

Redundancia N+1 con el switch RF de Cisco

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Switch RF](#)

[Configuración y operación del switch RF](#)

[Información Relacionada](#)

Introducción

Este documento proporciona información sobre la redundancia N+1 usando el switch RF de Cisco®.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

Antecedentes

Para obtener el máximo valor por su dinero, muchos operadores de cable han decidido

proporcionar redundancia para su red de fibra óptica en forma de fuentes de alimentación de respaldo adicionales en el nodo de fibra, fuentes de alimentación ininterrumpibles (UPS) con reserva de batería y gas natural y transmisores de fibra adicionales en el nodo. También se podrían asignar fibras más oscuras a cada nodo en caso de que se produzca una falla en la fibra.

Como se explicó anteriormente, el hardware es lo primero que se cubre en la planta exterior. ¿Qué hay de las señales reales de flujo ascendente (US) y descendente (DS) que viajan en el medio de transporte? En cuanto a los EE.UU., Cisco ha implementado técnicas de gestión avanzada del espectro para mantener los módems en línea y transmitir de forma óptima. Algunas de estas técnicas son el salto de frecuencia con capacidad avanzada de "mirar antes de saltar" a través de la tarjeta secundaria incorporada de analizador de espectro en la tarjeta S. Cisco también incorporó cambios en el perfil de modulación y en el ancho de canal. Todas estas características permiten que el módem permanezca en una zona clara del espectro, use un perfil de modulación más robusto y/o cambie el ancho de canal para mantener un servicio óptimo respecto del rendimiento y la disponibilidad. Al observar las frecuencias DS, puede elegir entre 64 o 256-QAM. Si bien estos esquemas de modulación son mucho menos robustos que los de EE.UU. en QPSK o 16-QAM, el espectro DS es mucho más predecible y está bajo control que el espectro de EE.UU.

El siguiente elemento lógico en el que debemos centrarnos es la disponibilidad de hardware en la cabecera. Si falla una única fuente de CA o CC, la copia de seguridad del generador puede utilizarse con fuentes de alimentación redundantes en caso de que se produzca un error.

Otro punto de fallo del hardware podría ser la alimentación del sistema de terminación del cable módem (CMTS). Las fuentes de alimentación uBR10K utilizan un algoritmo para el respaldo y el equilibrio de carga/uso compartido. Esto se denomina a veces N:1, que significa 1 para respaldo N con equilibrio de carga. En este caso, será de 1:1 y verá que la potencia total de CC es ligeramente superior, con dos módulos de entrada de alimentación (PEM), que si se utilizara uno para toda la carga. Ejecute el comando **sh cont clock-reference** para ver esta información.

```
ubr10k#sh cont clock-reference | inc Power Entry
Power Entry Module 0 Power:          510w
Power Entry Module 0 Voltage:        51v
Power Entry Module 1 Power:          561w
Power Entry Module 1 Voltage:        51v
```

Para centrarse en la disponibilidad de tarjetas de línea CMTS, Cisco ha desarrollado un protocolo para especificar cómo se comunicarán los CMTS entre sí en un escenario de alta disponibilidad. Este protocolo se denomina protocolo de conexión a conexión en espera activa (HCCP). Este protocolo proporciona un latido entre el dispositivo de protección y los dispositivos en funcionamiento para mantener las interfaces/dispositivos sincronizados con las tablas MAC, las configuraciones, etc. Cisco también ha desarrollado un switch RF para ofrecer una alta disponibilidad en el nivel del dominio MAC en vez de chasis por chasis. Un dominio MAC también se puede considerar como una subred RF, que es un DS y todos sus US asociados.

Cisco ha ofrecido redundancia 1+1 en el chasis de la serie uBR7200 durante unos años; sin embargo, un chasis completo debe permanecer inactivo como chasis de protección. La ventaja de hacer 1+1 no es necesaria, pero sí menos escalable. El uso de un switch RF permite que se realice redundancia en el nivel de interfaz para la disponibilidad N+1. Esto significa 1 para la copia de seguridad N sin equilibrio de carga/distribución. En lugar de que todo un chasis esté inactivo, es posible que tenga una tarjeta de protección/inactiva o una interfaz que proteja muchas otras interfaces. El uBR100012 se puede configurar como una tarjeta que protege a otras siete. Esto

ayuda con la economía porque ahora proporciona disponibilidad 7+1 y también supera los requisitos necesarios para PacketCable.

Una vez que se hayan tratado estos puntos, debe estar seguro de que dispone de redundancia para el lado de la red de retorno, también conocido como el lado WAN o LAN, según cómo se mire. El protocolo de router en espera en caliente (HSRP) lleva años funcionando y permite que las rutas redundantes entre routers proporcionen el nivel de disponibilidad necesario para este punto único de falla. El verdadero impulso para estas funciones es VoIP y el aumento de las presiones de la competencia para proporcionar el servicio más estable/disponible al cliente.

Secuencia operativa de eventos

Solución uBR10K

El HCCP se produce primero entre el chasis a través del latido. Dado que la solución uBR10K está contenida en un chasis, es posible que el latido no sea relevante. Si la comunicación interna y los cambios de la interfaz son exitosos, HCCP continuará enviando un comando al switch RF para alternar los relés apropiados.

