará para conservar la funcionalidad y estética en la infra, preservando la vida útil proyectada para las mejoras y adecuaciones realizadas.



Cada vez que se deba hacer algún tipo de mantenimiento, se debe tomar registro fotográfico como evidencia de este, con el fin de no generar conflictos al momento de algún tipo de reclamo.

7.1. VIDRIO TEMPLADO Y PUERTAS



Se realizó el suministro e instalación de divisiones y puertas en vidrio templado de 10 mm de espesor con polarizado negro y puertas de vidrio templado con sandblasting, todas cuentan cerraduras de sobreponer, poste pivote y herraje para su correcto funcionamiento.

Cuidados para el uso y limpieza

- Evite los golpes fuertes y/o continuos, especialmente en la zona de los bordes o las esquinas del vidrio, ya que esta es la zona de menor resistencia.
- Evite apoyarse sobre los vidrios, ya que su resistencia a la flexión se ve limitada por el tipo de instalación y accesorios usados.
- En puertas No forzar más de lo que permite la bisagra al abrir o cerrar ya que el exceso de fuerza ejercida puede generar que se rompa el panel.
- En lo posible, enjuague y utilice una escobilla de goma para eliminar las gotas de agua de los paneles de vidrio.
- Para que la superficie del vidrio se mantenga en perfecto estado, evita el uso de cuchillas o elementos afilados para raspar sustancias adheridas al vidrio, ya que pueden causar rayones. En su limpieza, mejor emplea bayetas de microfibra que estropajos o periódico.
- Utilice un producto especializado para limpieza de vidrios. Siga atentamente las instrucciones del producto.
- Ocasionalmente, limpie con un detergente suave diluido en agua, para mantener los paneles de vidrio como si fueran nuevos.
- Utilice una esponja o un paño suave húmedo. Nunca utilice un material abrasivo, como un cepillo o esponjilla metálica, ni papeles para limpiar las superficies.
- Nunca utilice productos de limpieza que contengan abrasivos o productos que contengan amoníaco, blanqueadores, ácidos, ceras, alcohol o solventes ni derivados del petróleo.
- Para evitar que se formen marcas de jabón o de magnesia del agua, hábituese a secar el vidrio con un paño suave después de cada limpieza, tal como secaría sus manos con una toalla.
- No exponga el vidrio a lubricantes esmaltantes incompatibles, jabones esmaltantes, juntas esmaltantes incompatibles, sellantes esmaltantes, productos de limpieza incompatibles, salida de humedad o de alcantarillado, contacto directo con pinturas, pegamentos solventes o insulación, o exposición a solventes o a humos químicos.

Recurrencia de mantenimientos en puertas y divisiones en vidrio templado:

ELEMENTO	ACCIÓN		FRECUENCIA
DIVISIONES	LIMPIEZA	SACUDIR	SEMANAL
		LAVAR	SEMANAL
	PROTECCIÓN	VERIFICAR ESTADO Y SUJECIÓN DE ANCLAJES	TRIMESTRAL
PUERTAS	LIMPIEZA	SACUDIR	SEMANAL
	PROTECCIÓN	LUBRICAR BISAGRAS Y CERRADURAS	TRIMESTRAL

Actividades de mantenimiento según tipo:

Mantenimientos Recurrentes:

- *Semanalmente* realizar la limpieza de los vidrios con un trapo seco o con líquido limpia vidrios y un paño suave.
- *Semanalmente* realizar la inspección visual del estado en el que se encuentran los paneles de vidrio, revisando que no tengan rayones, golpes o se encuentren despicados en los bordes.
- *Trimestralmente* se debe verificar la sujeción de los paneles inmóviles, si se encuentran flojos en los puntos de sujeción, realizar el respectivo con la herramienta adecuada.
- *Trimestralmente* se debe revisar el funcionamiento de las cerraduras, lubricar o aplicar grafito en caso de ser necesario.
- *Trimestralmente* se debe realizar la revisión del estado en el que se encuentran las bisagras de las puertas, engrasar y ajustar de ser necesario para prolongar la vida útil.

Mantenimientos Correctivos:

- En caso de evidenciar grietas en alguno de los paneles, reportar para generar el cambio del panel para evitar que el vidrio estalle.

7.2. CARPINTERÍA EN MADERA



Se realizó el suministro e instalación de recibidores al ingreso de las oficinas, puertas de madera y entrepaños en las diferentes oficinas del piso cinco y piso seis.

Cuidados para el uso y limpieza

- Evitar el contacto con el agua, esto evitara que los tableros presenten algún hinchamiento y daños que son estructurales con el tiempo, en caso de que caiga agua, limpiar rápido, así mismo, se recomienda no colocar objetos que tengan humedad circundante, por ejemplo, vasos con agua fría, procurar secar de inmediato para que el material no absorba el agua
- Evitar el exceso de sol, esto ayudará a que los tableros melaminicos afecten la calidad de estos, así se evitará que haya variación de tonalidades en ellos. Se recomienda utilizar cortinas o persianas para proteger los muebles de melamina de la luz solar excesiva.
- Evitar el moho, la humedad, calor intenso, ausencia de luz y ventilación propician la aparición de moho. Una limpieza adecuada ayudara a evitarlo.
- Evitar productos que dañen la melamina, para el cuidado de mobiliario de melamina se debe evitar el uso de productos disolventes de pintura, así como esponjas abrasivas o metálicas.
- No usar ceras ni aerosoles, lo único que conseguirás es engrasar el mueble. Tampoco se debe usar trapos que cuenten con cargas electroestáticas para atraer el polvo, ni que tengan grasa.
- Limpiar los muebles con un trapo suave y humedecido con agua o con un detergente diluido en agua, se debe evitar poner grandes cantidades de agua ya que puede deteriorar el tablero. Una vez se haya pasado el trapo húmedo, pasar otro tapo seco para quitar las marcas de agua.
- Evitar colocar objetos calientes directamente sobre el escritorio.

Recurrencia de mantenimientos en puestos de trabajo

ELEMENTO	ACCIÓN		FRECUENCIA
RECIBIDORES	LIMPIEZA	SACUDIR	SEMANAL
		LIMPIAR	SEMANAL
	PROTECCIÓN	VERIFICAR ESTADO Y SUJECCIÓN DE ANCLAJES	SEMESTRAL
ENTREPAÑOS	LIMPIEZA	SACUDIR	SEMANAL
		LIMPIAR	SEMANAL
	PROTECCIÓN	VERIFICAR ESTADO Y SUJECCIÓN DE ANCLAJES	TRIMESTRAL
PUERTAS	LIMPIEZA	SACUDIR	SEMANAL

		LIMPIAR	SEMANAL
	PROTECCIÓN	LUBRICAR BISAGRAS Y CERRADURAS	TRIMESTRAL

Actividades de mantenimiento según tipo:

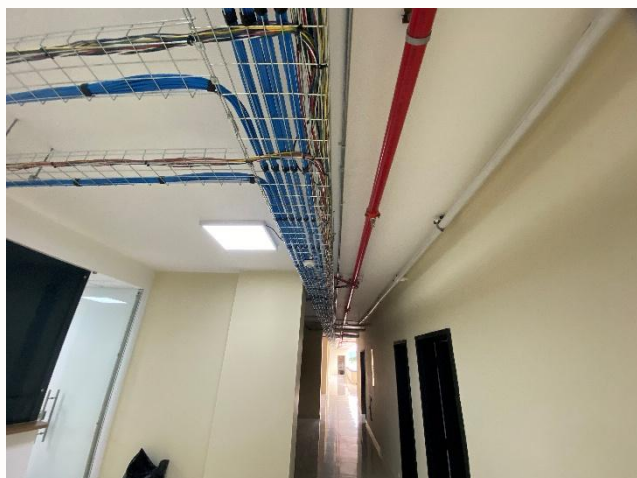
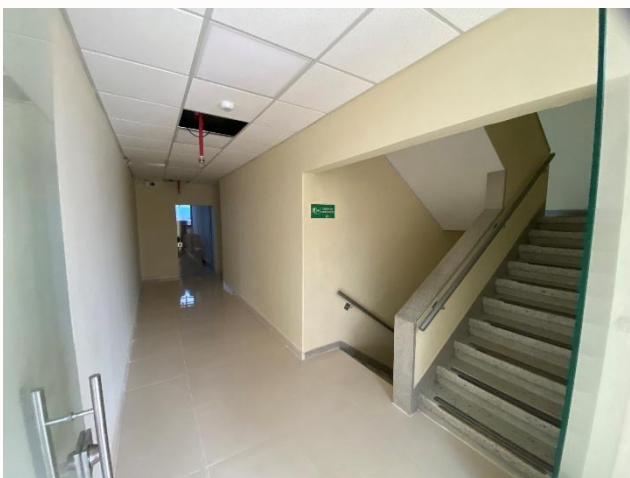
Mantenimientos Recurrentes:

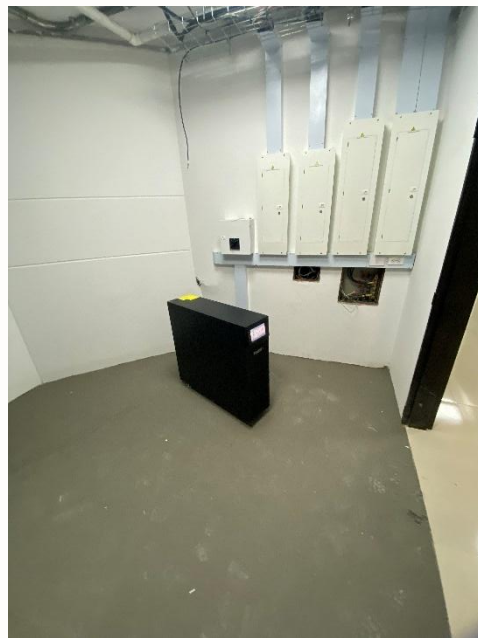
- Semanalmente realizar la limpieza de tableros de melamina de los recibidores, entrepaños y puertas con un trapo seco o con un detergente suave y un paño.
- Semanalmente realizar la inspección visual del estado en el que se encuentran tableros, revisando que no tengan rayones, golpes o se encuentren con los cubre cantos despegados.
- Trimestralmente, se debe verificar la sujeción y la lubricación de las puertas, se debe verificar la lubricación de las bisagras
- Trimestralmente se debe verificar la sujeción entre secciones de melamina en caso de que se presenten, si están flojas, realizar el ajuste respectivo con la herramienta adecuada.
- Trimestralmente se debe revisar el funcionamiento de las cerraduras, lubricar o aplicar grafito en caso de ser necesario.
- Trimestralmente se debe verificar la sujeción entre el tablero, si están flojos, realizar el ajuste respectivo con la herramienta adecuada.

Mantenimientos Correctivos:

- **Para Arañazos Leves:** Se pueden usar crayones o marcadores de melamina del color correspondiente. Aplica en la zona afectada y difumina suavemente con un paño limpio.
- **Para el caso de necesitar Rellenos:** Se puede utilizar masilla para madera o específica para melamina para rellenar agujeros o áreas desgastadas. Colocar la masilla con una espátula y alisar la superficie. Dejar que se seque según las instrucciones del producto.
- **Para Bordes Dañados:** Se puede utilizar masilla específica para melamina en el área dañada y alisarla con una espátula. Dejar secar y luego, lijar suavemente. Si los bordes se han desprendido, se debe utilizar pegamento especial para melamina o adhesivo de cianoacrilato. Aplicar el pegamento y presionar los bordes para que se adhieran, se puede usar cinta adhesiva para mantener la presión mientras se seca.
- **En caso de Restauración del Color:** Utilizar tintes específicos para melamina o crayones de retoque del color adecuado. Aplicar en la zona afectada y difuminar con un paño limpio. Considerar proteger con sellador o barniz para prevenir futuros daños.
- **Si se necesita Reemplazo de Piezas Dañadas:** Si se encuentra una pieza irreparable, no es posible conseguir los repuestos por separado.

7.3. PINTURAS







Se realizó la aplicación de pintura en muros existentes y muros nuevos en DryWall con pintura vinilo tipo 1 a 3 manos en colores blanco para las áreas internas de las oficinas y blanco hueso para los corredores del piso cinco y piso seis.

Cuidados para el uso y limpieza

- Revisar constantemente todas las superficies es el mejor hábito para determinar la necesidad de pintar.
- Se debe evitar derramar sobre la pintura productos químicos, disolventes o aguas procedentes de las jardineras o de la limpieza de otros elementos, así como la humedad que puede afectar las propiedades de la pintura.
- Se debe evitar los golpes y rozamientos.

- Se debe evitar la limpieza o contacto de la pintura con productos químicos o cáusticos capaces de alterar sus condiciones.
- En lo posible, se debe evitar colocar elementos, como chazos, que deterioren la pintura, por su difícil reposición.
- Si se observa la aparición de humedades sobre la superficie, se debe determinar lo antes posible el origen de dicha humedad, ya que su presencia deteriora el revestimiento.
- Se debe evitar el uso de materiales de corcho, madera, papel, textiles y sintéticos flexibles en baños, cocinas o locales con posible humedad y el roce de elementos duros sobre estas superficies.
- Existen en el mercado limpiadores diseñados específicamente para pinturas, que pueden ser una inversión inteligente para áreas de alto tráfico o cocinas, donde la grasa y otras sustancias pueden ser más difíciles de eliminar.
- Evitar el exceso de sol, esto ayudará a que haya variación de tonalidades en la pintura. Se recomienda utilizar cortinas o persianas para proteger las pinturas de la luz solar excesiva.
- Se deben alejar el mobiliario de las paredes ya que estos dejan marcas en las pinturas cuando están muy ceras.
- Para prevenir la aparición de moho, además de la ventilación, se recomienda considerar el uso de deshumidificadores en áreas propensas a la humedad. En caso de aparición de moho, se debe tratar la zona con productos antimoho antes de pintar para prevenir su reaparición.

PROFESIONAL CALIFICADO	FRECUENCIA
Anualmente o cuando se note el ennegrecimiento o desprendimiento de la pintura protectora, se procederá al repintado	Cada año

DAÑOS FRECUENTES	CAUSA DE DAÑOS
Ampollado	Humedad en la superficie, exposición a altas temperaturas
Amarillamiento	Envejecimiento de la pintura, en especial si es de esmalte. Exposición excesiva a los rayos del sol o, por el contrario, debido al nulo contacto con la luz
Arrugamiento	Pérdida de flexibilidad del recubrimiento por bajas temperaturas. Cambios bruscos de temperatura. Falta de preparación adecuada de la superficie.

Agrietamiento	Pérdida de flexibilidad del recubrimiento por bajas temperaturas. Cambios bruscos de temperatura. Falta de preparación adecuada de la superficie.
Cuarteamiento	Aplicación de recubrimiento demasiado rígido. Cambios bruscos de temperatura. Aplicación de pintura de esmalte directamente sobre pintura vinílica o recubrimiento sin que la capa inferior haya secado. Desgaste natural de un recubrimiento debido al paso del tiempo.
Baja resistencia a la alcalinidad.	Contacto con ambientes húmedos. Ausencia de sellador en una superficie altamente alcalina.
Burbujas y cráteres	Agitación excesiva de la pintura antes de aplicarla. Aplicación con un rodillo inadecuado. Aplicación de muchas manos de pintura en una misma superficie. Aplicación directa de pintura sobre una superficie muy porosa.
Craquelado y pelado	Inadecuada preparación de la superficie antes de pintar. Aplicación de una pintura de esmalte sobre una superficie húmeda. Aplicación de pintura excesivamente diluida. Falta de adherencia por presencia de contaminantes
Esgurrimiento	Aplicación de pintura en capas muy gruesas o lo contrario. Aplicación de pintura demasiado diluida. Aplicación con pistola a una distancia muy cercana de la superficie
Decoloración	Ataque excesivo de los rayos del sol y alcalinidad del medio ambiente. Uso de un color demasiado brillante que puede resultar vulnerable a los rayos del sol

Actividades de mantenimiento según tipo:

Mantenimientos Recurrentes:

- Mensualmente se debe realizar limpieza del polvo, se puede emplear un trapo de microfibra seco que atrape las partículas sin rayar la superficie. Si se presentan machas, optar por soluciones suaves; una

mezcla de agua con vinagre blanco puede ser efectiva para manchas difíciles sin dañar la pintura. Evitar el uso de esponjas abrasivas o cepillos duros.

- Trimestralmente se debe realizar la limpieza de la pintura con esponjas o trapos humedecidos con agua jabonosa.
- Anualmente se debe realizar la revisión del estado de conservación de la pintura.
- Anualmente se debe realizar la comprobación de la posible aparición de fisuras, desprendimientos, humedades y manchas.

Mantenimientos Correctivos:

- Antes de darle retoque de pintura a cualquier superficie hay que limpiarla y, en caso de ser necesario, resanarla.
- Si se observa algún daño en el revestimiento, no atribuible al uso, como falta de adherencia, porosidad importante, fisuras, manchas o humedades capilares, con riesgo de desprendimiento, se levantará la superficie afectada y se estudiará la causa por un técnico competente, que dictaminará su importancia y, en su caso, las reparaciones que deban efectuarse.
- Es conveniente supervisar aquellas áreas muy expuestas al agua de lluvia o que no reciben buena iluminación del sol; dondequiera que se detecten las manchas de moho en las paredes, se debe limpiar con un producto adecuado para eliminar este.
- Las reparaciones del revestimiento deberán realizarse con materiales análogos a los utilizados en el revestimiento original, manteniéndose siempre las juntas de contracción. Para evitar la aparición de parchados debidos a la diferente tonalidad de los colores, se debe picar el revestimiento.

7.4. REDES ELÉCTRICAS Y CONECTIVIDAD

7.4.1. INTERRUPTORES, TOMACORRIENTES, RED REGULADA, RED NORMAL, PUNTOS DE VOZ Y DATOS, ACOMETIDAS DE AIRE ACONDICIONADO Y LUMINARIAS.



Se realizó la instalación de puntos de iluminación, interruptores en cada oficina, red eléctrica regulada y no regulada para los puestos de trabajo, red de voz y datos mediante canaleta metálica en pared; con sus respectivos tomacorrientes y puertos para cables; se realizó el suministro de acometidas eléctricas para las

condensadoras y adicionalmente se realizó la del suministro e instalación de luminarias cuadradas tipo LED de 60 cm X 60 cm y luminarias tipo tortuga de emergencia.

Cuidados para el uso y limpieza

- Se recomienda no enchufar cualquier aparato en cualquier tomacorriente, esto debido a que cada aparato requiere una potencia distinta y cada tomacorriente está preparada para soportar una potencia máxima, si la potencia del aparato es superior a la que soporta el tomacorriente, puede quemarse la base del enchufe, la clavija o hasta la instalación.
- No se deben colocar lampara u otro elemento de iluminación directamente suspendidas del cable correspondiente a un punto de luz.
- Se debe comprobar la potencia de los dispositivos conectados para que no se vaya a sobre cargar la capacidad de la instalación.
- Se recomienda mantener los aparatos electrónicos desconectados si no se están usando para evitar sobre calentamientos.
- Se recomienda apagar las luminarias que no se esté usando, eso con el fin de mantener la vida útil por más tiempo ya que dichas luminarias tienen duración estimada de 30,000 horas.
- Se debe evitar el contacto de la humedad con la instalación o con los aparatos electrónicos.
- Se recomienda no manipular, modificar o reparar la instalación si no se cuenta con la respectiva capacitación o sin la supervisión de un técnico eléctrico calificado para ejecutar los trabajos.

Actividades de mantenimiento según tipo:

Mantenimientos Recurrentes:

- Mensualmente se debe revisar que en los tomacorrientes y áreas circundantes a los puntos de voz y datos o canaletas no se encuentra humedad.
- Mensualmente se debe verificar la sujeción de las canaletas a las paredes, si se evidencia que están sueltas, se recomienda realizar el ajuste respectivo con la herramienta adecuada.
- Trimestralmente se debe realizar la limpieza superficial con un paño seco o un poco húmedo de las canaletas, tomacorrientes y luminarias instaladas.
- Semestralmente se debe realizar revisión completa de los circuitos en especial verificando que la unión de los tomacorrientes con los cables se encuentra en buen estado, que no han cambiado de color.
- Semestralmente se debe verificar la sujeción de las luminarias, asegurándose de que no tienen un movimiento excesivo, si se siente movimiento, realizar el ajuste necesario para evitar que se caigan.

Mantenimientos Correctivos:

- En caso de ser necesario, cambiar los tomacorrientes si se encuentran derretidos alrededor, o si se encuentran de color oscuro.

- Con el paso del tiempo las luminarias cumplirán con su tiempo de vida útil. Pueden empezar a disminuir la intensidad o a parpadear, se recomienda realizar el cambio de la luminaria.
- En caso de evidenciar que al conectar algún artefacto eléctrico se genera un bajo, contactar a un técnico para que realice la correcta revisión y medición de los voltajes en el circuito y tome las correcciones necesarias.

7.4.2. TABLEROS ELÉCTRICOS



Se realizó la instalación de tableros eléctricos de sobre poner de 24 y 36 circuitos con su respectivo anclaje, herraje y totalizadores.

Cuidados para el uso y limpieza

- Se recomienda mantener el área alrededor de los tableros limpia y libre de materiales combustibles.
- No modificar la configuración de totalizadores o circuitos sin documentación ni autorización técnica.
- El acceso debe ser solo para personal calificado y protegido con elementos de seguridad apropiados.
- Asegurarse de que únicamente personal calificado opere o intervenga en el tablero, siguiendo siempre protocolos de seguridad eléctrica para evitar accidentes.
- Evitar la sobrecarga conectando solo los circuitos y equipos diseñados para cada espacio del tablero.

- El tablero debe permanecer cerrado y debidamente señalizado para restringir el acceso a personas no autorizadas.
- Desenergizar completamente el tablero antes de iniciar cualquier acción de limpieza o inspección.
- Utilizar brochas de cerdas suaves y aspiradora para retirar polvo del interior y exterior del gabinete.
- Emplear limpiadores dieléctricos, especialmente para los contactos eléctricos y pernos. No utilizar agua ni solventes inflamables en zonas internas.
- Verificar que no existan rastros de humedad, sustancias químicas o grasa que puedan generar cortocircuitos o corrosión.

Actividades de mantenimiento según tipo:

Mantenimiento Preventivo

- **Inspección visual:** Revisar el estado general, identificando daños, piezas flojas o signos de sobrecalentamiento.
- **Ajuste de conexiones:** Verificar el apriete de tornillería y terminales, empleando herramientas adecuadas y sin exceder el torque permitido para evitar dañar componentes.
- **Limpieza interna y externa:** Mantener libre de polvo y contaminantes el interior y exterior del tablero. Limpiar los contactos con productos dieléctricos no inflamables.
- **Verificación funcional:** Comprobar el estado del herraje, los interruptores automáticos y totalizador, operando cada componente para asegurar su correcto funcionamiento.
- **Chequeo de etiquetas y señalización:** Asegurar que toda la señalización de seguridad esté en su lugar y en buen estado.
- **Registro:** Documentar las acciones de mantenimiento e inspección efectuadas.

Mantenimiento Predictivo

- **Medición eléctrica:** Realizar mediciones de voltaje, corriente y resistencia de aislamiento, con los instrumentos calibrados, para anticipar posibles fallas.
- **Análisis termográfico:** Evaluar con cámara infrarroja para detectar posibles puntos calientes que indiquen conexiones defectuosas.

Mantenimiento Correctivo

- **Reemplazo de componentes:** Realizar el cambio inmediato de interruptores, fusibles o terminales que presenten daños o estén por debajo de la capacidad requerida.
- **Reparación de aislamientos:** Atender cualquier signo de daño en los aislantes de los cables y en el gabinete.
- **Corrección de desbalances:** Ajustar la distribución de cargas para evitar diferencias superiores al 10% entre fases

Mantenimientos Recurrentes:

TAREA	FRECUENCIA	OBSERVACIÓN
Limpieza interna y externa	Trimestral	Uso de aspiradora y brocha. No usar agua en la zona interna
Ajuste de conexiones	Trimestral	Verificar torque adecuado y estado de terminales
Medición eléctrica	Semestral	Voltaje, corriente y aislamiento
Verificación de etiquetas	Semestral	Reemplazar si están ilegibles.
Inspección y prueba de interruptores	Semestral	Operar todos los breakers para confirmar su correcto funcionamiento.
Reemplazo de piezas dañadas	Cuando se detecte	Inmediato ante daño o falla.
Retiro de corrosión/pintura	Anual o según requiera	Lijar zonas oxidadas y repintar con pintura apropiada.

7.4.3. RACKS



Se realizó el suministro e instalación de dos racks, uno ubicado en el cuarto técnico del piso cinco y otro ubicado en el cuarto técnico del piso seis.

Cuidados para el uso y limpieza

- Usar los racks solo para los fines para los que fueron diseñados: carga y almacenamiento. No sobrepasar la capacidad de carga indicada por el fabricante.
- Instalar los racks en interiores, protegidos de la intemperie; no han sido diseñados para resistir humedad, lluvia, viento o temperaturas extremas.
- No golpear la estructura ni modificar componentes del rack sin autorización técnica.
- Realizar limpieza regular para evitar acumulación de polvo, residuos o sustancias corrosivas. El polvo puede ocultar daños o dificultar la inspección.
- Utilizar aspiradoras antiestáticas y paños de microfibra secos o ligeramente humedecidos con productos no abrasivos.
- En racks para equipos electrónicos, apagar y desconectar todo antes de limpiar y reorganizar cables para favorecer la ventilación y evitar sobrecalentamientos.
- Evitar el uso de agua o productos líquidos cerca de partes eléctricas o componentes sensibles.
- Mantener cerrados los paneles y puertas para evitar el ingreso de polvo y manipulación no autorizada.
- Asegurarse de que todos los cables estén organizados y sujetos usando canaletas o cintas, evitando enredos y obstrucciones de ventilación.
- Desconectar equipos sensibles antes de manipular dentro del rack.

Actividades de mantenimiento según tipo:

Mantenimiento Preventivo

- Realizar una inspección visual mensual para identificar signos de polvo excesivo, humedad, corrosión, cables sueltos o mal distribuidos, tornillería floja y ventilación obstruida.
- Ajustar tornillos, pernos y anclajes, verificando que las estructuras se encuentren firmes y niveladas.
- Limpiar las superficies de los racks y sus componentes internos asegurando que no haya acumulación de suciedad o insectos.
- Revisar el correcto funcionamiento de ventiladores y sistemas de climatización o extracción si aplica.
- Etiquetar correctamente todo el cableado y puertos, verificando que las etiquetas estén visibles y legibles.
- Registrar cada acción preventiva en el historial de mantenimiento.

Mantenimiento Predictivo

- Cada 6 a 12 meses, efectuar una revisión de temperatura y humedad interna con sensores, vigilando los rangos seguros para los equipos.
- Usar cámaras termográficas para detectar posibles puntos de sobrecalentamiento provocados por ventilación deficiente o sobrecarga de equipos.
- Verificar el estado de los contactos eléctricos y sistemas de puesta a tierra.

Mantenimiento Correctivo

- Reemplazar o reparar componentes defectuosos como ventiladores, tornillería, bases o paneles dañados de inmediato tras una falla.
- Atender cortocircuitos, desbalanceos, deformaciones estructurales o corrosión avanzada apenas se detecten.
- Sustituir etiquetas ilegibles y reorganizar cableado si presenta obstrucciones o riesgo de daño.
- Documentar la causa, la intervención realizada y las acciones correctivas adoptadas.

Mantenimientos Recurrentes:

TAREA	FRECUENCIA	OBSERVACIÓN
Limpieza superficial	Mensual	Evitar líquidos cerca de equipos energizados.
Inspección visual general	Mensual	Comprobar integridad del rack, cableado y ventilación
Ajuste de pernos y tornillos	Trimestral	Verificar que no existan partes flojas o desplazadas.
Etiquetado y organización de cables	Trimestral	Reetiquetar y reordenar si es necesario.
Inspección de temperatura y humedad	Semestral	Utilizar instrumentación adecuada.
Mantenimiento correctivo de fallas	Cuando se detecte	Reparar/reemplazar partes dañadas al detectar un problema.

7.4.4. UPS



Se realizó el suministro e instalación de dos UPS de 20 kVA, una ubicada en el cuarto técnico del piso cinco y otra ubicada en el cuarto técnico del piso seis.

Cuidados para el uso y limpieza

- Instalar la UPS en un ambiente limpio, seco y bien ventilado, evitando la luz solar directa, vibraciones, polvo, humedad y gases corrosivos. La temperatura operativa ideal está entre 20°C y 25°C, sin exceder los 40°C.
- No ubicar objetos sobre la UPS ni cubrir las salidas de ventilación.
- Solo personal capacitado debe operar, instalar o intervenir la UPS.
- Nunca sobrecargar el equipo; respeta la capacidad máxima en kVA indicada por el fabricante.
- No conectar dispositivos que generen picos de corriente elevados (taladros, motores), ni equipos cuya falla pueda poner en riesgo vidas (equipos médicos, elevadores).
- Desconectar la UPS y asegurarse de que no hay tensión antes de limpiar.

- Usar un paño suave, seco o ligeramente humedecido para limpiar el exterior. No utilices líquidos, aerosoles, ni agua directamente sobre el equipo. Eliminar el polvo de rejillas y ventiladores con brocha suave o aspiradora antiestática.
- Si no cuenta con conocimientos técnicos, evitar abrir la UPS para limpiar internamente; esta labor debe ser realizada por un profesional.

Actividades de mantenimiento según tipo:

Mantenimiento Preventivo

- Revisión visual de la integridad exterior e interior del equipo: busca acumulación de polvo, presencia de cables o conexiones sueltas, corrosión, deformaciones, señales de sobrecalentamiento o ruidos anormales.
- Limpieza de ventiladores, rejillas y superficie exterior.
- Medición de parámetros eléctricos (voltaje, corriente) y verificación de indicadores y alarmas del panel LCD.
- Comprobación del estado de las baterías: realiza pruebas de carga y descarga, revisa voltaje y corriente de cada batería, asegúrate de que estén bien sujetas y libres de corrosión en los terminales.
- Ajuste y reapriete de todos los bornes, cables y conexiones eléctricas.
- Chequeo del firmware y actualizaciones si aplica.
- Calibración y prueba periódica de los sistemas de monitoreo

Mantenimiento Predictivo

- Medición y monitoreo de temperatura y humedad interna con sensores. Usa cámaras termográficas para identificar “puntos calientes” o zonas de sobrecalentamiento¹⁶.
- Revisión con software especializado del “estado de salud” de la UPS y las baterías, para anticipar fallas.
- Análisis del historial de alarmas y eventos registrados.

Mantenimiento Correctivo

- Sustitución inmediata de módulos defectuosos: baterías, ventiladores, placas electrónicas, inversores o contactores.
- Reparación de cortocircuitos, falsas conexiones, daños estructurales o corrosión avanzada.
- Reemplazo o reubicar etiquetas y señalización deterioradas.
- Documentar cada intervención y detallar piezas cambiadas, causa del fallo y acciones realizadas

Mantenimientos Recurrentes:

TAREA	FRECUENCIA	OBSERVACIÓN
Limpieza externa (pañó seco)	Mensual	Desenergizar antes. No usar líquidos.

Inspección general visual	Mensual	Verificar alarmas, indicadores, conexiones, ventiladores y presencia de polvo
Prueba de baterías	Trimestral	Cargar/descargar y medir voltaje y corriente por batería.
Ajuste de bornes y conexiones	Trimestral	Revisar torque y eliminar conexiones flojas
Revisión y limpieza de ventiladores y filtros	Trimestral	Limpiar y reemplazar según el fabricante.
Medición de parámetros eléctricos y temp/humedad	Semestral	Utilizar instrumentos de medición adecuados
Actualización de firmware	Anual	Según indicaciones de fabricante
Reemplazo de baterías	Cada 3-5 años	O antes si se detecta pérdida de capacidad
Cambio de ventiladores	Cada 5 años	Según vida útil estimada
Mantenimiento correctivo	Inmediato	Reparar o sustituir componentes dañados tras detectar fallas

Recomendaciones adicionales

- Utilizar solo repuestos originales recomendados por el fabricante.
- Mantener el área alrededor de la UPS libre de materiales combustibles y asegurada contra personal no autorizado.
- Programar el mantenimiento preventivo en horarios que no afecten la continuidad operativa de los sistemas protegidos.
- Consultar siempre el manual específico de tu modelo para particularidades de configuración y operación

Adicionalmente, se recomienda revisar el manual del usuario expedido por el fabricante anexo al presente manual de mantenimiento.

7.4.5. SWITCHES ARUBA DE 24 PUERTOS



Se realizó el suministro e instalación de tres Switches marca ARUBA de 24 puertos en el Rack ubicado en el cuarto técnico del piso cinco y cuatro Switches marca ARUBA de 24 puertos en el Rack ubicado en el cuarto técnico del piso seis.

Cuidados para el uso y limpieza

- Instalar el switch en un ambiente limpio y ventilado, evitando exposición directa al sol, humedad excesiva, polvo y fuentes de calor.
- Solo debe ser manipulado por personal capacitado para evitar configuraciones incorrectas o daños.
- Asegurar una correcta conexión a tierra y utilizar siempre el cable de alimentación suministrado por el fabricante.
- Evitar sobrecargar los circuitos de energía y los puertos de red
- Antes de limpiar, apagar y desconectar el switch de la corriente eléctrica.
- Limpiar el exterior con un paño suave, seco o ligeramente humedecido. No aplicar agua ni productos corrosivos sobre la superficie.
- Usar brocha suave o aspiradora antiestática para las rejillas de ventilación y retiro de polvo en los puertos.
- No abrir el equipo para limpieza interna a menos que sea personal técnico autorizado; la limpieza interna rutinaria no es requerida

Actividades de mantenimiento según tipo:

Mantenimiento Preventivo

- **Inspección visual mensual:** verificar que no haya daños exteriores, conexiones flojas o acumulación excesiva de polvo.
- **Limpieza externa mensual:** limpiar las superficies y ventilaciones siguiendo las recomendaciones anteriores.
- **Verificación de ventiladores y disipación:** asegurar de que nada obstruya la ventilación.
- **Chequeo funcional:** revisar los indicadores LED, alarmas y funcionamiento general del equipo.
- **Actualización de firmware:** revisar periódicamente si hay actualizaciones del sistema operativo del switch, aplicándolas según las indicaciones del fabricante para mantener la seguridad y el desempeño óptima

Mantenimiento Predictivo

- **Supervisión de temperatura y humedad:** cada 6 a 12 meses, medir condiciones ambientales alrededor del switch. Usar sensores o monitoreo remoto si está disponible.
- **Monitorización proactiva:** utilizar las herramientas de diagnóstico y monitoreo incluidas en la consola web o software Aruba Instant On para detectar anomalías antes de que causen fallas

Mantenimiento Correctivo

- **Intervención inmediata:** en caso de falla de algún puerto, daño en la fuente de poder, ventilador o componentes, reemplazar únicamente con repuestos originales.
- **Reparaciones estructurales:** atender daños en carcasa, soporte o sistemas de anclaje al detectarlos.
- **Firmware corrupto:** ante fallo de arranque, reinstalar el firmware siguiendo la guía oficial del modelo.
- **Registro:** documentar cada intervención y su causa para seguimiento

Mantenimientos Recurrentes:

TAREA	FRECUENCIA	OBSERVACIÓN
Limpieza externa (pañó seco)	Mensual	Evitar líquidos, solo paño seco o ligeramente húmedo
Inspección visual	Mensual	Revisar conexiones, ventilación y estado físico
Verificación funcional y LEDs	Mensual	Chequear alarmas, funcionamiento y conectividad.
Ajuste de conexiones	Trimestral	Reapretar si es necesario (solo técnicos autorizados)
Actualización de firmware	Semestral	Según notificaciones o revisiones del fabricante
Mantenimiento correctivo (reemplazo de piezas)	Inmediato	Realizar ante cualquier falla detectada

7.5. MUROS EN DRYWALL



Se realizó el levantamiento de muros en DryWall con un espesor de 12 cm, con su respectiva estructura metálica y aislamiento acústico y térmico interno. Se levantaron muros en los pisos cinco y seis con el fin de realizar la nueva distribución arquitectónica.

Cuidados para el uso y limpieza

- **Prevención de Humedad:** Es fundamental evitar fuentes de humedad, ya que el agua puede generar moho, afectar la integridad de las placas y dañar el aislamiento Frescasa. Es responsabilidad de los usuarios identificar y corregir posibles filtraciones o condensaciones en los espacios donde existan estos muros.

- **Carga y Fijaciones:** Los ocupantes o responsables de mantenimiento no deben colgar objetos pesados directamente sobre los muros de DryWall, a menos que utilicen anclajes especialmente diseñados para este tipo de material. El uso inadecuado de fijaciones puede causar fisuras, abolladuras o desprendimientos.
- **Protección contra Golpes:** Es importante manipular muebles y otros objetos con cuidado en las proximidades del muro.
- **Temperatura:** Se debe procurar mantener una temperatura ambiental estable y evitar cambios bruscos, ya que estos pueden afectar tanto las placas de yeso como el aislamiento.
- La limpieza debe realizarse con un paño suave o esponja ligeramente humedecida con agua. Los productos químicos abrasivos o el exceso de agua están prohibidos.
- Para eliminar el polvo, puede utilizarse una aspiradora de mano antiestática o brochas suaves, especialmente en esquinas y zonas de perfilería.
- Si existe una mancha difícil, se puede utilizar detergente suave diluido, asegurando el secado inmediato de la superficie después del procedimiento.
- El aislamiento Frescasa, una vez instalado detrás del muro, no requiere limpieza directa. Solamente debe verificarse su integridad en inspecciones periódicas o cuando se realicen reparaciones en el muro.

Actividades de mantenimiento según tipo:

Mantenimiento Preventivo

- Se aconseja realizar inspecciones visuales mensuales para detectar signos de humedad, grietas, golpes, daño en juntas o presencia de insectos y plagas.
- Es indispensable revisar periódicamente el estado de las juntas, sellos y esquinas. Si se detectan separaciones, se deben reaplicar masilla, cinta y pintura adecuada.
- Deben revisarse los anclajes y tornillos para asegurar que no existan elementos flojos.
- Un repintado periódico con pintura antihumedad permite proteger el muro y facilitar posteriores limpiezas.

Mantenimiento Predictivo

- Cada 6 a 12 meses, se recomienda controlar temperatura y humedad ambiental mediante sensores, anticipando problemas derivados de condiciones inadecuadas.
- Cuando se realicen intervenciones, el personal de mantenimiento debe verificar que el aislamiento Frescasa esté seco, sin señales de daño ni moho, y correctamente posicionado.

Mantenimiento Correctivo

- Si se presentan grietas o abolladuras, el equipo de mantenimiento debe rellenar con masilla específica para DryWall, lijar y pintar nuevamente. En daños mayores, se procederá al reemplazo del paño de yeso, comprobando el estado del aislamiento.

- Ante la identificación de aislamiento Frescasa mojado o dañado, será necesario su reemplazo, asegurando antes la corrección de la causa de humedad.
- Cualquier desprendimiento o deformación importante debe ser revisado y reparado, incluyendo ajuste de perfilería, repuesto de anclajes y, en casos severos, intervención de personal especializado.

Mantenimientos Recurrentes

TAREA	FRECUENCIA	OBSERVACIÓN
Limpieza superficial de muros	Mensual	Evitar abundante humedad; utilizar solamente paño suave
Inspección visual general	Mensual	Revisar fisuras, juntas, esquinas, pintura y efectos de humedad
Revisión y sellado de juntas	Cada 2 o 3 años	Utilizar pinturas antihumedad y masilla conforme especificación.
Verificación del aislamiento y sellos	Semestral	Comprobar sellado, sequedad e integridad del aislamiento
Reparación de daños menores	Inmediato	Masilla, lijado y repintado según requerimiento
Sustitución de paneles o aislamiento dañados	Inmediato	Frente a daño grave, filtraciones o humedad

Recomendaciones adicionales

- Mantener libres de humedad y fuentes de impacto las áreas adyacentes a los muros.
- Consultar siempre los instructivos del fabricante para el aislamiento Frescasa y los paneles de yeso utilizados.
- Hay que recordar que una instalación correcta y un mantenimiento periódico alargan la vida útil de la solución y preservan su funcionalidad térmica, acústica y estética.

7.6. REVESTIMIENTOS DE PISOS Y PAREDES DE BAÑO EN TABLETA CERÁMICA





Se realizó la instalación de revestimiento de pisos en cerámica con formato de 60 cm X 60 cm en las oficinas y corredores del piso cinco y piso seis, adicionalmente se instaló cerámica en el baño de hombres del piso cinco con revestimiento en las paredes en formato de 60 cm X 30 cm.

Cuidados para el uso y limpieza

- **Prevención de Daños y Desgaste:** Se recomienda colocar tapetes atrapa polvo en accesos para prevenir el ingreso de partículas abrasivas que puedan rayar el esmalte cerámico. Es importante evitar arrastrar muebles o elementos pesados directamente sobre la superficie; deben utilizarse protectores en las patas del mobiliario para prevenir rayones y fisuras.
- **Evitar la Exposición a Humedad Prolongada:** En el caso de las paredes y juntas, se aconseja secar de inmediato cualquier filtración o salpicadura para evitar deterioro en las boquillas y posibles desprendimientos. El exceso de agua puede infiltrarse en las juntas y debilitar el adhesivo.
- **Cuidados con Productos Químicos:** No deben usarse limpiadores ácidos, cloro, amoníaco, productos abrasivos ni detergentes en polvo, ya que estos pueden dañar el esmalte, afectar el color y debilitar las juntas. Solo se aplicarán productos de limpieza neutros y suaves, leyendo siempre las instrucciones de uso.
- Se debe barrer o aspirar la superficie para remover el polvo y residuos antes de trapear.

- Para limpieza diaria, basta un trapeador o paño suave humedecido en agua tibia y jabón neutro. Nunca se recomienda usar esponjas metálicas ni cepillos duros; en las juntas puede emplearse un cepillo de dientes suave.
- Ante manchas difíciles, debe prepararse una mezcla de agua y detergente suave o, en casos especiales, vinagre blanco diluido, realizando siempre una prueba en una zona poco visible antes de limpiar toda la superficie. Luego, enjuagar con agua limpia y secar con un paño.
- Luego de limpiar, se aconseja secar la superficie para evitar marcas de agua y darle brillo al acabado cerámico.
- El guarda escobas requiere el mismo tratamiento y debe mantenerse libre de suciedad acumulada en el borde, utilizando paños suaves o esponjas no abrasivas.

Actividades de mantenimiento según tipo:

Mantenimiento Preventivo

- **Inspección Visual Mensual:** El responsable debe revisar la superficie en busca de manchas, grietas, juntas deterioradas, levantamiento de boquillas o cerámicos sueltos, así como verificar la integridad del guarda escobas.
- **Limpieza Recurrente:** Se aconseja limpiar pisos y paredes al menos una vez por semana o según el nivel de uso, poniendo énfasis en retirar la suciedad de las juntas y los bordes.
- **Protección de Juntas:** Revisar que las juntas estén completas y no presenten desprendimientos, rellenando si es necesario para impedir filtraciones futuras.
- **Control de Humedad:** Identificar y corregir cualquier foco de humedad en muros o pisos, especialmente cerca de paredes externas o áreas húmedas.

Mantenimiento Predictivo

- **Inspección de Grietas y Juntas (Anual o Semestral):** Revisar de manera más exhaustiva el estado de las juntas de dilatación, rellenando o sellando las que presenten caída o desgaste considerable.
- **Revisión de Sonidos Huecos:** Evaluar periódicamente la existencia de losas "falsas" o con sonido hueco, lo que puede indicar desprendimiento. Ante hallazgos, debe planificarse el reemplazo de la pieza sospechosa.

Mantenimiento Correctivo

- **Reparación o Reemplazo de Cerámicos:** Ante fisuras, desprendimientos o daños evidentes, se debe retirar la pieza afectada y sustituirla por una pieza de reserva, asegurando una correcta aplicación del adhesivo y boquilla.
- **Sellado o Restauración de Juntas Dañadas:** Las juntas deterioradas deben eliminarse totalmente y reaplicarse con material adecuado; en ambientes húmedos, es preferible el uso de boquillas epóxicas.

- **Corrección de Deformaciones en Guarda Escobas:** Si el guarda escobas cerámico se afloja o se desprende, debe ser removido y adherido nuevamente con mortero o adhesivo específico.
- **Intervención Inmediata en Caso de Manchas Persistentes:** Ante manchas imposibles de remover con productos suaves, se recomienda consultar a un profesional para evitar daños mayores en la superficie cerámica.

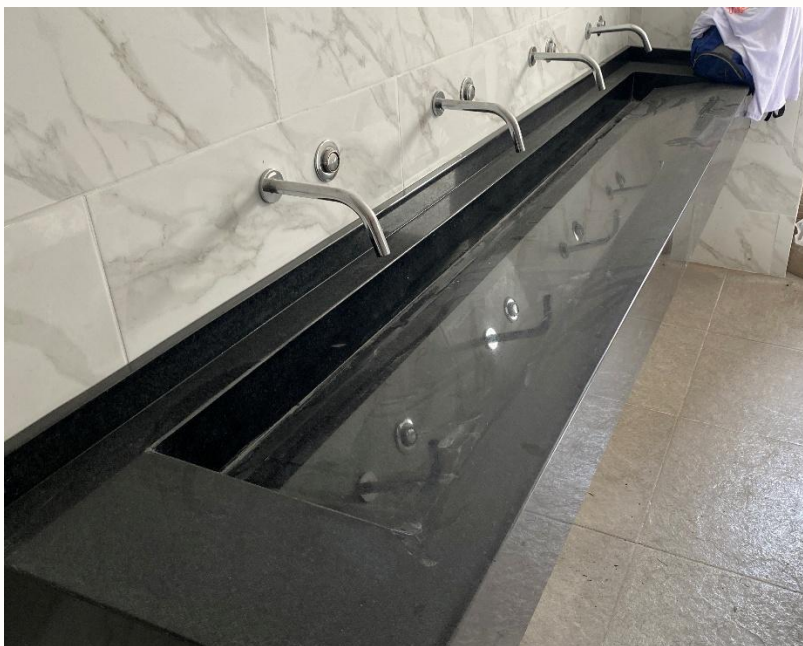
Mantenimientos Recurrentes

TAREA	FRECUENCIA	OBSERVACIÓN
Limpieza superficial (barrer, trapear, limpiar guarda escobas)	Diaria, Semanal o según uso	Evitar exceso de agua y aplicar solo productos neutros
Inspección visual general de superficies y juntas	Mensual	Revisar grietas, juntas, bordes de guarda escobas y manchas visible
Revisión y reparación/restauración de boquillas/juntas	Semestral o Anual	Rellenar juntas y sellar si es necesario
Reparación de cerámicos o guarda escobas dañados	Inmediato I	Sustituir piezas dañadas o sueltas

Recomendaciones adicionales

- Mantener el área protegida de fuentes de humedad y de impactos mecánicos.
- Consultar instrucciones del fabricante tanto para cerámicos como para adhesivos, boquillas y guarda escobas.
- Un uso responsable, limpieza periódica y mantenimiento planificado aseguran la durabilidad, el brillo y la funcionalidad de los enchapes cerámicos en pisos y paredes.

7.7. MESÓN LAVAMANOS EN GRANITO SAN GABRIEL



Se realizó la instalación de un mesón lavamanos en granito san Gabriel en el baño de hombres del piso cinco.

Cuidados para el uso y limpieza

- Se debe evitar apoyar objetos calientes directamente sobre el mesón, así como golpear su superficie con elementos pesados o punzantes.
- Es recomendable no utilizar el mesón como superficie de corte ni exponerlo a productos ácidos o corrosivos (blanqueadores, vinagre, limpiadores de cañerías o desengrasantes fuertes).
- Deben limpiarse de inmediato derrames de tintes, jabones, cosméticos o productos químicos para evitar manchas, ya que, aunque el granito es altamente resistente, puede absorber líquidos si no está adecuadamente sellado.
- Para prolongar el brillo, se sugiere utilizar bajo cada accesorio o elemento de uso frecuente (jaboneras, portacepillos, etc.) bases de goma o fieltro.
- No arrastrar objetos metálicos o cerámicos sobre la superficie.
- Evitar la acumulación de agua en las uniones o alrededor del lavamanos para prevenir marcas de cal o residuos blanquecinos.
- La superficie debe limpiarse diariamente con un paño suave o esponja no abrasiva y agua tibia, eliminando residuos de jabón y salpicaduras.

- Semanalmente, puede emplearse un detergente neutro diluido y enjuagar completamente para evitar la formación de películas opacas.
- Queda prohibido el uso de limpiadores ácidos, cloro, amoníaco, desengrasantes fuertes o productos abrasivos como polvos y esponjas de metal.
- Para preservar el brillo, después de limpiar y secar, se recomienda pulir suavemente con un paño seco de microfibra.

Actividades de mantenimiento según tipo:

Mantenimiento Preventivo

- **Sellado del Granito:** El mesón de granito requiere un sellado profesional inicial y su re-aplicación como mínimo una vez al año, dependiendo del nivel de uso y el tipo de sellador empleado, a fin de mantener su resistencia a las manchas y facilitar la limpieza.
- **Inspección Visual:** Cada tres meses se debe revisar si existen manchas, rayones, áreas opacas o pérdida de sellado (el agua no debe absorberse, sino formar gotas).
- **Limpieza Profunda:** Trimestralmente debe realizarse una limpieza profunda con un producto específico para granito, autorizado por el fabricante o proveedor.

Mantenimiento Predictivo

- **Detección Temprana de Problemas:** Semestralmente, el responsable debe verificar uniones, sellos de silicona y compatibilidad de accesorios, anticipando posibles filtraciones de agua o desprendimientos por desgaste del sellador.

Mantenimiento Correctivo

- **Restauración de Brillo:** Ante pérdida de brillo o aparición de áreas opacas, se podrá realizar un pulido profesional del granito utilizando discos y cremas específicas.
- **Eliminación de Manchas:** Las manchas que no salgan con el método de limpieza habitual pueden requerir el uso de una pasta especial para granito; se recomienda consultar al proveedor o a un especialista para evitar daños irreparables.
- **Reparación de Daños Estructurales:** Si se produce una fisura, desportillado o desprendimiento, es imprescindible contactar a un profesional para su restauración.

Mantenimientos Recurrentes

TAREA	FRECUENCIA	OBSERVACIÓN
Limpieza superficial	Diaria, Semanal o según uso	Usar paño suave, detergente neutro y secar completamente
Limpieza profunda con producto para granito	Trimestral	No aplicar sustancias abrasivas o ácidas

Revisión visual de sellado y superficie	Trimestral	Comprobar formación de gotas, ausencia de absorción
Sellado del granito	Anual o según uso	Usar solo selladores recomendados para granito
Reparación de daños o manchas persistentes	Inmediato	Acudir a especialistas si no se eliminan con técnicas básicas

Recomendaciones adicionales

- Mantener el área del lavamanos seca y ventilada cuando no esté en uso para evitar acumulación de humedad.
- Un uso responsable y el cumplimiento del plan de mantenimientos garantizarán la durabilidad, estética y funcionalidad del mesón en granito San Gabriel.

7.8. SANITARIOS Y ORINALES



Se realizó el suministro e instalación de cuatro sanitarios y tres orinales ubicados en el baño de hombres del piso cinco.

Cuidados para el uso y limpieza

- **Correcto Uso y Prevención de Daños:** Se recomienda que los usuarios hagan uso adecuado de los orinales y sanitarios evitando arrojar objetos sólidos, papeles no solubles, productos químicos no autorizados o basura en los mismos, ya que puede ocasionar obstrucciones y daños en el sistema hidráulico. Debe verificarse que los equipos estén bien fijados al piso o muro, evitando movimientos que puedan provocar fisuras o desprendimientos.
- **Evitar Golpes y Maltrato:** No deben apoyarse objetos pesados sobre la tapa o estructura de los sanitarios. Los golpes pueden fracturar la cerámica y poner en riesgo a los usuarios.

- **Cuidados con Agua y Productos:** Nunca se debe permitir el estancamiento prolongado de agua en el interior del sanitario u orinal, ya que esto favorece la formación de sarro y manchas persistentes.
- La limpieza debe realizarse con productos compatibles para cerámica o porcelana: detergentes neutros, desinfectantes suaves y paños o cepillos de cerdas plásticas. No se recomienda el uso de cepillos metálicos, productos abrasivos o cloro concentrado, pues pueden dañar brillantina y esmaltes.
- Es necesario limpiar diariamente el interior y exterior de orinales y sanitarios, haciendo énfasis en zonas propensas a acumulación de calcio o suciedad (bajo la tapa, borde, sifón).
- En caso de presencia de sarro, se debe aplicar productos desincrustantes específicos, siguiendo las instrucciones del fabricante.
- Deben limpiarse periódicamente los dispositivos de descarga (botón, manija, válvula), eliminando residuos que puedan dificultar el funcionamiento.

Actividades de mantenimiento según tipo:

Mantenimiento Preventivo

- **Inspección Visual Semanal:** El responsable debe revisar el estado físico general de la porcelana, tapas, fijaciones, válvulas y verificar la ausencia de fugas, manchas de sarro u obstrucciones.
- **Chequeo de Fugas y Funcionamiento:** Deben inspeccionarse semanalmente las uniones, mangueras y sistemas de descarga, asegurando que no existen fugas de agua ni pérdidas por válvulas.
- **Ajuste de Fijaciones:** Trimestralmente, se revisará que los pernos y tornillos estén firmemente anclados, sin movimiento o juego excesivo.
- **Limpieza Profunda Programada:** Puede programarse una limpieza intensiva mensual con desincrustantes seguros y desinfectantes para prevenir incrustaciones y malos olores.
- **Capacitación Bimestral:** El personal de limpieza debe recibir instrucciones periódicas para garantizar técnicas y productos apropiados, minimizando los daños por mal uso.

Mantenimiento Predictivo

- **Revisión Interna de Mecanismos:** Semestralmente, los mecanismos internos de descarga (flappers, válvulas, tubos de rebose) deben inspeccionarse y probarse para anticipar fallas por desgaste.
- **Monitoreo de Presión y Caudales:** Anualmente, puede verificarse que la presión hidráulica y los caudales sean los óptimos y que no existan taponamientos parciales en las líneas.

Mantenimiento Correctivo

- **Desobstrucción de Tuberías:** Al detectar taponamientos, deben emplearse sopladores, limpiadores profesionales y solo en casos controlados, productos químicos autorizados.
- **Reemplazo Inmediato de Piezas Dañadas:** Si se identifican fisuras, fugas, válvulas defectuosas o accesorios rotos, deben ser reemplazados inmediatamente por repuestos originales.

- **Corrección de Fugas:** Ante cualquier fuga, se debe aislar el sanitario u orinal, efectuar la reparación de sellos, empaques, mangueras o conexiones.
- **Recuperación de Brillo y Reparación de Manchas:** Ante pérdidas de brillo o manchas resistentes, debe consultarse a un proveedor especializado para tratamiento superficial acorde a la cerámica instalada.

Mantenimientos Recurrentes

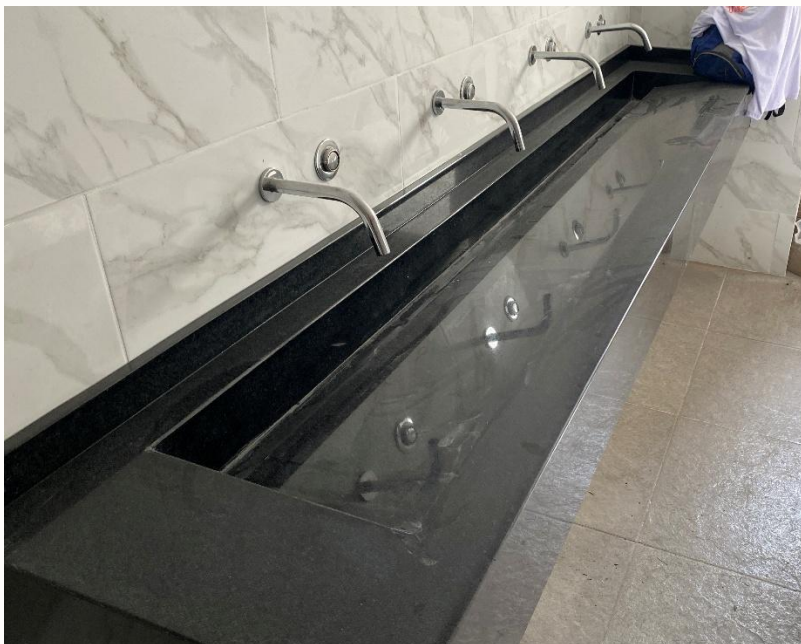
TAREA	FRECUENCIA	OBSERVACIÓN
Limpieza superficial y desinfección	Diaria	Uso de detergentes neutros y desinfectantes suaves
Inspección visual de sanitarios y orinales	Semanal	Revisar fijaciones, fugas, tapa, mecanismos de descarga
Limpieza profunda/desincrustante	Mensual	Aplicar productos específicos bajo supervisión
Chequeo y ajuste de válvulas y conexiones	Trimestral	Ajustar o cambiar tornillos, verificar presión de descarga
Inspección y prueba de mecanismos internos	Semestral	Reemplazo preventivo si se identifica desgaste
Reemplazo/repación de piezas, desobstrucciones	Inmediato	Atender taponamientos, fugas o daño estructural

Recomendaciones adicionales

- Mantener el área de acceso libre de obstáculos y fuentes de humedad prolongada.
- Consultar siempre los instructivos de cada fabricante tanto para sanitarios, orinales como para accesorios de limpieza recomendados.
- Un uso responsable, limpieza periódica y mantenimiento planificado asegurarán la higiene, funcionalidad y vida útil de los orinales y sanitarios.

Se anexan los manuales del fabricante

7.9. GRIFERÍA ANTIVANDÁLICA PARA LAVAMANOS



Se realizó el suministro e instalación de cuatro griferías antivandálicas para lavamanos ubicadas en el baño de hombre del piso cinco.

Cuidados para el uso y limpieza

- No se debe ejercer fuerza excesiva sobre la grifería ni intentar desmontar partes externas, pues estas están diseñadas para resistir impactos y manipulación indebida, pero no está garantizada su resistencia ante actos de vandalismo extremos.
- Es fundamental no arrojar agentes químicos, grasas, pinturas o residuos sólidos sobre el grifo, para prevenir obstrucciones o desgaste prematuro.
- La limpieza debe realizarse con un paño suave y productos de limpieza neutros y no abrasivos.
- No se deben emplear esponjas metálicas, productos ácidos, cloro concentrado, amoníaco ni limpiadores a vapor sobre la grifería.
- Es recomendable secar la grifería luego de la limpieza y tras su uso, especialmente en lugares con agua dura, para evitar la formación de manchas de cal y residuos minerales.
- Periódicamente, se debe desenroscar y limpiar el aireador o filtro ubicado en la base del pico de la grifería para eliminar acumulaciones de sedimentos.
- Durante la limpieza de paredes o lavamanos, se aconseja cubrir la grifería para evitar el contacto con agentes abrasivos o salpicaduras de productos fuertes.

Actividades de mantenimiento según tipo:

Mantenimiento Preventivo

- **Inspección Visual Semanal:** El responsable debe revisar el estado físico general de la porcelana, tapas, fijaciones, válvulas y verificar la ausencia de fugas, manchas de sarro u obstrucciones
- **Inspección Visual Mensual:** Cada mes, el responsable debe revisar la grifería para detectar fugas, goteos, movimiento anormal, daños en acabados o funcionamiento deficiente del mecanismo de cierre automático.
- **Limpieza Regular:** El mantenimiento incluye limpieza semanal o quincenal, según el nivel de uso, con productos y técnicas adecuados.
- **Chequeo de Fijaciones:** Trimestralmente deben revisarse los tornillos y anclajes internos para garantizar que la grifería esté firmemente sujeta y evitar movimientos que puedan facilitar daños o fugas.
- **Limpieza de Aireador y Filtros:** Desenroscar periódicamente (cada 3 meses o antes si el agua es muy dura) el aireador para eliminar incrustaciones de cal y residuos, asegurando así un flujo constante de agua sin obstrucciones.
- **Comprobación del Consumo y Funcionamiento:** Verificar de manera funcional que el cierre automático temporizado opera en el rango recomendado y que el caudal es el adecuado según ficha técnica del fabricante

Mantenimiento Predictivo

- **Control de Presión de Agua:** Semestralmente se recomienda revisar la presión del agua, asegurándose de que se encuentra dentro del rango operativo especificado (usualmente, entre 20–80 psi).
- **Inspección Interna del Mecanismo:** Durante revisiones programadas, el técnico debe desmontar el cuerpo controlador (solo personal capacitado) para lubricación y verificación de componentes internos, sellos y juntas.

Mantenimiento Correctivo

- **Reparación Inmediata de Fugas:** Ante cualquier fuga, se debe aislar la grifería, reemplazar empaques, o-rings o válvulas dañadas y ajustar conexiones internas sin demora.
- **Sustitución de Componentes:** En caso de fallas de cierre, daño por vandalismo, pérdida de acabado o desgaste excesivo, se deben reponer las partes afectadas solo con repuestos originales del fabricante.
- **Desobstrucción:** Ante obstrucciones en el flujo de agua, retirar y limpiar aireadores, filtros e inspeccionar internamente para eliminar posibles residuos.

- **Reparación o Reinstalación:** Si la grifería presenta movimientos o aflojamientos, se debe ajustar o reinstalar siguiendo las guías técnicas y asegurando la solidez de la fijación.
-

Mantenimientos Recurrentes

TAREA	FRECUENCIA	OBSERVACIÓN
Limpeza superficial y secado	Semanal/Quincenal	Usar paño suave y detergente neutro, evitar productos abrasivos
Inspección visual y fijaciones	Mensual	Revisar funcionamiento, fugas, anclajes y acabados
Limpeza de aireador/filtro	Trimestral	Eliminar incrustaciones y sedimentos, especialmente en zonas de agua dura
Lubricación y revisión de mecanismo interno	Semestral	Siempre por técnico capacitado, sin manipular sellos si no es necesario
Reparación de fugas o reemplazo de piezas	Inmediato	Ante cualquier fuga, daño de mecanismos o golpes

Recomendaciones adicionales

- El mantenimiento preventivo periódico es esencial para prolongar la vida útil y asegurar la higiene en zonas de alto tráfico.
- Ante dudas sobre la integridad o funcionamiento, no realizar intervenciones improvisadas y consultar a técnicos certificados o al proveedor.

Para información adicional, revisar la ficha técnica del proveedor, se anexa en el presente manual.

7.10. VENTANERÍA EN ALUMINIO



Se realizó el suministro e instalación de ventanería en aluminio con vidrio de seguridad, fue ubicada en la parte posterior de cada una de las oficinas del piso cinco y piso seis.

Cuidados para el uso y limpieza

- **Uso Responsable y Prevención de Daños:** Se debe evitar ejercer fuerza excesiva sobre las ventanas, golpear o apoyar objetos pesados sobre el vidrio o perfiles, así como manipular el sistema de apertura de forma brusca. No es recomendable colgar objetos ni alterar los sistemas de cierre o seguridad. El vidrio de seguridad, aunque es resistente, puede fracturarse ante impactos o apoyos inapropiados; por ello, conviene recordar que su resistencia depende del tipo de instalación y accesorios usados.
- **Superficies de Vidrio:** El vidrio de seguridad debe limpiarse regularmente con un paño suave humedecido en agua o con un detergente neutro y no abrasivo. Después de la limpieza, conviene secar de inmediato la superficie con otra tela seca para evitar marcas de agua o jabón. No deben emplearse productos ni materiales abrasivos (cepillos metálicos, estropajos, papel), ni productos que contengan amoníaco, blanqueadores, ácidos, ceras, alcohol o solventes, pues pueden atacar el vidrio y los perfiles de aluminio.
- **Perfiles de Aluminio:** Los perfiles deben limpiarse con agua y jabón neutro. Se recomienda emplear un paño suave o esponja para evitar rayaduras. Los restos de cemento, silicona u otros materiales deben ser removidos con productos compatibles, nunca con herramientas filosas ni disolventes fuertes.
- **Juntas y Herrajes:** Limpiar las juntas de goma o silicona con un trapo húmedo y jabón neutro. No usar disolventes ni químicos agresivos. En el caso de herrajes o bisagras, retirar el polvo y aplicar lubricante específico una o dos veces al año para prolongar la vida útil y mantener el buen funcionamiento.
-

Actividades de mantenimiento según tipo:

Mantenimiento Preventivo

- Realizar una limpieza general de vidrios y perfiles al menos cada tres meses, y con mayor frecuencia en ambientes expuestos a polvo, humedad o contaminación.
- Inspeccionar visualmente cada tres o seis meses el estado de sellos, juntas, tornillos, herrajes y movimientos para detectar signos de desgaste, juego, filtraciones o suciedad acumulada.
- Lubricar herrajes, bisagras y mecanismos móviles con aceite libre de resinas y ácidos, nunca con grasas derivadas del petróleo. Ajustar tornillos sueltos y verificar el cierre adecuado de ventanas y puertas.
- Revisar y limpiar periódicamente los orificios de drenaje de los marcos para evitar obstrucciones de agua, especialmente en temporada de lluvias.
- Verificar el correcto funcionamiento de los seguros y manillas, reapretando o alineando si fuera necesario.

Mantenimiento Predictivo

- Cada 6 a 12 meses, inspeccionar los vidrios y perfiles en busca de fisuras, desprendimientos de sellador o manchas. Si se detecta desgaste en las juntas o pérdida de estanqueidad, se debe programar el reemplazo preventivo antes de que ocurran fallas o filtraciones.
- En ambientes costeros o industriales, evaluar la existencia de corrosión en perfiles y tornillería. Aplicar tratamiento protector si se detectan signos tempranos de corrosión.

Mantenimiento Correctivo

- Si se identifican grietas, desprendimientos, rotura de vidrios, herrajes trabados, filtraciones de agua o deterioro de juntas, se debe actuar de inmediato reemplazando los componentes afectados por repuestos originales o materiales compatibles con aluminio y vidrio de seguridad.
- Se recomienda siempre la intervención de personal calificado para el cambio de vidrios o la reparación estructural de herrajes y mecanismos.

Mantenimientos Recurrentes

TAREA	FRECUENCIA	OBSERVACIÓN
Limpieza de vidrios y perfiles	Trimestral	Paño suave, detergente neutro, secado inmediato
Limpieza de juntas y drenajes	Trimestral	Verificar ausencia de obstrucciones y resecar luego
Inspección visual general	Semestral	Detectar signos de desgaste, grietas o corrosión

Lubricación de herrajes y mecanismos	Semestral/anual	Aplicar lubricante específico, evitar grasas agresivas
Ajuste de tornillos y fijaciones	Semestral	Reapretar elementos móviles y embellecedores
Reparación/reemplazo de vidrios o herrajes	Inmediato	Solo personal calificado, usar piezas originales

Recomendaciones adicionales

- Mantener despejada la zona próxima a las ventanas y evitar contacto con materiales corrosivos.
- Un mantenimiento programado garantiza durabilidad, funcionalidad, seguridad y estética de la ventanería en aluminio con vidrio de seguridad.

7.11. DIVISIONES DE BAÑOS EN ACERO INOXIDABLE





Se realizó el suministro e instalación de divisiones de baño en acero inoxidable las cuales fueron instaladas para dividir sanitarios y orinales en el baño de hombres del piso cinco.

Cuidados para el uso y limpieza

- **Uso Responsable y Prevención de Daños:** Se recomienda no ejercer fuerza excesiva sobre las puertas o paneles, ni golpear, rayar o suspender objetos pesados de las divisiones. Es fundamental evitar el contacto de los perfiles con ácidos, limpiadores abrasivos, herramientas metálicas o solventes agresivos.
- **Prevención de Manchas y Corrosión:** Aunque el acero inoxidable es altamente resistente a la oxidación, requiere mantenerse libre de contaminantes y residuos de productos químicos del baño para evitar la aparición de manchas, picaduras o corrosión incipiente.
- La limpieza debe realizarse periódicamente con un paño de algodón o microfibra, siguiendo el sentido del pulido del acero inoxidable y utilizando jabón líquido neutro y agua tibia. Nunca debe usarse cepillo metálico, esponjilla, productos clorados, ácidos, desengrasantes abrasivos ni amoníaco.
- Tras enjuagar, se debe secar completamente la superficie con un paño seco y suave para evitar manchas por humedad o agua.
- Para retirar manchas difíciles, puede aplicarse agua caliente y frotar suavemente con un cepillo de fibras de nylon o, en casos extremos, usar lija fina húmeda en el sentido del pulido.
- Es importante limpiar también periódicamente los herrajes, bisagras, chapetas y soportes, retirando residuos de jabón, polvo y suciedad acumulada.
- No se debe usar mangueras o agua a presión directamente sobre las divisiones para evitar filtraciones o afectación de herrajes internos.

Actividades de mantenimiento según tipo:

Mantenimiento Preventivo

- **Inspección Visual Mensual:** Se debe revisar la integridad de paneles, puertas y herrajes, buscando signos de piezas flojas, tornillos sueltos, desgaste o presencia de manchas, rayaduras, corrosión o residuos.
- **Limpieza Regular:** Mantener la limpieza semanal recurrirá en mejor apariencia, higiene y durabilidad del acero y sus accesorios.
- **Ajuste de Tornillería:** Cada tres meses, revisar y ajustar los tornillos, fijaciones y soportes para evitar aflojamientos por el uso continuo o vibraciones.
- **Verificación de Sellos y Juntas:** Revisar el estado de siliconas, juntas o gomas de estanqueidad, reemplazando si presentan daño, desprendimiento o deficiencia de sellado.

Mantenimiento Predictivo

- **Seguimiento de Estado de Superficies:** Cada 6-12 meses, verificar el estado superficial del acero y anticipar tratamiento de recuperación (pulido o limpieza especial) si aparecen manchas, decoloraciones o señales de corrosión incipiente.
- **Estado de Herrajes y Bisagras:** Lubricar con productos especializados los herrajes y bisagras en intervalos semestrales o cuando se perciban ruidos o dureza en el movimiento.

Mantenimiento Correctivo

- **Reemplazo de Piezas Dañadas:** Si se identifican piezas golpeadas, dobladas, rayadas o que no cumplen su función, se deben reemplazar inmediatamente por repuestos originales.
- **Eliminación de Manchas Persistentes o Corrosión:** Ante signos de corrosión o manchas imposibles de remover con limpieza básica, se recomienda limpiar con solventes apropiados bajo supervisión técnica o contactar a un especialista para repulido y recuperación.
- **Corrección de Daños en Fijaciones:** Cualquier filtración o desprendimiento de paneles, puertas o soportes requiere intervención inmediata para evitar accidentes o deterioros mayores.

Mantenimientos Recurrentes

TAREA	FRECUENCIA	OBSERVACIÓN
Limpieza superficial (paño, agua, jabón neutro)	Semanal	Secar completamente el acero después
Inspección visual de superficies y herrajes	Mensual	Revisar tornillos, manchas, rayaduras y presencia de residuos
Ajuste de tornillos y fijaciones	Trimestral	Asegurar todas las conexiones y herrajes
Limpieza y lubricación de bisagras/herrajes	Semestral	Usar lubricante especializado
Reparación/reemplazo de piezas dañadas	Inmediato	Solo repuestos originales; intervención profesional si es complejo

Recomendaciones adicionales

- La instalación y los ajustes mayores deben ser realizados solo por personal calificado, siguiendo especificaciones técnicas de fabricante.
- En baños públicos de alto tráfico, se recomienda aumentar la frecuencia de inspección y limpieza.
- Evitar apoyarse sobre los paneles o puertas y no colgar objetos en los perfiles.
- Mantener ventilados los baños para evitar acumulación de humedad y garantizar el mejor comportamiento del acero inoxidable.

Para efectos de garantías y con el fin de preservar la vida útil de los componentes descritos en el presente manual, es recomendable que cada vez que se realicen alguno de los mantenimientos preventivos, predictivos y correctivos, se diligencie el formato que se encuentra adjunto para llevar una trazabilidad, así mismo, se solicita que cada vez que se realice uno de los mantenimiento mencionados, se envíe la copia del respectivo formato diligenciado por completo al correo que se encuentra al inicio del manual.



ALBA VIVIANA TORRES USECHE

CC: 26.422.200

Representante legal

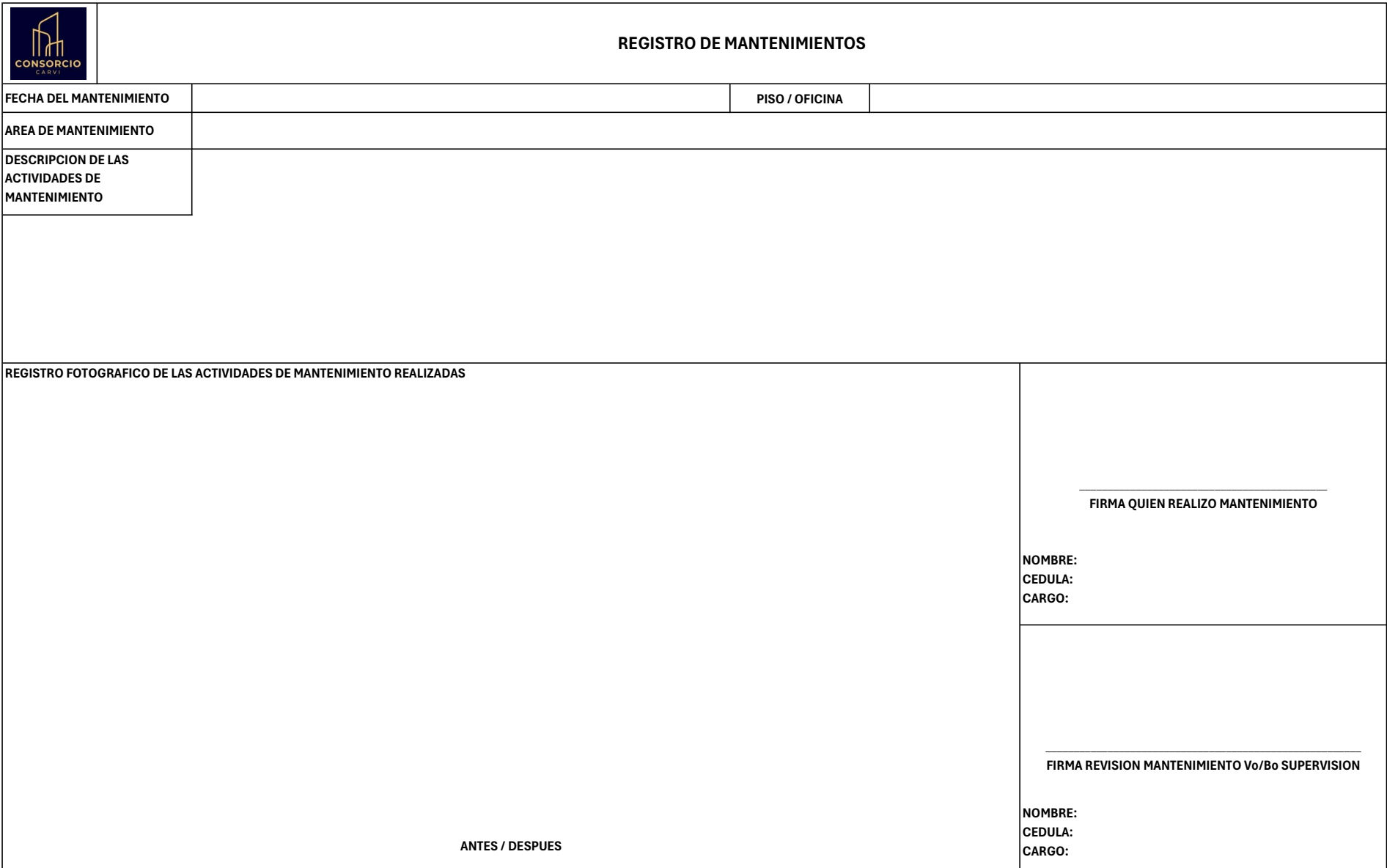
CONSORCIO CARVI

NIT: 901.895.769-3

consorciocarvi@yahoo.com

8. ANEXOS

8.1. FORMATO DE REALIZACIÓN DE MANTENIMIENTO.



8.2. MANUAL DE MANTENIMIENTO UPS



MANUAL DE USUARIO



Sistema de potencia ininterrumpida
POWEST EA9910-EA9915-EA9920



Importado y Comercializado para Colombia por:

Razón Social: NICOMAR ELECTRONICS S.A., NIT: 860 450 450 -1
Carrera 62 # 14 - 65 Puente Aranda; Bogotá - Colombia.

Importado y Comercializado para Ecuador por:

Razón Social: POWEST-ECUADOR S.A. RUC: 1792929113001
Dirección: Av. 6 de Diciembre N 33-12 e Ignacio Bossano. Edificio Torres
Bossano. Torre B. Ofc. 1104. Quito - Ecuador

Importado y Comercializado para Panamá por:

Razón Social: POWER WEST CORP.
Número de identificación 1946990-1-731123 DV.73
Av. Ricardo J. Alfaro - Edificio Golden Point Piso 23 oficina 2301
Ciudad de Panamá – Panamá

Importado y Comercializado para México por:

Razón Social: POWEST MÉXICO S.A. DE C.V.
RFC: PME240216K64
Av. Paseo de las palmas 525 piso 7
Lomas de Chapultepec, 11000 Ciudad de México.

HECHO EN CHINA

Gracias por seleccionar este sistema de alimentación ininterrumpida (UPS) usted. Le proporciona protección para el equipo conectado. Lea este manual antes de instalar el modelo EA9900, ya que proporciona información importante que deben seguirse durante la instalación y el mantenimiento de UPS y las baterías, lo que le permite ajustar correctamente a su sistema durante la máxima seguridad y rendimiento. Se incluye información sobre la atención al cliente y servicio, si es necesario. Si experimenta un problema con el UPS, por favor refiérase a la sección de Solución de problemas en este manual para corregir el problema. Si el problema no se corrige, por favor recoger información para que el personal de soporte técnico le puede ayudar de manera más eficaz.

Todos los derechos reservados.

La información contenida en este documento está sujeta a cambios sin previo aviso.

Instrucciones de seguridad importantes: (Guarde estas instrucciones)

GUARDE ESTAS INSTRUCCIONES - Este manual contiene instrucciones importantes para el modelo EA9900 que deben seguirse durante la instalación y mantenimiento del UPS y las baterías.

10kVA Durante Circuito de DC externa Dispositivo de protección actual - “PRECAUCIÓN - Para reducir el riesgo de incendio, conecte sólo a un circuito provisto con DC 63 amperios máximo circuito rama sobre protección de corriente de acuerdo con el Código Eléctrico Nacional, ANSI / NFPA 70” .

15 / 20kVA Durante Circuito de DC externa Dispositivo de protección actual - “PRECAUCIÓN - Para reducir el riesgo de incendio, conecte sólo a un circuito provisto con DC 125 amperios máximo circuito ramificación sobre protección de corriente de acuerdo con el Código Eléctrico Nacional, ANSI / NFPA 70” .

¡PRECAUCIÓN! (UPS que tiene baterías internas): Riesgo de descarga eléctrica - Las partes conductoras dentro de esta unidad se energizan de la alimentación de la batería, incluso cuando se desconecta la alimentación de CA de entrada.

¡PRECAUCIÓN! (Ninguna pieza que puedan generar): Riesgo de descarga eléctrica, no quite la tapa. No hay piezas en el interior. Consulte al personal de servicio calificado.

¡PRECAUCIÓN! (No aislado de suministro de la batería): Riesgo de choque eléctrico, circuito de la batería no está aislada de la entrada de AC, puede existir tensión peligrosa entre terminales de la batería y de tierra. Prueba antes de tocarlos.

ADVERTENCIA! (Fusibles): Para reducir el riesgo de incendio, reemplace sólo con el mismo tipo y tamaño de fusible.

ADVERTENCIA! Unidad diseñada para ser instalado en un ambiente controlado.

¡PRECAUCIÓN! No tire las baterías al fuego, la batería podría explotar.

¡PRECAUCIÓN! No abra ni rompa la batería, el electrolito liberado es dañino para la piel y ojos.

¡PRECAUCIÓN! Una batería puede presentar un riesgo de descarga eléctrica y la corriente de cortocircuito. La siguiente precaución debe ser observada cuando se trabaja con baterías:

- No lleve relojes, anillos u otros objetos metálicos.
- Use herramientas con mangos aislados.

Para reducir el riesgo de descarga eléctrica, desconecte el UPS de la alimentación principal antes de instalar un equipo inter cable de señal de la cara. Vuelva a conectar el cable de alimentación sólo después de que se han realizado las interconexiones de señalización.

El mantenimiento de las baterías debe ser realizado o supervisado por personal con conocimiento de las baterías y las precauciones necesarias. El personal no autorizado lejos de las baterías.

Para el reemplazo de las baterías situadas en un área de acceso **SERVICIO**.

1) Mantenimiento de las baterías debe ser realizado o supervisado por personal experto en baterías y las precauciones necesarias.

2) Existe riesgo de explosión si la batería se sustituye por un tipo incorrecto. Al cambiar las pilas, reemplace con el mismo tipo y número de baterías o paquetes de baterías.

3) PRECAUCIÓN: No tire las baterías al fuego. Las baterías pueden explotar. Deseche las baterías usadas de acuerdo con las instrucciones.

4) PRECAUCIÓN: No abra ni rompa las pilas. El electrolito liberado es dañino para la piel y los ojos. Puede ser tóxico.

5) PRECAUCIÓN: Una batería puede presentar un riesgo de descarga eléctrica y la corriente de cortocircuito. Los siguientes se deben tomar precauciones cuando se trabaja con baterías:

- a. Retire relojes, anillos u otros objetos metálicos.
- b. Utilice herramientas con mangos aislados.
- c. Use guantes y botas de goma.
- d. No deje herramientas o piezas metálicas sobre las baterías.
- e. Desconectar la fuente de carga antes de conectar o desconectar los terminales de la batería.
- f. Determinar si la batería está conectada a tierra de forma inadvertida. Si a tierra inadvertidamente, retire la fuente de la tierra. El contacto con cualquier parte de una batería conectada a tierra puede provocar una descarga eléctrica. La probabilidad de tal choque puede ser reducido si estos motivos se eliminan durante la instalación y el mantenimiento.

Estas unidades UPS son extremadamente pesados. Se debe tener precaución en el equipo móvil y posicionamiento. Las instrucciones contenidas en este manual de seguridad se consideran importantes y deben ser seguidos de cerca en todo momento durante la instalación y el mantenimiento de seguimiento de UPS y las baterías.



PRECAUCIÓN

La unidad tiene una cantidad peligrosa de la tensión. Si el indicador está en UPS, puntos de venta de la unidad puede tener una cantidad peligrosa de la tensión incluso cuando no está conectado a la toma de corriente porque la batería puede continuar suministrando energía.

Se debe tener cuidado para llevar a cabo la instalación en el interior, libre de partículas eléctricamente conductoras que se encuentran bajo control de la temperatura y la humedad, con el fin de reducir el riesgo de descarga eléctrica.

Lo mejor es desconectar el dispositivo mediante el cable de alimentación. Asegúrese de que el equipo se coloca en una posición cerca de la salida donde fácilmente accesible.

A excepción de la sustitución de las baterías, todo el mantenimiento de este equipo debe ser llevado a cabo personal calificado.

Antes de realizar cualquier trabajo de mantenimiento, reparación, o el envío, en primer lugar asegurarse de que todo este desconectado y apagado completamente.

Para instrucciones de seguridad adicionales, por favor utilice el manual de seguridad como referencia.

Los símbolos especiales

Los siguientes símbolos utilizados en los UPS que advierten de precauciones:



RIESGO DE DESCARGA ELÉCTRICA - Tener en cuenta la advertencia de que un riesgo de descarga eléctrica está presente



PRECAUCIÓN: CONSULTE EL MANUAL DEL OPERADOR - Consulte el manual del operador para obtener información adicional, tales como instrucciones de funcionamiento y mantenimiento.



TERMINAL DE TIERRA SEGURO - Indica terreno seguro primario



Por favor, no deseches de los UPS o las baterías del UPS como el UPS puede tener baterías de plomo-ácido regulada por válvula. Por favor, reciclar las pilas de manera apropiada.

1. Características Principales.

1.1 Recapitulación

Estas series UPS es una especie de tres en tres de salida de alta frecuencia en línea de UPS.

El UPS puede resolver La mayoría de los problemas de suministro de energía, tales como apagón, de la sobretensión, bajo voltaje, voltaje repentino gota, oscilante decreciente de medida, impulso de alta tensión, fluctuaciones de voltaje en, oleaje, corriente de entrada, Distorsión armónica (THD), la interferencia de ruido, Fluctuaciones de frecuencia , Etc..

Este UPS se puede aplicar a diferentes aplicaciones de computadora dispositivo, El equipamiento Nuevo Testamento, sistema de comunicación al equipo de la industria.

1.2 Funciones y características

- **En 3phase / 3 fases de salida del UPS**

Es el sistema UPS de alta densidad 3Fases En / 3Fases hacia fuera, de los cuales la corriente de entrada se mantiene en equilibrio. No hay problema de desequilibrio podría ocurrir.

- **Control digital**

Esta serie de UPS está controlado por procesador de señal digital (DSP); Aumentar la seguridad, aumenta la fiabilidad, el rendimiento, la autoprotección, y autodiagnóstico y así sucesivamente.

- **Batería configurable**

El sistema de batería es configurable en bloques de 16, 18, 20,22 o 24 según su necesidad..

- **La corriente de carga es configurable**

A través de la configuración de la herramienta, el usuario puede ajustar la capacidad de las baterías, así como corriente de carga razonable y corriente de carga máxima. Modo de voltaje constante, modo de corriente constante o en el modo flotante pueden conmutarse automáticamente y sin problemas.

- **Método de carga inteligente**

La serie UPS adopta el avanzado de carga de tres etapas método-

1ª etapa: alta carga de corriente constante actual para garantizar a cargar a 90%;

2ª etapa: Voltaje constante Con el fin de revitalizar la batería y las pilas estén completamente cargada

3ª etapa: el modo flotante. Con este método de carga de 3 etapas, se extiende la vida de las baterías y garantiza una carga rápida.

- **LCD Monitor** Con LCD más pantallas LED, el usuario puede obtener fácilmente el estado del UPS y sus parámetros de funcionamiento, tales como entrada / tensión de salida, frecuencia y carga% de carga, de las baterías y la temperatura ambiente, etc.
- **Función de Monitoreo Inteligente** a través de la tarjeta SNMP opcional, es posible controlar de forma remota y controlar el UPS.
- **EPO Función** Los UPS de la serie se pueden cortar completamente cuando se pulsa el EPO. Función REPO (EPO remoto) también está disponible en esta serie de UPS.

1.3 Configuración del sistema

El dispositivo UPS y las baterías externas conforman el sistema. Dependiendo de los requisitos del sitio y de la carga de la instalación, algunas opciones adicionales están disponibles para la solución. La planificación de un sistema de UPS, el siguiente debe ser tomada en cuenta:

- La demanda total del sistema protegido dictará la potencia de salida (VA). Permitir un margen de expansiones futuras o de cálculo inexactitudes de los requisitos de potencia medidos.
- El tiempo de respaldo requerido, indicará el tamaño necesario de la batería. Si la carga es inferior a la potencia nominal del UPS, entonces el tiempo real de autonomía en las baterías es más largo
- Las siguientes opciones están disponibles:

Opciones de conectividad por -SNMP / WEB/Relé tarjeta Paquetes mixtos de baterías terminados la configuración de batería De equiparación y la cantidad máxima: 10kVA Máximo 4 paquetes de baterías de 80pcs / 7Ah, +/- 120Vdc, 56UNA; 15 / 20kVA Máximo 4 paquetes de baterías de 80pcs / 7Ah, +/- 120Vcorriente continua, 111UNA; 10kVA Máximo 4 paquetes de baterías de 80pcs / 9Ah, +/- 120Vdc, 56UNA; 15 / 20kVA Máximo 4 paquetes de baterías de 80pcs / 9Ah, +/- 120Vcorriente continua, 111UNA; 10kVAMáximo 1 paquetes de baterías de 300Ah, +/-96Vcorriente continua (16pcs), +/-108Vcorriente continua (18 piezas), +/-120Vcorriente continua (20pcs), +/-132Vcorriente continua (22pcs), +/-144Vcorriente continua (24pcs), 56A. 15 / 20kVA Máximo 1 paquetes de baterías de 300Ah, +/-96Vcorriente continua (16pcs), +/-108Vcorriente continua (18 piezas), +/-120Vcorriente continua (20pcs), +/-132Vcorriente continua (22pcs), +/-144Vcorriente continua (24pcs), 111A.

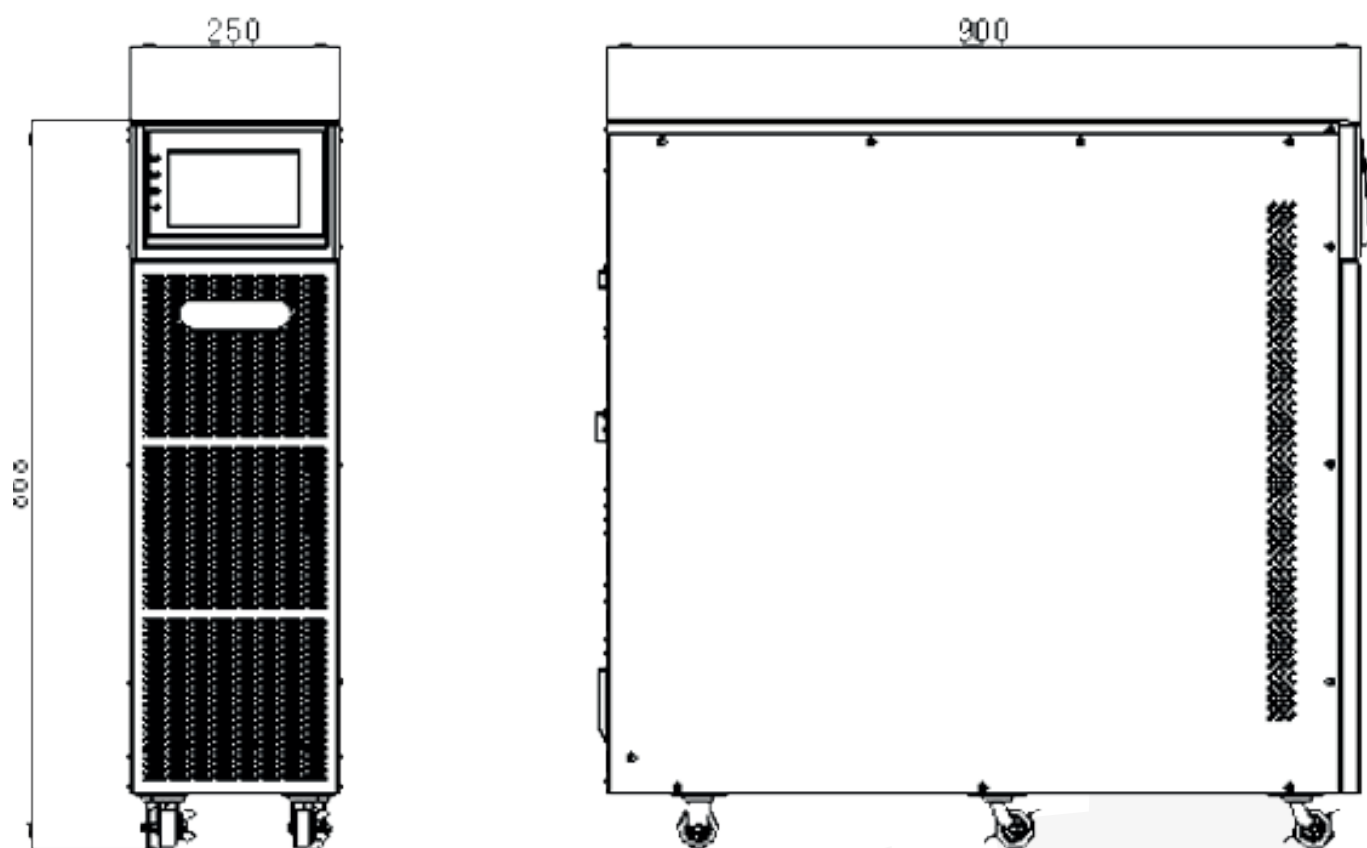
Consulte la sección de especificaciones de este manual para obtener información adicional del modelo.

2. Instalación

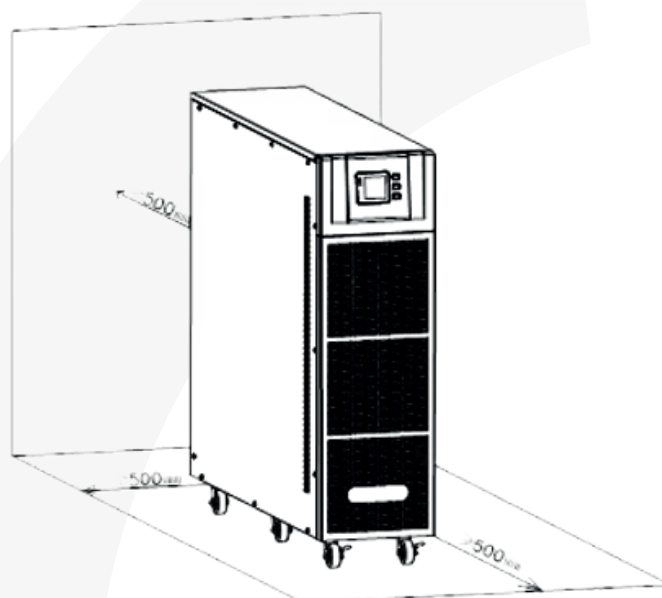
2.1 Instalación

Dimensión (mm)

2.1.2 Instalación

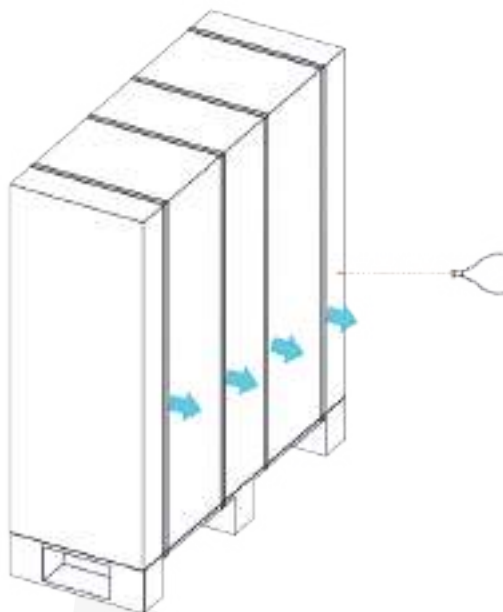


Deje un espacio alrededor del gabinete para el funcionamiento y la ventilación

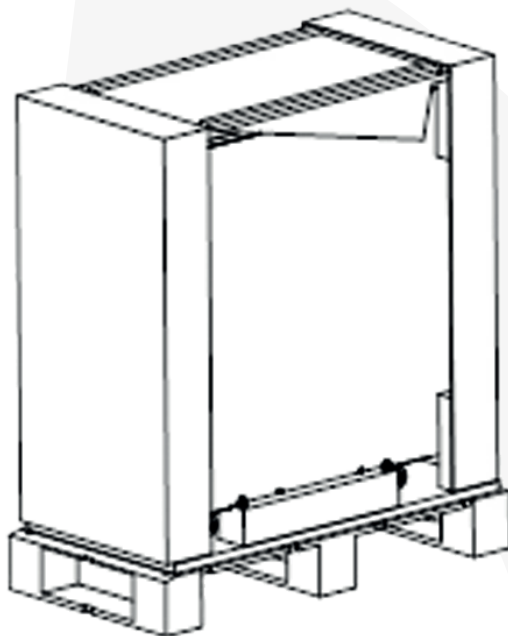


Comprobación de desempaquetado

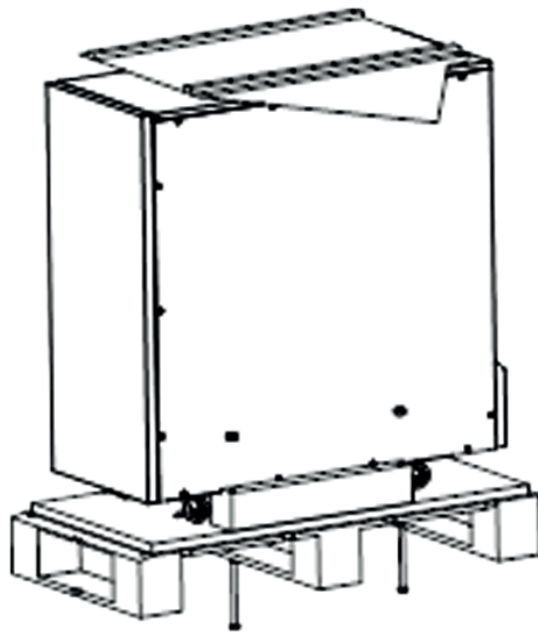
1. No se incline el UPS cuando se mueve hacia fuera del embalaje
2. Compruebe el aspecto para ver si el UPS está dañado o no durante la transportación, No encienda el UPS en su caso de encontrar algo dañado o anormal al momento de desembalaje. Póngase en contacto con el distribuidor inmediatamente.
3. Compruebe los accesorios de acuerdo a la lista de embalaje y póngase en contacto con el distribuidor en caso de que falten partes.



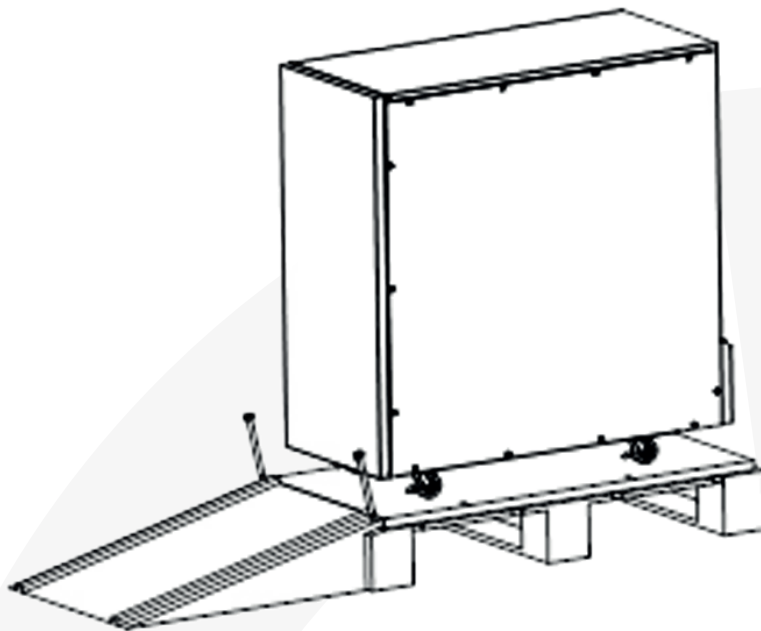
Cortar el vendaje



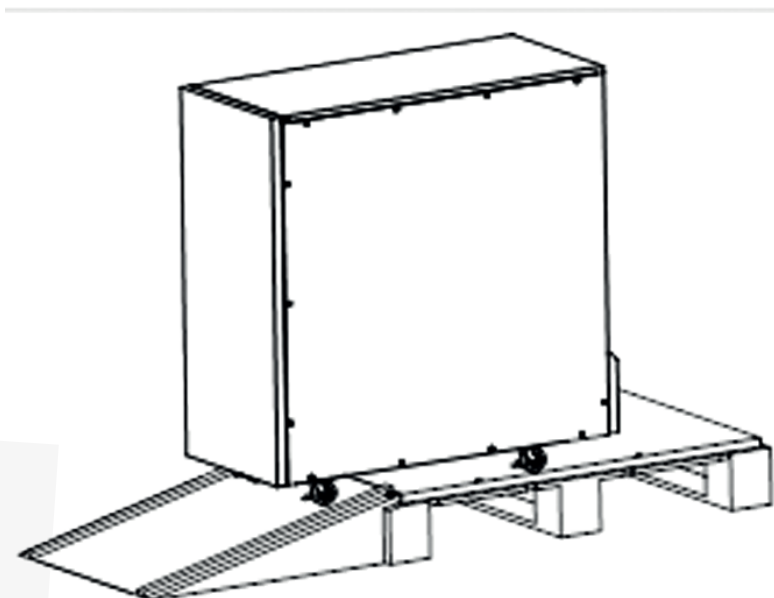
Retire el envase exterior del gabinete



Retire el paquete interior del gabinete, afloje los tornillos y retire la barra de madera fijado a la carcasa.

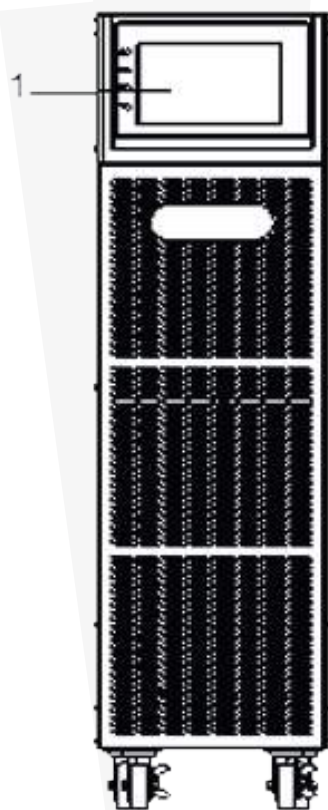


Coloque la placa de inclinación a la tierra, utilice los tornillos abrochados de la última etapa de sujetar el tablero inclinado con paleta.

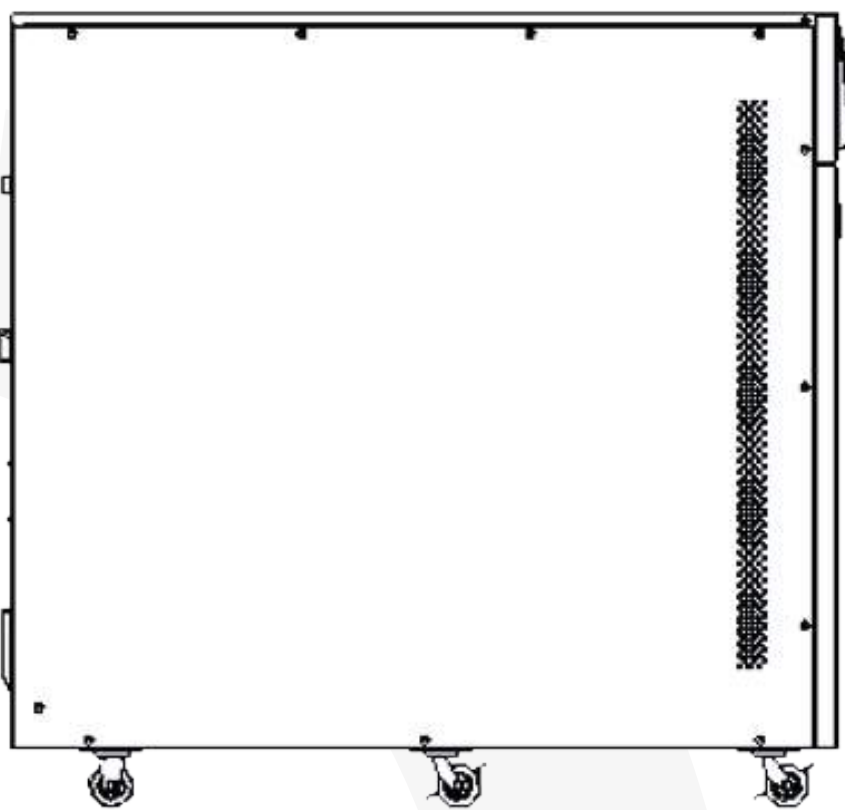


Poco a poco se deslizan por el gabinete de la paleta.

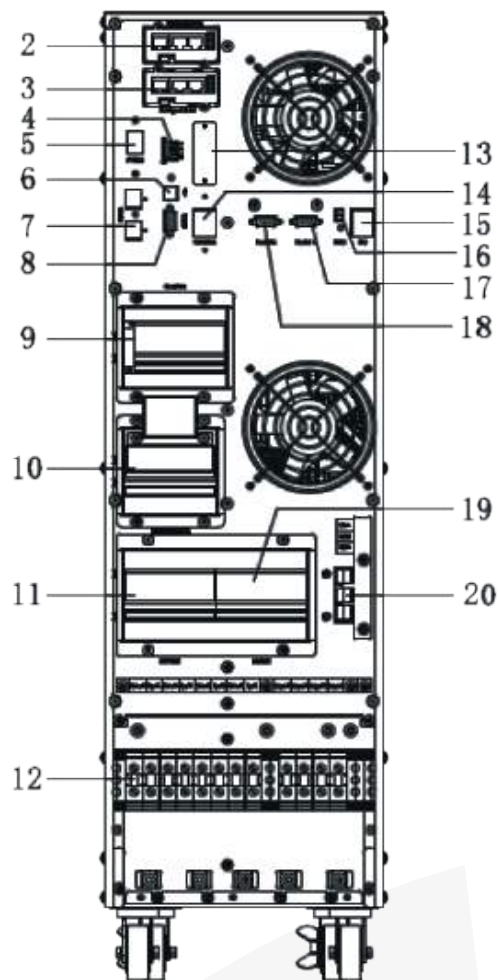
2.2 gabinete de Outlook



Vista frontal

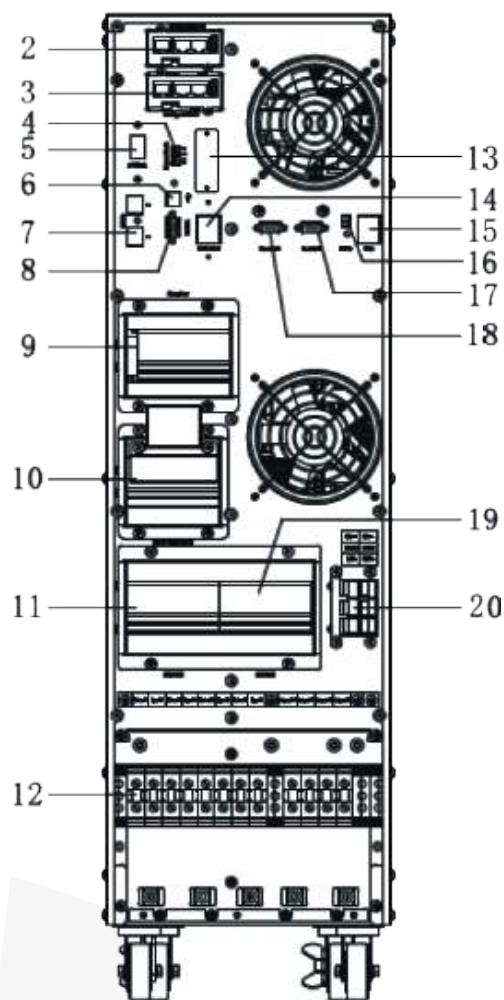


Vista lateral



10kVA Vista trasera (bloque de terminales sin cubierta)

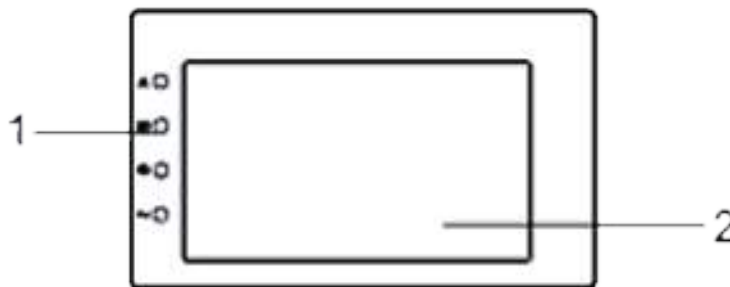
(1) Panel LCD	(2) Ranura Inteligente 1 (tarjeta SNMP / tarjeta de relé)
(3) Ranura inteligente 2 (tarjeta SNMP / Tarjeta de relé)	(4) Puerto de contacto seco
(5) Interruptor de alimentación	(6) Puerto USB
(7) Puerto RS485	(8) RS232
(9) O / Switch P	(10) El interruptor de mantenimiento y su cubierta
(11) Derivación Cambiar	(12) Bloque de terminales para la entrada, salida y GND
(13) Puerto EVENTOS	(14) Botón de arranque en frío
(15) Interruptor EPO	(16) Puerto REPO
(17) Puerto paralelo 2	(18) 1 puerto paralelo
(19) I / Switch P	(20) Bloque de terminales para la batería



15-20kVA Vista trasera (bloque de terminales sin cubierta)

(1) Panel LCD	(2) Ranura inteligente 1 (tarjeta SNMP / tarjeta Relay)
(3) Ranura inteligente 2 (tarjeta SNMP / Tarjeta de relé)	(4) Puerto de contacto seco
(5) Interruptor de alimentación	(6) Puerto USB
(7) Puerto RS485	(8) RS232
(9) O / Switch P	(10) El interruptor de mantenimiento y su cubierta
(11) Derivación Cambiar	(12) Bloque de terminales para la entrada, salida y GND
(13) Puerto EVENTOS	(14) Botón de arranque en frío
(15) Interruptor EPO	(16) Puerto REPO
(17) Puerto paralelo 2	(18) 1 puerto paralelo
(19) I / Switch P	(20) Bloque de terminales para la batería

2.3 Panel de control LCD



Introducción panel de control LCD

(1) LED (de arriba a abajo: “alarma”, “derivación”, “batería”, “inversor”)

(2) LCD monitor

2.4 Notas de instalación

- Por favor, coloque los UPS en un ambiente limpio, estable, evitar la vibración, polvo, humedad, gas y líquido inflamable, corrosivo. Esto para evitar desde lo alto temperatura ambiente, un sistema de extractores habitaciones se recomienda estar instalado. Los filtros de aire opcionales están disponibles si el UPS opera en un ambiente polvoriento.
- La temperatura ambiente alrededor de UPS debe mantener en una gama de 0°C~40°C. Si la temperatura ambiente supera los 40°C, La capacidad de carga nominal debe ser reducida en un 12% por cada 5°C. La temperatura máx. no puede ser mayor que 50°C.
- Para el desmonte del UPS bajo bajas temperaturas, verifique podría estar en una condición de condensación. Los UPS no se pueden instalar a menos que el interior y exterior del equipo estén totalmente seco. De lo contrario, habrá un peligro de descarga eléctrica.
- Las baterías deben ser montados en un ambiente donde la temperatura está dentro de las especificaciones requeridas. La temperatura es un factor importante en la determinación de la vida de la batería y capacidad. En una instalación normal, la temperatura de la batería se mantiene entre 15°C y 25°C. Mantenga las pilas lejos de fuentes de calor o de aire principal ventilación zona, etcétera



¡ADVERTENCIA!

Los datos típicos de rendimiento de la batería se indican para una temperatura de funcionamiento entre 20°C y 25°C. Operando por encima de este rango se reducirá la duración de la batería mientras que la operación por debajo de este rango se reducirá la capacidad de la batería.

- En caso de que el equipo no puede instalar de inmediato se debe almacenar en una habitación con el fin de protegerlo contra la humedad y fuentes de calor excesivo.

¡PRECAUCIÓN!



Una batería no utilizada debe ser recargada cada 6 meses Temporalmente conectar el UPS a una red de alimentación de AC adecuados y activarlo durante el tiempo necesario para recargar las baterías.

- La altitud máxima de operación en condiciones normales es de 1500 metros. La capacidad de carga debe reducirse cuando el UPS está instalado en el lugar cuya altitud es superior a 1.500 metros, que se muestra como la siguiente tabla:

(Coeficiente de carga igual Carga máxima en la altura colocar dividida por la potencia nominal del UPS)

Altitud	1500	2000	2500	3000	3500	4000	4500	5000
Carga	100%	95%	90%	85%	80%	75%	70%	65%

- El enfriamiento de la UPS depende del ventilador, por lo que debe ser mantenido en un área con buena ventilación. Hay muchos agujeros de ventilación en la parte frontal y trasera, por lo cual no deberían ser bloqueados por ningún objeto extraño.

2.5 Dispositivos de protección externos

Por razones de seguridad, es necesaria la instalación de un disyuntor de circuito externo en la entrada de AC y a la batería.

Batería externa

Los UPS y sus baterías asociados están protegidos contra el efecto de sobre-corriente a través de un compatibles DC disyuntor termo-magnético situado cerca de la batería.

Salida de UPS

Cualquier placa de distribución externa utilizada para la distribución de carga deberá estar equipado con dispositivos de protección a fin de evitar el riesgo de sobrecarga del UPS.

Protección contra la sobre tensión

Un dispositivo de protección deberá estar instalado en el panel de distribución de la energía de la red entrante, y debe identificar la capacidad de los cables de alimentación de corriente, así como la capacidad de sobrecarga del sistema.

¡PRECAUCIÓN!



Seleccionar un disyuntor termo magnético con una curva de disparo IEC 60947-2do (Normal) para 125% de la corriente como se enumeran a continuación.

- **10kVA: Breaker de entrada requerido 50A.**
- **15kVA: Breaker de entrada requerido 63A.**
- **20kVA: Breaker de entrada requerido 80A.**

2.6 Cables de poder

El diseño del cable debe cumplir con las tensiones y corrientes previstas en esta sección, y de acuerdo con las ordenanzas locales los códigos eléctricos.



¡ADVERTENCIA!

Al poner en marcha, asegúrese de que usted es consciente de la ubicación y operación DEL EXTERIOR AISLADORES que están conectados a la UPS ENTRADA / BYPASS SUMINISTRO DE LA UTILIDAD PANEL distribución. COMPRUEBE si estos suministros están aislados eléctricamente, y post ninguna señal de advertencia NECESARIAS A EVITAR CUALQUIER operación inadvertida

Tamaños de cable

MODELO UPS	Tamaños de cable (cableado THHW a 75 ° C)			
	UNA	UNA	ENTRADA DE CC	TOMA DE TIERRA
10kVA	8 AWG	8 AWG	6 AWG	8 AWG
15kVA	6 AWG	6 AWG	2 * 6 AWG	6 AWG
20 kVA	4 AWG	4 AWG	2 * 6 AWG	4 AWG

Torque tornillo instalado Recomendado

	Posición		
	ACINPUT	ACOUTPUT	TOMA DE TIERRA
Tipo de tornillo	METRO	METRO	METRO
El par recomendado (Nm)	6.5	6.5	6.5



¡PRECAUCIÓN!

Cable de tierra de protección: conectar cada armario a una toma de tierra, siguiendo la ruta más corta posible.



¡ADVERTENCIA!

FAILURE seguir los procedimientos PUESTA A TIERRA adecuada puede dar lugar interferencias electromagnéticas O PELIGROS INVOLUCRANDO choque eléctrico y FUEGO.

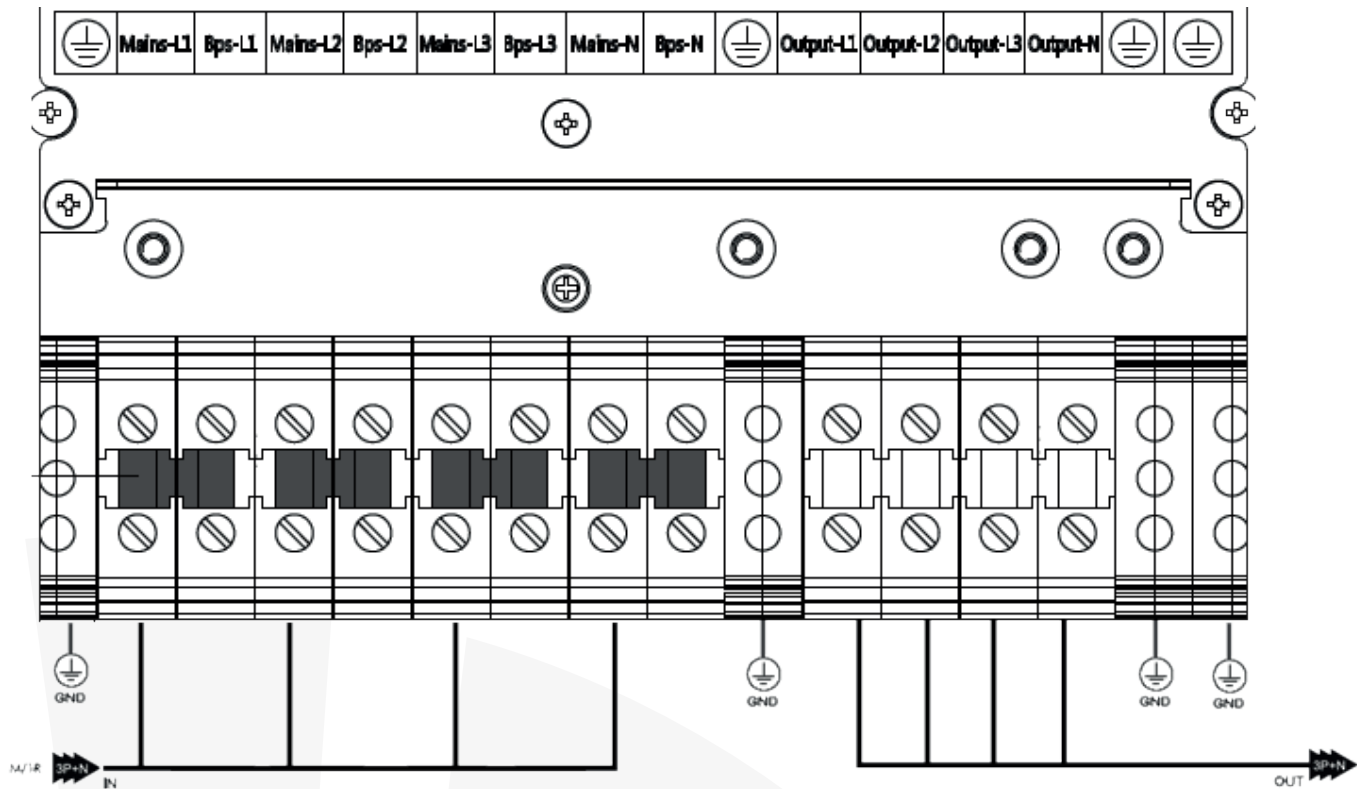
2.7 Cable de alimentación conecte

Una vez que el equipo ha sido finalmente colocado y asegurado, conectar los cables de alimentación como se describe en el siguiente procedimiento. Compruebe que el UPS está totalmente aislado de su fuente de alimentación externa y que todo esté aislado de energía de los UPS están

abiertos. Comprobar para ver si están aislado eléctricamente, y después de algunas señales de alerta necesarias para evitar su activación involuntaria.

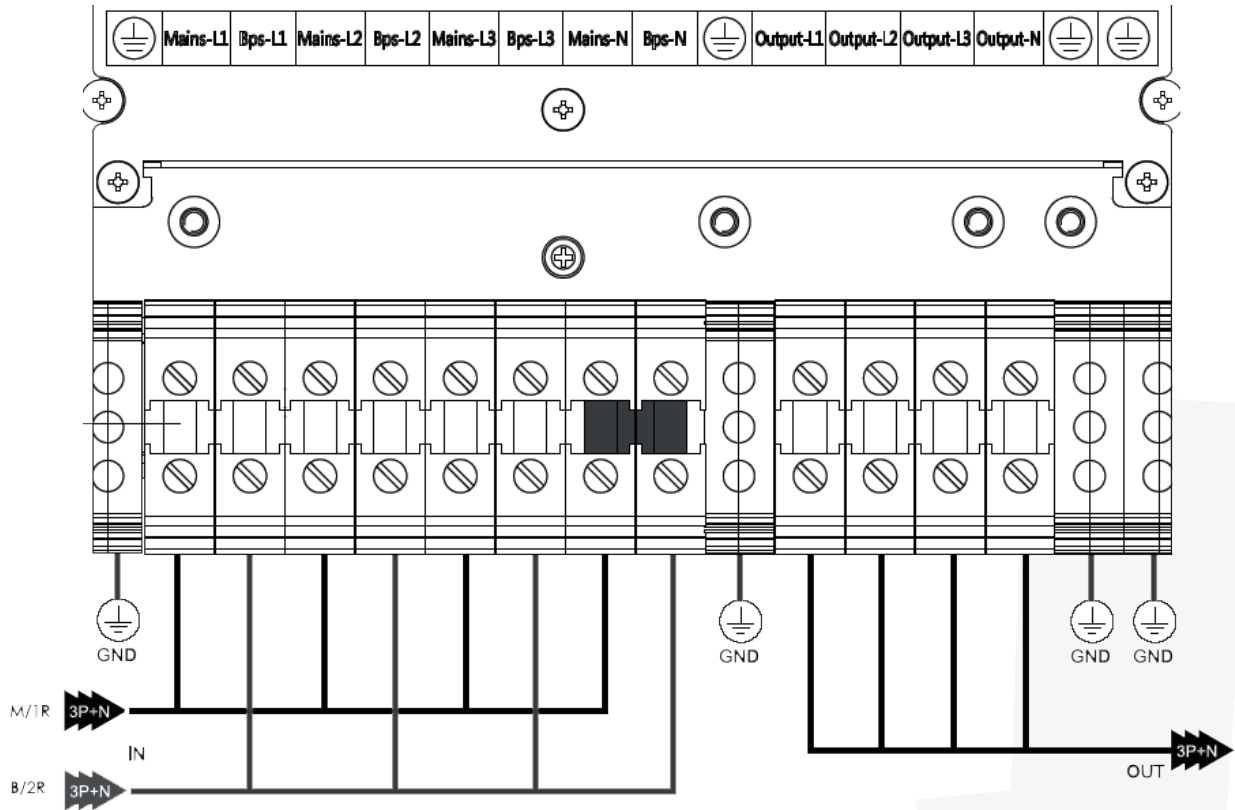
Abrir el panel posterior del UPS; Retire la tapa de terminales para cableado fácil.

2.7.1 conexión de entrada común



M / 1R	Línea de entrada primaria	EN FUERA	De entrada y salida
		Salida-L1:	Fase de salida L1
-L1 de entrada:	Entrada primaria Fase L1	Salida-L2:	Fase de salida L2
-L2 de entrada:	Entrada primaria Fase L1	Salida-L3:	Fase de salida L3
-L3 de entrada:	Entrada primaria Fase L1	Salida-N:	Salida Neutro
Input-N:	Neutro de entrada para la entrada primaria y secundaria	GND:	Toma de tierra
		BAT +:	Terminal positivo de la cadena de baterías
		BAT N:	Terminal neutro de la cadena de baterías
		BAT-:	Polo negativo de la cadena de baterías

Conexión de entrada dividida



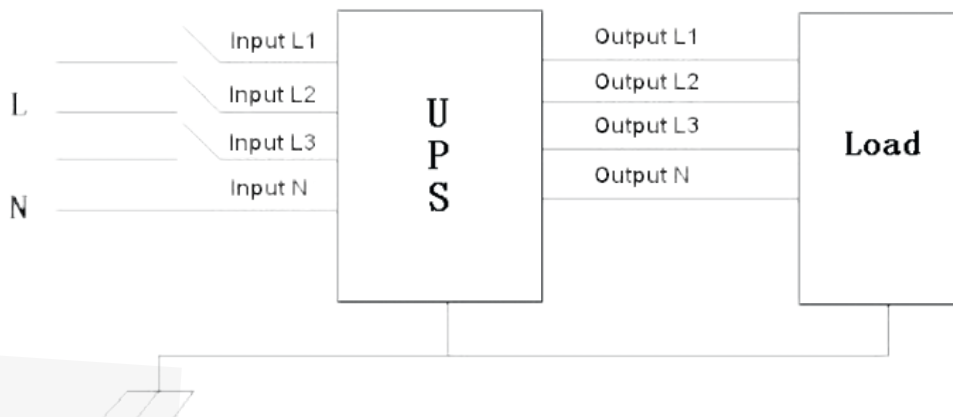
M / 1R Línea de entrada primaria	EN FUERA De entrada y salida
B / 2R línea de entrada secundaria / Bypass (opcional)	Salida-L1: Fase de salida L1
Mains-L1: Entrada primaria Fase L1	Salida-L2: Fase de salida L2
Mains-L2: Entrada primaria Fase L2	Salida-L3: Fase de salida L3
Mains-L3: Entrada primaria Fase L3	Salida-N: Salida Neutro
Input-N: Neutro de entrada para la entrada primaria y secundaria	GND: Toma de tierra
Bps-L1: Entrada secundaria Fase L1	BAT +: Terminal positivo de la cadena de baterías
Bps-L2: Entrada secundaria Fase L2	BAT N: Terminal neutro de la cadena de baterías
Bps-L3: Entrada secundaria Fase L3	BAT -: Polo negativo de la cadena de baterías

¡Advertencia!



En el caso de la operación “de derivación dividir”, asegúrese de que el cobre entre cada uno de las líneas de entrada se han eliminado. La entrada de CA y los suministros de derivación de AC deben ser referenciados al mismo punto neutro.

Elija el cable de alimentación adecuado. (Consulte la tabla anterior) y prestar atención to el diámetro del terminal de conexión del cable ese debe ser mayor que o igual a la de los polos de conexión;



¡ADVERTENCIA!



Si el equipo de carga no está dispuesto a aceptar el poder de la llegada del técnico de puesta a continuación, asegurar que los cables de salida del sistema están aislados de forma segura en sus extremos

Conecte la tierra de seguridad y los cables de conexión a tierra necesaria para el tornillo de tierra de cobre ubicado en el piso del equipo debajo de las conexiones de alimentación. Todos los armarios de la UPS deben estar conectados a tierra.

¡PRECAUCIÓN!



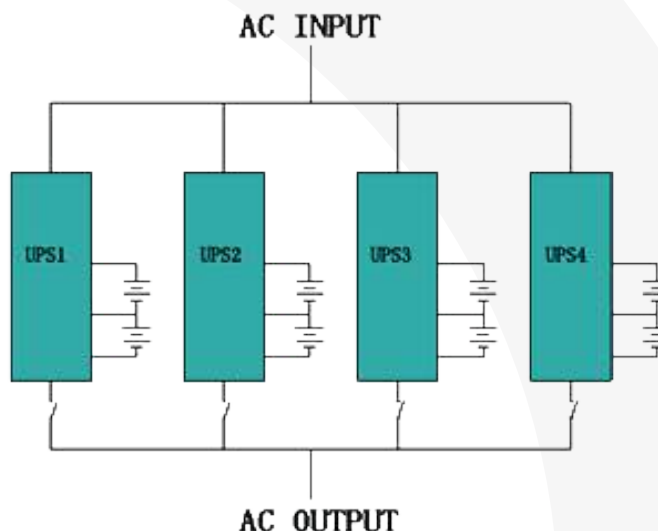
La puesta a tierra y la disposición de sujeción del neutro deben estar en conformidad con los códigos locales y nacionales de prácticas.

2.8 TPS instalación paralela

La sección siguientes introducir el específica procedimientos de instalación al sistema paralelo.

La instalación de gabinetes

Conectar todos los UPS es necesario que se ponga en sistema paralelo como abajo cuadro.



Asegurese de que cada disyuntor de entrada de la UPS esté en “apagado” posición y allí no hay ninguna salida de cada UPS conectados. Grupos de la batería se pueden conectar por separado o en paralelo, lo que significa que el propio sistema proporciona tanto batería separada y la batería común.

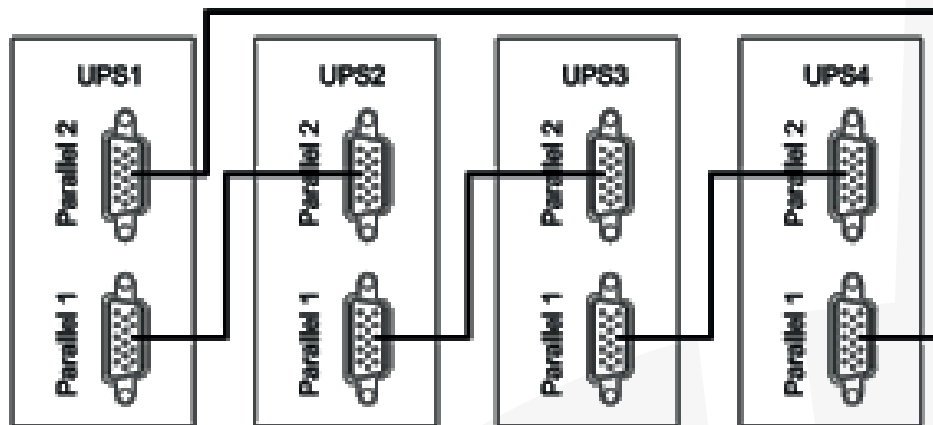


¡ADVERTENCIA!

Asegúrese de que el N, L1, L2, L3 líneas son correctos, y de puesta a tierra está bien conectado.

La instalación del cable paralelo

Apantallados y cables dobles de control de aislamiento disponibles deben estar interconectados en una configuración de anillo entre unidades UPS como se muestra a continuación. La configuración de anillo asegura una alta fiabilidad del control.



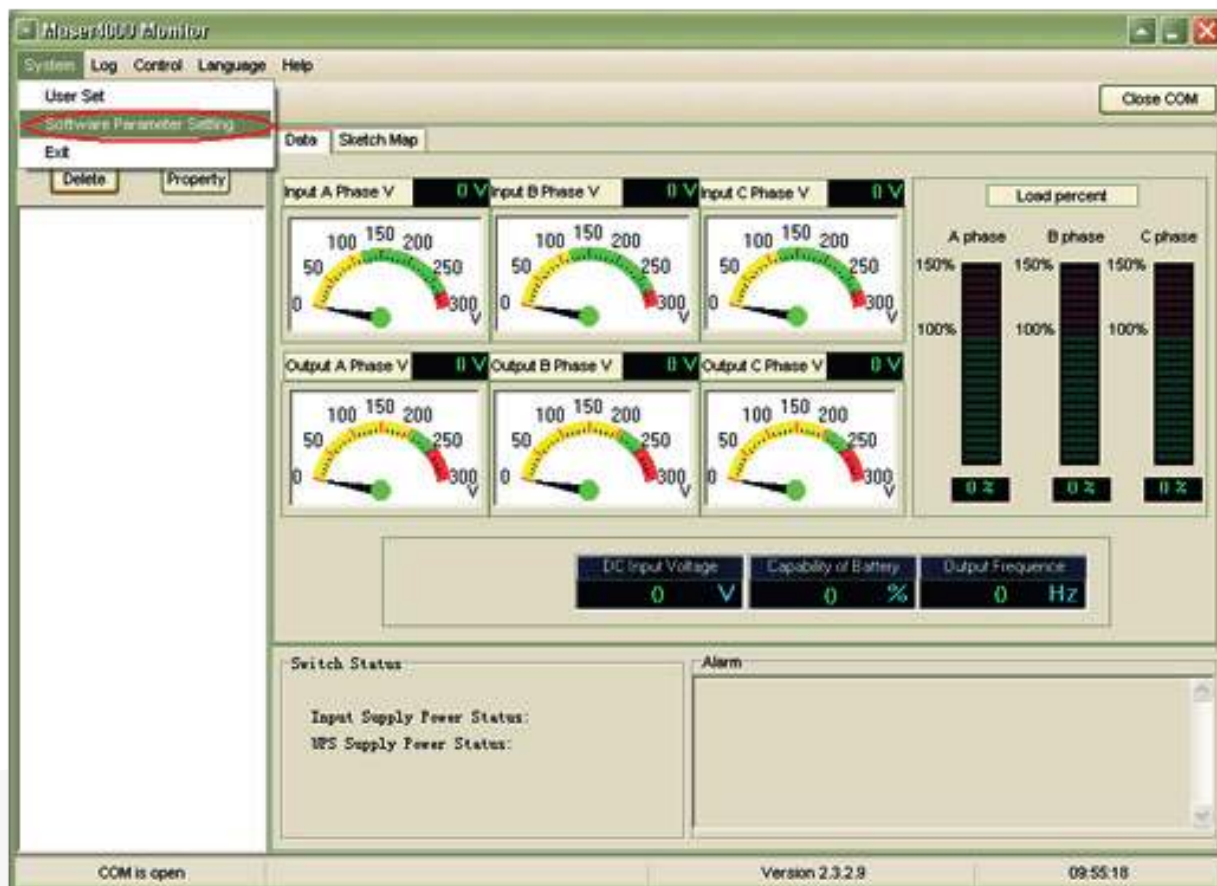
Requisito para el sistema paralelo

Un grupo de UPS en paralelo se comporta como una gran UPS sistema, pero con la ventaja de presentar una mayor fiabilidad. Con el fin de asegurar que todos los UPS se utilizan por igual y cumplen con las normas de cableado pertinentes, por favor siga los requisitos de abajo

- 1)** Todos los UPS deben ser de la misma calificación y ser conectado a la misma fuente de derivación.
- 2)** Las salidas de todos la UPS debe estar conectado a un bus de salida común.
- 3)** La longitud y la especificación de los cables de alimentación, incluyendo los cables de entrada de derivación y los cables de salida del UPS deben ser los mismos. Esto facilita la compartición de carga cuando se opera en el modo de derivación.

2.9 acceso a una computadora

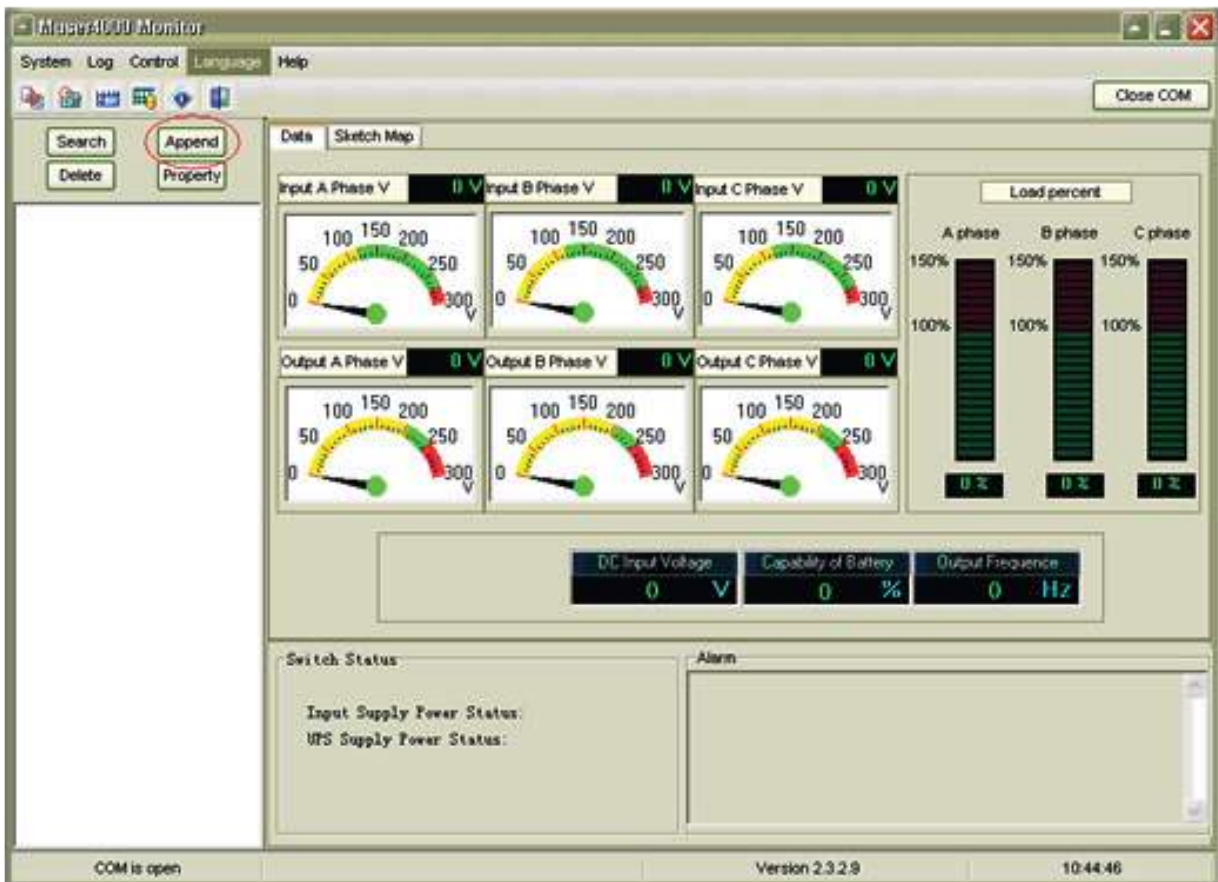
- Un extremo de un cable USB conecta al ordenador, conecte el otro extremo al puerto USB de la UPS.
- Abra el software Muser4000, haga clic en el botón “sistema”.



- Una ventana de “software de parametrización” sale como abajo, COM elegir de acuerdo a la UPS, elegir la velocidad de transmisión de 9600, protocolo de elegir “HIP”; a continuación, guardar este ajuste.



- En la página principal del Muser4000, haga clic en el botón de “Agregar”, luego va a una ventana de “Añadir equipo”.



- Puso el nombre de UPS en “Nombre del equipo,” y la dirección ID UPS’ en ‘dirección de equipo’.



- Haga clic en el botón “Añadir”, entonces la conexión entre el UPS y el ordenador se lleva a cabo.



¡PRECAUCIÓN!

Cuando la UPS trabajó en el inversor. Si desea utilizar la PC para ajustar la tensión de salida y la frecuencia. Debe apagar el inversor primero

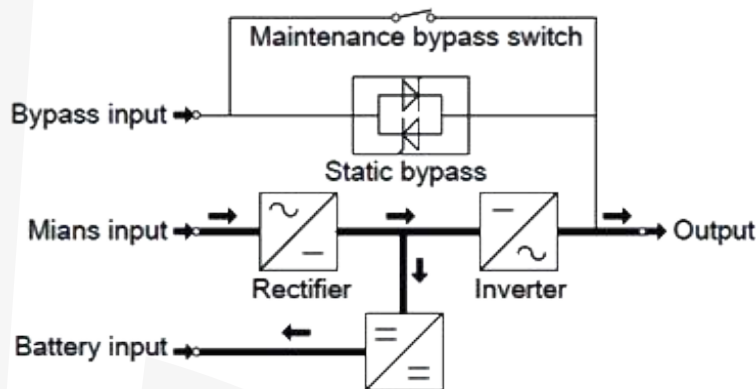
3. Operación

3.1 Modos de operación

El UPS es una de doble conversión en línea UPS que puede operar en los siguientes modos alternativos:

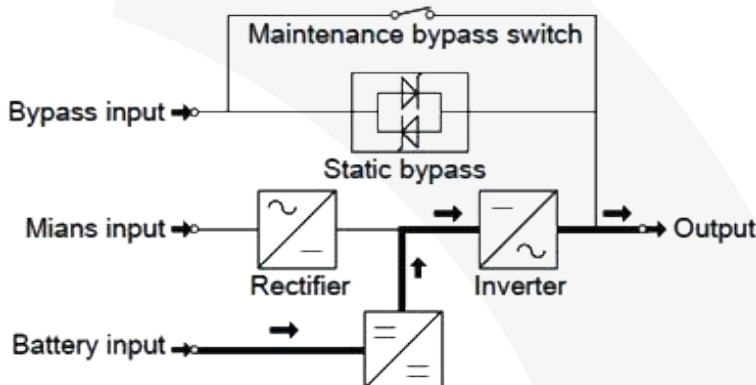
- **Modo normal**

El rectificador / cargador de la energía deriva de la corriente AC y suministra energía DC al inversor mientras flota e impulsar cargar la batería al mismo tiempo. A continuación, el inversor convierte la corriente continua a corriente alterna y suministros a la carga.



- **El modo de batería (Modo de Energía almacenada)**

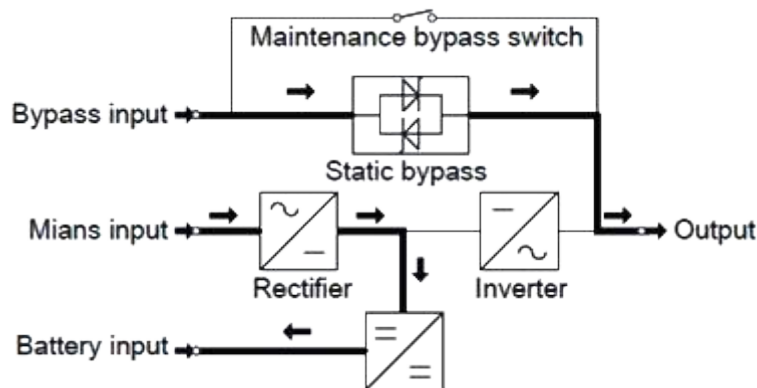
Si la fuente de entrada de la red de AC falla, el inversor, el cual obtiene energía de la batería, suministra la carga crítica. No hay poder interrupción a la carga crítica. El UPS volverá automáticamente al modo normal cuando se recupere AC.



- **El modo de bypass**

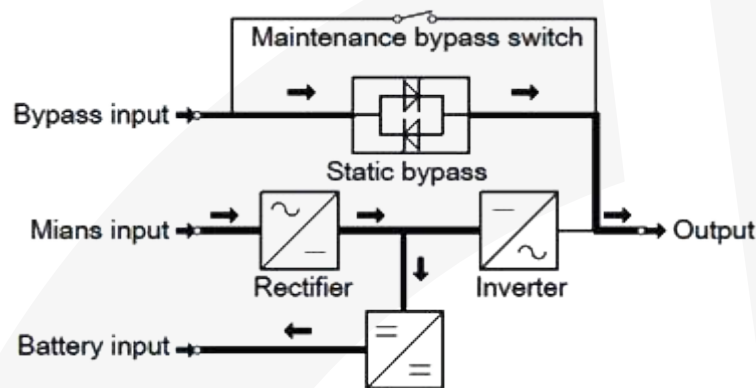
Si el inversor está fuera de servicio, o si se produce sobrecarga, el interruptor de transferencia estática será activado para transferir la carga desde el suministro de inversor a alimentación de bypass sin interrupción a la carga crítica. En el caso de que la salida del inversor no está sincro-

nizado con la fuente de AC de derivación, el conmutador estático llevará a cabo una transferencia de la carga desde el inversor a la derivación con la interrupción de energía a la carga crítica. Esto es para evitar la puesta en paralelo de fuentes de AC no sincronizados. Esta interrupción es programable pero típicamente ajustado a ser inferior a un ciclo eléctrico por ejemplo menos de 15 ms (50 Hz) o menor que 13.33ms (60Hz).



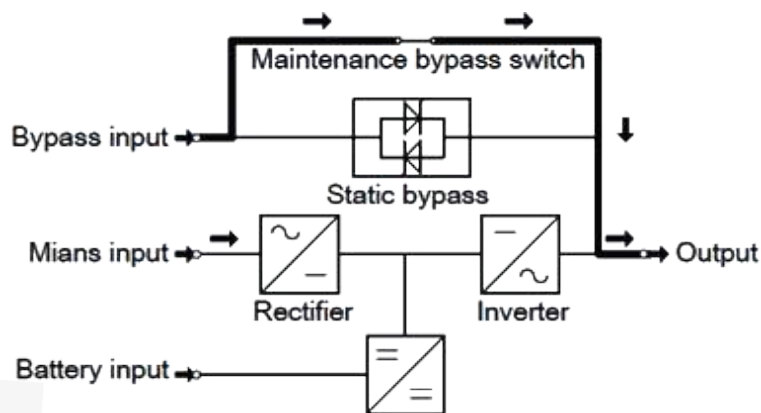
- **Modo ecológico**

Cuando la UPS está en modalidad de AC y el requisito de la carga no es crítica, los UPS se pueden establecer en el modo ECO con el fin de aumentar la eficiencia de la potencia suministrada. En el modo ECO, el UPS funciona en modo de línea interactiva, por lo que el UPS transferirá para eludir la oferta. Cuando el aire acondicionado está fuera de la ventana de ajuste, el UPS cambiará de derivación a inversor y suministra energía desde la batería, y luego la pantalla LCD muestra toda la información relacionada en la pantalla.



- **El modo de mantenimiento (Bypass Manual)**

Un interruptor de derivación manual está disponible para asegurar la continuidad del suministro a la carga crítica cuando el UPS está fuera de servicio o en la reparación y este manual lleva interruptor de derivación para equivalente clasificación de carga.



3.2 Activar / desactivar UPS

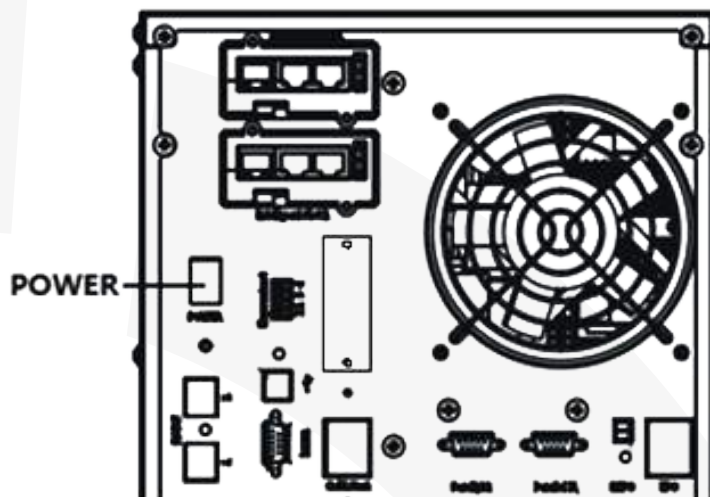
Procedimiento de re arranque



¡PRECAUCIÓN!

¡Asegúrese de puesta a tierra se realiza correctamente!

- Ajuste el interruptor de la batería a la posición “ON” para UPS de largo plazo.
- Active el equipo cambiar para UPS estándar.



¡PRECAUCIÓN!

Compruebe si la carga está conectada de manera segura con la salida de la UPS. Si la carga no está listo para recibir energía de los UPS, asegúrese de que está segura aislado de los terminales de salida del UPS

- Conectar el interruptor de entrada del UPS

Si la entrada del rectificador está dentro del rango de voltaje, el rectificador se iniciará en 30 segundos, el inversor se pondrá en marcha después de entonces.

- Conectar el interruptor de salida del UPS Si el rectificador falla en el arranque, el LED se iluminará de derivación. Cuando el inversor se pone en marcha, el UPS transferirá desde el modo de derivación a modo de inversor, y luego se apaga la LED de derivación y el inversor LED se ilumina. No importa si el UPS puede funcionar normalmente o no, todo el estado se mostrará en la pantalla LCD.

Procedimiento de prueba



¡ATENCIÓN!

El UPS está funcionando normalmente. Puede tardar 60 segundos para aumentar el sistema y realizar Auto test completo.

- Desconectar la red eléctrica para simular fallo de red, el rectificador se apagará y la batería debería alimentar el inversor sin interrupción. En este momento, los LED de la batería deben estar encendidos.
- Conectar la red eléctrica para simular recuperación utilidad, el rectificador se reiniciará automáticamente después de 20 segundos y el inversor suministrará a la carga. Se sugiere utilizar cargas ficticias para la prueba. El UPS puede ser cargado hasta su capacidad máxima durante la prueba de carga.

Bypass de mantenimiento

Para alimentar la carga a través de red, es posible que simplemente activa el interruptor de derivación mecánica interna.



¡PRECAUCIÓN!

La carga no está protegida por el UPS cuando el sistema de derivación mecánica interna es activa y la potencia no está condicionada.

Cambiar a Bypass de mantenimiento



¡PRECAUCIÓN!

Si el UPS está funcionando normalmente y puede ser controlado a través de la pantalla, llevar a cabo los pasos 1 a 5; de lo contrario, saltar al paso 4.

- Abra la cubierta del interruptor de mantenimiento, el UPS vuelve al modo de derivación automática.
- Activar el interruptor Mantenimiento;
- Desconectar el interruptor de la batería;
- Apagar el interruptor de la red,
- Desconectar disyuntor de salida;

En este momento la fuente de derivación suministrará a la carga a través del interruptor de MANTENIMIENTO.

Cambiar a la operación normal (de derivación mecánica)



¡ATENCIÓN!

Nunca trate de cambiar el UPS al funcionamiento normal hasta que haya comprobado que no hay fallos interna del UPS

- Encender la disyuntor de salida.
- Encender el interruptor de entrada.

Los poderes de UPS la bypass estático en lugar de la bypass de mantenimiento, a continuación, el bypass LED se iluminará.

- Apagar la disyuntor de derivación de mantenimiento, Entonces la salida es suministrada por el bypass estático del UPS.
- Ponerse la cubierta del interruptor de mantenimiento.

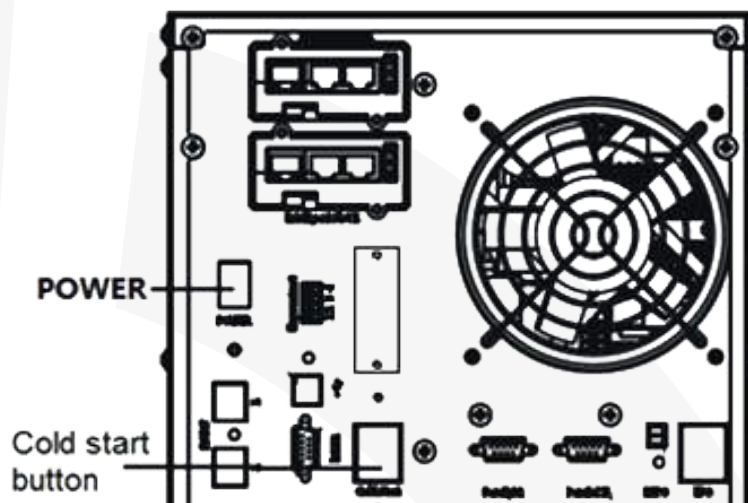
El rectificador funcionará normalmente después de 30 segundos. Si el inversor funciona normalmente, el sistema será transferido de modo de derivación al modo normal.

Procedimiento de arranque en frío

¡PRECAUCIÓN!

Siga estos procedimientos cuando la entrada Cortes del suministro de AC., Pero la batería es normal

- Ajuste el interruptor de la batería a la posición “ON” para UPS de largo plazo.
- Encienda el interruptor de alimentación para UPS estándar.
- Encienda el interruptor de salida.
- Active el equipo cambiar (Potencia va a alimentar a la placa de potencia auxiliar).



- Desencadenar la botón de arranque en frío.

Cuando la batería normal, rectificador inicia la operación, 30s posteriores, se inicia inversor y opera y batería LED

¡PRECAUCIÓN!



Por favor, pulse el botón de inicio de cerca después de 30 segundos hasta que se cierre el interruptor de la batería.

Apagar procedimiento

¡ATENCIÓN!



Este procedimiento debe seguirse para apagar completamente el UPS y la carga. Después de que todos los interruptores de alimentación, se abren los aisladores y los interruptores de circuito, no habrá salida.

Modo en línea:

- Pulse OFF para apagar el UPS, esperando aproximadamente 30 segundos.
- Apagar el interruptor BATTERY para UPS de funcionamiento largos. Abra el interruptor de energía de la batería para UPS estándar.
- Apagar el interruptor de entrada.
- Apagar La salida interruptor automático. Los UPS se apagan;
- Para aislar completamente el UPS desde de suministro de AC, todos los interruptores de entrada de utilidad será completamente apagados.
- El panel primario de distribución de entrada, que a menudo se encuentra muy lejos desde el área de UPS, así que una etiqueta debe ser publicado en un lugar visible por el personal de servicio y mantenimiento, que el circuito UPS está en mantenimiento.

Modo batería:

- Pulse OFF para apagar el UPS, esperando aproximadamente 30 segundos.
- Apagar el interruptor BATTERY para UPS de funcionamiento largos. Abra el interruptor de energía de la batería para UPS estándar.
- Apagar La salida interruptor automático. Los UPS se apagan.

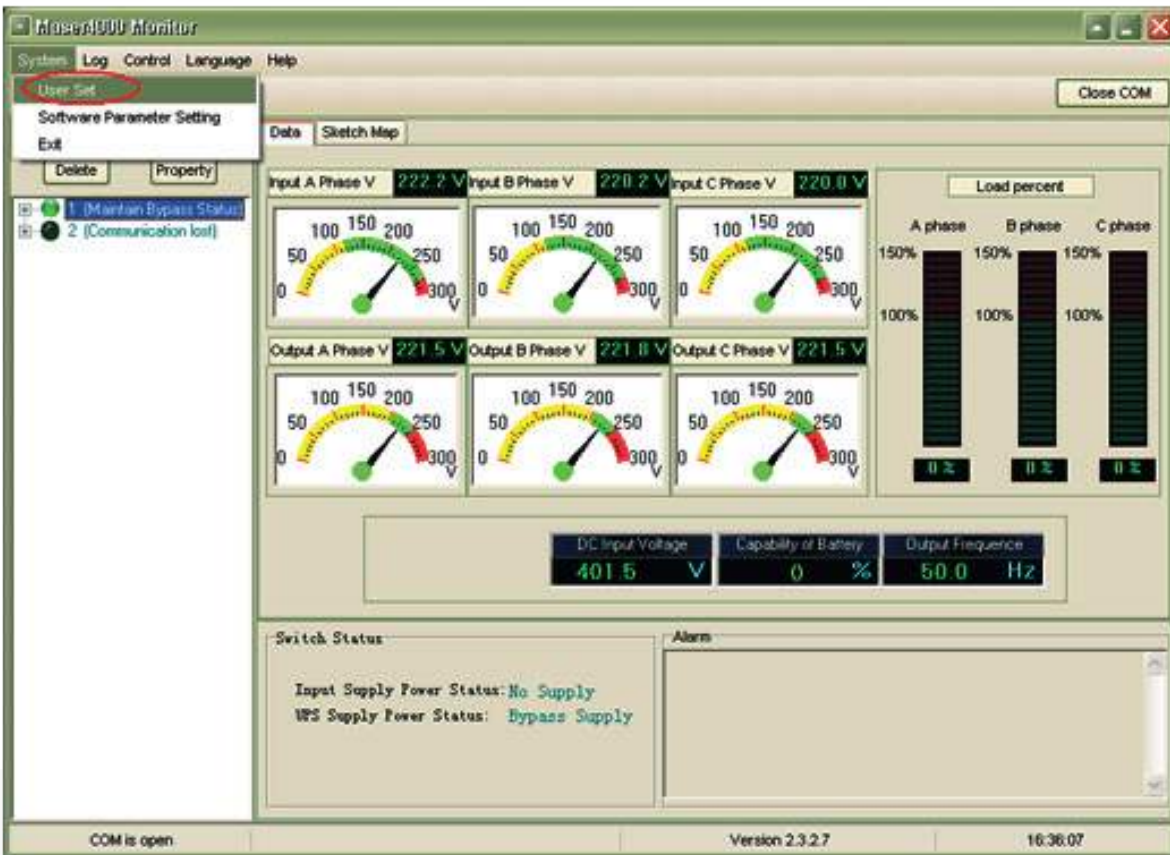
¡ADVERTENCIA!



Espere durante unos 5 minutos para que los condensadores de barras conductoras internas de DC se descarguen completamente.

Configuración en paralelo

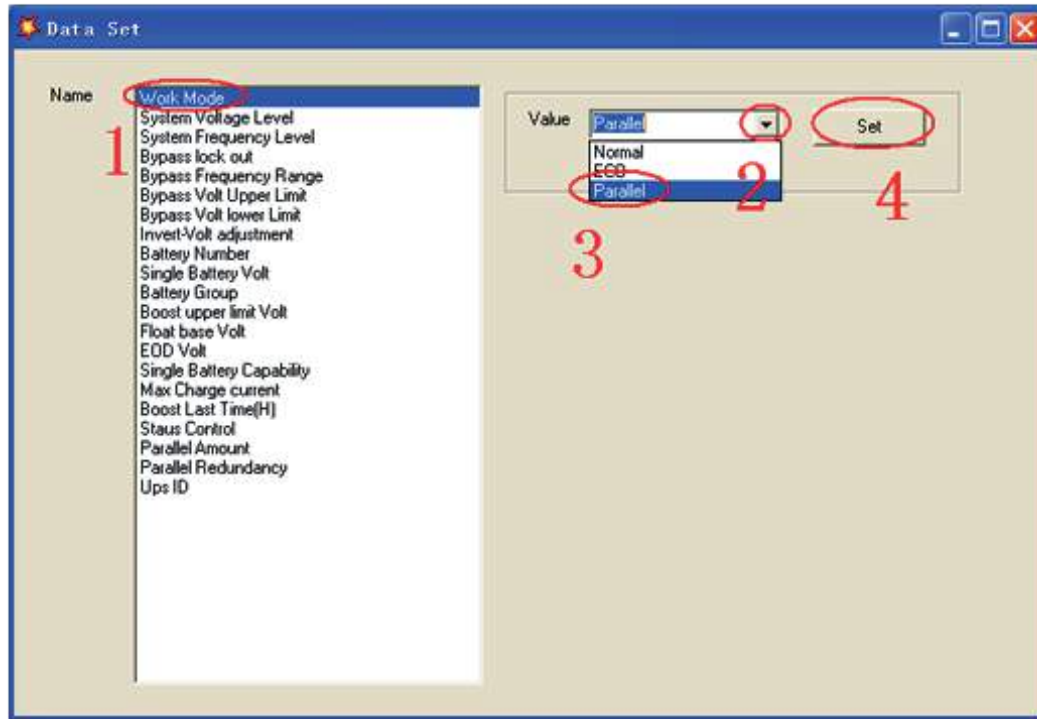
- Conectar la UPS con el ordenador. Encienda el UPS.
- Abra el software Muser4000, después de conectar con la UPS correctamente, haga clic en “Sistema” -> “Set User”



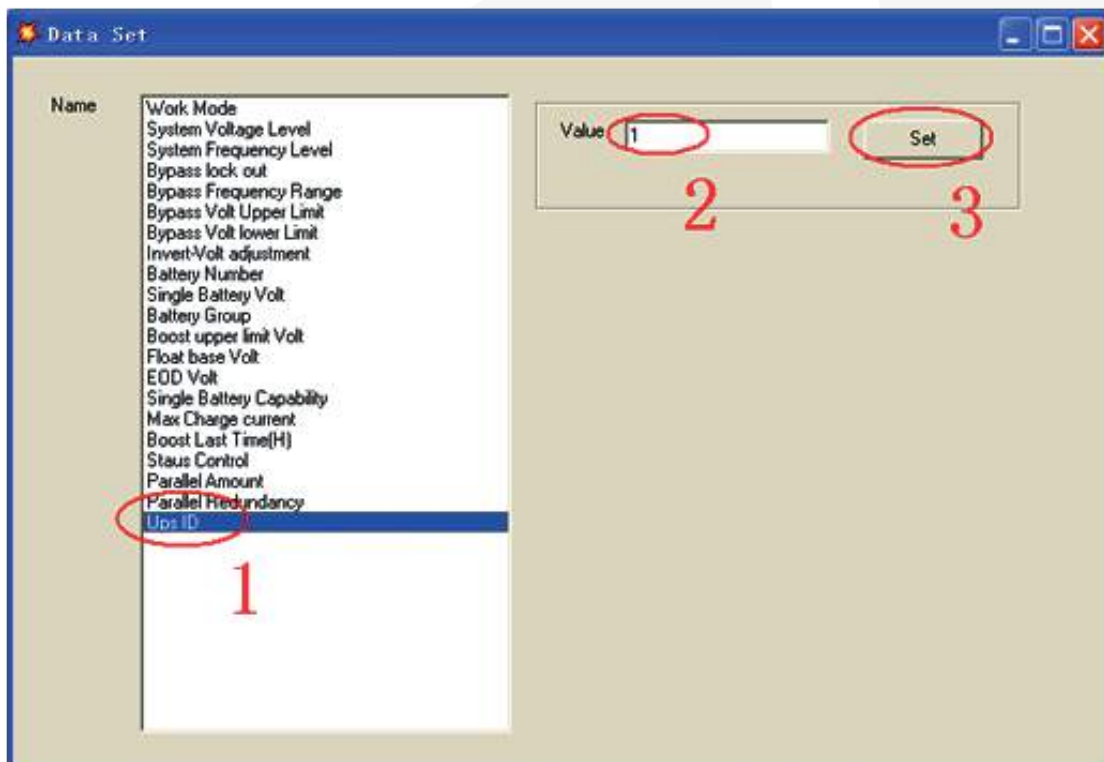
- Haga clic en “Configuración” en la ventana “User Set”;

The screenshot shows the 'User Set' configuration window. The 'Set' button is circled in red. The window contains various configuration options for Work Mode, System Voltage Level, System Frequency Level, Parallel Amount, Bypass lock out, Parallel Redundancy, Bypass Frequency Range, Bypass Volt Upper Limit, Bypass Volt lower Limit, Invert-Volt adjustment, Ups ID, Output, Auto Turn-on, Buzzer, Battery Set, Single Battery Capability(AH), Single Battery Volt.(V), Boost upper limit Volt.(V/Cell), EOD Volt(0.01V/Cell), Battery Group, Boost Charge, Float base Volt.(V/Cell), Max Charge current(A), and Boost Last Time(H).

- En la ventana de “conjunto de datos,” haga clic en “modo de trabajo” , seleccione “paralelo” para el valor, a continuación, haga clic en “Set,” como se muestra en la imagen siguiente. Si el UPS emite un “bip,” eso significa que el ajuste es correcto.



- En la ventana de “conjunto de datos,” haga clic en “Ups ID,” escriba un valor para el ID de UPS en paralelo en el lado derecho, como “1,” a continuación, haga clic en “Set,” como se muestra en la imagen siguiente. Si suena la UPS un “bip,” eso significa que el ajuste es correcto.

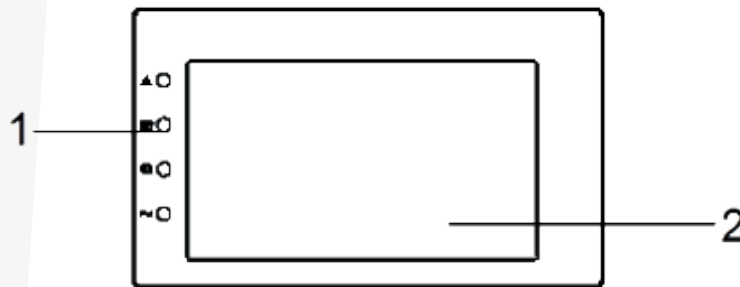


¡PRECAUCIÓN!



Después de cambiar el ID de sistema paralelo, la conexión entre Muser4000 y el equipo podría ser interrumpido. Si esto ocurre, vuelva a conectar de acuerdo con las instrucciones descritas antes.

3.3 La pantalla LCD



Introducción panel de control LCD

(1) LED (de arriba a abajo: “alarma”, “derivación”, “batería”, “inversor”)

(2) LCD monitor

Introducción

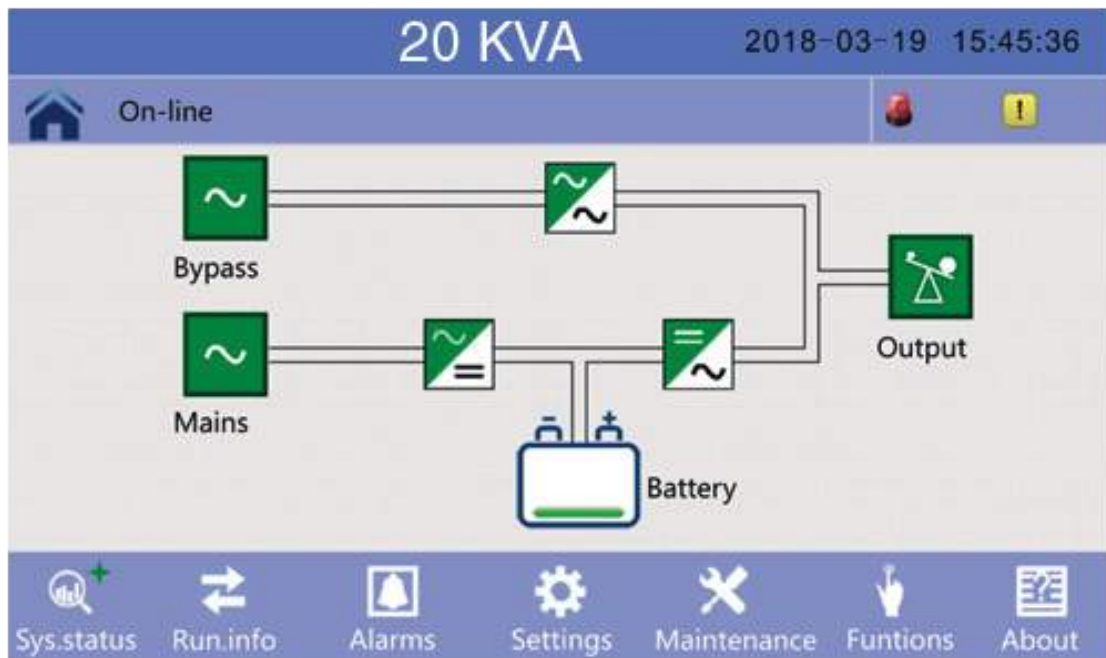
La pantalla proporciona más funciones que las descritas en este manual.

¡PRECAUCIÓN!

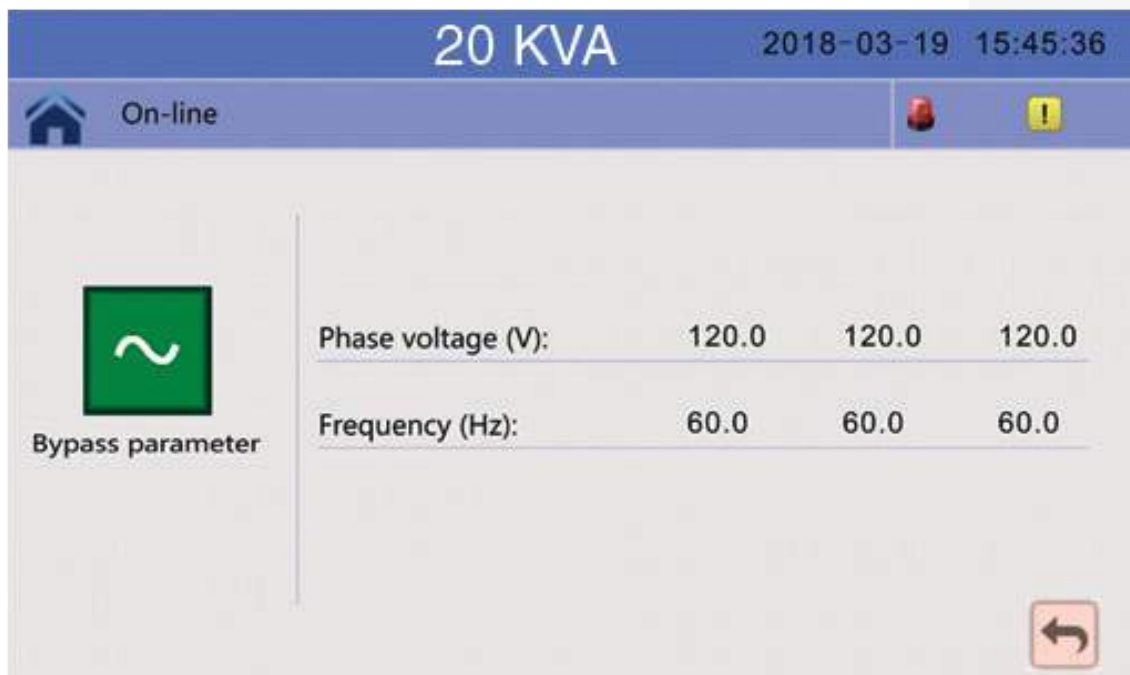


El ajuste de la mayoría parámetro no se puede ajustar cuando el UPS está en el modo inversor.

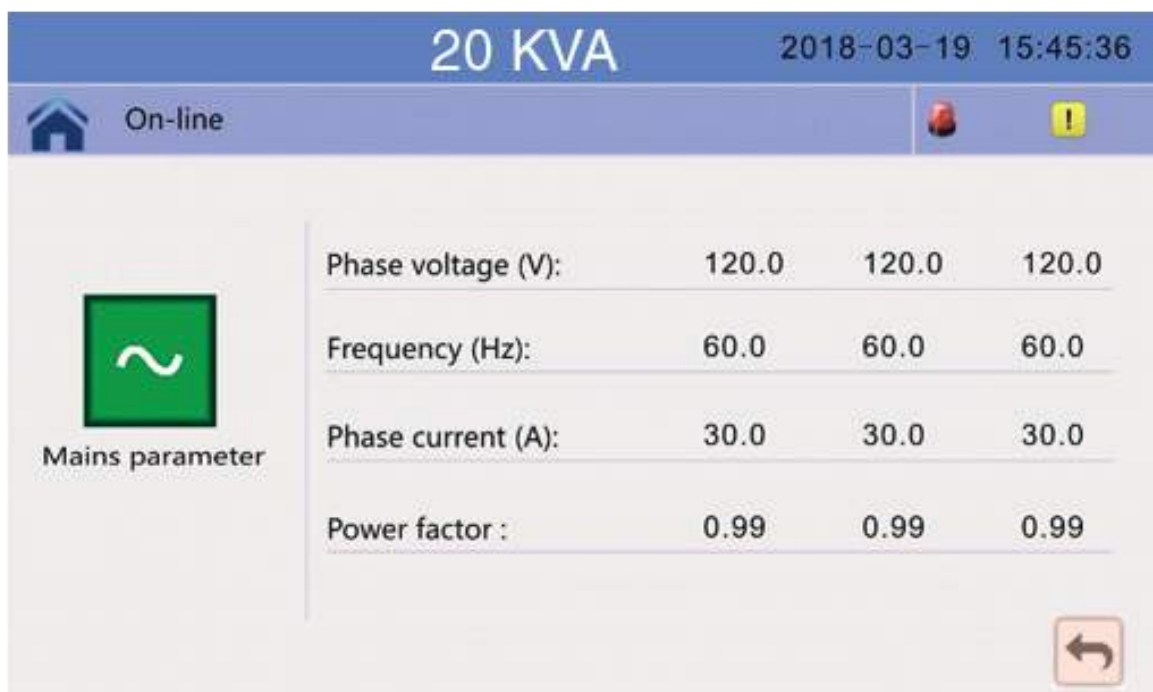
3.3.1 Página de inicio 1, Muestran el funcionamiento de la UPS diagrama de flujoY existen los datos Entrada de entrada, de salida, de la batería.



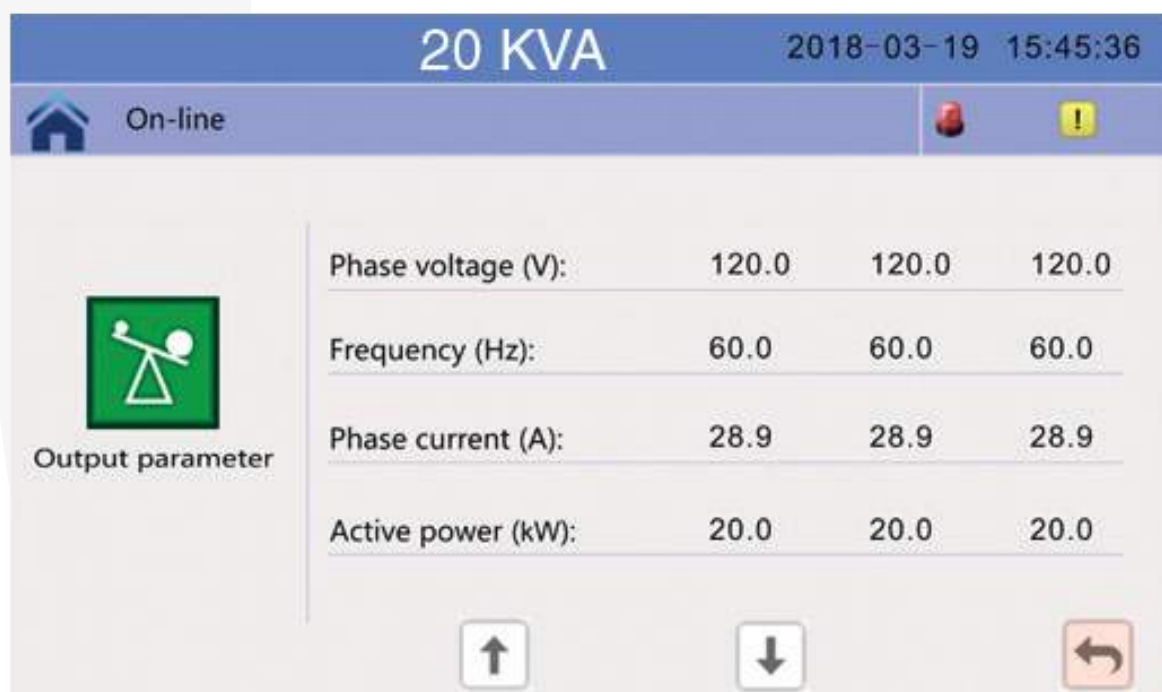
1) Haga clic en el icono de bypass, para entrar en la ventana de datos de derivación, haga clic en la parte de atrás icono volver a la última ventana y haga clic en la página principal icono saltar a la página principal.



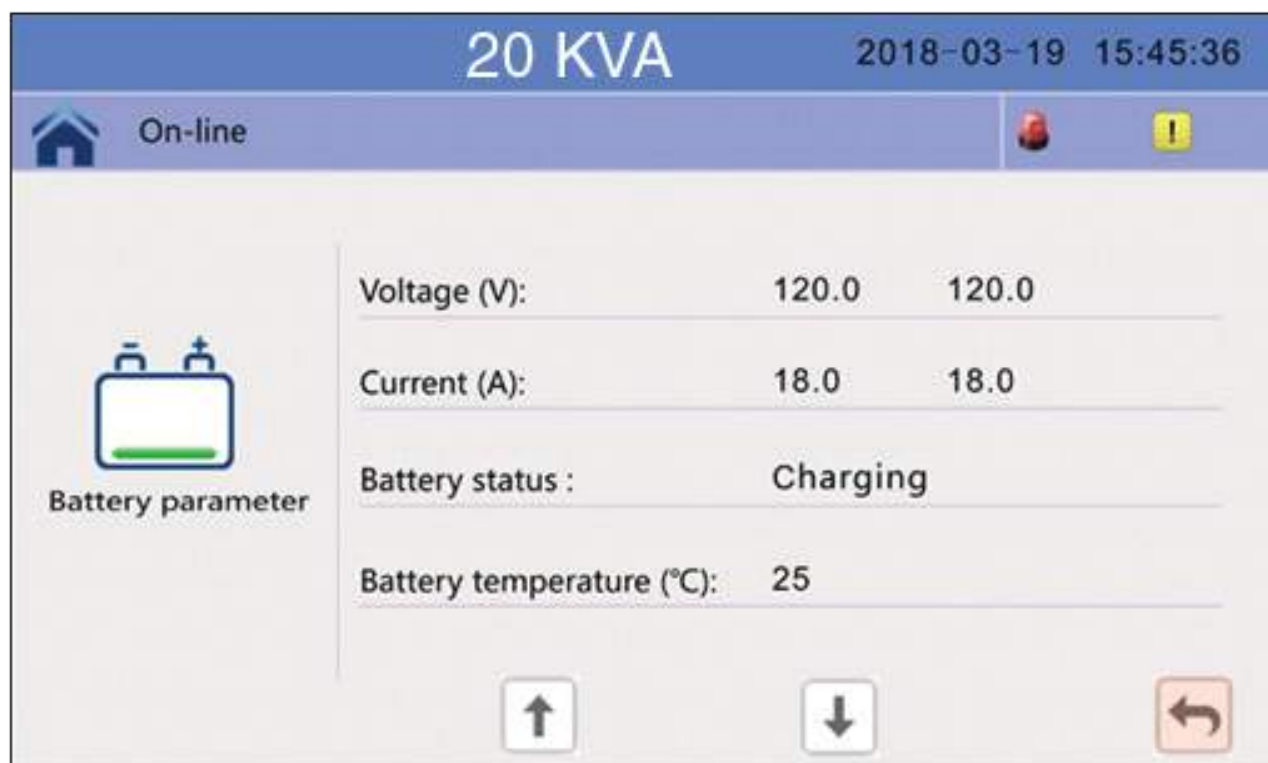
2) Haga clic en la red eléctrica icono para introducir la red eléctrica ventana de datos, haga clic en la parte de atrás icono volver a la última ventana y haga clic en la página principal icono saltar a la página principal.