Solución uBR7200

El HCCP se produce primero entre el chasis a través del latido. A continuación, se envía un comando de la protección 7200 al convertidor ascendente (UPx) para cambiar la frecuencia. La UPx envía un ACK. El 7200 Protect envía un comando para inhabilitar el módulo UPx en funcionamiento y espera un ACK. El 7200 Protect luego envía un comando para habilitar el módulo UPx de protección y espera un ACK. Si todo esto funciona o no se envía ACK desde el módulo UPx en funcionamiento, continuará y enviará un comando al switch para alternar los relés apropiados.

Hay dos tipos de mecanismos de latidos que son relevantes para el HCCP. Se enumeran a continuación.

1. helloACK entre el trabajo y la protección: la LC de protección envía un mensaje hello a cada una de las LC en funcionamiento en su grupo y espera un helloACK en respuesta. La frecuencia de envío de hello y helloACK se puede configurar en la LC de protección con CLI. Además, el tiempo de saludo mínimo en el 7200 es de 0,6 segundos, mientras que el mínimo en el uBR10K es de 1,6 segundos.
2. Mecanismo de pulso de sincronización: es un mecanismo de latido del plano de datos HCCP y su frecuencia no es configurable. Los pulsos de sincronización son enviados por cada LC en funcionamiento a su LC de protección de peer. Este pulso de sincronización se envía una vez por segundo. Si faltan tres pulsos síncronos, el par se declara inactivo. Cisco está trabajando en un mecanismo de detección rápida de fallas para detectar un desperfecto en funcionamiento en el controlador de excepciones en menos de 500 ms. La versión objetivo es 12.2(15)BC. En el VXR, ambos mecanismos pueden detectar fallas, sin embargo, dado que el uBR10K es todo HCCP interno, sólo el segundo es relevante.

Switch RF

Cisco decidió utilizar un switch de RF externo en lugar de una tarjeta de línea o un cableado interno que funcionaría como un switch de RF debido a la escalabilidad y complejidad futuras. El

switch externo se puede apilar y utilizar para varios escenarios, diferentes densidades y equipos antiguos.

Hay 252 conexiones en la parte posterior del switch en un paquete de 3 unidades en rack (3RU). 1 RU mide 1,75 pulgadas. El convertidor ascendente VCom HD4040 es de 2RU.

Si la placa de interconexiones está configurada de cierta manera para un switch interno, se limita la flexibilidad para hacer diferentes densidades de tarjeta de línea más adelante. Si una tarjeta de línea es demasiado densa, demasiados puertos de US se ven afectados por fallas que son específicas de un solo US o DS y de una sola tarjeta en general. Es por eso que se necesita un switch y redundancia desde el principio. Más densidad equivale a más clientes que se ven afectados por un único evento. ¿Qué sucede si se venden tarjetas DS puras y tarjetas US puras? En el futuro, podrá hacer coincidir los puertos de US y DS entre las tarjetas de línea. El diseño externo protege mi inversión en el futuro.

Nunca podrá hacer redundancia entre chasis con un switch interno. Si desea ahorrar dinero y tiene cuatro uBR 7200 respaldados por uno, se necesita un switch de RF externo. A menos que esté pensando en tener tarjetas de línea en un chasis respaldadas por otra en el mismo chasis. El único problema es que si todo el chasis deja de funcionar, no tendrá respaldo.

Los números de disponibilidad pueden ser mejores para un switch externo (al menos en lo que se refiere a la electrónica, no al cableado) debido a que los componentes son menos activos. Dado que el switch tiene un diseño pasivo total en el chasis, el modo de funcionamiento normal está operativo, incluso si se eliminan los módulos activos. Los relés sólo se encuentran en la trayectoria de protección con una trayectoria de trabajo totalmente pasiva y se pueden conmutar para probar el switch sin afectar al modo de funcionamiento real. Esto significa que el modo de funcionamiento normal no se verá afectado por una falla de alimentación en el switch, un módulo de switch que se retira o una falla del switch. El negativo de esto es la pérdida de inserción de potencialmente 6 a 8 dB en la frecuencia DS más alta de 860 MHz.

El diseño externo también permite la migración del cableado y los intercambios de tarjeta de línea. Si alguien desea actualizar de una tarjeta 2x8 a una tarjeta 5x20, la tarjeta de línea puede verse obligada a conmutar por error al modo de protección. La tarjeta de línea se puede cambiar al ritmo que determine con la tarjeta más nueva y densa 5x20 y se puede conectar para dominios futuros. Los dos dominios que se encontraban en el modo de protección se volverán a conmutar a la interfaz/ dominios correspondientes en la tarjeta 5x20. Se deben abordar otros problemas, como que el 5x20 tendrá convertidores ascendentes internos y comandos de conector.

El panel frontal tiene las luces, el cable de alimentación para CA o CC, la conectividad Ethernet, la conectividad RS-232 y un interruptor de alimentación para designar CA, CC o apagado. También se envía una herramienta de extracción de cables con cada switch. Asegúrese de quitar la funda de goma antes de su uso. La fuerza de extracción se puede ajustar con un destornillador atornillando en el sentido de las agujas del reloj en la parte posterior de la herramienta.

La siguiente imagen es la vista frontal del switch RF.

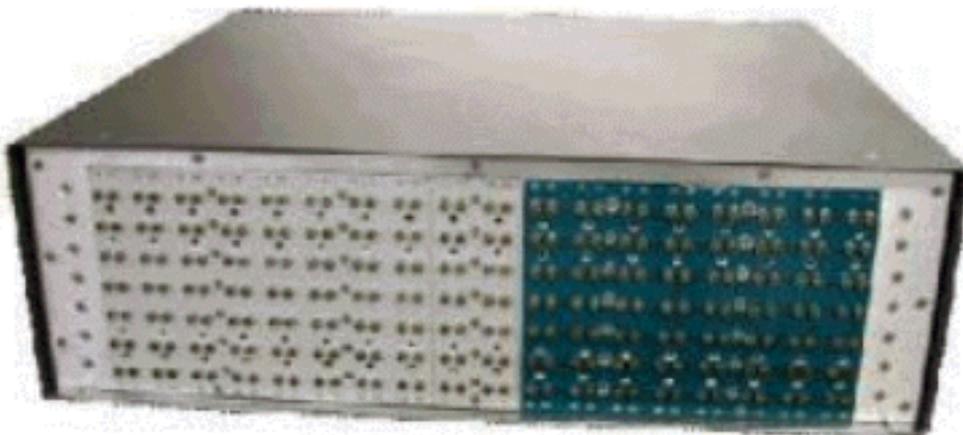


Hay diez módulos US (mostrados en azul) y tres DS (mostrados en gris) instalados en el switch RF 3x10. La parte inferior izquierda se conoce como módulo N y está en blanco. Los módulos de la parte frontal, comenzando por la esquina superior derecha, son los números 1-13 y se correlacionan con los puertos A-M. El módulo ascendente 1 tiene todos los relés para el puerto A en las ranuras 1 a 8 y protege 1 y 2 en la parte posterior. El Módulo 2 está a la izquierda y tiene todos los relés para el puerto H en las ranuras 1 a 8 y protege 1 y 2.

Los módulos pueden intercambiarse en caliente, sin embargo, la extracción de la tarjeta es muy difícil. Es extremadamente apretado y los dos tornillos cautivos deben aflojarse antes de tirarse. Es posible que deba abrir con un destornillador o girar hacia la izquierda y hacia la derecha mientras se extrae.

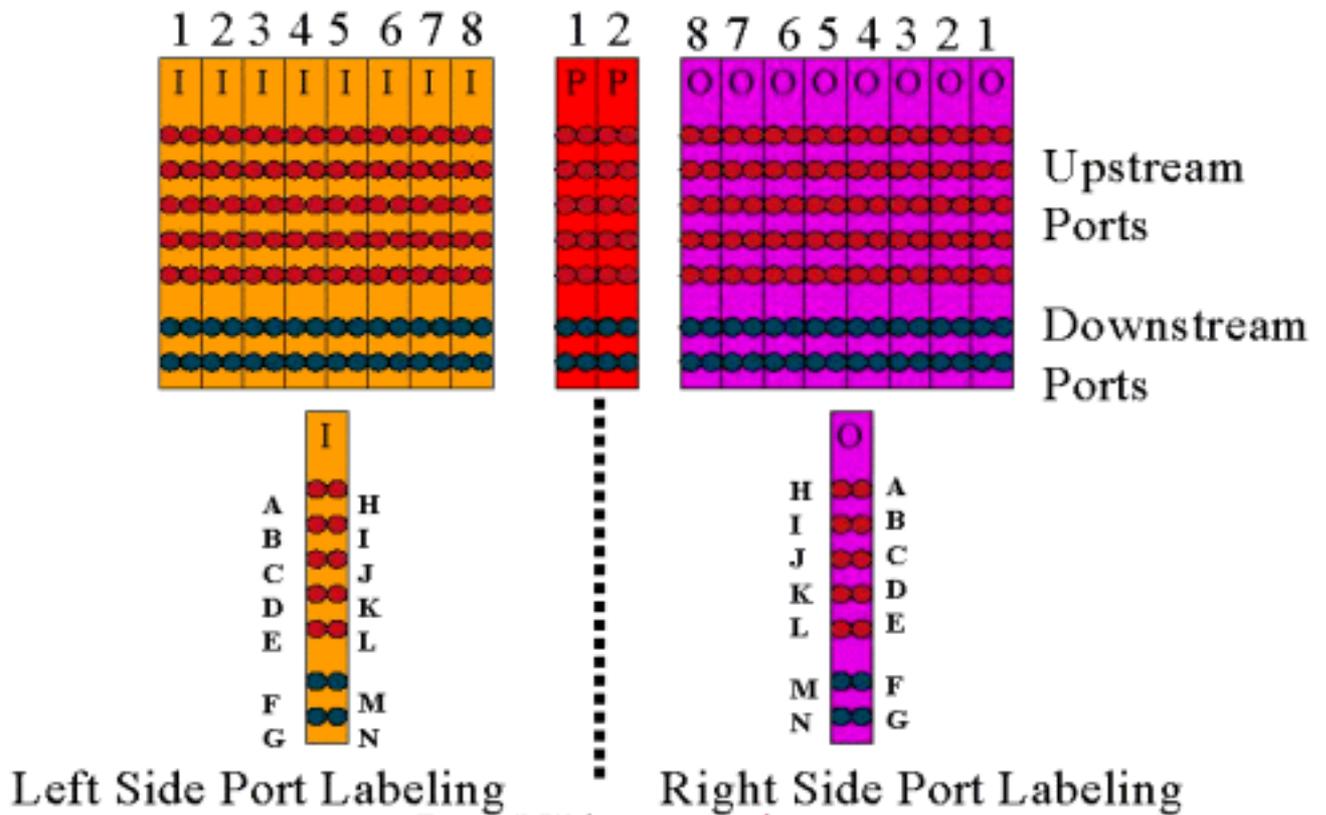
El panel posterior tiene etiquetas que dicen **CMTS**, **Protect** y **Cable Plant**. El lado **CMTS** es para las entradas de trabajo. El lado de la **Planta de Cables** contiene todas las salidas para alimentar la planta de cables.