3) Haga click en la Carga icono para introducir la salida ventana de datos, haga clic en la parte de atrás icono volver a la última ventana y haga clic en la página principal icono saltar a la página principal.



4) Haga clic en la batería icono para introducir el batería ventana de datos, haga clic en la parte de atrás icono volver a la última ventana y haga clic en la página principal icono saltar a la página principal.



3.3.2 Haga clic en el icono de Runn. Info para entrar a la página de información.



1) Haga clic en el icono tiempo de ejecución para introducir el estado ventana de datos, puede ver el estado del interruptor, haga clic en la parte de atrás icono volver a la última ventana y haga clic en la página principal icono saltar a la página principal.



2) Haga clic en la datos ENV icono para entrar El estado ventana de datos, puede ver los datos de la temperatura después de que el sensor de temperatura conectado, haga clic en la parte de atrás icono volver a la última ventana y haga clic en la página principal icono saltar a la página principal.



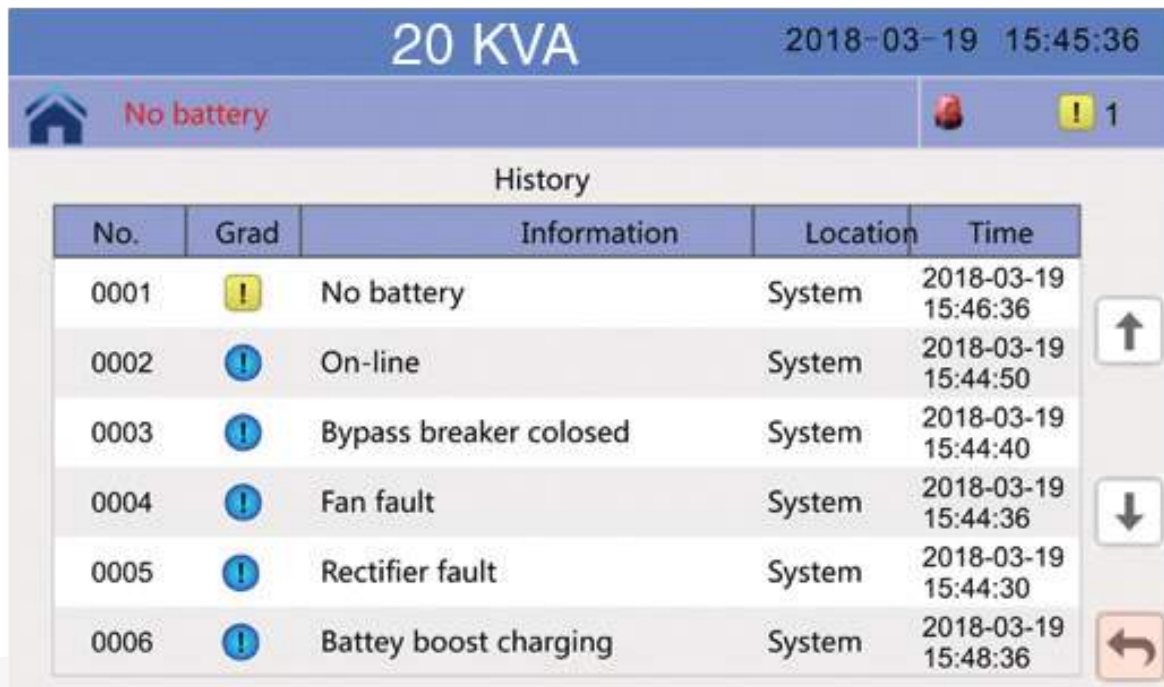
3.3.3 Haga clic en Alarma icono para entrar a la página de alarmas.



1) Haga clic en la alarma activa icono para introducir el módulo ventana de datos, puede ver los datos de alarma, haga clic en la parte de atrás icono volver a la última ventana y haga clic en la página principal icono saltar a la página principal.



2) Haga clic en la historia icono para introducir la ventana de historia, puede ver los datos de la historia, haga clic en la parte de atrás icono volver a la última ventana y haga clic en la página principal icono saltar a la página principal.



No.	Grad	Information	Location	Time
0001	!	No battery	System	2018-03-19 15:46:36
0002	!	On-line	System	2018-03-19 15:44:50
0003	!	Bypass breaker colosed	System	2018-03-19 15:44:40
0004	!	Fan fault	System	2018-03-19 15:44:36
0005	!	Rectifier fault	System	2018-03-19 15:44:30
0006	!	Battey boost charging	System	2018-03-19 15:48:36

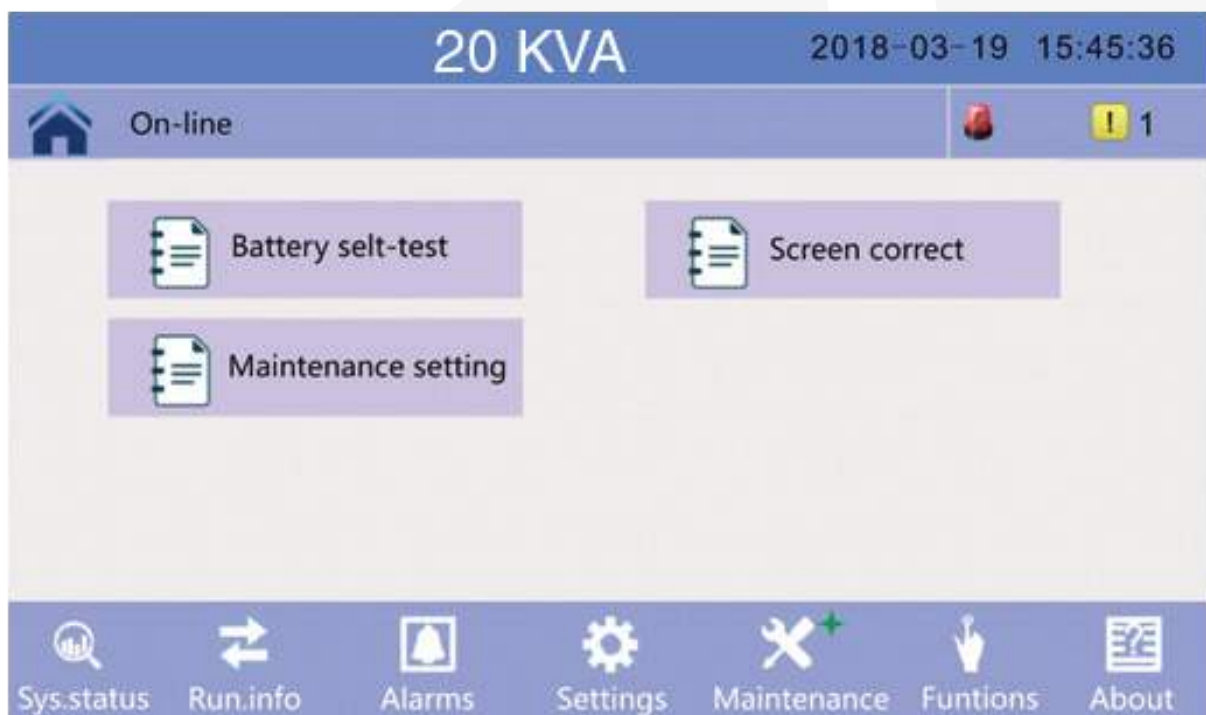
3.3.4 Haga clic en el establecimiento de icono para entrar en la página configurando, haga clic en la parte de atrás icono volver a la última ventana y haga clic en la página principal icono saltar a la página principal



3.3.5 Haga clic en icono de mantenimiento a entrar en la página configurando, haga clic en la parte de atrás icono volver a la última ventana y haga clic en la página principal icono saltar a la página principal



3.3.6 Haga clic en icono de la función de entrar en la página configurando, haga clic en la parte de atrás icono volver a la última ventana y haga clic en la página principal icono saltar a la página principal



3.4 Comisión de sistema paralelo

Sistema paralelo debe encargando cuando el autónomo son todos intactos.

Tomar 4 unidades en paralelo, por ejemplo.

- Confirmar la secuencia de entrada / conexión cables de salida y la fase de entrada son correctos; apague el interruptor de la batería, y medir el voltaje de +/- bate de todos los grupos de la batería son normales.
- Conecte el cable paralelo, debe estar formado conexión de bucle.
- Activar el interruptor de entrada de la unidad 1, y el acceso ajuste de interfaz para establecer el modo de trabajo, ID, número paralelo, número redundante LCD. Requieren establecer el número de serie, la capacidad de la batería. El nivel de tensión de salida y el rango de protección de derivación son configuración predeterminada.
- Apague el interruptor de entrada de la unidad 1, y asegúrese de que el UPS está apagado. Activar el interruptor de entrada de la unidad 2, acceda a la interfaz de configuración de LCD, de configurar el modo paralelo de trabajo, ID (NO.2), paralelas 4 unidades, el número redundante. La otra configuración son los mismos como UPS 1 operación.
- Para las unidades 3 y 4 UPS, el ajuste de funcionamiento son todos los mismos que la unidad 1 y 2.
- A su vez en Bypass / input / disyuntor de salida de todos los UPS en paralelo, a continuación, confirmar todos los ajustes son correctos. Cada UPS tiene su diferente ID adeudado.
- A su vez en todo el interruptor de la batería y confirmar el parámetro (V / I) son normales.
- Conectada la carga y comprobar si la corriente de salida son el equilibrio.
- Encender y apagar el interruptor de utilidad para probar todo el sistema UPS de convertidores de utilidad a la batería y la función restaurada están trabajando hallazgo

3.5 Mensajes de la pantalla / Solución de problemas

Su sección enumera los mensajes de eventos y alarma de que el UPS puede mostrar. Los mensajes se muestran en orden alfabético. Esta sección aparece con cada mensaje de alarma para ayudar a solucionar problemas.

Display mensajes

Estado de funcionamiento y el modo (s)

C

Código	Stand de información para	LED			
		Culpa	Derivación	Batería	Inversor
1	Inicializado	EXTINGUIR	EXTINGUIR	EXTINGUIR	EXTINGUIR
2	Modo de espera	EXTINGUIR	EXTINGUIR	X	EXTINGUIR
3	Ninguna salida	EXTINGUIR	EXTINGUIR	X	EXTINGUIR
4	Modo Bypass	EXTINGUIR	LIGERO	X	EXTINGUIR
5	Modo de utilidad	EXTINGUIR	EXTINGUIR	X	LIGERO
6	Modo batería	EXTINGUIR	EXTINGUIR	LIGERO	EXTINGUIR

7	Batería de auto-diagnóstico	EXTINGUIR	EXTINGUIR	LIGERO	EXTINGUIR
8	Inversor se está iniciando	EXTINGUIR	X	X	EXTINGUIR
9	Modo ecológico	EXTINGUIR	X	X	X
10	EPO	LIGERO	EXTINGUIR	X	EXTINGUIR
11	Modo de derivación de mantenimiento	EXTINGUIR	EXTINGUIR	EXTINGUIR	EXTINGUIR
12	Modo de fallo	LIGERO	X	X	X

PRECAUCIÓN: "X" significa que se determina por otras condiciones

Información de alarmas

Código de fallo	UPS alarma de advertencia	Zumbador	LED
1	Fallo del rectificador	un sonido continuo	Fallo LED Lit
2	Falla del inversor	un sonido continuo	Fallo LED Lit
3	Inversor tiristor corta	un sonido continuo	Fallo LED Lit
4	Tiristor variador roto	un sonido continuo	Fallo LED Lit
5	Tiristor de derivación corta	un sonido continuo	Fallo LED Lit
6	Tiristores de bypass roto	un sonido continuo	Fallo LED Lit
7	fusible roto	un sonido continuo	Fallo LED Lit
8	fallo del relé en paralelo	un sonido continuo	Fallo LED Lit
9	fallo del ventilador	un sonido continuo	Fallo LED Lit
10	reserva	un sonido continuo	Fallo LED Lit
11	error de alimentación auxiliar	un sonido continuo	Fallo LED Lit
12	Falla de Inicialización	un sonido continuo	Fallo LED Lit
13	Culpa cargador P-batería	un sonido continuo	Fallo LED Lit
14	Culpa cargador N-batería	un sonido continuo	Fallo LED Lit
15	Bus sobretensión CC	un sonido continuo	Fallo LED Lit
dieciséis	Bus de CC por debajo del voltaje	un sonido continuo	Fallo LED Lit
17	desequilibrio del bus de CC	un sonido continuo	Fallo LED Lit
18	arranque suave falló	un sonido continuo	Fallo LED Lit
19	Rectificador de temperatura excesiva	Dos veces por segundo	Fallo LED Lit
20	Sobre temperatura del inversor	Dos veces por segundo	Fallo LED Lit
21	pérdida neutra de entrada	Dos veces por segundo	Fallo LED Lit
22	batería inversa	Dos veces por segundo	Fallo LED Lit
23	Error de conexión del cable	Dos veces por segundo	Fallo LED Lit
24	CAN Comm. Culpa	Dos veces por segundo	Fallo LED Lit
25	culpa reparto de carga en paralelo	Dos veces por segundo	Fallo LED Lit
26	Batería sobre voltaje	Una vez por segundo	Fallo intermitente LED
27	Fallo de red de cableado del sitio	Una vez por segundo	Fallo intermitente LED
28	Avería Anulado el cableado del sitio	Una vez por segundo	Fallo intermitente LED

29	Cortocircuito de salida	Una vez por segundo	Fallo intermitente LED
30	Rectificador de corriente excesiva	Una vez por segundo	Fallo intermitente LED
31	Bypass sobre corriente	Una vez por segundo	BPS LED parpadeante
32	Sobrecarga	Una vez por segundo	INV o BPS LED intermitente
33	Sin batería	Una vez por segundo	LED parpadeante de la batería
34	Batería bajo voltaje	Una vez por segundo	LED parpadeante de la batería
35	Pre-aviso de batería baja	Una vez por segundo	LED parpadeante de la batería
36	Error de comunicación interna	Una vez por 2 segundos	Fallo intermitente LED
37	Componente de	Una vez por 2 segundos	INV LED parpadeante
38	Sobrecarga en paralelo	Una vez por 2 segundos	INV LED parpadeante
39	Voltios	Una vez por 2 segundos	Batería LED encendido
40	Frec red. anormal	Una vez por 2 segundos	Batería LED encendido
41	Desviación no disponible		BPS LED parpadeante
42	Bypass incapaz de rastrear		BPS LED parpadeante
43	Inversor en no válido		
44	reserva		
45	inversor no en		
46	interruptor de salida no en	Una vez por 3 segundos	

3.6 opciones

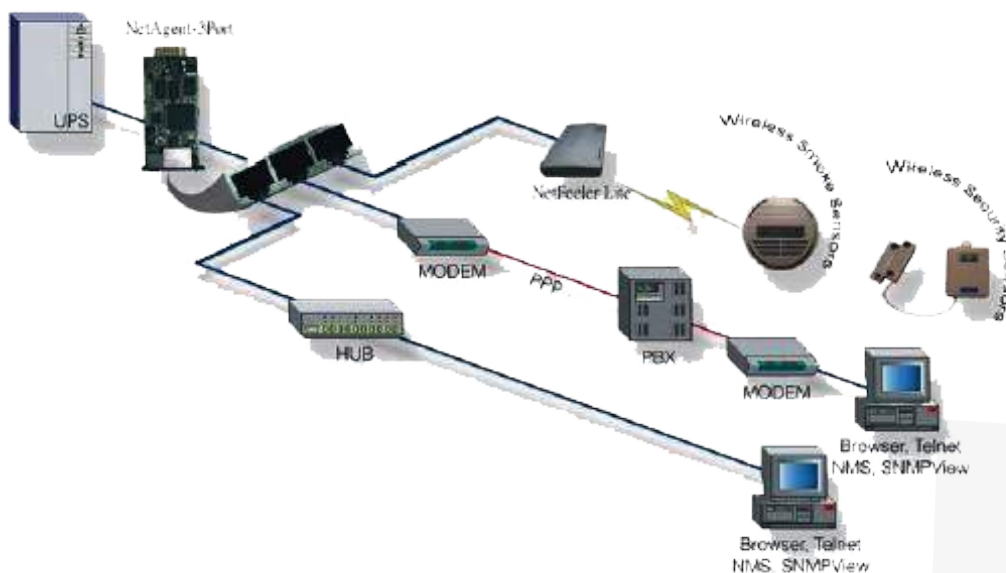
Tarjeta SNMP: SNMP interna / SNMP externo opcional

- Aflojar los 2 tornillos de par (en cada lado de la tarjeta).
- Tire con cuidado de la tarjeta. Invierta el procedimiento de reinstalación

La ranura llamado SNMP soporta el protocolo MEGATEC. Aconsejamos que el puerto NetAgent II-3 es también una herramienta para monitorizar de forma remota y gestionar cualquier sistema UPS

Net Agent II-3Ports soporta la función de módem de acceso telefónico en (PPP) para permitir el control remoto a través de Internet cuando la red no está disponible.

Además de las características de un estándar Net Agent Mini, Net Agent II tiene la opción de añadir Net Feeler Lite para detectar la temperatura, la humedad, el humo y sensores de seguridad. Por lo tanto, haciendo Net Agent II una herramienta de gestión. Net Agent II también soporta múltiples idiomas y está configurado para la detección automática de idioma basado en la web.

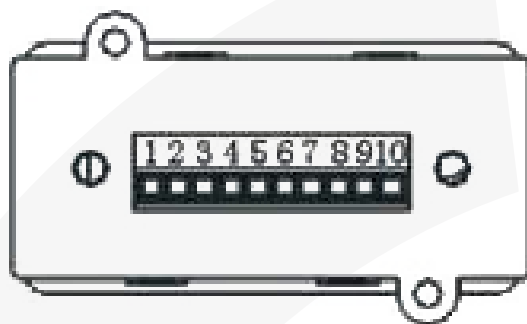


Topología típica de la Red de Gestión de UPS

Tarjeta de relé

Un terminal de 10 pines es compatible para ofrecer las señales de bypass, Cortes del suministro, inversor encendido, batería baja, falla del UPS, UPS de alarma y cierre del sistema UPS. La tarjeta de comunicación de relé contiene seis salidas de contacto seco y una entrada seco. Las entradas y salidas están programadas de fábrica de acuerdo a las funciones enumeradas en la tabla

Tabla: contactos de relé (tarjeta de comunicación)



Alfiler	Función descriptiva	Entrada o salida
1	La falta de utilidad	Salida
2	Batería	
3		
4	Bypass	
5	Falla de UPS	
6	El inversor	
7	Resumen de alarmas	
8	Común	
9	Apagado remoto +	De entrada (5 ~ 12V)

44

Entrada de bypass	Calificación de voltaje CA	208 / 120Vac o 220/127 V CA, 50 / 60Hz, 3-Phase, 4-Wire Plus Ground		
	Rango de voltaje de bypass	Límite superior: + 10, + 15, + 20 o 25% (por defecto: 20)		
		Límite inferior: -10, -20, -30 o -40 (por defecto: -30)		
	Rango de frecuencia de bypass	± 10%		
	Sincronización - Ventana	± 1% / ± 2% / ± 4% / ± 5% / ± 10% opcional (por defecto: ± 10%)		
	actual Max (A)	Breaker 50A	Breaker 63A	Breaker 80A
	la protección contra la corriente, línea de bypass	Interruptor magneto		
	Valoración actual del cable neutro (A)	1,7 x In		
Entrada del generador		Apoyo		
SALIDA				
La salida del variador	Factor de potencia	1.0		
	Tensión nominal de CA 1	208 / 120Vac o 220/127 V CA,		
	Regulación	± 1%		
	Respuesta de tensión transitoria	± 5% (carga lineal)		
	Balance de fase	120 ° ± 1 ° (100% de carga desequilibrada)		
	Frecuencia	1ª línea Modo: sincronizar con entrada; cuando la frecuencia de entrada		
	Factor de cresta	3: 1		
	La distorsión armónica (THD)	<1% (carga lineal), <3% (carga no lineal)		
	Capacidad de sobrecarga	Modo AC	Carga	
Murciélago. Modo		Carga		
Eficiencia	Modo normal	Hasta un 94%		
BATERÍA				

Batería	Voltaje de la batería	La unidad estándar	± 120Vdc (20pcs 12V9AH); (2x20pcs 12V9AH);	± 120Vdc (2x20pcs 12V9AH); (3x20pcs 12V9AH opcional)	± 120Vdc (3x20pcs 12V9AH);
		Unidad de largo plazo	± 96V \ ± 108V \ ± 120 V \ ± 132 V \ ± 144Vdc; cantidad de batería (opcional)		
	Tensión de flotación	2.25V / célula (seleccionable de 2.20-2.29V / célula) modo de carga de corriente constante y tensión constante			
	Impulsar voltaje de carga	2.30V / célula (seleccionable de 2.30-2.40V / célula) modo de carga de corriente constante y tensión constante			
	Final de la descarga	1,75 V / célula (seleccionable de 1,60 o 1.90V / célula)			
	Corriente de carga (A) (corriente de carga se puede ajustar de acuerdo con la capacidad de la batería instalada)	Unidad estándar: 1.35A (2,7; 4.05A opcional) largo unidad de ejecución: Max. 20A actual (limitado por la corriente de entrada)	Unidad estándar: 2.7A (4.05A opcional) Unidad de largo plazo: Max. 20A actual (limitado por la corriente de entrada)	Unidad estándar: 4.05A unidad de largo plazo: Max. 20A actual (limitado por la corriente de entrada)	
CARACTERÍSTICAS DEL SISTEMA					
Tiempo de transferencia	En la transferencia sincronizada	Utilidad de la batería: 0 ms; Utilidad para pasar por alto: 0 ms			
	La transferencia asincrónica	Transferencia asíncrono: 15 ms (50 Hz), 13.3ms (60 Hz)			
Alarmas	Sobrecarga, la utilidad anormal, mal funcionamiento del UPS, batería baja, etc.				
Protección	Corto circuito, sobrecarga, sobre temperatura, batería baja, alarma de fallo de ventilador.				
Interface de comunicación	USB, RS232, RS485, puerto paralelo, contacto y ranura inteligente, tarjeta de SNMP (opcional), la tarjeta de relé (opcional), sensor de temperatura de la batería (opcional)				
AMBIENTAL					
Ambiente	Temperatura de funcionamiento	0			
	Temperatura de almacenamiento	-25			
	Humedad	0 ~ 95% sin condensación			
	Ruido acústico	<55dB de 1M distancia		<58dB de 1M distancia	
	Altitud	<1500m.When> 1500m, menor será la potencia nominal para su uso			
FÍSICO					
Dimensión D x W x H (mm)	900x250x868				
Peso neto / kg)		136/77	188/78	239/79	
NORMAS					

Certificaciones de seguridad	UL 1778, IEC / EN 62040-1, IEC / EN 60950-1
EMC	FCC Parte 15: 2015, IEC / EN62040-2, IEC61000-4-2, IEC61000-4-3, IEC 61000-4-4, IEC61000-4-5, IEC61000-4-6, IEC61000-4-8

Coincidencia paquete de la batería		
Modelo	Peso (Kg)	Dimensión D x W x H (mm)
norte	260	900x250x868
norte	261	900x250x868

Apéndice 2 Problemas y soluciones

En caso de que la UPS no pueda trabajar normalmente, podría ser mal en la instalación, el cableado o la operación compruebe todos los aspectos, pasos para su instalación y encendido estén bien en primer lugar. Si todos estos aspectos se verifican sin ningún problema consulte con el agente local de inmediato y proporcione información a continuación.

1. Nombre del modelo y número de serie.
2. Trate de describir el fallo con más detalles, tales como información de pantalla LCD, LED luces de estado, etc.

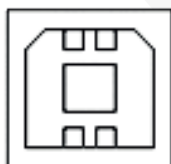
Lea el manual del usuario, que puede ayudar mucho para el uso de este UPS de la manera correcta. FAQ (preguntas más frecuentes) puede ayudar a solucionar el problema fácilmente.

No.	Problema	Razón posible	Solución
1	Utilidad es conectado, pero la UPS no puede ser encendida.	La alimentación de entrada no está conectado; bajo voltaje de entrada; El switch entrada de la UPS no está encendido.	Medir la tensión de entrada UPS / frecuencia está dentro de la ventana. Compruebe si la entrada del UPS está encendido
2	Utilidad normal, pero el indicador LED no luz enciende, la UPS opera en el modo de batería	Los interruptores de entrada de la UPS no está encendido; cable de entrada es no bien conectado	Activar el interruptor de entrada; Asegúrese de que el cable de entrada es bien conectado.
3	Las UPS no indica ninguna falla, pero la salida no tiene tensión	Cable de salida no está bien conectado; Disyuntor de salida no se ha encendido	Asegúrese de que el cable de salida esté bien conectado; Active el interruptor de salida.
4	LED de batería está parpadeando, pero sin tensión de carga y la corriente	Interruptor de la batería no se enciende, o se deterioran las baterías, o la batería se conecta a la inversa. El número y la capacidad de la batería no se ajustan correctamente.	Si la UPS opera en modo de batería, verifique la tensión de entrada y verifique el tiempo de autonomía restante necesario para su sistema.

5	LED de batería está parpadeando, pero sin tensión de carga y la corriente.	<p>Interruptor de la batería no se enciende, o se deterioran las baterías, o la batería se conecta a la inversa.</p> <p>El número y la capacidad de la batería no se ajustan correctamente.</p>	Encender el interruptor de la batería. Si la UPS ES son dañado, necesitará reemplazar las baterías de todo el grupo, desconecte los cables de la batería correctamente; Ir a la configuración de la pantalla LCD la el número y la capacidad de la batería, el conjunto de datos correctos.
6	Buzz pitido cada 0,5 segundos y Pantalla LCD "sobrecarga de salida"	Sobrecarga	Quitar algo de carga
7	Buzzer pitido largos, Pantalla LCD de código de error "29"	los salida del UPS es en cortocircuito	Asegúrese de que la carga no está dentro cortocircuito y reinicie el UPS.
8	El UPS sólo funciona en el modo de derivación	El UPS está definido en modo ECO	Establecer el UPS a modo de trabajo Modo normal
9	No se puede iniciar Negro	<p>interruptor de la batería es mal cerrada: fusible de la batería no está abierto: O Batería baja:</p> <p>La cantidad de batería ajustado de manera incorrecta; Interruptor de alimentación en el panel trasero se enciende.</p>	Cierre el interruptor de la batería: Cambiar el fusible: Recargar la batería: Encienda el UPS con el AC para establecer la cantidad y cantidad de batería; Active el interruptor de alimentación.
10	Zumbador suena continuamente y la pantalla LCD indica 1,3,5,9,15, etc. códigos de fallo	UPS está fuera de servicio	Consulte con su agente local para su reparación

Apéndice 3 Puerto de comunicación USB definición

Definición de Puerto:



Conexión entre el puerto USB del PC y el puerto USB del UPS.

Puerto USB del PC	Puerto USB UPS	Descripción
Pin 1	Pin 1	PC: + 5V
Pin 2	Pin 2	PC: señal de DPLUS
Pin 3	Pin 3	PC: señal de DMINUS
Pin 4	Pin 4	Tierra de la señal

Función disponible de USB

- Monitor de estado de la alimentación del UPS.
- Datos de alarma del monitor de UPS.
- Parámetros de funcionamiento del monitor de UPS.
- Sincronización de encendido / apagado el establecimiento.

Formato de datos de comunicación

----- Velocidad de transmisión 9600 bps

Longitud en bytes de 8 bits -----

Poco extremo ----- 1 bit

Comprobación de paridad ----- ninguno

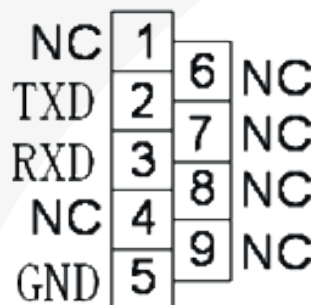


¡PRECAUCIÓN!

USB, RS232 y RS485 no se pueden utilizar al mismo tiempo, sólo se puede utilizar uno de ellos a la vez.

Apéndice 4 puerto de comunicación RS232 definición

Definición de puerto macho:



La conexión entre el puerto RS232 del PC y el puerto RS232 del UPS

Puerto de la PC RS232	UPS puerto RS232	
Pin 2	Pin 2	UPS
Pin 3	Pin 3	Ordenador personal
Pin 5	Pin 5	Suelo

Función disponible de RS232

- Monitor de estado de la alimentación del UPS.
- Datos de alarma del monitor de UPS.
- Parámetros de funcionamiento del monitor de UPS.
- Sincronización de encendido / apagado el establecimiento.

Formato de datos RS-232 de comunicación

----- Velocidad de transmisión 9600 bps

Longitud en bytes de 8 bits -----

Poco extremo ----- 1 bit

Comprobación de paridad ----- ninguno



¡PRECAUCIÓN!

USB, RS232 y RS485 no se pueden utilizar al mismo tiempo, sólo se puede utilizar uno de ellos a la vez.

Apéndice definición de puerto de comunicación RS-485 5

Definición de Puerto:



La conexión entre el Dispositivos puerto RS485 y el puerto RS485 UPS.

Dispositivo	UPS	Descripción
Pin 1	Pin 1	485
Alfiler	Alfiler	485
Pin7	Pin7	+ 12Vdc
Pin8	Pin8	GND

Función disponible de RS485

- Monitor de estado de la alimentación del UPS.
- Datos de alarma del monitor de UPS.
- Parámetros de funcionamiento del monitor de UPS.
- Sincronización de encendido / apagado el establecimiento.
- Entorno de monitorización de la temperatura de la batería.
- Carga de modulación de tensión en función de la temperatura baterías

Formato de datos de comunicación

----- velocidad de transmisión 9600 bps

Longitud en bytes de 8 bits -----

Poco extremo ----- 1 bit

Comprobación de paridad ----- ninguno



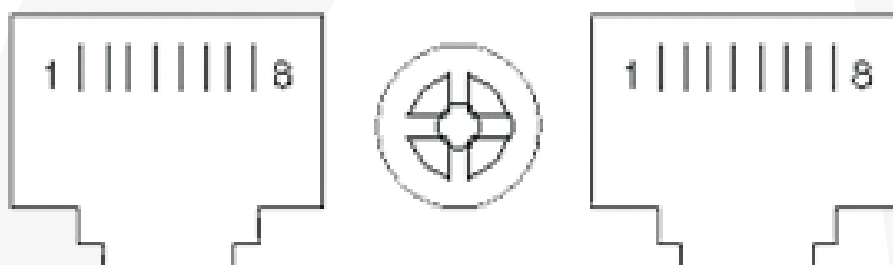
¡PRECAUCIÓN!

USB, RS232 y RS485 no se pueden utilizar al mismo tiempo, sólo se puede utilizar uno de ellos a la vez.

Puerto RS485 pin7 es 12Vdc!

Apéndice definición de puerto de comunicación 6 BAT_T

Definición de Puerto:



La conexión entre el sensor Temperatura RJ45 babor y UPS RJ45 Puerto.

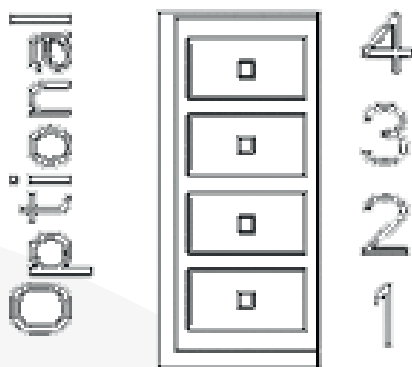
Senador de la temperatura	UPS BAT_T (RJ45)	Descripción
Alfiler	Alfiler	TX
Alfiler	Alfiler	RX
Alfiler	Alfiler	12V
Alfiler	Alfiler	GND

Función disponible de BAT_T

- Entorno de monitorización de la temperatura de la batería.
- Carga de modulación de tensión en función de la temperatura baterías.

Apéndice 7 Opcional definición de puerto

Definición de puerto macho:



Instrucción:

Relé de contacto seco Puerto 5A / 277VAC

UPS	Instrucción
Pin1	Normalmente, Carolina del Norte
Pin2	Normalmente NO
Pin3	/
Alfiler	Común

Función 1 Descripción (por defecto, puente J6 interno):

- Conducir el disyuntor de derivación cuando retroalimente la alarma.

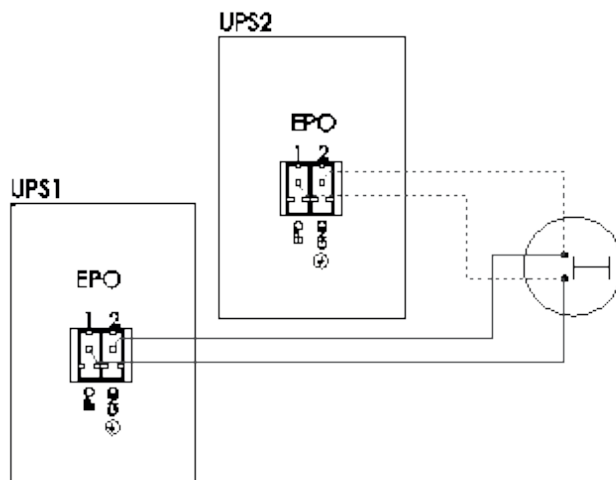
Función 2 Descripción (opcional, puente J5 interno):

- Conducir el batería interruptor automático cuando el voltaje de batería baja.

8 Apéndice Instrucciones de EPO

Definición de Puerto:

Diagrama de conexión:



La conexión entre el botón y UPS REPO Puerto.

Botón	UPS REPO	Descripción
Alfiler	Alfiler	EPO
Alfiler	Alfiler	GND

- Un interruptor de parada de emergencia remoto (señal de contacto seco y “normalmente abierto” - no incluido) se pueden instalar en un lugar remoto y conexión a través de simples cables al conector de REPO.
- El interruptor remoto puede estar conectado a varios UPS en una arquitectura paralela permitiendo que el usuario detiene todas las unidades a la vez.







POWERST®

8.3. MANUAL DEL USUARIO SWITCHES - ARUBA



HPE Networking Instant On 1930 Switch Series

Management and Configuration Guide

Instant 

Published: November 2024

Edition: 3.1.0



Hewlett Packard
Enterprise

Copyright Information

© Copyright 2024 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, please check if the code is available in the HPE Software Center at <https://myenterpriselicense.hpe.com/cwp-ui/software> but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd, Spring, TX 77389
United States of America



Chapter 1: About This Document	5
Applicable Products	5
Latest Version Available Online	5
Related Documents	5
Supported Features	6
Chapter 2: Getting Started	8
Connecting the Switch to the Network	8
Selecting Local Web Management Mode	9
Getting Started With the Web Interface	10
Chapter 3: Dashboard	17
Chapter 4: Setup Network	24
Get Connected	24
System Time	28
User Management	32
Schedule Configuration	38
Chapter 5: Switching	43
Port Configuration	43
Port Mirroring	50
Loop Protection	52
IGMP Snooping	54
SNMP	62
Interface Auto Recovery	75
Trunk Configuration	78
EEE Configuration	82
Chapter 6: Spanning Tree	85
Global Settings	85
CST Configuration	89
MSTP Configuration	93
Chapter 7: VLAN	100
VLAN Configuration	100
Voice VLAN Configuration	106
Chapter 8: Neighbor Discovery	110
LLDP	110
LLDP-MED	117

Chapter 9: Power Over Ethernet	123
PoE Configuration	123
Chapter 10: Routing	131
Routing Configuration.....	131
DHCP Relay	140
ARP Table.....	143
Chapter 11: Quality of Service (QoS)	146
Access Control Lists	146
Class of Service	154
Chapter 12: Security	161
RADIUS Configuration	161
Port Access Control	165
Port Security	175
Protected Ports	178
DHCP Snooping	179
ARP Attack Protection	183
Denial of Service Protection	187
HTTPS Certificate	191
Chapter 13: Diagnostics	197
Logging.....	197
Ping	201
Traceroute	204
Support File	207
Cable Test.....	209
MAC Table	211
RMON	212
Chapter 14: Maintenance	221
Dual Image Configuration	221
Backup and Update Files	222
Configuration File Operations	224
Reset	225
Chapter 15: Support	228
Websites	228
Accessing HPE Networking Support	228
Accessing Updates.....	228
Warranty Information	229
Regulatory Information	229
Documentation Feedback	229



Chapter 1

About This Document

The HPE Networking Instant On 1930 Switch Series are designed to meet the needs of small business network environments — simple to set up and manage and are secure and reliable. HPE Networking Instant On deployments can be managed through a mobile application supported on iOS and Android, through a cloud portal that is accessible through a web browser, or using a local web GUI. This manual details using the web GUI to manage the switch.

Applicable Products

This guide applies to these products:

- HPE Networking Instant On 1930 8G 2SFP Switch
- HPE Networking Instant On 1930 8G Class4 PoE 2SFP 124W Switch
- HPE Networking Instant On 1930 24G 4SFP/SFP+ Switch
- HPE Networking Instant On 1930 24G Class4 PoE 4SFP/SFP+ 195W Switch
- HPE Networking Instant On 1930 24G Class4 PoE 4SFP/SFP+ 370W Switch
- HPE Networking Instant On 1930 48G 4SFP/SFP+ Switch
- HPE Networking Instant On 1930 48G Class4 PoE 4SFP/SFP+ 370W Switch

Latest Version Available Online

Updates to this document can occur after initial publication. For the latest versions of product documentation, see the links provided in the Websites chapter of this document or visit the HPE Networking Instant On Support site at:

<https://community.arubainstanton.com>

Related Documents

- *HPE Networking Instant On 1930 Installation and Getting Started Guide*
- *START HERE: Installation, Safety, and Regulatory Information for the HPE Networking Instant On 1930 Switches*
- *HPE Instant On User Guide*

Supported Features

HPE Networking Instant On 1930 Switch Series switches include support for the following:

- IEEE 802.3 10BASE-T
- IEEE 802.3u 100BASE-TX
- IEEE 802.3ab 1000BASE-T
- Cable Test
- HTTP and HTTPS sessions (5 sessions total)
- 16,384 MAC entries
- MAC aging (configurable)
- IEEE 802.3af: Power over Ethernet
- IEEE 802.3at
- IEEE 802.3x: Flow control
- IEEE 802.1Q: VLANs
- IEEE 802.1p
- ACLs (named ACL - IPv4 and MAC). Up to 100 ACLs. No limit to number of ACLs per interface
- Access Control Entries (ACEs) - up to 480
- IEEE 802.1D: Spanning Tree Protocol
- IEEE 802.1W: Rapid Spanning Tree Protocol
- IEEE 802.1S: Multiple Spanning Tree Protocol supporting 8 MST instances
- IEEE 802.1AB: Link Layer Discovery Protocol (LLDP and LLDP-MED)
- Trunk (LAG) support
 - LAGs
 - 8 port units: up to 4 LAGS - up to 4 active port members in each
 - 24 port units: up to 8 LAGS - up to 8 active port members in each
 - 48 port units: up to 16 LAGS - up to 8 active port members in each
 - IEEE 802.3ad: Link aggregation (LACP). The number of LACP candidate ports is twice the number of supported active port members in the LAG.
 - Static Trunks
- Jumbo packet support (9216 bytes)
- Auto-MDI/MDIX
- Storm Control (global)
- Ingress Rate Limiting (per port)
- Port Mirroring
- IGMP Snooping v1/v2
- Global time scheduler (3 schedules)
 - PoE
 - Port shutdown
 - Access Control Entries (ACE)
- Static IPv4 address assignment - up to 32 interfaces
- Static IPv6 address assignment - on the management interface
- DHCP client
- DHCP fallback

- User Accounts (up to 5, Read/write, Read only)
- Password management (aging, lockout, strength check, key word exclusion)
- SNMPv1/v2c/v3
- RMON (groups: Alarm, Event, History & Statistics)
- RADIUS (up to 4 combined RADIUS authentication / accounting servers)
- RADIUS Accounting
- RADIUS assigned VLANs
- RADIUS MAC authentication (EAP equivalent to “RADIUS”, MD5)
- 802.1x port based access control
- 802.1x Guest VLAN
- 802.1x MAC authentication - configurable username and password
- Port Security
- Protected Ports
- ARP Attack Protection
- DoS Protection
- SNTP (RFC 2030)
- Loop Protection
- IEEE 802.3az: Energy Efficient Ethernet
- IPv4 Static Routing - 32 route entries
- Routing (VLAN, Interface)
- DHCP Relay (IPv4)
- DHCP snooping
- ARP table – 509 entries
- 802.1p/DSCP priority to queue mapping
- Number of egress queues (traffic priority) – 4
- 802.1p port based priority
- Auto Voice VLAN
- Ping (IPv4/IPv6)
- Traceroute (IPv4/IPv6)
- Dual image support
- Firmware Update over HTTP, HTTPS, TFTP, SCP
- Configuration File backup / restore
- Syslog Log (local & remote)
 - 1 remote syslog server
 - Up to 1000 entries on Buffered log
 - Up to 200 in Log file (Flash)

Chapter 2

Getting Started

This chapter describes how to make the initial connections to the switch and provides an overview of the web interface.

Connecting the Switch to the Network

To enable remote management of the switch through a web browser, the switch must be connected to the network. By default, the switch is configured to acquire an IP address from a DHCP server on the network. If the switch does not obtain an address from a DHCP server, the switch will be assigned the IP address 192.168.1.1.



To use DHCP for IP network configuration, the switch must be connected to the same network as the DHCP server. You will need to access your DHCP server to determine the IP address assigned to the switch. The switch supports LLDP (Link Layer Discovery Protocol), allowing discovery of its IP address from a connected switch or management station. If DHCP is used for configuration and the switch fails to be configured, the IP address 192.168.1.1 is assigned to the switch interface.

To access the web interface on the switch, using the default IP address:

1. Connect the switch to the management PC or to the network using any of the available network ports.
2. Power on the switch.
3. Set the IP address of the management PC's network adapter to be in the same subnet as the switch. For example, set it to IP address 192.168.1.2, mask 255.255.255.0.
4. Enter the IP address 192.168.1.1 in the web browser. See **Browser Support** for web browser requirements.

Thereafter, use the web interface to configure a different IP address or configure the switch as a DHCP client so that it receives a dynamically assigned IP address from the network.

After the switch is able to communicate on your network, enter its IP address into your web browser's address field to access the switch management tool, interface or features.

Browser Support

The following browsers, with JavaScript enabled, are supported:

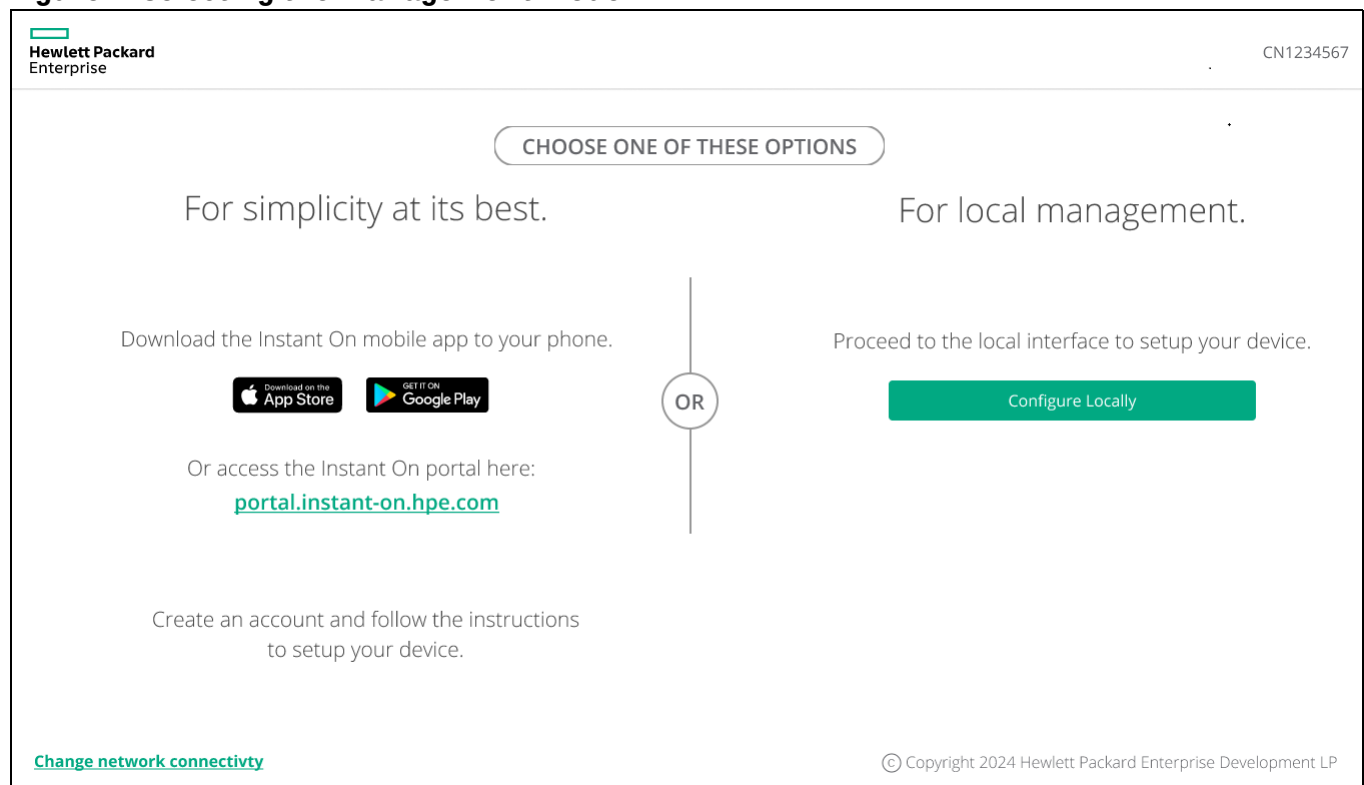
Table 1: Browser Support

Browser	Version
Firefox	104 105 (latest - 105.0.1)
Chrome	105 106 (latest - 106.0.5249.61)
Safari	15.0 (MacOS only)
Edge	105 (latest - 105.0.1343.50), (Win10 only)

Selecting Local Web Management Mode

Upon first connecting directly to the switch, you are presented with a welcome page indicating the choice to manage the switch locally using the web interface (detailed in this guide). In addition the welcome page outlines instructions to create and configure a portal account. Simply follow the instructions provided in the links to create, activate and connect your switch to the cloud portal.

Figure 1: Selecting the Management Mode



The screen captures shown in this document were taken from a sample system, with sample values.

Select **Configure Locally** to manage the switch locally using the web interface and continue on in this guide. If you would rather use the Aruba Instant On Cloud Portal to manage the switch, see the *HPE Networking Instant On 1930 Switch Series Installation and Getting Started Guide* and the *HPE Networking Instant On User Guide*.

Getting Started With the Web Interface

This section describes how to log on to the switch and provides information about the page layout.

Logging On

Follow these steps to log on through the web interface:

1. Open a web browser and enter the IP address of the switch in the web browser address field.
2. On the Login screen, enter the username and password (if one has been set), and then click **Log In**. On the initial login, the username is **admin** and there is no password.
3. Following the initial login, you are prompted to update the username and password.
4. Once the username and password are updated, you are required to login again using the newly configured username and password.



To set the password or change the username, see [User Management](#).

Figure 2: Login Screen

A screenshot of the login screen for the HPE Networking Instant On 1930 8p Gigabit 2p SFP Switch JL680A. The screen features the Hewlett Packard Enterprise logo in the top left corner. The main heading is 'Instant On' with a power icon. Below this, the device model 'HPE Networking Instant On 1930 8p Gigabit 2p SFP Switch JL680A' is displayed. There are two input fields: 'Username' and 'Password'. A blue 'LOGIN' button is positioned below the password field. At the bottom, there is a link for 'Instant On Community' and a copyright notice: '© Copyright 2019-2024 Hewlett Packard Enterprise Development LP'.

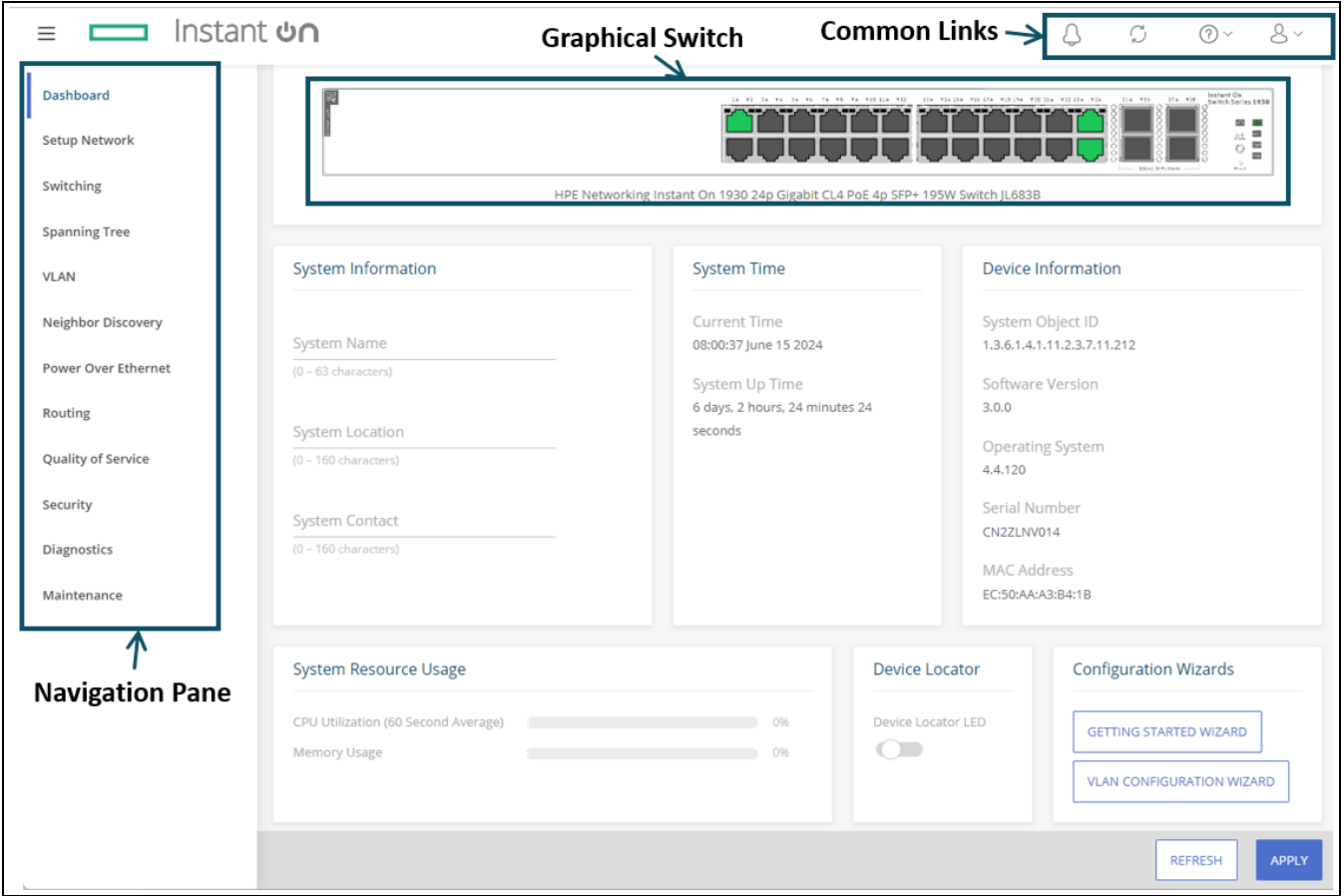
GUI Interface Layout and Features

The Dashboard displays when you first log on and when you click **Dashboard** in the navigation pane. See [3](#) for more information.

You can click the **Setup Network** link beneath **Dashboard** to display the **Get Connected** page, which you use to set up a management connection to the switch. See [Get Connected](#) for more information.

The graphical switch displays summary information for the switch LEDs and port status. For information on this feature see [Switch Panel View](#).

Figure 3: Interface Layout and Features

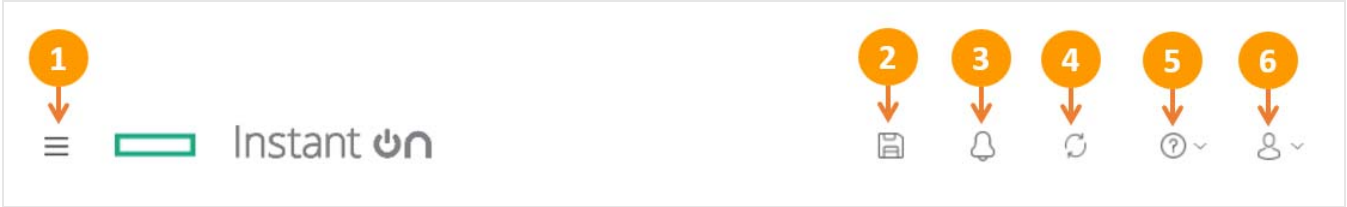


Click on any topic in the navigation pane to display related configuration options.

Common Page Elements

The upper panel includes the following buttons that are common to all the screens:

Figure 4: Upper Panel



Use the buttons to do the following:

Table 2: Upper Panel Components

Label	Description
1	Click Show Navigation  to toggle the navigation pane that shows all the screens that are available for the switch.
2	Click Save Configuration  to save the current configuration. This icon appears only when there are unsaved changes.
3	Click Notification  to view the latest notifications on the system in a panel that appears on the right side of the screen. Click again to close the panel. The notification has the following modes <ul style="list-style-type: none">• Grey: If there are no unread logs of severity Warning or higher.• Orange: If there are unread logs of severity Warning, but no unread logs of a higher severity.• Red: If there are unread logs of severity Error or higher.
4	Click Refresh  to refresh the screen.
5	Click Help  on any page to display a help panel that explains the fields and configuration options on the page.
6	Click Profile  to view your profile information, or to log out.



If there is a recovery from an unexpected restart, an  icon appears in the upper panel. Click the icon to go to the logging page which should provide additional information on the crash.

The bottom of the screen includes the following buttons:

- Click  to send the updated configuration to the switch. Applied changes update the switch running configuration and take effect immediately. If you want the switch to retain these changes across a reboot, you must first save the configuration.
- Click  to refresh the page with the latest information from the switch.

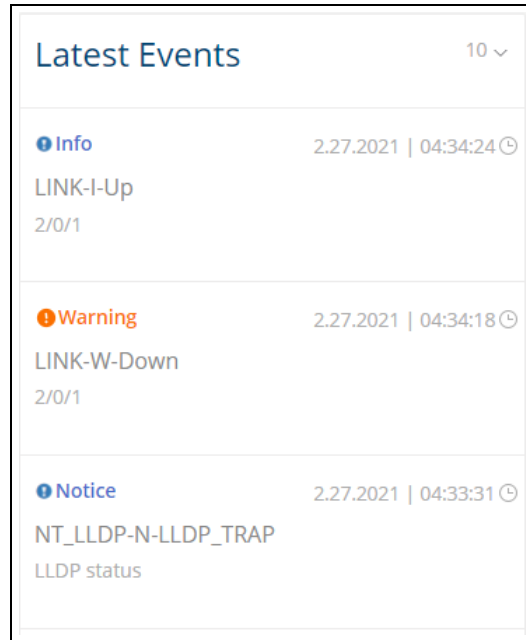
Saving Changes

When you click , changes are saved to the running configuration file in RAM. Unless you save them to system flash memory, the changes will be lost if the system reboots. To save them permanently, click  on the upper-right side of the page.

Latest Events Panel

To view the **Latest Events** panel, click the Notification  icon in the upper panel. The panel appears on the right side of the screen. Click again to close the panel.

Figure 5: Latest Events Panel



The Latest Events panel contains, by default, the most recent 10 logs in descending chronological order (the most recent event appears first). When a new event occurs, it will appear at the top of the panel, pushing the rest of the events down.

To set the number of displayed events (10, 20, 50), click the drop-down **10** icon at the top of the list, and select the appropriate setting.

Each event display has the following components:

- Severity indication: This indication is displayed as an icon and the name of the severity level in a color based on the severity:
 - Blue - Severity lower than Warning
 - Orange - Severity of Warning
 - Red - Severity higher than Warning
- Date and time of the event.
- Text of the event.

Click the SHOW MORE button at the bottom of the list, to open the Diagnostics > **Logging** panel with the full information on the events logged by the switch.

Switch Panel View

The switch panel view, shown below, displayed at the top of some of the pages as a representation of the physical switch to provide status information about individual ports. The switch panel view enables easy system configuration and web-based navigation.

You can right-click anywhere on the view and select from the menu to display the product and port information on the Dashboard page, to refresh the graphic display, and to set the automatic refresh rate.

Figure 6: Switch Panel View

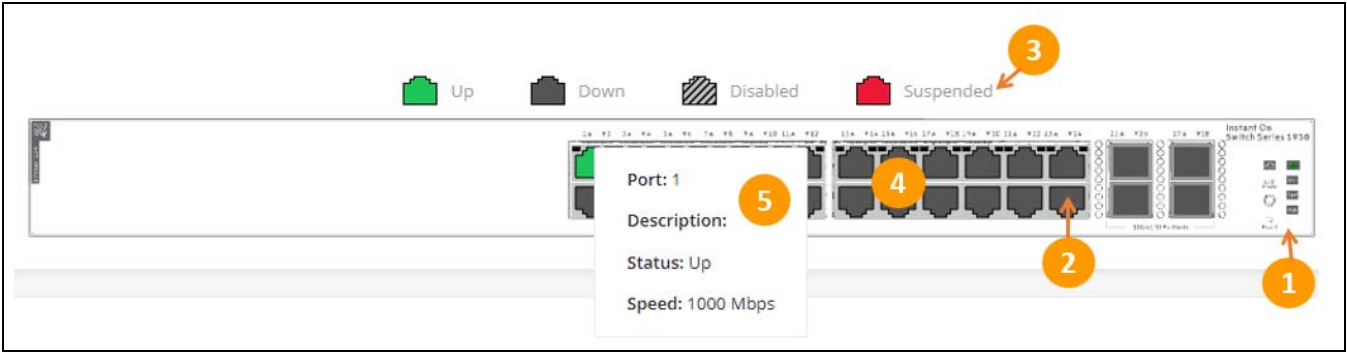


Table 3: Switch Panel Components

Label	Description
1	System LEDs
2	Port status indicator
3	Legend. The Legend shows port status for different features.
4	Port configuration and summary. Point or click on any port for options.
5	Switch panel ports display the port description and status. Right-click options are available to refresh port status or set the refresh rate.

Port State Indicator

Each port in the switch view is visually represented by one of the following state images.

Table 4: Port State Indicators

Port State	Image	Description
Up		The port is connected, enabled, and the link is up. This state image also applies to stack links in the Active state.
Down		The port is connected and enabled, but the link is down (likely because no cable is connected).
Disabled		The port has been administratively disabled. This state image also applies to stack links in the Inactive state.
Suspended		The port has an error condition and may or may not be active.

Port Information

You can hover the mouse on any port in the Switch Panel View to display the following information about the port:

- Port name. If the port is a trunk member, the trunk ID of the trunk is appended to the port name (for example: Port: 30 (TRK 7))
- Description. The description of the port, or the trunk if the port is a trunk member.
- The link status. Up, Down, Disabled, or Suspended. If the port is a trunk member, the status should be that of the trunk.

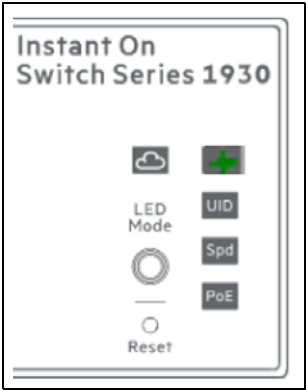
- **Speed.** The current speed of the port This field is only displayed for ports or trunks that are up. If the port is a trunk member, the speed is that of the trunk.

You can right-click a port to refresh the switch view, display and configure the switch refresh rate.

System LEDs

The following System LEDs reflect the status of the actual LEDs on the switch:

Figure 7: System LED Indicators



Some of the indications are reflected only on the LED on front panel and not on the GUI representation of the LED.

Table 5: System LED Indicators

Indicator	Color	Image	Description
Power	Green/ Orange		<ul style="list-style-type: none"> • On (green)—The switch is receiving power. This is an indication of normal operating condition. • Off—The switch is powered off or is NOT receiving power. • Slow flash (orange) <ul style="list-style-type: none"> • Self-test and initialization is in progress (boot-up). • A fault or self-test failure has occurred on the switch, one of the switch ports, the PSU, or the fan. The Status LED for the component with the fault will blink simultaneously.
UID (Locator)	Blue		<ul style="list-style-type: none"> • Blinking slowly—The locator function has been enabled to help physically locate the standalone unit, stack or a specific unit within the stack. • Off— Locator function was not activated by user, or if activated – function was manually disabled by user, or the Locator function timer has expired.
Speed Mode	Green		<ul style="list-style-type: none"> • On— Speed Mode has been selected and port LEDs are used to indicate port speed information. • Off— Speed Mode is not selected.
PoE Mode	Green/ Orange		<ul style="list-style-type: none"> • On solid green - PoE Mode has been selected and port LEDs are used to indicate PoE information. • On solid orange - PoE Mode is selected, and a port has an internal PoE hardware failure. The specific port LED with fault also flashes in this case. • Slow flash orange - PoE Mode has NOT been selected, but a port has an internal PoE hardware failure. <p>NOTE: In this case, the specific Port LED will NOT flash.</p> <ul style="list-style-type: none"> • LED is off - PoE mode is not selected, and there are no PoE hardware failures on ports.

Indicator	Color	Image	Description
Cloud LED	green/ orange		<p>Indicates the Cloud status of the switch:</p> <ul style="list-style-type: none"> • Slow flash green—the switch is in the process of establishing a connection, to the cloud portal. • On green—the switch has successfully completed the "onboarding process/procedure" and is fully operational, in cloud managed mode (connected to cloud portal). • On orange—The switch has detected an error/fault, and cannot connect to the cloud portal <p>NOTE - the Global Status LED does not flash.</p> <ul style="list-style-type: none"> • Alternating between green/orange—the switch is connected to the cloud portal, and ready for setup, through the App/Portal <p>This is a temporary state, which occurs while the switch is connected to the cloud portal, but not fully on-boarded yet.</p>
LED Mode			<p>This button determines the Port LED indication. Press this button to change to a different mode. The supported modes are:</p> <ul style="list-style-type: none"> • Link/activity - this is the default mode of device operation. There is no indication for this mode (speed and PoE Mode LEDs are off). The LED Mode will switch back to the link/activity state 10 minutes after selecting a non-default mode (speed or PoE) • Speed • PoE (for units that support PoE) <p>The speed and PoE LED modes have specific global LED indicating the selected mode.</p>
Reset button			<p>Reset the system. Press and release to reset the switch. Press and hold for 5 seconds or longer, to reset the switch to factory defaults.</p>

Chapter 3

Dashboard

You can use the Dashboard page to display and configure basic information about the system, and to use device configuration wizards.

The Dashboard page displays basic information such as the graphical display of switch, configurable switch name and description, System time and Switch information including the software and operating system versions. This page also shows resource usage statistics, and allows you to enable the switch locator LED.

The page also supports the following configuration wizards:

- Getting Started Wizard
- VLAN Configuration Wizard

This page is displayed when you first log on, or when you click **Dashboard** in the navigation pane.

The Dashboard is made up of various tiles, each of which contain various information about the switch. Each tile is described here.

Device View

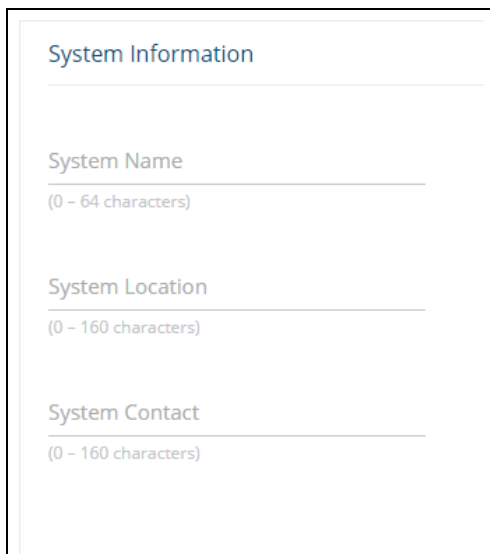
The top of the Dashboard page shows a graphical representation of the switch front panel. This panel view has a display of the ports, each with its current status.

Click a port in this screen, to open the **Switching > Port Configuration** page.

For more information, see [Switch Panel View](#).

System Information

Figure 8: System Information Tile



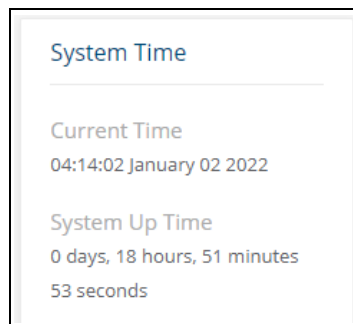
The screenshot shows a 'System Information' tile with three input fields. Each field has a label, a horizontal input line, and a character limit in parentheses below it. The fields are: 'System Name' (0 - 64 characters), 'System Location' (0 - 160 characters), and 'System Contact' (0 - 160 characters).

Field	Character Limit
System Name	0 - 64 characters
System Location	0 - 160 characters
System Contact	0 - 160 characters

Table 6: System Information Fields

Field	Description
System Name	Enter the preferred name to identify this switch. A maximum of 63 alpha-numeric, case-sensitive characters is allowed. The system name must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. The user-configurable switch name will appear in the login screen banner.
System Location	Enter the location of this switch. A maximum of 160 alpha-numeric, case-sensitive characters is allowed, including special characters (!, ", #, \$, %, &, ', (,), *, +, ,, -, ., /, :, ;, <, =, >, ?, @, [,], \, ^, _ ` , {, }, ~, and space). This field is blank by default.
System Contact	Enter the name of the contact person for this switch. A maximum of 160 alpha-numeric, case-sensitive characters is allowed, including special characters (!, ", #, \$, %, &, ', (,), *, +, ,, -, ., /, :, ;, <, =, >, ?, @, [,], \, ^, _ ` , {, }, ~, and space). This field is blank by default.

System Time

Figure 9: System Time Tile**Table 7: System Time Field**

Field	Description
Current Time	The current time in hours, minutes, and seconds as configured (24-hr format), and the current date in month, day, and year format.
System Up Time	The time in days, hours, minutes, and seconds since the last switch reboot.

Device Information

Figure 10: Device information Tile

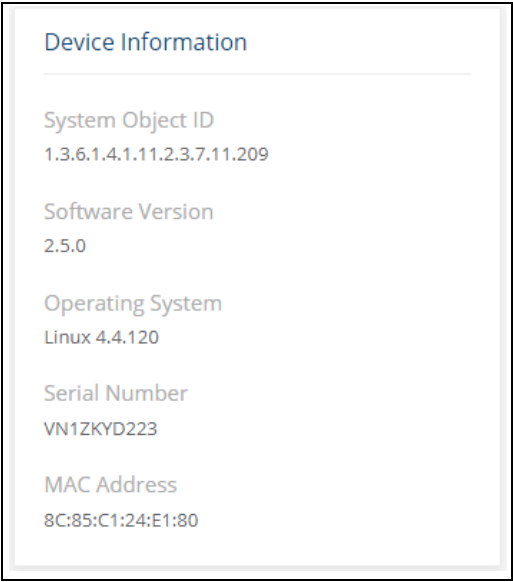


Table 8: Device Information Fields



The values that appear in the figures in this document are example values.

Field	Description
System Object ID	The base object ID for the switch's enterprise MIB.
Software Version	The version of the code running on the switch.
Operating System	The version of the operating system running on the switch.
Serial Number	The unique serial number assigned to the switch.
MAC Address	Device base MAC address.

System Resource Usage

Figure 11: System Resource Usage Tile

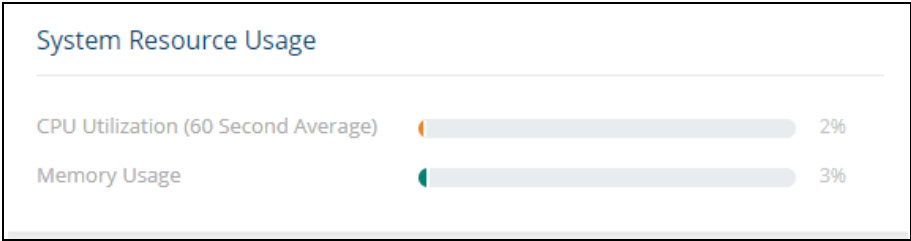


Table 9: System Resource Usage Fields

Field	Description
CPU Utilization	The percentage of CPU utilization for the entire system averaged over the past 60 seconds.
Memory Usage	The percentage of TCAM memory resources currently in use. These resources are utilized by features such as Quality of Service and ACLs.

Device Locator

Figure 12: Device Locator Tile

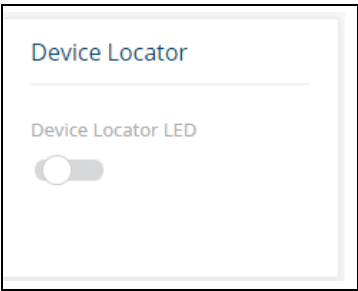


Table 10: Device Locator Field

Field	Description
Device Locator LED	Enable this feature to start flashing the physical device locator LED for 30 minutes.

Configuration Wizards

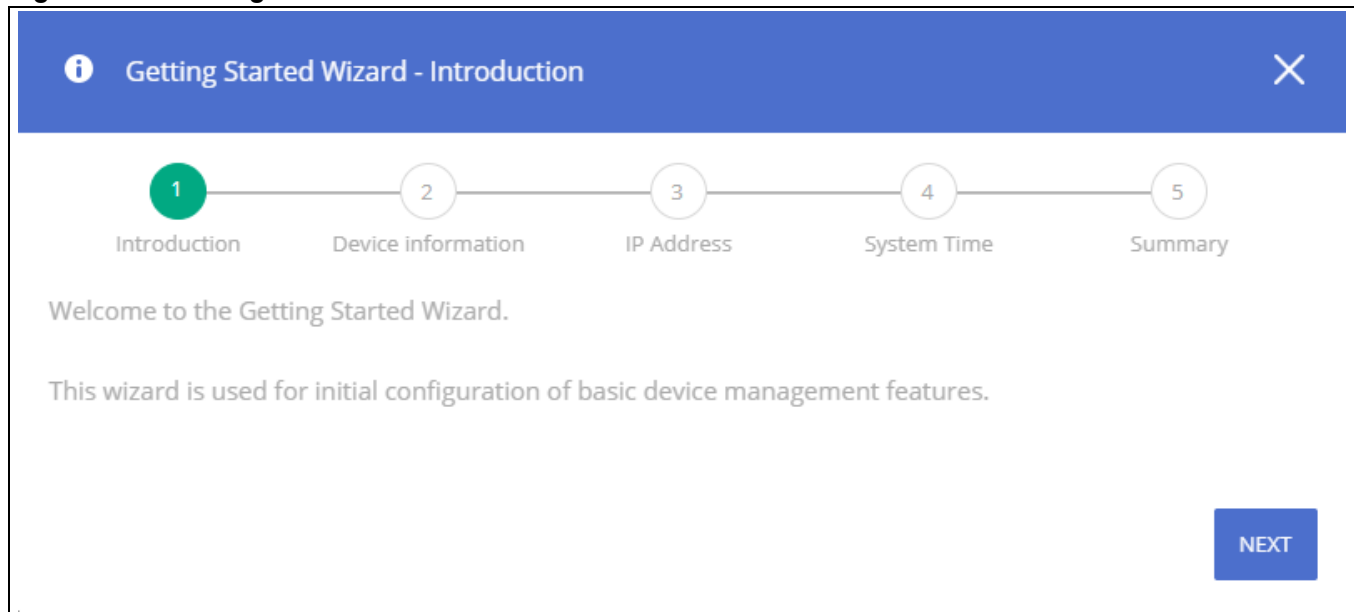
The HPE Networking Instant On 1930 provides the following wizards:

- Getting Started Wizard
- VLAN Configuration Wizard

Getting Started Wizard

Click the **GETTING STARTED WIZARD** button to open the Getting Started Wizard that walks you through the stages of initial configuration of the basic management features of the HPE Networking Instant On 1930 Switch Series.

Figure 13: Getting Started Wizard



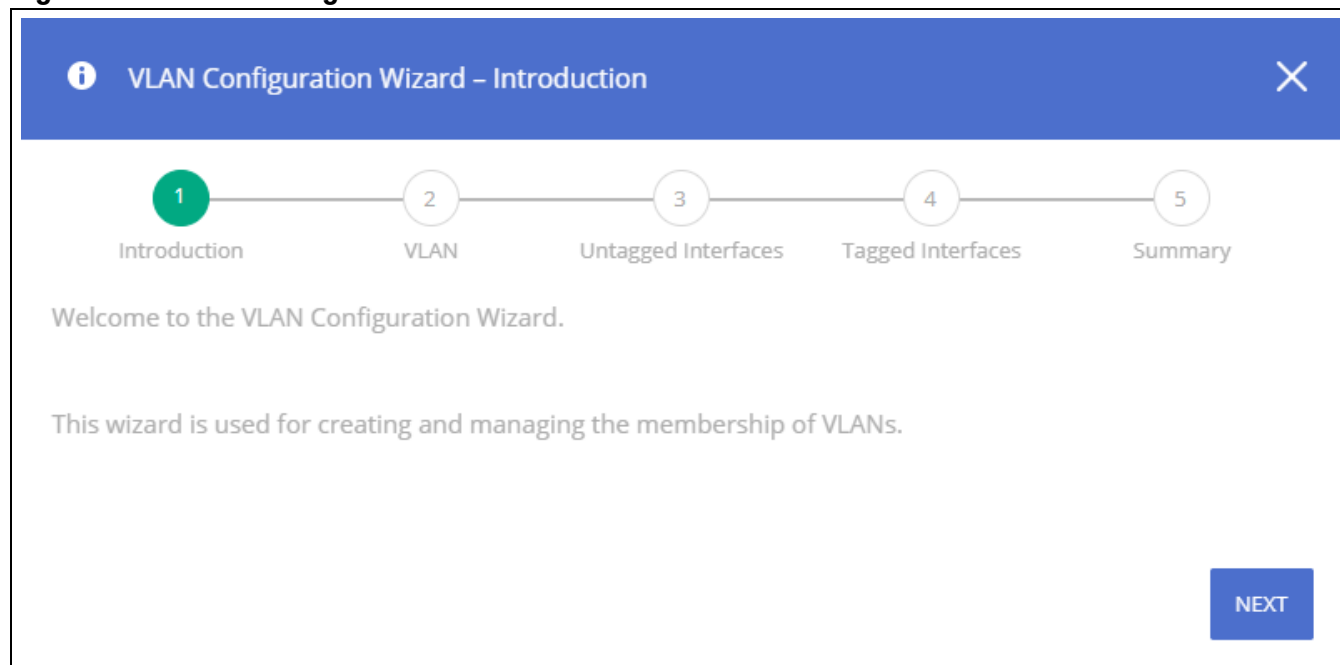
These are the steps that the wizard takes you through.

- Step 1 - Introduction screen. Click the **NEXT** button to proceed with the configuration wizard.
- Step 2 - Device Information, enter a System Name, System Location and System Contact information to help identify the device.
Click **NEXT** to go to the next screen in the configuration wizard.
- Step 3 - IP Address. Set up the IP interface. For more information on the fields in this screen, see [VLAN Configuration Fields](#), and [IPv4 Setup Fields](#).
Click **NEXT** to go to the next screen in the configuration wizard.
- Step 4 - System Time. Set up the device clock. For more information on the fields in this screen, see [Time Configuration Fields](#).
Click **NEXT** to go to the next screen in the configuration wizard.
- Step 5 - Summary. This screen details the changes that were configured. Click **APPLY** to apply the changes to the next session.
- The next screen shows that all the steps were taken and the configuration is successful.
Click **CLOSE** to close the wizard.

VLAN Configuration Wizard

Click the **VLAN CONFIGURATION WIZARD** button to open the VLAN Configuration Wizard that walks you through the stages of initial configuration of the a Virtual Local Area Network (VLAN) on the HPE Networking Instant On 1930 Switch Series.

Figure 14: VLAN Configuration Wizard



These are the steps that the wizard takes you through.

- Step 1 - Introduction screen. Click the **NEXT** button to proceed with the configuration wizard.
- Step 2 - VLAN. Select the VLAN type that you would like to create. If you create a new VLAN, you can enter a name for your VLAN. If you want to manage an existing VLAN, select it from the drop-down. Click **NEXT** to go to the next screen in the configuration wizard.
- Step 3 - Untagged Interfaces. Select the interfaces that should be untagged. Use Ctrl-click to select specific interfaces, use Shift-click to select a range of interfaces. The selected interfaces are listed at the bottom of the screen. For more information on tagged and untagged interfaces, see [“VLAN Membership - By VLAN Tab Fields”](#). Click **NEXT** to go to the next screen in the configuration wizard.
- Step 4 - Tagged Interfaces. Select the interfaces that should be tagged. Use Ctrl-click to select specific interfaces, use Shift-click to select a range of interfaces. The selected interfaces are listed at the bottom of the screen. Click **NEXT** to go to the next screen in the configuration wizard.
- Step 5 - Summary. This screen details the VLAN ID, and the untagged/tagged members of the VLAN. Click **APPLY** to apply the changes to the next session.
- The next screen shows that all the steps were taken and the configuration is successful. Click **CLOSE** to close the wizard.

To view the changes, go to **VLAN > VLAN Configuration**.

Active Users

Figure 15: Active Users Tile

Active Users

Display: 10

Username	Connected From	Session Time
AIOUser1	10.5.229.216	27:51
AIOUser1	*	01:03

1

Table 11: Active Users Fields



The Active Users tile displays only if more than one user is logged into the system.

Field	Description
Username	The username of each logged in user.
Connected From	The IP address from which the user logged in.
Session Time	The amount of time the user session has been active, in hours, minutes, and seconds.

You can use the Setup Network pages to configure how a management computer connects to the switch, to set up system time settings, and to manage switch administrator accounts and passwords.

Get Connected

Use the **Get Connected** page to configure settings for the switches management interface. The management interface is defined by an IP address, subnet mask, and gateway.

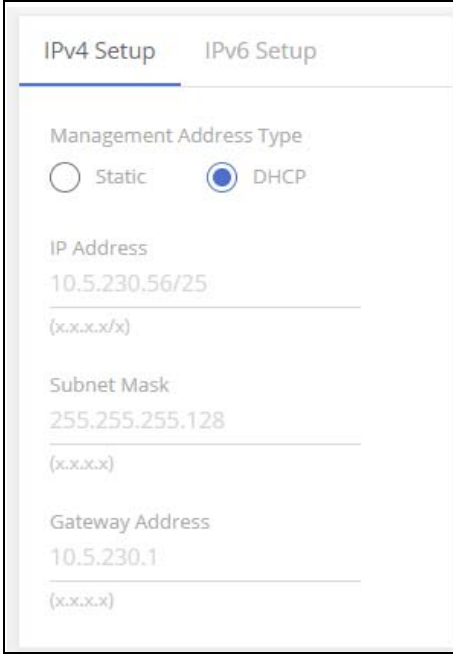
To display the Get Connected page, click **Setup Network > Get Connected**.

The following sections explain the various tiles and the configuration options within each tile.

IPv4 Setup Tab

To view the IPv4 Setup options, click on the **IPv4 Setup** tab in the tile.

Figure 16: IPv4 Setup Tab



The screenshot shows the 'IPv4 Setup' tab selected. It contains the following configuration options:

- Management Address Type:** Two radio buttons are present. 'Static' is unselected, and 'DHCP' is selected (indicated by a blue dot).
- IP Address:** A text field containing '10.5.230.56/25' with a placeholder '(x.x.x.x/x)' below it.
- Subnet Mask:** A text field containing '255.255.255.128' with a placeholder '(x.x.x.x)' below it.
- Gateway Address:** A text field containing '10.5.230.1' with a placeholder '(x.x.x.x)' below it.

Table 12: IPv4 Setup Fields

A power cycle does not reset the IP address to its factory-default value. If the configured IP address is unknown, you can perform a manual reset to factory defaults to regain access to the switch (see [**Reset to Factory Defaults**](#)).

Field	Description
Management Address Type	<p>Select the type of network connection:</p> <ul style="list-style-type: none">• Static—Select this option to configure the IP address, subnet mask, and gateway fields for data entry.• DHCP—Select this option to configure the switch to obtain IP information from a DHCP server on the network. If the DHCP server responds, then the assigned IP address is used. If DHCP is enabled but the DHCP server does not respond, the default static IP address 192.168.1.1 is used. DHCP operation is enabled by default. <p>When a DHCP server assigns an IP address to the switch, it specifies the time for which the assignment is valid. Only a user-configured static IP address is saved to flash.</p> <p>CAUTION: Changing the protocol type or IP address discontinues the current connection; you can log on again using the new IP address information.</p>
IP Address	<p>The IPv4 address for the switch.</p> <p>If the Protocol Type is set to DHCP, this field displays the IP address assigned by the DHCP server. If the Protocol Type is set to Static, the IP address can be manually configured in this field. The default IP address is 192.168.1.1.</p>
Subnet Mask	<p>The IPv4 subnet address to be used. The default IP subnet address is 255.255.255.0.</p>
Gateway Address	<p>The IPv4 gateway address to be used. When in doubt, set this to be the same as the default gateway address used by your PC.</p>

IPv6 Setup Tab

To view the IPv6 Setup options, click on the **IPv6 Setup** tab in the tile.

Figure 17: IPv6 Setup Tab



A power cycle does not reset the IP address to its factory-default value. If the configured IP address is unknown, you can perform a manual reset to factory defaults to regain access to the switch.

Table 13: IPv6 Setup Fields

Field	Description
IPv6 Status	Enables or disables the IPv6 administrative mode on the management interface.
DCHP Network Configuration	Specify whether the switch should attempt to acquire network information from a DHCPv6 server. Set as Disabled to disable the DHCPv6 client on the management interface.
IPv6 Stateless Autoconfig	Sets the IPv6 stateless address autoconfiguration mode on the management interface. <ul style="list-style-type: none"> Enabled – The management interface can acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of Router Advertisement messages. Disabled – The management interface will not use the native IPv6 address autoconfiguration to acquire an IPv6 address.
Static IPv6 Address	Specify the IPv6 address to add to the interface.
Dynamic IPv6 Address	Lists the IPv6 addresses on the management interface that have been dynamically configured through IPv6 autoconfiguration or DHCPv6.
EUI Flag	Select this option to enable the Extended Universal Identifier (EUI) flag for IPv6 address, or clear the option to omit the flag.
IPv6 Gateway	Specify the default gateway for the IPv6 management interface.

Field	Description
DHCPv6 Client DUID	The client identifier used by the DHCPv6 client when sending messages to the DHCPv6 server.

HTTP/S Management Settings

Use this tile to view and modify the HTTP or Secure HTTP (HTTPS) settings on the switch. HTTPS increases the security of web-based management by encrypting communication between the administrative system and the switch.

To set HTTP management, click on the **HTTP Management** tab, to set HTTPS management, click the **HTTPS Management** tab.

Figure 18: HTTP/S Management Settings Tabs

Table 14: HTTP/S Management Settings Fields

Field	Description
HTTP/S Management	Enables or disables the HTTP or HTTPS administrative mode. When enabled, the switch can be accessed through a web browser using the HTTP/S protocol. By default HTTP/S management is enabled.
Port	The TCP port number on which the HTTP/S server listens for requests. Existing HTTP/S login sessions are closed whenever this value is changed. All new HTTP sessions must use the new port number. Note: Before changing this value, check your system to make sure the desired port number is not currently being used by any other service. For HTTP the default is 80, for HTTPS the default is 443. The valid range for this port number is 1025-59999.
Session Soft Timeout	Session inactivity timeout value, in minutes. A logged-in user that does not exhibit any HTTP/S activity for this amount of time is automatically logged out of the HTTP/S session. By default, the timeout is 10 minutes. The valid range is 1-60.
Session Hard Timeout	Session hard timeout value, in hours. A user connected to the switch through an HTTP/S session is automatically logged out after this amount of time regardless of the amount of HTTP/S activity that occurs. By default, the timeout is 24 hours. The valid range is 1-168.

Management VLAN Settings

Figure 19: Management VLAN Tile

Management VLAN

Management VLAN ID

1

Table 15: Management VLAN Fields

Field	Description
Management VLAN ID	<p>The Management IP address configured on this tile is applied to the Management VLAN. By default, the management VLAN ID is 1. The management VLAN can be any value between 1 and 4092. All ports are members of VLAN 1 by default; the administrator may want to create a different VLAN to assign as the management VLAN. In this case, the IP address is applied to the other VLAN configured by the user.</p> <p>A VLAN that does not have any member ports (either tagged or untagged) cannot be configured as the management VLAN.</p> <p>When the network protocol is configured to be DHCP, any change in the configured management VLAN ID may cause disruption in connectivity because the switch acquires a new IP address when the management subnet is changed. To reconnect to the switch, the user must determine the new IP address by viewing the log on the DHCP server.</p>

Click **APPLY** to update the switch configuration. Changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

System Time

Click **Setup Network > System Time** to configure the system clock, SNTP client functionality, system time zone, and daylight saving time settings.

Time Configuration

You can configure the system time manually or acquire time information automatically from a Simple Network Time Protocol (SNTP) server. Using SNTP ensures accurate network switch clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The software operates only as an SNTP client and cannot provide time services to other systems.

Figure 20: Time Configuration Tile

Time Configuration

System Time Source

☒ SNTP ☐ Manual

Time

21:21 

Date

Aug 01 2019 

SNTP Server

(x.x.x.x)

Server Port

123

(1 - 65535)

Last Update Time

N/A

Last Attempt Time

N/A

Last Attempt Status

Unknown

Time Zone Settings

Time Zone GMT 00:00 

Table 16: Time Configuration Fields

Field	Description
System Time Source	Select SNTP (Simple Network Time Protocol) to configure the switch to acquire its time settings from an SNTP server. When selected, only the SNTP Configuration fields are available for configuration. Select Manual to disable SNTP and configure the time manually. You can manually set the date and time in the fields mentioned below.
Time	The current time. This value is determined by an SNTP server. When SNTP is disabled, the system time increments from the active image creation time stamp. You can also configure the time manually.
Date	The current date. This value is determined by an SNTP server. When SNTP is disabled, the system time increments the active image creation time stamp.
SNTP Server	Specify the IPv4 address of the SNTP server to which requests should be sent.
Server Port	Specify the server's UDP port for SNTP. The range is 1 to 65535 and the default is 123.
Last Update Time	The date and time (GMT) when the SNTP client last updated the system clock.
Last Attempt Time	The date and time (GMT) of the last SNTP request or receipt of an unsolicited message.