La siguiente imagen es la vista posterior del switch RF.



Las ocho entradas de trabajo se numeran de izquierda a derecha. Los dos sistemas de protección están en el medio y los 8 resultados están a la derecha.

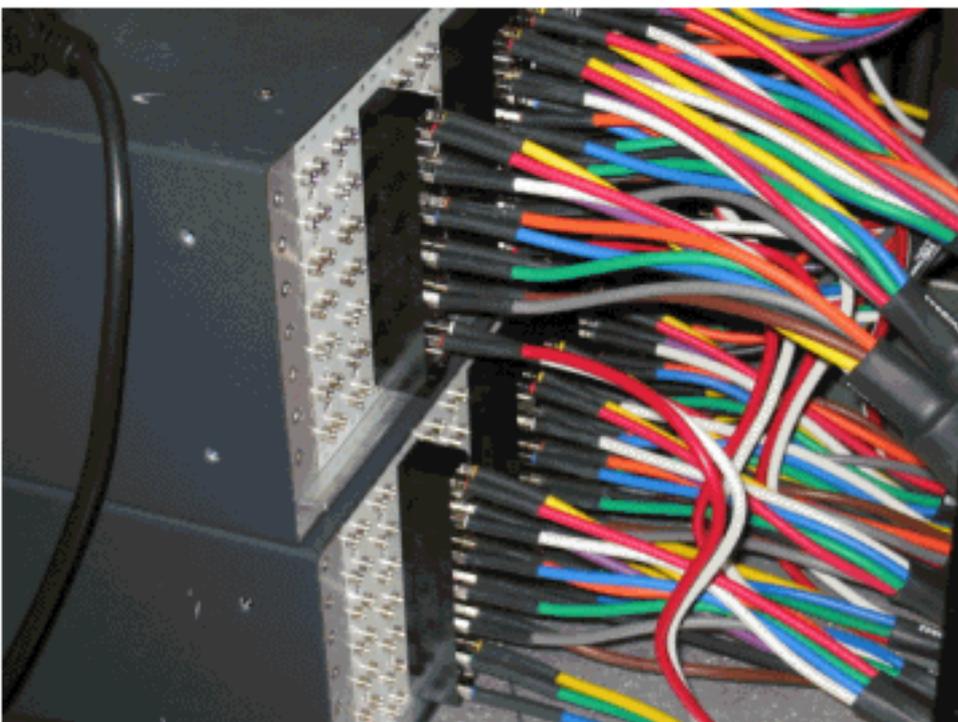
La siguiente imagen es el esquema de numeración del switch RF.



Nota: No se utiliza el puerto N.

La salida (color púrpura) representa la planta de cable. La salida 1 está en el extremo derecho mientras que la entrada 1 está en el extremo izquierdo. Los puertos también están duplicados. Recuerde, el puerto N no se utiliza. Asegúrese de utilizar la uniformidad en el cableado.

Esta imagen a continuación es la vista posterior del switch RF con el encabezado de 14 puertos y el cable coaxial especial Belden mini con conectores MCX.



Los conectores MCX se pueden conectar directamente al switch; sin embargo, corre el riesgo de conexiones sueltas, emisiones y posibles desconexiones intermitentes. Cisco desarrolló un

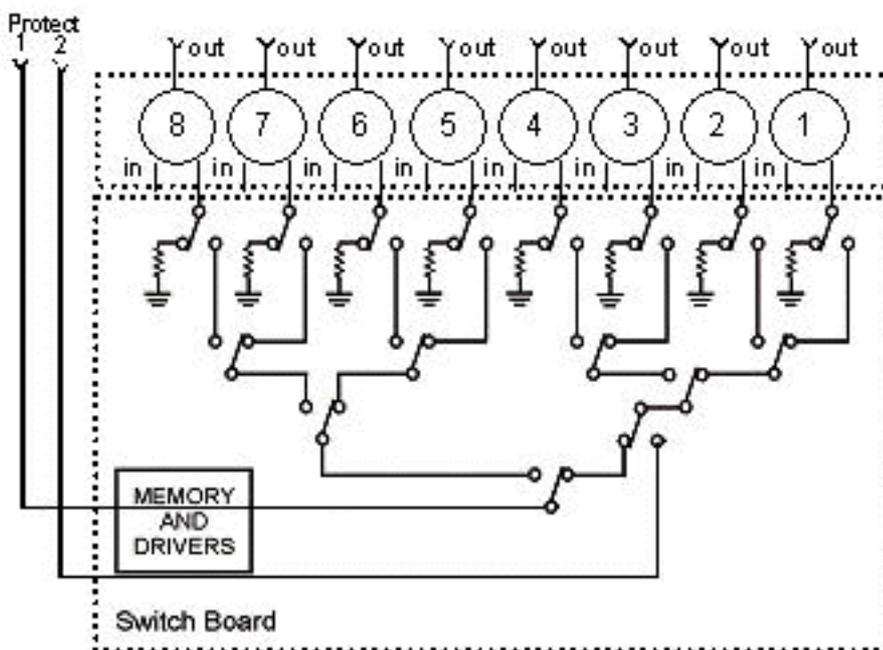
encabezado para resolver este tipo de problemas.

Los conectores MCX se encajan en el encabezado y hay una herramienta especial que se envía con cada compra de switch para extracción. El cabezal tiene dos pins de guía y se conecta de un solo modo. Hay un pequeño bisel en el borde superior para indicar la parte superior del encabezado. Hay dos tornillos de cabeza plana para conectar el encabezado al switch. También se suministra un soporte de administración de cables con cada switch RF.