Field	Description
Last Attempt Status	<p>The status of the last update request to the SNTP server, which can be one of the following values:</p> <ul style="list-style-type: none"> Unknown —None of the following values apply or no message has been received. Up—The SNTP operation was successful and the system time was updated. Request Timed Out—A SNTP request timed out without receiving a response from the SNTP server. Down—Connection not established with SNTP server. In Process—currently establishing connection with SNTP server.
Time Zone Settings	
Time Zone	The currently set time zone. To edit, click the Edit button  . The default is (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London.
Acronym	The acronym for the time zone, if one is configured on the system (for example, PST, EDT).

Daylight Saving Configuration

The Daylight Saving Configuration tile is used to configure if and when Daylight Saving Time (DST) occurs within your time zone. When configured, the system time adjusts automatically one hour forward at the start of the DST period, and one hour backward at the end.

To display the Daylight Saving Configuration tile, click **Setup Network > System Time** in the navigation pane.

Figure 21: Daylight Saving Configuration Tile

Daylight Saving Configuration

Daylight Saving Time

Recurring

Non Recurring Range

Start Date

Jul 28 2019

Starting Time of Day

End Date

Ending Time of Day

Recurring Range

Start Week

Last

Start Day

Sunday

Start Month

Table 17: Daylight Saving Configuration Fields

Field	Description
Daylight Saving Time	<p>Select how DST will operate:</p> <ul style="list-style-type: none"> Disable—No clock adjustment will be made for DST. This is the default selection. EU—The system clock uses the standard recurring daylight saving time settings used in countries in the European Union. USA—The system clock uses the standard recurring daylight saving time settings used in the United States. Recurring—The settings will be in effect for the upcoming period and subsequent years. Non-Recurring—The settings will be in effect only for a specified period during the year (that is, they will not carry forward to subsequent years). <p>When a DST mode is enabled, the clock will be adjusted one hour forward at the start of the DST period and one hour backward at the end.</p>
Non Recurring Range	<p>Set the following to indicate when the change to DST occurs and when it ends. These fields are editable when Non-Recurring is selected as the DST mode:</p> <ul style="list-style-type: none"> Start Date—Use the calendar to set the day, month, and year when the change to DST occurs. Starting Time of Day—Set the hour and minutes when the change to DST occurs. Or, enter the hours and minutes in 24-hour format (HH:MM). End Date—Use the calendar to set the day, month, and year when the change from DST occurs. Ending Time of Day—Set the hour and minutes when the change from DST occurs. Or, enter the hours and minutes in 24-hour format (HH:MM).

Field	Description
Recurring Range	<p>When Recurring is selected as the DST mode, the following fields display:</p> <ul style="list-style-type: none"> Start/End Week—Set the week of the month, from 1 to 5, when the change to/from DST occurs. The default is 1 (the first week of the month). Start/End Day—Set the day of the week when the change to/from DST occurs. Start/End Month—Set the month when the change to/from DST occurs. Starting/Ending Time of Day—Set the hour and minutes when the change to/from DST occurs.

Click **APPLY** to update the switch configuration. Changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

User Management

By default, the switch contains only the *admin* user account, which has read/write privileges. Upon first login, you are prompted to change the default username and password.

Click **Setup Network > User Management** to add switch management users, change user settings, or remove users.

Authentication of device management can be configured from the [RADIUS Configuration](#) page.

Logged In Sessions

The Logged In Sessions tile identifies the users that are logged in to the management interface of the switch. The tile also provides information about their connections.

Figure 22: Logged In Sessions Tile

Username	Connected From	Session Time	Session Type
guest	10.4.82.2	39:07	HTTP

Table 18: Logged In Sessions Fields

Field	Description
Username	The name that identifies the user account.
Connected From	Identifies the administrative system that is the source of the connection. For remote connections, this field shows the IP address of the administrative system.
Session Time	Shows the amount of time in hours, minutes, and seconds since the user logged onto the system.
Session Type	Shows the type of session, which can be HTTP or HTTPS.

User Accounts

If you log on to the switch with a user account with read/write privileges (such as admin), you can use the **User Accounts** tile to assign passwords and set security parameters for the User accounts. You can add up to five accounts. You can delete all accounts except for one Read/Write account.

Figure 23: User Accounts Tile

User Accounts								
☐	Username		Access Level	Lockout Status		Password Expiration		
☐	admin		Read/Write	False		N/A		

Table 19: User Accounts Fields

Field	Description
Username	A unique ID or name used to identify this user account.
Access Level	Indicates the access or privilege level for this user. The options are: <ul style="list-style-type: none">Read/Write - The user can view and modify the configuration.Read Only - The user can view the configuration but cannot modify any fields.
Lockout Status	Provides the current lockout status for this user. If the lockout status is True, the user cannot access the management interface even if the correct username and password are provided. The user has been locked out of the system due to a failure to supply the correct password within the configured number of login attempts.
Password Expiration	Indicates the current expiration date (if any) of the password.

From this tile, use the available buttons to add or remove users or to edit the settings for an existing user. Use the **Unlock Account** button to unlock a user account.

Adding a User Account

To add a new user account, from the User Accounts tile, click the **Add Entry** button and configure the settings.

Figure 24: Add New User Dialog Box

 Add New User 

Username

(1 – 20 characters)

Password Configuration Method

☒ Regular ☐ Encrypted

Password

(8 – 64 characters)

Confirm

(8 – 64 characters)

Access Level

☒ Read Only ☐ Read/Write

CANCEL

APPLY

Configure the settings for the new user.

Table 20: New User Configuration Fields

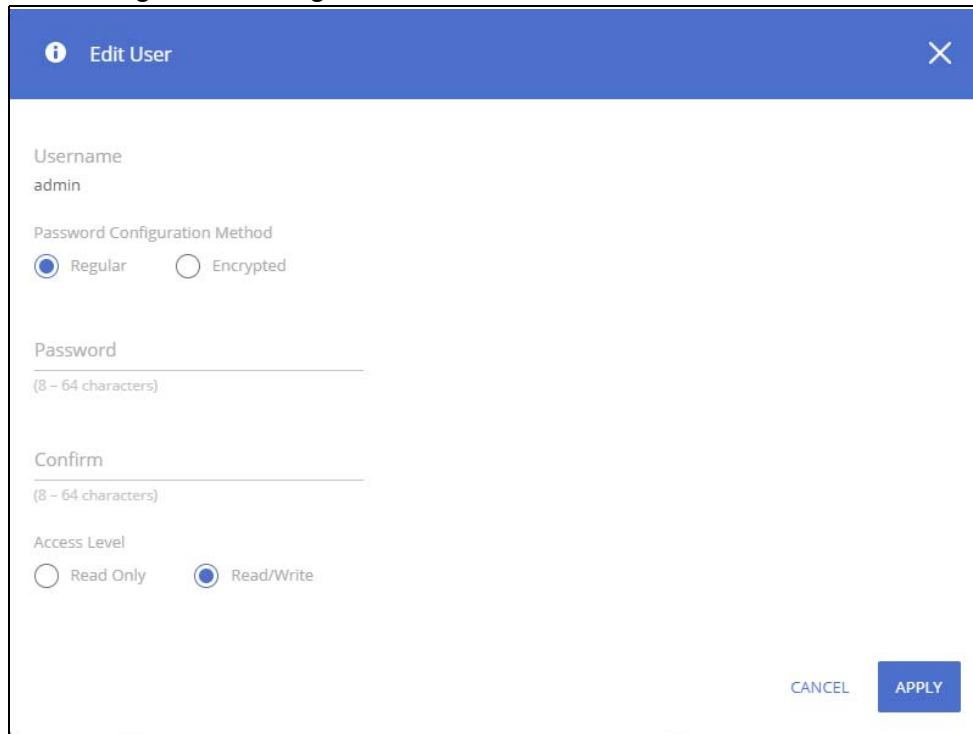
Field	Description
Username	Enter the name you want to give to the new account. (You can only enter data in this field when you are creating a new account.) Usernames are up to 20 alphanumeric characters in length and are not case sensitive. Valid characters include all the alphanumeric characters and the dash ('-') and underscore ('_') characters. Username <i>default</i> is not valid.
Password Configuration Method	Specify Regular for unencrypted passwords, or Encrypted to enter a password that is already encrypted. This option is usually used when the password is copied from an existing configuration file.
Password	Enter the password for the account. It will not display as it is typed, only asterisks (*) or dots (.) will show, based on the browser used. By default, passwords must be greater than eight characters and can be up to 64 characters in length, and are case sensitive.
Confirm	Enter the password again, to confirm that you entered it correctly. This field will not display, but will show asterisks (*) or dots (.), based on the browser you use.
Access Level	Indicates the access or privilege level for this user. The options are: <ul style="list-style-type: none">Read Only - The user can view the configuration but cannot modify any fields.Read/Write - The user can view and modify the configuration.

Click **APPLY**.

Changing User Account Information

You cannot change the name of an existing user, but you can change the password, privilege, and password settings. To change user information, select the username with the information to change and click the **Edit** button . Update the fields as needed, and click **APPLY**.

Figure 25: Edit Existing User Dialog Box

The image shows a dialog box titled "Edit User" with a blue header bar containing an information icon and a close button. The main area is white and contains several fields: "Username" with the value "admin", "Password Configuration Method" with radio buttons for "Regular" (selected) and "Encrypted", "Password" and "Confirm" text boxes (both with "(8 - 64 characters)" below them), and "Access Level" with radio buttons for "Read Only" and "Read/Write" (selected). At the bottom right are "CANCEL" and "APPLY" buttons.

Edit User

Username
admin

Password Configuration Method
☒ Regular ☐ Encrypted

Password
(8 - 64 characters)

Confirm
(8 - 64 characters)

Access Level
☐ Read Only ☒ Read/Write

CANCEL APPLY

Removing a User Account

To remove any of the user accounts, select one or more users to remove. Click the **Remove** button  to delete the selected users.

Account Security Settings

Use this tile to configure rules for locally-administered passwords.

Figure 26: Account Security Settings Tile

Account Security Settings

Password Aging

Password Aging Time

1

(1 – 365) Days

Account Lockout

Lockout Attempts

1

(1 – 5) Login Attempts

Table 21: Account Security Settings Fields

Field	Description
Password Aging	Activate this to enable setting a maximum age for a user password. Users will need to change their password before the maximum age.
Password Aging Time	Set the amount of days that the password can be used before it is changed to a new password.
Account Lockout	Activate this to enable setting a maximum number of password attempts before the account is locked.
Lockout Attempts	After a user fails to log in this number of times, the user is locked out until the password is reset by the administrator.

Password Strength Rules

The rules you set determine the strength of local passwords that switch users can associate with their user-names. The strength of a password is a function of length, complexity, and randomness.

Figure 27: Password Strength Rules Tile

Password Strength Rules

Password Strength Enforcement

Minimum Length

8

(0 – 64 characters)

Character Repetition Enforcement

Maximum Number of Repeated Characters

1

(1 – 16)

Minimum Character Classes

0

(0 – 4)

Table 22: Password Strength Rules Fields

Field	Description
Password Strength Enforcement	Enable or disable the password strength check feature. Enabling this feature forces the user to configure passwords that comply with the strong password configuration specified in the following fields.
Minimum Length	Passwords must have at least this many characters (0 to 64).
Character Repetition Enforcement	Enable or disable the character repetition enforcement feature. Enabling this feature limits the number of repeated characters allowed in the password.
Maximum Number of Repeated Characters	Specify the maximum number of repeated characters a password is allowed to include. An example of four repeated characters is aaaa.
Minimum Character Classes	Specify the minimum number of character classes a password must contain. There are four character classes: <ul style="list-style-type: none">• Uppercase• Lowercase• Numbers• Special Characters

Password Keyword Exclusion

Use the Keyword Exclusion configuration option to add keywords that are not allowed as part of a password.

Figure 28: Password Exclusion Tile

Password Keyword Exclusion

Keyword

Table 23: Password Exclusion Field

Field	Description
Keyword	<p>The list of keywords that a valid password must not contain. Excluded keyword checking is case-insensitive. Additionally, a password cannot contain the backwards version of an excluded keyword. For example, if pass is an excluded keyword, passwords such as 23passA2c, ssapword, and PAsSworD are prohibited. Use the plus and minus buttons to perform the following tasks:</p> <ul style="list-style-type: none"> To add a keyword to the list, click Add, type the word to exclude in the Keyword field, and click APPLY. To remove one or more keywords from the list, select each keyword to delete and click Remove.

Click **APPLY** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Schedule Configuration

The switch provides three schedules. When a schedule is applied to a feature or setting, the feature is enabled when the schedule is active and disabled when the schedule is inactive.

Each schedule can have one absolute schedule and multiple periodic schedules. Schedules can be applied to these features:

- PoE - to set the time ranges when PoE power is provided.
- Port Admin status - to set the time ranges when the port is operationally enabled.
- ACEs - to set the time ranges when the ACE is active.

Click **Setup Network > Schedule** to view or configure the schedules.

Schedules

Figure 29: Schedules Tile

Schedules

⊕ | 🗑️ | ↺ Display: 10 ▾

⚠️ The system time is currently set manually. It is recommended to use SNTP to set the system time when using the scheduling feature.

Schedule Name
Schedule-1 ▾

☐ Type	▲ Start	Ends
☐ Absolute	08:00 June 08, 2021	20:00 June 08, 2021
☐ Periodic	07:00 Mon	08:00 Mon

Table 24: Schedules Fields

Field	Description
Schedule Name	Select the schedule to view from the drop-down list to display information on time periods configured for the schedule, if any.
Type	The type of time period entry, which is one of the following: <ul style="list-style-type: none">• Absolute—A single time period that occurs once or has an undefined start or end period. The duration of an absolute entry can be hours, days, or even years.• Periodic—A recurring entry that takes place at fixed intervals. This type of entry occurs at the same time on one or more days of the week.
Start	For an absolute entry, this field indicates the time, day, month, and year that the entry begins. If this field is blank, the absolute entry became active when it was configured. For a periodic entry, this field indicates the time and day(s) of the week that the entry begins.
Ends	For an absolute entry, indicates the time, day, month, and year that the entry ends. If this field is blank, the absolute entry does not have a defined end. For a periodic entry, this field indicates the time and day(s) of the week that the entry ends.



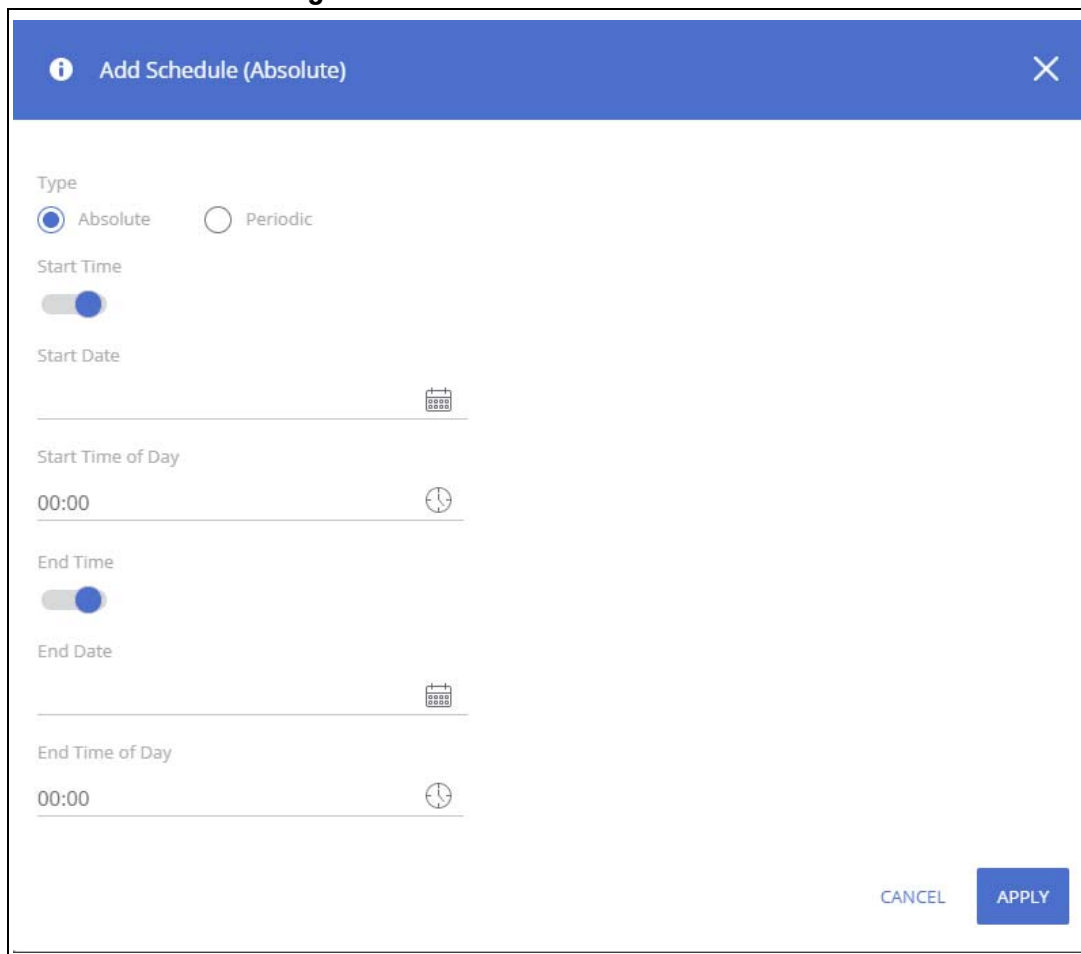
Schedules require setting the system clock manually, or via SNTP. SNTP provides better accuracy.

To view or configure a schedule, go to the **Schedule Name** drop-down and select the schedule.

Adding a Schedule

To add a schedule, from the Schedules tile, click the **Add Entry** button  and configure the settings.

Figure 30: Add Schedule Dialog Box - Absolute Schedule



The dialog box is titled "Add Schedule (Absolute)" with a blue header bar containing an information icon and a close button. The main content area is white and contains the following fields:

- Type:** Two radio buttons are present: "Absolute" (selected) and "Periodic".
- Start Time:** A toggle switch is shown in the "on" position.
- Start Date:** A text input field with a calendar icon to its right.
- Start Time of Day:** A text input field showing "00:00" with a clock icon to its right.
- End Time:** A toggle switch is shown in the "on" position.
- End Date:** A text input field with a calendar icon to its right.
- End Time of Day:** A text input field showing "00:00" with a clock icon to its right.

At the bottom right of the dialog box, there are two buttons: "CANCEL" and "APPLY".

Figure 31: Add Schedule Dialog Box - Periodic Schedule

 Add Schedule (Periodic) 

Type

☐ Absolute ☒ Periodic

Start Day

Monday

Start Time of Day

08:00

End Day

Thursday

End Time of Day

10:00

CANCEL

APPLY

Table 25: New Schedule Configuration Fields

Field	Description
Type	The type of schedule. Can be one of the following: <ul style="list-style-type: none">Absolute. There can one absolute schedule in each schedule. The absolute schedule does not repeat.Periodic. Each schedule can have multiple periodic schedules. A periodic schedule occurs at the same time every day or on one or more days of the week.
Absolute Schedule Fields	
Start Time	Enable the Start Time setting to apply the schedule Start Date. If the Start Time is disabled, the schedule Start Date will be active at the time of configuration.
Start Date	Select the start date from the calendar.
Start Time of Day	Set the time of day to start the schedule.
End Time	Activate this field to enable setting the End point of the schedule. If End Time is not activated, the schedule continues indefinitely.
End Date	Select the end date from the calendar.
End Time of Day	Set the time of day to end the schedule.
Periodic Schedule Fields	
Start Day	Select the day of the week to start the schedule, from the drop-down list.
Start Time of Day	Set the time of day to start the schedule.
End Day	Select the day of the week to end the schedule, from the drop-down list.

Field	Description
End Time of Day	Set the time of day to end the schedule.

Click **APPLY** to save the changes for the current switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Removing a Schedule

To remove a schedule, you must remove all ACL and port related schedule configurations (port state, or PoE). Once the schedule is not in use by any ACL, port state or PoE configuration, select it in the Schedules tile, and click the **Remove** button  .

You can use the Switching pages to configure port operation and various Layer 2 features and capabilities.

Port Configuration

You can use the Port Configuration tiles to display port status, configure port settings, and view statistics on packets transmitted on the port.

To view this page, click **Switching** > **Port Configuration** in the navigation pane.

Device View

The top of the Port Configuration page shows a graphical representation of the switch front panel. This panel view has a display of the ports, each with its current status.

Click a port in this screen, to open the **Switching > Port Configuration** dialog box. If the port is a trunk member, the **Switching > Trunk Configuration** dialog box appears.

For more information, see [Switch Panel View](#).

Global Configuration

These are the global configuration options that you can set:

Figure 32: Global Configuration

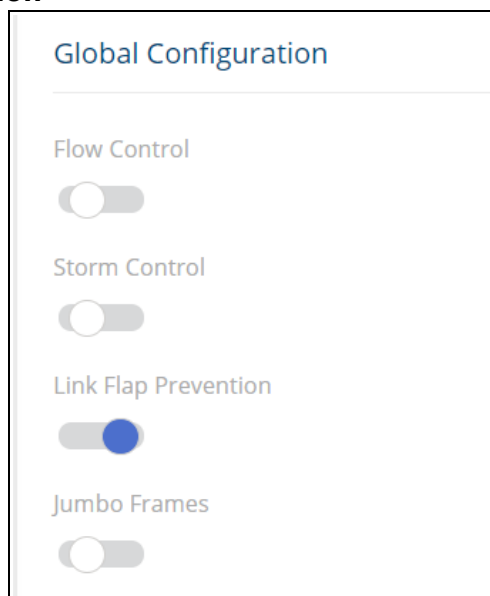


Table 26: Global Configuration Fields

Field	Description
Flow Control	When a port becomes congested, it may begin dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss. When 802.3x flow control is enabled, a lower-speed switch can communicate with a higher-speed switch by requesting that the higher-speed switch refrain from sending packets. Transmissions are temporarily halted to prevent buffer overflows.
Storm Control	<p>The switch supports both Global and per interface storm control settings. This is the global storm control setting. For information on per interface storm control, see Modifying Interface Settings. By default, global storm control is disabled.</p> <p>The Storm Control feature protects against conditions where incoming packets flood the LAN, causing network performance degradation. The software includes Storm Control protection for unicast traffic with an unknown destination, and for broadcast and multicast traffic.</p> <p>When enabled, the following storm control settings are applied to all switch interfaces:</p> <ul style="list-style-type: none"> Storm Control rate limit - 5% of interface speed. The limit is applied separately to each type of storm control - unicast (including unknown unicast), multicast or broadcast. Packets that exceed the threshold limits are dropped.
Link Flap Prevention	<p>A link-flap event is triggered if an interface changes its link state (link-up or link-down event) 3 or more times a second - for 10 seconds or more.</p> <p>In such a case, the port is suspended and the following syslog message and SNMP trap are generated: %LINK-W-PORT_SUSPENDED: Port <i><port number></i> suspended by link-flapping Where <i><port number></i> is the number of the port that was suspended.</p> <p>A port that is suspended by link flap prevention can be recovered by one of the following:</p> <ul style="list-style-type: none"> If auto-recovery is enabled for link flap prevention - after the timeout expires, the port attempts to recover. If auto-recovery is disabled - you may attempt to manually recover the port in the Suspended Interface tile on the Switching > Interface Auto Recovery page.
Jumbo Frames	<p>Sets both MTU and MRU values</p> <ul style="list-style-type: none"> If disabled - frame size is limited to 1518 bytes If enabled - For bridging: frame size is limited to 9216 bytes. For Routing: frame size is limited to 9000 bytes <p>Changing this setting requires saving the configuration and rebooting the switch. The new setting is applied only after reboot.</p>



Flow control requires link speed to be set to auto-negotiate. If auto-negotiation is OFF or if the port speed was configured manually, then flow control is not negotiated with or advertised to the peer. Additionally, the flow control PAUSE frame configuration may be lost if the auto-negotiation is disabled on the port.



Interface storm control settings override the Global storm control settings. This means that if an interface has a specific setting for a certain storm type - the interface will use those settings and not the global setting.



The storm control threshold percentage is translated to a packets-per-second value that is used by the switch hardware to rate-limit the incoming traffic. This translation assumes a 512 byte packet size to determine the packets-per-second threshold based on the port speed. For example, the 5% threshold applied to a 1 Gbps port equates to approximately 11748 packets-per-second, regardless of the actual packet sizes received by the port.

Interface Configuration

The Interface Configuration tile displays the operational and administrative status of each port and enables port configuration.



If connecting a 10GBaseT transceiver, do not choose Auto-Neg or 1G speed.

Figure 33: Interface Configuration Tile

Interface Configuration											
☐ Interface ▲	Description	Type	Admin Mode	Schedule	Physical Mode	Physical Status	Auto Negotiation Capabilities	STP Mode	LACP Mode	Link Status	
☐ 1		Normal	Enabled	None	Auto	Unknown	10h 10f 100h 100f 1000f	Enabled	N/A	Link Down	
☐ 2		Normal	Enabled	None	Auto	Unknown	10h 10f 100h 100f 1000f	Enabled	N/A	Link Down	
☐ 3		Normal	Enabled	None	Auto	Unknown	10h 10f 100h 100f 1000f	Enabled	N/A	Link Down	
☐ 4		Normal	Enabled	None	Auto	Unknown	10h 10f 100h 100f 1000f	Enabled	N/A	Link Down	

Table 27: Interface Configuration Fields

Field	Description
Interface	The port or trunk ID.
Description	The current description, if any, associated with the interface to help identify it.
Type	The interface type, which can be one of the following: <ul style="list-style-type: none">• Normal—The port is a normal port, which means it is not a Link Aggregation Group (LAG) member (also known as Trunk), or configured for port mirroring. All ports are normal ports by default.• Trunk Member—The port is a member of a trunk.• Mirrored—The port is configured to mirror its traffic (ingress, egress, or both) to another port (the probe port).• Probe—The port is configured to receive mirrored traffic from one or more source ports.
Admin Mode	The administrative mode of the interface. If a port or trunk is administratively disabled, it cannot forward traffic. The possible values are: <ul style="list-style-type: none">• Enabled—Administratively enabled.• Disabled—Administratively disabled.
Schedule	The schedule for activation of certain switch features, as defined in Schedule Configuration .
Physical Mode	The port speed and duplex mode. The modes are: <ul style="list-style-type: none">• Auto—the duplex mode and speed are set from the auto-negotiation process, based on the advertised capabilities.• Manual—the speed and duplex mode are those set manually by the user.
Physical Status	Indicates the port speed and duplex mode for physical interfaces. When a port is down, the physical status is unknown.

Field	Description
Auto Negotiation Capabilities	Indicates the list of configured capabilities for a port when Auto Negotiate is enabled.
STP Mode	<p>The Spanning Tree Protocol (STP) Administrative Mode associated with the port or LAG. STP is a layer 2 protocol that provides a tree topology for switches on a bridged LAN. STP allows a network to have redundant paths without the risk of network loops by providing a single path between end stations on a network. The possible values for STP mode are:</p> <ul style="list-style-type: none"> • Enabled—Spanning tree is enabled for this port. • Disabled—Spanning tree is disabled for this port.
LACP Mode	<p>Indicates the Link Aggregation Control Protocol administration state. This field can have the following values:</p> <ul style="list-style-type: none"> • Enabled—The port is a Trunk member. Trunk is an LACP Trunk. • Disabled—The port is a Trunk member. Trunk is a Static Trunk (not LACP). • N/A—The port is not a member of a Trunk, or port type is Trunk (TRK).
Link Status	<p>Indicates the link status of the port. The possible values are:</p> <ul style="list-style-type: none"> • Link Up. • Link Down. • Suspended—Automatically disabled by the system due to schedule configurations, or error conditions. For example, an interface may be disabled by the switch due to an error condition. See the error logs for more information.

Modifying Interface Settings

To change the port configuration of one or more interfaces, check the box to the left of one or more interfaces and click **Edit**  . To edit all the interfaces at the same time, click **Edit All**  .

Figure 34: Edit Port Configuration Dialog Box

Edit Port Configuration

Interface

1/1

Admin Mode

☒

Schedule

None

STP Mode

☒

Link Trap

☒

Physical Mode

Auto Negotiate

Negotiation Values

☒ 10M ☒ 100M ☒ 1G

Description

(0 – 64 characters)

Storm Control Limits

Broadcast Storm Control

☐

Broadcast Storm Control Limit Type

☒ Percent ☐ Rate

Broadcast Storm Control Limit

5

(1 – 100)

Broadcast Storm Control Action

None

Multicast Storm Control

☐

Multicast Storm Control Limit Type

CANCEL

APPLY

Click **APPLY** to save the changes for the current switch configuration. The changes take effect immediately and are applied to each of the selected interfaces. The changes are not retained across a switch reset unless you click **Save Configuration**.

Table 28: Edit Port Configuration Fields

Field	Description
Interface	Indicates the interface(s) that were selected for configuration.
Admin Mode	Enable or disable the port.
Schedule	Select one of the previously defined schedules. See Schedule Configuration for more information on schedules.
STP Mode	Enable or disable STP on the interface.
Link Trap	Enable or disable generating a trap when the interface link status (up/down) changes.
Physical Mode	Set the port speed and duplex to either auto-negotiation or one of the available options.
Negotiation Values	Determines the link speed settings advertised by the switch during the auto-negotiation.
Description	Describe the interface to help identify it.
Storm Control Limits	
Broadcast Storm Control	Enable or disable Broadcast Storm Control. If enabled, this feature limits the amount of broadcast frames accepted and forwarded by the port. If the broadcast traffic on the Ethernet port exceeds the configured threshold, the system blocks (discards) the broadcast traffic.
Broadcast Storm Control Limit Type	Select Percent or Rate for the type of broadcast storm control.
Broadcast Storm Control Limit	Set the threshold for broadcast storm control. Limits are defined as percentage, or rate of kbits per second. Valid values are 1-100. The default is 5.
Broadcast Storm Control Action	Storm control packets that exceed the threshold limit are dropped. This control specifies the additional actions to take if a broadcast storm is detected on the interface. The available options are: <ul style="list-style-type: none"> • None: No additional action is taken. • Trap: In addition to dropping exceeding traffic, a syslog message and an SNMP trap is sent approximately every 30 seconds until the broadcast storm recovers. • Shutdown: The interface which receives broadcast packets at a rate which is above the threshold is suspended.
Multicast Storm Control	Enable or disable Multicast Storm Control. If enabled, this feature limits the amount of multicast frames accepted and forwarded by the port. If the multicast traffic on the Ethernet port exceeds the configured threshold, the system blocks (discards) the multicast traffic.
Multicast Storm Control Limit Type	Select Percent or Rate for the type of multicast storm control.
Multicast Storm Control Limit	Set the threshold for multicast storm control. Limits are defined as percentage, or rate of kbits per second. Valid values are 1-100. The default is 5.
Multicast Storm Control Action	Storm control packets that exceed the threshold limit are dropped. This control specifies the additional actions to take if a multicast storm is detected on the interface. The available options are: <ul style="list-style-type: none"> • None: No additional action is taken. • Trap: In addition to dropping exceeding traffic, a syslog message and an SNMP trap is sent approximately every 30 seconds until multicast storm recovers. • Shutdown: The interface which receives multicast packets at a rate which is above the threshold is suspended.
Unicast Storm Control	Enable or disable Unicast Storm Control. If enabled, this feature limits the amount of unknown unicast frames accepted and forwarded by the switch. If the unicast traffic on the Ethernet port exceeds the configured threshold, the system blocks (discards) the unicast traffic.
Unicast Storm Control Limit Type	Select Percent or Rate for the type of unicast storm control.

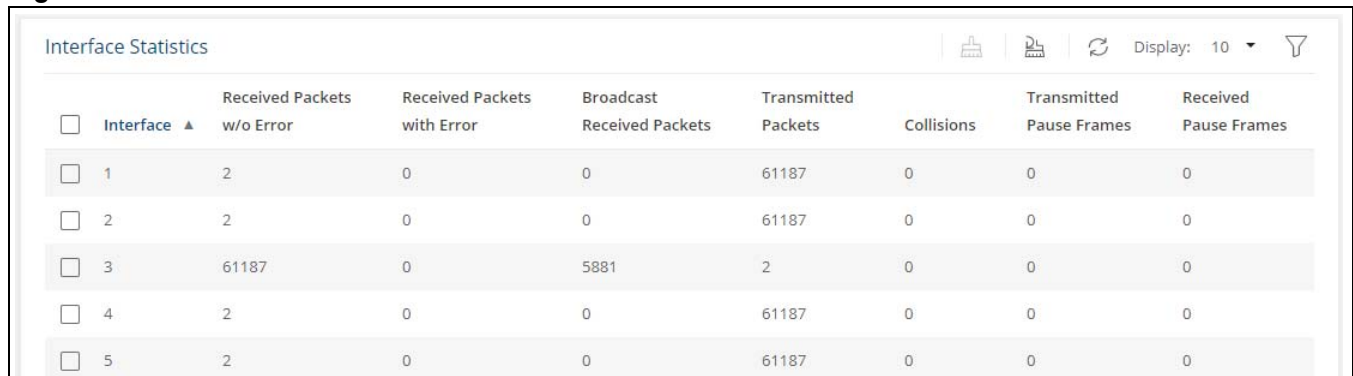
Field	Description
Unicast Storm Control Limit	Set the threshold for unicast storm control. Limits are defined as percentage, or rate of kbits per second. Valid values are 1-100. The default is 5.
Unicast Storm Control Action	Storm control packets that exceed the threshold limit are dropped. This control specifies the additional actions to take if a unicast storm is detected on the interface. The available options are: <ul style="list-style-type: none"> None: No additional action is taken. Trap: In addition to dropping exceeding traffic, a syslog message and an SNMP trap is sent approximately every 30 seconds until unicast storm control recovers. Shutdown: The interface which receives unicast packets at a rate which is above the threshold is suspended.

Interface Statistics

The Interface Statistics tile displays statistics on packets transmitted and received on each port or trunk. These statistics can be used to identify potential problems with the switch. The displayed values are the accumulated totals since the last clear operation.

To display the Interface Statistics tile, click **Switching > Port Configuration** in the navigation pane and scroll down to the **Interface Statistics** tile.

Figure 35: Interface Statistics Tile



☐ Interface ▲	Received Packets w/o Error	Received Packets with Error	Broadcast Received Packets	Transmitted Packets	Collisions	Transmitted Pause Frames	Received Pause Frames
☐ 1	2	0	0	61187	0	0	0
☐ 2	2	0	0	61187	0	0	0
☐ 3	61187	0	5881	2	0	0	0
☐ 4	2	0	0	61187	0	0	0
☐ 5	2	0	0	61187	0	0	0

Table 29: Interface Statistics Fields

Field	Description
Interface	The port or trunk ID.
Received Packets w/o Error	The count of packets received on the port without any packet errors.
Received Packets with Error	The count of packets received on the port with errors.
Broadcast Received Packets	The count of broadcast packets received on the port.
Transmitted Packets	The number of packets transmitted out of the port.
Collisions	The number of packet collisions.
Transmitted Pause Frames	The number of Ethernet pause frames transmitted. This information is collected for ports but not for trunks.
Received Pause Frames	The number of Ethernet pause frames received. This information is collected for ports but not for trunks.

Select a row and click **Clear**  to reset the row counters to zero.

Click **Clear All**  to reset all counters to zero.

Port Mirroring

Port Mirroring is used to monitor the network traffic that one or more ports send and receive. The Port Mirroring feature creates a copy of the traffic that the source interface handles and sends it to a probe port (also known as destination port).

All traffic from the source interfaces can be mirrored and sent to the probe port. A network protocol analyzer is typically connected to the destination port. Multiple switch ports can be configured as source interfaces, with each port mirrored to the same probe port.

To view this page, click **Switching > Port Mirroring** in the navigation pane.



When configuring port mirroring, avoid oversubscribing the destination port to prevent the loss of mirrored data.
While a port is used as the destination port for mirrored data, the port cannot be used for any other purpose; the port will not receive and forward traffic.

Mirroring Sessions

To display the Mirroring Sessions tile, click **Switching > Port Mirroring** in the navigation pane. The Mirroring Sessions tile appears.

Figure 36: Mirroring Sessions Tile

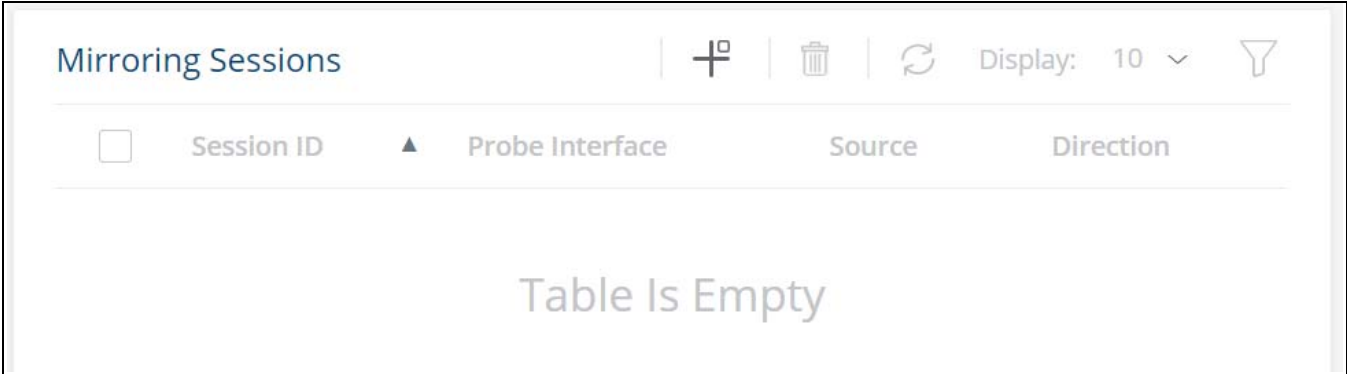


Table 30: Mirroring Sessions Fields

Field	Description
Session ID	The port mirroring session ID. Up to four port mirroring sessions are allowed.
Probe Interface	The switch port to which packets will be mirrored. Typically, a network protocol analyzer is connected to this port. If the port is configured as an interface or probe port, it receives traffic from all configured source ports.
Source	The ports or VLAN configured to mirror traffic to the destination. NOTE: You can configure multiple source ports or one source VLAN per session. VLANs can be defined as sources only in Session ID 1.
Direction	The direction of traffic on the source port (or source ports) that is sent to the specified destination. A source VLAN mirrors RX traffic only. Possible values for source ports are: <ul style="list-style-type: none">Tx/Rx – Both ingress and egress traffic.Rx – Ingress traffic only.Tx – Egress traffic only.

Configuring a Port Mirroring Session

To add a session in the **Mirroring Sessions** pane, click **Add**  .

To edit an existing session, click the check box to the left of the session entry and click **Edit**  . To remove an existing session, click the check box to the left of the session entry and click **Remove**  .

Figure 37: Add Mirroring Dialog Box

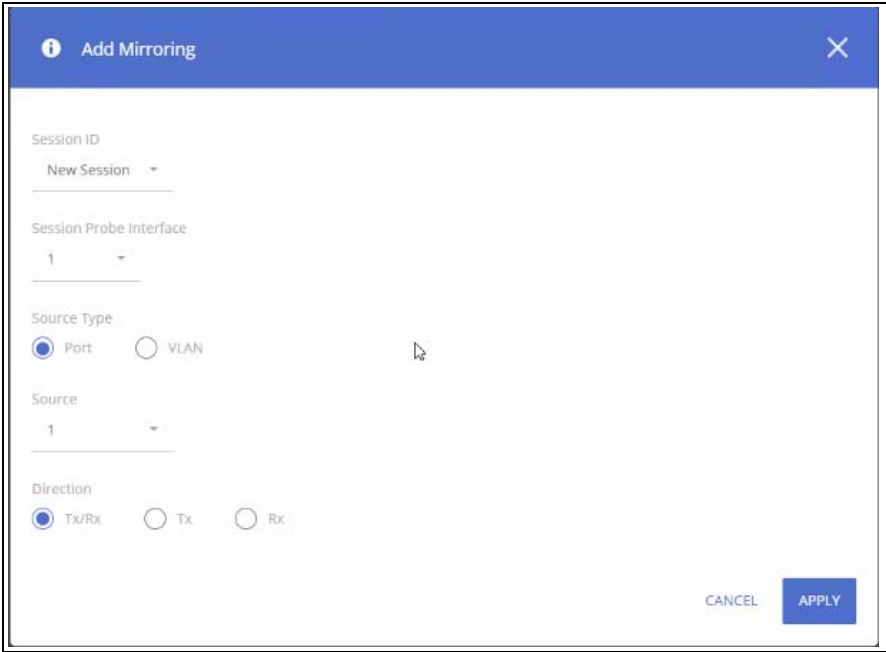
The image shows a dialog box titled "Add Mirroring" with a blue header bar containing an information icon and a close button. The dialog contains several fields: "Session ID" with a dropdown menu showing "New Session"; "Session Probe Interface" with a dropdown menu showing "1"; "Source Type" with two radio buttons, "Port" (selected) and "VLAN"; "Source" with a dropdown menu showing "1"; and "Direction" with three radio buttons, "Tx/Rx" (selected), "Tx", and "Rx". At the bottom right, there are "CANCEL" and "APPLY" buttons.

Table 31: Add Mirroring Dialog Box Fields

Field	Description
Session ID	The identifier for the session being configured. For a new session, the ID is New Session.
Session Probe Interface	The physical port to use as the source probe port to which traffic will be mirrored.
Source Type	The type of interface to use as the source: <ul style="list-style-type: none">• Port – Traffic is mirrored to and/or from a physical port on the switch.• VLAN – Traffic to a configured VLAN is mirrored. In other words, all the packets received on all the physical ports that are members of the VLAN are mirrored. VLAN can be specified as source only if the session ID is 1.
Source	Specify the source interfaces for mirrored traffic. interface type depends on the value set in the Source Type field.
Direction	The direction of traffic on the source port (or source ports) that is sent to the specified destination. A source VLAN mirrors only received packets. Possible values for source ports are: <ul style="list-style-type: none">• Tx/Rx – Both ingress and egress traffic.• Tx – Egress traffic only.• Rx – Ingress traffic only.

Click **APPLY** to apply the changes to the system.



A port will be removed from a VLAN when it becomes a destination (probe) port.



A port cannot be defined as a destination (probe) port if it is configured as a member of a LAG.

Loop Protection

Loops on a network consume resources and can degrade network performance. Detecting loops manually can be very cumbersome and time consuming. The HPE Networking Instant On 1930 Switch Series software provides an automatic loop protection feature.

This feature allows loop detection in the network for switches that do not run spanning tree, or on which STP feature is disabled.

When loop protection is enabled on the switch and on one or more interfaces (ports or trunks), the interfaces send loop protection protocol data units (PDUs) to the multicast destination address 09:00:09:09:13:A6, using the switch's base MAC address as the source address.

If STP is enabled on switch the interface will send PDUs only if STP is in the forwarding state.

When an interface receives a loop protection PDU, it compares the source MAC address with switch base MAC address and if there is a match a loop state is detected. Upon detection of a loop, the port is disabled. Once a port is disabled, for the duration of one second, other ports will not process loop protection PDUs. This is to allow the network to stabilize, following disabling the port.

A port that is disabled by loop protection can be recovered by one of the following:

- If auto-recovery is enabled for loop protection- after the timeout expires, the port attempts to recover.
- If auto-recovery is disabled - you may attempt to manually recover the port in the **Suspended Interface** tile on the **Switching > Interface Auto Recovery** page.

To view this page, click **Switching > Loop Protection** in the navigation pane.

Global Configuration

Figure 38: Global Configuration

The screenshot shows the 'Global Configuration' page. Under the 'Loop Protection' section, there is a toggle switch that is currently turned on (blue). Below this, the 'Transmission Time' is set to '10' seconds, with a range of '(5 - 60) Seconds' indicated below the input field.

Table 32: Global Configuration Fields

Field	Description
Loop Protection	Select Enabled or Disabled to administratively enable or disable this feature globally on the switch. This feature is disabled by default.

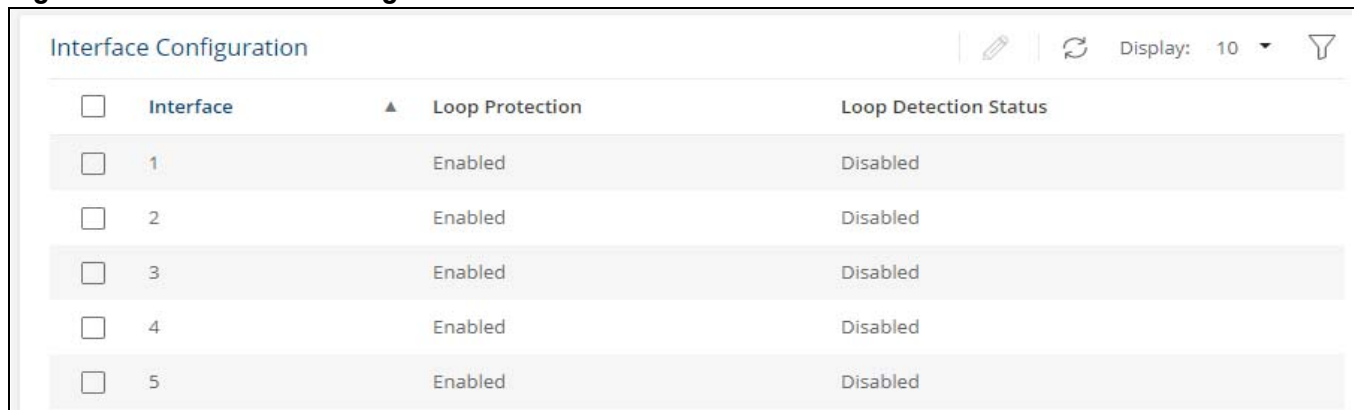
Field	Description
Transmission Time	The interval at which the switch sends loop protection PDUs on interfaces on which Loop Protection is enabled. The range is 5 to 60 seconds and the default is 10 seconds.

If you modify these settings, click **APPLY** to save the changes for the current switch configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Interface Configuration

Use the Interface Configuration tile enable Loop Detection and to display the status of this feature on each port. To display this tile, click **Switching > Loop Protection** in the navigation pane.

Figure 39: Interface Configuration Tile



☐ Interface	▲ Loop Protection	Loop Detection Status
☐ 1	Enabled	Disabled
☐ 2	Enabled	Disabled
☐ 3	Enabled	Disabled
☐ 4	Enabled	Disabled
☐ 5	Enabled	Disabled

Table 33: Loop Protection Interface Configuration Fields

Field	Description
Interface	The port or trunk ID.
Loop Protection	Indicates whether the feature is administratively enabled or disabled on the port. Loop Protection is disabled by default.
Loop Detection Status	The current loop protection status of the port. <ul style="list-style-type: none"> Enabled - no loop present Disabled - Loop detection is disabled, or the port is down Loop detected - Loop has been detected and port disabled Inactive - Loop detection operational state is disable for the port

Loop Protection Configuration

To configure loop protection for a specific interface, select the checkbox to the left of the interface entry and click **Edit**  .

Figure 40: Edit Loop Detection Dialog Box

The dialog box titled "Edit Loop Detection" contains the following elements:

- Header:** A blue bar with an information icon (i) and the title "Edit Loop Detection". A close button (X) is in the top right corner.
- Interface:** A text field labeled "Interface" with the value "1".
- Loop Protection:** A toggle switch labeled "Loop Protection" which is currently in the "off" position.
- Buttons:** "CANCEL" and "APPLY" buttons are located at the bottom right of the dialog.

Table 34: Edit Loop Protection Fields

Field	Description
Interface	The port or ports that are being configured.
Loop Protection	Enable or Disable to administratively enable or disable this feature on the selected interfaces. By default, this feature is disabled on all interfaces.

Click **APPLY** to save the changes for the current switch configuration. Your changes take effect immediately. The changes are not retained across a switch reset unless you click **Save Configuration**.

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows a switch to forward multicast traffic intelligently. Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports, which could affect network performance.

When enabled, the switch supports IGMPv1 and IGMPv2.

Global Configuration

To enable IGMP snooping and view global status information, click **Switching > IGMP Snooping** in the navigation pane.

Figure 41: Global Configuration Tile

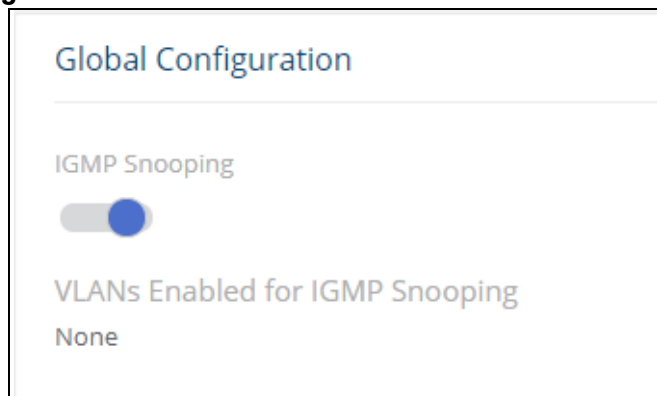


Table 35: Global Configuration Fields

Field	Description
IGMP Snooping	Set as Enabled to globally enable IGMP snooping on the switch. This feature is disabled by default.
VLANs Enabled for IGMP Snooping	Identifies the VLAN ID of each VLAN on which IGMP snooping is administratively enabled. If IGMP snooping is not enabled on any VLANs, this field shows None .

If you change the Admin Mode, click **APPLY** to save the changes for the current switch configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

IPv4 Unregistered Multicast

The IPv4 Unregistered Multicast feature enables configuring the handling of Multicast Frames that belong to unregistered Multicast groups. Unregistered Multicast groups are the groups that are not known to the switch. The Multicast switch (when it operates as an L2 switch) learns about Multicast groups by IGMP Snooping, or by static configuration.

Normally, Multicast frames are always flooded to all ports in the VLAN. If IGMP Snooping is enabled, the switch learns about the existence of Multicast groups and keeps track of which ports joined to which Multicast group. This enables the switch to forward the Multicast frames (from a registered Multicast group) only to ports that are registered to that Multicast group.

All unregistered Multicast frames, i.e. the Multicast frames that do not belong to a registered Multicast group, are still flooded to all ports on the VLAN. The **IPv4 Unregistered Multicast** feature enables to configure whether to forward or to filter these Multicast frames to specific ports.

This configuration is done per egress port. Once an egress port has been set to filter/forward then this port's configuration is valid for any VLAN it is member of or will be member of.

Figure 42: IPv4 Unregistered Multicast

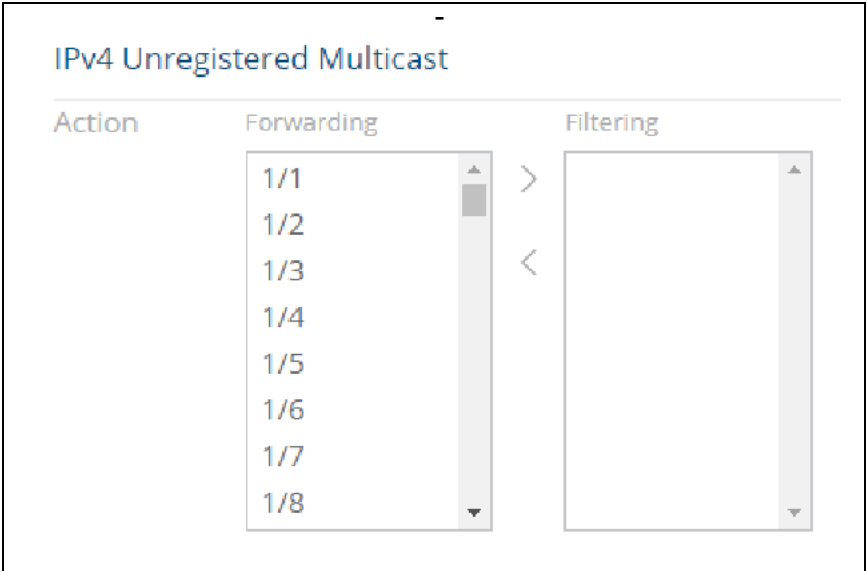


Table 36: IPv4 Unregistered Multicast Fields

Field	Description
Forwarding	This box lists the ports from which unregistered multicast addresses are forwarded to all the ports on the VLAN. Use the arrow buttons to move addresses to or from this list.
Filtering	This box lists the ports from which unregistered multicast addresses are filtered. Use the arrow buttons to move addresses to or from this list.

IGMP Snooping VLAN Configuration

Use the **IGMP Snooping VLAN Configuration** tile to configure IGMP snooping settings on specific VLANs. To access the tile, click **Switching > IGMP Snooping** in the navigation pane.

Figure 43: IGMP Snooping VLAN Configuration Tile

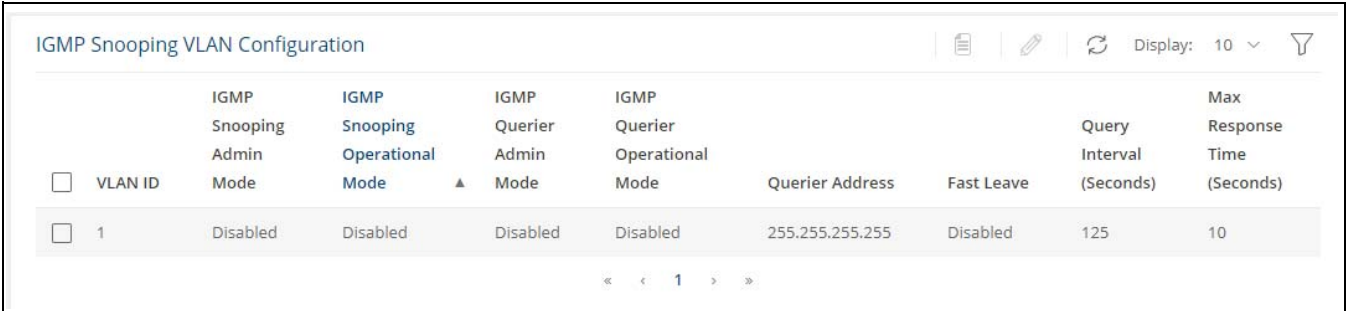
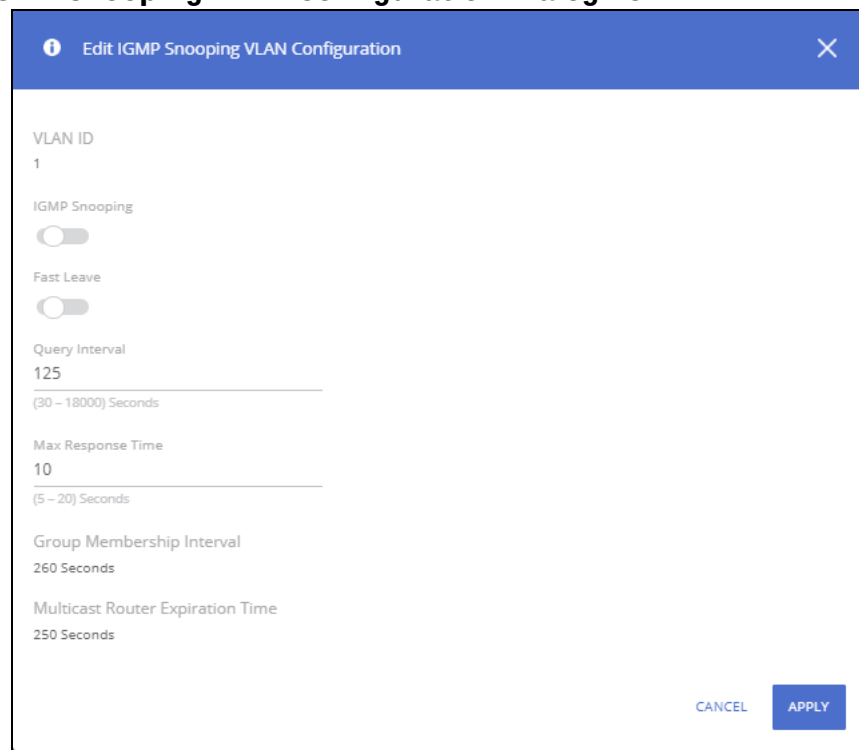


Table 37: IGMP Snooping VLAN Configuration Fields

Field	Description
VLAN ID	The VLAN interface associated with the rest of the data in the row. When configuring IGMP snooping settings, this field identifies the VLAN interface(s) that are being configured.
IGMP Snooping Admin Mode	The administrative mode of IGMP snooping on the VLAN interface. IGMP snooping must be enabled globally and on an VLAN interface to be able to snoop IGMP packets and determine which segments should receive multicast packets directed to the group address.
Fast Leave	The administrative mode of Fast Leave on the VLAN interface. If Fast Leave is enabled, the VLAN interface can be immediately removed from the Layer 2 forwarding table entry upon receiving an IGMP leave message for a multicast group without first sending out MAC-based general queries.
Query Interval (Seconds)	The expected Frequency, in seconds, at which IGMP query messages are forwarded on this VLAN interface.
Max Response Time (Seconds)	The maximum number of seconds a host can wait before sending a group report once it receives a membership query. The specified value should be less than the Group Membership Interval.
Group Membership Interval (Seconds)	The number of seconds the VLAN interface should wait for a report for a particular group on the VLAN interface before the IGMP snooping feature deletes the VLAN interface from the group. This field is read-only. The value shown is calculated based on the following formula: $\text{Query interval} * 2 + \text{max response time}$
Multicast Router Expiration Time (Seconds)	The number of seconds the VLAN interface should wait to receive a query before it is removed from the list of VLAN interfaces with multicast routers attached. This field is read-only. The value shown is calculated based on the following formula: $\text{Query interval} * 2$

To change the snooping VLAN configuration, check the box to the left of one or more interfaces and click **Edit**  .

Figure 44: Edit IGMP Snooping VLAN Configuration Dialog Box

The dialog box is titled "Edit IGMP Snooping VLAN Configuration" and contains the following fields and controls:

- VLAN ID:** 1
- IGMP Snooping:** A toggle switch that is currently turned on.
- Fast Leave:** A toggle switch that is currently turned off.
- Query Interval:** 125 (30 – 18000) Seconds
- Max Response Time:** 10 (5 – 20) Seconds
- Group Membership Interval:** 260 Seconds
- Multicast Router Expiration Time:** 250 Seconds

At the bottom right, there are two buttons: "CANCEL" and "APPLY".

Click **APPLY** to save the changes for the current switch configuration. The changes take effect immediately and are applied to each of the selected interfaces. The changes are not retained across a switch reset unless you click **Save Configuration**.

Table 38: Edit IGMP Snooping VLAN Configuration Fields

Field	Description
VLAN ID	The VLAN interface(s) that are being configured.
IGMP Snooping	The administrative mode of IGMP snooping on the VLAN interface. To be operational, IGMP snooping needs to be enabled globally and on the VLAN.
Fast Leave	The administrative mode of Fast Leave on the VLAN interface. If Fast Leave is enabled, the VLAN interface can be immediately removed from the Layer 2 forwarding table entry upon receiving an IGMP leave message for a multicast group without first sending out group-based general queries.
Query Interval	The expected Frequency, in seconds, at which IGMP query messages are sent on this VLAN interface.
Max Response Time	The maximum number of seconds a host can wait before sending a group report once it receives a membership query. The specified value should be less than the Group Membership Interval.
Group Membership Interval	The interval that must pass before the router decides that no members of a group or source exist on the network. This value is not configurable. The default is 260 seconds.
Multicast Router Expiration Time	The number of seconds after which a multicast router entry is timed out. This value is not configurable. The default value is 250 seconds.

The **Details**  button displays the **IGMP Snooping VLAN Configuration** fields and the operational values related to IGMP snooping timers on the interface.

Figure 45: IGMP Snooping VLAN Details

IGMP Snooping VLAN Details

VLAN ID

1

IGMP Snooping Administrative Mode

Disabled

Fast Leave

Disabled

Administrative Query Interval

125

Operational Query Interval

125

Administrative Max Response Time

10

Operational Max Response Time

10

Administrative Group Membership Interval

260

Operational Group Membership Interval

260

Administrative Router Expiration Time

250

Operational Router Expiration Time

250

CLOSE

These are the additional fields that are shown in the **Details** dialog box.

Table 39: IGMP Snooping VLAN Additional Details Fields

Field	Description
Administrative Query Interval	Indicates the value that was configured for the Query Interval parameter.
Operational Query Interval	Indicates the Query Interval configured for this VLAN.
Administrative Max Response Time	Indicates the Max Response Time configured for this VLAN.
Operational Max Response Time	Indicates the operational value of the Max Response Time parameter.
Administrative Group Membership Interval	Indicates the Group Membership Interval configured for this VLAN. The following formula is used to calculate the Group Membership Interval: (Query Interval (configured))*2 + Max Response Time (configured).
Operational Group Membership Interval	Indicates the operational value of the Group Membership Interval parameter.

Field	Description
Administrative Router Expiration Time	Indicates the Router Expiration Time configured for this VLAN.
Operational Router Expiration Time	Indicates the operational value of the Router Expiration Time parameter.

IGMP Snooping Multicast Router Interface Configuration

Use this tile to manually configure an interface within a VLAN as a IGMP snooping multicast router interface. If a multicast router is attached to the switch, its existence can be learned dynamically. You can also statically configure an interface as a multicast router interface, which is an interface that faces a multicast router and receives multicast traffic.

To access the tile, click **Switching** > **IGMP Snooping** in the navigation pane.

Figure 46: IGMP Snooping Multicast Router Configuration Tile

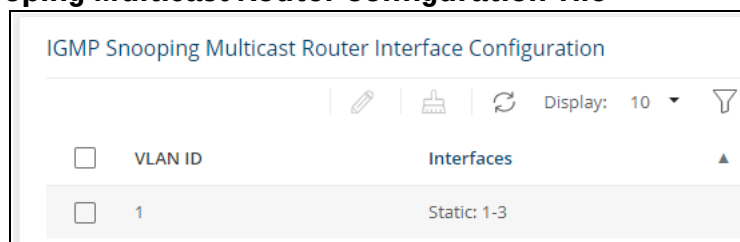


Table 40: IGMP Snooping Multicast Router Configuration Fields

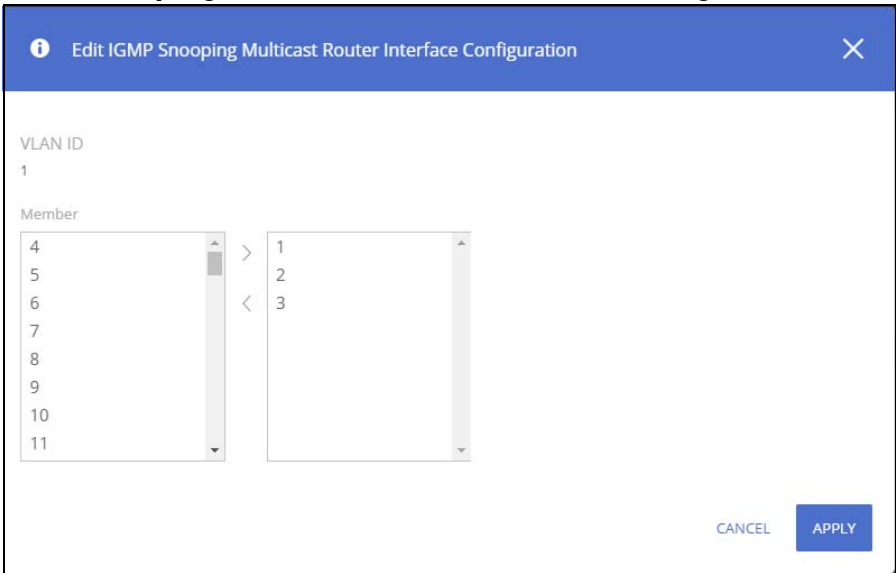
Field	Description
VLAN ID	The VLAN ID associated with the rest of the data in the row. When configuring the IGMP snooping multicast router settings, this field identifies the VLAN(s) that are being configured
Interfaces	List the ports in this VLAN which are Multicast Router interfaces. Membership can be dynamic or static.

Configuring Multicast Router Settings on Interfaces

To remove a static entry, click **Remove Static**  .

To change the multicast router membership for one or more interfaces, select each entry (that is, VLAN) you wish to modify and click **Edit**  .

Figure 47: Edit IGMP Snooping Multicast Router Interface Configuration Dialog Box



Select one or more interfaces that you want to configure as IGMP snooping multicast router interfaces and click the right arrow. To remove an interface from the list on the right, select it and press the left arrow.

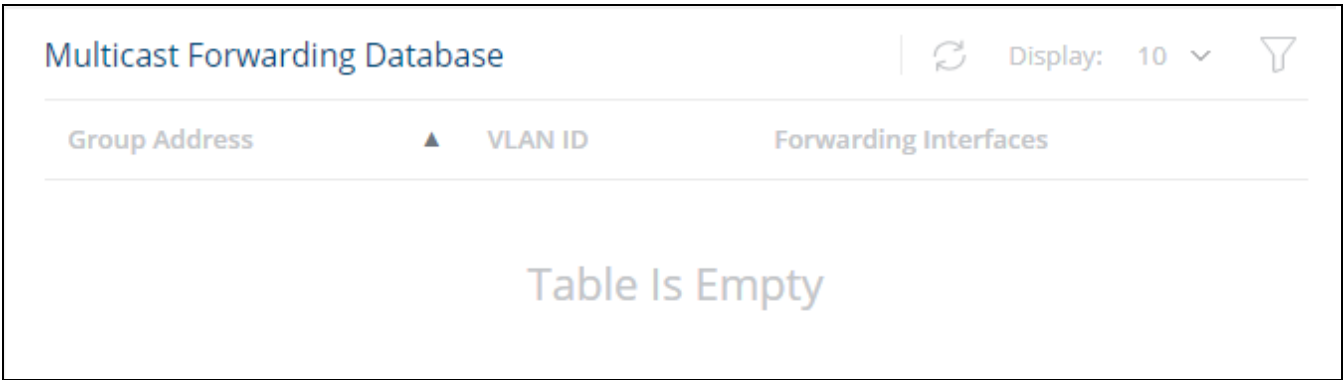
Click **APPLY** to save the changes for the current switch configuration. The changes take effect immediately and are applied to each of the selected interfaces. The changes are not retained across a switch reset unless you click **Save Configuration**.

Multicast Forwarding Database

This tile displays the Multicast group addresses learned from IGMP. Interface membership is displayed for each VLAN

To access the tile, click **Switching > IGMP Snooping** in the navigation pane.

Figure 48: Multicast Forwarding Database Tile



To refresh the list, click **Refresh**  .

To filter the list, click **Filter**  .

Table 41: Multicast Forwarding Database Fields

Field	Description
Group Address	The Multicast group for which information is displayed.
VLAN ID	The ID of the VLANs on which multicast groups were registered.
Forwarding Interfaces	Interfaces that are registered to this group.

SNMP

Simple Network Management Protocol (SNMP) provides a method for managing network devices. The switch supports SNMP version 1, SNMP version 2, and SNMP version 3.

SNMP v1 and v2

The SNMP agent maintains a list of variables, which are used to manage the switch. The variables are defined in the *Management Information Base* (MIB). The MIB presents the variables controlled by the agent. The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agent are controlled by access strings (also called community strings).

SNMP v3

SNMP v3 also applies access control and a new traps mechanism to SNMPv1 and SNMPv2 PDUs. In addition, the User Security Model (USM) is defined for SNMPv3 and includes:

- **Authentication:** Provides data integrity and data origin authentication.
- **Privacy:** Protects against disclosure of message content. Cipher-Block-Chaining (CBC) is used for encryption. Either authentication is enabled on an SNMP message, or both authentication and privacy are enabled on an SNMP message. However privacy cannot be enabled without authentication.
- **Timeliness:** Protects against message delay or message redundancy. The SNMP agent compares an incoming message to the message time information.
- **Key Management:** Defines key generation, key updates, and key use.

The switch supports SNMP notification filters based on Object IDs (OID). OIDs are used by the system to manage switch features. SNMP v3 supports the following features:

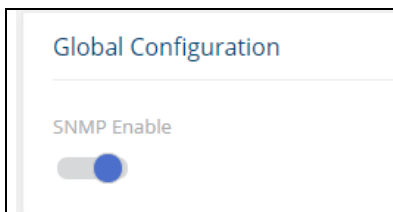
- Security
- Feature Access Control
- Traps

Authentication or Privacy Keys are modified in the SNMPv3 User Security Model (USM).

Global Configuration

To globally enable SNMP, set **SNMP Enable** in the **Global Configuration** section. Click **APPLY** to save the changes for the current switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Figure 49: Global SNMP



Community Configuration

Access rights are managed by defining communities on the Community Configuration tile. When the community names are changed, access rights are also changed. SNMP Communities are defined only for SNMP v1 and SNMP v2.

Use the SNMP Community Configuration tile to add SNMP communities and community groups.

To display the Community Configuration tile, click **Switching > SNMP** in the navigation pane.

Figure 50: Community Configuration Tile

Community Configuration							Display: 10		
☐	Community Name	▲	IP Address	Community Type	Access	View	Group Name		
☐	comg1		0.0.0.0	Community Group			DefaultRead		

Table 42: Community Configuration Fields

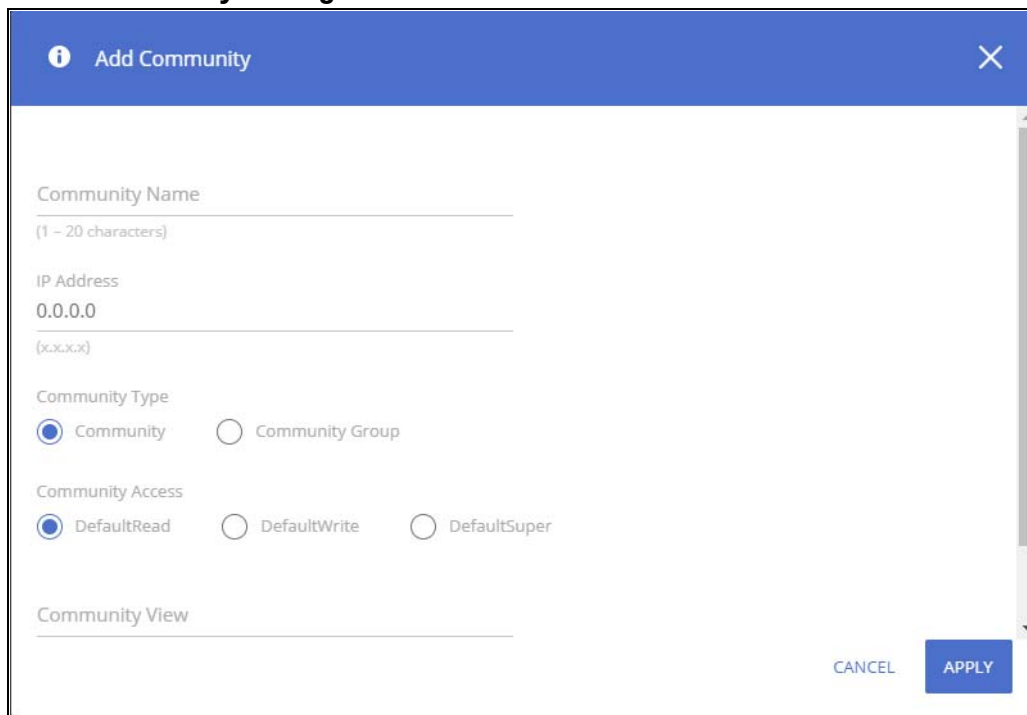
Field	Description
Community Name	Community name used in SNMPv1/v2 packets. This is configured in the client and identifies the access the user may connect with.
IP Address	Specifies the IP address that can connect with this community. The address must be an IPv4 address.
Community Type	This is either Community or Community Group .
Community Access	Specifies the access control policy for the community. This is available only for Communities.. The default access privileges are as follows: <ul style="list-style-type: none">• DefaultRead: Read access to the entire MIB tree except to SNMP configuration objects.• DefaultWrite: Write access to the entire MIB tree except to SNMP configuration objects.• DefaultSuper: Read and Write access to the entire MIB tree.
View	Specifies the community view for the community. This is available only for Communities.. If the value is empty, then no access is granted. A view is used to restrict or grant access to specific MIB trees. For example, it is possible to define a view to grant access to the mib-2 tree but deny access to the RMON MIB subtree, or a view could allow access to only the RADIUS Accounting and Authentication MIBs. In this way, it is possible to define a community that has access rights of a (restricted) view.
Group Name	Identifies the Group associated with this Community entry. This is available only for Community Groups.

Click **APPLY** to save the changes for the current switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Adding/Editing an SNMP Community or Community Group

To add a new SNMP community, click **Add** . The **Add Community** dialog box appears.

Figure 51: Add Community Dialog Box

The image shows a dialog box titled "Add Community" with a blue header bar containing an information icon and a close button. The main area is white and contains several form fields: "Community Name" with a placeholder "(1 - 20 characters)", "IP Address" with a placeholder "0.0.0.0" and "(x.x.x.x)", "Community Type" with two radio buttons "Community" (selected) and "Community Group", "Community Access" with three radio buttons "DefaultRead" (selected), "DefaultWrite", and "DefaultSuper", and "Community View" with a text input field. At the bottom right, there are "CANCEL" and "APPLY" buttons.

To edit an existing SNMP community, check the box to the left of the community to edit, and click **Edit** . The **Edit Community** dialog box appears.

Configure the community fields and click **APPLY**.

Removing an SNMP Community or Community Group

To remove an SNMP community or community group, select each item to delete and click **Remove** .

SNMP Trap Receivers

The SNMP Trap Receivers tile includes two tabs:

- SNMP Trap Receivers v1/v2.
- SNMP Trap Receivers v3.

To access the Trap Receiver v1/v2 Configuration tile, click **Switching** > **SNMP** in the navigation pane. The **SNMP Trap Receivers v1/v2** tab is selected by default.

SNMP Trap Receivers v1/v2

Use the SNMP v1/v2 Trap Receivers tab to configure settings for each SNMPv1 or SNMPv2 management host that will receive notifications about traps generated by the switch. The SNMP management host is also known as the SNMP trap receiver.

You can configure up to 8 SNMP trap receivers in this tab.



Creating a new SNMPv1/2 trap with the same IP address as an existing one will overwrite the the existing entry even if configured with a different SNMP version.

Figure 52: SNMP Trap Receivers v1/v2 Tab

SNMP Trap Receivers v1/v2		SNMP Trap Receivers v3						Display: 10		
☐	Host IP Address	Community Name	Notify Type	SNMP Version	Timeout (Sec)	Retries	Filter	UDP Port		
☐	1.1.1.1	Trap1	Traps	v1				162		

Table 43: SNMP Trap Receivers v1/v2 Fields

Field	Description
Host IP Address	The IP address of the SNMP management host that will receive traps generated by the switch.
Community Name	The name of the SNMP community that includes the SNMP management host and the SNMP agent on the switch.
Notify Type	The type of SNMP notification to send the SNMP management host: <ul style="list-style-type: none">• Trap – An SNMP message that notifies the host when a certain event has occurred on the switch. The message is not acknowledged by the SNMP management host.• Inform – An SNMP message that notifies the host when a certain event has occurred on the switch. The message is acknowledged by the SNMP management host. This type of notification is not available for SNMPv1.
SNMP Version	The version of SNMP to use, which is either SNMPv1 or SNMPv2.
Timeout Value	The number of seconds to wait for an acknowledgment from the SNMP management host before resending an inform message.
Retries	The number of times to resend an inform message that is not acknowledged by the SNMP management host.
Filter	The name of the filter for the SNMP management host. The filter defines which MIB OID notifications to be sent or not sent to the SNMP management host. This field is optional.
UDP Port	The UDP port on the SNMP management host that will receive the SNMP notifications. If no value is specified when configuring a receiver, the default UDP port value is used.

Click **APPLY** to save the changes for the current switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Adding an SNMP v1/v2 Trap Receiver

To add a SNMP v1/v2 trap receiver, click **Add** . The **Add Trap Receiver** dialog box appears.

Figure 53: Add Trap Receiver Dialog Box

Add Trap Receiver

Host IP Address

(x.x.x.x)

Community Name

(1 – 20 characters)

Notify Type

☒ Trap ☐ Inform

SNMP Version

☒ SNMPv1 ☐ SNMPv2

Timeout Value

CANCEL

APPLY

Configure the required fields and click **APPLY**. Note that the Retries and Timeout Value fields are available only if the selected **Notify Type** is **Inform**.

To edit an existing trap receiver, select it in the table, click **Edit**  , and edit the fields as needed.

Removing an SNMP v1/v2 Trap Receiver

To remove an SNMP v1/v2 trap receiver, select each item to delete and click **Remove**  .

SNMP Trap Receivers v3

Use the SNMP Trap Receivers v3 tab to configure settings for each SNMPv3 management host that will receive notifications about traps generated by the switch. The SNMP management host is also known as the SNMP trap receiver.

You can configure up to 8 SNMP trap receivers in this tab.

To access the Trap Receiver v3 Configuration tab, click **Switching > SNMP** in the navigation pane, and then click the **SNMP Trap Receivers v3** tab.

Figure 54: SNMP v3 Trap Receivers Tab

SNMP Trap Receivers v1/v2 SNMP Trap Receivers v3									
☐		Host IP Address	▲	Username	Notify Type	Security Level	Timeout (Sec)	Retries	Filter
☐		1.1.1.1		admin	Traps	No Auth No Priv			162

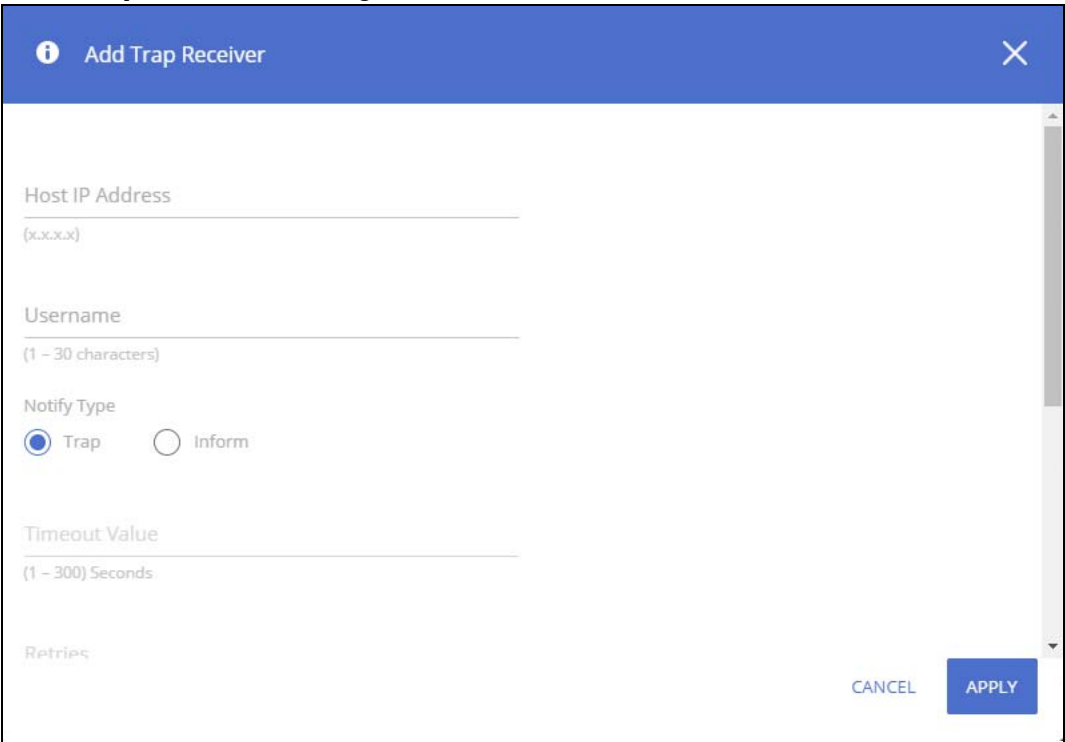
Table 44: SNMP Trap Receivers v3 Fields

Field	Description
Host IP Address	The IP address of the SNMP management host that will receive traps generated by the switch.
Username	The name of the SNMP user that is authorized to receive the SNMP notification.
Notify Type	The type of SNMP notification to send the SNMP management host: <ul style="list-style-type: none">• Inform – An SNMP message that notifies the host when a certain event has occurred on the switch. The message is acknowledged by the SNMP management host. This type of notification is not available for SNMPv1.• Trap – An SNMP message that notifies the host when a certain event has occurred on the switch. The message is not acknowledged by the SNMP management host.
Timeout Value	The number of seconds to wait for an acknowledgment from the SNMP management host before resending an inform message.
Retries	The number of times to resend an inform message that is not acknowledged by the SNMP management host.
Security Level	The security level associated with the SNMP user, which is one of the following: <ul style="list-style-type: none">• No Auth No Priv – No authentication and no data encryption (no security).• Auth No Priv – Authentication, but no data encryption. With this security level, users send SNMP messages that use an MD5 key/password for authentication, but not a DES key/password for encryption.• Auth Priv – Authentication and data encryption. With this security level, users send an MD5 key/password for authentication and a DES key/password for encryption.
Filter	The name of the filter for the SNMP management host. The filter defines which MIB objects to include or exclude from the view. This field is optional.
UDP Port	The UDP port on the SNMP management host that will receive the SNMP notifications. If no value is specified when configuring a receiver, the default UDP port value is used.

Adding an SNMP v3 Trap Receiver

To add a SNMP v3 trap receiver, click **Add**  . The **Add Trap Receiver** dialog box appears.

Figure 55: Add Trap Receiver Dialog Box



The dialog box has a blue header with an information icon, the title "Add Trap Receiver", and a close button. The main area contains the following fields and controls:

- Host IP Address:** A text input field with a placeholder "(x.x.x.x)".
- Username:** A text input field with a placeholder "(1 - 30 characters)".
- Notify Type:** Two radio buttons labeled "Trap" (selected) and "Inform".
- Timeout Value:** A text input field with a placeholder "(1 - 300) Seconds". This field is disabled when "Trap" is selected.
- Retries:** A text input field with a placeholder "(1 - 30) Retries". This field is disabled when "Trap" is selected.
- Buttons:** "CANCEL" and "APPLY" buttons at the bottom right.

Configure the required fields and click **APPLY**. Note that the Retries and Timeout Value fields are available only if the selected Notify Type is Inform.

To edit an existing trap receiver, select it in the table, click **Edit** , and edit the fields as needed.

Removing an SNMP v3 Trap Receiver

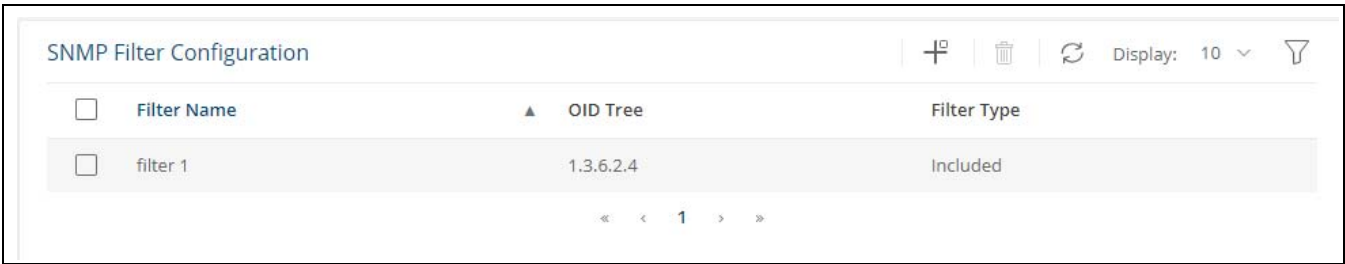
To remove an SNMP v3trap receiver, select each item to delete and click **Remove**  .

SNMP Filter Configuration

The SNMP Filter Configuration tile enables you to configure SNMP notification filters. An SNMP filter defines Object IDs (OIDs) that are included or excluded from the filter.

After defining a notification filter, it can be attached to an SNMP receiver using the SNMP Trap Receivers tile (V1/2 or V3 receiver).

Figure 56: SNMP Filter Configuration Tile



The tile has a title "SNMP Filter Configuration" and a toolbar with icons for adding, deleting, and refreshing, along with a "Display: 10" dropdown and a filter icon.

☐	Filter Name	OID Tree	Filter Type
☐	filter 1	1.3.6.2.4	Included

At the bottom of the table are pagination controls: << < 1 > >>

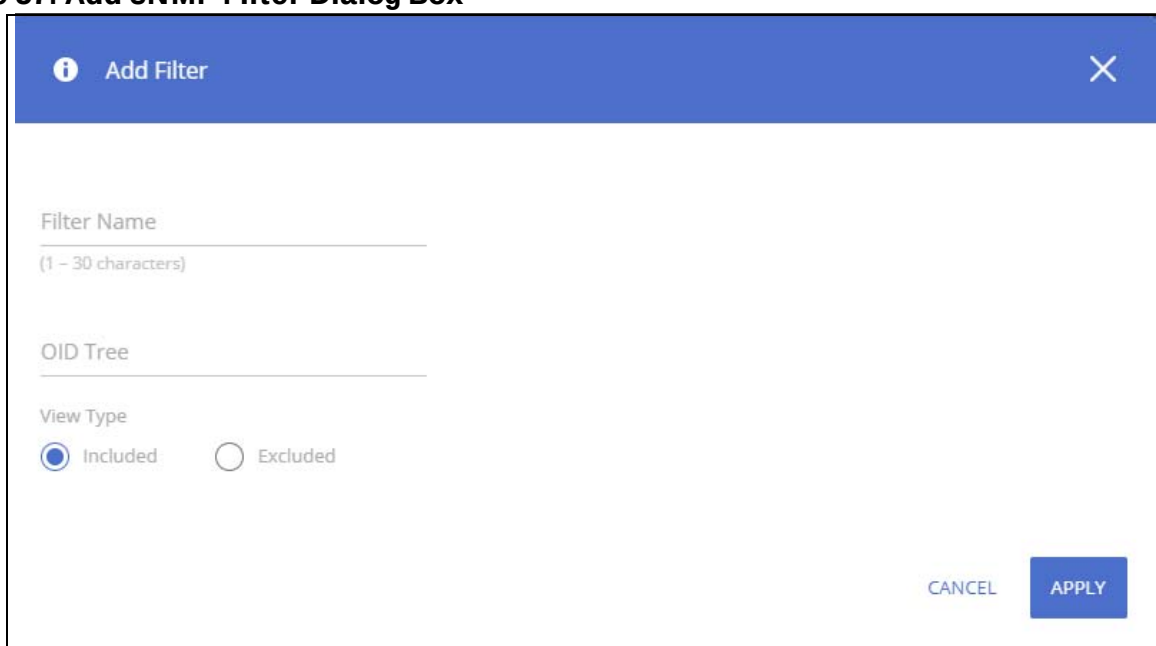
Table 45: SNMP Filter Configuration Fields

Field	Description
Filter Name	The name of the filter configuration name.
OID	The node in the MIB tree that is included or excluded in this SNMP filter.
Filter Type	The type of SNMP filter: <ul style="list-style-type: none">• Excluded - notifications are not sent for this OID• Included - notifications are sent for this OID.

Click **APPLY** to save the changes for the current switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Adding an SNMP Configuration Filter

To add a SNMP configuration filter, click **Add** . The **Add SNMP Configuration** dialog box appears.

Figure 57: Add SNMP Filter Dialog BoxThe image shows a dialog box titled "Add Filter" with a blue header bar containing an information icon and a close button. The main area is white and contains three input fields: "Filter Name" with a placeholder "(1 - 30 characters)", "OID Tree", and "View Type". Under "View Type", there are two radio buttons: "Included" (which is selected) and "Excluded". At the bottom right, there are two buttons: "CANCEL" and "APPLY".

For the OID tree, use the ASN.1 subtree object identifier format, such as 1.3.6.2.4.

To specify a subtree family, replace a single sub-identifier with the asterisk (*) wildcard. For example, 1.3.*.4. In this case, the asterisk (*) is replaced with '0' in the table.

In addition to the OID tree, specify a filter name and type, and click **APPLY** to add the SNMP filter to the table.

Removing an SNMP Filter

To remove an SNMP filter, select each item to delete and click **Remove** .

SNMP Access Control Group Configuration

Use this tile to configure SNMP access control groups. These SNMP groups allow network managers to assign different levels of authorization and access rights to specific switch features and their attributes.

The SNMP group can be referenced by the SNMP community to provide security and context for agents receiving requests and initiating traps as well as for management systems and their tasks. An SNMP agent will not respond to a request from a management system outside of its configured group, but an agent can be a member of multiple groups at the same time to allow communication with SNMP managers from different groups. Several default SNMP groups are preconfigured on the system.

To access the SNMP Access Control Group Configuration tile, click **Switching > SNMP** in the navigation pane.

Figure 58: SNMP Access Control Group Configuration Tile

SNMP Access Control Group Configuration						
☐	Group Name	SNMP Version	Security Level	Read	Write	Notify
☐	DefaultRead	v3	No Auth No Priv	Default		Default
☐	DefaultSuper	v1	No Auth No Priv	DefaultSuper	DefaultSuper	DefaultSuper
☐	DefaultWrite	v3	No Auth No Priv	Default	Default	Default
☐	g1	v3	No Auth No Priv			Default

Table 46: SNMP Access Control Group Configuration Fields

Field	Description
Group Name	The name that identifies the SNMP group.
SNMP Version	The SNMP version associated with the group.
Security Level	The security level associated with the group, which is one of the following: <ul style="list-style-type: none">No Auth No Priv – No authentication and no data encryption (no security). This is the only Security Level available for SNMPv1 and SNMPv2 groups.Auth No Priv – Authentication, but no data encryption. With this security level, users send SNMP messages that use an MD5 key/password for authentication, but not a DES key/password for encryption.Auth Priv – Authentication and data encryption. With this security level, users send an MD5 key/password for authentication and a DES key/password for encryption.
Read	The level of read access rights for the group. The menu includes the available SNMP views. When adding a group, enable this setting to allow the field to be configured, then select the desired view that restricts management access to viewing the contents of the agent.
Write	The level of write access rights for the group. The menu includes the available SNMP views. When adding a group, enable this setting to allow the field to be configured, then select the desired view that permits management read-write access to viewing the contents of the agent, but not to the community.
Notify	The level of notify access rights for the group.

Adding an SNMP Access Control Group

To add a SNMP access control group click **Add** . The **Add Access Control Group** dialog box appears.

Figure 59: Add New Access Control Group Dialog Box

Add Access Control Group

Group Name

(1 - 30 characters)

SNMP Version

☒ SNMPv1

☐ SNMPv2

☐ SNMPv3

Security Level

☒ No Auth No Priv

☐ Auth No Priv

☐ Auth Priv

Read Access

☐

Default

Write Access

☐

Default

Notification Access

☐

Default

CANCEL

APPLY

Configure the required fields and click **APPLY**.

Removing an SNMP Access Control Group

To remove an SNMP Access Control Group receiver, select each item to delete and click **Remove**  .

SNMP User Configuration

The SNMP User Configuration tile provides the capability to configure the SNMP v3 user accounts. To access the User Configuration tile, click **Switching > SNMP** and scroll down to the **SNMP User Configuration** tile.

Figure 60: SNMP User Configuration Tile

SNMP User Configuration					
<div><div><div></div><div></div><div></div></div><div>Display: 10</div><div></div></div>					
☐	Username	Group Name	Engine ID	Authentication	Privacy
☐	admin	admin	8000000b03000016052019	None	None

Table 47: SNMP User Configuration Fields

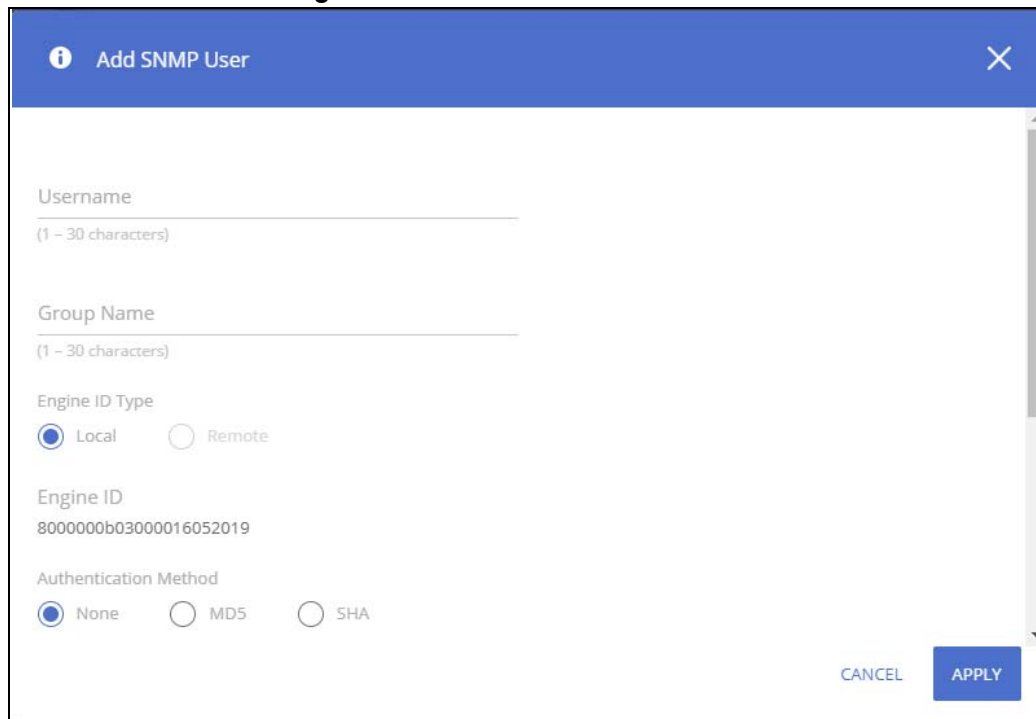
Field	Description
Username	Specifies the name of the SNMP user being added for the User-based Security Model (USM). Each Username must be unique within the SNMP agent user list. A Username cannot contain any leading or embedded blanks.

Field	Description
Group Name	A SNMP group is a group to which hosts running the SNMP service belong. A group name parameter is simply the name of that group by which SNMP communities are identified. The use of a group name provides some security and context for agents receiving requests and initiating traps and does the same for management systems and their tasks. An SNMP agent won't respond to a request from a management system outside its configured group, but an agent can be a member of multiple groups at the same time. This allows for communications with SNMP managers from different groups.
Engine ID	Each SNMPv3 agent has an engine ID that uniquely identifies the agent in the network. This field takes an hexadecimal string in the form of 0102030405.
Authentication	The authentication protocol to be used on authenticated messages on behalf of the user. <ul style="list-style-type: none"> • None - No authentication will be used for this user. • MD5 - MD5 protocol will be used. This option requires a password of 1-32 hexadecimal characters. • SHA - SHA protocol will be used. This option requires a password of 1-32 hexadecimal characters.
Privacy	Specifies the privacy protocol to be used on encrypted messages on behalf of the specified user. This parameter is only valid if the value in the Authentication Method field is not None. <ul style="list-style-type: none"> • None - No privacy protocol will be used. • DES - DES protocol will be used. This option requires an authentication key of 1-32 hexadecimal characters.

Adding an SNMP User

To add an SNMP v3 user, click **Add** . The **Add SNMP User** screen appears.

Figure 61: Add SNMP User Dialog Box



The dialog box titled "Add SNMP User" contains the following fields and options:

- Username**: A text input field with a placeholder "(1 - 30 characters)".
- Group Name**: A text input field with a placeholder "(1 - 30 characters)".
- Engine ID Type**: Two radio buttons, "Local" (selected) and "Remote".
- Engine ID**: A text input field containing the value "8000000b03000016052019".
- Authentication Method**: Three radio buttons, "None" (selected), "MD5", and "SHA".

At the bottom right, there are two buttons: "CANCEL" and "APPLY".

The following fields appear in the configuration dialog, but are not described in [SNMP User Configuration Fields](#).

Table 48: Add SNMP User Fields

Field	Description
Engine ID Type	Specify whether the engine ID for the SNMP v3 agent is local or remote. If the agent is local, the engine ID is automatically generated. If the agent is remote, you must specify the engine ID.
Authentication Method	The authentication protocol to be used on authenticated messages on behalf of the user. <ul style="list-style-type: none">• None - No authentication will be used for this user.• MD5 - MD5 protocol will be used. This option requires a password of 1-32 hexadecimal characters.• SHA - SHA protocol will be used. This option requires a password of 1-32 hexadecimal characters.
Password	If the Authentication Method is MD5 or SHA, use this field to specify the password used to generate the key to be used in authenticating messages on behalf of this user. If the Authentication Method is MD5-Key or SHA-Key, use this field to specify the pregenerated MD5 or SHA authentication key.
Privacy Key	This field is available on the Add New SNMP User dialog box. Specifies the password used to generate the key to be used in encrypting messages to and from this user. This parameter must be specified if the value in the Privacy field is not None.

Configure the required fields and click **APPLY**

Removing an SNMP User

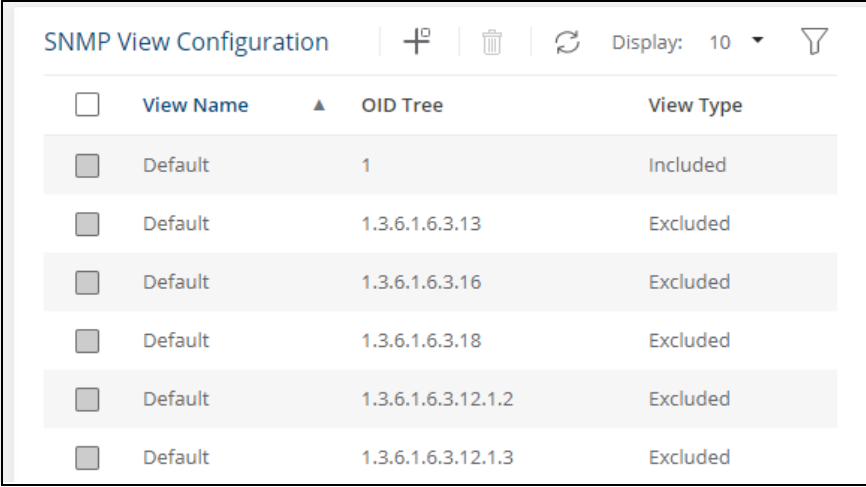
To remove one or more SNMP v3 users, select each user to delete and click **Remove**  .

SNMP View Configuration

Use the SNMP View Configuration tile to configure SNMP views. These SNMP views allow network managers to control access to different parts of the MIB hierarchy permitting or denying access to objects. Once configured, views are associated to access control groups to complete access privileges.

To access the SNMP View Configuration tile, click **Switching > SNMP** and scroll down to the SNMP View Configuration tile.

Figure 62: SNMP View Configuration Tile



The screenshot shows the 'SNMP View Configuration' tile. At the top, there is a title bar with the title 'SNMP View Configuration' and several icons: a plus sign, a trash can, a refresh arrow, and a filter funnel. To the right of the icons is a 'Display: 10' dropdown menu. Below the title bar is a table with four columns: a checkbox, 'View Name', 'OID Tree', and 'View Type'. The table contains seven rows. The first row has a checked checkbox, 'Default', '1', and 'Included'. The remaining six rows have unchecked checkboxes, 'Default', various OID values (1.3.6.1.6.3.13, 1.3.6.1.6.3.16, 1.3.6.1.6.3.18, 1.3.6.1.6.3.12.1.2, 1.3.6.1.6.3.12.1.3), and 'Excluded'.

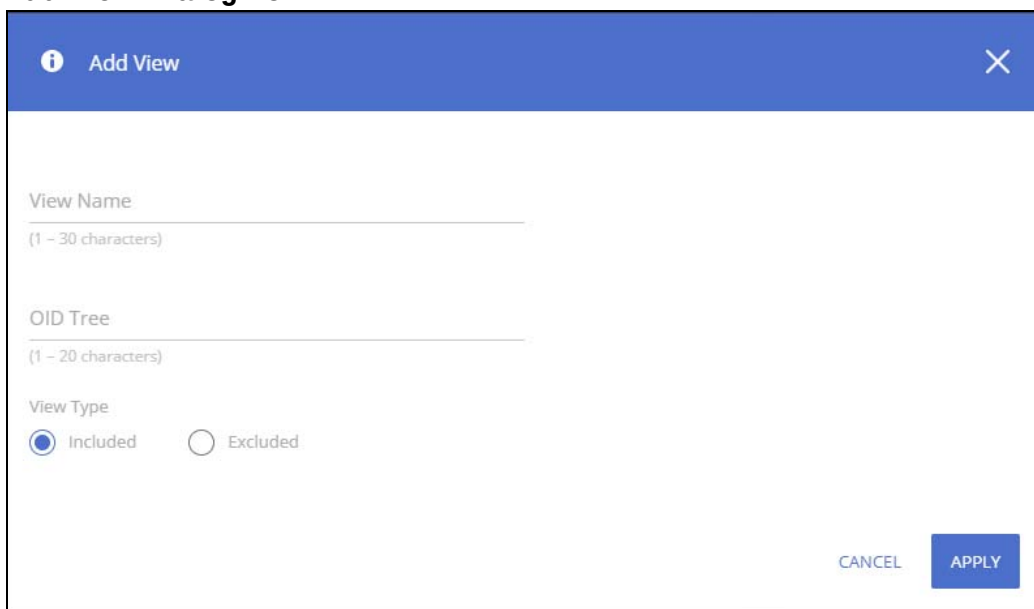
☐	View Name	OID Tree	View Type
☒	Default	1	Included
☐	Default	1.3.6.1.6.3.13	Excluded
☐	Default	1.3.6.1.6.3.16	Excluded
☐	Default	1.3.6.1.6.3.18	Excluded
☐	Default	1.3.6.1.6.3.12.1.2	Excluded
☐	Default	1.3.6.1.6.3.12.1.3	Excluded

Table 49: SNMP View Entry Fields

Field	Description
View Name	The name that identifies the SNMP view.
OID Tree	The ASN.1 subtree to be included or excluded from the view.
View Type	Type of access granted to the specified ASN.1 subtree: <ul style="list-style-type: none">• Included – Access is granted to this subtree.• Excluded – Access is denied to this subtree.

Adding an SNMP View

To add an SNMP view, click **Add** . The **Add View** screen appears.

Figure 63: Add View Dialog BoxThe image shows a dialog box titled "Add View" with a blue header bar containing an information icon and a close button. The main area is white and contains three input fields: "View Name" with a placeholder "(1 - 30 characters)", "OID Tree" with a placeholder "(1 - 20 characters)", and "View Type" with two radio buttons labeled "Included" (selected) and "Excluded". At the bottom right, there are two buttons: "CANCEL" and "APPLY".

Configure the required fields and click **APPLY**

Removing an SNMP View

To remove one or more SNMP views, select each view to delete and click **Remove** . Only user-configured views can be removed.

Remote Engine ID Configuration

To use SNMPv3, an engine ID must be specified for the SNMP Agent. The engine ID must be unique within an administrative domain. The switch uses a Local Engine ID. The Local Engine ID is not configurable and is auto generated based on switch MAC address.

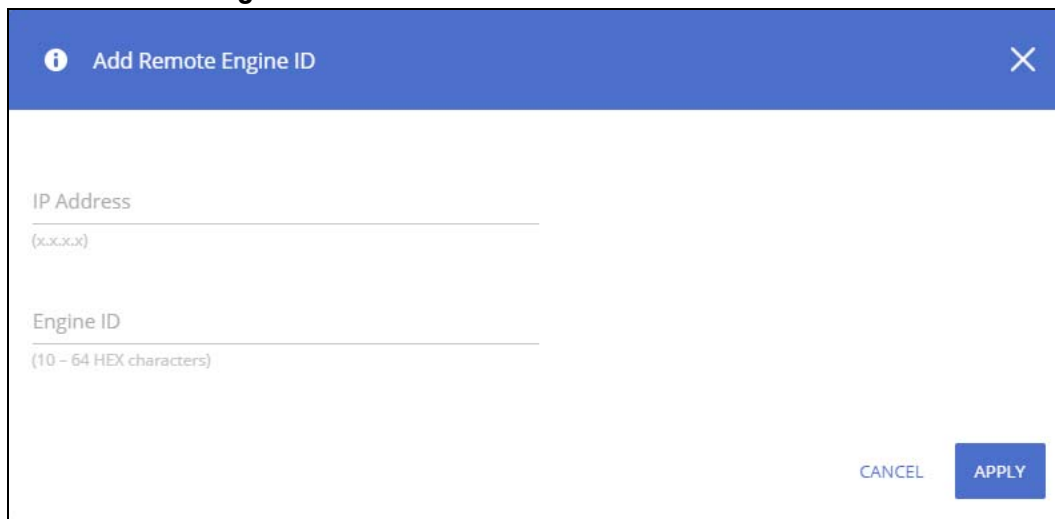
For remote SNMP Agents, Receiving informs or traps, a unique SNMP engine ID needs to be configured. Use this dialog box to configure the remote Engine ID for specific hosts.

Table 50: Remote Engine ID Configuration Entry Fields

Field	Description
IP Address	The IP Address of the remote SNMP Agent
Engine ID	The engine ID of the remote Agent. The engine ID is a concatenated hexadecimal string (10 – 64 HEX characters).

Adding a Remote Engine ID Configuration

To add a **Remote Engine ID Configuration**, click **Add**  . The **Add Remote Engine ID** screen appears.

Figure 64: Add Remote Engine ID

Configure the required fields and click **APPLY**.

Removing a Remote Engine ID Configuration

To remove one or more remote engine IDs, select each engine to delete and click **Remove**  .

Interface Auto Recovery

A number of features on the switch may set the port to a suspended state, when defined error conditions are met. The auto recover feature enables a suspended port to exit this suspended state after a period of time.

Features supported by Auto Recovery are listed below. Each feature is listed with the error conditions that cause a port to be placed into the suspended state:

- **BPDUGuard**: If a port that has the BPDUGuard feature enabled receives a BPDUG, the port state is set to Suspended.
- **Storm Control**: Interface level storm control setting includes a "shutdown" action. If this action is selected and the incoming rate of unicast (with unknown destination), multicast, or broadcast packets exceeds a set threshold, the port moves to the Suspended state. See [Modifying Interface Settings](#) for more information.
- **Port Security**: If a port that has the Violation Shutdown Mode feature enabled receives unknown MAC addresses after the MAC limit is reached, the port moves to the Suspended state.

- **Loop Protection:** If a loop is detected on an interface with loop protection enabled, the port state is set to Suspended.
- **Link flap Prevention:** If excessive link flapping is detected on an interface on which link flap prevention is enabled, the port state is set to Suspended.

When a port has been placed into a Suspended state, the port is shutdown, and no traffic is sent or received on the port until it is either manually enabled by the administrator or re-enabled by the Auto Recovery feature.

The Auto Recovery feature automatically re-enables a suspended port when the error conditions that caused the port to be disabled are no longer detected. The switch utilizes a configurable Auto Recovery timer to periodically check the error condition at set intervals. If the error condition is no longer present, the port is re-enabled. The administrator can manually override the timer setting by re-enabling a port at any time.

Auto Recovery is disabled by default for all conditions except Link Flap Prevention. If Auto Recovery is disabled after ports have been placed in a suspended state, they will remain disabled until an administrator manually enables them.

Use the **Auto Recovery Configuration** page to configure **Auto Recovery** settings for all the components. To display this page, click **Switching > Interface Auto Recovery**.

Global Configuration

These are the global configuration options that you can set:

Figure 65: Global Configuration

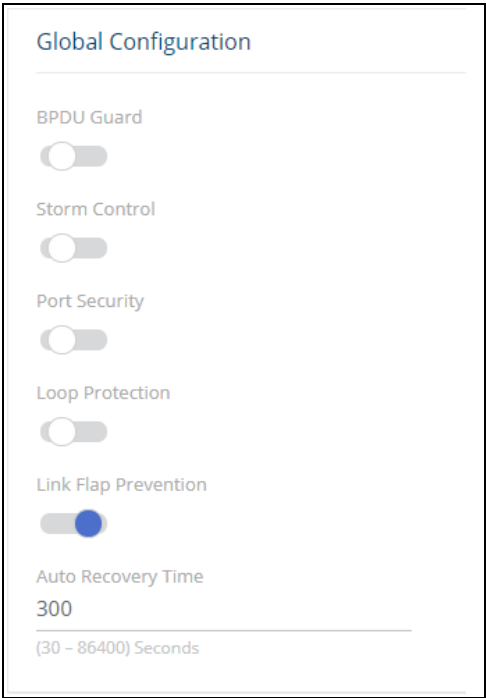


Table 51: Interface Auto Recovery Global Configuration Fields

Field	Description
BPDUGuard	When BPDUGuard Auto Recovery is enabled, the port will be enabled once the configured Recovery Time expires. If the port receives another BPDUGuard, it will be disabled again. If the BPDUGuard Auto Recovery mode is disabled, a port that has received a BPDUGuard and has been placed in the suspended state will remain in that state until an administrator manually enables it. BPDUGuard Auto Recovery is disabled by default.

Field	Description
Storm Control	If the incoming rate of unicast (with unknown destination), multicast, or broadcast packets exceeds a set threshold, the port moves to the suspended state. When Storm Control Auto Recovery is enabled, the port will be enabled once the configured Recovery Time expires. If the port continues to receive unicast (with unknown destination), multicast, or broadcast packets exceeding the set threshold, that port will be disabled again. Storm Control Auto Recovery is disabled by default.
Port Security	If a port that has the Violation Shutdown Mode feature enabled receives unknown MAC addresses after the MAC limit is reached, the port moves to the suspended state. When Port Security Auto Recovery is enabled, the port will be enabled once the configured Recovery Time expires. If the port continues to receive unknown MAC addresses after the MAC limit is reached, the port will be disabled again. Port Security Auto Recovery is disabled by default.
Loop Protection	If a loop is detected on an interface with loop protection enabled, the port state is set to Suspended. Loop Protection is disabled by default.
Link Flap Prevention	If excessive link flapping is detected on an interface on which link flap prevention is enabled, the port state is set to Suspended. Link Flap Prevention is enabled by default.
Auto Recovery Time	This configures the Auto Recovery time interval, in seconds. The Auto Recovery time interval is common for all the components. The default value of the timer is 300 seconds and the range is from 30 to 86400 seconds.

If you modify these settings, click **APPLY** to save the changes for the current switch configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Use the Auto Recovery Configuration page to configure Auto Recovery settings for all the components. To display this page, click **Switching > Interface Auto Recovery**.

Suspended Interfaces

The Suspended Interface tile displays interfaces suspended due to one of the conditions specified in [Interface Auto Recovery Global Configuration Fields](#) and the time to recover (if enabled).

Figure 66: Suspended Interfaces

Interface	Reason	Time to Recover (seconds)
☐ 1/1	Loop Protection	300

Table 52: Suspended Interfaces Fields

Field	Description
Interface	The interface that is suspended. If no interfaces are in the suspended state, the table is blank.

Field	Description
Reason	<p>If the switch detects an error condition for an interface, the switch puts the interface in the suspended state, meaning that it has been intentionally disabled because it has encountered errors. The reasons that the interface can go into a suspended state include the following:</p> <ul style="list-style-type: none"> • BPDU Guard • Storm Control • Port Security • Loop Protection • Link Flap Prevention
Time to Recover (seconds)	<p>When Auto Recovery is enabled and the interface is placed in the suspended state, then a recovery timer starts for that interface. Once this timer expires, the switch checks if the interface is in the suspended state. If yes, then the switch enables the interface.</p>

To re-enable one or more interfaces select them from the Suspended Interface table and click the **Recover Interface**  button.



If the error condition still exists on the interface it may be shutdown again due to this condition.

Trunk Configuration

Trunks allow for the aggregation of multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and throughput by providing load sharing capability.

A trunk interface can be either static or dynamic:

- **Dynamic**—Dynamic trunks use the Link Aggregation Control Protocol (LACP, IEEE standard 802.3ad). An LACP-enabled port automatically detects the presence of other directly attached switches supporting LACP and exchanges Link Aggregation Control Protocol Data Units (LACPDUs) with links in the trunk. The PDUs contain information about each link and enable the trunk to maintain them.
- **Static**—Static trunks are assigned to a trunk group by the administrator. Members do not exchange LACPDUs. A static trunk does not require a partner system to be able to aggregate its member ports. This is the default trunk type.

All members of a trunk must participate in the same protocols. A static trunk interface does not require a partner system to be able to aggregate its member ports.

From a system perspective, a Trunk is treated as a physical port. A Trunk and a physical port use the same configuration parameters for parameters such as: administrative enable/disable, port priority, and path cost.

A trunk failure of one or more of the links does not stop traffic. Upon failure, the traffic mapped to a link is dynamically reassigned to the remaining links of the trunk. Similarly when links are added to a trunk, existing traffic may automatically shift to a different link member within the trunk. Before shifting traffic, the system ensures reordered frames do not exist.

When a link is added to a trunk it retains its configuration. However this configuration is not active. Once the link is removed from the trunk all the interface-configured settings become active.

These are the support configurations for the various switches:

Number of ports per-switch	Number of trunks supported	Number of trunk members supported
8 port per-switch	4 trunks	4 trunk members
24 port per-switch	8 trunks	4 trunk members
48 port per-switch	16 trunks	8 trunk members

To display this page, click **Switching > Trunk Configuration**.

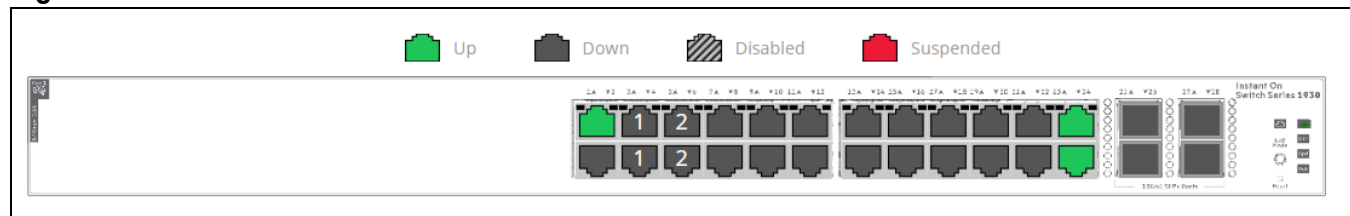


Trunks are sometimes referred to as link aggregation groups (LAGs) or port-channels.

Device View

The top of the Trunk Configuration page shows a graphical representation of the switch front panel. This panel view has a display of the ports, each with its current status. The Trunk ports also show the Trunk ID.

Figure 67: Switch Panel View



Click a trunk member (indicated with a trunk number) in this screen, to open the **Switching > Trunk Configuration** page.

For more information, see [Switch Panel View](#).

Global Configuration

You can use the Global Configuration page to select the hashing algorithm used to distribute traffic load among the physical ports of the trunk while preserving the per-flow packet order. The hashing algorithm uses various packet attributes to determine the outgoing physical port. This setting is global and effects all system LAGs.

The following sets of packet attributes can be used to compute the hashing algorithm:

- Source and Destination MAC, IP and TCP/UDP Port fields
- Source and Destination MAC fields
- Source and Destination MAC and IP fields (this is the default)

Figure 68: Trunk Configuration Global Configuration Section

Global Configuration

Load Balance

Source/Destination MAC-IP

Table 53: Trunk Configuration Global Configuration Fields

Field	Description
Load Balance	These are the Load balance options: <ul style="list-style-type: none">Source/Destination MAC-IP-TCP/UDP PortSource/Destination MACSource/Destination MAC-IP

Click **APPLY** to update the trunk configuration.

Trunk Configuration Tile

You can use the Trunk Configuration page to view and edit trunks. The number of trunks on the system is fixed, and by default there are no port members in trunks. You can enable, disable, and edit settings for each trunk.

To access the trunk configuration, click **Switching > Trunk Configuration** in the navigation pane.

Figure 69: Trunk Configuration

Trunk Configuration							
Trunk	Description	Type	Admin Mode	Link Status	Members	Active Ports	
☐ TRK 1		Static	Enabled	Down			
☐ TRK 2		Static	Enabled	Down			
☐ TRK 3		Static	Enabled	Down			
☐ TRK 4		Static	Enabled	Down			
☐ TRK 5		Static	Enabled	Down			
☐ TRK 6		Static	Enabled	Down			
☐ TRK 7		Static	Enabled	Down			

The following information is displayed for each trunk.

Table 54: Trunk Configuration Fields

Field	Description
Trunk	The trunk ID.
Description	The trunk description, if any, associated with the interface to help identify it.

Field	Description
Type	<p>Trunks can be either dynamic or static, but not both:</p> <ul style="list-style-type: none"> LACP—Link Aggregation Control Protocol (LACP, IEEE standard 802.3ad). An LACP-enabled port automatically detects the presence of other aggregation-capable network devices in the system and exchanges Link Aggregation Control Protocol Data Units (LACPDU) with links in the trunk. The PDUs contain information about each link and enable the trunk to maintain them. Static—Static trunks are assigned to a bundle by the administrator. Members do not exchange LACPDUs. A static trunk does not require a partner system to be able to aggregate its member ports. This is the default port type.
Admin Mode	Whether the trunk is administratively enabled or disabled. This setting is enabled by default.
Link Status	Indicates the operational status of the trunk interface, which can be Up, Up (SFP) for ports with an installed SFP transceiver, or Down.
Members	The ports that are members of the trunk. By default, no ports belong to any trunk.
Active Ports	The ports that are actively participating members of a trunk. A member port that is operationally or administratively disabled or does not have a link is not an active port.

Modifying Trunk Settings

To modify a trunk, select it and click **Edit** . The **Edit Trunk Configuration** page displays:

Figure 70: Edit Trunk Configuration Dialog Box

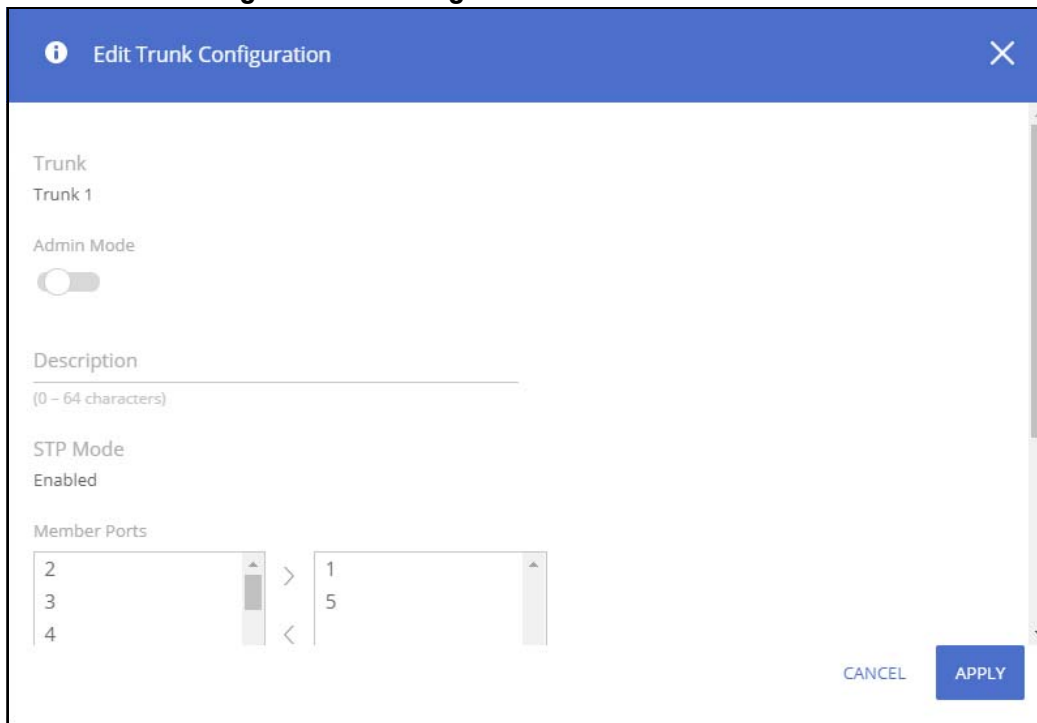


Table 55: Edit Trunk Configuration Fields

Field	Description
Trunk	The trunk ID.
Admin Mode	Administratively enable or disable the trunk.
Description	Enter a description for the trunk.

Field	Description
STP Mode	The spanning tree protocol (STP) mode of the trunk. When enabled, the trunk participates in the STP operation to help prevent network loops. This is a read-only field. Use the CST Configuration tile to set the TRUNK STP mode. By default, the STP mode is enabled.
Port Membership	The list on the left shows ports that are not members of the trunk. The list on the right shows the ports that are members of the trunk. Use the arrows to move ports between the lists.
Trunk Type	Choose Static for a static trunk. Choose LACP for dynamic trunk.

Note the following considerations when configuring trunks and trunk members:

- All ports in a trunk must have the same full-duplex speed.
- A port that is added to a trunk retains its VLAN configuration as a "shadow" configuration, meaning the port VLAN configuration is not active while the port is a member of the trunk. When the port is removed from the trunk, the port VLAN configuration becomes active.
- When ports are members of a trunk, they take on the STP configuration for the trunk. When ports are removed from a trunk, they take on their earlier configured STP states.

Click **APPLY** to save any changes to the currently selected trunk. The changes take effect immediately.

EEE Configuration

The Energy Efficient Ethernet (EEE) technologies, as defined by the IEEE 802.3az task force. These features are designed to reduce per-port power usage by shutting down ports when no link is present or when activity is low.

To display the EEE configuration page, click **Switching > EEE Configuration** in the navigation pane.

Global Configuration

Figure 71: Global Configuration

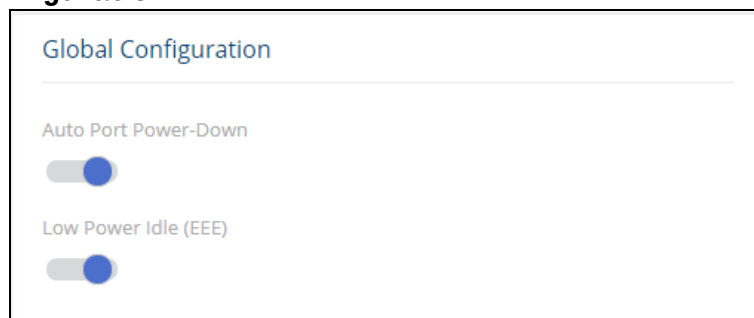


Table 56: Global Configuration Fields

Field	Description
Auto Port Power-Down	When this feature is enabled and the port link is down, the PHY automatically goes down for a short period of time. The port wakes up when it senses activity on the link. This feature enables saving power consumption when no link partner is present. This feature is enabled by default.

Field	Description
Low Power Idle (EEE)	<p>When this feature is enabled and there is not traffic on the port, the port enters a low-power mode, to reduce power consumption.</p> <p>The EEE feature works on ports in auto-negotiation mode, where the port is negotiated to either 100 Mbps full duplex, or 1 Gbps (1000 Mbps) full duplex.</p> <p>The EEE feature is enabled by default.</p> <p>NOTE: EEE is active only if port auto-negotiation mode is enabled.</p>

Click **APPLY** to save any changes for the current switch configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Global Status

When EEE is enabled, you can use the EEE Status tile to view estimated power savings and power consumption information.

Figure 72: Global Status

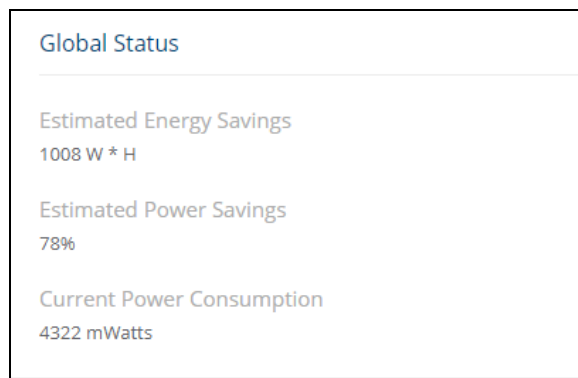


Table 57: Global Status Fields

Field	Description
Estimated Energy Savings	The estimated cumulative energy saved on the switch (in watts x hours) due to the Energy Efficient Ethernet feature.
Estimated Power Savings	The estimated percentage of power conserved on all ports due to the Energy Efficient Ethernet feature. For example, 10% means that the switch required 10% less power.
Current Power Consumption	The estimated power consumption by all ports.

Interface Status

This page displays EEE status information for each interface.

To display the Interface Status page, click **Switching > EEE Configuration** in the navigation pane.

Figure 73: Interface Status Tile

Interface ▲	Link Partner EEE Support	Auto Port Power-Down Status	LLDP Wakeup Time Negotiation	Rx Wakeup Time	Tx Wakeup Time
1	No	Active	No	0	0
2	Yes	Inactive	No	17	17
3	Yes	Inactive	No	17	17
4	Yes	Inactive	No	17	17
5	Yes	Inactive	No	17	17
6	Yes	Inactive	No	17	17
7	No	Active	No	0	0
8	Yes	Inactive	No	17	17
9	Yes	Inactive	No	17	17
10	No	Active	No	0	0

« ‹ 1 2 3 4 5 6 › »

REFRESH APPLY

Table 58: EEE Status Fields

Field	Description
Interface	The interface ID.
Link Partner EEE Support	Displays Yes if the interface has received EEE messages (called Type-Length Values, or TLVs) from a link partner, or No if it has not.
Auto Port Power-Down Status	The current operational state of Auto Port Power-Down mode. <ul style="list-style-type: none"> No Energy Detected – power saving mode is active (link status is down) Inactive – power saving mode is not active (link status is up).
LLDP Wakeup Time Negotiation	Indicates whether the EEE wakeup time is negotiated with the link partner (Yes or No).
Rx Wakeup Time	The Rx wakeup time in effect for the port, if negotiated by LLDP (otherwise, 0).
Tx Wakeup Time	The Tx wakeup time in effect for the port, if negotiated by LLDP (otherwise, 0).

To refresh the information displayed in the table, click **Refresh**  .



Chapter 6

Spanning Tree

Spanning Tree Protocol (STP) is a Layer 2 protocol that provides a tree topology for switches on a bridged LAN. STP allows a network to have redundant paths without the risk of network loops. STP uses the spanning-tree algorithm to provide a single path between end stations on a network. When STP is enabled, bridges on a network exchange bridge protocol data units (BPDUs) to communicate changes in the network topology and to provide information that helps determine the optimal paths between network segments.

HPE Networking Instant On 1930 Switch Series switches support STP versions IEEE 802.1D (STP), 802.1w (Rapid STP, or RSTP) and 802.1s Multiple spanning tree (MSTP) with up to 8 instances. RSTP reduces the convergence time for network topology changes to about 3 to 5 seconds from the 30 seconds or more for the IEEE 802.1D STP standard. RSTP is intended as a complete replacement for STP, but can still inter-operate with switches running the STP protocol by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

To display the Spanning Tree General Settings page, click **Spanning Tree > General Settings** in the navigation pane.

Global Settings

Use the Global Settings page to configure global Spanning Tree settings on the Switch.

Global Configuration

Figure 74: Spanning Tree Global Configuration Page

Global Configuration

Spanning Tree Admin Mode

☒

Spanning Tree Maximum Hops

20

(6 – 40)

Protocol Version

☐ STP
☒ RSTP
☐ MSTP

Configuration Name

00:00:00:12:17:29

(1 – 32 characters)

Bridge Priority

32768

Configuration Revision Level

0

(0 – 65535)

Bridge Max Age

20

(6 – 40) Seconds

BPDU Filter

☐

Bridge Forward Delay

15

(4 – 30) Seconds

Table 59: Spanning Tree Global Configuration Fields

Field	Description
Spanning Tree Admin Mode	The administrative mode of STP on the switch. When enabled, the switch participates in the root bridge election process and exchanges Bridge Protocol Data Units (BPDUs) with other switches in the spanning tree to determine the root path costs and maintain topology information. By default, Admin Mode is enabled.
Protocol Version	The STP version the switch uses, which is one of the following: <ul style="list-style-type: none"> STP (IEEE 802.1d) – Classic STP provides a single path between end stations, avoiding and eliminating loops. RSTP (IEEE 802.1w) – Rapid Spanning Tree Protocol (RSTP) behaves like classic STP but also has the ability to configure and recognize full-duplex connectivity and ports that are connected to end stations, resulting in rapid transitioning of the port to the Forwarding state and the suppression of Topology Change Notifications. This is the default protocol. MSTP (IEEE 802.1s) – Multiple Spanning Tree Protocol (MSTP) includes all the advantages of RSTP and also supports multiple spanning tree instances to efficiently channel VLAN traffic over different interfaces. MSTP is compatible with both RSTP and STP.
Bridge Priority	The value that helps determine which bridge in the spanning tree is elected as the root bridge during STP convergence. A lower value increases the probability that the bridge becomes the root bridge. The default priority is 32768. The valid range is 0-61440, in steps of 4096.
Bridge Max Age	The amount of time a bridge waits before implementing a topological change. The default is 20. The valid range is 6-40.
Bridge Forward Delay	The amount of time a bridge remains in a listening and learning state before forwarding packets. The default is 15. The valid range is 4-30.

Field	Description
Spanning Tree Maximum Hops	The maximum number of hops a Bridge Protocol Data Unit (BPDU) is allowed to traverse within the spanning tree region before it is discarded.
Configuration Name	The name of the MSTP region. Each switch that participates in the same MSTP region must share the same Configuration Name, Configuration Revision Level, and MST-to-VLAN mappings.
Configuration Revision Level	The revision number of the MSTP region. This number must be the same on all switches that participate in the MSTP region.
BPDU Filter	When enabled, this feature filters the BPDU traffic on ports when spanning tree is disabled. When disabled, BPDU traffic is flooded on all ports.

If you modify any settings, Click **APPLY** to update the switch configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Global Settings

These are the Global Settings that you can view:

Figure 75. Spanning Tree Global Settings Page

Global Settings		
Root Bridge Identifier 32768:00:00:A1:A2:A3:A4	Root Path Cost 80000	Topology Change Count 2
Bridge Hello Time 2 Seconds	Root Port 23	Root Guarded Interfaces N/A
Spanning Tree Tx Hold Count 3	Max Age 20 Seconds	TCN Guarded Interfaces 1-28,TRK1-TRK8
Bridge Identifier 32768:38:21:C7:CA:11:E6	Forward Delay 15 Seconds	BPDU Filtered Interfaces N/A
Time Since Topology Change 19:25:19	Hold Time 1 Seconds	CST Path Cost 0
Configuration Digest Key AC36177F50283CD4B83821D8AB26DE62	CST Regional Root 32768:38:21:C7:CA:11:E6	Configuration Format Selector 0

Table 60: Spanning Tree Global Settings Fields

Field	Description
Root Bridge Identifier	The bridge identifier of the root bridge for the spanning tree. The identifier is made up of the bridge priority and the base MAC address. When electing the root bridge for the spanning tree, if the bridge priorities for multiple bridges are equal, the bridge with the lowest MAC address is elected as the root bridge.
Bridge Hello Time	The amount of time the root bridge waits between sending hello BPDUs.
Spanning Tree Tx Hold Count	The maximum number of BPDUs that a bridge is allowed to send within a hello time window.

Field	Description
Bridge Identifier	A unique value that is automatically generated based on the bridge priority value and the base MAC address of the bridge. When electing the root bridge for the spanning tree, if the bridge priorities for multiple bridges are equal, the bridge with the lowest MAC address is elected as the root bridge.
Time Since Topology Change	The amount of time that has passed since the topology of the spanning tree has changed since the switch was last reset.
Configuration Digest Key	The 16 byte signature of type HMAC-MD5 created from the MST Configuration Table (a VLAN ID-to-MST ID mapping). Use this field to compare between devices and determine if they have the same MSTP global configuration.
Root Path Cost	The path cost to the designated root for the CST. Traffic from a connected switch to the root bridge takes the least-cost path to the bridge.
Root Port	The port on the bridge with the least-cost path to the designated root for the CST.
Max Age	The amount of time a bridge waits before implementing a topological change.
Forward Delay	The forward delay value for the root port bridge.
Hold Time	The minimum amount of time between transmissions of Configuration BPDUs.
CST Regional Root	The bridge identifier of the CST regional root. The identifier is made up of the priority value and the base MAC address of the regional root bridge.
CST Path Cost	The path cost to the CST tree regional root.
Topology Change Count	The number of topology changes that occurred since last time the device reloaded.
Root Guarded Interfaces	A list of interfaces currently having the Root Guard parameter set.
TCN Guarded Interfaces	A list of interfaces currently having the TCN Guard parameter set.
BPDU Filtered Interfaces	A list of interfaces currently having the BPDU Filter parameter set.
Configuration Format Selector	The version of the configuration format being used in the exchange of BPDUs.

Spanning Tree Statistics

Use the Spanning Tree Statistics page to view information about the number of bridge protocol data units (BPDUs) transmitted and received on each port.

To view the Spanning Tree Statistics tile, click **Spanning Tree > General Setting** in the navigation pane, and scroll down to the **Spanning Tree Statistics** tile.

Figure 76: Spanning Tree Statistics Page

Spanning Tree Statistics			
Interface	▲	RX BPDUs	TX BPDUs
1		0	0
2		0	0
3		0	0

Table 61: Spanning Tree Statistics Fields

Field	Description
Interface	The port or trunk associated with the rest of the data in the row.
RX BPDUs	The number of STP/RSTP/MSTP (IEEE 802.1d) BPDUs received by the interface.
TX BPDUs	The number of STP/RSTP/MSTP BPDUs sent by the interface.

To clear the data in the Statistics table, click **Clear All**  .

To refresh the data shown in the Statistics table, click **Refresh**  .

To filter the data shown in the Statistics table, click **Filter**  . A filter box appears below the headers. you can select the interface that you want to view, or sort by the BPDUs values (highest to lowest, or vice versa).

CST Configuration

Use the CST Configuration page to view and configure the Common Spanning Tree (CST) settings for each interface on the switch. To configure CST settings for an interface and to view additional information about the interface's role in the CST topology, select the interface to view or configure and click **Edit**.

To view the CST Configuration page, click **Spanning Tree > CST Configuration** in the navigation pane.

CST Port Configuration

Figure 77: CST Port Configuration Tile

CST Port Configuration     Display: 10  						
☐	Interface	▲ Port Role	Port Forwarding State	Port Priority	Port Path Cost	
☐	1	Disabled	Disabled	128	2000000	
☐	2	Disabled	Disabled	128	20000	
☐	3	Designated	Forwarding	128	20000	
☐	4	Designated	Forwarding	128	20000	

Table 62: CST Port Configuration Fields

Field	Description
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring CST settings for an interface, this field identifies the interface being configured.
Port Role	<p>The role of the port within the CST, which is one of the following:</p> <ul style="list-style-type: none"> • Root – A port on the non-root bridge that has the least-cost path to the root bridge. • Designated – A port that has the least-cost path to the root bridge on its segment. • Alternate – A blocked port that has an alternate path to the root bridge. • Backup – A blocked port that has a redundant path to the same network segment as another port on the bridge. • Master – The port on a bridge within an MST instance that links the MST instance to other STP regions. • Disabled – The port is physically down, or administratively disabled and is not part of the spanning tree.
Port Forwarding State	<ul style="list-style-type: none"> • Blocking – The port discards user traffic and receives, but does not send, BPDUs. During the election process, all ports are in the blocking state. The port is blocked to prevent network loops. • Listening – The port sends and receives BPDUs and evaluates information to provide a loop-free topology. This state occurs during network convergence and is the first state in transitioning to the forwarding state. • Learning – The port learns the MAC addresses of frames it receives and begins to populate the MAC address table. This state occurs during network convergence and is the second state in transitioning to the forwarding state. • Forwarding – The port sends and receives user traffic. • Disabled – The port is physically down, or administratively disabled and is not part of the spanning tree.
Port Priority	The priority for the port within the CST. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost from the assigned port to this port.

Additional Actions on CST Ports

The following actions are available when you select one or more CST Ports:

- **View Details**  . This option is available if you have a single port selected. For more information, see [CST Port Details Fields](#).
- **Edit CST Settings**  . This option is available if you select one or more ports. The same settings are applied to all selected interfaces. For more information, see [Edit CST Port Fields](#).
- **Clear Detected Protocols**  . This option is available if you select one or more ports. Click this button to restart the STP migration process with the link partner. This forces STP mode renegotiation with the link partner.

Figure 78: Edit CST Port Settings Page

Edit CST Port Settings

Interface
3

STP State
☒

Port Priority
128

Port Path Cost
0
(1 – 200000000; 0 for Auto)

Edge Port
☒ Auto ☐ Enable ☐ Disable

BPDU Filter
☐

BPDU Guard
☐

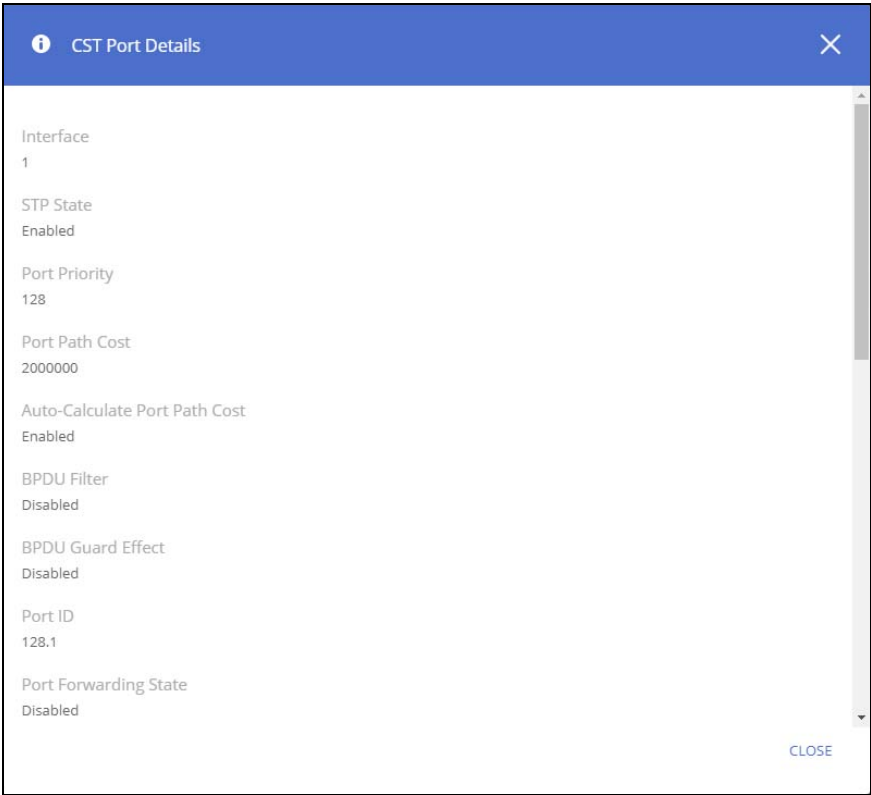
CANCEL APPLY

Table 63: Edit CST Port Fields

Field	Description
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring CST settings for an interface, this field identifies the interface being configured.
STP State	The port STP state. If set to enabled, the port will be part of the spanning tree topology. If set to disable, the port will not participate in spanning tree topology. The default state is enabled.
Port Priority	The priority for the port within the CST. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost associated with this port. If set to 0 cost will be determined based on port speed (auto).
Edge Port	Indicates whether the interface is configured as an edge port the following settings are supported: <ul style="list-style-type: none"> Auto - Enables edge port on switch, but only following a few seconds delay after port is up (this is the default) Enable - edge port is enabled on interface Disable - edge port is disabled on interface.
BPDU Filter	When enabled, this feature filters the BPDU traffic on the port, if STP is administratively disabled on interface. This feature requires BPDU filtering to be enabled globally.
BPDU Guard	When enabled, BPDU Guard can disable edge ports that receive BPDU packets. This prevents a new switch from entering the existing STP topology. Thus devices that were originally not a part of STP are not allowed to influence the STP topology.
Root Guard	When enabled, Root Guard allows the interface to discard any superior information it receives to protect the root of the switch from changing. The port gets put into discarding state and does not forward any frames.
TCN Guard	When enabled, TCN Guard restricts the interface from propagating any topology change information received through that interface.

To view additional information about an interface's role in the CST topology, select the interface to view, and then click **Details**  .

Figure 79: CST Port Details Page



The following table describes the fields in the **CST Port Details** dialog box.

Table 64: CST Port Details Fields

Field	Description
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring CST settings for an interface, this field identifies the interface being configured.
STP State	The port STP state. If set to enabled, the port will be part of the spanning tree topology. If set to disable, the port will not participate in spanning tree topology. The default state is enabled.
Port Priority	The priority for the port within the CST. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost associated with this port. If set to 0 cost will be determined based on port speed (auto).
Auto-Calculate Port Path Cost	Shows whether the path cost from the port to the root bridge is automatically determined by the speed of the interface (Enabled) or configured manually (Disabled).
BPDU Filter	When enabled, this feature filters the BPDU traffic on the port, if STP is administratively disabled on interface. This feature requires BPDU filtering to be enabled globally.
BPDU Guard Effect	When enabled, BPDU Guard can disable edge ports that receive BPDU packets. This prevents a new switch from entering the existing STP topology. Thus devices that were originally not a part of STP are not allowed to influence the STP topology.
Port ID	A unique value that is automatically generated based on the port priority value and the interface index.

Field	Description
Port Forwarding State	<ul style="list-style-type: none"> Blocking – The port discards user traffic and receives, but does not send, BPDUs. During the election process, all ports are in the blocking state. The port is blocked to prevent network loops. Listening – The port sends and receives BPDUs and evaluates information to provide a loop-free topology. This state occurs during network convergence and is the first state in transitioning to the forwarding state. Learning – The port learns the MAC addresses of frames it receives and begins to populate the MAC address table. This state occurs during network convergence and is the second state in transitioning to the forwarding state. Forwarding – The port sends and receives user traffic. Disabled – The port is administratively disabled and is not part of the spanning tree.
Port Role	<p>The role of the port within the CST, which is one of the following:</p> <ul style="list-style-type: none"> Root – A port on the non-root bridge that has the least-cost path to the root bridge. Designated – A port that has the least-cost path to the root bridge on its segment. Alternate – A blocked port that has an alternate path to the root bridge. Backup – A blocked port that has a redundant path to the same network segment as another port on the bridge. Master – The port on a bridge within an MST instance that links the MST instance to other STP regions. Disabled – The port is administratively disabled and is not part of the spanning tree.
Designated Root	The bridge ID of the root bridge for the CST.
Designated Cost	The path cost offered to the LAN by the designated port.
Designated Bridge	The bridge ID of the bridge with the designated port.
Designated Port	The port ID of the designated port.
Admin Edge Port	The edge port setting on port - Auto, Enabled or Disabled.
Edge Port	Indicates if edge port is Active or Inactive on the interface.
Point-to-point MAC	Indicates whether the link type for the interface is a point-to-point link.
Root Guard	When enabled, Root Guard allows the interface to discard any superior information it receives to protect the root of the switch from changing. The port gets put into discarding state and does not forward any frames.
TCN Guard	When enabled, TCN Guard restricts the interface from propagating any topology change information received through that interface.
CST Regional Root	The bridge ID of the bridge that has been elected as the root bridge of the CST region.
CST Path Cost	The path cost from the interface to the CST regional root.

MSTP Configuration

Multiple Spanning Tree Protocol (MSTP) allows the creation of spanning tree instances based upon a VLAN or groups of VLANs. Configuring spanning tree instances creates an active topology with a better distribution of network traffic and an increase in available bandwidth when compared to classic STP.

To display the Spanning Tree MSTP Configuration page, click **Spanning Tree > MSTP Configuration** in the navigation pane.

MSTP Configuration Tile

Figure 80: MSTP Configuration Tile

MSTP Configuration								
<div> <div>+</div> <div>✎</div> <div>🗑</div> <div>↺</div> <div>Display: 10</div> <div>⌵</div> </div>								
☐	MSTP ID ▲	Priority	# of Associated VLANs	Bridge Identifier	Time Since Topology Change	Designated Root	Root Path Cost	Root Port
☐	1	4096	1	4096:00:00:44:44:55:88	23	4096:00:00:44:44:55:88	0	0
<div>« < 1 > »</div>								

Table 65: MSTP Configuration Fields

Field	Description
MSTP ID	The number that identifies the MSTP instance.
Priority	The bridge priority for the spanning-tree instance. This value affects the likelihood that the bridge is selected as the root bridge. A lower value increases the probability that the bridge is selected as the root bridge.
# of Associated VLANs	The number of VLANs that are mapped to the MSTI. This number does not contain any information about the VLAN IDs that are mapped to the instance.
Bridge Identifier	A unique value that is automatically generated based on the bridge priority value of the MSTI and the base MAC address of the bridge. When electing the root bridge for an MST instance, if the bridge priorities for multiple bridges are equal, the bridge with the lowest MAC address is elected as the root bridge.
Time Since Topology Change	The amount of time that has passed since the topology of the MSTI has changed.
Designated Root	The bridge identifier of the root bridge for the MST instance. The identifier is made up of the bridge priority and the base MAC address.
Root Path Cost	The path cost to the designated root for this MST instance. Traffic from a connected switch to the root bridge takes the least-cost path to the bridge. If the value is 0, the cost is automatically calculated based on port speed.
Root Port	The port on the bridge with the least-cost path to the designated root for the MST instance.

If you modify any settings, click **APPLY** to update the switch configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Adding, Editing or Removing an MSTP Configuration

To add an MSTP Instance configuration, click **Add** .

To edit an existing configuration, click the check box to the left of the entry and click **Edit** . The fields in the **Add** and **Edit** dialog boxes are the same.

To remove an existing MSTP Instance, click the check box to the left of the session entry and click **Remove** .

Figure 81: Edit MSTP Entry

Edit MSTP Entry

MSTP ID

999

Priority

12288

VLAN Association

1

3

4

100

101

102

105

107

>

103

104

106

CANCEL

APPLY

Table 66: Add/Edit MSTP Entry Fields

Field	Description
MSTP ID	Enter a unique number that identifies the MSTP instance. Valid values are 1-4094
Priority	Enter The bridge priority for the spanning-tree instance. This value affects the likelihood that the bridge is selected as the root bridge. A lower value increases the probability that the bridge is selected as the root bridge.
VLAN Association	Specify the VLANs to associate to this MSTP instance. the VLANs are specified by their VLAN ID.

MSTP Port Configuration

From the MSTP Port Configuration tile, you can view additional details about the MSTP settings on a port or configure additional settings for one or more ports.

To display the Spanning Tree MSTP Port Configuration tile, click **Spanning Tree > MSTP Configuration** in the navigation pane.

Figure 82: MSTP Port Configuration Tile

☐	Interface	Port Role	Port Forwarding State	Port Priority	Port Path Cost
☐	1	Disabled	Disabled	128	2000000
☐	2	Disabled	Disabled	128	20000
☐	3	Designated	Forwarding	128	20000
☐	4	Designated	Forwarding	128	20000

Table 67: MSTP Port Configuration Fields

Field	Description
MSTP ID	The menu contains the ID of each MST instance that has been created on the switch. The menu will display an instance only if there are port members in one of the VLANs mapped to this instance. Select a certain Instance ID to view and configure interface setting for that instance.
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring MST settings for an interface, this field identifies the interface being configured.
Port Role	The role of the port within the MST, which is one of the following: <ul style="list-style-type: none"> Root – A port on the non-root bridge that has the least-cost path to the root bridge. Designated – A port that has the least-cost path to the root bridge on its segment. Alternate – A blocked port that has an alternate path to the root bridge. Backup – A blocked port that has a redundant path to the same network segment as another port on the bridge. Master – The port on a bridge within an MST instance that links the MST instance to other STP regions. Disabled – The port is physically down, or administratively disabled and is not part of the spanning tree.
Port Forwarding State	<ul style="list-style-type: none"> Blocking – The port discards user traffic and receives, but does not send, BPDUs. During the election process, all ports are in the blocking state. The port is blocked to prevent network loops. Listening – The port sends and receives BPDUs and evaluates information to provide a loop-free topology. This state occurs during network convergence and is the first state in transitioning to the forwarding state. Learning – The port learns the MAC addresses of frames it receives and begins to populate the MAC address table. This state occurs during network convergence and is the second state in transitioning to the forwarding state. Forwarding – The port sends and receives user traffic. Disabled – The port is physically down, or administratively disabled and is not part of the spanning tree.
Port Priority	The priority for the port within the MSTI. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost associated to this port, for this instance.

Viewing MSTP Port Details or Editing MSTP Port Settings

To configure MST settings for one or more interfaces, first select the appropriate MST instance from the MSTP ID menu. Then, select the interfaces to configure and click **Edit** . The same settings are applied to all selected interfaces.

Figure 83: Edit MSTP Port Settings Dialog Box

Edit MSTP Port Settings

MSTP ID

1

Interface

1-2

Port Priority

128

Port Path Cost

0

(1 – 200000000; 0 for Auto)

STP State

☒

CANCEL

APPLY

Table 68: Edit MSTP Port Settings Fields

Field	Description
MSTP ID	The ID of each MST instance this port is associated with.
Interface	Identifies the interface.
Port Priority	The priority for the port within the MSTI. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost associated to this port within the MSTI.
STP State	Spanning tree state of this interface. Can be Enable or Disable, Disable is the default.

To view additional information about an interface's role in the MST topology, select the MST instance and the interface to view, and then click **Details**  .

Figure 84: MSTP Port Details

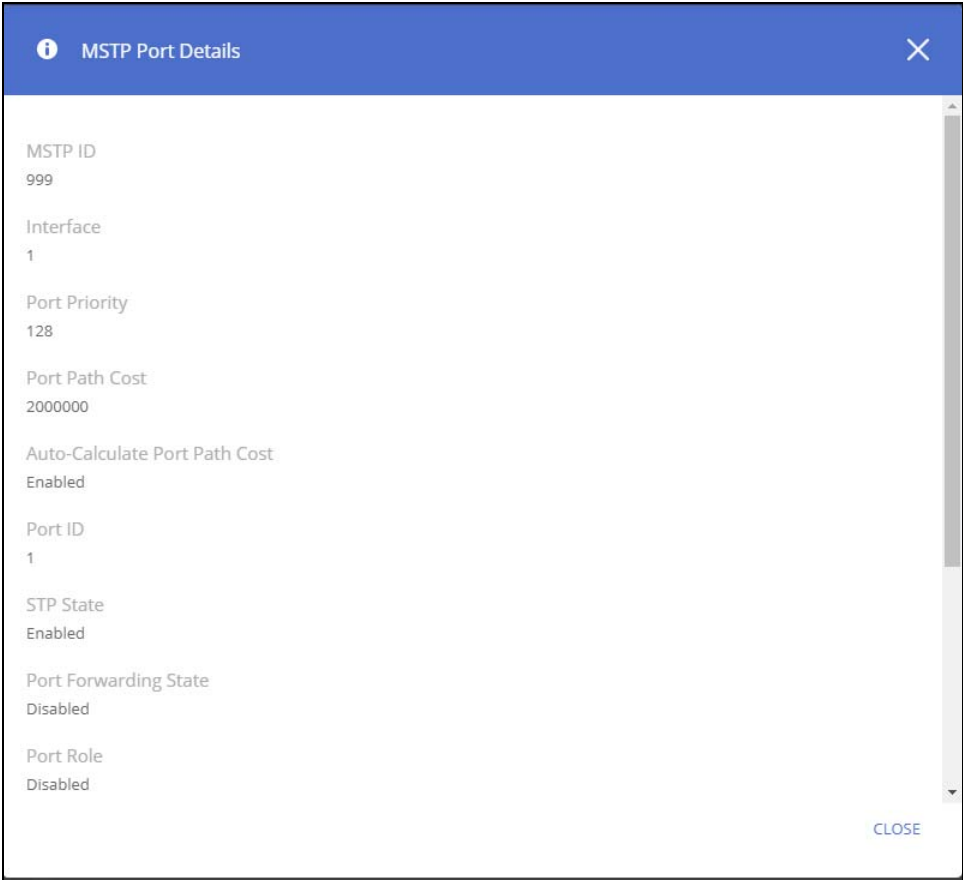


Table 69: MSTP Port Details Fields

Field	Description
MSTP ID	The ID of each MST instance this port is associated with.
Interface	Identifies the interface.
Port Priority	The priority for the port within the MSTI. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost from the port to the root bridge.
Auto-Calculate Port Path Cost	Shows whether the path cost from the port to the root bridge is automatically determined by the speed of the interface (Enabled) or configured manually (Disabled).
Port ID	A unique value that is automatically generated based on the port priority value and the interface index.
STP State	Spanning tree state of this interface. Can be Enable or Disable, Disable is the default.
Port Forwarding State	<ul style="list-style-type: none">Blocking – The port discards user traffic and receives, but does not send, BPDUs. During the election process, all ports are in the blocking state. The port is blocked to prevent network loops.Listening – The port sends and receives BPDUs and evaluates information to provide a loop-free topology. This state occurs during network convergence and is the first state in transitioning to the forwarding state.Learning – The port learns the MAC addresses of frames it receives and begins to populate the MAC address table. This state occurs during network convergence and is the second state in transitioning to the forwarding state.Forwarding – The port sends and receives user traffic.Disabled – The port is physically down, or administratively disabled and is not part of the spanning tree.

Field	Description
Port Role	<p>The role of the port within the MST, which is one of the following:</p> <ul style="list-style-type: none"> • Root – A port on the non-root bridge that has the least-cost path to the root bridge. • Designated – A port that has the least-cost path to the root bridge on its segment. • Alternate – A blocked port that has an alternate path to the root bridge. • Backup – A blocked port that has a redundant path to the same network segment as another port on the bridge. • Master – The port on a bridge within an MST instance that links the MST instance to other STP regions. • Disabled – The port is administratively disabled and is not part of the spanning tree.
Designated Root	The bridge ID of the root bridge for the MST instance.
Designated Cost	The path cost offered to the LAN by the designated port.
Designated Bridge	The bridge ID of the bridge with the designated port.
Designated Port	The port ID of the designated port.

If you modify any MSTP port settings, click **APPLY** to save the changes for the current boot session. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

On a Layer 2 switch, Virtual LAN (VLAN) support offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header. Like a router, a VLAN switch partitions the network into logical segments. Partitioning the network provides better administration, security, and multicast traffic management.

A VLAN is a set of end stations and the switch ports that connect them. Many reasons exist for the logical division, such as department or project membership. The only physical requirement is that the end station and the port to which it is connected both belong to the same VLAN.

Each VLAN in a network has an associated VLAN ID, which displays in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station may omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet may either reject it or insert a tag using its default VLAN ID. A given port may handle traffic for more than one VLAN, but it can only support one default VLAN ID.

HPE Networking Instant On 1930 Switch Series switches support up to 256 VLANs.

VLAN Configuration

Use the VLAN Configuration page to view information on VLANs currently defined on the switch and to add and edit VLAN information.

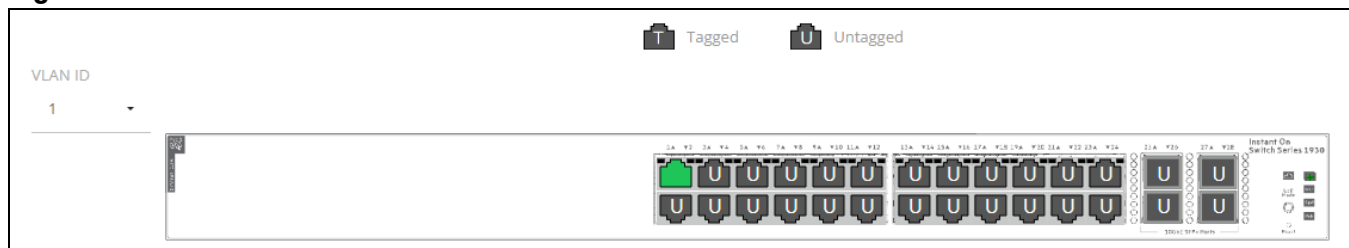
To view the VLAN Configuration page, click **VLAN > VLAN Configuration** in the navigation pane.

Device View

The top of the VLAN Configuration page shows a graphical representation of the switch front panel. This panel view has a display of the ports, each with its current status.

Select the VLAN ID to view from the drop-down on the left side of the display.

Figure 85: VLAN Switch Panel View



The VLAN Switch Panel View shows the tagging behavior for each port in this VLAN:

- **Tagged**—The port is a tagged member of the selected VLAN. When frames in this VLAN are forwarded on this port, the VLAN ID will be included in the frame's Ethernet header.
- **Untagged**—The port is an untagged member of the selected VLAN. When frames in this VLAN are forwarded on this port, the VLAN ID will not be included in the frame's Ethernet header.

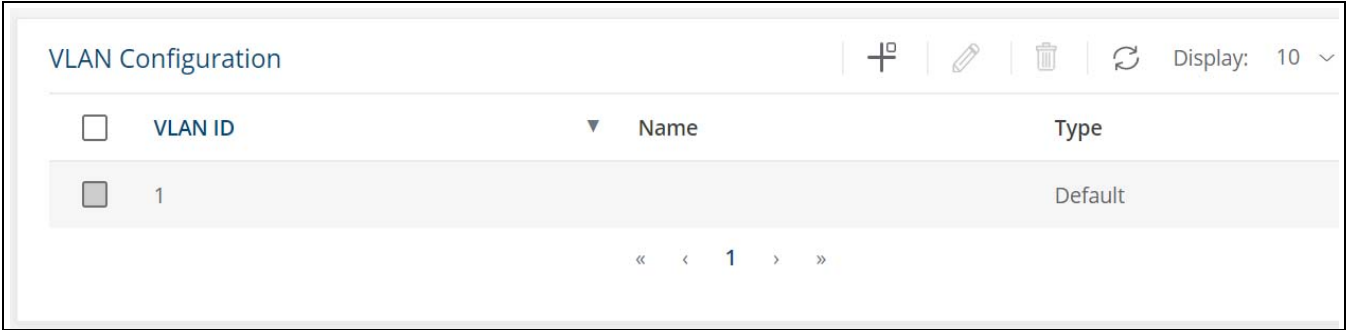
If there is no indication, this means that the port is not a member of a VLAN. For more information, see [Switch Panel View](#).

Click on a port to open the **Edit VLAN Membership** dialog box. The content of the dialog depends on the currently active **VLAN Membership** tab.

Click **APPLY** to save any changes for the currently selected VLAN interface.

VLAN Configuration

Figure 86: VLAN Configuration Tile



By default, VLAN 1 is defined on the switch and designated as the default VLAN. VLAN 1 cannot be modified or deleted. All ports are members of VLAN 1 by default.

VLAN 1 is also the default management VLAN, which identifies the VLAN that management users must be a member of. The administrator can configure a different VLAN as the management VLAN. See [Management VLAN Settings](#) for additional information about the management VLAN.

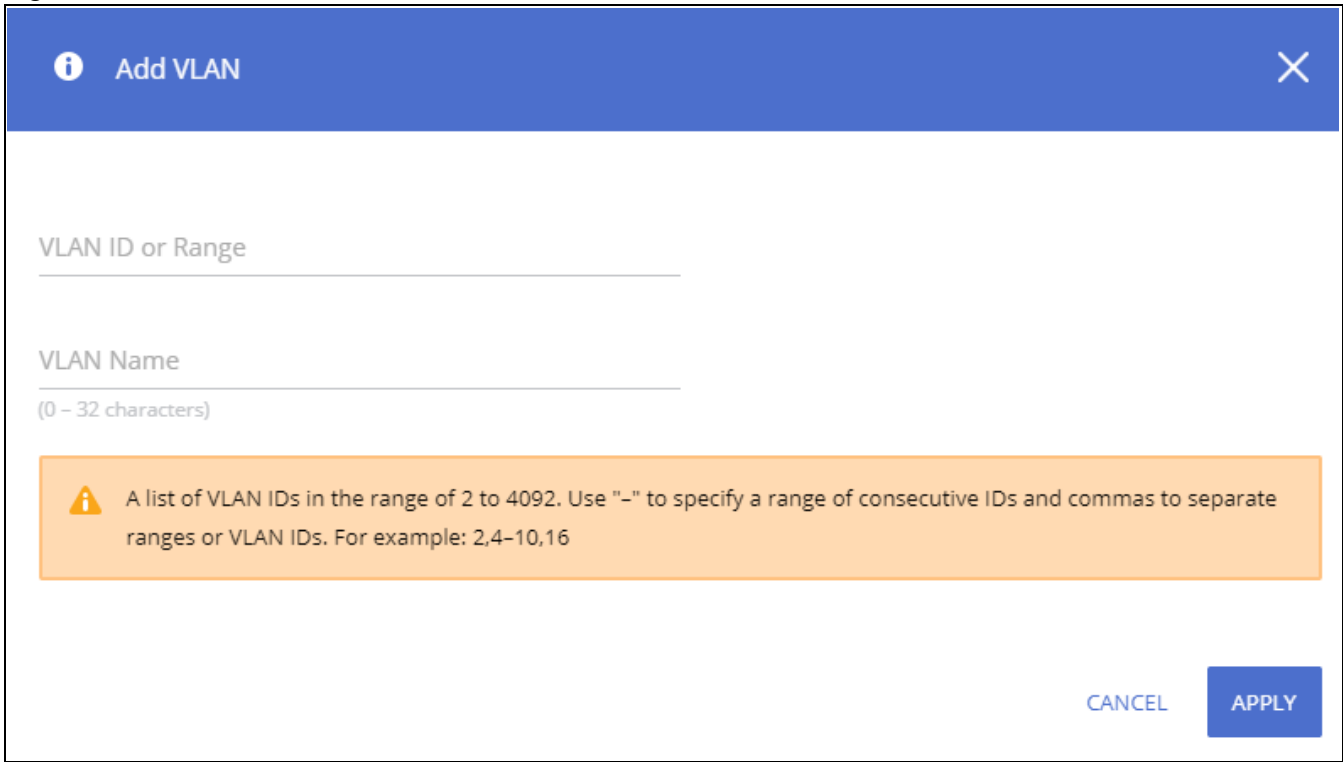
The following information is displayed for each VLAN:

Table 70: VLAN Configuration Fields

Field	Description
VLAN ID	The numerical VLAN identifier (VID) assigned to the VLAN, from 1 to 4092. Note: VLAN 0 (VID = 0x000 in a frame) is reserved and is used to indicate that the frame does not belong to any VLAN. In this case, the 802.1Q tag specifies only a priority and the value is referred to as a <i>priority tag</i> .
Name	A user-configurable name that identifies the VLAN.
Type	The type of VLAN, which can be one of the following: <ul style="list-style-type: none">• Default—The default VLAN. This VLAN is always present, and the VLAN ID is 1.• RADIUS— A VLAN created by a RADIUS VLAN assignment.• Static—A user-configured VLAN.

To add a VLAN, click **Add** .

Figure 87: Add VLAN



The 'Add VLAN' dialog box features a blue header with an information icon and a close button. It contains two input fields: 'VLAN ID or Range' and 'VLAN Name' (with a '(0 - 32 characters)' hint). An orange warning box states: 'A list of VLAN IDs in the range of 2 to 4092. Use "-" to specify a range of consecutive IDs and commas to separate ranges or VLAN IDs. For example: 2,4-10,16'. At the bottom right are 'CANCEL' and 'APPLY' buttons.

In the **VLAN ID or Range** field, specify one or more VLAN IDs in the range 2 to 4092.



VLAN 4093 and 4094 are reserved for internal system use.

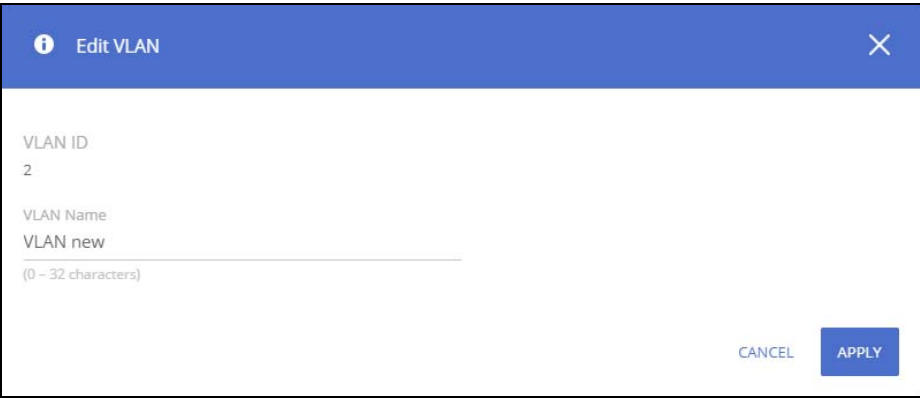
To create a range of VLANs, specify the beginning and ending VLAN IDs, separated by a dash. Optionally you can define a name for the VLAN in the **VLAN Name** field.

To create multiple non-sequential VLANs, separate each VLAN ID with a comma. You can create up to 256 VLANs.

When you have entered the VLAN IDs and/or range(s) as needed, click **APPLY**.

To change the VLAN name, select it on the VLAN Configuration tile and click **Edit**  .

Figure 88: Edit VLAN Dialog Box



The 'Edit VLAN' dialog box has a blue header with an information icon and a close button. It shows the 'VLAN ID' field with the value '2' and the 'VLAN Name' field with the value 'VLAN new' (with a '(0 - 32 characters)' hint). At the bottom right are 'CANCEL' and 'APPLY' buttons.

In the **Edit VLAN** dialog box, specify the new name consisting of 0 to 32 alphanumeric characters and click **APPLY**.

To remove a VLAN, select the VLAN in the table, and click **Remove**  .

VLAN Membership

By default, all ports and trunks are assigned membership in the default VLAN (VLAN 1). If you create additional VLANs, you can add interfaces as members of the new VLANs and configure VLAN tagging settings for the interfaces. You can also modify interface memberships in VLAN 1.

To configure interface VLAN memberships, click **VLAN > VLAN Configuration** in the navigation pane and scroll down to the VLAN Membership tile.

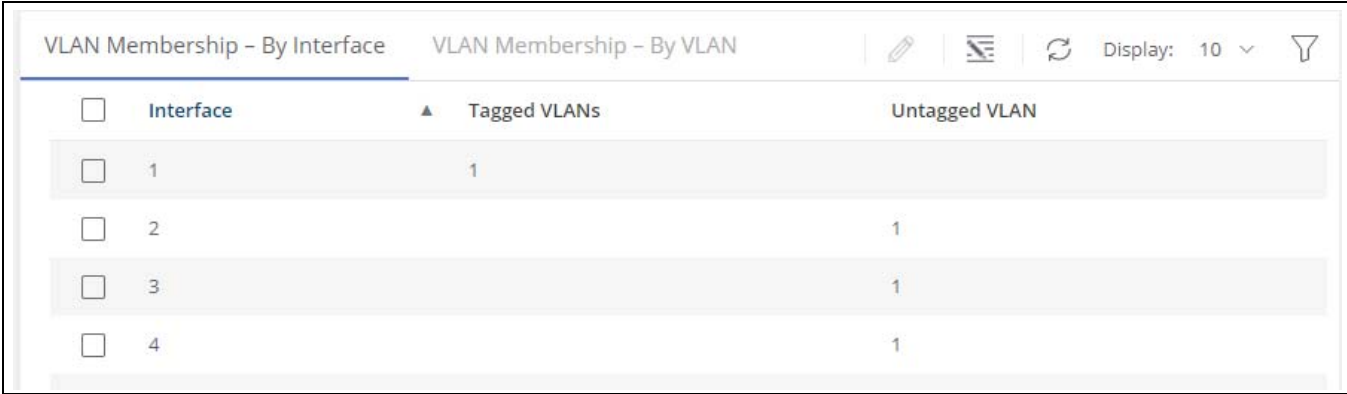
This tile has two tabs:

- VLAN Membership - By Interface - for configuring the interface to VLAN membership for one or more VLANs.
- VLAN Membership - By VLAN - for configuring VLAN membership participation for one or more interfaces.

VLAN Membership - By Interface Tab

Use the VLAN Membership - By Interface tab to view the tagging behavior of each interface in the VLAN.

Figure 89: VLAN Membership - By Interface Tab



VLAN Membership - By Interface		VLAN Membership - By VLAN				Display: 10	
☐ Interface		▲ Tagged VLANs		Untagged VLAN			
☐ 1		1					
☐ 2				1			
☐ 3				1			
☐ 4				1			

Table 71: VLAN Membership - By Interface Fields

Field	Description
Interface	The port or trunk ID.
Tagged VLANs	The port is a tagged member of the specified VLAN(s). When frames in these VLANs are forwarded on this port, the VLAN ID will be included in the frame's Ethernet header.
Untagged VLAN	The port is an untagged member of the specified VLAN. When frames in this VLAN are forwarded on this port, the VLAN ID will not be included in the frame's Ethernet header.

To configure VLAN Membership - By Interface, select one or more ports and click **Edit**  . Or, click **Edit All**  to configure all ports at the same time.

On the **Edit VLAN Membership** page, enter the **Tagged VLAN(s)** for this interface, you can enter a range, or comma-separated list.

In addition, you can enter a single Untagged VLAN. The untagged VLAN cannot be one of the Tagged VLANs.

VLAN Membership - By VLAN Tab

Use the VLAN Membership - By VLAN tab to configure the participation mode of each interface in the VLAN.

Figure 90: VLAN Membership - By VLAN Tab

VLAN ID	Interface	Participation	Tagging
1	1	Included	Tagged
	2	Included	Untagged
	3	Included	Untagged

Table 72: VLAN Membership - By VLAN Tab Fields

Field	Description
VLAN ID	Select the VLAN ID for which you want to view interface memberships.
Interface	The port or trunk ID.
Participation	The participation mode of the interface in the selected VLAN, which is one of the following: <ul style="list-style-type: none">Included – The port is a member of the selected VLAN. This mode is also equivalent to registration fixed in the IEEE 802.1Q standard.Excluded – The port is not a member of the selected VLAN. This mode is also equivalent to registration forbidden in the IEEE 802.1Q standard.
Tagging	The tagging behavior for each port in this VLAN, which is one of the following: <ul style="list-style-type: none">Tagged—The port is a tagged member of the selected VLAN. When frames in this VLAN are forwarded on this port, the VLAN ID will be included in the frame's Ethernet header.Untagged—The port is an untagged member of the selected VLAN. When frames in this VLAN are forwarded on this port, the VLAN ID will not be included in the frame's Ethernet header.

To configure VLAN Membership - By VLAN, select the VLAN to configure, from the VLAN ID drop-down, then select one or interfaces and click **Edit** . Or, click **Edit All** to configure all the interfaces at the same time.

On the **Edit VLAN Membership** page, configure the **Participation** and **Tagging** settings to specify whether the ports are excluded from the VLAN or are included as a tagged or untagged member.

Consider the following guidelines when editing VLAN port memberships and settings:

- A port can be an untagged member of only one VLAN.
If you change the VLAN that a port is an untagged member of, then the port will be excluded from the VLAN where it was previously an untagged member.
- A port can be a tagged member of multiple VLANs.
- Every port must be a member of at least one VLAN, as either a tagged or an untagged member.
- You cannot exclude a port from a VLAN unless the port is a member of at least one other VLAN.
- If you exclude a port from the management VLAN, a computer connected to the switch through that port will be unable to access the switch management interface.
- Ports belonging to a trunk cannot be assigned membership in a VLAN, although the trunk itself can be a member of one or more VLANs. If VLAN configuration was applied to such a port before it was assigned to

a trunk, this VLAN configuration will be retained as an inactive configuration and will not be displayed. When the port is removed from the trunk, the VLAN configuration will become active.

Click **APPLY** to save any changes for the currently selected VLAN. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

VLAN Interface Configuration

Use the VLAN Interface Configuration tile to configure the way interfaces handle VLAN-tagged, priority-tagged, and untagged traffic.

To view this tile, click **VLAN > VLAN Configuration** in the navigation pane.

Figure 91: VLAN Interface Configuration Tile

☐	Interface ▲	Port VLAN ID	Acceptable Frame Type	Ingress Filtering	Untagged VLAN	Tagged VLANs
☐	1	1	Tagged and Untagged	Enabled	1	1
☐	2	1	Tagged and Untagged	Enabled	1	1
☐	3	1	Tagged and Untagged	Enabled	1	1
☐	4	1	Tagged and Untagged	Enabled	1	1
☐	5	1	Tagged and Untagged	Enabled	1	1

Table 73: VLAN Interface Configuration Fields

Field	Description
Interface	Identifies the physical interface or LAG associated with the rest of the data in the row.
Port VLAN ID	The VLAN ID assigned to untagged or priority tagged frames received on this port. This value is also known as the Port VLAN ID (PVID). In a tagged frame, the VLAN is identified by the VLAN ID in the tag.
Acceptable Frame Type	Indicates how the interface handles untagged and priority tagged frames: <ul style="list-style-type: none"> Tagged and Untagged – Untagged, priority tagged and tagged frames received on the interface are accepted and assigned the value of the Port VLAN ID for this interface. Tagged Only – The interface discards any untagged or priority tagged frames it receives. Untagged Only – The interface discards any tagged frames it receives. For all options, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN standard.
Ingress Filtering	Shows how the port handles tagged frames. <ul style="list-style-type: none"> Enabled: A tagged frame is discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. This is the default setting Disabled: All tagged frames are accepted.
Untagged VLAN	VLAN that is configured on the port to transmit egress packets as untagged.
Tagged VLANs	VLANs that are configured on the port to transmit egress packets as tagged.

To modify these settings for one or more interfaces, select the interface and click **Edit** . Or, click **Edit All** to configure all interfaces at the same time.

Voice VLAN Configuration

Use the Voice VLAN Configuration page to configure the global administrative mode of the Voice VLAN feature as well as the per-port settings. When Voice VLAN is configured on a port that receives both voice and data traffic, it can help ensure that the voice traffic has priority.

The switch supports OUI based Voice VLAN with the ability to dynamically detect voice traffic based on telephony OUI's.

The voice VLAN ID must be manually configured through the switch's web interface and ports enabled to participate in the voice VLAN. When the switch receives a packet with a source MAC address matching to one of the configured telephony OUIs, the port is dynamically placed in the voice VLAN.

The switch supports up to 16 OUIs. You can manually add or remove OUIs. The switch also supports pre-defined OUIs that exist on the switch by default. If the switch is reset back to factory defaults, only the pre-defined OUIs are available.

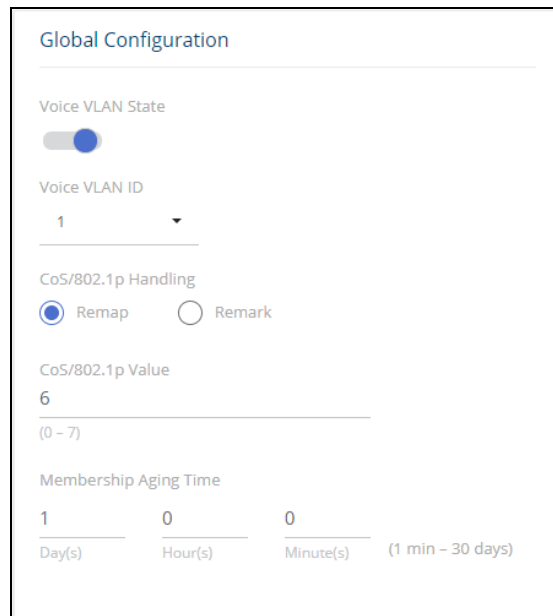
These are the pre-defined OUIs:

- Siemens (00-01-e3)
- Avaya (00-09-6e)
- 3Com (00-0f-e2)
- H3C (00-60-b9)
- Cisco (00-03-6b)
- Polycom (64-16-7F)
- Yealink (80-5E-0C)

To display the Voice VLAN Configuration page, click **VLAN > Voice VLAN Configuration** in the navigation pane.