Sugerencia: También puede instalar el encabezado en el switch y, a continuación, insertar los conectores MCX en el encabezado. Esto puede hacer que sea más sencillo instalarlo. No apriete el encabezado al switch hasta que se hayan instalado todos los conectores.

[Configuración y operación del switch RF](#)

La siguiente imagen es un diagrama de bloques del switch RF.



Los componentes del combinador se encuentran en el chasis del switch, pero los relés están en cada módulo individual extraíble. Cada relay termina con una carga de 75 ohmios, solamente en la trayectoria Protect, no en la trayectoria de entrada/funcionamiento.

Configure la comunicación serial con el switch consolando con HyperTerminal o TeraTerm, un cable de consola/transpuesto, un adaptador de 9 pines a RJ-45 de Cisco y con una velocidad en baudios de 9600.

Establezca una dirección IP y una máscara ejecutando el comando **set ip addr ip add subnet mask**. Una vez hecho esto, puede realizar Telnet y también configurar una contraseña de Telnet. A continuación, configure el esquema de protección, ya sea 4+1 u 8+1, ejecutando el comando **set prot 4/8**. El valor predeterminado es 8+1, donde la protección 1 cubre las ocho ranuras de entrada. En el modo 4+1, proteja 1 cubre las ranuras 5-8 y proteja 2 las ranuras 1-4.

La cadena de comunidad SNMP es **privada** y se puede cambiar, pero no se admite en el uBR10K.

[Configuración de Bitmaps](#)

Lo siguiente importante a establecer son los grupos de switches, que requieren mapas de bits hexadecimales. El mapa de bits del switch RF tiene una longitud total de 32 bits (8 caracteres hexadecimales) y se calcula como se muestra a continuación. Hay una calculadora de Excel disponible para su uso.

Tenga en cuenta el grupo 1, que tiene cuatro cables estadounidenses conectados a la izquierda de un encabezado de switch de RF en la ranura 1, y 1 DS conectados al lado izquierdo del mismo encabezado. Los puertos utilizados serían ABCDF. Para cada puerto involucrado en el switching, el bit correspondiente se establece en 1. Si un puerto no está involucrado en el switching, ese bit de puerto está configurado en 0.

El grupo 1 se muestra a continuación.

```
A H B I C J D K E L F M G N X X X X X X X X X X X X X X X X X X
(1 0 1 0)(1 0 1 0)(0 0 1 0)(0 0 0 0)(0 0 0 0)(0 0 0 0)(0 0 0 0)(0 0 0 0) - binary
  10    10    2     0     0     0     0     0     0     0     0     0     0     0     0     0     0 - decimal
= A A 2 0 0 0 0 0 (in hexadecimal).
```

Nota: Los bits 14 a 32 son "no importa" (X).

Para el grupo 2, el lado derecho del encabezado está cableado y el mapa de bits se muestra a continuación.

```
A H B I C J D K E L F M G N X X X X X X X X X X X X X X X X X X
(0 1 0 1)(0 1 0 1)(0 0 0 1)(0 0 0 0)(0 0 0 0)(0 0 0 0)(0 0 0 0)(0 0 0 0)
  5     5     1     0     0     0     0     0     0     0     0     0     0     0     0     0
= 5 5 1 0 0 0 0 0 (hex)
```

Es necesario configurar los grupos de switches, o el switch no comprenderá qué puertos y retransmisiones se deben alternar. Al configurar mapas de bits, el número se puede ingresar como formato decimal o se debe ingresar con 0x delante del código hexadecimal para que el software reconozca que es hexadecimal. Ejecute el comando **set group Group2 0x55100000** para asignar el mapa de bits. Group2 es una cadena de palabras alfanumérica que debe comenzar con una letra.

Sugerencia: Los dos mapas de bits anteriores forman parte del diseño de referencia recomendado. El modo 4+1 es completamente diferente y se recomienda utilizar la calculadora de mapa de bits. Si realiza un esquema de protección 4+1, tendría cuatro grupos HCCP. HCCP grupos 1 y 2 en la tarjeta Protect 2 y HCCP grupos 3 y 4 en la tarjeta Protect 1card. Además, proteja 1 cubre las ranuras 5-8 en el switch; sin embargo, en la configuración uBR, esas ranuras se denominan ranuras 1-4.

Si conmuta puertos individuales en lugar de dominios MAC, debe saber qué esquema de protección está ejecutando y utilizar la tabla a continuación para saber qué número de grupo usar. Suponga que el switch está en el modo 4+1. El comando se muestra a continuación para el uBR10K.

```
hccp 1 channel-switch 1 us rfs witch-module 1.10.84.3 10 1
```

Esto indica la dirección IP del switch y el módulo 26, que indica la tarjeta de protección 2 que realiza una copia de seguridad del puerto G en un esquema 4+1, y el módulo 10, que indica la tarjeta de protección 2 que realiza una copia de seguridad del puerto C. Todo esto está en la ranura 1 del switch.

La siguiente tabla muestra ambos modos y qué número se relaciona con el puerto respectivo.

Modo 8+1'	Modo 4+1'
A(1) H(2)	A(1,2) H(3,4)
B(3) I(4)	B(5,6) I(7,8)
C(5) J(6)	C(9,10) J(11,12)
D(7) K(8)	D(13,14) K(15,16)
E(9) L(10)	E(17,18) L(19,20)
F(11) M(12)	F(21,22) M(23,24)
G(13) N(14)	G(25,26) N(27,28)

[Configuración de la Configuración de la Ranura](#)

El nuevo firmware permite configurar el chasis para cualquier combinación de tarjetas de flujo ascendente o descendente. Esto se logra mediante el uso del nuevo comando CLI **set slot config USslots DSslots**.