Global Configuration

Figure 92: Global Configuration



The screenshot shows the 'Global Configuration' page for Voice VLAN settings. It includes a toggle for 'Voice VLAN State' which is currently turned on. Below this is a dropdown for 'Voice VLAN ID' set to '1'. The 'CoS/802.1p Handling' section has two radio buttons: 'Remap' (selected) and 'Remark'. The 'CoS/802.1p Value' is set to '6' with a range of '(0 - 7)'. The 'Membership Aging Time' section has three input fields: '1' for Day(s), '0' for Hour(s), and '0' for Minute(s), with a note '(1 min - 30 days)'.

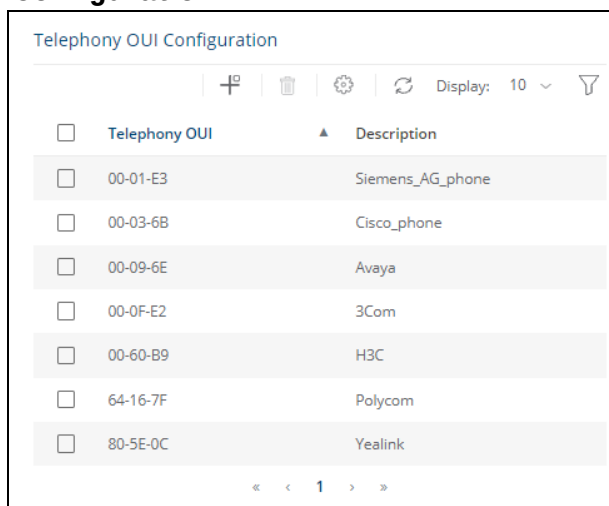
Global Configuration			
Voice VLAN State			
☒			
Voice VLAN ID			
1			
CoS/802.1p Handling			
☒ Remap ☐ Remark			
CoS/802.1p Value			
6			
(0 - 7)			
Membership Aging Time			
1	0	0	
Day(s)	Hour(s)	Minute(s)	(1 min - 30 days)

Table 74: Global Configuration Fields

Field	Description
Voice VLAN State	Set as Enabled to globally enable Voice VLAN operation. The Voice VLAN still needs to be enabled on the interface that requires the voice VLAN operation.
Voice VLAN ID	Specify the VLAN that will carry voice traffic on enabled interfaces.
CoS/802.1p Handling	Define the Class of Service (CoS) setting for the voice traffic received on enabled interfaces: <ul style="list-style-type: none"> Remap - remap incoming voice traffic to the CoS specified in the "CoS/802.1p Value" field. Remark - remap and remark the L2 field of incoming voice traffic to the CoS specified in the "CoS/802.1p Value" field.
CoS/802.1p Value	The CoS value to remap or remark to.
Membership Aging Time	Set the maximum duration (days, hours and minutes) that the enabled port will be a member of the voice VLAN, after receiving voice VLAN traffic.

Telephony OUI Configuration

Use the Telephony OUI Configuration tile to add a MAC address prefix to the voice VLAN OUI table. The MAC prefixes in the OUI are used to identify voice traffic received on ports that are voice VLAN enabled.

Figure 93: Telephony OUI Configuration**Table 75: Telephony OUI Configuration Fields**

Field	Description
Telephony OUI	Specify the MAC address prefix which will be used to identify voice traffic.
Description	Description of the Telephony OUI.

To add a configuration, click **Add** .

To remove a configuration, select it and click **Remove** .

To restore the defaults, click **Restore Default** .

Click **APPLY** to save any changes for the currently selected configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Voice VLAN Interface Settings

Figure 94: Voice VLAN Interface Settings Page

Voice VLAN Interface Settings								Display: 10 	
☐	Interface	▲	Admin Voice VLAN Membership	Operational Voice VLAN Membership	QoS Mode				
☐	1		Disabled	Inactive	MAC Address				
☐	2		Disabled	Inactive	MAC Address				
☐	3		Disabled	Inactive	MAC Address				
☐	4		Disabled	Inactive	MAC Address				
☐	5		Disabled	Inactive	MAC Address				

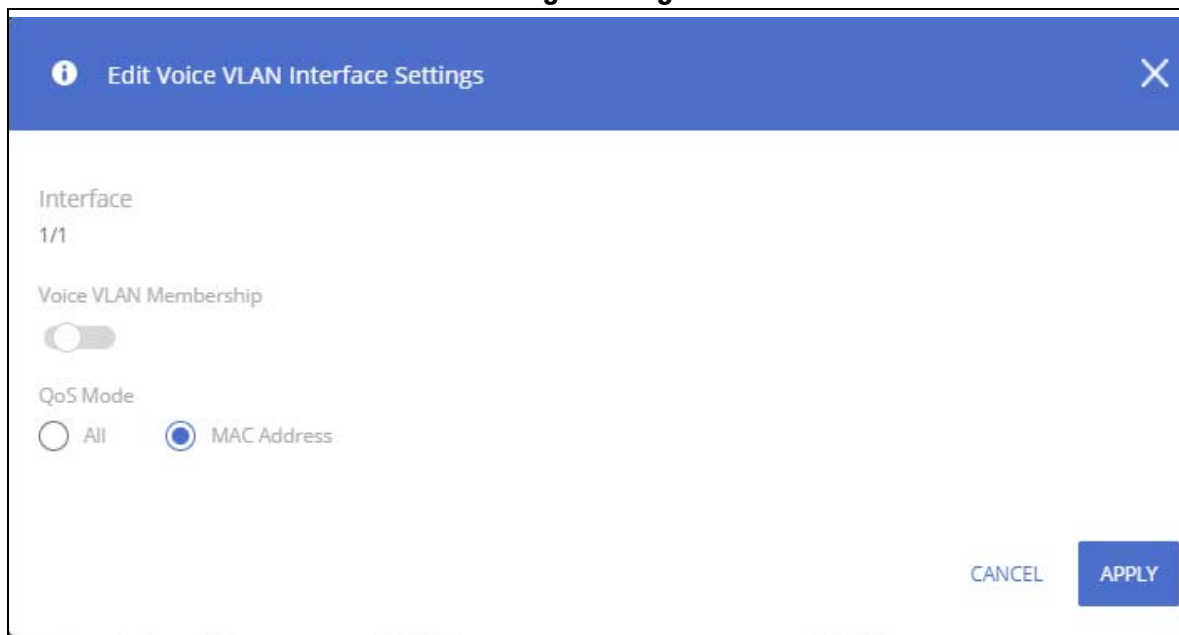
Table 76: Voice VLAN Interface Settings Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring the Voice VLAN Interface settings, this field identifies the interface(s) that are being configured.
Admin Voice VLAN Membership	Click Enable or Disable to enable the Voice VLAN feature on the interface. When Voice VLAN is enabled globally and configured on interfaces that carry voice traffic, this feature can help ensure that the sound quality of an IP phone does not deteriorate when data traffic on the port is high. NOTE: In the edit window, the field name is Voice VLAN Membership.
Operational Voice VLAN Membership	This is a read only field that indicates the operational status of the Voice VLAN feature on the interface. The Interface Voice VLAN operational status will be in the active state if all the following conditions exist: <ul style="list-style-type: none">• Voice VLAN must be globally enabled and enabled on the interface.• The interface must be up.• The interface must have a link and be receiving traffic with source OUI matching one of those in the Telephony OUI Configuration table. An example for active state is if interface receives a voice call with source MAC that equals one of the listed OUI. An example of Inactive state is if such a call ended and the OUI MAC entry aged out.
QoS Mode	The Quality of Service override mode: <ul style="list-style-type: none">• All - the voice VLAN QoS attributes will be applied to all traffic forwarded on this port on the voice VLAN.• MAC Address - the voice VLAN QoS attributes will be applied only to packets with source MAC matching one of those in the OUI table.

To modify these settings for one or more interfaces, select the interface and click **Edit**  .

To configure all interfaces at the same time, click **Edit All**  .

Figure 95: Edit Voice VLAN Interface Settings Dialog Box



The dialog box has a blue header bar with the title "Edit Voice VLAN Interface Settings" and a close button (X) in the top right corner. The main content area is white and contains the following settings:

- Interface:** 1/1
- Voice VLAN Membership:** A toggle switch that is currently turned off.
- QoS Mode:** Two radio buttons are present: "All" (which is unselected) and "MAC Address" (which is selected with a blue dot).

In the bottom right corner, there are two buttons: a light blue "CANCEL" button and a dark blue "APPLY" button.

Click **APPLY** to update the switch configuration. Your changes take effect immediately, but are not retained across a switch reset unless you click **Save Configuration**.



Chapter 8

Neighbor Discovery

LLDP is a standard discovery protocol defined by IEEE 802.1AB. It allows stations residing on a LAN to advertise device capabilities, physical descriptions, and management information to other devices on the network. A network management system (NMS) can access and display this information.

LLDP is a one-way protocol; there are no request/response sequences. Information is advertised in LLDP Protocol Data Units (LLDPDUs) by stations implementing the LLDP transmit function, and LLDPDUs are received and processed by stations implementing the receive function. The transmit and receive functions can be enabled and disabled separately per port. By default, both functions are enabled on all ports.

LLDP-MED is an extension of the LLDP standard. LLDP-MED uses LLDP's organizationally-specific Type-Length-Value (TLV) extensions and defines additional TLVs.

LLDP-MED can be utilized for many advanced features in a VoIP network environment. These features include basic configuration, network policy configuration, location identification (including for Emergency Call Service / E911), inventory management, and more.

LLDP-MED provides extensions to the IEEE 802.1AB base protocol to allow for these functions, and also provides behavioral requirements for devices implementing the extensions to enable correct multi-vendor inter-operation.

LLDP

Use the LLDP page to configure Global LLDP, to view LLDP Global Information, to configure the protocol on individual interfaces, and to view LLDP information and statistics.

To view the LLDP page, click **Neighbor Discovery > LLDP** in the navigation pane.

LLDP Global Configuration

Figure 96: LLDP Global Configuration Tile

LLDP Global Configuration

Transmit Interval

30

(5 – 32768) Seconds

Transmit Hold Multiplier

4

(2 – 10) Seconds

Re-Initialization Delay

2

(1 – 10) Seconds

Modification Interval

5

(5 – 3600) Seconds

You can configure the following global settings:

Table 77: LLDP Global Configuration Fields

Field	Description
Transmit Interval	Specify the time between transmission of LLDPDUs. The range is from 5 to 32768 seconds and the default is 30 seconds.
Transmit Hold Multiplier	Specify the multiplier value on the transmit interval, which is used to compute the time-to-live (TTL) value associated with LLDPDUs. The range is from 2 to 10 seconds, and the default is 4 seconds.
Re-Initialization Delay	Specify the number of seconds to wait before attempting to re-initialize LLDP on a port after the LLDP operating mode on the port changes. The range is from 1 to 10 seconds and the default is 2 seconds.
Modification Interval	Specify the minimum number of seconds to wait between transmissions of remote data change notifications. The range is from 5 to 3600 seconds and the default is 5 seconds.

If you change these settings, click **APPLY** to save any changes for the current boot session. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

LLDP Global Information

Use the LLDP Global Information tile to view the information that is included in the switch LLDP advertisement.

Figure 97: LLDP Global Information

LLDP Global Information
Chassis ID
00:00:B0:17:12:00
Chassis ID Subtype
MAC Address
Capabilities Supported
Bridge
Capabilities Enabled
Bridge

Table 78: LLDP Global Information Fields

Field	Description
Chassis ID	The hardware platform identifier for the switch.
Chassis ID Subtype	The type of information used to identify the chassis.
Capabilities Supported	The primary function(s) the switch supports.
Capabilities Enabled	The primary function(s) the switch supports that are enabled.

Interface Configuration

The following information is displayed for each LLDP interface.

Figure 98: Interface Configuration

Interface Configuration						
☐	Interface ▲	Link Status	Transmit	Receive	Notify	Transmit Management Information
☐	1	Link Down	Enabled	Enabled	Enabled	Yes
☐	2	Link Up	Enabled	Enabled	Enabled	Yes
☐	3	Link Up	Enabled	Enabled	Enabled	Yes
☐	4	Link Up	Enabled	Enabled	Enabled	Yes
☐	5	Link Up	Enabled	Enabled	Enabled	Yes

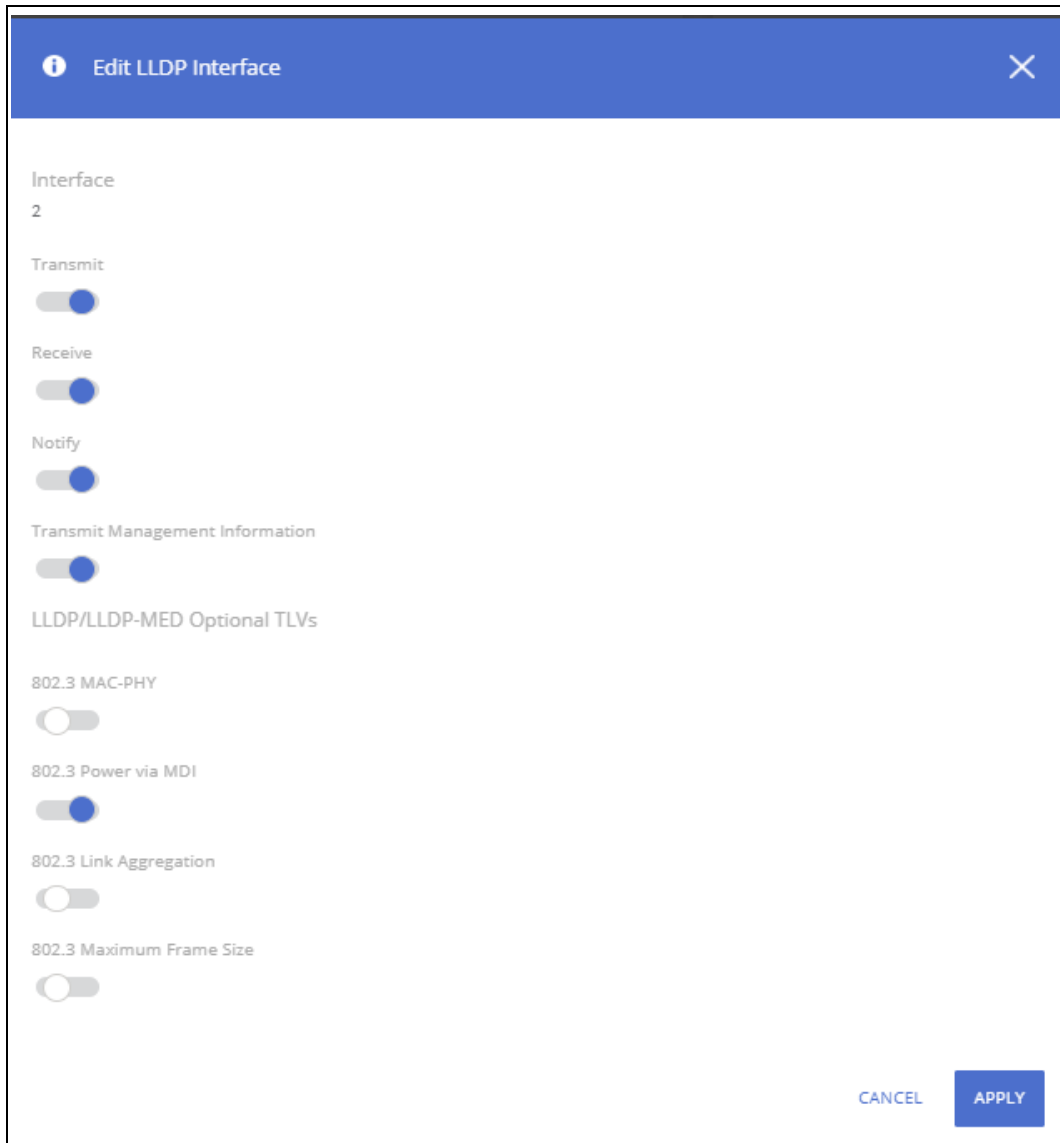
Table 79: Interface Configuration Fields

Field	Description
Interface	The port ID.
Link Status	The link status of the interface, which is either Up or Down. An interface that is down does not forward traffic.

Field	Description
Transmit	The LLDP advertise (transmit) mode on the interface. If the transmit mode is enabled, the interface sends LLDPDUs that advertise the mandatory TLVs that are enabled.
Receive	The LLDP receive mode on the interface. If the receive mode is enabled, the switch can receive LLDPDUs from other devices.
Notify	Enable to have LLDP generate a log file entry.
Transmit Management Information	Indicates whether management address information for the local switch is transmitted in LLDPDUs. Other remote managers can obtain information about the switch by using its advertised management address

To modify interface settings, select one or more interfaces and click **Edit**  to display the **Edit LLDP Interface** page. Or, click **Edit All**  to configure all interfaces at the same time.

Figure 99: Edit LLDP Interface



Edit LLDP Interface

Interface
2

Transmit
☒

Receive
☒

Notify
☒

Transmit Management Information
☒

LLDP/LLDP-MED Optional TLVs

802.3 MAC-PHY
☐

802.3 Power via MDI
☒

802.3 Link Aggregation
☐

802.3 Maximum Frame Size
☐

CANCEL
APPLY

The following additional options are configurable from the **Edit** dialog.

Table 80: Additional LLDP Interface Fields

Field	Description
802.3 MAC-PHY	Duplex and bit rate capability and the current duplex and bit rate settings of the sending device.
802.3 Power via MDI	This field appears for PoE devices. This TLV supports the following extensions. <ul style="list-style-type: none"> Type 2 (12 octets) Type 3 (29 octets) This option is enabled by default.
802.3 Link Aggregation	Set to enable the link (associated with the port on which the LLDP PDU is transmitted) to be aggregated.
802.3 Maximum Frame Size	Maximum frame size capability of the MAC/PHY implementation.

Device Information Tile

This tile has two tabs:

- Remote Device Information - for the remote devices
- Local Device Information - for the local devices

To display the Device Information tabs, click **Neighbor Discovery > LLDP** in the navigation pane, and scroll down to the **Remote/Local Device Information** tile.

Remote Device Information Tab

Use the Remote Device Information tab to view information about remote devices for which the switch has received LLDP information. Interfaces that have this option enabled display in this table only if they have received LLDP notifications from a remote device.

Figure 100: Remote Device Information Tab

Interface	Remote ID	Chassis ID	Port ID	Port Description	System Name	Capabilities Supported	Capabilities Enabled	System ID
1/1	3	00:00:00:02:17:03	1/2	1/2		Bridge	Bridge	

Table 81: Remote Device Information Fields

Field	Description
Interface	The device interface that received the LLDP data from the remote system.
Remote ID	The identifier assigned to the remote system that sent the LLDPDU.
Chassis ID	The hardware platform ID for the remote system.
Port ID	The physical address of the port on the remote device that sent the LLDP data.
Port Description	The port description configured on the remote device. If the port description is not configured, the field may show the interface number of the remote port, or it may be blank.
System Name	The system description configured on the remote device. If the system description is not configured, the field is blank.

Field	Description
Capabilities Supported	The capabilities on the remote device. The possible capabilities include: Repeater, Bridge, WLAN AP, Router, Telephone, DOCSIS cable device, and Station.
Capabilities Enabled	The capabilities on the remote device that are enabled.
System ID	The reported management IP or MAC addresses of the remote device.

Local Device Information Tab

Use the Local Device Information tab to view LLDP information for switch interfaces.

To display this tab, click **Neighbor Discovery > LLDP** in the navigation pane and click the **Local Device Information** tab (next to the **Remote Device Information** tab).

Figure 101: Local Device Information Tab

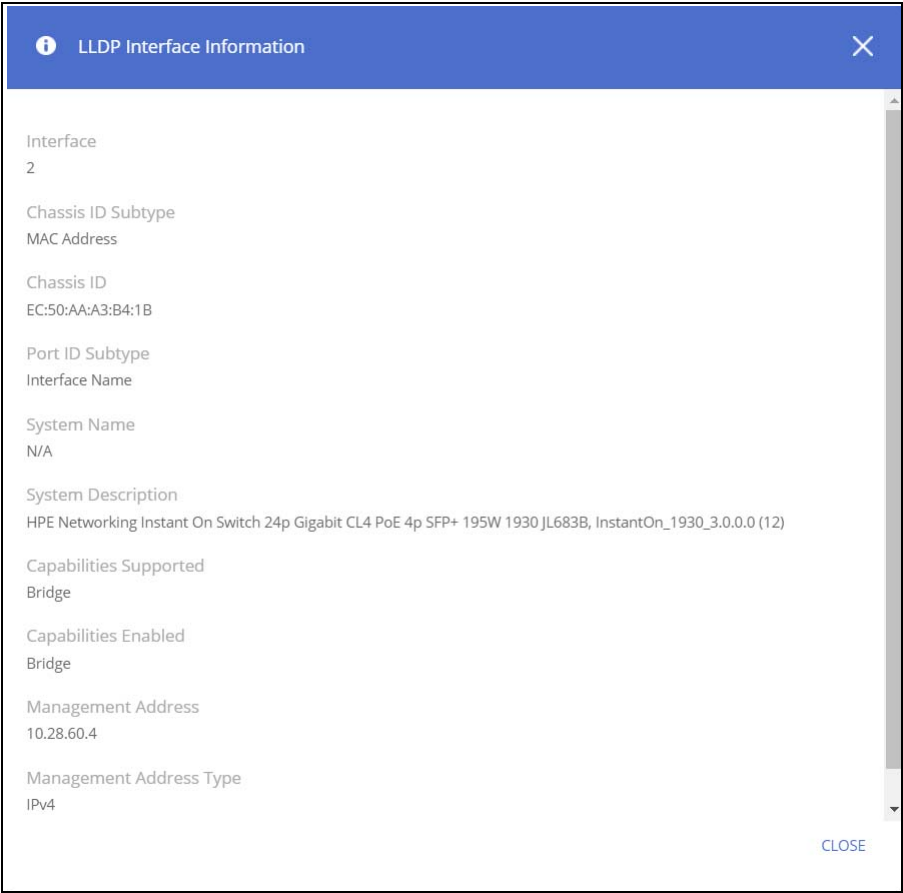
Remote Device Information		Local Device Information			Display: 10	
Interface	Port ID	Port ID Subtype	Port Description			
1	1	Interface Name	1			
2	2	Interface Name	2			
3	3	Interface Name	3			
4	4	Interface Name	4			
5	5	Interface Name	5			

Table 82: Local Interface Information Fields

Field	Description
Interface	The interface ID.
Port ID	The port identifier, which is the interface name.
Port ID Subtype	The type of information used to identify the interface.
Port Description	A description of the port.

To view additional information about an interface, select the interface row and click **Details** .

Figure 102: LLDP Interface Information



This page displays the following fields.

Table 83: LLDP Interface Information Fields

Field	Description
Interface	The interface ID.
Chassis ID Subtype	The type of information used to identify the chassis.
Chassis ID	The hardware platform identifier for the switch.
Port ID Subtype	The type of information used to identify the interface
System Name	The user-configured system name for the switch. The system name is configured on the Dashboard page.
System Description	The switch description which includes information about the product model and platform.
Capabilities Supported	The primary function(s) the switch supports.
Capabilities Enabled	The primary function(s) the switch supports that are enabled.
Management Address	The address, such as an IP address, associated with the management interface of the switch.
Management Address Type	The protocol type or standard associated with the management address.

LLDP Statistics

The Link Layer Discovery Protocol (LLDP) Statistics tile displays per-port information for LLDP and LLDP-MED frames transmitted and received on the switch.

To display the LLDP Statistics tile, click **Neighbor Discovery > LLDP** in the navigation pane.

Figure 103: LLDP Statistics Tile

LLDP Statistics							
Interface ▲	Transmitted Frames	Received Frames	Discarded Frames	Errors	Discarded TLVs	Unrecognized TLVs	Neighbor Ageouts
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0

Table 84: LLDP Statistics Fields

Field	Description
Interface	The interface ID.
Transmitted Frames	The number of LLDP frames transmitted on the interface.
Received Frames	The number of LLDP frames received on the interface.
Discarded Frames	The number of LLDP frames the interface discarded for any reason.
Errors	The number of invalid LLDP frames received by the LLDP agent on the interface.
Discarded TLVs	The number of received LLDP TLVs that were discarded.
Unrecognized TLVs	The number of received LLDP TLVs that were not recognized.
Neighbor Ageouts	The number of LLDP neighbors that aged out on this interface.

Click **Clear All**  to reset all statistics to 0.

LLDP-MED

Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) is an enhancement to LLDP that enables:

- Auto-discovery of LAN policies (such as VLAN and Layer 2 Priority settings) for VoIP phones and other network elements.
- Switch location discovery for creation of location databases. For example, this information is used during emergency calls to identify the location of the MED (for VoIP and enhanced 911 services).
- Extended and automated power management of Power over Ethernet (PoE) endpoints.

- Inventory management, enabling network administrators to track their network devices and determine their characteristics (manufacturer, software and hardware versions, serial/asset number).
- To view and configure global Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) settings, click **Neighbor Discovery > LLDP-MED** in the navigation pane.

LLDP-MED Global Configuration

Figure 104: LLDP-MED Global Configuration Tile

LLDP-MED Global Configuration

Fast Start Repeat Counter

3

(1 - 10)

Device Class

Network Connectivity

The following global settings display:

Table 85: LLDP-MED Global Configuration Fields

Field	Description
Fast Start Repeat Counter	The number of LLDP-MED Protocol Data Units (LLDPDUs) that are transmitted during the fast start period when LLDP-MED is enabled. The valid range is 1-10. The default is 3.
Device Class	The device's MED classification. The HPE Networking Instant On 1930 Switch Series switch is classified as a Network Connectivity device.

If you change the Fast Start Repeat Counter value, click **APPLY** to save any changes for the current boot session. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

LLDP Global Information

Use the LLDP Global Information tile to view the information that is included in the switch LLDP advertisement.



The same tile appears in the LLDP page.

Figure 105: LLDP Global Information

LLDP Global Information
Chassis ID
00:00:B0:17:12:00
Chassis ID Subtype
MAC Address
Capabilities Supported
Bridge
Capabilities Enabled
Bridge

Table 86: LLDP Global Information Fields

Field	Description
Chassis ID	The hardware platform identifier for the switch.
Chassis ID Subtype	The type of information used to identify the chassis.
Capabilities Supported	The primary function(s) the switch supports.
Capabilities Enabled	The primary function(s) the switch supports that are enabled.

Interface Configuration

Use this tile to view and configure the interfaces.

To view the Interface Configuration tile, click **Neighbor Discovery > LLDP-MED** in the navigation pane.

Figure 106: Interface Configuration Tile

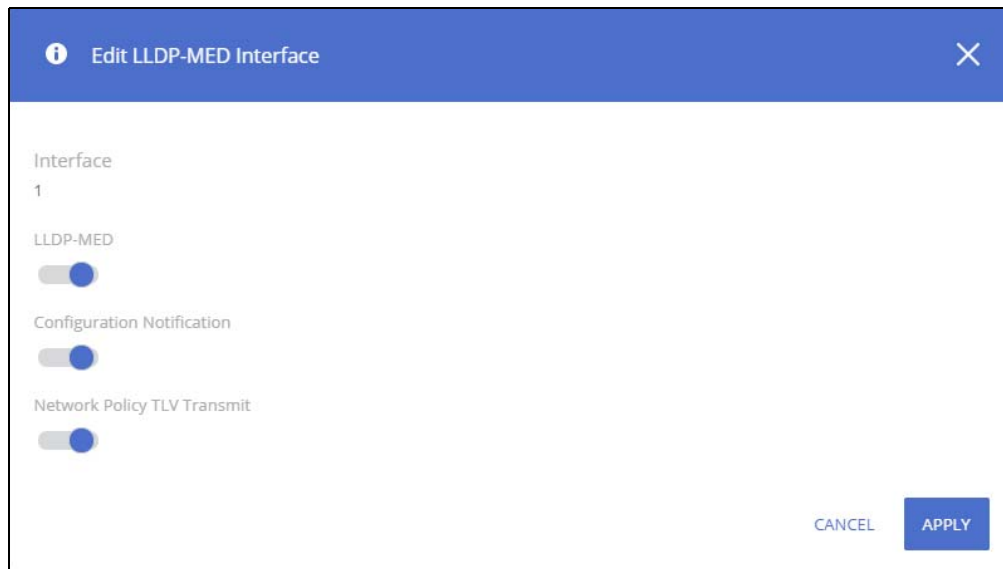
Interface Configuration										Display: 10	
☐	Interface ▲	Link Status	MED Mode	Notification Status	Operational Status	Transmitted TLVs					
☐	1	Link Down	Enabled	Disabled	Disabled	Capabilities, Network Policy					
☐	2	Link Up	Enabled	Disabled	Disabled	Capabilities, Network Policy					
☐	3	Link Up	Enabled	Disabled	Disabled	Capabilities, Network Policy					
☐	4	Link Up	Enabled	Disabled	Disabled	Capabilities, Network Policy					
☐	5	Link Up	Enabled	Disabled	Disabled	Capabilities, Network Policy					

The following information is displayed for each port:

Table 87: LLDP-MED Interface Configuration Fields

Field	Description
Interface	The ID of the physical and trunk interfaces.
Link Status	The link status of the interface, which is either Up or Down. An interface that is down does not forward traffic.
MED Mode	The administrative status of LLDP-MED on the interface. When enabled, the LLDP-MED transmit and receive functions are effectively enabled on the interface. This feature is enabled by default.
Notification Status	Indicates whether LLDP-MED topology change notifications are enabled or disabled on the interface. This feature is disabled by default.
Operational Status	Indicates whether the interface is configured to transmit TLVs. To transmit TLVs, the interface must be enabled to receive and transmit LLDPDUs and must be connected to an LLDP-MED switch. The switch waits for the LLDP-MED switch to advertise its information before the switch transmits its own LLDP-MED TLVs, at which point the operational status becomes enabled.
Transmitted TLVs	The LLDP-MED TLV(s) that the interface transmits. The HPE Networking Instant On 1930 Switch Series switch, can transmit TLVs of the following types: <ul style="list-style-type: none"> Capabilities Network Policy Power Sourcing Entity (PSE)

To enable or disable LLDP-MED on one or more interfaces, and to configure related features, select the interfaces and click **Edit** . Or, click **Edit All**  to configure all ports at the same time.

Figure 107: Edit LLDP-MED Interface

Table 88: Edit LLDP-MED Interface Fields

Field	Description
Interface	The port ID.
LLDP-MED	Enable/disable LLDP-MED on interface. Default is Enabled.
Configuration Notification	Enable/disable on interface sending topology change notifications. Default is Disabled.
Network Policy TLV Transmit	Enable/disable on interface sending Network policy TLV. Default is Enabled.

Remote Device Information

Use the LLDP-MED Remote Device Information page to view information about the remote devices the local system has learned through the LLDP-MED data units received on its interfaces. Information is available about remote devices only if an interface receives an LLDP-MED data unit from a switch.

To view this page, click **Neighbor Discovery > LLDP-MED** in the navigation pane.

Figure 108: LLDP-MED Remote Device Information Page

Remote Device Information			
Interface	Remote ID	Device Class	System ID
47	2	Undefined	10.5.227.130

Table 89: LLDP Remote Device Summary Fields

Field	Description
Interface	The local interface that has received LLDP-MED data units from remote devices.
Remote ID	The client identifier assigned to the remote system that sent the LLDP-MED data unit.
Device Class	The MED Classification advertised by the TLV from the remote device. The following three classifications represent the actual endpoints: <ul style="list-style-type: none">• Class I Generic (for example, IP Communication Controller)• Class II Media (for example, Conference Bridge)• Class III Communication (for example, IP Telephone) The fourth device is Network Connectivity Device, which is typically a device such as a LAN switch or router, IEEE 802.1 bridge, or IEEE 802.11 wireless access point.
System ID	The reported management IP addresses of the remote device.

Displaying Remote Device Details

To view additional information about a remote device, select the row including remote device information and click **Details** .

The following fields appear on the **LLDP-MED Remote Device Information** page:

Table 90: LLDP Remote Device Information Fields

Field	Description
Interface	The local interface that has received LLDP-MED data units from remote devices.
Remote ID	The client identifier assigned to the remote system that sent the LLDP-MED data unit.
System ID	The reported management IP addresses of the remote device.
Capabilities	
Capabilities Supported	The supported capabilities that were received in the MED TLV on this interface.
Capabilities Enabled	The supported capabilities on the remote device that are also enabled.
Device Class	The MED Classification advertised by the TLV from the remote device.
Inventory	
This section describes the information in the inventory TLVs received in the LLDP-MED frames on this interface.	

Field	Description
Hardware Revision	The hardware version advertised by the remote device.
Firmware Revision	The firmware version advertised by the remote device.
Software Revision	The software version advertised by the remote device.
Serial Number	The serial number advertised by the remote device.
Manufacturer Name	The name of the system manufacturer advertised by the remote device.
Model Name	The name of the system model advertised by the remote device.
Asset ID	The system asset ID advertised by the remote device.
Extended PoE	
This section describes whether the remote device is advertised as a PoE device.	
Device Type	If the remote device is a PoE device, this field identifies the PoE device type of the remote device connected to the port.
Extended PoE-PD	
This section describes the information about the remote PoE powered device.	
Required	If the remote device is a PoE device, this field details the remote ports PD power requirement in Watts.
Source	If the remote device is a PoE device, this field details the remote ports PoE PD power source.
Priority	If the remote device is a PoE device, this field details the remote ports PD power priority.
Network Policy Information	
This section describes the information in the network policy TLVs received in the LLDP-MED frames on this interface.	
Media Application Type	<p>The media application type received in the TLV from the remote device. The application types are unknown, voice-signaling, guest-voice, guest-voice-signaling, soft-phone-voice, video-conferencing, streaming-video, video-signaling.</p> <p>Each application type that is transmitted has the VLAN ID, priority, DSCP, tagged bit status and unknown bit status.</p> <p>The port on the remote device may transmit one or many such application types. This information is displayed only when a network policy TLV has been received.</p>
VLAN ID	The VLAN ID associated with a particular policy type.
Priority	The user priority associated with a particular policy type.
DSCP	The Differentiated Services Code Point value associated with a particular policy type.
Unknown Bit Status	The unknown bit associated with a particular policy type.
Tagged Bit Status	Identifies whether the network policy is defined for tagged or untagged VLANs.

Chapter 9

Power Over Ethernet

Power over Ethernet (PoE) functionality is supported on certain HPE Networking Instant On 1930 Switch Series switch models, enabling designated switch ports to provide power to connected devices. These PoE ports are referred to as power source equipment (PSE).

The devices receiving power through PoE are referred to as powered devices (PDs).

The PoE software supports two power modes to allocate power by Usage (default) or Class. The default usage mode reclaims unused power for use by new PD connections or increased power demand by existing powered PDs. The configurable class mode reserves the full PD requested class power from the total available power budget.

Ports are assigned one of three configurable PoE priority values (Critical, High, and Low). When more power is requested than is available on the switch, the switch provides power to high priority ports before lower priority ports. Power allocation can be scheduled so that power is supplied only during that schedule time.

The 1930 Class 4 PoE switches support the IEEE 802.3af/at standards providing 30W of power for Class 4 PD connections while maintaining backwards compatibility with IEEE 802.3af/at standards.

All PoE Class 4 switch ports are capable of delivering 30W per PoE port, up to the maximum power supply budget.

You can limit the power of a port using the Class Limit feature.



The information in this chapter relates to switches that support PoE. This page appears only if the switch supports PoE.

The following table shows the maximum power per SKU that the switch can provide to all PoE ports combined.

Table 91: PoE Maximum Power per Model

Switch	PoE Support	Maximum Power
HPE Networking Instant On 1930 8G 2SFP+ Class 4 PoE 125W Switch	8 Ports class 4 PoE	125W
HPE Networking Instant On 1930 24G 4SFP Class 4 PoE 195W Switch	24 Ports class 4 PoE	195W
HPE Networking Instant On 1930 24G 4SFP Class 4 PoE 370W Switch	24 Ports class 4 PoE	370W
HPE Networking Instant On 1930 48G 4SFP Class 4 PoE 370W Switch	48 Ports class 4 PoE	370W

PoE Configuration

Use the PoE Configuration Page to view PoE status, consumption history and Port Configuration.

To view this page, click **Power Over Ethernet > PoE Configuration** in the navigation pane.

Device View

The top of the PoE Configuration page shows a graphical representation of the switch front panel. This panel view can show the Activity status, Priority and Class of the ports. Click the radio buttons to show the related information.

Activity

Click the **Activity** radio button to show which ports have the following conditions:

Activity State	Image	Description
Fault		There is a fault in the port activity.
Power Denied		Power is denied for this port.
Sourcing Power		This port is providing power.

Priority

Click the **Priority** radio button to show the priority of the ports on the switch.

- L - this indicates Low priority
- H - this indicates High priority
- C - this indicates Critical priority

The following graphic shows the PoE Switch panel view with the Priorities showing on the ports.

Figure 109: PoE Switch Panel View - Priority



Class

Click the **Class** radio button to show the class of the ports on the switch.

- 0 - this indicates 0.44-12.95W
- 1 - this indicates 0.44-3.84W
- 2 - this indicates 3.84- 6.49W
- 3 - this indicates 6.49-12.95W
- 4 - this indicates 12.95-25.5W

Click a PoE port in this screen to open the **Edit Port PoE Configuration** page.

For more information, see [Switch Panel View](#).

Status

The Status tile displays PoE global information: the total power, actual power consumption, and PoE status.

Figure 110: Status Tile

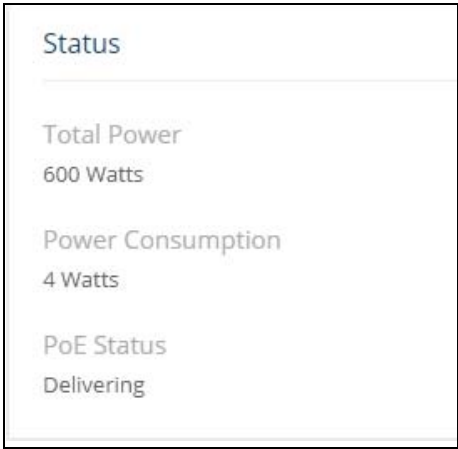


Table 92: Status Fields

Field	Description
Total Power (Watts)	The total power in watts that can be provided by the switch.
Power Consumption (Watts)	The amount of power in watts currently being consumed by connected PoE devices (PD).
PoE Status	<div>The current status of the switch PoE functionality. Possible values are:<ul style="list-style-type: none">Delivering—At least one port on the switch is delivering power to a connected switch, and no port is in Fault state.Idle—The PoE functionality is operational but no ports are delivering power, and no ports have errors.Faulty—one or more ports is not functioning due to a hardware fault or is in the hardware fault-recovery state.Not Functional—PoE is not functional on switch due to a hardware failure.Error—One or more ports is in PoE fault state. this does not include hardware-related fault states.</div>



PoE Fault and Activity status is also indicated through the switch port and PoE LEDs. See [System LEDs](#) for more information.

Consumption History

The Consumption History tile provides information on average PoE consumption on the switch over the last hour, day and week. This information is useful for monitoring PoE trends and behavior.

The consumption history information is saved to the switch non-volatile memory so it is available after switch reboot.

Figure 111: Consumption History Tile

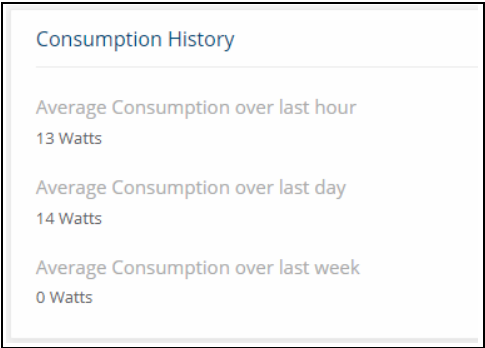


Table 93: Consumption History Fields

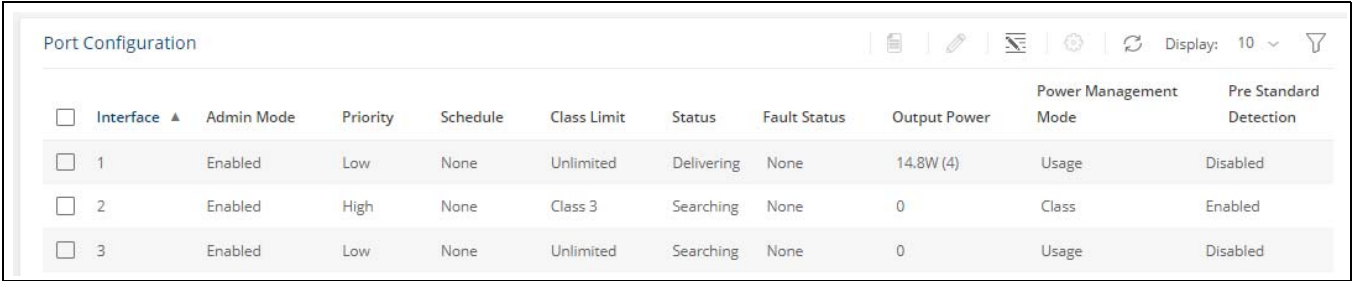
Field	Description
Average Consumption over last hour	The average power consumption by PDs attached to the switch, over the last hour (in units of watts).
Average Consumption over last day	The average power consumption by PDs attached to the switch, over the last day (in units of watts).
Average Consumption over last week	The average power consumption by PDs attached to the switch, over the last week (in units of watts).

Port Configuration

You can use the PoE Port Configuration page to administratively enable or disable PoE on ports and to view and configure the port priority and other settings.

To view this page, click **Power Over Ethernet > PoE Configuration** in the navigation pane.

Figure 112: PoE Port Configuration Tile



The following settings are displayed.

Table 94: PoE Port Configuration Fields

Field	Description
Interface	The port number.
Admin Mode	Indicates whether PoE is administratively enabled or disabled on the port. This feature is enabled by default.
Priority	The priority of the port when allocating available power. Power is delivered to the higher-priority ports when needed before providing it to the lower priority ports. Possible values are Critical, High and Low. Low is the lowest priority and the default for all ports.

Field	Description
Schedule	<p>The scheduled time when source power is available on this port. Options are:</p> <ul style="list-style-type: none"> • None—Source power is available at all times. This is the default selection. • Schedule 1—Source power is available during the configured schedule in Schedule 1. • Schedule 2—Source power is available during the configured schedule in Schedule 2. • Schedule 3—Source power is available during the configured schedule in Schedule 3. <p>You can configure schedules on the Schedule Configuration page in Setup Network.</p>
Class Limit	<p>By default, the power is not limited (ports can deliver up to class 4)</p> <ul style="list-style-type: none"> • The class limit of a port can be set to class 3 or unlimited.
Pre-Standard Detection	<p>Indicates whether Pre-Standard Detection is allowed. The 4-point detection scheme defined in IEEE 802.3 is used by default. If this mechanism fails to detect a connected PD, and pre-standard detection is allowed, then pre-standard detection is used.</p>
Power Management Mode	<p>Select the method by which the PoE controller determines supplied power. Possible values are:</p> <ul style="list-style-type: none"> • Class—The power allocated to each port is reserved and is not available to any other port, even when less than the maximum allocation is being used. • Usage—The power allocated to each port is not reserved. Unused power may be allocated from one port to another as needed, up to the power limit defined for each port. This is the default selection.
Status	<p>The status of the port as a provider of Power over Ethernet. Such devices are referred to as power-sourcing equipment (PSE). Possible values are:</p> <ul style="list-style-type: none"> • Disabled—The operational status of the PSE is disabled. • Delivering Power—The PSE is delivering power. • Fault—The PSE has experienced a fault condition. • Searching—The PSE is transitioning between states. • Recovering—the port is recovering from a previous condition of internal hardware fault.
Output Power	Power consumed on port, in watts.
Fault Status	<p>Indicates the type of fault condition that exists on the port . Possible values are:</p> <ul style="list-style-type: none"> • None - the port is not in fault condition. • Short - a Short fault condition exists on the port. • Overload - a PoE Overload fault condition exists on the port. • Underload - a PoE Underload fault condition exists on the port. • Power Denied - Power on port is denied due to power over-subscription condition on the switch. • Hardware Fault - a general Hardware fault occurred on the switch which prevents power on port • Internal HW Fault - a hardware fault occurred on the interface. • Other - a fault of a type not specified above occurred on the port. <p>NOTE: This field is relevant only if the status of the port is Fault.</p>

Edit Port PoE Configuration

To change PoE settings for a port, select the checkbox associated with it and click **Edit**  . Or, click **Edit All**  to configure all PoE enabled ports at the same time.

Figure 113: Edit Port PoE Configuration Page

Edit Port PoE Configuration

Interface

1

Admin Mode

Schedule

None

Priority

Critical

High

Low

Class Limit

Unlimited

Allow Pre-Standard Detection

Power Management Mode

Usage

Class

CANCEL

APPLY

Click **APPLY** to save any changes for the current boot session. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

PoE Port Details

To view additional PoE configuration information for a port, select the port and click **Details**  .

Figure 114: PoE Port Details Page

 PoE Port Details



Interface

8

Class Limit

Class 3

Assigned Class

3

Measured Class

3

Output Voltage

0 Volts

Output Current

0 mAmps

Negotiated Power

0 Watts

Output Power

0 Watts

Event Counters

Overloads

0

Denials

0

Absences

0

Invalid Signatures

0

CLEAR COUNTERS

CLOSE

Table 95: PoE Port Details Fields

Field	Description
Class Limit	Shows the class limit: <ul style="list-style-type: none">UnlimitedClass 3
Assigned Class	The class of power actually supplied to the powered device. This class may be lower than the measured class because of lack of available power or if the port does not support the measured class.
Measured Class	The class of power requested by the powered device. Possible values are Unknown and Class 0 through Class 4. A higher class value indicates that the switch provides higher power.

Field	Description
Output Voltage	The voltage being applied to the connected switch.
Output Current	The current in milliamps being drawn by the connected switch.
Negotiated Power	Power in watts negotiated between the port and connected switch.
Output Power	Power in watts being drawn by the connected switch.
Event Counters	
Overloads	The number of power overload events detected on the port.
Denials	The number of times that the powered device was denied power.
Absences	The number of times that power was stopped to the powered device, because the powered device was not detected.
Invalid Signatures	The number of that an invalid signature was received. Signatures are the means by which the powered device identifies itself to the PSE. Signatures are generated during powered device detection, classification, or maintenance.



The **Re-activate**  button appears when there is a disabled port due to a hardware failure. Ports that are in hardware fault state may recover automatically from this state, however, in some cases you may need to manually re-activate this port.

To manually re-activate the port, select the row with the hardware failure and click the **Re-activate**  button.

Routing provides a means of transmitting IPv4 packets between subnets on the network. Routing is disabled by default. Static routing means that routes need to be added by the system administrator and are not learned through a routing protocol.

The device supports:

- Up to 32 IPv4 interfaces:
 - An IPv4 address can be configured on VLAN, LAG or Physical interface
 - Single IPv4 address per interface
- Up to 32-IPv4 static routes

Routing configuration is necessary only if the switch is used as a Layer 3 switch that routes packets between subnets. If the switch is used as a Layer 2 switch that handles switching only, it typically connects to an external Layer 3 switch that handles the routing functions; therefore, routing configuration is not required on the Layer 2 switch.

You can use the Routing pages to configure Layer 3 features and capabilities.

Routing Configuration

Use the Routing Configuration page to configure Global features, view and edit Port IP and VLAN IP routing, Static Routing and Route Table, IP Routing Statistics and ICMP Statistics.

To view the Routing Configuration page, click **Routing** > **Routing Configuration** in the navigation pane.

Global Configuration

Use the Global Configuration page to configure global IPv4 routing settings on the switch. These are the global settings for Routing:

Figure 115: Global Configuration Page

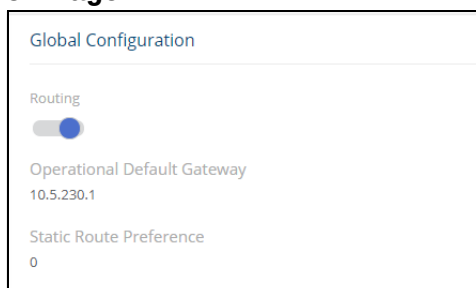


Table 96: Routing Configuration Fields

Field	Description
Routing	The administrative mode of routing on the switch. The options are as follows: <ul style="list-style-type: none"> • Enable – The switch can act as a Layer 3 switch by routing packets between interfaces configured for IP routing. • Disable – The switch acts as a Layer 2 bridge and switches traffic between interfaces. The switch does not perform any internetwork routing.
Operational Default Gateway	The IP address of the default gateway for the switch. If the destination IP address in a packet does not match any routes in the routing table, the packet is sent to the default gateway. The gateway displayed in this field is the next hop on switch with the lowest metric.
Static Route Preference	The default distance (preference) for static routes. Lower route-distance values are preferred when determining the best route. The value configured for Static Route Preference is used when using the CLI to configure a static route and no preference is specified. This field is not configurable and has a value of 1.

Port IP and VLAN IP Tile

To view the Port IP interface information, click the **Port IP** tab.

To view the VLAN IP interface information, click the **VLAN IP** tab.

The Port IP and the VLAN IP tabs show the same fields. These tabs show summary information about the routing configuration for all interfaces.

The following figure shows the Port IP tab.

Figure 116: Port IP Tile

Port IP		VLAN IP						
Interface ▲		Status	IP Address	Subnet Mask	Admin Mode	State	MAC Address	Proxy ARP
☒	1	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:00:44:44:55:89	Disabled
☐	2	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:00:44:44:55:8A	Disabled
☐	3	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:00:44:44:55:8B	Disabled
☐	4	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:00:44:44:55:8C	Disabled
☐	5	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:00:44:44:55:8D	Disabled

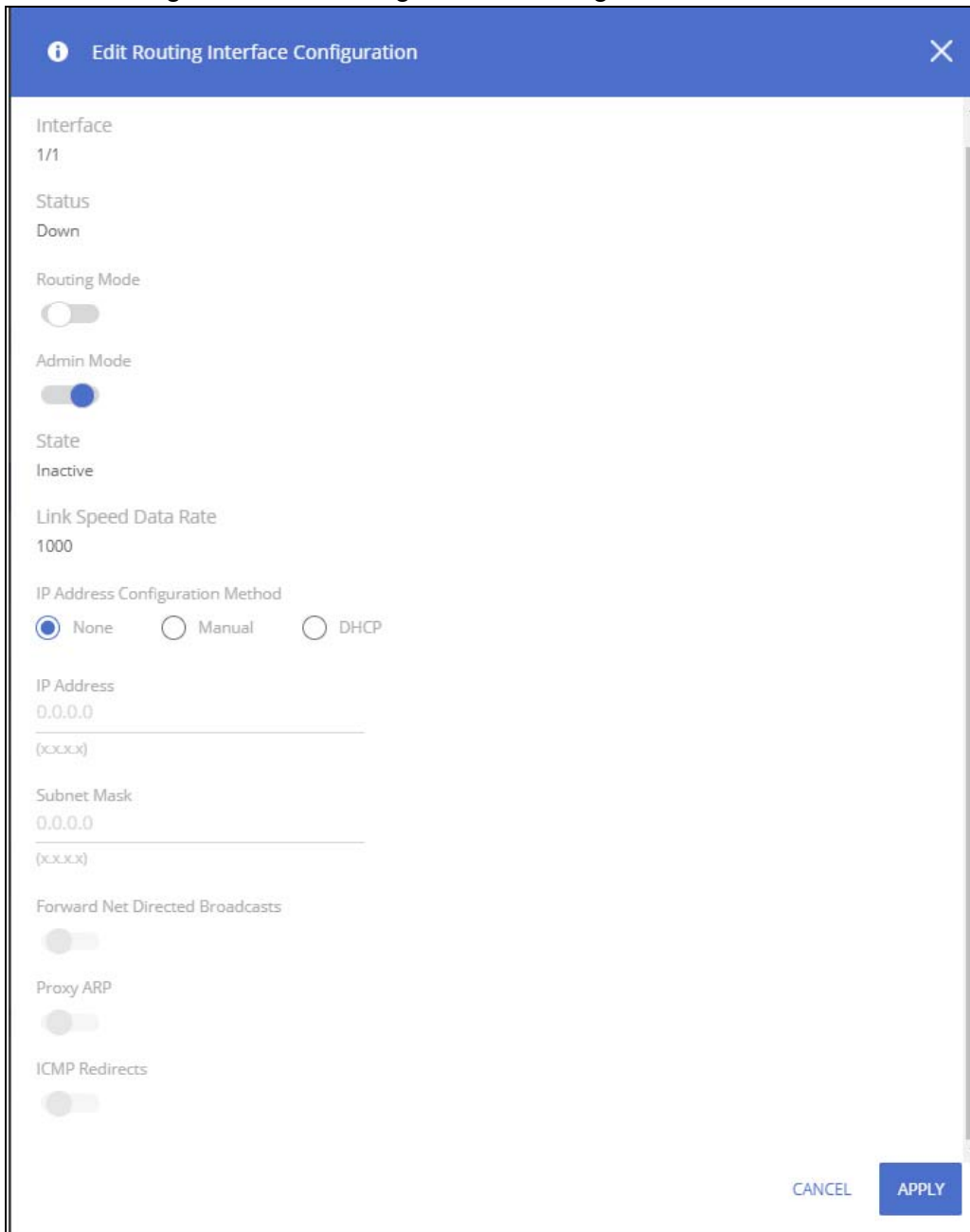
Table 97: Port/VLAN IP Fields

Field	Description
Interface/VLAN ID	The interface associated with the rest of the data in the row. When viewing information about the routing settings for an interface, this field identifies the interface being viewed.
Status	It indicates whether the interface is capable of routing IP packets (Up) or cannot route packets (Down). For the status to be Up, the routing mode and administrative mode for the interface must be enabled. Additionally, the interface must have an IP address and be physically up (active link). NOTE: This field is only relevant to Port IP interfaces.
IP Address	The IP address of the interface.
Subnet Mask	The IP subnet mask for the interface (also known as the network mask or netmask). It defines the portion of the interface's IP address that is used to identify the attached network.

Field	Description
Admin Mode	The administrative mode of the interface, which is either Enabled or Disabled.
State	This field is only available in the Port IP tab. The state of the interface, which is either Active or Inactive. An interface is considered active if the link is up, and the interface is in a forwarding state.
MAC Address	The burned-in physical address used for routing traffic on this interface. The format is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
Proxy ARP	Indicates whether proxy ARP is enabled or disabled on the interface. When proxy ARP is enabled, the interface can respond to an ARP request for a host other than itself. An interface can act as an ARP proxy if it is aware of the destination and can route packets to the intended host, which is on a different subnet than the host that sent the ARP request.

To edit an interface, select the Port IP or VLAN IP in the tile and then click **Edit**  .

Figure 117: Edit Routing Interface Configuration Dialog Box



The dialog box is titled "Edit Routing Interface Configuration" with a close button (X) in the top right corner. It contains the following fields and controls:

- Interface:** 1/1
- Status:** Down
- Routing Mode:** A toggle switch currently turned off.
- Admin Mode:** A toggle switch currently turned on (blue).
- State:** Inactive
- Link Speed Data Rate:** 1000
- IP Address Configuration Method:** Three radio buttons: **None** (selected), Manual, and DHCP.
- IP Address:** A text field containing "0.0.0.0" with a placeholder "(xxxx)" below it.
- Subnet Mask:** A text field containing "0.0.0.0" with a placeholder "(xxxx)" below it.
- Forward Net Directed Broadcasts:** A toggle switch currently turned off.
- Proxy ARP:** A toggle switch currently turned off.
- ICMP Redirects:** A toggle switch currently turned off.

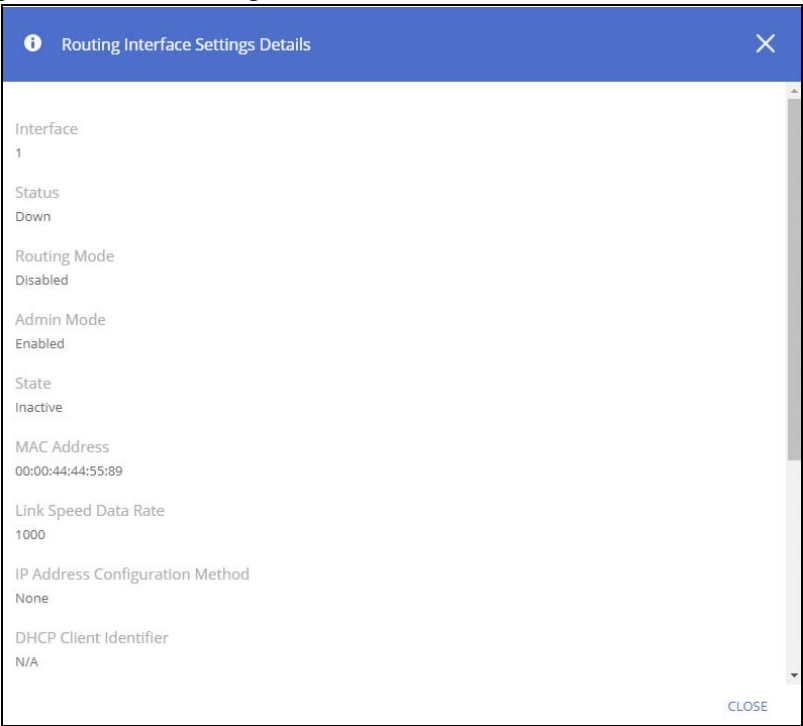
At the bottom right, there are two buttons: "CANCEL" and "APPLY".

Table 98: Edit Routing Interface Configuration Fields

Field	Description
Interface/VLAN ID	The selected interface, or VLAN ID, that is being edited.
Status	Indicates whether the interface is currently capable of routing IP packets (Up) or cannot route packets (Down). For the status to be Up, the routing mode and administrative mode for the interface must be enabled. Additionally, the interface must have an IP address and be physically up (active link). NOTE: For VLAN interfaces, routing mode is always enabled.
Routing Mode	The administrative mode of IP routing on the interface. NOTE: This setting is available only for IP port. for VLAN interfaces this setting is always enabled.
Admin Mode	The administrative mode of the interface. If a port interface is administratively disabled, it cannot forward traffic. If a VLAN interface is administratively disabled the VLAN forwards only L2 traffic.
State	Displays the state of the interface, which is either Active or Inactive. An interface is considered active if the link is up, and the interface is in a forwarding state. This field is not displayed for VLAN ID.
Link Speed Data Rate	Displays the physical link data rate of the interface.
IP Address Configuration Method	The method to use for configuring an IP address on the interface, which can be one of the following: <ul style="list-style-type: none"> None – No address is to be configured. Manual – The address is to be statically configured. When this option is active you can specify the IP address and subnet mask in the available fields. DHCP – The interface will attempt to acquire an IP address from a network DHCP server.
IP Address	The IP address of the interface. This field can be configured only when the selected IP Address Configuration Method is Manual. If the method is DHCP, the interface attempts to lease an IP address from a DHCP server on the network, and the IP address appears in this field (read-only) after it is acquired. If this field displays IP address of 0.0.0.0, the IP Address Configuration Method might be None, or the method might be DHCP and the interface is unable to lease an address.
Subnet Mask	The IP subnet mask for the interface (also known as the network mask or netmask). This field can be configured only when the selected IP Address Configuration Method is Manual.
Forward Net Directed Broadcasts	Determines how the interface handles network-directed broadcast packets. A network-directed broadcast is a broadcast directed to a specific subnet. If this option is activated, network directed broadcasts are forwarded. If this option is clear, network directed broadcasts are dropped. NOTE: This setting is available only if the IP Address Configuration Method is manual.
Proxy ARP	When this option is active, proxy ARP is enabled, and the interface can respond to an ARP request for a host other than itself. An interface can act as an ARP proxy if it is aware of the destination and can route packets to the intended host, which is on a different subnet than the host that sent the ARP request.
ICMP Redirects	When this option is active, the interface is allowed to send ICMP Redirect messages. An ICMP Redirect message notifies a host when a better route to a particular destination is available on the network segment.

To view additional routing configuration information for an interface, select the radio button to the left of the interface and click **Details**  .

Figure 118: Routing Interface Settings Details



The following information describes the fields in the **Details** dialog box that are not displayed on the **Edit Routing Interface Configuration** dialog box.

Table 99: Routing Interface Settings Details Fields

Field	Description
MAC Address	The MAC address of the IP interface.
DHCP Client Identifier	The DHCP Client Identifier (Option 61) is used by DHCP clients to specify their unique identifier. DHCP servers use this value to index their database of address bindings. This value is expected to be unique for all clients in an administrative domain. The Client Identifier string is displayed beside the check box once DHCP is enabled on the port on which the Client identifier option is active. This setting is always enabled for an interface that used DHCP to acquire IP address.

Click **APPLY** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Static Routing/Route Table Tile

To display the Static Routing/Route Table tile, click **Routing > Routing Configuration** in the navigation pane, and scroll down to the **Static Routing/Route Table** tile.

To view the Static Routing information, click the **Static Routing** tab.

To view the Routing Table information, click the **Routing Table** tab.

Static Routing Tab

Use the Static Routing tab to create and display static routes.

Figure 119: Static Routing Tab



Table 100: Static Routing Fields

Field	Description
Network Address	The IP route prefix for the destination.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Next Hop IP Address	The next hop router address to use when forwarding traffic to the destination.
Next Hop Interface	The outgoing interface to use when forwarding traffic to the destination.
Preference	The preferences configured for the added routes.

Adding a Static Route

To add a static route:

- 1. Click **Add**  .

Figure 120: Add Route Page

 Add Route 

Route Type

☐ Default ☒ Static ☐ Static Reject

Network Address

Subnet Mask

Next Hop IP Address

Preference

CANCEL

APPLY

- 2. Enter the Route information:
Next to **Route Type**, select **Default** route, **Static** or **Static Reject** from the menu.

- **Default:** Configures the gateway to remote networks when no other route in the table matches the destination IP subnet of the traffic. Enter the default gateway address in the **Next Hop IP Address** field and optionally change the **Preference** field.
The **Network Address** and **Subnet Mask** fields are grayed out and will be updated with the value of 0.0.0.0 after clicking the **APPLY** button.
- **Static:** Configures the Next Hop for traffic with a matching destination IP subnet. Enter values for **Network Address**, **Subnet Mask**, **Next Hop IP Address**, and **Preference**.
- **Static Reject:** Packets to these destinations will be dropped.



The route type you select determines the fields available on the page.

3. Click **APPLY**.

The new route is added to the **Static Routing/Route Table** tab.

Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

To remove one or more configured routes, select each route to delete and click **Remove** .

Route Table Tab

The route table manager collects routes from multiple sources: static routes and local routes. The route table manager may learn multiple routes to the same destination from multiple sources. The route table displays only the most preferred route to each destination.

To display the Route Table page, click **Routing > Routing Configuration** in the navigation pane, scroll down to the **Static Routing/Route Table** tile and click the **Route Table** tab.

Figure 121: Route Table Tab

Static Routing		Route Table		Display: 10	
Network Address	Subnet Mask	Protocol	Next Hop IP Address	Next Hop Interface	
0.0.0.0	0.0.0.0	Default	10.5.230.1	VLAN 1	
10.5.230.0	255.255.255.128	Local	10.5.230.77	VLAN 1	
« < 1 > »					

Table 101: Route Table Fields

Field	Description
Network Address	The IP route prefix for the destination.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Protocol	This field tells which protocol created the specified route. The possibilities are one of the following: <ul style="list-style-type: none"> • Local • Static • Default

Field	Description
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly-attached network.
Next Hop Interface	The outgoing interface to use when forwarding traffic to the destination. For a static reject route, the next hop is Null.

Click **Refresh**  to update the information on the screen.

IP Routing Statistics/ICMP Statistics Tile

To display the IP Routing/ICMP Statistics tile, click **Routing > Routing Configuration** in the navigation pane, and scroll down to the **IP Routing Statistics/ICMP Statistics** tile.

To view the IP Routing Statistics, click the **IP Routing Statistics** tab.

To view the ICMP Statistics, click the **ICMP Statistics** tab.

IP Routing Statistics Tab

Figure 122: IP Routing Statistics Tab

IP Routing Statistics		ICMP Statistics
IpInReceives	IpInDelivers	IpReasmOKs
74682	63968	0
IpInHdrErrors	IpOutRequests	IpReasmFails
9028	24913	0
IpInAddrErrors	IpOutDiscards	IpFragOKs
10	0	0
IpForwDatagrams	IpOutNoRoutes	IpFragFails
0	4	0
IpInUnknownProtos	IpReasmTimeout	IpFragCreates
0	10	0
IpInDiscards	IpReasmReqds	
0	0	

Table 102: Routing IP Statistics Fields

Field	Description
IpInReceives	The total number of input datagrams received from interfaces, including those received in error.
IpInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

Field	Description
IpInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
IpFowdDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter includes only those packets which were Source-Routed through this entity, and the Source-Route option processing was successful.
IpInUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
IpInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
IpInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
IpOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
IpOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
IpOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this 'no-route' criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
IpReasmTimeout	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
IpReasmReqds	The number of IP fragments received which needed to be reassembled at this entity.
IpReasmOKs	The number of IP datagrams successfully re-assembled.
IpReasmFails	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.
IpFragOKs	The number of IP datagrams that have been successfully fragmented at this entity.
IpFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.
IpFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.

ICMP Statistics Tab

Table 103: ICMP Statistics Fields

Field	Description
IcmpInMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.
IcmpInErrors	The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
IcmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
IcmpInTimeExcds	The number of ICMP Time Exceeded messages received.
IcmpInParmProbs	The number of ICMP Parameter Problem messages received.

Field	Description
IcmpInSrcQuenchs	The number of ICMP Source Quench messages received.
IcmpInRedirects	The number of ICMP Redirect messages received.
IcmpInEchos	The number of ICMP Echo (request) messages received.
IcmpInEchoReps	The number of ICMP Echo Reply messages received.
IcmpInTimestamps	The number of ICMP Timestamp (request) messages received.
IcmpInTimestampReps	The number of ICMP Timestamp Reply messages received.
IcmpInAddrMasks	The number of ICMP Address Mask Request messages received.
IcmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
IcmpOutMsgs	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
IcmpOutErrors	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
IcmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
IcmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
IcmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
IcmpOutSrcQuenchs	The number of ICMP Source Quench messages sent.
IcmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object is always zero, since hosts do not send redirects.
IcmpOutEchos	The number of ICMP Echo (request) messages sent.
IcmpOutEchoReps	The number of ICMP Echo Reply messages sent.
IcmpOutTimestamps	The number of ICMP Timestamp (request) messages.
IcmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
IcmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
IcmpOutAddrMasksReps	The number of ICMP Address Mask Reply messages sent.

DHCP Relay

HPE Networking Instant On 1930 Switch Series switches can be used to relay packets between a DHCP client and server on different subnets. The switch acts as an L3 relay agent and must have an IP interface on the client subnets. If it does not have an IP interface on the server's subnet, it should be able to route traffic toward the server's subnet.

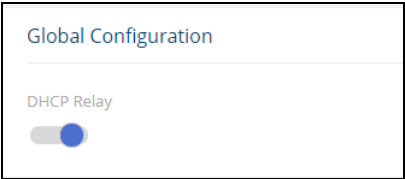
Global Configuration

Use the DHCP Relay Global Configuration page to enable the DHCP relay feature on the switch.

To display the DHCP Relay Global Configuration page, click **Routing > DHCP Relay** in the navigation pane.

If you change the administrative mode of the feature, Click **APPLY** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Figure 123: DHCP Relay Global Configuration Page



Server Configuration

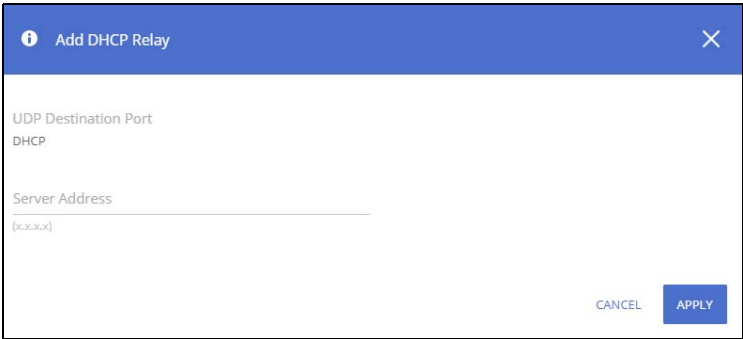
Use the Server Configuration tile view and configure information about DHCP servers where packets should be relayed.

Table 104: Server Configuration Fields

Field	Description
UDP Destination Port	The destination UDP port number of UDP packets to be relayed.
Server Address	The IPv4 address of the server to which packets are relayed for the specific UDP Destination Port.

To add a DHCP server to which packets are relayed, click **Add**  to open the **Add DHCP Relay** dialog box, specify the IP address of the DHCP server, and click **APPLY**.

Figure 124: Add DHCP Relay Dialog Box



To remove one or more configured DHCP servers, select each server to delete and click **Remove**  .

DHCP Relay Interfaces

Use the DHCP Relay Interface page to add, view, or delete the DHCP relay configuration on a selected routing interface.

To display the DHCP Relay Interface page, click **Routing > DHCP Relay** in the navigation pane.



DHCP relay is operational on a VLAN or interface, only if it is enabled for routing. To enable routing on an interface or VLAN, use the Port IP and VLAN tile.

Figure 125: DHCP Relay Interfaces Page

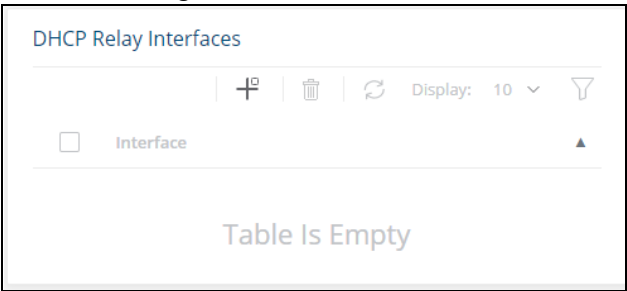


Table 105: DHCP Relay Interface Fields

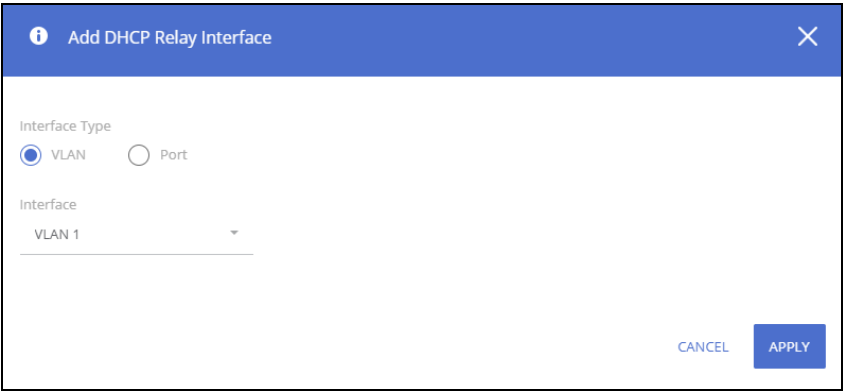
Field	Description
Interface	The routing interface that has the DHCP relay feature configured.

Adding a DHCP Server

To configure an interface or VLAN that can relay DHCP packets to a DHCP server:

- 1. Click **Add** + to open **Add DHCP Relay Interface** dialog box.

Figure 126: Add DHCP Relay Interface Dialog Box



- 2. Select the Interface type: VLAN or Port
- 3. Select the interface from the drop-down menu.
- 4. Click **APPLY**.

Removing a Relay Interface

To remove the DHCP relay capabilities from one or more VLANs or interfaces, select each interface and click **Remove** .

ARP Table

The Address Resolution Protocol (ARP) protocol associates a layer 2 MAC address with a layer 3 IPv4 address. software features both dynamic and manual ARP configuration. With manual ARP configuration, you can add static entries into the ARP table.

If the ARP table is full – new entries are rejected, and an appropriate Syslog message is generated.

The number of supported ARP entries is 509. To dynamically add an ARP entry for a new station, the switch sends an ARP request. Up to 3 requests are sent with an interval of 3 seconds between them.

- If an entry related to a host station times out, it is removed from the table.
- If an entry related to a router or gateway ages out, the switch sends an ARP request for an entry IP address and only if there is no response, the entry is removed from the ARP table.

Global Configuration

Use this page to change the configuration parameters for the ARP Table.

To display the ARP Table Configuration page, click **Routing > ARP Table** in the navigation pane.

Figure 127: Global Configuration

Global Configuration

Age Time

1200

(15 – 21600) seconds

Table 107: Global Configuration Fields

Field	Description
Age Time	The amount of time, in seconds, that a dynamic ARP entry remains in the ARP table before aging out. Valid range is 15-21600. Default is 1200.

Click **APPLY** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

ARP Table Tile

Use the ARP Table page to add an entry to the Address Resolution Protocol (ARP) table and to view existing entries.

To display the ARP Table page, click **Routing > ARP Table** in the navigation pane.

Figure 128: ARP Table Page

ARP Table

Display: 10

<div></div>	IP Address	<div></div>	MAC Address	Interface	Type
<div></div>	10.5.230.1		00:44:44:44:44:44	VLAN 1	Dynamic

1

Table 108: ARP Table Fields

Field	Description
IP Address	The IP address of a network host on a subnet attached to one of the switch's routing interfaces. When adding a static ARP entry, specify the IP address for the entry after you click Add .
MAC Address	The unicast MAC address (hardware address) associated with the network host. When adding a static ARP entry, specify the MAC address to associate with the IP address in the entry.
Interface	The routing interface associated with the ARP entry. The network host is associated with the switch through this interface. When adding a static ARP entry, specify the interface to associate with this entry.
Type	The ARP entry type: <ul style="list-style-type: none">Dynamic – An ARP entry that has been learned by the routerStatic – An ARP entry configured by the user

Adding a Static ARP Entry

To add a static ARP entry:

1. Click **Add** to open the The **Add Static ARP Entry** dialog box opens.

Figure 129: Add Static ARP Entry Page

Add Static ARP Entry

IP Address

(x.x.x.x)

MAC Address

(xxxxxxxxxxxx)

Interface

VLAN 1

CANCEL

APPLY

2. Specify the IP address and its associated MAC address.
3. Specify the interface (VLAN or Port) to associate to this static entry.
4. Click **APPLY**.

Removing an ARP Entry

To delete one or more ARP entries, select each entry to delete and click **Remove**  . Note that ARP entries designated as Local cannot be removed.

Chapter 11

Quality of Service (QoS)

You can use the QoS pages to configure Access Control Lists (ACLs) and Class of Service (CoS).

Access Control Lists

Access Control Lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and above all provide security for the network.

HPE Networking Instant On 1930 Switch Series switches support IPv4 and MAC inbound ACLs. The maximum number of ACLs is 50, with up to 480 ACEs.

To configure an ACL:

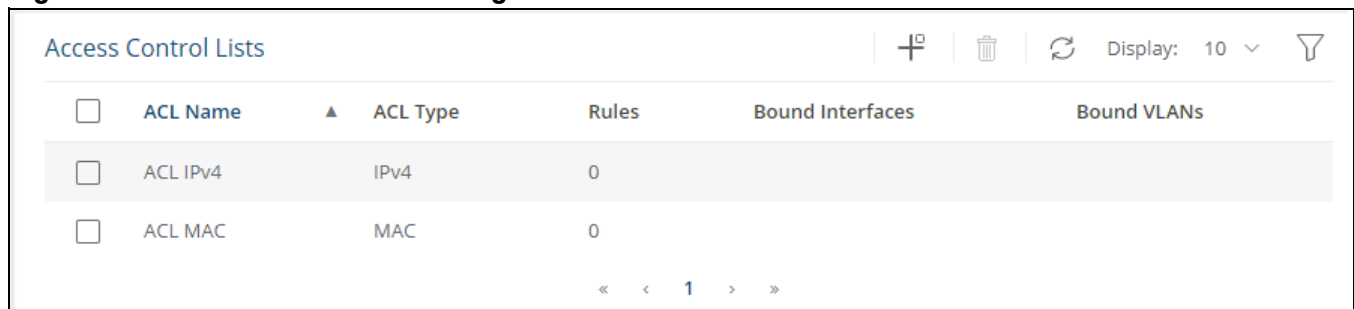
1. Create an IPv4, or MAC-based rule and assign a unique ACL ID. See [Access Control Lists](#) for more information.
2. Define the rules, which can identify protocols, source and destination IP and MAC addresses, and other packet-matching criteria. See [IPv4 ACL Rules Tab](#) for more information.
3. Use the ID number to assign the ACL to a port or to a VLAN interface. See [Interface Configuration Tab](#) for more information.

Access Control Lists

Use the Access Control Lists page to add or remove ACLs, and to view information about the MAC and IP ACLs configured on the switch.

To display the Access Control Lists tile, click **QoS > Access Control Lists** in the navigation pane.

Figure 130: Access Control List Page



☐	ACL Name	ACL Type	Rules	Bound Interfaces	Bound VLANs
☐	ACL IPv4	IPv4	0		
☐	ACL MAC	MAC	0		

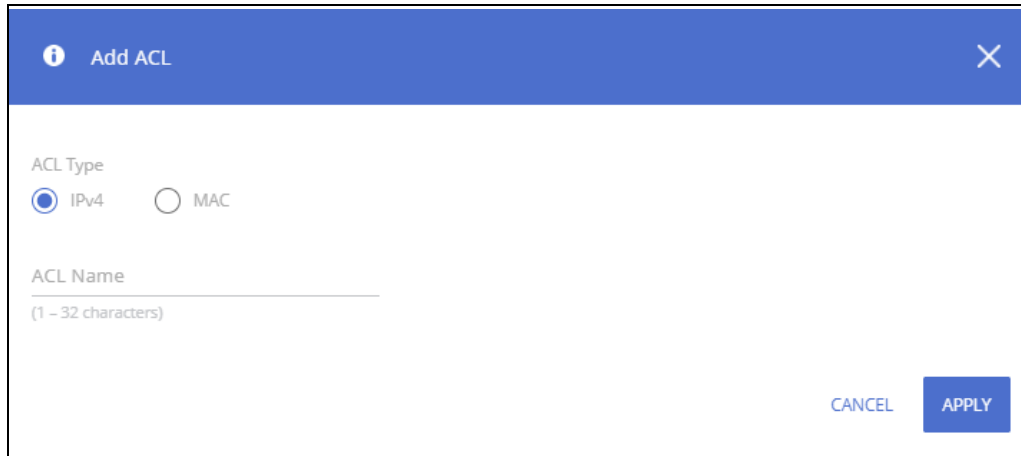
Table 109: Access Control Lists Fields

Field	Description
ACL Name	The name that identifies the ACL, 1-32 characters, case sensitive.
ACL Type	The type of ACL. The ACL type determines the criteria that can be used to match packets. These are the ACL types: <ul style="list-style-type: none">IPv4 – Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of IPv4 packets.MAC – Match criteria can be based on the source and destination MAC addresses, 802.1p user priority, VLAN ID, and EtherType value within Ethernet frames.
Rules	The number of rules currently configured for the ACL.
Bound Interfaces	The interface(s) to which the ACL has been applied.
Bound VLANs	The VLAN(s) to which the ACL has been applied.

Adding an ACL

To add an ACL:

1. Click **Add**  to open the **Add ACL** dialog box.

Figure 131: Add ACL Dialog BoxThe image shows a dialog box titled "Add ACL" with a blue header bar containing an information icon and a close button. The main area is white and contains two radio buttons for "ACL Type": "IPv4" (selected) and "MAC". Below this is a text input field for "ACL Name" with a placeholder "(1 - 32 characters)". At the bottom right, there are two buttons: "CANCEL" and "APPLY".

2. Specify the type of ACL to add.
3. Assign a name.
4. Click **APPLY**.

To delete one or more ACLs, select each entry to delete and click **Remove** .

IPv4 ACL Rules/MAC ACL Rules Tile

The **IPv4 ACL Rules/MAC ACL Rules** tile enables adding and editing rules to ACLs created by users. To view the IPv4 ACL Rules click the **IPv4 ACL Rules** tab.

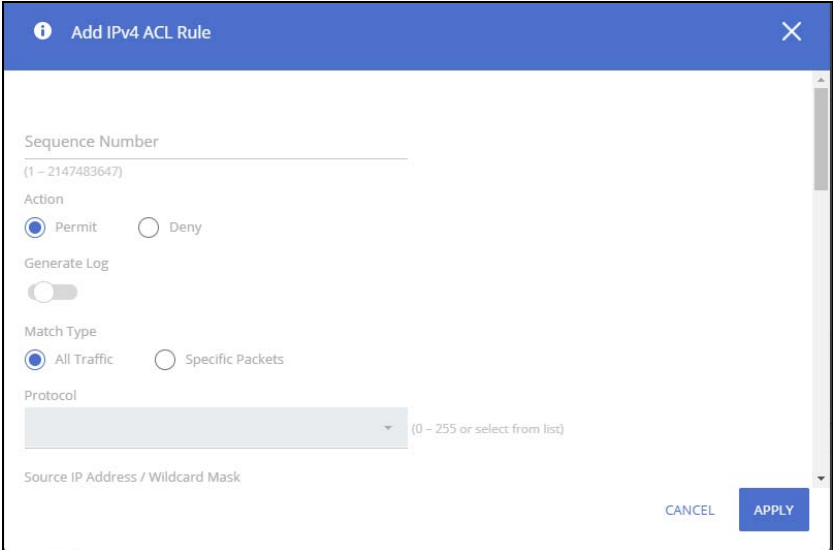
To view the MAC ACL Rules click the **MAC ACL Rules** tab.

IPv4 ACL Rules Tab

To add a rule to an IPv4 ACL:

1. From the **IPv4 ACL Rules** tab, click the drop-down button next to the ACL Name list, select the name of the IPv4 ACL to configure.
2. Click **Add**  to open the **Add IPv4 ACL Rule** dialog box.

Figure 132: Add IPv4 ACL Rule Dialog Box

The dialog box is titled "Add IPv4 ACL Rule" with a close button (X) in the top right corner. It contains several fields and options: "Sequence Number" with a text input field and a range "(1 - 2147483647)" below it; "Action" with two radio buttons, "Permit" (selected) and "Deny"; "Generate Log" with a toggle switch currently turned off; "Match Type" with two radio buttons, "All Traffic" (selected) and "Specific Packets"; "Protocol" with a dropdown menu and a range "(0 - 255 or select from list)" to its right; and "Source IP Address / Wildcard Mask" with a text input field. At the bottom right are "CANCEL" and "APPLY" buttons.

3. Specify a **Sequence Number** to indicate the position of a rule within the ACL.
4. Specify the **Action** for the rule:
 - Permit – The packet or frame is forwarded.
 - Deny – The packet or frame is dropped.
5. To create a log of the ACL, set **Generate Log** to enable. If enabled, the switch sends an informational SYS-LOG message if a receive packet matched the entry.
6. Select the appropriate **Schedule** from the drop-down list.
7. Specify the **Match Conditions** and rule attributes shown in **IPv4 ACL Match Criteria** below.
8. Click **APPLY**.

Table 110: IPv4 ACL Match Criteria

Field	Description
Match Type	<ul style="list-style-type: none">• All Traffic - When this option is selected, all packets will match the rule and will be either permitted or denied. This option is exclusive to all other match criteria, so if All Traffic is selected, no other match criteria can be configured.• Specific Packets - Select this option to configure the match criteria on the ACL.
Protocol	The IANA-assigned protocol number to match within the IP packet. You can also specify one of the keywords provided in the drop-down menu.

Field	Description
Source IP Address / Wildcard Mask	<p>The source IP address in the packet and source IP wildcard mask (in the second field) to compare to the IP address in a packet header. Wildcard masks determines which bits in the IP address are used and which bits are ignored.</p> <p>A wildcard mask of 255.255.255.255 indicates that all bits are ignored.</p> <p>A wildcard of 0.0.0.0 indicates that no bit is ignored.</p> <p>Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A '1' in a bit position of the ACL mask indicates the corresponding bit can be ignored. This field is required when you configure a source IP address.</p>
Source L4 Port	<p>The TCP/UDP source port to match in the packet header. The Source L4 Port and Destination L4 port are configurable only if the protocol is either TCP or UDP.</p> <p>User can select port ID from the range 1-65535, or select predefined protocols. These are predefined protocols available for TCP: BGP, Domain, Echo, FTP, FTP-Data, HTTP, SMTP, Telnet, POP2, or POP3.</p> <p>For UDP protocol: Domain, Echo, NTP, RIP, SNMP, TFTP, Time, or WHO.</p>
Destination IP Address / Wildcard Mask	<p>The destination IP address in the packet and destination IP wildcard mask (in the second field) to compare to the IP address in a packet header. Wildcard masks determines which bits in the IP address are used and which bits are ignored.</p> <p>A wildcard mask of 255.255.255.255 indicates that no bit is important.</p> <p>A wildcard of 0.0.0.0 indicates that all of the bits are important.</p> <p>Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A 1 in a bit position of the ACL mask indicates the corresponding bit can be ignored.</p> <p>This field is required when you configure a destination IP address.</p>
Destination L4 Port	<p>The TCP/UDP destination port to match in the packet header. The Source L4 Port and Destination L4 port are configurable only if the protocol is either TCP or UDP.</p> <p>You can select a port ID from the range 1-65535, or select predefined protocols. These are predefined protocols available for TCP: BGP, Domain, Echo, FTP, FTP-Data, HTTP, SMTP, Telnet, POP2, or POP3.</p> <p>For UDP protocol: Domain, Echo, NTP, RIP, SNMP, TFTP, Time, or WHO.</p>
IGMP Type	IP ACL rule to match on the specified IGMP message type. This option is available only if the protocol is IGMP.
ICMP Type	IP ACL rule to match on the specified ICMP message type. This option is available only if the protocol is ICMP.
ICMP Code	IP ACL rule to match on the specified ICMP message code. This option is available only if the protocol is ICMP.
TCP Flags	<p>IP ACL rule to match on the TCP flags. When a + flag is specified, a match occurs if the flag is set in the TCP header. When a - flag is specified, a match occurs if the flag is not set in the TCP header. These are the available options: FIN, SYN, RST, PSH, ACK, URG.</p> <p>NOTE: This option is available only if the protocol is TCP.</p>
Service Type	<p>The service type to match in the IP header. The options in this menu are alternative ways of specifying a match condition for the same Service Type field in the IP header, but each service type uses a different user notation. After you select the service type, specify the value for the service type in the appropriate field. Only the field associated with the selected service type can be configured. The services types are as follows:</p> <ul style="list-style-type: none"> IP DSCP – Matches the packet IP DiffServ Code Point (DSCP) value to the rule. The DSCP value is defined as the high-order six bits of the Service Type octet in the IP header. IP Precedence – Matches the IP Precedence value to the rule. The IP Precedence field in a packet is defined as the high-order three bits of the Service Type octet in the IP header.

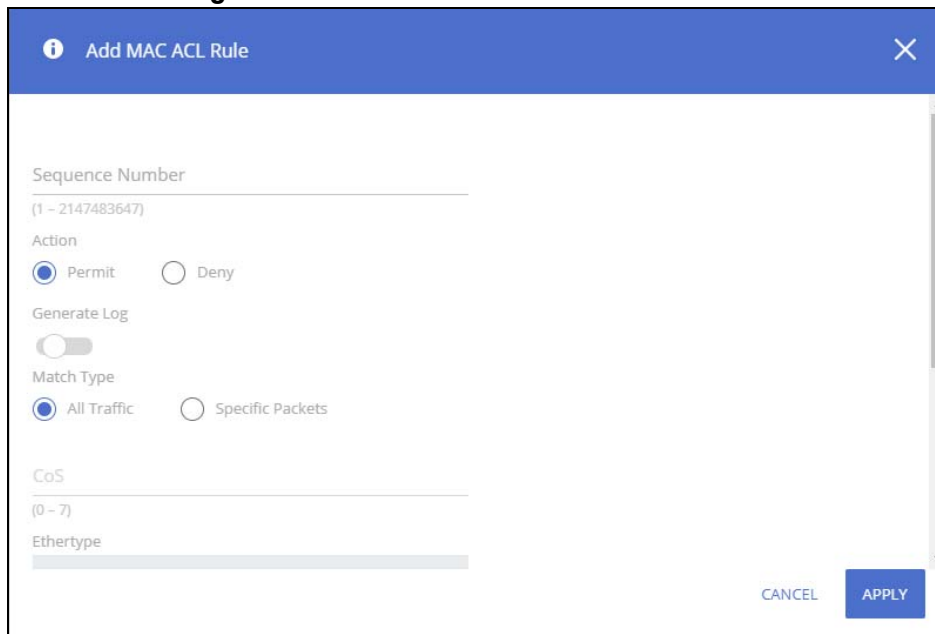
To remove a rule, select it in the list and click **Remove**  .

MAC ACL Rules Tab

To add a rule to an Extended MAC ACL:

1. From the **MAC ACL Rules** tab, click the drop-down button next to the ACL Name list, select the ID of the extended MAC ACL. The ID is up to 32 alphanumeric characters.
2. Click **Add**  to open the **Add MAC ACL Rule** dialog box.

Figure 133: Add MAC ACL Page



The dialog box titled "Add MAC ACL Rule" contains the following fields and options:

- Sequence Number:** A text input field with a range of (1 - 2147483647).
- Action:** Two radio buttons: ☒ Permit and ☐ Deny.
- Generate Log:** A toggle switch currently turned off.
- Match Type:** Two radio buttons: ☒ All Traffic and ☐ Specific Packets.
- CoS:** A text input field with a range of (0 - 7).
- Ethertype:** A text input field.
- Buttons:** CANCEL and APPLY buttons at the bottom right.

3. Specify a **Sequence Number** to indicate the position of a rule within the ACL.
4. Specify the **Action** for the rule:
 - Permit – The packet or frame is forwarded.
 - Deny – The packet or frame is dropped.
5. To create a log of the ACL, set **Generate Log** to enable. If enabled, the switch sends an informational SYS-LOG message if a receive packet matched the entry.
6. Select the appropriate **Schedule** from the drop-down list.
7. Specify the **Match Conditions** and rule attributes shown in **MAC ACL Match Criteria** below.
8. Click **APPLY**.

Table 111: MAC ACL Match Criteria

Field	Description
Match Type	<ul style="list-style-type: none">• All Traffic - When this option is selected, all packets will match the rule and will be either permitted or denied. This option is exclusive to all other match criteria, so if All Traffic is selected, no other match criteria can be configured.• Specific Packets - Select this option to configure the match criteria on the ACL.
CoS	The 802.1p user priority value to match within the Ethernet frame. The valid range is 0-7. The default is none.
Ethertype	The EtherType value to match in an Ethernet frame. Specify the number associated with the EtherType (range 600 – FFFF hex), or specify one of the keywords from the drop-down list.

Field	Description
Source MAC Address / Mask	The MAC address to match to an Ethernet frame's source port MAC address. If desired, enter the MAC Mask associated with the source MAC to match. The MAC address mask specifies which bits in the source MAC to compare against an Ethernet frame. Use F's and zeros in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a zero in a bit position means that the data must equal the value given for that bit. For example, if the MAC address is aa_bb_cc_dd_ee_ff, and the mask is 00_00_ff_ff_ff_ff, all MAC addresses with aa_bb_xx_xx_xx_xx result in a match (where x is any hexadecimal number).
Destination MAC Address / Mask	The MAC address to match to an Ethernet frame's destination port MAC address. If desired, enter the MAC Mask associated with the destination MAC to match. The MAC address mask specifies which bits in the destination MAC to compare against an Ethernet frame. Use F's and zeros in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a zero in a bit position means that the data must equal the value given for that bit. For example, if the MAC address is aa_bb_cc_dd_ee_ff, and the mask is 00_00_ff_ff_ff_ff, all MAC addresses with aa_bb_xx_xx_xx_xx result in a match (where x is any hexadecimal number).
VLAN	The VLAN ID to match within the Ethernet frame.

To remove a rule, select it in the list and click **Remove**  .

Interface and VLAN Configuration Tile

Use this tile to bind an ACL to ports, LAGs or VLANs. Multiple ACLs can be configured on a port/lag interface. In this case a sequence number determines the order in which the ACL is applied to traffic, compared to other ACLs configured on the interface. The ACL with the lowest sequence number is applied first, and the other ACLs are applied in ascending numerical order.

To display the Interface Configuration tab, click the **Interface Configuration** tab.

To display the VLAN Configuration tab, click the **VLAN Configuration** tab.

Interface Configuration Tab

When binding an ACL to an interface the user can specify additional Traffic Rule Attributes per each ACL. The Traffic Rule Attributes will be applied only to ACEs with the permit rule.

Figure 134: Interface Configuration Tab

Interface Configuration		VLAN Configuration						Display: 10		
☐	Interface ▲	Direction	ACL Type	ACL Identifier	Sequence Number	Queue	Flow	Committed Rate	Burst Size	
Table Is Empty										

Table 112: Interface Configuration Fields

Field	Description
Interface	The interface that has an associated ACL.
Direction	Indicates whether the packet is checked against the rules in an ACL when it is received on an interface (Inbound) or after it has been received, routed, and is ready to exit an interface (Outbound). Only the inbound direction is supported.

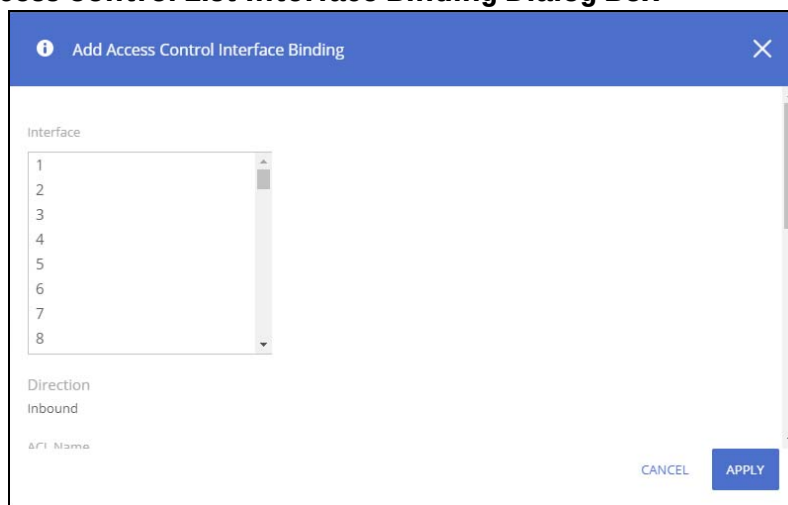
Field	Description
ACL Type	The type of ACL. The ACL type determines the criteria that can be used to match packets. The type also determines which attributes can be applied to matching traffic. IPv4 ACLs classify Layer 3 and Layer 4 IPv4 traffic and MAC ACLs classify Layer 2 traffic. <ul style="list-style-type: none"> IPv4 – Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of IPv4 packets. MAC – Match criteria can be based on the source and destination MAC addresses, 802.1p user priority, VLAN ID, and EtherType value within Ethernet frames.
ACL Identifier	The menu contains the ID for each ACL that exists on the system. Before you add or remove a rule, you must select the ID of the ACL from the menu.
Sequence Number	The number that indicates the position of a rule within the ACL. The rules are displayed based on their position within the ACL, but can also be renumbered. Packets are checked against the rule criteria in order, from the lowest-numbered rule to the highest. When the packet matches the criteria in a rule, it is handled according to the rule action and attributes. If no rule matches a packet, the packet is discarded based on the implicit deny all rule, which is the final rule in every ACL.
Queue	The number (0-3) that identifies the hardware egress queue that handles all packets matching this rule.
Flow	The traffic flow action used: <ul style="list-style-type: none"> Unchanged - the flow is unchanged. Redirect – Allows traffic that matches a rule to be redirected to the selected interface instead of being processed on the original port. The redirect function and mirror function are mutually exclusive. Mirror – Provides the ability to mirror traffic that matches a rule to the selected interface. Mirroring is similar to the redirect function, except that in flow-based mirroring a copy of the permitted traffic is delivered to the mirror interface while the packet itself is forwarded normally through the switch.
Committed Rate	The allowed transmission rate for frames on the interface. Range:100 – 10000000 kbits/sec.
Burst Size	The number of bytes allowed in a temporary traffic burst. Range: 3000 – 19173960 Bytes.

Associating an ACL with an Interface

To apply an ACL to an interface:

1. In the Interface Configuration tab, click **Add**  .
The **Add Access Control List Interface Binding** dialog box appears.

Figure 135: Add Access Control List Interface Binding Dialog Box



2. Select one or more interfaces to associate with the ACL.
To select multiple interfaces, Ctrl + click each interface, or Shift + click a contiguous set of interfaces.

Only Inbound ACLs are supported.

3. Select the ACL name to associate with the interface or interfaces, from the drop-down list.
4. For the sequence number, select between **Auto** or specify a sequence number. If **Auto** is selected, the rule is automatically assigned a sequence number after it is successfully added to the ACL.
5. Under the **Actions** separator, enter values for **Assign Queue**, **Flow Action**, **Interface**, **Committed Rate**, and **Burst Size**. See details on the appropriate values in **Interface Configuration** Fields.
6. Click **APPLY**.

To remove one or more ACL-interface associations, select each entry to delete and click **Remove**  .

VLAN Configuration Tab

Use this page to associate one or more ACLs with one or more VLANs on the switch.

To display the VLAN Configuration tab, click **Quality of Service > Access Control Lists** and scroll down to **Interface/VLAN Configuration** tile, and click on the **VLAN Configuration** tab.

Figure 136: VLAN Configuration Tab



☐	VLAN ID	Direction	ACL Type	ACL Identifier
Table Is Empty				

Table 113: VLAN Configuration Fields

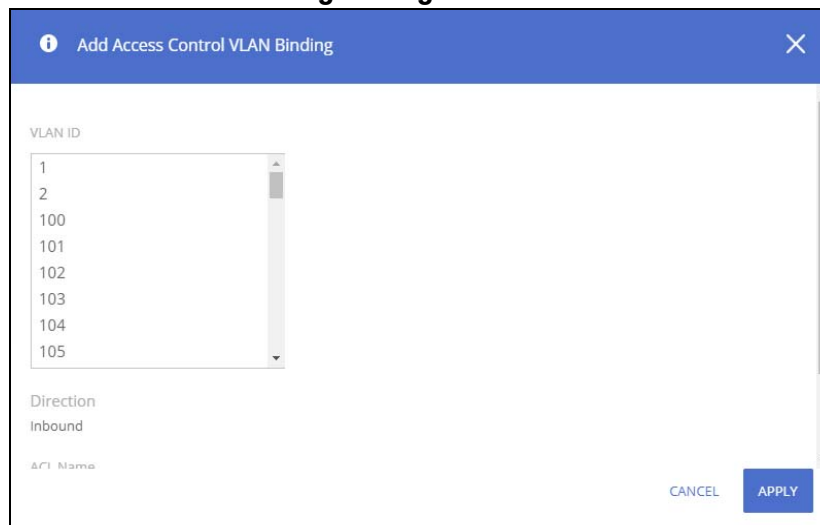
Field	Description
VLAN ID	The ID of the VLAN associated with the rest of the data in the row.
Direction	Indicates whether the packet is checked against the rules in an ACL when it is received on a VLAN (Inbound) or after it has been received, routed, and is ready to exit a VLAN (Outbound). Only the inbound direction is supported.
ACL Type	The type of ACL, which is either IPv4, or MAC.
ACL Identifier	The name that identifies the ACL.

Associating an ACL with a VLAN

To apply an ACL to a VLAN:

1. Click **Add**  .
The **Add Access Control VLAN Binding** page appears.

Figure 137: Access Control VLAN Binding Dialog Box



2. Select one or more VLANs to associate with the ACL.
To select multiple VLANs, Ctrl + click each VLAN, or Shift + click a contiguous set of VLANs.
3. Select the ACL name to associate with the VLAN or VLANs.
4. Click **APPLY**.

To remove one or more ACL-VLAN associations, select each entry to delete and click **Remove**  .

Class of Service

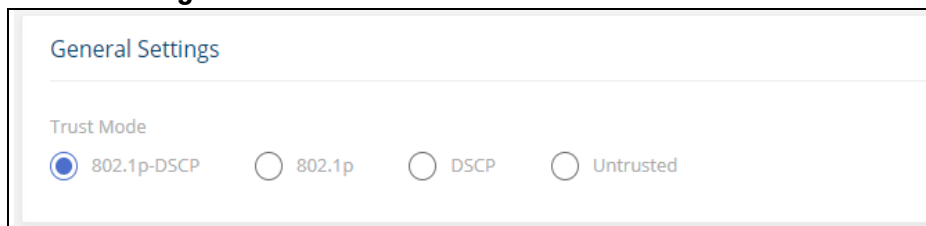
The Class of Service (CoS) queueing feature lets you directly configure certain aspects of switch queueing. This provides the desired QoS behavior for different types of network traffic when the complexities of Diff-Serv are not required. The priority of a packet arriving at an interface can be used to steer the packet to the appropriate outbound CoS queue through a mapping table. CoS queue characteristics that affect queue mapping, such as minimum guaranteed bandwidth, transmission rate shaping, etc., are user-configurable at the queue (or port) level.

To display the tile, click **QoS > Class of Service** in the navigation pane.

General Settings

Use the **General Settings** tile to configure the Trust Mode.

Figure 138: General Settings Tile



Trust mode is a global parameter that defines ingress traffic on all switch interfaces. Select one of the following:

- 802.1p-DSCP - Classifies ingress packets with the packet IP DSCP values for IP packets. For other packet types, ingress traffic is classified with the packet 802.1p priority value encoded within the packet. In the case that a frame is not an IP packet and is untagged, the frame is assigned to the queue associated with the default CoS value defined for the interface in the **Interface Configuration** tile.
- 802.1p – Classifies ingress packets with the packet encoded 802.1 priority value. For untagged packets, the frame is assigned to the queue associated with the default CoS value defined for the interface in the **Interface Configuration** tile.
- DSCP – Classifies ingress packets with the packet IP DSCP value. If the frame is not an IP frame it is assigned to the queue associated with CoS value 0.
- Untrusted – The interface ignores any priority designations encoded in incoming packets. Frames are assigned to the queue associated with CoS 0.

Click **APPLY** to update the configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

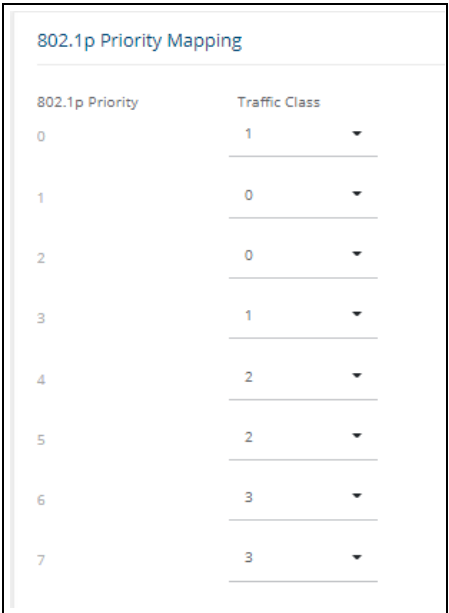
802.1p Priority Mapping

The IEEE 802.1p feature allows traffic prioritization at the MAC level. The switch can prioritize traffic based on the 802.1p tag attached to the L2 frame. Each port on the switch has multiple queues to give preference to certain packets over others based on the Class of Service (CoS) criteria you specify. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets get held in the queue until the scheduler authorizes the queue for transmission.

Use the 802.1p Priority Mapping page to assign 802.1p priority values to various traffic classes. The setting is applied to all interfaces on the switch.

To display the tile, click **QoS > Class of Service** in the navigation pane.

Figure 139: 802.1p Priority Mapping Tile



802.1p Priority	Traffic Class
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Table 114: 802.1p Priority Mapping Configuration Fields

Field	Description
802.1p Priority	The 802.1p priority value to be mapped.
Traffic Class	The internal traffic class to which the corresponding 802.1p priority value is mapped. The default value for each 802.1p priority level is displayed for reference.

Configuring 802.1p CoS Mapping

To configure the 802.1p mapping for one or more interfaces:

1. Select the 802.1p Priority Mapping value to configure and select the traffic class to map to the 802.1p priority value for the interface from the drop-down button.
2. Repeat for any other 802.1p Priority Mapping you wish to configure.
3. Click **APPLY** to update the switch configuration.

Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Queue Configuration

Use the **Queue Configuration** page to define what a particular queue does by configuring switch egress queues. User-configurable parameters control the amount of bandwidth used by the queue, the queue depth during times of congestion, and the scheduling of packet transmission from the set of all queues on a port.

To display the Queue Configuration tile, click **Quality of Service > Class of Service**.

Figure 140: Queue Configuration Tile

Queue Configuration				
Queue	Scheduler Type		WRR Weight (1 - 255)	WRR Percentage
0	☒ WRR	☐ Strict Priority	2	40.00 %
1	☒ WRR	☐ Strict Priority	3	60.00 %
2	☐ WRR	☒ Strict Priority	1	
3	☐ WRR	☒ Strict Priority	1	

Table 115: Queue Configuration Fields

Field	Description
Queue	The queue to be configured.

Field	Description
Schedule Type	Select the type of queue processing per-queue. This enables creating the desired service characteristics for different types of traffic. <ul style="list-style-type: none"> WRR: Weighted round robin associates a weight to each queue. Strict Priority: Strict priority services traffic with the highest priority on a queue first.
WRR Weight	The weight assigned to queues that are configured to the Weighted Round Robin Scheduler Type. The valid range is 1-255. The default is according to the queue.
WRR Percentage	Displays the calculated percentage of traffic for this queue compare to all other queues that are set to WRR schedule. The ratio for each queue is defined as the queue weight divided by the sum of all queue weights (the normalized weight). This sets the bandwidth allocation of each queue. All queues participate in the WRR, excluding the expedite queues, whose corresponding weight is not used in the ratio calculation.

Click **APPLY** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

DSCP CoS Mapping

Use the DSCP CoS Mapping tile to map an IP DSCP value to an internal traffic class.

To display the DSCP CoS Mapping tile, click **QoS > Class of Service** in the navigation pane, and scroll down to the **DSCP CoS Mapping** tile.

Figure 141: DSCP CoS Mapping Tile

DSCP CoS Mapping							
IP DSCP	Traffic Class	IP DSCP	Traffic Class	IP DSCP	Traffic Class	IP DSCP	Traffic Class
0 - be/cs0	☐ 0 ☒ 1 ☐ 2 ☐ 3	16 - cs2	☐ 0 ☒ 1 ☐ 2 ☐ 3	32 - cs4	☐ 0 ☐ 1 ☐ 2 ☒ 3	48 - cs6	☒ 0 ☐ 1 ☐ 2 ☐ 3
1	☐ 0 ☒ 1 ☐ 2 ☐ 3	17	☐ 0 ☒ 1 ☐ 2 ☐ 3	33	☐ 0 ☐ 1 ☐ 2 ☒ 3	49	☒ 0 ☐ 1 ☐ 2 ☐ 3
2	☐ 0 ☒ 1 ☐ 2 ☐ 3	18 - af21	☐ 0 ☒ 1 ☐ 2 ☐ 3	34 - af41	☐ 0 ☐ 1 ☐ 2 ☒ 3	50	☒ 0 ☐ 1 ☐ 2 ☐ 3
3	☐ 0 ☒ 1 ☐ 2 ☐ 3	19	☐ 0 ☒ 1 ☐ 2 ☐ 3	35	☐ 0 ☐ 1 ☐ 2 ☒ 3	51	☒ 0 ☐ 1 ☐ 2 ☐ 3
4	☐ 0 ☒ 1 ☐ 2 ☐ 3	20 - af22	☐ 0 ☒ 1 ☐ 2 ☐ 3	36 - af42	☐ 0 ☐ 1 ☐ 2 ☒ 3	52	☒ 0 ☐ 1 ☐ 2 ☐ 3
5	☐ 0 ☒ 1 ☐ 2 ☐ 3	21	☐ 0 ☒ 1 ☐ 2 ☐ 3	37	☐ 0 ☐ 1 ☐ 2 ☒ 3	53	☒ 0 ☐ 1 ☐ 2 ☐ 3
6	☐ 0 ☒ 1 ☐ 2 ☐ 3	22 - af23	☐ 0 ☒ 1 ☐ 2 ☐ 3	38 - af43	☐ 0 ☐ 1 ☐ 2 ☒ 3	54	☒ 0 ☐ 1 ☐ 2 ☐ 3
7	☐ 0 ☒ 1 ☐ 2 ☐ 3	23	☐ 0 ☒ 1 ☐ 2 ☐ 3	39	☐ 0 ☐ 1 ☐ 2 ☒ 3	55	☒ 0 ☐ 1 ☐ 2 ☐ 3
8 - cs1	☒ 0 ☐ 1 ☐ 2 ☐ 3	24 - cs3	☐ 0 ☐ 1 ☒ 2 ☐ 3	40 - cs5	☐ 0 ☐ 1 ☐ 2 ☒ 3	56 - cs7	☒ 0 ☐ 1 ☐ 2 ☐ 3
9	☒ 0 ☐ 1 ☐ 2 ☐ 3	25	☐ 0 ☐ 1 ☒ 2 ☐ 3	41	☐ 0 ☐ 1 ☐ 2 ☒ 3	57	☒ 0 ☐ 1 ☐ 2 ☐ 3
10 - af11	☒ 0 ☐ 1 ☐ 2 ☐ 3	26 - af31	☐ 0 ☐ 1 ☒ 2 ☐ 3	42	☐ 0 ☐ 1 ☐ 2 ☒ 3	58	☒ 0 ☐ 1 ☐ 2 ☐ 3
11	☒ 0 ☐ 1 ☐ 2 ☐ 3	27	☐ 0 ☐ 1 ☒ 2 ☐ 3	43	☐ 0 ☐ 1 ☐ 2 ☒ 3	59	☒ 0 ☐ 1 ☐ 2 ☐ 3
12 - af12	☒ 0 ☐ 1 ☐ 2 ☐ 3	28 - af32	☐ 0 ☐ 1 ☒ 2 ☐ 3	44	☐ 0 ☐ 1 ☐ 2 ☒ 3	60	☒ 0 ☐ 1 ☐ 2 ☐ 3
13	☒ 0 ☐ 1 ☐ 2 ☐ 3	29	☐ 0 ☐ 1 ☒ 2 ☐ 3	45	☐ 0 ☐ 1 ☐ 2 ☒ 3	61	☒ 0 ☐ 1 ☐ 2 ☐ 3

Table 116: DSCP CoS Mapping Configuration Fields

Field	Description
IP DSCP	Lists the IP DSCP values to which you can map an internal traffic class. The values range from 0-63.
Traffic Class	The traffic class is the hardware queue for a port. Higher traffic class values indicate a higher queue position. Before traffic in a lower queue is sent, it must wait for traffic in higher queues to be sent. Valid range is 0 to 7. The page displays the default values per each IP DSCP.

Click **APPLY** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Interface CoS Configuration

Use the **Interface CoS Configuration** page to configure the Default CoS and apply an interface shaping rate to all ports or to a specific port.

To display the **Interface Configuration** tile, click **QoS > Class of Service** in the navigation pane, and scroll down to the tile.

Figure 142: Interface CoS Configuration Tile

☐ Interface	▲ Default 802.1p Priority	Shaping Rate
☐ 1	0	
☐ 2	0	
☐ 3	0	
☐ 4	0	
☐ 5	0	
☐ 6	0	

Table 117: Interface CoS Configuration Fields

Field	Description
Interface	Selects the CoS configurable interface to be affected by the Interface Shaping Rate.
Default 802.1p Priority	Sets the default CoS for the interface. This is the default CoS value used for Global trust mode 802.1p, or 802.1p-DSCP.
Shaping Rate	Sets the limit on how much traffic can leave a port. The limit on maximum transmission bandwidth has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bound to the interface. Possible values for the rate: 64 – 10,000,000 Kbits/Sec.

Configuring the CoS on an Interface

To configure the CoS for all the interfaces, click **Edit All** .

To configure the CoS for one or more interfaces:

1. Select each interface to configure and click **Edit** . If you select multiple interfaces, or if you use click **Edit All** , the same settings are applied to all selected interfaces. The **Edit CoS Configuration** dialog box appears.

Figure 143: Edit CoS Configuration Dialog Bo

Interface
1

Default CoS
0

(0 - 7)

CANCEL APPLY

2. Specify the Default 802.1p Priority value, and the shaping rate for all interfaces identified in the Interface field(s).
3. Click **APPLY** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration** .

Queue Statistics

Use the **Queue Statistics** tile to get information on the Queues.

To display the **Queue Statistics** tile, click **QoS > Class of Service** in the navigation pane, and scroll down to the tile.

Figure 144: Queue Statistics Tile

☐	Interface ▲	Queue	Transmitted Packets	Tail Dropped Packets	Transmitted Bytes	Tail Dropped Bytes
☐	1	0	0	0	0	0
☐	1	1	0	0	0	0
☐	1	2	0	0	0	0
☐	1	3	0	0	0	0
☐	2	0	0	0	0	0
☐	2	1	0	0	0	0

Table 118: Queue Statistics Fields

Field	Description
Interface	The interface identifier.
Queue	The specific queue to which the information relates.
Transmitted Packets	The number of packets that were transmitted on this queue.
Tail Dropped Packets	The number of packets that were tail dropped on this queue.
Transmitted Bytes	The number of bytes that were transmitted on this queue.
Tail Dropped Bytes	The number of bytes that were tail dropped on this queue.

Select an interface and click **Clear**  to clear statistics from the Queues that are associated with the selected interface.

The HPE Networking Instant On 1930 Switch Series series switch software includes a robust set of built-in security features to secure access to the switch management interface and to protect the network.

RADIUS Configuration

Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. The HPE Networking Instant On 1930 Switch Series switch includes a RADIUS client that can contact one or more RADIUS servers for various Authentication and Accounting (AAA) services. The RADIUS server maintains a centralized database that contains per-user information.

The switch can connect to up to 4 RADIUS servers. At each given time only 1 of these RADIUS servers is used for both Authentication and Authorization. The switch will send the RADIUS packets to the RADIUS server with the highest priority that is not in “dead time” period.

A server is placed in a “dead time” period if it did not respond to a switch request for “Max number of retransmits” The dead time is 2000 minutes. If a server is placed in dead time the switch will send the RADIUS frames to the RADIUS server with next highest priority. If the dead time expired, the switch will try once again to send frames to the RADIUS server with higher priority.

RADIUS as a Device Management Authenticator

By default, the user accounts configured on the switch are used for device Management Authentication. However, the RADIUS server can be configured as the first device management authenticator. In this case the user accounts are used as backup in case the configured RADIUS server is not reachable.

When configured as a device management authenticator, the RADIUS server receives the user credentials from the switch and looks up the entry in the RADIUS user database. The RADIUS server can reply with one of the following responses:

- Reject – user credentials do not match an entry in RADIUS Database. User is denied access to device management.
- Accept + RADIUS service-type attribute is set to 6 (Administrative) – user is granted access with read/write permission.
- Accept + RADIUS service-type attribute is set to 7 (NAS Prompt) – user is granted access with read only permission.

Global Configuration

Use the Global Configuration page to configure global settings for the Remote Authentication Dial-In User Service (RADIUS) feature and to configure one or more RADIUS servers for the switch to contact.

To display the Global Configuration tile, click **Security > RADIUS Configuration** in the navigation pane.

Figure 145: Global Configuration Tile

Global Configuration

802.1x Authentication Mode

802.1x Accounting Mode

Max Number of Retransmits

3

(1 – 15)

Timeout Duration

3

(1 – 30) Seconds

RADIUS Management Authentication

Table 119: Global Configuration Fields

Field	Description
802.1x Authentication Mode	<p>Specifies whether the IEEE 802.1x authentication mode on the switch relies on RADIUS services for 802.1x supplicant authentication.</p> <p>When this setting is selected, and port-based authentication is enabled for the switch, RADIUS will be used for the 802.1x authentication process. Specifically, the credentials presented by the authenticating station (the 802.1x supplicant) are sent to the configured RADIUS server(s) for verification.</p>
802.1x Accounting Mode	<p>Specifies whether the IEEE 802.1X accounting mode on the switch is enabled or disabled.</p> <p>When this setting is selected, RADIUS is used for session accounting. Specifically, an accounting event is sent to the configured RADIUS server(s) at the start and end of each 802.1x session.</p>
Max Number of Retransmits	<p>The maximum number of times the RADIUS client on the switch will retransmit a request packet to a configured RADIUS server after a response is not received.</p> <p>If multiple RADIUS servers are configured, the max retransmit value will be exhausted on the first server before the next server is attempted.</p> <p>A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS server equals the sum of (retransmit × timeout) for all configured servers.</p> <p>If the RADIUS request was generated by a user login attempt, all user interfaces are blocked until the RADIUS application returns a response.</p>
Timeout Duration	<p>The number of seconds the RADIUS client waits for a response from the RADIUS server.</p> <p>Consideration to maximum delay time should be given when configuring RADIUS timeout and RADIUS max retransmit values.</p>
RADIUS Management Authentication	<p>Specifies whether the RADIUS Management Authentication mode on the switch is enabled or disabled.</p> <p>When this setting is selected, the RADIUS server is used as the first source for device management authentication. In this case, the user account database is the backup authenticator.</p>

Click **APPLY** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Radius Server Configuration

Figure 146: RADIUS Server Configuration Tile

RADIUS Server Configuration

Current IP Address Authentication Port Accounting Port Server Priority

Table Is Empty

Table 120: RADIUS Server Configuration Fields

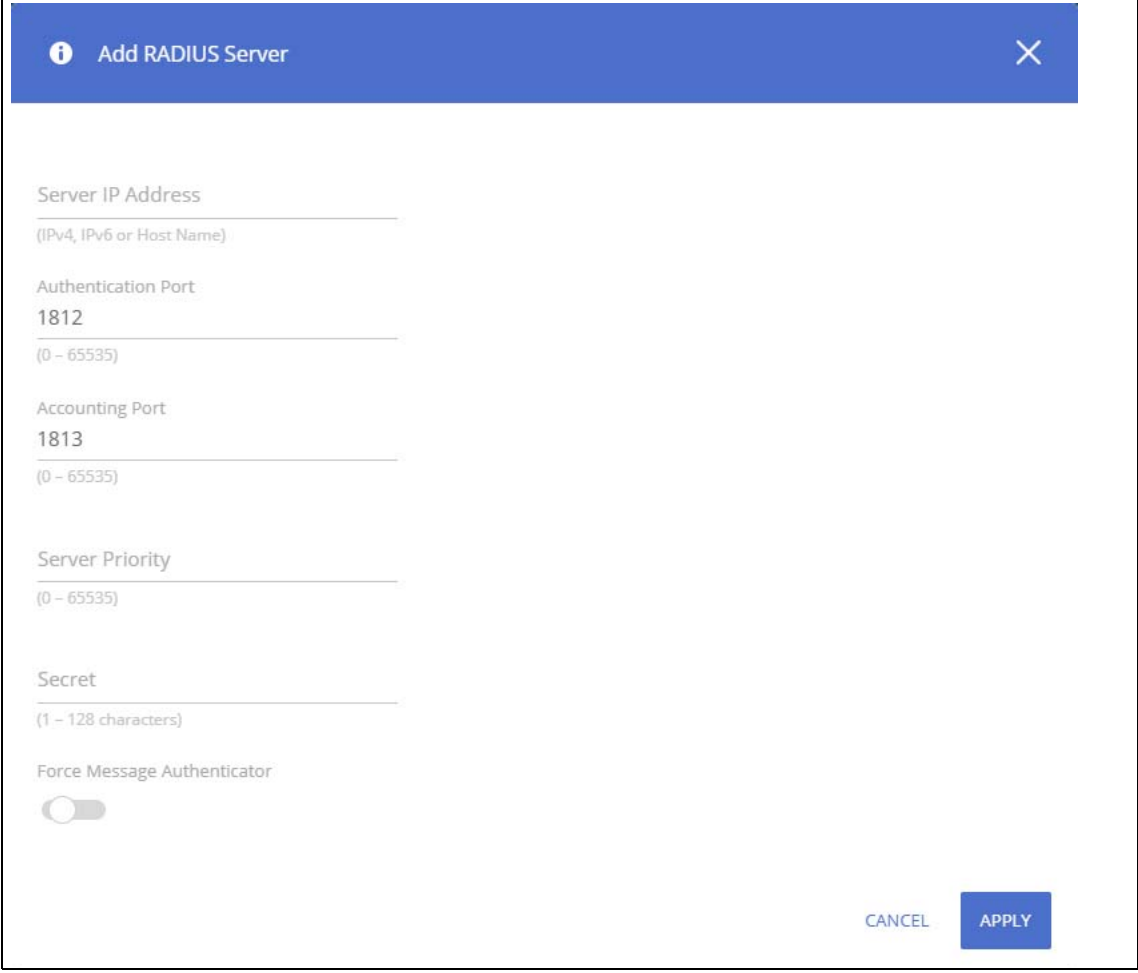
Field	Description
Current	Identifies whether the configured RADIUS server is the current server for the authentication server group. <ul style="list-style-type: none">• True—The server is the current server for the authentication.• False—The server is not the current server for authentication. When the switch sends a RADIUS request to the RADIUS server, the request is directed to the server selected as the current server. Initially the server with the highest priority (lowest number value in priority field) is selected as the current server. If the server with the highest priority fails, one of the other servers becomes the current server.
IP Address	The IP address of the RADIUS server. Can be one of the following: <ul style="list-style-type: none">• IPv4 address• IPv6 global address, in the format of X:X:X::X• Hostname - specify the server hostname
AuthenticationPort	Identifies the authentication port the server uses for handling RADIUS authentication requests. The port is a UDP port.
Accounting Port	Identifies the accounting port the server uses for handling RADIUS accounting packets. The port is a UDP port.
Server Priority	Displays the RADIUS server priority. Lower value means server has a higher priority. The switch will use the RADIUS server with highest priority that is not in dead time. Range: 0-65535

Adding a RADIUS Server

To add a RADIUS server to the switch configuration:

1. Click **Add**  . The **Add RADIUS Server** dialog box appears.

Figure 147: Add RADIUS Server Dialog Box

The image shows a dialog box titled "Add RADIUS Server" with a blue header bar containing an information icon and a close button. The main area is white and contains several input fields: "Server IP Address" with a placeholder "(IPv4, IPv6 or Host Name)", "Authentication Port" with the value "1812" and a range "(0 - 65535)", "Accounting Port" with the value "1813" and a range "(0 - 65535)", "Server Priority" with a range "(0 - 65535)", and "Secret" with a range "(1 - 128 characters)". At the bottom left is a "Force Message Authenticator" toggle switch, which is currently turned off. At the bottom right are two buttons: "CANCEL" and "APPLY".

Add RADIUS Server

Server IP Address
(IPv4, IPv6 or Host Name)

Authentication Port
1812
(0 - 65535)

Accounting Port
1813
(0 - 65535)

Server Priority
(0 - 65535)

Secret
(1 - 128 characters)

Force Message Authenticator
☐

CANCEL APPLY

2. Specify the required information about the RADIUS server.
3. Enter the Secret (1-128 chars) - This is the shared secret text string used for authenticating and encrypting all RADIUS communications between the RADIUS client on the switch and the RADIUS server. The secret specified in this field must match the shared secret configured on the RADIUS server.
4. Optionally, set the **Force Message Authenticator**. Use this setting to define that all types of RADIUS responses from the specified RADIUS server must include the Message-Authenticator attribute (RADIUS attribute 80).
 - If this setting is enabled, any type of RADIUS response that does not include the Message-Authenticator attribute will be silently discarded and the event will be logged.
 - If this setting is disabled, then RADIUS responses that do not include this attribute will be discarded only if they are part of an RADIUS exchange using EAP authentication.
 - By default, this setting is disabled.
5. Click **APPLY** to update the switch configuration.
Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Changing RADIUS Server Settings

To change settings for an existing RADIUS server:

1. Select the RADIUS server to configure.

2. Click **Edit**  .

The **Edit RADIUS Server** page appears.

3. Update the RADIUS server information as needed. The IP address of an existing RADIUS server cannot be changed.
4. Click **APPLY** to update the switch configuration.
Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

To delete one or more RADIUS servers, select each entry to delete and click **Remove**  .

Port Access Control

In port-based authentication mode, when 802.1X is enabled globally and on the port, successful authentication of any one supplicant attached to the port results in all users being able to use the port without restrictions. At any given time, only one supplicant is allowed to attempt authentication on a port in this mode. Ports in this mode are under bidirectional control. This is the default authentication mode.

The 802.1X network has three components:

- **Authenticators:** Specifies the port that is authenticated before permitting network access.
- **Supplicants:** Specifies host connected to the authenticated port requesting access to the network services.
- **Authentication Server:** Specifies the external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the user is authorized to access network services.

Global Configuration

Use this tile to configure the global Port Access Control settings on the switch. The port-based access control feature uses IEEE 802.1X to enable the authentication of system users through a RADIUS server. Only authenticated and approved network users can transmit and receive data. Supplicants (clients connected to authenticated ports that request access to the network) are authenticated using the Extensible Authentication Protocol (EAP). Also supported are PEAP, EAP-TTLS, and EAP-TLS.

To display the Global Configuration tile, click **Security > Port Access Control** in the navigation pane.

Figure 148: Global Configuration Tile

Global Configuration

Admin Mode

EAPOL Flood Mode

Guest VLAN

Guest VLAN ID

Guest VLAN Timeout

Immediate

(30 – 180) Seconds

Table 121: Global Configuration Fields

Field	Description
Admin Mode	Select Enable or Disable 802.1x mode on the switch. The default is Disable. This feature permits port-based authentication on the switch.
EAPOL Flood Mode	The administrative mode of the Extensible Authentication Protocol (EAP) over LAN (EAPOL) flood support on the switch If flood mode is enabled, then the switch will bridge 802.1x PDUs received on switch interfaces. In flood mode the switch filters (drops) such PDUs. The default setting is disable. EAPOL Flood Mode can be enabled when Admin Mode and Monitor Mode are disabled.
Guest VLAN	Displays the admin mode of 802.1x guest VLAN. if enabled - guest VLAN can be enabled on ports using the guest VLAN ID. Default setting is disable.
Guest VLAN ID	The VLAN ID for the guest VLAN. The guest VLAN allows the port to provide a distinguished service to unauthenticated users. This feature provides a mechanism to allow users access to hosts on the guest VLAN. NOTE: this field can be configured only if guest VLAN admin mode is set to enable.
Guest VLAN Timeout	Set Immediate or the number of second for the guest VLAN timeout. The Guest VLAN timeout specifies the time delay in seconds between enabling 802.1X (or port up) and adding the port to the guest VLAN. Set Immediate to apply the guest VLAN immediately.

Click **APPLY** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.



The Guest VLAN needs to be enabled on the required ports (in addition to configuring it globally). An IP address can be configured on the guest VLAN. However this IP interface will not provide the unauthenticated supplicants the ability to manage the device and will not provide them with routing capabilities.

MAC Authentication Settings

Use this tile to configure the MAC authentication settings. The MAC authentication settings enable you to customize the format in which MAC authentication requests are sent to the RADIUS server.

To display the Global Configuration tile, click **Security > Port Access Control** in the navigation pane.

Figure 149: MAC Authentication Settings Tile

MAC Authentication Settings

MAC Authentication Type

☒ EAP-MD5 ☐ PAP

Username Group Size

☐ 1 ☐ 2 ☐ 4 ☒ 12

Username Delimiter

☒ - ☐ : ☐ .

Username Casing

☐ Uppercase ☒ Lowercase

Password

☒ Use username ☐ (1 - 32 characters)

Table 122: MAC Authentication Fields

Field	Description
MAC Authentication Type	Select EAP-MD5 or PAP.
Username Group Size	The number of characters between each delimiter. Available values are 1, 2 (the default) 4 and 12 (which indicates no delimiter).
Username Delimiter	Select the delimiter to use in username. Supported values are "-" (Hyphen), ":" (Colon) and . (period). The default is colon (":")
Username Casing	Select Uppercase or Lowercase for the letters a-f of the MAC address. Default is Lowercase.
Password	Select Use username to use the MAC Authentication username (in its defined format) as the password. To use a different password, select the other radio button and enter the password. This password will be used for all MAC Authentication supplicants.

Click **APPLY** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Port Configuration

To display the Port Configuration tile, click **Security > Port Access Control** in the navigation pane, and scroll down to the **Port Configuration** tile.

Figure 150: Port Configuration

Port Configuration					
☐	Interface	PAE Capabilities	Control Mode	Operating Control Mode	PAE State
☐	1	Authenticator	Force Authorized	N/A	Initialize
☐	2	Authenticator	Force Authorized	N/A	Initialize
☐	3	Authenticator	Auto	N/A	Initialize
☐	4	Authenticator	Force Authorized	N/A	Initialize

Table 123: Port Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row.
PAE Capabilities	<p>The Port Access Entity (PAE) role, which is one of the following:</p> <ul style="list-style-type: none"> Authenticator – The port enforces authentication and passes authentication information from a remote supplicant (similar to a client or host) to the authentication server. If the server successfully authenticates the supplicant, the port allows access. Supplicant – The port must be granted permission by the authentication server before it can access the remote authenticator port.
Control Mode	<p>The port-based access control mode configured on the port, which is one of the following:</p> <ul style="list-style-type: none"> Auto – The port is unauthorized until a successful authentication exchange has taken place. Force Authorized – The port sends and receives normal traffic without client port-based authentication. Force Unauthorized – The port ignores supplicant authentication attempts and does not provide authentication services to the client. MAC-Based – This mode allows multiple supplicants connected to the same port to each authenticate individually. Each host connected to the port must authenticate separately in order to gain access to the network. The hosts are distinguished by their MAC addresses.
Operating Control Mode	<p>The control mode under which the port is actually operating, which is one of the following:</p> <ul style="list-style-type: none"> Auto Force Authorized Force Unauthorized MAC-Based N/A <p>If the mode is N/A, port-based access control is not applicable to the port. If the port is in detached state it cannot participate in port access control. Additionally, if port-based access control is globally disabled, the status for all ports is N/A.</p>
PAE State	<p>The current state of the authenticator PAE state machine, which is the 802.1X process that controls access to the port. The state can be one of the following:</p> <ul style="list-style-type: none"> Initialize Disconnected Connecting Authenticating Authenticated Aborting Held Force Authorized Force Unauthorized

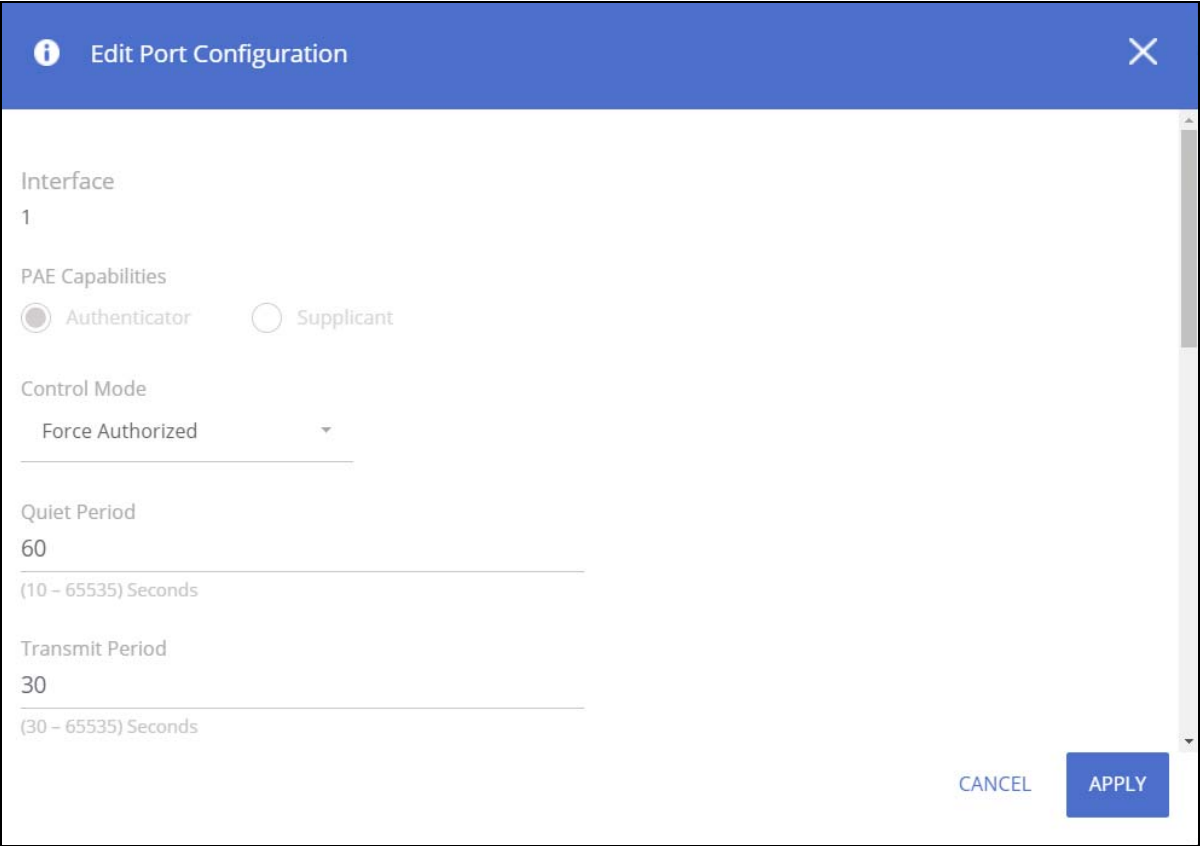
Configuring Port Access Control on an Interface

To configure the port access control settings on an interface:

1. Select the interface to configure.

2. Click **Edit**  .
The **Edit Port Configuration** dialog box appears.

Figure 151: Edit Port Configuration Page



Edit Port Configuration

Interface
1

PAE Capabilities
☒ Authenticator ☐ Supplicant

Control Mode
Force Authorized

Quiet Period
60
(10 – 65535) Seconds

Transmit Period
30
(30 – 65535) Seconds

CANCEL APPLY

3. Update the interface settings. The following table describes the fields in the dialog box.
4. Click **APPLY** to update the switch configuration.
Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Table 124: Edit Port Configuration Fields

Field	Description
Interface	The interface with the settings to view or configure. If you have been redirected to this page, this field is read-only and displays the interface that was selected on the Port Access Control Port Summary page.
PAE Capabilities	The Port Access Entity (PAE) role, which is one of the following: <ul style="list-style-type: none">• Authenticator – The port enforces authentication and passes authentication information from a remote supplicant (client or host) to the authentication server. If the server successfully authenticates the supplicant, the port allows access.• Supplicant – The port is connected to an authenticator port and must be granted permission by the authentication server before it can send and receive traffic through the remote port.

Field	Description
Authenticator Options	
The fields in this section are displayed and can be changed only when the PAE Capabilities field of the selected port is configured as Authenticator.	
Control Mode	<p>The port-based access control mode on the port, which is one of the following:</p> <ul style="list-style-type: none"> • Auto – The port is unauthorized until a successful authentication exchange has taken place. • Force Authorized – The port sends and receives normal traffic without client port-based authentication. • Force Unauthorized – The port ignores supplicant authentication attempts and does not provide authentication services to the client. • MAC-Based – This mode allows multiple supplicants connected to the same port to each authenticate individually. Each host connected to the port must authenticate separately in order to gain access to the network. The hosts are distinguished by their MAC addresses. This control mode is required for MAC Authentication mode.
Quiet Period	The number of seconds that the port remains in the quiet state following a failed authentication exchange.
Transmit Period	The value, in seconds, of the timer used by the authenticator state machine on the port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant.
Monitor Mode	<p>Enable this option to allow network access on the port even in cases where there is a failure to authenticate. However in such a case a log is generated with the results of the authentication process for diagnostic purposes.</p> <p>Monitor mode provides a way for network administrators to identify possible issues with the port-based access control configuration on the switch without affecting the network access to the users of the switch.</p>
VLAN Assignment	<p>The authentication server can provide information to the switch about which VLAN to assign the supplicant, and whether the port should be added as a tagged or untagged member of this VLAN. Enable this option to allow a port to be placed into a particular VLAN, based on the result of the authentication or type of 802.1X authentication. A client uses when it accesses the switch.</p> <p>Notes:</p> <ul style="list-style-type: none"> • If the port is not already a member of the VLAN specified by the RADIUS reply, the port will join the specified VLAN as a tagged or un-tagged member, based on the information indicated by the RADIUS reply for the supplicant. • If the port is already a member of the VLAN specified by the RADIUS server (whether via user configuration or via 802.1x dynamic VLAN assignment), then the tagged indication provided by the RADIUS reply must match the tag status of the VLAN on the port. If this is not the case, the authentication for such a supplicant will fail. • If the port is already a static (configured by user) member of the VLAN returned by the RADIUS server for the supplicant, then: <ul style="list-style-type: none"> • If the tag indication returned by the RADIUS server for the new supplicant matches that of the Static VLAN configured on the port, then the 802.1x authentication of the supplicant will succeed. • If the tag indication returned by the RADIUS server for the new supplicant DOES NOT match that of the static VLAN configured on the port, then the 802.1x authentication for this supplicant will fail. • If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN as part of the authentication, the supplicant is accepted and classified based on regular VLAN rules. • If the RADIUS server authorized the supplicant with a VLAN ID that does not exist on switch, the switch will dynamically create the specified VLAN ID. If last supplicant with this VLAN ID assignment is removed from switch the VLAN will also be removed.
Guest VLAN	Enable guest VLAN operation on port.
Supplicant Timeout	The amount of time that the port waits for a response before retransmitting an EAP request frame to the client.
Server Timeout	The amount of time the port waits for a response from the authentication server.
Maximum Requests	The maximum number of times that the port sends an EAP request frame (assuming that no response is received) to the client before restarting the authentication process.

Field	Description
MAC Authentication	The MAC Authentication mode of the port, which can be enabled or disabled. When MAC Authentication is enabled on the port (along with the Authenticator role and MAC-based control mode), stations connected to the port that do not support 802.1X can still be authenticated at the RADIUS server using the station's MAC address. Specifically, when the port detects a new, unauthorized station on the port, the switch first attempts to authenticate it using 802.1X. If the station does not respond, then after a time-out period, the switch extracts the station's MAC address from the detected packets and sends this to the RADIUS server for authentication. The RADIUS server responds with an authentication result, which is then applied to the port using the station's MAC address in MAC-based control mode.
Re-Authentication Period	Specify the amount of time that clients can be connected to the port without being reauthenticated. Values are 300 – 4294967295 Seconds, or Never . If this field is set to Never , connected clients are not forced to reauthenticate periodically.
Maximum Users	The maximum number of clients supported on the port if the Control Mode on the port is MAC-based 802.1X authentication. This field is configurable only if the control mode is set to MAC based .
Supplicant Options The fields in this section are displayed and can be changed only when the PAE Capabilities field for the selected port is configured as Supplicant.	
Control Mode	The port-based access control mode on the port, which is one of the following: <ul style="list-style-type: none"> Auto – The port is in an unauthorized state until a successful authentication exchange has taken place between the supplicant port, the authenticator port, and the authentication server. Force Authorized – The port is placed into an authorized state and does not require client port-based authentication to be able to send and receive traffic.
Credentials	Select the credentials to use for port authentication from the drop down box. Supplicant credentials need to be created before they are available for selection in this control
Start Period	The amount of time the supplicant port waits for a response from the authenticator port after sending a Start packet. If no response is received, the supplicant retransmits the Start packet.
Held Period	The amount of time the supplicant port waits before contacting the authenticator port after an active 802.1X session fails.
Maximum Start Messages	The maximum number of Start packets the supplicant port sends to the authenticator port without receiving a response before it considers the authenticator to be 802.1X-unaware.

Select one or more rows and click the **Additional Option**   drop-down to initiate one of the following operations (this option is available only when the port is an authenticator and the operating control mode is **Auto**):

- **Reauthenticate:** select this option to force the associated interface to restart the authentication process.
- **Initialize:** select this option to reset the 802.1X state machine on the associated interface to the initialization state. Traffic sent to and from the port is blocked during the authentication process.

Viewing Per-port 802.1X Details

To view the detailed 802.1X configuration on an interface, select the interface and click **Details**. See **Configuring Port Access Control on an Interface** for information about the fields the **Port Access Control Port Details** page displays. Note that the fields that display after you click **Details** depend on whether the port is configured with **Authenticator** or **Supplicant PAE Capabilities**.

VLAN Authentication

This tile provides authentication configuration, and information on the VLANs.

Hosts that fail the authentication might be denied access to the network or placed on a VLAN created for unauthenticated clients. This VLAN might be configured with limited network access. Only tagged unauthenticated traffic is allowed on such VLANs. Authentication can be disabled on any VLAN created by the user but not on a Guest VLAN or the Default VLAN.

Figure 152: VLAN Authentication Tile

VLAN Authentication				Display: 10	
☐	VLAN ID	VLAN Authentication			
☐	1	Enabled			
☐	2	Enabled			
<div>« < 1 > »</div>					

Select a VLAN ID and click **Edit**  to enable/disable the VLAN Authentication for the selected VLAN. The default for all VLANs is enable (Authentication is required on the VLAN).

Supplicant Credentials

This tile provides credential information on the supplicants.

Figure 153: Supplicant Credentials Tile

Supplicant Credentials

Display: 10

<div>☐</div>	Name	<div>▲</div> Username	Description
Table Is Empty			

Table 125: Supplicant Credentials Fields

Field	Description
Name	The supplicant credential name.
Username	The name the client uses to identify itself as a supplicant to the authentication server.
Description	Optional description of the credentials.

To add a supplicant to the list, click **Add**  and enter the appropriate fields. In addition to the fields in the table, you also need to enter the password that the client uses as credentials to identify as a supplicant to the authentication server.

To edit an existing supplicant, select it in the list, and click **Edit**  and edit the appropriate fields as needed.

To remove an existing supplicant, select it in the list, and **Remove**  .

Access Control Client Information

This tile provides information on the supplicant devices that are connected to the local authenticator ports. If there are no active 802.1X sessions, the table is empty.

To access the Access Control Client Information tile, click **Security > Port Access Control** in the navigation pane, and then scroll down to the **Access Control Client Information** tile.

Figure 154: Access Control Client Information Tile

Access Control Client Information Display: 10

Interface	Username	Supplicant MAC Address	Authentication Method	Session Time (HHH:MM:SS)	VLAN ID
Table Is Empty					

Table 126: Access Control Client Information Fields

Field	Description
Interface	The local interface associated with the rest of the data in the row.
Username	The name the client uses to identify itself as a supplicant to the authentication server.
Supplicant MAC Address	The MAC address of the supplicant that is connected to the port.
Authentication Method	Indicates if client was authenticated using 802.1x credentials or based only on supplicant MAC address.
Session Time	The amount of time that has passed since the connected supplicant was granted access to the network through the authenticator port.
VLAN ID	The ID of the VLAN the supplicant was placed in as a result of the authentication process.

Access Control Statistics

Use this tile to view information about the Extensible Authentication Protocol over LAN (EAPOL) frames and EAP messages sent and received by the local interfaces. To view additional per-interface EAPOL and EAP message statistics, select the interface with the information to view and click **Details**.

To access the Access Control Statistics tile, click **Security > Port Access Control** in the navigation pane, and scroll down to the **Access Control Statistics** tile.

Figure 155: Access Control Statistics Tile

Access Control Statistics Display: 10

☐	Interface	PAE Capabilities	EAPOL Frames Received	EAPOL Frames Transmitted	Last EAPOL Frame Version	Last EAPOL Frame Source
☐	1	Authenticator	2	0	0	00:00:00:00:00:00
☐	2	Authenticator	0	0	0	00:00:00:00:00:00
☐	3	Authenticator	4	0	0	00:00:00:00:00:00
☐	4	Authenticator	3	0	0	00:00:00:00:00:00

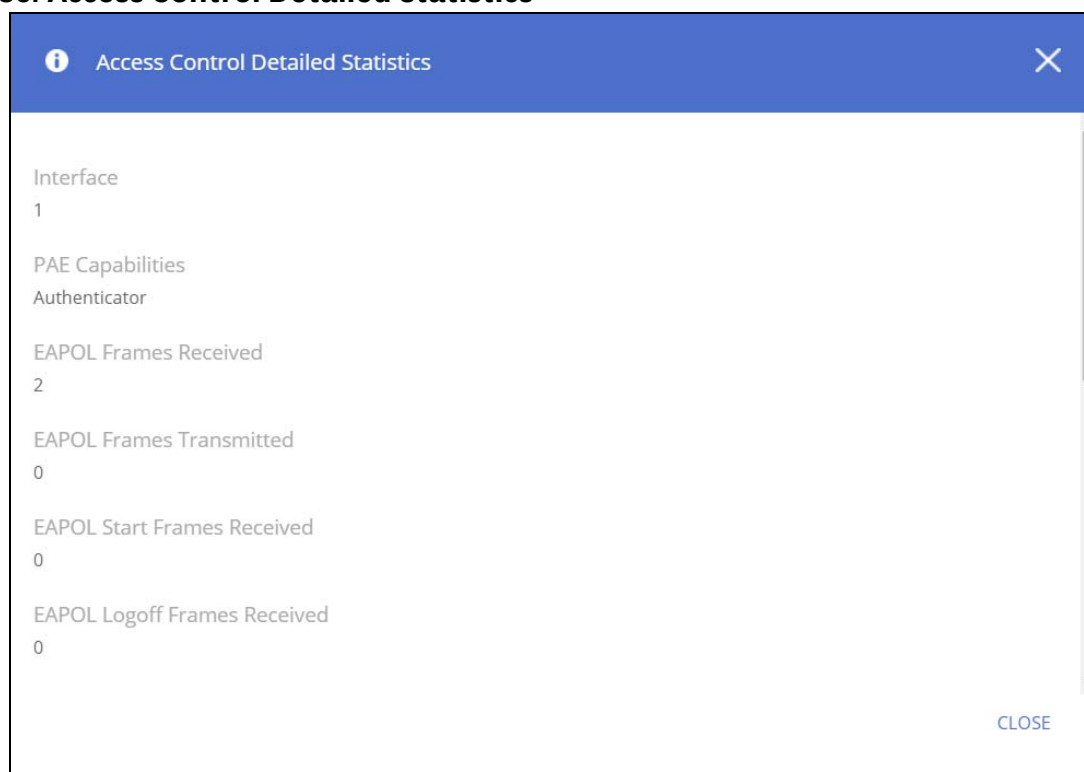
Table 127: Access Control Statistics Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When viewing detailed information for an interface, this field identifies the interface being viewed.
PAE Capabilities	The Port Access Entity (PAE) role, which is one of the following: <ul style="list-style-type: none"> Authenticator – The port enforces authentication and passes authentication information from a remote supplicant (similar to a client or host) to the authentication server. If the server successfully authenticates the supplicant, the port allows access. Supplicant – The port must be granted permission by the authentication server before it can access the remote authenticator port.
EAPOL Frames Received	The total number of valid EAPOL frames received on the interface.
EAPOL Frames Transmitted	The total number of valid EAPOL frames sent by the interface.
Last EAPOL Frame Version	The protocol version number attached to the most recently received EAPOL frame.
Last EAPOL Frame Source	The Source MAC Address attached to the most recently received EAPOL frame.

To reset all statistics counters to 0, select each interface with the statistics to reset and click **Clear**.

Access Control Details

To view Access Control Detailed Statistics, select an interface and click **Details**  .

Figure 156: Access Control Detailed Statistics

The following table describes the additional fields that appear in the Details window. The fields this window displays depend on whether the interface is configured as an authenticator or supplicant, as noted in the applicable field descriptions.

Table 128: Access Control Statistics Fields

Field	Description
Authenticator Fields The fields in this section are displayed only when the PAE Capabilities field for the selected port is configured as Authenticator.	
EAPOL Start Frames Received	The total number of EAPOL-Start frames received on the interface. EAPOL-Start frames are sent by a supplicant to initiate the 802.1X authentication process when it connects to the interface.
EAPOL Logoff Frames Received	The total number of EAPOL-Logoff frames received on the interface. EAPOL-Logoff frames are sent by a supplicant to indicate that it is disconnecting from the network, and the interface can return to the unauthorized state.
EAP Response/ID Frames Received	The total number of EAP-Response Identity frames the interface has received. EAP-Response Identity frames are sent by a supplicant to provide user information that is used to for authentication.
EAP Response Frames Received	The total number of EAP-Response frames the interface has received. EAP-Response frames are sent from a supplicant to an authentication server during the authentication process.
EAP Request/ID Frames Transmitted	The total number of EAP-Request Identity frames the interface has sent. EAP-Request Identity frames are sent from an authenticator to a supplicant to request user information that is used to for authentication.
EAP Request Frames Transmitted	The total number of EAP-Request frames the interface has sent. EAP-Request frames are sent from an authentication server to the client to request authentication information.
Invalid EAPOL Frames Received	The number of unrecognized EAPOL frames received on the interface.
EAPOL Length Error Frames Received	The number of EAPOL frames with an invalid packet body length received on the interface.

Port Security

Port security, also known as port MAC locking, allows you to limit the number of source MAC addresses that can be learned on a port. When port security is enabled on a port, that port's MAC addresses are removed from the Layer 2 Forwarding Database. If a port reaches the configured limit, any other addresses beyond that limit are not learned, and the frames are discarded. Frames with a source MAC address that have already been learned will be forwarded. Port security can help secure the network by preventing unknown devices from forwarding packets into the network.

Port Security Configuration

Use this tile to view and configure the port security settings for each interface.

To view the Port Security Configuration tile, click **Security > Port Security** in the navigation pane.

Figure 157: Port Security Configuration Tile

Port Security Configuration							Display: 10
☐	Interface ▲	Port Security	Max Addresses Allowed	Sticky Mode	Violation Trap	Violation Shutdown	
☐	1	Disabled	1	Disabled	Disabled	Disabled	
☐	2	Disabled	1	Disabled	Disabled	Disabled	
☐	3	Disabled	1	Disabled	Disabled	Disabled	
☐	4	Disabled	1	Disabled	Disabled	Disabled	

To configure port security settings on one or more interfaces, select the interface or interfaces to configure, and click **Edit** .

To configure all interfaces at the same time, click **Edit All** .

Table 129: Port Security Interface Status Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring the port security settings for one or more interfaces, this field lists the interfaces that are being configured.
Port Security	The administrative mode of the port security feature on the interface.
Max Addresses Allowed	<p>The number of source MAC addresses that can be dynamically learned on an interface. If an interface reaches the configured limit, any other addresses beyond that limit are not learned, and the frames are discarded.</p> <p>Frames with a source MAC address that has already been learned are forwarded. A dynamically-learned MAC address is removed from the MAC address table. if the entry ages out, the link goes down, or the system resets.</p> <p>NOTE: The behavior of a dynamically-learned address changes if the sticky mode for the interface is enabled or the address is converted to a static MAC address.</p>
Sticky Mode	<p>The sticky MAC address learning mode is one of the following:</p> <ul style="list-style-type: none"> Enabled - MAC addresses learned or manually configured on this interface are learned in sticky mode. A sticky-mode MAC address is a MAC address that does not age out and is added to the running configuration. If the running configuration is saved to the startup configuration, the sticky addresses are saved to persistent storage and do not need to be relearned when the switch restarts. Upon enabling sticky mode on an interface, all dynamically learned MAC addresses in the MAC address table for that interface are converted to sticky mode. Additionally, new addresses dynamically learned on the interface will also become sticky. Disabled - When a link goes down on a port, all of the dynamically learned addresses are cleared from the source MAC address table the feature maintains. When the link is restored, the interface can once again learn addresses up to the specified limit. If sticky mode is disabled after being enabled on an interface, the sticky-mode addresses learned or manually configured on the interface are converted to dynamic entries and are automatically removed from persistent storage.
Violation Trap	Indicates whether the port security feature sends a trap to the SNMP agent when a port is locked and a frame with a MAC address not currently in the table arrives on the port. A port is considered to be locked once it has reached the maximum number of allowed dynamic or static MAC address entries in the port security MAC address table.
Violation Shutdown	Indicates whether the port security feature shuts down the port when a port is locked and a frame with a MAC address not currently in the table arrives on the port. A port is considered to be locked once it has reached the maximum number of allowed dynamic or static MAC address entries in the port security MAC address table.

Static/Dynamic MAC Addresses

To view the static MAC address information, click the **Static MAC Address** tab.

To view the dynamic MAC address information, click the **Dynamic MAC Address** tab.

Static MAC Addresses Tab

Use this tab to display, add and remove the static MAC addresses of hosts that are allowed to send traffic to specific interfaces on the switch. The number of MAC addresses you can associate with each interface is determined by the maximum static MAC addresses allowed on a given interface.

The Static MAC Address tab lists the following type of MAC addresses learned on ports that are enabled for port security:

- MAC addressed learned on interfaces set to sticky mode disable, which were converted to static addresses by users.
- MAC addressed learned dynamically by switch on interfaces that are sticky mode enabled.

To display this tab, click **Security > Port Security** in the navigation pane, and then click the **Static MAC Addresses** tab.

Figure 158: Static MAC Addresses Tab

Static MAC Addresses

Dynamic MAC Addresses

Display: 10

<div><div></div><div>Interface</div></div>	<div><div></div><div>MAC Address</div></div>	<div><div></div><div>VLAN ID</div></div>	<div><div></div><div>Sticky Mode</div></div>
<div>Table Is Empty</div>			

Use the buttons to perform the following tasks:

- To associate a static MAC address with an interface, click **Add** and configure the settings in the available fields.
- To remove one or more configured static MAC address entries, select each entry to delete and click **Remove** .

Table 130: Static MAC Addresses Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When adding a static MAC address entry, use the Interface menu to select the interface to associate with the permitted MAC address.
MAC Address	The MAC address of the host that is allowed to forward packets on the associated interface.
VLAN ID	The ID of the VLAN that includes the host with the specified MAC address.
Sticky Mode	Indicates whether the static MAC address entry is added in sticky mode. When adding a static MAC address entry, the Sticky Mode field can be selected only if it is enabled on the interface.

The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Dynamic MAC Addresses Tab

Use this tab to view the dynamic MAC address entries that have been learned on interfaces set to sticky mode disable. From this page, you can also convert dynamic MAC address entries to static MAC address entries for a given interface.

To display this tab, click **Security > Port Security** in the navigation pane, and then click the **Dynamic MAC Addresses** tab.

Figure 159: Port Security Dynamic MAC Addresses Tab



Table 131: Port Security Dynamic MAC Addresses Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. Use the Interface menu to select the interface to display. NOTE: Only interfaces that have Port Security enabled and Sticky Mode disabled are available for selection.
MAC Address	The MAC address that was learned on the port. An address is dynamically learned when a frame arrives on the interface and the source MAC address in the frame is added to the MAC address table.
VLAN ID	The VLAN ID specified in the Ethernet frame received by the interface.
Type	The type of MAC address. The supported type is Learned .

Convert Dynamic MAC Addresses to Static MAC Addresses

To convert dynamic MAC addresses to static MAC addresses: Select the row(s) you wish to convert, click **Convert to Static** and then click **APPLY**.
The converted dynamic MAC addresses can be viewed in the **Static MAC Addresses** tab. They are converted with Sticky mode Disabled.

Protected Ports

The Protected Ports feature provides L2 isolation between interfaces (Ethernet ports and LAGs) that share the same broadcast domain (VLAN) with other interfaces.
Ports can be defined to one of the following 2 modes:

- Protected ports: These ports can send traffic only to unprotected ports. Packets received on a protected port are filtered at the egress of the other protected ports.
- Unprotected ports: These ports send traffic to any port. This is the default setting of all interfaces.

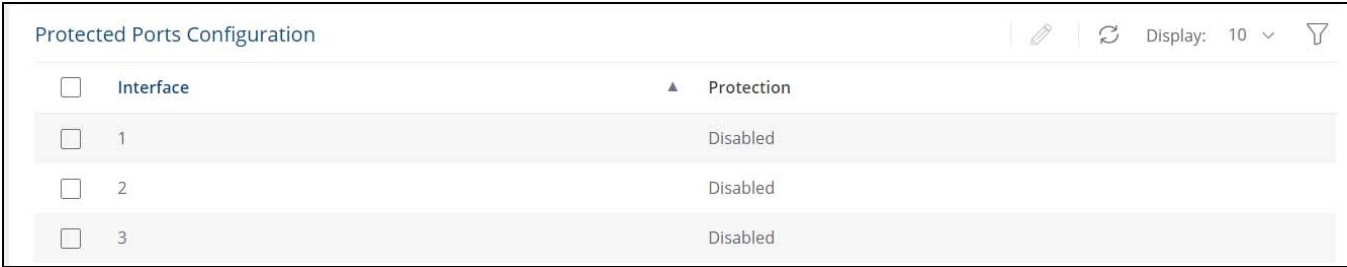
Port Protection is independent from any and all other features and configuration settings. For example: a user can place two protected ports into a common VLAN, and they will not be able to communicate with each other; By the same token, a protected port will not be able to communicate with an unprotected port, if the two ports are not in the same VLAN.

Protected Ports Configuration

Use this page to configure and view protected ports settings.

To view the Protected Ports Configuration tile, click **Security > Protected Ports** in the navigation pane.

Figure 160: Protected Ports Configuration Tile



Interface	Protection
☐ 1	Disabled
☐ 2	Disabled
☐ 3	Disabled

Table 132: Protected Ports Configuration Fields

Field	Description
Interface	The port or trunk ID.
Protection	Displays the Admin state of Port Protection on the interface: <ul style="list-style-type: none">• Disabled - port is an unprotected port. this is the default setting.• Enabled - port is a protected port

To change the Protection setting of an interface: create a protected ports group and add ports to the group:

1. Select the row(s) you wish to edit.
2. Click **Edit**  .
The **Edit Port Protection** dialog box appears.



Edit Port Protection

Interface
1, 3, 5

Port Protection
☐

CANCEL APPLY

3. Enable or disable Port Protection as needed.
4. Click **APPLY**.

DHCP Snooping

DHCP snooping provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, also referred to as a DHCP snooping binding table. DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. DHCP snooping differentiates between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

Interfaces are defined as trusted or untrusted by the administrator. Trusted interfaces are usually connected to DHCP servers or to switches/hosts that DHCP packet filtering is not required for them. Untrusted interfaces are connected to untrusted hosts, or to switches that are connected to untrusted hosts.

The Database is updated by interception of DHCPACK, DHCPDECLINE and DHCPRELEASE packets. The switch does not update the DHCP snooping database when a station moves to other interface. When DHCP snooping is disabled for a VLAN the bindings that were collected for that VLAN are removed. Periodically the Database is saved to the backup database on switch flash memory. This database is persistent across reboot. To ensure that the lease time in the database is accurate, backup to database will be active only if the system clock was set through SNTP, DHCP on the switch, or manually by user. Backup to database is optional. You can enable or disabled the backup.

Global Configuration

Use this tile to configure the global DHCP snooping options:

Figure 161: Global Configuration Tile

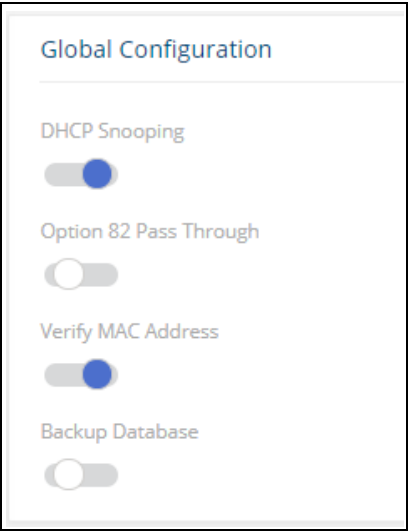


Table 133: Global Configuration Fields

Field	Description
DHCP Snooping	Enable or disable. By default, DHCP snooping is disabled. NOTE: DHCP snooping still needs to be enabled per VLAN to make it operational for that VLAN.
Option 82 Pass Through	Enabled or disable. By default, option 82 pass through is disabled. <ul style="list-style-type: none">• Disable - DHCP packets with option-82 information from an untrusted port are discarded.• Enable - DHCP packets with option-82 information from an untrusted port are forwarded.
Verify MAC Address	Enabled or disable. By default, MAC address verification is enabled. If enabled, the switch verifies that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address in the packet.
Backup Database	Enabled/ Disabled. By default, database backup is disabled. <ul style="list-style-type: none">• Disable - DHCP snooping entries are not saved to a table on switch flash memory.• Enable - DHCP snooping entries are saved to a table on switch flash memory, and saved across reboots. To activate flash database update, you need to set the clock (manually or through SNTP).

VLAN Settings

Use the VLAN Settings tile to set enable DHCP Snooping on the required VLANs.

Figure 162: VLAN Settings Tile

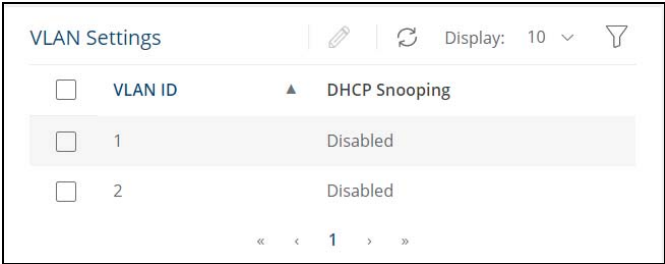


Table 134: VLAN Settings Fields

Field	Description
VLAN ID	Identifier for the VLAN.
DHCP Snooping	Enabled or disable. By default, DHCP snooping is disabled.

To change the setting for DHCP snooping, select a VLAN and click **Edit**  .

Interface Settings

Use the Interface Settings tile to set ports to DHCP snooping trusted or untrusted state.

Figure 163: Interface Settings Tile

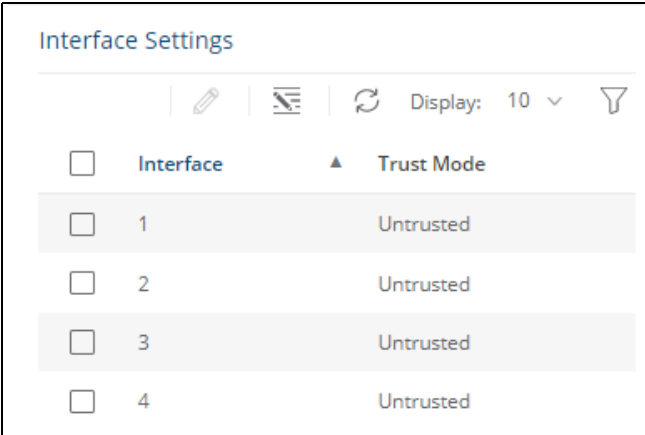


Table 135: Interface Settings Fields

Field	Description
Interface	Identifier for the interface.
Trust Mode	Trusted or Untrusted. By default, DHCP snooping is untrusted.

Select one or more interface(s) and click **Edit**  to toggle the trusted interface feature.

Click **Edit All**  to configure all interfaces at the same time.

Figure 164: Edit DHCP Snooping Interface Settings Dialog

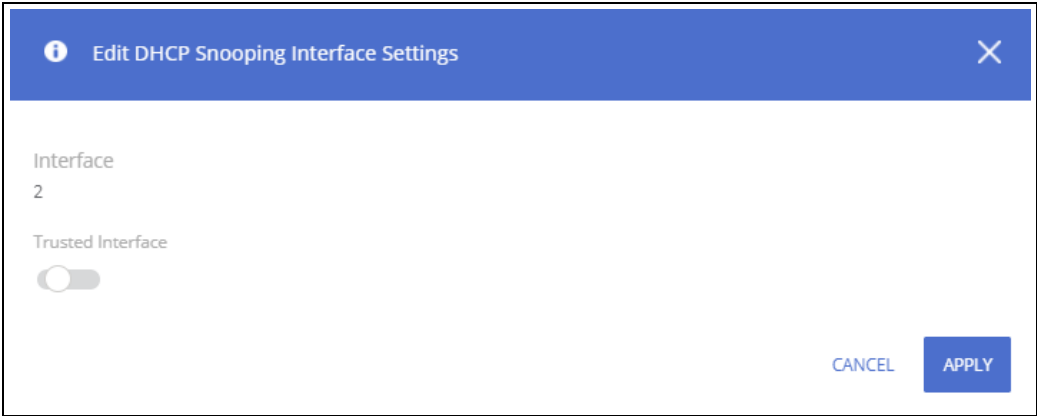


Table 136: Edit DHCP Snooping Interface Settings Fields

Field	Description
Interface	The interface(s) selected for editing.
Trusted Interface	Enable/disable as needed.

Click **APPLY** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Binding Database

Use the **Binding Database** setting tile to view the DHCP Snooping Binding table which show DHCP clients learned on untrusted ports.

Figure 165: Binding Database Tile



Table 137: Binding Database Fields

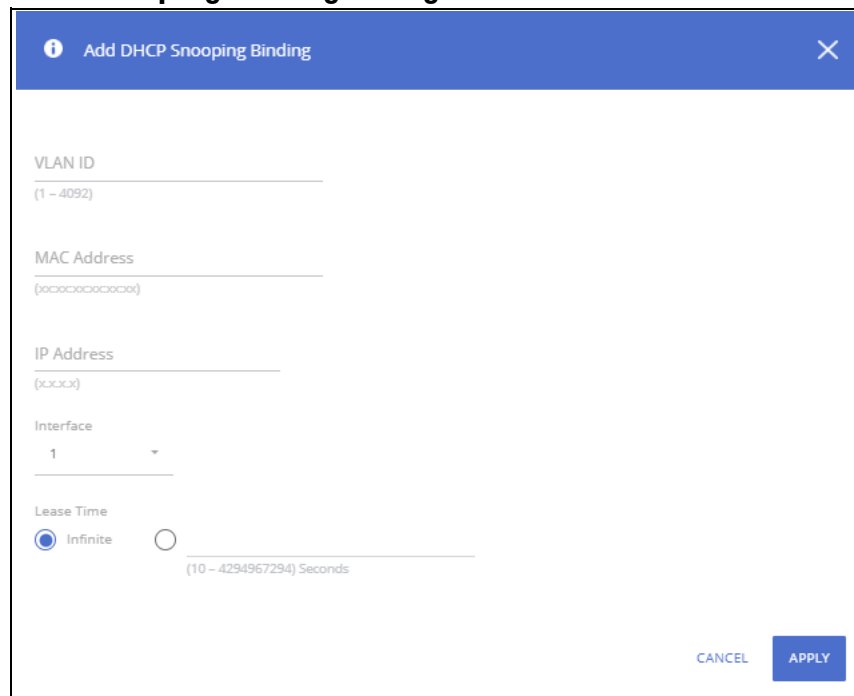
Field	Description
VLAN ID	The VLAN to which the DHCP client is connected
MAC Address	DHCP client Source MAC address.
IP Address	DHCP client IP address.
Interface	Switch interface to which the DHCP client is connected.
Lease Time	DHCP address lease time. This may be configured for entries that are not volatile. Configure the entry lease-time or set it to infinite.

To remove a database, select it and click **Delete**  .

Click **Clear All**  to remove all entries in the database

To add a static DHCP binding database click **Add**  and enter the appropriate values for the binding database fields.

Figure 166: Add DHCP Snooping Binding Dialog Box



The dialog box titled "Add DHCP Snooping Binding" contains the following fields and controls:

- VLAN ID:** A text input field with a placeholder "(1 - 4092)".
- MAC Address:** A text input field with a placeholder "(xxxxxxxxxxxx)".
- IP Address:** A text input field with a placeholder "(xxxx)".
- Interface:** A dropdown menu showing "1".
- Lease Time:** Two radio buttons, "Infinite" (selected) and an unlabeled one. Below them is a text input field with a placeholder "(10 - 4294967294) Seconds".
- Buttons:** "CANCEL" and "APPLY" buttons at the bottom right.

ARP Attack Protection

ARP attack protection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

The ARP inspection feature defines two types of interfaces:

- **Trusted interface:** The switch does not check ARP packets that are received on the trusted interface; it simply forwards the packets.
- **Untrusted interface.** ARP inspection is performed only on untrusted interfaces.

When a packet arrives on an untrusted interfaces the following logic is implemented:

If the VLAN that the packet arrived on has ARP static binding list defined, then search that list.

- If the IP address is found and the MAC address in the list matches the packet's MAC address
 - the packet is valid and is forwarded.
- If the IP address is found and the MAC address in the list does not match the packet's MAC address
 - the packet is not valid and is dropped.

If the packet's IP address was not found in the ARP static binding, and DHCP snooping is enabled for that VLAN then search the DHCP snooping database for the packet's <VLAN - IP address> pair.

- If the <VLAN - IP address> pair was found, and the MAC address and the interface in the database match the packet's MAC address and ingress interface
 - the packet is valid and is forwarded.

- If the packet's IP address was not found in the ARP static binding and in the DHCP snooping - the packet is not valid and is dropped.

If the ARP packet's header check is configured then the following additional checks are preformed:

- Source MAC: Compare the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.
- Destination MAC: Compare the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses.
- IP addresses: Compare the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

Global Configuration

Use this tile to configure the global ARP Attack options:

Figure 167: Global Configuration Tile

Global Configuration

ARP Attack Protection

ARP Header Validation

ARP Protection Logging

ARP Protection Logging Interval

5

(0 - 86400) Seconds

Table 138: Global Configuration Fields

Field	Description
ARP Attack Protection	Enable or disable. By default, ARP Protection is disabled.
ARP Header Validation	Enabled or disable. By default, ARP Header Validation is disabled. <ul style="list-style-type: none"> • Disable - ARP header checks are not performed in addition to regular ARP protection validation. • Enable - ARP header checks are performed in addition to regular ARP protection validation.
ARP Protection Logging	Enabled or disable. By default, ARP Protection Logging is enabled. If enabled, when an ARP attack occurs, a SYSLOG message is sent.
ARP Protection logging Interval	If ARP Protection Logging is enabled, use this setting to define the interval between SYSLOG messages. By default, the interval is 5 seconds.

Click **APPLY** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Interface Settings

Use the **Interface Setting** tile to set the interface mode to Trusted or Untrusted:

Figure 168: Interface Settings Tile

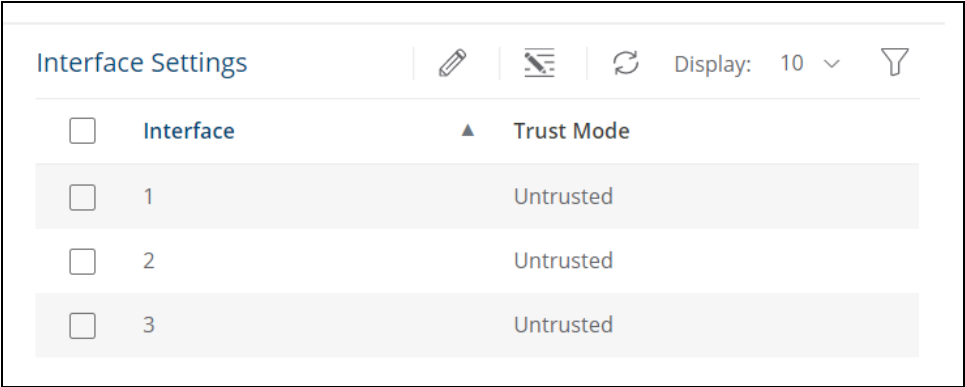
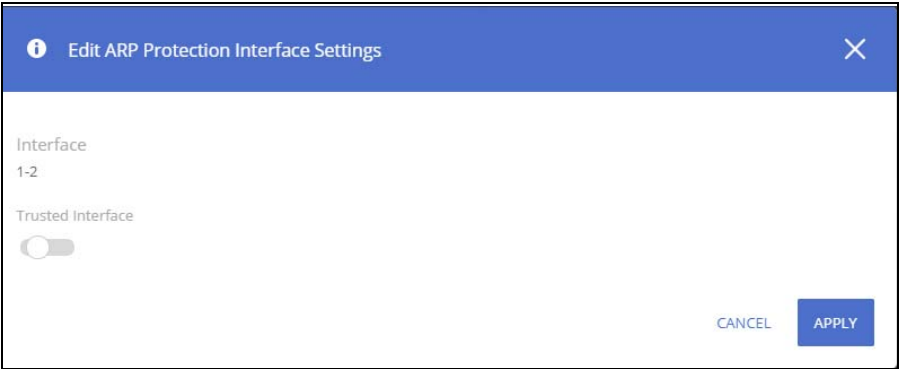


Table 139: Interface Settings Fields

Field	Description
Interface	Identifier for the interface.
Trust Mode	Trusted or Untrusted. If Untrusted ARP Protection validation is performed on the interface

To change the trusted setting, select one or more interfaces and click **Edit**  .

Click **Edit All**  to configure all interfaces at the same time:



ARP Access Control Rules

Use this tile to configure the ARP Access Controls rules. These rules are used for validation of ARP frames.

Figure 169: Access Control Rules Tile



Table 140: Access Control Rules Fields

Field	Description
List Name	The name of the list of access control rules.
IP Address	The IP address of a trusted ARP frame (associated to a MAC address in this row)
MAC Address	The MAC address of a trusted ARP frame (associated to an IP Address in this row)

To add an **ARP Access Rule**, click **Add** . For the **List Type**, select **New list** to create a new list with an access rule. To create an access rule on an existing list, click **Existing List** and select the list from the drop-down list. Next, enter the values as required in the dialog box, and click **APPLY**.

Figure 170: Add ARP Access Control Rule Dialog Box

To remove a ARP Access Rule, select it and click **Delete** .

VLAN Settings

Use this tile to configure the enable or disable ARP protection on VLAN interfaces:

Figure 171: VLAN Settings Tile

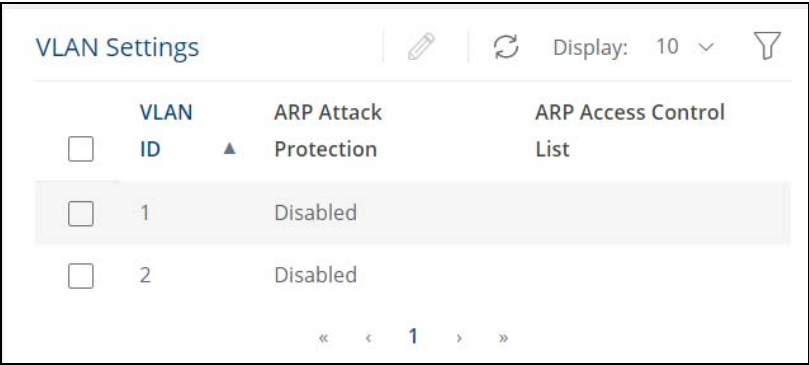
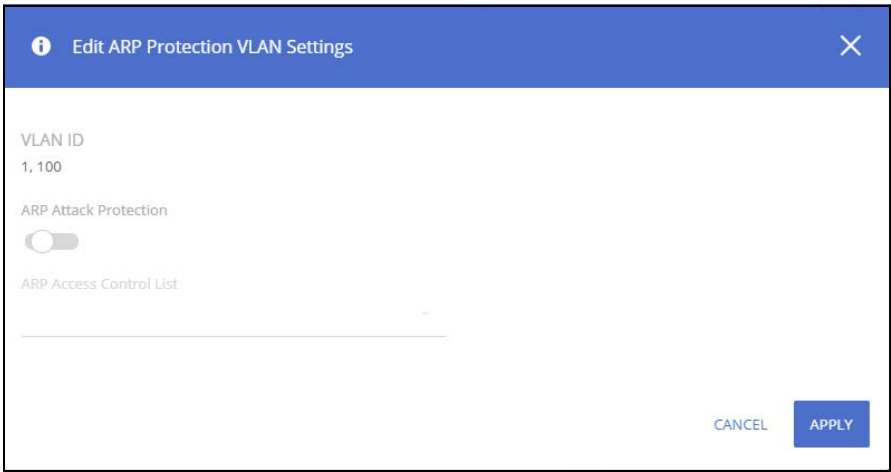


Table 141: VLAN Settings Fields

Field	Description
VLAN ID	The VLAN to which the ARP Attack Protection setting is connected.
ARP Attack Protection	Enable or disable. By default, ARP Protection is disabled.
ARP Access Control List	Association of the VLAN to an ARP Access control List created by user

To edit one or more VLAN Settings entries, do the following:

1. Select the entry(ies) you wish to edit and click **Edit** .



2. Enable or disable the ARP Attack Protection as needed.
3. If you enable ARP Attack Protection, you can also associate the protection with an ARP Access Control List.