Los parámetros **US** y **DS** son máscaras de bits de enteros hexadecimales de 16 bits que representan si el módulo está habilitado/configurado para ese tipo de tarjeta, con el bit más a la derecha que representa el módulo 1. Consulte la nueva calculadora de mapas de bits para ver las configuraciones automatizadas.

Por ejemplo, si desea configurar un chasis con cuatro tarjetas de línea, tarjetas de flujo ascendente en los módulos 1-2 y tarjetas de flujo descendente en los módulos 3-4, ejecute el comando **set slot config 0x0003 0X000c**.

La configuración de la ranura se almacena en nvmem, separado del firmware de la aplicación. Esto permite actualizaciones futuras del firmware de la aplicación sin que el usuario deba reprogramar la configuración de la ranura y permite una distribución de código de aplicación única para cualquier configuración de switch de RF.

Normalmente, la fábrica haría esta configuración cuando se construya la unidad, sin embargo, esto le permitiría cambiar la configuración en el campo si lo desea, y usar cualquier número/mezcla de tarjetas que pueda necesitar en el futuro.

Abajo se brinda un ejemplo de configuración.

```
10 upstream/3 downstream/1 empty (current configuration):
    upstream bitmask = 0000 0011 1111 1111 = 0x03ff
    dnstream bitmask = 0001 1100 0000 0000 = 0x1c00

    SET SLOT CONFIG 0x03ff 0x1c00
```

```
12 upstream/2 downstream (new configuration):
    upstream bitmask = 0000 1111 1111 1111 = 0x0fff
    dnstream bitmask = 0011 0000 0000 0000 = 0x3000

SET SLOT CONFIG 0x0fff 0x3000
```

[Prueba de los Relays del Switch RF](#)

Cisco recomienda probar los relés una vez a la semana y al menos una vez al mes. Consola o Telnet en el switch y ejecute el comando **test module**. Si se configura una contraseña en el switch RF, ejecute el comando **password *password name para utilizar el comando test***. Esto probará todos los relés a la vez y volverá al modo de funcionamiento normal. No utilice este comando de prueba mientras esté en el modo de protección. **No utilice este comando de prueba mientras esté en el modo de protección.**

Sugerencia: Puede alternar los relés en el switch sin afectar al convertidor ascendente o a cualquiera de los módems. Esto es importante si se prueban los relés sin cambiar ninguna de las tarjetas de línea o los convertidores ascendentes correspondientes. Si se habilita un relay en el switch y se produce una conmutación por fallas, pasará al estado adecuado y no sólo conmutará de un estado a otro.

Ejecute el comando **switch 13 1** para probar el puerto G en el slot 1 del switch. Puede probar un mapa de bits completo ejecutando el comando **switch *group name* 1**. Ejecute el comando **switch *group name* 0** (o **idle**) para inhabilitar los relés para el modo de trabajo normal.

Además, el cliente debe realizar una prueba de failover de CLI de un grupo HCCP (ejecute el comando **hccp *g switch m***) **desde el CMTS para probar la tarjeta de protección y la trayectoria de protección**. Este tipo de conmutación por fallas puede tardar entre 4 y 6 segundos, y puede causar que un pequeño porcentaje de módems se desconecte. Por lo tanto, esta prueba debería realizarse con menor frecuencia y sólo durante las horas no pico. Las pruebas anteriores ayudarán a mejorar la disponibilidad general del sistema.

[Actualización del código del switch RF](#)

Siga los pasos a continuación.

1. Cargue las nuevas imágenes en el uBR con un disco Flash en la ranura 0.
2. Configure los siguientes comandos en el uBR.

```
tftp-server disk0: rfs330-bf-1935022g alias rfs330-bf-1935022g
tftp-server disk0: rfs330-fl-1935030h alias rfs330-fl-1935030h
```

3. Inicie la consola en el switch y ejecute el comando **set tftp-host {ip-addr}**. Utilice la dirección IP del uBR para las transferencias TFTP.
4. Ejecute el comando **copy tftp:rfs330-bf-1935022g bf:** para cargar la memoria flash de inicialización y **copiar tftp:rfs330-fl-1935030h fl:** para cargar la memoria Flash.
5. Reinicie o recargue para que se ejecute el nuevo código. Escriba **PASS SYSTEM** y **Save Config** para actualizar los nuevos campos nvmem. Reinicie de nuevo para que todo esto surta efecto.

Advertencia: Es posible que deba restablecer parte de la configuración después de la recarga,

como la dirección IP del switch. Revise la configuración del switch después de volver a cargar para verificarla. Una vez actualizado a la versión 3.5, se puede agregar una dirección de gateway predeterminada al switch y se pueden realizar nuevas actualizaciones en el switch a través de subredes de forma remota. El único límite es que si se carga desde estaciones Unix, el nuevo nombre de imagen debe ser letras minúsculas. Esta nueva imagen también agrega una opción de cliente DHCP y una configuración de chasis/módulo.

Operación DHCP

Esta versión incluye soporte completo para un cliente DHCP. La operación DHCP se habilita de forma predeterminada, a menos que el usuario haya establecido una IP estática desde la CLI. Los comandos se han agregado/mejorado para soportar la operación DHCP.

Cuando se inicia el switch RF, verifica si se ha activado DHCP. Esto se realiza a través de la CLI de diversas maneras. Puede utilizar cualquiera de los siguientes comandos para habilitar DHCP:

```
set ip address dhcp
set ip address ip adress subnet mask no set ip address
!--- To set the default, since DHCP is now the default.
```

El switch RF ya no asume una IP estática de 10.0.0.1 como en las versiones anteriores a 3.00.

Si se activa, el switch RF instala el cliente DHCP e intenta localizar un servidor DHCP para solicitar una concesión. De forma predeterminada, el cliente solicita un tiempo de arrendamiento de 0xffffffff (arrendamiento infinito), pero esto puede cambiarse ejecutando el comando **set dhcp lease leasetime_secs**. Dado que el tiempo de arrendamiento real se concede desde el servidor, este comando se utiliza principalmente para la depuración/prueba y no se debe requerir para el funcionamiento normal.

Si se encuentra un servidor, el cliente solicita la configuración de la dirección IP y la máscara de subred, una dirección de gateway y la ubicación de un servidor TFTP. La dirección del gateway se toma de la opción 3 (opción del router). La dirección del servidor TFTP se puede especificar de varias maneras. El cliente verifica la opción next-server (siaddr), la opción 66 (nombre del servidor TFTP) y la opción 150 (dirección del servidor TFTP). Si los tres anteriores están ausentes, la dirección del servidor TFTP es la dirección predeterminada del servidor DHCP. Si el servidor concede una concesión, el cliente DHCP registra el tiempo de concesión ofrecido para la renovación y continúa con el proceso de inicio, instalando las otras aplicaciones de red (Telnet y SNMP) y la CLI.

Si un servidor no se encuentra dentro de los 20-30 segundos, el cliente DHCP se suspende y la CLI se ejecuta. El cliente DHCP se ejecutará en segundo plano intentando ponerse en contacto con un servidor aproximadamente cada cinco segundos hasta que se encuentre un servidor, se asigne una IP estática a través de la CLI o se reinicie el sistema.

La CLI permite al usuario anular cualquiera de los parámetros de red que se pueden recibir a través del servidor y asignar valores estáticos para estos parámetros. Todos los parámetros del comando **set xxx** se almacenan en nvmem y se utilizan a través de reinicios. Dado que los parámetros de red actuales pueden provenir ahora de DHCP o de la CLI, se han implementado algunos cambios/nuevos comandos. El comando existente **show config** se ha cambiado para mostrar la configuración de todos los parámetros nvmem, que no son necesariamente los que están vigentes en ese momento.

Para obtener los parámetros de red actuales en uso, el nuevo comando **show ip** se ha agregado. Además de los parámetros de red, este comando también muestra el modo IP actual (estático frente a DHCP), el estado del cliente DHCP y el estado de las aplicaciones Telnet y SNMP (que sólo se inician si existe una IP válida).

Se ha agregado un comando adicional, **show dhcp**, con fines informativos. Este comando muestra los valores recibidos del servidor DHCP, así como el estado del tiempo de concesión. Los valores de hora mostrados se muestran en el formato HH:MM:SS y son relativos a la hora actual del sistema, que también se muestra.

La asignación de valores estáticos para cualquiera de los parámetros de red configurables debe entrar en vigor inmediatamente y reemplazar la configuración actual sin ninguna otra acción. Esto permite que algunos de los parámetros permanezcan dinámicos, mientras se fijan otros. Por ejemplo, DHCP se puede utilizar para obtener la dirección IP, mientras se conserva la configuración para el servidor TFTP configurado a través de la CLI. La única excepción a esto es cuando se pasa de utilizar una IP estática a DHCP. Dado que el cliente DHCP sólo se instala en el arranque según sea necesario, la transición de una IP estática a DHCP requiere que el sistema se reinicie para que DHCP tenga efecto.

Indicadores luminosos

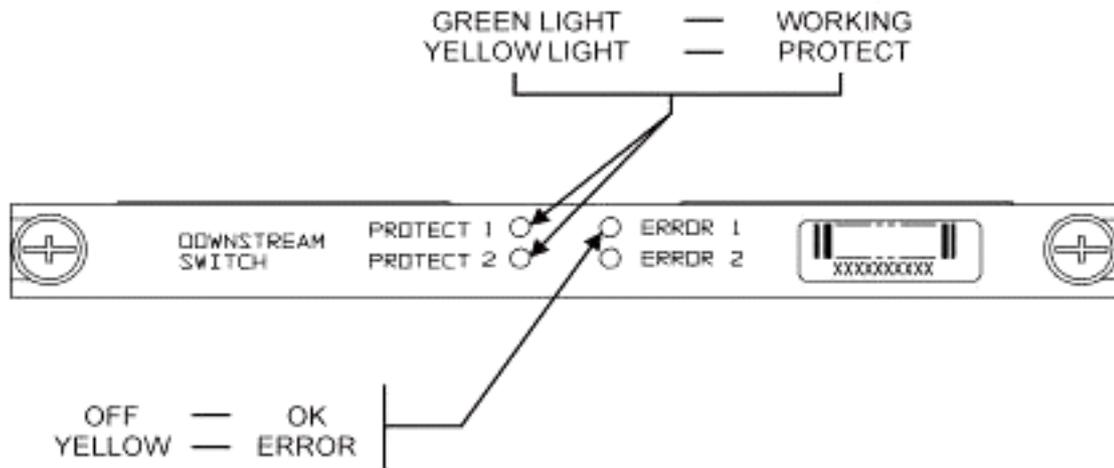
Los indicadores luminosos LED del módulo correspondiente pasarán de verde a ámbar/amarillo. El diseño es opuesto al de la parte posterior, lo que significa que si el grupo de switches de la izquierda del encabezado en la ranura 1 del switch falla en un modo 8+1, los LED de protección 1 de la derecha pasarán de verde a ámbar para mostrar que los relés han cambiado.