Denial of Service Protection

The HPE Networking Instant On 1930 Switch Series switches include Denial-of-Service (DoS) and ICMP (ping) protection features to help protect against various high-volume traffic scenarios or malicious attacks.

A DoS attack is an attempt to saturate the switch or the network, with external communication requests to prevent the switch, or network from performing efficiently, or at all. You can enable DoS protection that prevents common types of DoS attacks.



For some of the settings, the DoS feature does not generate notifications (such as error messages, SYSLOG messages, or SNMP traps) if a DoS attack occurs. The switch will simply drop DoS-related packets.

The ICMP security options help prevent the switch and the network from attacks that involve issues with the ICMP echo request packets (pings) that the switch receives.

To display the Global Settings tile, click **Security > Denial of Service Protection** in the navigation pane.

Global Settings

Figure 172: Global Settings

Global Settings

Interface Level DoS Protection

☒

Block SYN-FIN Packets

☐

SYN Protection Mode

☐ Disabled

☐ Log

☒ Log and Block

SYN Protection Threshold

80

(20 – 200) Packets per Second

SYN Protection Period

60

(10 – 600) Seconds

Table 142: Global Settings Fields

Field	Description
Interface Level DoS Protection	Enable this option to enable Interface level DoS settings(see SYN Attack Status Tab for more information). Interface level protection cannot be enabled if an Access Control List is attached to any switch interface.
Block SYN-FIN Packets	Enable this option to drop, on all interfaces, TCP packets in which both SYN and FIN flags are set.

Field	Description
SYN Protection Mode	Enables SYN Protection on the switch. SYN Protection detects TCP SYN traffic sent to the switch IP address(es) above the defined threshold and acts accordingly. Possible values are: <ul style="list-style-type: none"> Disabled - SYN Protection is disabled on the switch. This is the default setting. Log – SYN Protection is enabled on the switch. If the TCP SYN traffic rate on a certain interface is higher than the defined threshold, the violation is reported through Syslog. Log and Block - SYN Protection is enabled on the switch. If the TCP SYN traffic rate on a certain interface is higher than the defined threshold, the violation is reported through Syslog. In addition, all TCP SYN traffic on the interface is dropped for the specified duration.
SYN Protection Threshold	Defines The threshold applied to interface to activate SYN protection. Valid range is 20-200 Packets per second. Default is 80 Packets per second.
SYN Protection Period	The timeout (in seconds) after which an interface blocked by this feature gets unblocked. This setting is available only if SYN Protection mode is set to Log and Block. NOTE: If a SYN attack is still active on this interface it might become blocked again. Range is 10-600 seconds, default is 60 seconds.

Click **APPLY** to save any changes for the current boot session. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Syn Attack Status/Interface Settings Tile

To view the SYN attack status, click the **SYN Attack Status** tab.

To view the Interface settings information, click the **Interface Settings** tab.

SYN Attack Status Tab

The SYN Attack Status tab displays the TCP SYN Protection status and last SYN attack on each interface.

Figure 173: SYN Attack Status Tab

Interface	Status	Last SYN Attack
1	Normal	
2	Normal	
3	Attacked	14-Dec-2021 07:07:16 Blocked and Logged
4	Normal	

Table 143: SYN Attack Status Fields

Field	Description
Interface	Interface identifier.
Status	Current status of the interface. Possible values are: <ul style="list-style-type: none"> Normal - TCP SYN protection is not enabled or the interface is not under a TCP SYN attack. Attacked - Interface is currently under a TCP SYN attack.
Last SYN Attack	The last time stamp in which the switch identified a SYN attack on this interface.

Interface Settings Tab

The Interface Settings tab enables configuring and provides information on the ICMP Attack Prevention and SYN Rate Protection settings for the interfaces.



The **Interface Setting** tab is enabled only if **Interface Level Dos Protection** state is enabled. Settings configured on interfaces are active only if the **Interface Level Dos Protection** setting is enabled.

Figure 174: Interface Settings

SYN Attack Status		Interface Settings				Display: 10	
☐	Interface	☐ ICMP Attack Prevention		☐ SYN Rate Protection			
☐	1	Disabled		Disabled			
☐	2	Enabled		Enabled			

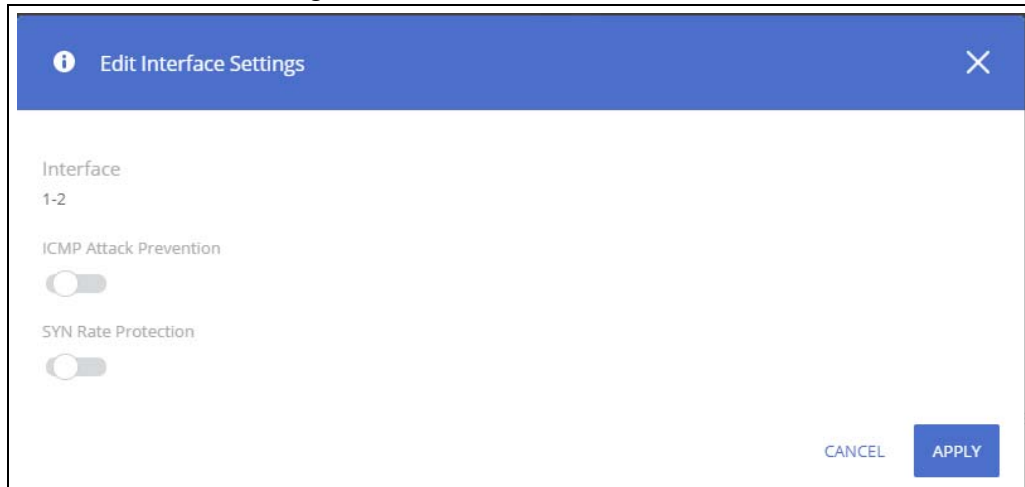
Table 144: Interface Settings Fields

Field	Description
Interface	Interface identifier.
ICMP Attack Prevention	Enabled or Disabled. If enabled, the interface will drop any ICMP request packet received on the interface. By default, ICMP Attack Prevention is disabled.
SYN Rate Protection	Enabled or Disabled. If enabled on an interface, this setting limits ingress TCP packets with the following flag settings to 250 packets per second: <ul style="list-style-type: none">• SYN=1• ACK=0• FIN=0 Packets above the rate are dropped. By default Syn Rate Protection is disabled.

To change the setting for one or more interfaces, select it and click **Edit**  . Or, click **Edit All**  to configure all interfaces at the same time.

The **Edit Interface Settings** dialog box appears. Set the **ICMP Attack Prevention** and the **SYN Rate Protection** as required, and click **APPLY**.

Figure 175: Edit Interface Settings



HTTPS Certificate

Secure HTTP (HTTPS) enables the transmission of HTTP over Transport Layer Security (TLS) connection. Using HTTPS ensures that the web based management session is protected from unwanted eavesdropping.

Information encryption and decryption are performed by a pair of a public and private keys.

- Data encrypted with the public key can only be decrypted with the private key.
- The public key is shared between server and clients, while the private key is never given out.

The certificate used for HTTPS sessions is also used to prove the identity of the server (the switch) to clients (management stations). Certificates are issued and signed by well known Certificate Authorities (CAs) trusted by the management station. A signed certificate stores data about the site (IP address/URL, Company name, Country, etc.). The browser inspects the signature and only if the signature is correctly verified the certificate is trusted, otherwise it notifies the user that the certificate is unsigned by a well-known authority.

The switch supports generation of a single certificate and exporting to CA for signing and allows importing of the signed certificate for use by the switch for HTTPS sessions.

To enable users to benefit from a secured connectivity, without the need to sign a certificate by a CA - the switch also supports the use of unsigned certificates (also known as self-signed certificates). Although self-signed certificates do not prove the switch identity to the browser, they do enable securing the management session using the public and private key.

The certificate and key pairs are stored as part of the switch configuration file. If the switch startup file does not include a certificate then a self-signed certificate will be generated automatically as part of the switch boot sequence.

HTTPS Certificate Settings

The HTTPS Certificate Settings tile displays the current certificate details and provides several buttons at the bottom of the page to perform actions relating to HTTPS certification.

Figure 176: HTTPS Certificate Settings Tile

HTTPS Certificate Settings

Common Name

10.5.235.225

Valid Dates

August 26 2019 - August 25 2020

Source

Auto Generated

REFRESH

GENERATE CERTIFICATE

GENERATE CERTIFICATE REQUEST

IMPORT CERTIFICATE

VIEW CERTIFICATE DETAILS

Table 145: HTTPS Certificate Settings Fields

Field	Description
Common Name	Specifies the fully qualified switch URL or IP address.
Valid Dates	The start and end dates for the certificate.
Source	Specifies whether the certificate was generated by the system (auto generated) or by the user (self-defined).

Use the buttons at the bottom of the page to perform actions relating to HTTPS certification:

Generate a Self-Signed Certificate

Generating a new certificate overrides any previous certificate used. You can delete a self-signed certificate that you created. In this case, the switch will auto generate a self-signed certificate.
To generate a self-signed certificate, click the **GENERATE CERTIFICATE** button to view the dialog box.

Figure 177: Generate Certificate Dialog Box

Generate Certificate

Common Name

(1 – 64 characters)

Organization Unit

(0 – 64 characters)

Organization Name

(0 – 64 characters)

Location

(0 – 64 characters)

State

(0 – 64 characters)

Country

(0 – 2 characters)

Duration

365

(30 – 3650) Days

Regenerate RSA Key

☒

RSA Key Length

☒ 2048 bits

☐ 3072 bits

CLEAR

CANCEL

APPLY

Enter the following fields:

Table 146: Generate Certificate Fields

Field	Description
Common Name	Enter the fully qualified switch URL or IP address. If unspecified, defaults to the lowest IP address of the switch at time of generation.
Organization Unit	Enter the organization unit or department name. If unspecified, field is left empty.
Organization Name	Enter the organization name. If unspecified, field is left empty.
Location	Enter the location or city name. If unspecified, field is left empty.

Field	Description
State	Enter the state or province name. If unspecified, field is left empty.
Country	Enter the country name abbreviation. If unspecified, field is left empty.
Duration	Enter the number of days that the certificate is valid. If unspecified, the duration is set to 365 days (1 year).
Regenerate RSA Key	Enable this feature to regenerate a pair of RSA keys. If disabled, the existing key set is used.
RSA Key Length	Select the preferred key length. By default, key length is 2048.

Click **APPLY** to generate the certificate.

Click **CANCEL** to cancel the operation.

Click **CLEAR** to clear the fields.

Using a Certificate Signed by a Certificate Authority

In order to use a certificate that is signed by a Certificate Authority (CA), you need to complete the following steps:

1. Generate a certificate request: Click **GENERATE CERTIFICATE REQUEST** and enter the fields as defined in [Generate a Self-Signed Certificate](#).



The Duration and RSA Key Regeneration fields do not appear in the certificate request, since they are not required. If new keys are needed, you need to generate a self-signed certificate before generating a certificate request.

2. Export the certificate for signing: In the **Certificate Request** box that appears, click **COPY TO CLIPBOARD** to copy the generated certificate request to a file, and send the file to the CA for signing.
3. After the Certificate is signed by a CA, import it back to the device. The certificate needs to be imported as a PEM encoding/file type. Import the signed certificate: Click **IMPORT CERTIFICATE** and copy the certificate, and optionally RSA keys and the Public Key that you received from the CA to the dialog box fields(see ["Import Certificate Dialog Box"](#)).
 - If keys are imported together with the certificate, the public key found in the certificate must match the imported key.
 - If keys are not imported with the certificates, the public key found in the certificate must match the public key stored on the switch.
4. After copying the keys, click **APPLY**.
Importing a CA signed certificate overrides the certificate currently used on the switch.

Figure 178: Import Certificate Dialog Box

 Import Certificate 

Certificate

eFbLMwXUTe0oBXa/zz++w5XzXyWil4pgmJLggYQq+WNi5QkCFfc5y2blyu+GfH1P4AffwEG4f9JU/uOg9CnIW4F9IMzk17juVIR9s8X95vn+wN2G9vFfPyj154zuqpXHt4lMSqr10ek1wWnlPaaTlitEqOO1ZBqHU1RXmymN5IngY+E8lxtjpy7vyKO3TBAMm6sPJ1bUwkvxYIP/dj7WUtPjpPfdpu6NZYRV6gOD2lMYaQWM9Uo6wnlnob/
-----END CERTIFICATE-----

Import RSA Keys

☒

Public Key

-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAvoIkVN2vxyz3eRA1Ah9jawhrhwMFNf6ArCCg3vIjxWqMDUL69tvK5EuAizYLY/3nYjv/ea
l4RIEBydYcuQz9OQ36f9L+AUaQxnXiQjmcEaVE9xtGl/ZoJcMoZYLjFMe+NcQ1VUKA5gdAV0k8+o4N4qju
C/wa87jhRYq9VBDWOFzHD8LpG4f/r2wtj2/N08xfRNOA2qfzeL/Px4lo9RjeSsZXTDCaKmot2WaFLGjK0c
i7VMFh8ZjsOixJQDovKjniNkpguz6J21O3dPwDNw2Qtd7evsYzxQBQjpWZAlaWid7bzQxt6B7Bx0r1KuLS

Private Key

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAvoIkVN2vxyz3eRA1Ah9jawhrhwMFNf6ArCCg3vIjxWqMDUL69tvK5EuAizYLY/3nY
jv/ea4RIEBydYcuQz9OQ36f9L+AUaQxnXiQjmcEaVE9xtGl/ZoJcMoZYLjFMe+NcQ1VUKA5gdAV0k8+o4
N4qjuC/wa87jhRYq9VBDWOFzHD8LpG4f/r2wtj2/N08xfRNOA2qfzeL/Px4lo9RjeSsZXTDCaKmot2WaF
LGjK0ci7VMFh8ZjsOixJQDovKjniNkpguz6J21O3dPwDNw2Qtd7evsYzxQBQjpWZAlaWid7bzQxt6B7Bx0

CANCEL

APPLY

Table 147: Import Certificate Fields

Field	Description
Certificate	Paste the signed certificate into this text box.
Import RSA Keys	Enable if you need to import RSA keys.
Public Key	If Import RSA Keys is enabled, paste the public key to this text box.
Private Key	If Import RSA Keys is enabled, paste the private key to this text box.

View a Certificate

To view the current certificate details, click the **VIEW CERTIFICATE DETAILS** button.

Figure 179: Certificate Details

Certificate Details

×

Certificate

-----BEGIN CERTIFICATE-----
MIIDITCCAqkCEE/C42KlvGFy1h7U0tIO2L4wDQYJKoZIhvcNAQELBQAwTzELMAkG
A1UEBhMCICAxCjAIBgNVBAGMASAxCjAIBgNVBACMASAxEDAQOBgNVBAMMBzAuMC4w
LjAxCjAIBgNVBAoMASAxCjAIBgNVBAsMASAwHhcNMTkxMjAyMDEzMTU2WhcNMjAx
MjAxMDEzMTU2WjBPMQswCQYDVQGEwglDEKMAgGA1UECAwBIDEKMAgGA1UEBwwB

Public Key

-----BEGIN RSA PUBLIC KEY-----
MIIBBgKCAQEAE82ZcB/a0YaLnGWn8NbavFbpSpqebYrYMjqlvQ62J3A/nIYVK/sEdGtCEgiSjrCzXmo0Crc
N+q/Ok7hyRWcKmvLxjEhRLRBFZXgTZmMBHk4GfXs3vCb9aBBFPkCPFQby1aBPxh+HrCNK9/irvDOJZU
5EglP7wGe/6m24hh1QQDrDgDgKPTGHgCQ2w141YNmAiEegn3fYoZjkyLRqkrpfuVgR8/K1a3z8us1Wpr
R4LMNIOAqPDPI3LtjueJe/vlR3pVH/49wrlO/yrn6Bomwh/Y3JnHuO8jdbGSd53QnFBgVSuroov7dHWKtV

Private Key

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAE82ZcB/a0YaLnGWn8NbavFbpSpqebYrYMjqlvQ62J3A/nIYVK/sEdGtCEgiSjrCzXmo
0CrcN+q/Ok7hyRWcKmvLxjEhRLRBFZXgTZmMBHk4GfXs3vCb9aBBFPkCPFQby1aBPxh+HrCNK9/irvD
OJZU5EglP7wGe/6m24hh1QQDrDgDgKPTGHgCQ2w141YNmAiEegn3fYoZjkyLRqkrpfuVgR8/K1a3z8us1
WprR4LMNIOAqPDPI3LtjueJe/vlR3pVH/49wrlO/yrn6Bomwh/Y3JnHuO8jdbGSd53QnFBgVSuroov7dH

Fingerprint

52:DD:41:26:51:37:7B:81:10:B8:68:13:25:33:70:E7:9B:16:F1:98

CLOSE

Table 148: Certificate Details Fields

Field	Description
Certificate	Non-editable text box with the certificate.
Public Key	Non-editable text box with the public key.
Private Key	Non-editable text box with the private key.
Fingerprint	The public key fingerprint.

Delete a Certificate

To delete the current certificate, click the **DELETE CERTIFICATE** button.

You can use the Diagnostics pages to help troubleshoot network issues, view log and configuration information.

Logging

To configure log setting and display the Logging page, click **Diagnostics > Logging** in the navigation pane.

Unexpected Restart Information

The **Unexpected Restart Information** tile appears only if an unexpected restart that hasn't been cleared is registered on the switch. When an unexpected restart has occurred a notification appears on the masthead. When this notification icon is clicked, the application navigates to this page.

If there has been an unexpected restart of the switch, additional information is displayed near the top of the Logging page to alert the user of the event. The Crash Log text box displays information about the restart event, which may be helpful to technical support in diagnosing its cause. The crash log is part of the Log File entries (see [Log File Tab](#) for more information). The file stored into non-volatile memory so that it is preserved upon reboot.

When the switch is reset to factory defaults, all crash log information is erased.

Figure 180: Unexpected Restart Information Tile



To clear the unexpected restart alert, click **Clear Unexpected Restart** this clears the unexpected restart notification from the masthead, and the **Unexpected Restart Information** tile. You can click **Save Crash Log** to save the contents of the crash log to a text file using the browser save functionality.

Global Log Settings

Use this tile to define buffered logging settings. These log messages are not preserved across device reboots.

Figure 181: Global Log Settings

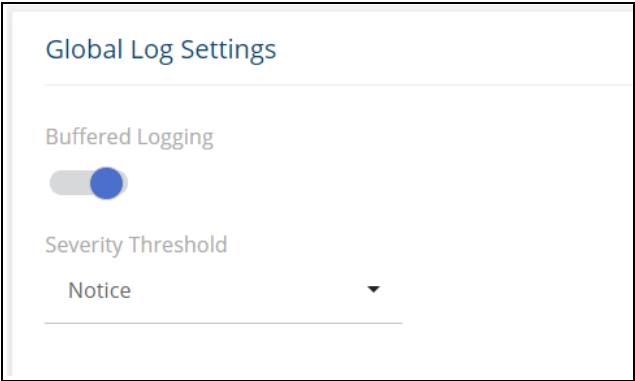


Table 149: Global Log Settings Fields

Field	Description
Buffered Logging	Enable or disable buffered logging.
Severity Threshold	<p>Choose the appropriate severity threshold from the drop-down button. The severity can be one of the following (lowest to highest):</p> <ul style="list-style-type: none">• Debug—The switch is providing debug-level information.• Info—The switch is providing non-critical information. This is the default level.• Notice—The switch is experiencing normal but significant conditions.• Warning—The switch is experiencing conditions that require user attention.• Error—The switch is experiencing non-urgent failures.• Critical—The switch is experiencing primary system failures.• Alert—Action must be taken immediately.• Emergency—The switch is unusable. <p>When selecting a certain severity threshold the switch will provide that severity and all higher severity.</p>

Remote Log Server

Use this tile to enable logging messages to a remote SYSLOG server, and to define the server address and other settings.

Figure 182: Remote Log Server

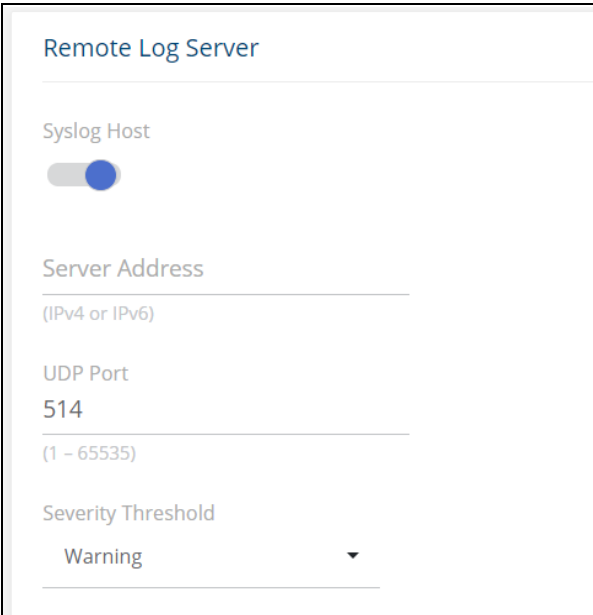


Table 150: Remote Log Server Fields

Field	Description
Syslog Host	Enables and disables logging to configured syslog host. When the syslog admin mode is disabled, the switch does not relay logs to syslog host. When enabled, messages are sent to configured host. This feature is disabled by default
Server Address	The IP address of the remote host that receives the log messages. The address can be one of the following: <ul style="list-style-type: none"> IPv4 address IPv6 global address, in the format of X:X:X::X
UDP Port	The UDP port, on the logging host, to send syslog messages. The port ID can be any value from 1 to 65535. The default is 514
Severity Threshold	Choose the appropriate severity threshold from the drop-down button. See descriptions for the available levels in Global Log Settings Fields

Buffered Log/Log File

To view the Buffered Log information, click the **Buffered Log** tab.

To view the Log File information, click the **Log File** tab.

Buffered Log Tab

The log messages that the switch generates in response to events, faults, errors, and configuration changes are stored locally on the switch in the RAM (cache). This collection of log files is called the buffered log. When the buffered log file reaches the maximum size, the oldest message is deleted from the RAM when a new message is added. If the system restarts, all messages are cleared. The Log page displays the 1000 most recent system messages, such as configuration failures and user sessions. The newest log entry, by default, is displayed at the top of the list.

To view this tab, click **Diagnostics > Logging** in the navigation pane, and click the **Log File** tab in the **Buffered Log/Log File** Tile.

Figure 183: Buffered Log Tab

Buffered Log		Log File			  Display: 10  
Index ▲	Log Time	Severity	Component	Description	
1	Oct 7 2021 01:08:25	Notice	SYSLOG-N-LOGGING	Logging started.	
2	Oct 7 2021 01:08:13	Info	BOOTP_DHCP_CL-I- DHCPCONFIGURED	The device has been configured on interface Vlan 1 , IP 10.5.227.151, mask 255.255.255.224, DHCP server 10.5.227.131	

Table 151: Buffered Log Tab Fields

Field	Description
Index	The log number.
Log Time	Time at which the log was created.
Severity	<p>The severity level associated with the log message. The severity can be one of the following:</p> <ul style="list-style-type: none"> Emergency—The switch is unusable. Alert—Action must be taken immediately. Critical—The switch is experiencing primary system failures. Error—The switch is experiencing non-urgent failures. Warning—The switch is experiencing conditions that require user attention. Notice—The switch is experiencing normal but significant conditions. Info—The switch is providing non-critical information. Debug—The switch is providing debug-level information.
Component	The system component that issued the log entry.
Description	A text description of the event.

Click **Clear**  to delete all log messages. You may be required to confirm the delete before the logs are removed.

For information on configuring log settings, see [Global Log Settings](#).

Log File Tab

The system sends logging messages to the local flash (Log file). When using this feature, all events with error level and higher are logged to a flash Log file and will be available for viewing even after system reboot.

When the log file reaches the maximum size, the oldest message is deleted from the flash when a new message is added.

To view this tab, click **Diagnostics > Logging** in the navigation pane, and click the **Log File** tab in the **Buffered Log/Log File** Tile.

Figure 184: Log File Tab**Table 152: Log File Tab Fields**

Field	Description
Index	The log number.
Log Time	Time at which the log was created.

Field	Description
Severity	<p>The severity level associated with the log message. The severity can be one of the following:</p> <ul style="list-style-type: none"> • Emergency—The switch is unusable. • Alert—Action must be taken immediately. • Critical—The switch is experiencing primary system failures. • Error—The switch is experiencing non-urgent failures. • Warning—The switch is experiencing conditions that require user attention. • Notice—The switch is experiencing normal but significant conditions. • Info—The switch is providing non-critical information. • Debug—The switch is providing debug-level information.
Component	The system component that issued the log entry.
Description	A text description of the event.

Click **Clear**  to delete all log messages. You may be required to confirm the delete before the logs are removed.

Ping

A ping request is an Internet Control Message Protocol (ICMP) echo request packet. The switch supports both ICMP for sending ping requests to IPv4 addresses and ICMPv6 for sending ping requests to IPv6 addresses.

IPv4/IPv6

To view the IPv4 information, click the **IPv4** tab.

To view the IPv6 information, click the **IPv6** tab.

IPv4 Tab

Use the IPv4 tab to send one or more ping requests from the switch to a specified IPv4 address. You can use the ping request to check whether the switch can communicate with a particular host on an IP network. The information you enter on this page is not saved as part of the switch configuration.

To display the IPv4 tab, click **Diagnostics > Ping** in the navigation pane, and ensure the **IPv4** tab is selected.

Figure 185: IPv4 Tab

IPv4IPv6

IP Address

IPv4 or Host Name

Count

3

(1 - 15)

Timeout

3

(1 - 60) Seconds

Interval

1000

(200 - 65535) Milliseconds

Size

64

(64 - 1518) Bytes

Source

☒ None

☐ IP Address

☐ Interface

Source IP Address

(x.x.x.x)

Source Interface

VLAN 1

Table 153: IPv4 Fields

Field	Description
IP Address	Specify the IP address you want to reach.
Count	Specify the number of packets to send. The range is 1 to 15 packets and the default is 3 packets.
Timeout	The number of seconds to wait for a reply to a ping before considering the request as Timed out.
Interval	The number of milliseconds between receiving a response to a ping (be it a success or a timeout), and sending the next ping. The range is 200-65535 milliseconds, and the default is 1000 milliseconds.
Size	Specify the size of the ping packet to be sent. Changing the size allows you to troubleshoot connectivity issues with a variety of packet sizes. The range is from 0 to 1518 bytes, and the default is 64 bytes.
Source	The source IP address or interface to use when sending a ping request which can be one of the following: <ul style="list-style-type: none">None – No specific source is required.IP Address – Use the IP address specified in the Source IPv4 Address field as the source.Interface – Use the specified switch interface as a source.
Source IP Address	The source IP address to use when sending a ping request. This field is enabled when IP Address is selected as the source option.
Source Interface	The interface to use when sending a ping request. This field is enabled when Interface is selected as the source option. The default interface to use is the network port.

Click **APPLY** to ping the specified host. Click **Stop Ping** to end a ping in progress. If you do not click **Stop Ping**, the pings continue until the number of pings specified in the Count field has been reached — even if you navigate away from the Ping page.

The results of the ping operation can be viewed in the [Ping Results](#) tile.

IPv6 Tab

Use the Ping IPv6 tab to send one or more ping requests from the switch to a specified IPv6 address. You can use the ping request to check whether the switch can communicate with a particular host on an IPv6 network. The information you enter on this page is not saved as part of the switch configuration.

To display the Ping IPv6 tab, click **Diagnostics > Ping** in the navigation pane, and then click the **IPv6** tab.

Figure 186: IPv6 Tab

IPv4

IPv6

IP Address

(xxxxxxxxxxxx)

Count

3

(1 – 15)

Timeout

3

(1 – 60) Seconds

Interval

1000

(200 – 65535) Milliseconds

Size

68

(68 – 1518) Bytes

Table 154: IPv6 Fields

Field	Description
IP Address	Enter the global or link-local IPv6 address to ping.
Count	Specify the number of packets to send. The range is 1 to 15 packets and the default is 3 packets.
Timeout	The number of seconds to wait for a reply to a ping before considering the request as Timed out.
Interval	The number of milliseconds between receiveing a response to a ping (be it a success or a timeout), and sending the next ping. The range is 200-65535 milliseconds, and the default is 1000 milliseconds.
Size	Specify the size of the ping packet to be sent. Changing the size allows you to troubleshoot connectivity issues with a variety of packet sizes. The range is from 68 to 1518 bytes, and the default is 68 bytes.

Click **APPLY** to ping the specified host. Click **Stop Ping** to end a ping in progress. If you do not click **Stop Ping**, the pings continue until the number of pings specified in the Count field has been reached — even if you navigate away from the Ping page.

The results of the ping operation can be viewed in the [Ping Results](#) tile.

Ping Results

This tile shows the Ping status and results.

Table 155: Ping Results Fields

Field	Description
Status	The current status of the ping test, which can be one of the following: <ul style="list-style-type: none">• Not Started—The ping test has not been initiated since viewing the page.• In Progress—The ping test has been initiated and is running.• Done—The test has completed, and information about the test is displayed in the Results area.
Results	The results of the ping test, which includes the following information: <ul style="list-style-type: none">• The IP address of the switch that was pinged.• The Internet Control Message Protocol (ICMP) number of the packet, starting from 1.• The time it took to receive a reply, in microseconds.• The number of ping packets sent and received, the percent of packets that were lost, and the minimum, average, and maximum round-trip time for the responses in milliseconds.

Traceroute

Traceroute is a diagnostic tool that provides information about the route a packet takes from the switch to a specific IPv4 or IPv6 address as well as the amount of time it takes for the packet to reach its destination.

IPv4/IPv6

To view the IPv4 information, click the **IPv4** tab.

To view the IPv6 information, click the **IPv6** tab.

IPv4 Tab

Use this tab to determine the Layer 3 path a packet takes from the switch to a specific IP address. When you initiate the traceroute command by clicking the **Apply** button, the switch sends a series of traceroute probes toward the destination. The results list the IP address of each layer 3 switch a probe passes through until it reaches its destination - or fails to reach its destination and is discarded. The information you enter on this page is not saved as part of the switch configuration.

To display the Traceroute IPv4 tab, click **Diagnostics > Traceroute** in the navigation pane, and ensure the **IPv4** tab is selected.

Figure 187: IPv4 Tab

IPv4IPv6

IP Address

(x.x.x.x)

Probes Per Hop

3

(1 - 10)

Max TTL

30

(1 - 255)

Interval

3

(1 - 60) Seconds

Size

64

(64 - 1518) Bytes

Source

☒ None

☐ IP Address

☐ Interface

Table 156: IPv4 Fields

Field	Description
IP Address	The IP address of the system to attempt to reach.
Probes Per Hop	Traceroute works by sending UDP packets with increasing Time-To-Live (TTL) values. Specify the number of probes sent with each TTL.
Max TTL	The maximum TTL. The traceroute terminates after sending probes that can be layer 3 forwarded this number of times. If the destination is further away, the traceroute will not reach it.
Timeout	The number of seconds to wait for a reply to a traceroute before considering the request as Timed out.
Size	The size of probe payload in bytes.
Source	The source to use when sending the traceroute, which can be one of the following: <ul style="list-style-type: none">None – No source is required.IP Address – Use the IP address specified in the Source IPv4 Address field as the source.Interface – Use the specified switch interface as a source.
Source IP Address	The source IPv4 address to use when sending the traceroute. This field is enabled when IP Address is selected as source option.
Source Interface	The source interface to use when sending the traceroute. This field is enabled when Interface is selected as source option.

Click **APPLY** to send the traceroute to the specified host and **Stop Traceroute** to end a traceroute in progress.

The Trace Operation status and results are displayed in the **Traceroute Results** pane.

IPv6 Tab

Use this tab to determine the Layer 3 path a packet takes from the switch to a specific IPv6 address. When you initiate the traceroute command by clicking the **Apply** button, the switch sends a series of traceroute probes toward the destination. The results list the IPv6 address of each Layer 3 switch a probe passes through until it reaches its destination - or fails to reach its destination and is discarded. The information you enter on this page is not saved as part of the switch configuration.

To display the Traceroute IPv6 tab, click **Diagnostics > Traceroute** in the navigation pane, and click the **IPv6** tab.

Figure 188: IPv6 Tab

IPv4

IPv6

IP Address

(XXXXXXXXXXXX)

Probes Per Hop

3

(1 – 10)

Max TTL

30

(1 – 255)

Interval

3

(1 – 60) Seconds

Size

68

(68 – 1518) Bytes

Table 157: IPv6 Fields

Field	Description
IP Address	The IPv6 address of the system to attempt to reach.
Probes Per Hop	Traceroute works by sending UDP packets with increasing Time-To-Live (TTL) values. Specify the number of probes sent with each TTL.
Max TTL	The maximum TTL. The traceroute terminates after sending probes that can be layer 3 forwarded this number of times. If the destination is further away, the traceroute will not reach it.
Timeout	The number of seconds to wait for a reply to a traceroute before considering the request as Timed out.
Size	The size of probe payload in bytes.

Click **APPLY** to send the traceroute to the specified host and **Stop Traceroute** to end a traceroute in progress.

The Trace Operation status and results are displayed in the Traceroute Results pane.

Traceroute Results

Table 158: Traceroute Results Fields

Field	Description
Status	The current status of the traceroute, which can be: <ul style="list-style-type: none">• Not Started – The traceroute has not been initiated since viewing the page.• In Progress – The traceroute has been initiated and is running.• Done – The traceroute has completed, and information about the traceroute is displayed in the Results area.
Results	The results of the traceroute are displayed.

Support File

Use the support file page to display summary information for the switch on a single page.

To display the Support File page, click **Diagnostics > Support File** in the navigation pane and click the **GENERATE SUPPORT INFORMATION** button. The [Support File Page](#) shows a partial view of the resulting information.



Generating the support file may take several minutes. During this time switch management will not be available.

Figure 189: Support File Page

Support File

[GENERATE SUPPORT INFORMATION](#)[DOWNLOAD AS TEXT](#)

System Information

System Name

SwitchA

System Location

AIO

System Contact

Admin

System Time

Current Time

11:00:30 January 03 2022

System Up Time

0 days, 20 hours, 46 minutes 31 seconds

The support file page includes the following information:

- System Information—A system description, name, location, and contact information, along with date and time information.
- System Time—Current Time and System Up Time.
- Device Information—Software and OS versions.
- System Resource Usage—CPU and memory usage data.
- Image Status and Image Description—The active and backup image status and versions.
- Buffered Log and Configuration—Messages and logging configuration details.
- Syslog Configuration—Syslog status and remote port and address information.
- Locator LED Configuration—Locator LED status.
- MAC Table—Address forwarding table and summary statistics.
- Time Configuration and Time Zone—SNTP client status and time zone configuration.
- Daylight Saving Time—The daylight saving time mode on the system.
- Date Range and Recurring Date—Configuration of the date range or recurring date.
- Network Details—Switch IP and MAC addresses.
- Web Parameters and Management Access—Web session timeout and access port and management VLAN information.

- User Accounts and Passwords—User access, logged-in users, and password manager configuration.
- Port Status and Port Summary Statistics—Port and trunk configuration details, summary, and statistics.
- Port Mirroring Configuration—Enable/disable status and source and destination port configuration
- Flow Control and Storm Control Configuration—Enable/disable status.
- Spanning Tree Switch Configuration—Global and per-port configuration, status, and statistics.
- Loop Protection Configuration and Status—Per interface configuration and statistics
- IGMP Snooping—Enable/disable information and statistics
- SNMP—SNMP v1/v2/v3 information.
- Auto Recovery Components and Configuration —Enable/disable status of auto recovery by supported feature and recovery time
- VLAN Configuration—Configured VLANs, VLAN port membership, and VLAN port configuration.
- Auto Voice VLAN Configuration—Voice VLAN settings.
- Trunk Configuration and Trunk Statistics—Trunk configuration details and flap count statistics
- LLDP and LLDP-MED Configuration—Global settings and per-port LLDP configuration and activity
- Routing IP—Routing IP configuration, interface configuration, statistics, and IP route summary.
- DHCP Relay—Configuration and statistics.
- ARP Table—Summary, configuration, and statistics.
- Access Control List—Configuration, summary (global, interface, and VLAN), and statistics.
- CoS—802.1p CoS mapping per interface, DSCP CoS global mapping configuration, CoS trust configuration, CoS interface queue configuration.
- Auto DoS Features—Enable/disable status.
- ICMP Settings—Global ICMP configuration.
- RADIUS—RADIUS authentication and accounting configuration, status, and statistics.
- Port Access Control—Global settings and per-port Authentication control and status
- Port Security—Global enable/disable status, per-port status, and Static and Dynamic MAC addresses.
- Protected Ports Configuration—Configured groups and protected ports.
- Green Features (EEE) Configuration—Global and per-port enable/disable status and power consumption data
- PoE Configuration—On switches that support PoE, global and per-port configuration and schedule settings.

Support file information can be saved and downloaded to management system using the native browser file system. The name of the downloaded file is SupportFile.htm.

To download the support file, click the **DOWNLOAD AS TEXT** button. This button is only displayed after the support information is gathered and shown on the screen.

Cable Test

This feature detects and reports potential cabling issues, such as cable opens, or cable shorts, on Copper Links. This feature also provides the distance to the fault if exists, and total length of cable.

Cable length measurement is available when link is up. Length is automatically detected. A length report has a minimum length of 50 meter and is provided with a 30 meter range (up to 50, 50 to 80, 80 to 110, longer than 110).



Only short circuits across wires within a pair are reported. If there is a short circuit across wires not in a pair, it will not be reported.

To display the Cable Test page, click **Diagnostics > Cable Test** in the navigation pane.

Interface Configuration

This tile shows the interface configuration of the cables.

Figure 190: Interface Configuration

Interface Configuration				
☐	Interface	▲ Test Result	Distance to Fault	Last Update
☐	1			14-Dec-2021 07:43:30
☐	2			
☐	3	Ok		14-Dec-2021 07:43:31
☐	4			
☐	5	No Cable		14-Dec-2021 07:38:34
☐	6	No Cable		14-Dec-2021 07:38:42
☐	7	Short	11m	14-Dec-2021 07:38:50

To run a test, select one or more interfaces and click the **Test**  button.

Before the cable test runs, you will see a Port Cable Test Warning message:

While being tested, ports are briefly shut down. Would you like to continue?

Click **OK** to continue, click **CANCEL** to cancel the cable test.



Cable status test requires activation, per-interface by user. Activation of the test will cause link down state for a few milliseconds.

Table 159: Interface Configuration Fields

Field	Description
Interface	The interface ID.
Test Result	This field appears only after a test was run on the interface. These are the test result options: <ul style="list-style-type: none">• OK• No Cable• Short• Open Cable• Unknown
Distance to Fault	This field appears only after a test was run on the interface. In the case of a fault, this column shows the distance to the fault.
Last Update	This field appears only after a test was run on the interface. The last time a test was activated on this interface.

Field	Description
Cable Length	Length reports has a minimum length of 50 meters and provides a 30 meter resolution (up to 50, 50 to 80, 80 to 110, and so on) NOTE: Cable length info is not available for interfaces with traffic rates below 1 Gbps.
Port Status	Displays the current port status.

MAC Table

The MAC address table keeps track of the Media Access Control (MAC) addresses associated with each port. This table enables the switch to forward unicast traffic through the appropriate port. The MAC address table is sometimes called the bridge table or the forwarding database. The address table supports up to 16K MAC address entries for all the port devices.

To display the MAC Table page, click **Diagnostics > MAC Table** in the navigation pane.

Global Configuration

This tile shows the MAC table global configuration. To configure a setting select it, enter the new configuration and click **APPLY**.

Figure 191: Global Configuration

Global Configuration

Maximum Addresses Supported
16384

MAC Address Aging Interval
300
(10 - 400) Seconds

Table 160: Global Configuration Fields

Field	Description
Maximum Addresses Supported	The maximum number of MAC address entries that can be learned on the switch.
MAC Address Aging Interval	The MAC address table (forwarding database) contains static entries, which never age out, and dynamically-learned entries, which are removed if they are not updated within a given time. Specify the number of seconds a dynamic address should remain in the MAC address table after it has been learned.

MAC Address Table

Figure 192: MAC Address Table Tile

MAC Address Table					
VLAN ID	MAC Address	Interface	Interface Index	Status	
1	00:00:00:11:11:11	47	47	Learned	
1	00:00:44:44:55:88	CPU	0	Management	
1	00:22:12:52:03:77	47	47	Learned	

Table 161: MAC Address Table Fields

Field	Description
VLAN ID	The VLAN with which the MAC address is associated.
MAC Address	A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a six-byte MAC address, with each byte separated by colons.
Interface	The port where this address was learned. The port identified in this field is the port through which the MAC address can be reached. <i>CPU</i> is a special source port used for internal management on the switch.
Interface Index	The Interface Index of the MIB interface table entry associated with the source port. This value helps identify an interface when using SNMP to manage the switch.
Status	Provides information about the entry and why it is in the table. Possible values are the following: <ul style="list-style-type: none">• Learned—The address has been automatically learned by the switch and can age out when it is not in use. Dynamic addresses are learned by examining information in incoming Ethernet frames.• Management—The burned-in MAC address of the switch.• Static — The MAC address was added manually by the system administrator.• Other—The address was added dynamically through an unidentified protocol or method.

RMON

Remote Monitoring (RMON) is an extension to the Simple Network Management Protocol (SNMP) that provides comprehensive network monitoring capabilities. In standard SNMP, the switch has to be queried to obtain information. RMON is proactive and can set alarms on a variety of traffic conditions, including specific types of errors. The RMON standard is an SNMP MIB definition described in RFC 1757 for Ethernet.

The following RMON groups are supported:

- RMON Statistics (Group 1)
- History (Group 2)
- Events (Group 9)
- Alarms (Group 3)

Each group is detailed below.

RMON Statistics

The RMON (Ethernet) statistics are counts of packets, octets (or bytes), broadcasts, multicasts and collisions on the local segment, as well as the number of occurrences of dropped packets by the agent.

Figure 193: RMON Statistics

RMON Statistics						
<div> <div></div> <div></div> <div></div> <div></div> <div>Display: 10</div> <div></div> </div>						
Interface	▲	Bytes Received	Frames	Packets Received	Drop Events	Errors
☐ 1		67388	1005459	485	0	0
☐ 2		3353	1005001	26	0	0
☐ 3		135441940	1005130	1005102	0	0

Table 162: RMON Statistics Fields

Field	Description
Interface	The interface identifier.
Bytes Received	Total number of octets of data (including those in bad packets) received on the interface (excluding framing bits but including FCS octets).
Frames	The total number of frames sent and received on the interface. The frame count includes only frames sizes of 64 bytes to max size allowed on interface (2048 bytes).
Packets Received	Total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Drop Events	Total number of events in which packets were dropped by the interface due to lack of resources. Note that this number is not necessarily the number of packets dropped. It is the number of times this condition was detected.
Errors	Total number of packets received on the interface with an Error.

Select an interface and click **Details**  to see a breakdown of the various types of frames by frame size, and error frames by error type.

Table 163: RMON Statistics Details Fields

Field	Description
Interface	The interface identifier.
Bytes Received	Total number of octets of data (including those in bad packets) received on the interface (excluding framing bits but including FCS octets).
Drop Events	Total number of events in which packets were dropped by the interface due to lack of resources. Note that this number is not necessarily the number of packets dropped. It is the number of times this condition was detected.
Rx Packets	The number of packets of all types received on the interface during the sample time.
Rx Broadcast Packets	The number of Broadcast packets received on the interface during the sample time.
Rx Multicast Packets	The number of Multicast packets received on the interface during the sample time
CRC/Align Errors	The number of packets with a CRC Align error received on the interface during the sample time.
Undersize Packets	The number of Undersize packets received on the interface during the sample time.
Oversize Packets	The number of Oversize packets received on the interface during the sample time.
Fragments	The number of fragment type packets received on the interface during the sample time.
Jabbers	The number of Jabber type packets received on the interface during the sample time.
Collisions	The estimated number of collisions which occurred on the interface during the sample time.

Field	Description
64 Byte Frames	Total number of packets (including bad packets) received that are 64 byte frames in length (excluding framing bits but including FCS byte frames).
65 – 127 Byte Frames	Total number of packets (including bad packets) received that are between 65 and 127 byte frames in length inclusive (excluding framing bits but including FCS byte frames).
128 – 255 Byte Frames	Total number of packets (including bad packets) received that are between 128 and 255 byte frames in length inclusive (excluding framing bits but including FCS byte frames).
256 – 511 Byte Frames	Total number of packets (including bad packets) received that are between 256 and 511 byte frames in length inclusive (excluding framing bits but including FCS byte frames).
512 – 1023 Byte Frames	Total number of packets (including bad packets) received that were between 512 and 1023 byte frames in length inclusive (excluding framing bits but including FCS byte frames).
1024 Byte or Larger Frames	Total number of packets (including bad packets) received that were between 1024 byte frames and the maximum frame size in length inclusive (excluding framing bits but including FCS byte frames).

Select an interface and click **Clear**  to clear the RMON and interface statistics from the selected interface.

Click **Clear All**  to clear the RMON and interface statistics from all the interfaces.

History Collectors/Log

The History group provides historical views of the statistics provided in the Statistics group, with the exception of frame size counters which are provided only on a real-time basis. Up to 300 entries can be displayed.

To view the History Collector information, click the **History Collectors** tab.

To view the History Log information, click the **History Log** tab.

History Collectors Tab

Use the History Collectors tab to define the ID and parameters of the History info to view. Only Collector IDs that were defined in the History Collector tab are available.

Figure 194: History Collectors Tab

History Collectors	History Log					Display: 10 	
☐	Entry ID	▲	Source Interface	Bucket Size	Sampling Interval	Owner	Samples Logged
Table Is Empty							

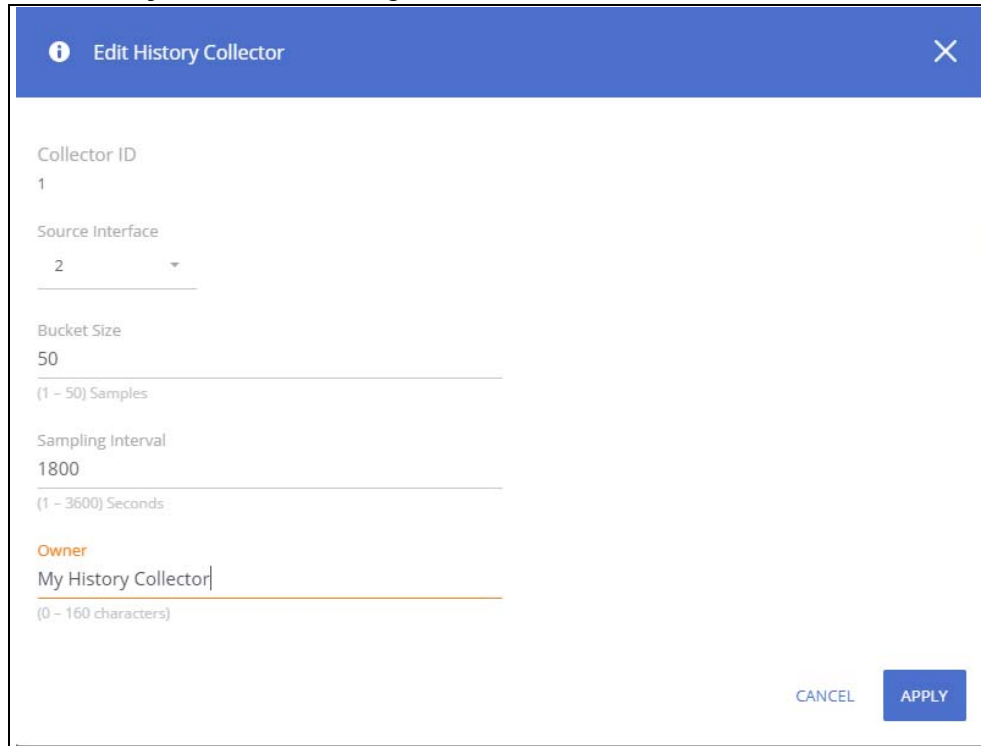
Table 164: History Collectors Fields

Field	Description
Entry ID	The entry identifier.
Source Interface	The source interface (port or LAG) to sample in this entry.
Bucket Size	The number of samples to store. Range: 1 - 50, default: 50

Field	Description
Sampling Interval	The number of seconds in each polling cycle. Range: 1-3600, default: 1800
Owner	The name of the owner of the RMON group of statistics. This parameter is optional and can be left empty.
Samples Logged	The granted number of samples to be saved. this field is updated by system and cannot be configured by the user.

To add a collector, click **Add** . The **Add History Collector** dialog box appears.

Figure 195: Edit History Collector Dialog Box



The dialog box titled "Edit History Collector" contains the following fields:

- Collector ID:** 1
- Source Interface:** 2 (dropdown menu)
- Bucket Size:** 50 (range: 1 - 50) Samples
- Sampling Interval:** 1800 (range: 1 - 3600) Seconds
- Owner:** My History Collector (range: 0 - 160 characters)

Buttons: CANCEL, APPLY

Enter the appropriate fields as needed.

To edit an existing collector, click the check box to the left of the collector entry and click **Edit** . The **Edit History Collector** dialog box appears.

To remove an existing collector, click the check box to the left of the collector entry and click **Remove** .

History Log Tab

Use the History Log tab to view the information itself (based on the definition in the History Collector tab). For more information on the log types, see [RMON Statistics](#).

Figure 196: History Log Tab

History Collectors		History Log											
History Collector ID													
1													
Sample Number	▲	Drops	Rx Bytes	Rx Packets	Broadcast Packets	Multicast Packets	CRC Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Utilization
42		0	0	0	0	0	0	0	0	0	0	0	0%
43		0	0	0	0	0	0	0	0	0	0	0	0%
44		0	0	0	0	0	0	0	0	0	0	0	0%

Table 165: History Log Fields

Field	Description
History Collector ID	The ID of the history collector. Click the drop-down to select the collector to view.
Sample Number	The ID of the sample related to info in this row.
Drops	The number of drop events which occurred on the interface during the sample time.
Rx Bytes	The number of bytes received on the interface during the sample time.
Rx Packets	The number of packets of all types received on the interface during the sample time.
Broadcast Packets	The number of broadcast packets received on the interface during the sample time.
Multicast Packets	The number of Multicast packets received on the interface during the sample time
CRC Align Errors	The number of packets with a CRC Align error received on the interface during the sample time.
Undersize Packets	The number of Undersize packets received on the interface during the sample time.
Oversize Packets	The number of Oversize packets received on the interface during the sample time.
Fragments	The number of fragment type packets received on the interface during the sample time.
Jabbers	The number of Jabber type packets received on the interface during the sample time.
Collisions	The estimated number of collisions which occurred on the interface during the sample time.
Utilization	Average port utilization during the sample time.

RMON Events/Event Log

The Events group provides the capability for users to generate events entries as logs, SNMP traps or both to the management station. Events can originate from a crossed threshold on any counter or administrative events from the agent, such as a power failure or reset. The trigger for each event is defined in the Alarm group (see **RMON Alarms**). The log includes the time of day for each event and a description of the event.

To view the RMON Events information, click the **RMON Events** tab.

To view the Events Log information, click the **Event Log** tab.

RMON Events Tab

Use the RMON Events tab to configure ID and settings of events (RMON Events).

Figure 197: RMON Events

RMON EventsEvent Log

Display: 10

<div></div>	Entry ID	Description	Community	Owner	Log Event	Trap	Last Occurrence
Table Is Empty							

Table 166: RMON Events Fields

Field	Description
Entry ID	The entry identifier. Range is 1-65535
Description	A description of this event.
Community	The SNMP community string to be included when traps are sent to SNMP Manager.
Owner	The name of the owner of the RMON group of statistics. This parameter is optional and can be left empty.
Log Event	Enable or disable logging events. If set to enable, adds an entry to the RMON Event Log table when an alarm is triggered.
Trap	Enable or disable setting a trap. If set to enable, sends a trap to the remote log server and SNMP Manager when an alarm is triggered.
Last Occurrence	The last time an event defined by this entry occurred.

To add an Event, click **Add**  . The **Add RMON Event** dialog box appears:

 Add RMON Event 

Event ID

1

(1 – 65535)

Description

new RMON Event

(0 – 127 characters)

Community

2

(0 – 127 characters)

Owner

My Event

(0 – 160 characters)

Log Event

☒

Trap

☒

CANCEL

APPLY

Enter the appropriate fields as needed.

To edit an existing event, click the check box to the left of the event entry and click **Edit**  . The **Edit RMON Event** dialog box appears.

To remove an existing event, click the check box to the left of the event entry and click **Remove**  .

Event Log Tab

Use the Event Log tab to view the event log. The Event Log displays the log of RMON events (actions) that were triggered (occurred).

Figure 198: RMON Event Log

RMON Events		Event Log			
Event ID ▲	Log ID	Log Time	Description		
1	2	Dec 11 2019 19:34:58	MIB Var.: 1.3.6.1.2.1.2.2.1.10.48 , Absolute , Rising , Actual Val: 66855353 , Thresh.Set:		
1	5	Dec 11 2019 19:43:23	MIB Var.: 1.3.6.1.2.1.2.2.1.16.48 , Absolute , Rising , Actual Val: 54945670 , Thresh.Set:		

Table 167: RMON Event Log Fields

Field	Description
Event ID	The ID of the event which is configured for the triggered alarm.
Log ID	The Log ID within the specific event.
Log Time	Time that the log entry occurred.
Description	Description of the alarm that triggered the event.

RMON Alarms

The Alarms group provides a mechanism for setting thresholds and sampling intervals to generate events on any RMON counters or any other SNMP object counter maintained by the agent. Both the rising and falling thresholds must be configured. After a rising threshold is crossed, another rising event is not generated until the matching falling threshold is crossed. The alarm also indicates the action to be taken if the threshold is crossed.

Figure 199: RMON Alarms

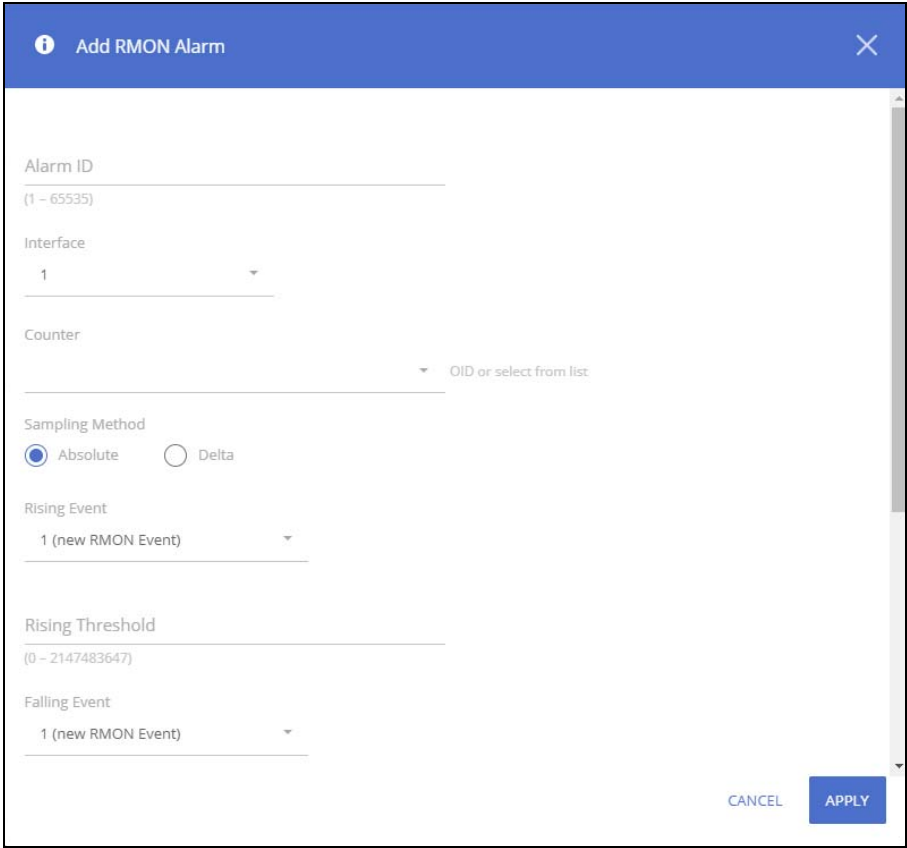
RMON Alarms									
☐	Alarm ID ▲	Interface	Counter	Sampling Method	Current Value	Rising Threshold	Rising Event	Falling Threshold	
Table Is Empty									

Table 168: RMON Alarms Fields

Field	Description
Alarm ID	The alarm identifier.
Interface	the switch interface on which the Alarm is applied.

Field	Description
Counter	Counter type (from list) to sample.
Sampling Method	The sampling method: <ul style="list-style-type: none"> Absolute - Specifies that the selected variable value is compared directly with the threshold at the end of the sampling interval. Delta - Specifies that the selected variable value of the previous sample is subtracted from the current value, and the difference is compared with the threshold.
Current Value	The current value of the counter.
Rising Threshold	Specifies the value which triggers the rising event Range: 1-2147483647
Rising Event	Specifies the ID of the event triggered when a rising threshold is crossed. The ID is displayed with the description configured for this event. Range: 0-65535 - Only created events are available for selection.
Falling Threshold	Specifies the value which triggers the falling event. Range: 0-2147483647
Falling Event	Specifies the index of the event triggered when a rising threshold is crossed. The ID is displayed with the description configured for this event. Range: 1-65535 - Only created events are available for selection.
Startup Alarm	Defines the type of event that will first trigger this alarm: <ul style="list-style-type: none"> Rising and Falling (the default) - Either rising or falling event can first trigger this alarm Rising - this event can be first triggered by the defined rising event Falling - this event can be first triggered by the defined falling event
Interval	The interval in seconds during which the data is sampled and compared with rising and falling thresholds. Range: 1-2147483647 seconds.
Owner	The name of the owner of the RMON alarm. This parameter is optional and can be left empty.

To add an Alarm, click **Add**  .



The dialog box is titled "Add RMON Alarm" with an information icon on the left and a close icon on the right. It contains the following fields and controls:

- Alarm ID**: A text input field with a range "(1 - 65535)".
- Interface**: A dropdown menu with "1" selected.
- Counter**: A dropdown menu with a placeholder "OID or select from list".
- Sampling Method**: Two radio buttons, "Absolute" (selected) and "Delta".
- Rising Event**: A dropdown menu with "1 (new RMON Event)" selected.
- Rising Threshold**: A text input field with a range "(0 - 2147483647)".
- Falling Event**: A dropdown menu with "1 (new RMON Event)" selected.
- At the bottom right, there are two buttons: "CANCEL" and "APPLY".

To edit an existing alarm, click the check box to the left of the alarm entry and click **Edit**  . The **Edit RMON Alarm** dialog box appears.

Enter the appropriate fields as needed in the **Add/Edit RMON Alarm** dialog box.

To remove an existing alarm, click the check box to the left of the alarm entry and click **Remove**  .

You can use the maintenance pages to upgrade software, save the switch configuration, and select which of two software images is the active image and which is the backup image.

Dual Image Configuration

The switch can store up to two software images. One image is the active image and the other is the backup image (not actively running on the switch). You can select which image to load during the next boot cycle and add a description for each image on the switch.

To display the Dual Image Configuration page, click **Maintenance > Dual Image Configuration**.

Figure 200: Dual Image Configuration Page

The screenshot shows the 'Dual Image Configuration' page. It contains the following fields and options:

- Dual Image Configuration** (Section Header)
- Active Image Version**: 2.5.0
- Active Image Description**: (0 - 60 characters)
- Backup Image Version**: 2.5.0
- Backup Image Description**: (0 - 60 characters)
- Next Active Image**:
 - ☒ Active (2.5.0)
 - ☐ Backup (2.5.0)

Table 169: Dual Image Configuration Fields

Field	Description
Active Image Version	The version ID of the Active image
Active Image Description	Description of the Active image.
Backup Image Version	The version ID of the Backup image.

Field	Description
Backup Image Description	Description of the Backup image.
Next Active Image	The firmware image that will become active the next time the switch is rebooted. To make the current backup image the active image, select Backup, then reboot the switch. When a new image is loaded to the Backup Image, the Backup Image automatically becomes the next active image.

Click **APPLY** to save your changes to the switch.

Backup and Update Files

The Backup and Update page enables you to save a backup of the switch's image, configuration files or error log (transfer a file from the switch), or update the switch firmware and configuration files (transfer a file to the switch), from a remote system.

Files can be backed up and updated using HTTP, TFTP, or SCP protocols.

Secure Copy Protocol (SCP) is a protocol which allows secure file transfer between hosts on the network. SCP runs over TCP port 22, and uses SSH for data transfer and authentication thereby ensuring confidentiality of transferred data.

The switch acts as an SCP client and it can send or receive files to/from an SCP server. The switch uses user-name and password credentials to authenticate to the SCP server.

To display this page, click **Maintenance > Backup and Update Files** in the navigation pane. You need to use the **Next** ➤ and **Back** ◀ buttons to complete the various fields and start the transfer process. These are the steps for filling in the backup or update operation:

1. Select the Operation Type and then click **Next** ➤
 - Select **Update** to update the switch firmware or configuration files (transfer a file to the switch).
NOTE: Firmware upgrades can only be performed on the backup image.
 - Select **Backup** to save a backup of the current image, configuration file or error log (transfer a file from the switch).

Figure 201: Select Backup or Update

2. Select the **File Type** and then click **Next** ➤.

These are the available file types:

File Type	Description	Available for Operation Type
Active Image	Select this option to backup/copy the active image file. The active image file is the one running currently on the switch.	Backup only

File Type	Description	Available for Operation Type
Backup Image	Select this option to transfer a new image to the switch. The code file is stored as the backup image. After updating the backup image, you can use the Dual Image Configuration page to make it the active image upon the next reboot. NOTE: You cannot directly update the active image.	Update and Backup
Startup Configuration	Select this option to update or backup the stored configuration file. In case of startup configuration update, if the copy operation resulted in an error (for example wrong configuration lines), the update is stopped.	Update and Backup
Running Configuration	Select this option to back up the running configuration file.	Backup only
Backup Configuration	Select this option to update or backup the stored backup configuration file. The backup configuration file is stored on the switch for future reference. It is not active unless copied to the running configuration.	Update only
Error Log	Select this option to backup the switch log file. The log file is the file on flash. It stores syslog messages, from level error and higher.	Backup only

3. Select the Transfer Protocol, and then click **Next** .

These are the available protocols:

- HTTP - this protocol does not require any additional fields
- TFTP - this protocol requires the Server Address and File Name
- SCP - this protocol requires the Server Address, Username, Password, and File Name

4. Enter any additional fields as required.

Field	Description
Server Address	(TFTP/SCP only) Enter the IP address of the TFTP/SCP server to use for file transfer (Update or Backup).
Username	For SCP transfer, if the server requires authentication, specify the user name for remote login to the server that will receive the file.
Password	For SCP transfer, if the server requires authentication, specify the password for remote login to the server that will receive the file.
File Name	(TFTP/SCP only) Enter the path on the server where you want to put the file followed by the name to be applied to the file as it is saved. This can differ from the actual file name on the switch. The path can be 0 to 160 characters and the file name can be 1 to 120 characters. The file name can have ASCII printable characters, excluding the following: \\, /, :, *, ?, ", <, >,

5. Click **START FILE TRANSFER** to start the transfer. For a TFTP or SFTP backup, the switch begins the transfer to the specified location. For an HTTP update, browse to the location on your management station where the file you want to update to switch is located.

For HTTP backup - the file will be saved to the download folder specified by the browser.

Figure 202: File Transfer Example - TFTP Protocol

Backup and Update Files

Operation Type

Update (Transfer a file to the switch)

File Type

Backup Image

Transfer Protocol

TFTP

Server Address

(x.x.x.x)

File Name

(1 - 160 characters)

START FILE TRANSFER

Configuration File Operations

Use this page to copy the information contained in one configuration file to another configuration file on the switch.

To display this page, click **Maintenance > Configuration File Operations** in the navigation pane.

Figure 203: Configuration File Operations Page

Configuration File Operations

Source File

Running Configuration

Destination File

Startup Configuration

Table 170: Configuration File Operations Fields

Field	Description
Source File	Select the configuration file that will overwrite the contents in the selected destination file. The source file options are as follows: <ul style="list-style-type: none">• Running Configuration - The file that contains the configuration that is currently active on the system. Copying the running configuration file to the startup configuration file is effectively the same as performing a Save.• Startup Configuration - The file that contains the configuration that loads when the system boots.• Backup Configuration - The file that is used to store a copy of the running or startup configuration. This option is available after you copy the running or startup configuration to backup.
Destination File	Select file to be overwritten by the contents in the selected source file. The destination file options are as follows: <ul style="list-style-type: none">• Startup Configuration - The file that contains the configuration that loads when the system boots.• Backup Configuration - The file that is used to store a copy of the running or startup configuration.

After you specify the source file to copy and the destination file to overwrite, click **START FILE TRANSFER** to initiate the file transfer operation.

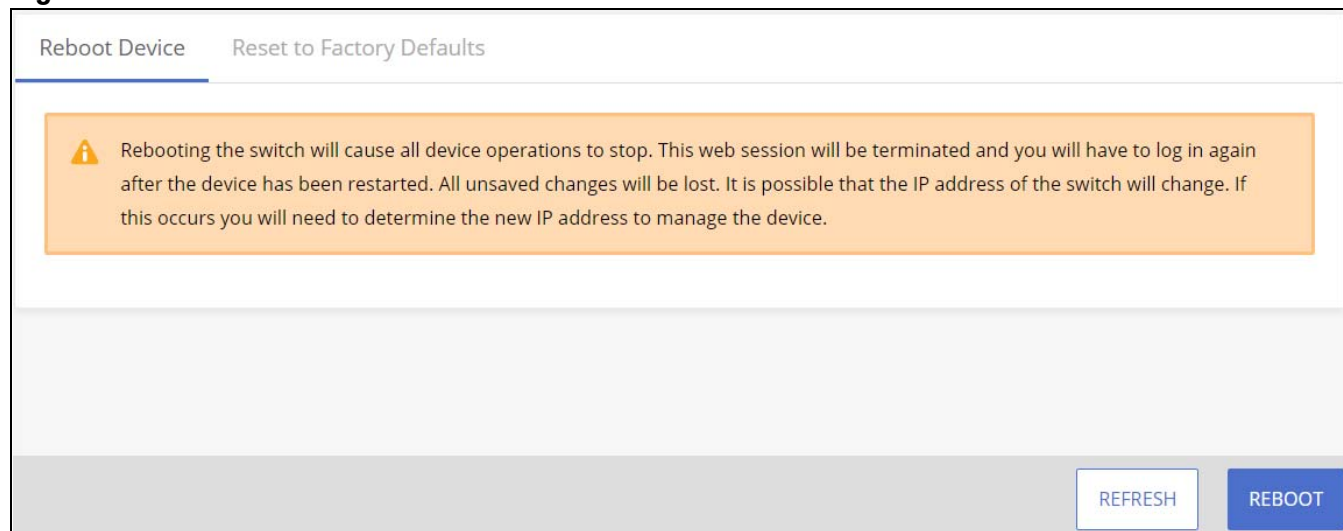
Reset

This page enables Rebooting the switch or Resetting to Factory Defaults.

Reboot Device

Use this feature to perform a software reboot of the switch. If you applied configuration changes, click the **Save Configuration** button in the upper-right of any page before rebooting. If the switch is configured to use DHCP to acquire its IP address, the address may change upon restart; you will need to determine the address before logging back in to the management utility.

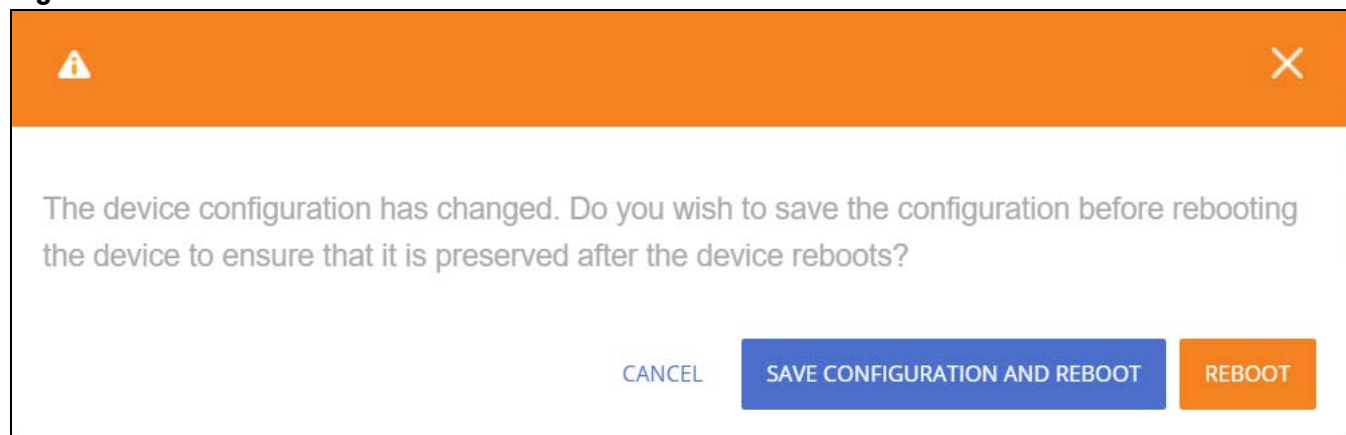
To display the Reboot Device page, click **Maintenance > Reset**, and make sure the **Reboot Device** tab is selected.

Figure 204: Reboot Device Tab

Click **REBOOT** to reboot the switch.

If the switch configuration has changed but has not been saved, a window appears after you click REBOOT to enable you to save the current configuration before rebooting the switch.

Figure 205: Save Before Reboot



Reset to Factory Defaults

You can use the Reset To Factory Defaults page to reboot the switch and restore all switch settings to their factory default values and to erase all entries in the switch log file stored in the non-volatile memory. Following Reset to Factory default the switch will reset and all configuration changes, including those that were previously saved, are reset in the running system by this action.

If the switch is configured to use DHCP to acquire its IP address, the address may change upon restart; you will need to determine the address before logging back in to the management utility.

To display the **Reset to Factory Defaults** page, click **Maintenance > Reset**, and make sure the **Reset to Factory Defaults** tab is selected.



It is recommended that you back up the current configuration file prior to restoring the factory defaults configuration. See [Backup and Update Files](#) for instructions.

Figure 206: Reset to Factory Defaults Page

Reboot Device Reset to Factory Defaults

 This action resets all configuration parameters to their factory default settings and reboots the device. All configuration changes, including those that were previously saved, are reset by this action. This web session will be terminated and you will have to log in again after the device have been restarted. It is possible that the IP address of the switch will change. If this occurs you will need to determine the new IP address to manage the device.

REFRESH RESET

Click **RESET** to reboot the switch and restore the system to the default settings.

Websites

Main Instant On site:

<https://instant-on.hpe.com/>

Support:

<https://instant-on.hpe.com/contact-support/>

Instant On social forums and knowledge base:

<https://community.arubainstanton.com/>

Security Bulletins:

<https://www.arubanetworks.com/support-services/security-bulletins/>

End-user license agreement:

<https://instant-on.com/eula/>

Instant On EOS Policy:

<https://www.arubainstanton.com/files/EOS-Policy.pdf>

Accessing HPE Networking Support

To access HPE Networking Support, go to <https://instant-on.hpe.com/contact-support/>.

Be sure to collect the following information before contacting Support:

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing Updates

To download product updates:

- Instant On Support Portal [Instant-On - Community & Software Downloads](#)

If you are unable to find your product in the InstantOn Support Portal, you may need to search My Networking, where older networking products can be found:

My Networking www.hpe.com/networking/software

To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:

www.hpe.com/support/AccessToSupportMaterials



Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

To subscribe to eNewsletters and alerts: www.hpe.com/support/e-updates

Warranty Information

To view warranty information for your product, go to <https://www.hpe.com/support/Networking-Warranties>.

Regulatory Information

To view the regulatory information for your product, view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at the Hewlett Packard Enterprise Support Center: www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional Regulatory Information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at: www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH: www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see: www.hpe.com/info/environment

Documentation Feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docs-feedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and

publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

8.4. MANUAL DEL USUARIO SANITARIOS Y ORINALES

**KLIPEN**

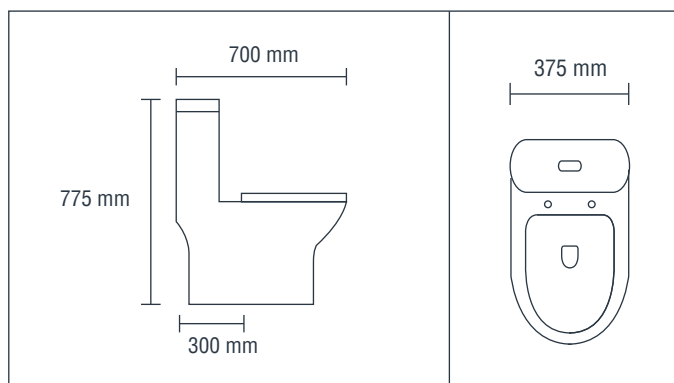
SANITARIO

POWER VULCANO



DESCRIPCIÓN:

Sanitario “One Piece” que brinda un diseño moderno y compacto. Cuenta con tecnología “Power flush”, que evacúa altas cantidades de sólidos por medio de descargas con bajo consumo de agua. Esto, junto a su sistema de accionamiento con botón “Dual”, lo hacen el sanitario ahorrador ideal. Este modelo es de fácil limpieza ya que no genera espacios donde se pueda acumular polvo o suciedades. Cuenta con asiento de cuerpo delgado y liviano que complementan la estética general del producto.



INFORMACIÓN TÉCNICA

	Modelo: One Piece.		Presión de trabajo: 20-80 (PSI).		Doble pulsador: Descarga reducida y normal.
	Dimensiones: 700*375*775 (mm).		Salida: 300 (mm).		Consumo de Agua: 3.5 L y 5 L
	Tipología de sanitario: Sifónico.		Asiento: Cierre lento.		Peso: Neto: 43 Kg. / Bruto: 46 Kg.
	Sistema de descarga: Cyclon.		MISO: 1,000 gramos.		

WE INSPIRE · YOU LIVE

CARACTERÍSTICAS TÉCNICAS

Sanitario Sifónico	Con medida de espejo de agua que evita la devolución de malos olores.
Descarga Cyclon (sin anillo interior)	Realiza una limpieza completa al circular el agua, con mayor profundidad, por las paredes internas del sanitario.
Forma del sanitario:	Elongado
Color	Blanco.
Grosor del cuerpo	15 (mm).
Trampa	S-trap.
Diámetro de entrada	28 (mm).
Diámetro de salida del tanque	7 (mm).
Diámetro salida de desagüe	85 (mm)
Capacidad del tanque	9-10 Litros.
Incluye	Mecanismo interno, asiento sanitario (tapa taza) Nota: Requiere Kit de Instalación (se vende por separado).
Sifón	Esmaltado
Asiento (tapa taza)	De cierre lento, material polipropileno, 155 mm de distancia entre orificios de visagras tamaño: 435*365 (mm).
Cuerpo fabricado en loza sanitaria vitrificada y esmaltado en todas sus áreas visibles. La absorción de las piezas es inferior al 0.5%. Fabricado e inspeccionado bajo norma internacional ASME A112.19.2-2003	

INSTRUCCIONES DE MANTENIMIENTO

KLIPEN fabrica su loza sanitaria vitrificada para cumplir con las más altas normas de calidad internacional, debido a ello son productos muy fáciles de limpiar evitando así el crecimiento de microorganismos nocivos para la salud.

Realice la limpieza empleando exclusivamente jabón neutro y agua. Use solamente esponjas suaves y nunca materiales abrasivos ya que estos afectan la durabilidad del esmalte.

Nunca utilice productos tipo pastilla y otro dentro del tanque ya que esto afecta el desempeño de la pieza.

GARANTÍA

- Garantía de por vida en loza sanitaria.
- Garantía de 5 años para mecanismo interno.

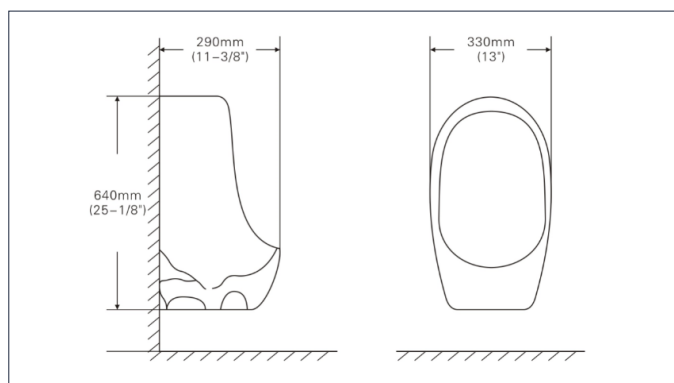
**KLIPEN**

ORINAL CITY



DESCRIPCIÓN:

Nuestro Orinal City brinda una combinación ideal entre diseño y funcionalidad. Gracias a su descarga de lavado, permite evitar problemas en la línea de drenaje y reduce los ciclos de mantenimiento. Cuando se instala correctamente cumple con requerimientos A.D.A.



INFORMACIÓN TÉCNICA

	Modelo: Orinal.		Presión de trabajo: 20-80 (PSI).		Doble pulsador: No aplica.
	Dimensiones: 330*290*640 (mm).		Salida: 180 (mm).		Consumo de Agua: 0.5 L
	Tipología de sanitario: Washdown.		Asiento: No aplica.		Peso: Neto: 16 Kg. / Bruto: 18 Kg.
	Sistema de descarga: No aplica.		MISO: No aplica.		

WE INSPIRE · YOU LIVE

CARACTERÍSTICAS TÉCNICAS

Descarga	Por limpieza
Color	Blanco.
Grosor del cuerpo	13 (mm).
Trampa	P-trap.
Diámetro de entrada	32 (mm)
Diámetro de salida	Diámetro interior: 42mm / Diámetro exterior: 55mm

Cuerpo fabricado en loza sanitaria vitrificada y esmaltado en todas sus áreas visibles. La absorción de las piezas es inferior al 0.5%. Fabricado e inspeccionado bajo norma internacional ASME A112.19.2-2003.

INSTRUCCIONES DE MANTENIMIENTO

KLIPEN fabrica su loza sanitaria vitrificada para cumplir con las más altas normas de calidad internacional, debido a ello son productos muy fáciles de limpiar evitando así el crecimiento de microorganismos nocivos para la salud.

Realice la limpieza empleando exclusivamente jabón neutro y agua. Use solamente esponjas suaves y nunca materiales abrasivos ya que estos afectan la durabilidad del esmalte.

Nunca utilice productos tipo pastilla y otro dentro del tanque ya que esto afecta el desempeño de la pieza.

GARANTÍA

- Garantía de por vida en loza sanitaria.
- Garantía de 5 años para mecanismo interno.

8.5. MANUAL DEL USUARIO GRIFERÍA DE LAVAMANOS

PUSH PICO EMPOTRADO

Grifería Tipo Push - Para Lavamanos

Referencia: 701330001

- Consumo de agua de **0.33** Lpf (Litros por ciclo)



Nuestra grifería para lavamanos institucional de pared, tiene sistema de accionamiento suave tipo push de cierre automático y cuenta con regadera de pico empotrado, lo que la convierte en aliada perfecta para las necesidades de instituciones o lugares públicos de alto tráfico y está diseñada para un óptimo funcionamiento y durabilidad.

Características y Beneficios

- Pico con diseño minimalista acorde con los nuevos diseños de baños.
- Diseño robusto y adecuado para alto tráfico con un grado elevado de antivandalismo.
- Funcionamiento silencioso.
- Cuerpo en latón resistente a la corrosión.
- Válvula compacta que ahorra espacio.
- Temporizador que evita el desperdicio de agua.
- Accionamiento fácil y cómodo.
- Higiénica y fácil de limpiar.
- Cierre automático temporizado entre 5 a 9 segundos.
- Graduación de caudal por facilidad de las 7 posiciones que trae el cartucho.

Información Técnica

Material :

Cuerpo :	Latón acabado natural
Botón :	Latón con recubrimiento de cromo
Escudo y Portaescudo :	Latón con recubrimiento de cromo
Acabado :	Cromado
Peso Neto :	77gr. / 1,70Lb
Peso Bruto :	860gr. / 1,90Lb
Diámetro de tubería para la instalación :	1/2" NPT
Presión de trabajo :	20 - 80 PSI
Torque de cierre :	Ajustar con una llave hasta obtener un selle perfecto.
Ciclo de Vida y Desempeño de la descarga :	150,000 ciclos

Cuidados y Limpieza

Los acabados superficiales son aquellos que le imprimen una apariencia especial y estética a su producto y además le brindan protección. Para prolongar sus cualidades es vital que la limpieza profunda del producto se haga únicamente con agua y jabón suave y que en el secado y el brillo se utilice un paño de algodón limpio, dicha limpieza se recomienda 2 veces a la semana, y en zonas costeras a diario por la salinidad del ambiente. Por ningún motivo deben usarse elementos abrasivos, ácidos o disolventes para la limpieza del producto. Los acabados pueden variar su comportamiento en zonas costeras y/o en ambientes corrosivos.

Repuestos

Referencia	Descripción
O2121111	UNIDAD DE CONTROL LVM/ORINAL
O21341111	ESCUDO VÁLVULA LVM/ ORINAL
O21371111	PORTA-ESCUDO VÁLVULA LVM/ORINAL
O22071111	LLAVE BOCA FIJA INSTITUCIONAL

Cumplimiento de Normas

Este producto cumple con los requerimientos y especificaciones de :



NTC 1644
Accesorios de
Suministro fontanería



SERVICIO
TÉCNICO



AHORRO
DE AGUA



AÑOS DE
GARANTÍA
DE PRODUCTO



AÑOS DE
GARANTÍA
(ACABADOS)

Corona tiene un informe de Sostenibilidad corporativo anual que sigue los lineamientos del GRI Sustainability Report. Puedes encantarlo en el siguiente link: <https://empresa.corona.co/sos-corona.co>

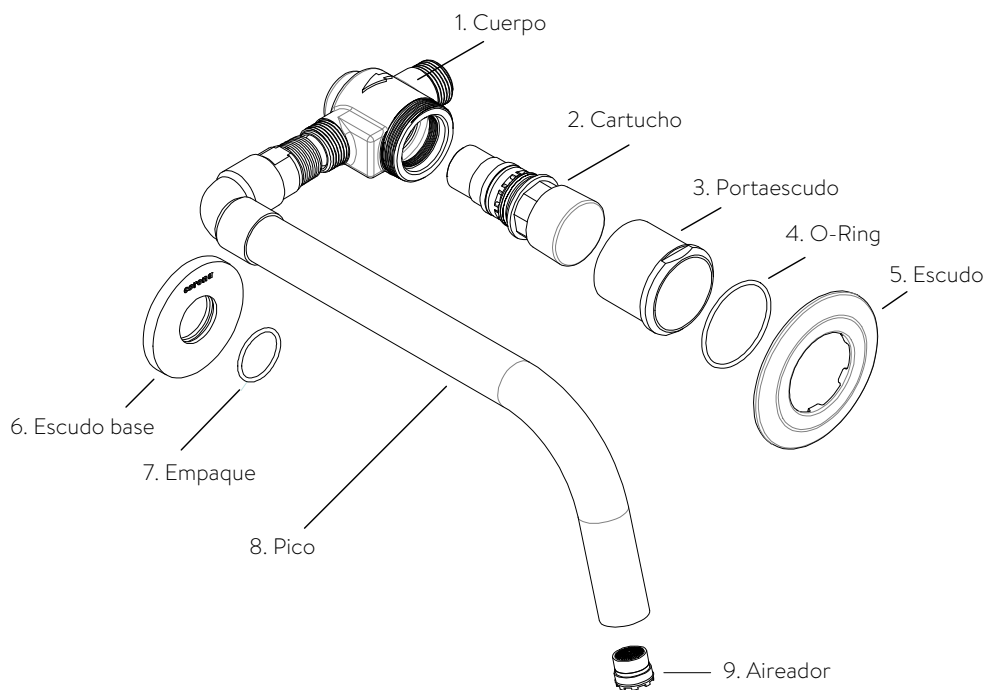
corona

PUSH PICO EMPOTRADO

Grifería Tipo Push - Para Lavamanos

Ref.: 701330001

Plano de Explosión



Planos Técnicos

*Estas dimensiones son nominales y están sujetas a cambios sin previo aviso.
Unidades: mm

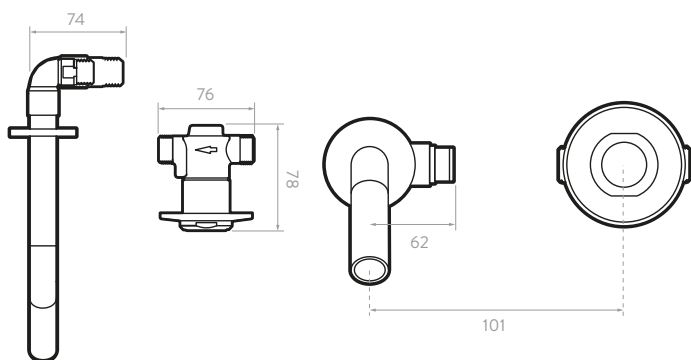
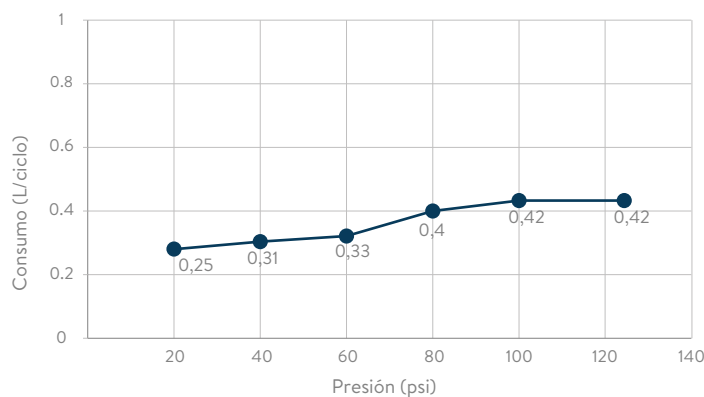


Diagrama de Consumo



Líneas de atención al cliente:

Colombia: Bogotá (601) 404 88 84 / Resto del país 01 8000 5120 30

Centro America: Guatemala (502) 1-800-6240-109 / Nicaragua (505) 2249-5521

El Salvador (503) 2274-4620 / Honduras San Pedro Sula (504) 9470-9391

Honduras Tegucigalpa (504) 9441-1968 / Costa Rica (506) 4001-4966 /

Panamá (50n 8000-202 contacto_ca.ci@corona.co.com)

México: Directo (81) 8125 2000 / LADA sin costo 01 800 705 1020

Si usted desea ver nuestra línea completa de productos por favor ingrese a: corona.co

corona