La siguiente imagen muestra las diferencias de color en los LED y no representa una falla específica.



- Luz LED n° 1 Verde/Amarillo para indicar que funciona/protege 1
- LED n.º 2 Verde/Amarillo para indicar que funciona/protege 2
- LED n.º 3 apagado/amarillo para indicar un problema en el canal 1
- LED n.º 4 apagado/amarillo para indicar un problema en el canal 2

A continuación se muestra el diagrama de módulos.



La siguiente imagen muestra los indicadores del controlador Ethernet.

- SYS
 - Self Test Blinking Green
 - System OK Steady On Green
 - ERR Command Error Off/Green
 - ACT (Activity) Blinking Green 10 Base T
 - LINK Off/Green 10 Base T
 - Tx Blinking Green Serial Port
 - Rx Blinking Green Serial Port
- Power Supply:**
- OFF/ON Off/Green



[Problemas de cliente y aplicaciones](#)

Algunos puntos que pueden considerarse problemas son el coste, la utilización de todos los componentes, la pérdida de inserción, el diseño físico, los conectores y el cable pequeños, y la disponibilidad y compatibilidad de estos componentes.

La pérdida de inserción de 6 dB mientras estaba en el modo de trabajo podría ser un problema. También hay más pérdidas de inserción (aproximadamente 1-2 dB) cuando el switch entra en el modo de protección. Esto depende de la frecuencia que está usando para DS. La pérdida de inserción de US es de aproximadamente 4.5 dB.

La aceptación del sector puede llevar tiempo en lo que respecta a los conectores MCX más pequeños y al cable coaxial más pequeño que se utiliza para la solución. AOL Time Warner decidió adquirir 3,050 metros (10,000 pies) de este estilo de cable para redistribuir algunos de los cableados en Estados Unidos en sus cabeceras. Charter también está usando este cableado ahora. Si empiezan a usar el cable, será cuestión de tiempo antes de que ellos y otros fabricantes empiecen a usar el nuevo conector más pequeño también. El nuevo convertidor ascendente de

VCom utiliza ahora conectores MCX.

WhiteSands Engineering genera los kits de cables para Cisco. Cisco debe disponer de un estilo mínimo de kits de cables para satisfacer nuestro diseño recomendado. Puede ir directamente a WhiteSands para obtener pedidos especiales por cable. Puede obtener las herramientas necesarias para la conexión de CablePrep o WhiteSands.

El número de parte del switch RF distingue entre mayúsculas y minúsculas. Debe ingresar **uBR-RFSW** para pedir el switch.

Problemas operativos

Tenga en cuenta las situaciones que se describen a continuación.

Una tarjeta de línea 5x20 se equivoca y la tarjeta de línea de protección toma el control. Desconecta la tarjeta de línea defectuosa y la señal DS de la retroalimentación de la tarjeta de línea de protección al final del cable desconectado que se solía conectar a la otra tarjeta de línea y ahora no se termina.

Esto causará una discordancia de impedancia y una energía reflectante que será de aproximadamente 7 dB hacia abajo desde la señal original. Esto se debe a que el divisor en el chasis del switch sólo tendrá aproximadamente 7 dB de aislamiento cuando el puerto común no se termine. Las frecuencias afectadas estarán relacionadas con la longitud física del cable que se desconectó.

Esta idea ayudará a mitigar el riesgo potencial de que el nivel de DS cambie hasta 3 dB:

- Termine los cables DS con terminadores de 75 ohmios. Es posible que se necesiten terminadores MCX especiales.

En otra situación, el acceso Telnet del switch RF desde la consola uBR10K crea entradas dobles al escribir. Una solución consiste en desactivar el eco local. Por ejemplo, desde la CLI, ejecute **telnet ip address /noecho**. Debe presionar **control break** para salir, o **control]** para el modo de comando Telnet, y escribir **quit** o **send break**. Otra forma de desconectarse es presionar **Control+Mayús+6+x** y escribir **disco 1** de la línea de comandos uBR. Para algunas secuencias de interrupción estándar, consulte [Combinaciones de Secuencias Estándar de Teclas de Interrupción Durante la Recuperación de Contraseña](#).

Aplicaciones confusas

Consideremos la situación descrita a continuación.

Los cables de protección de US en la uBR se pueden utilizar para probar la potencia de la señal para el funcionamiento correspondiente. Por ejemplo, suponga que tiene el switch en el modo 8+1, un blade en funcionamiento en la ranura 8/0 del uBR, un blade de protección en la ranura 8/1 y el cableado en funcionamiento hasta la ranura 1 del switch. Para probar el nivel de energía de US en US0 de la tarjeta 8/0, Telnet o la consola en el switch y ejecute el **comando switch 1 1**. Esto activará el relay desde la ranura 1 del switch para el Módulo 1, que también se conoce como puerto A del switch. Desconecte el cable en US0 del servidor blade de protección y conéctelo a un analizador de espectro. Podrá probar la señal de US que en realidad va al US0 en funcionamiento.

Comandos show

Utilice los siguientes comandos para resolver problemas.

show version

```
rfswitch>sh ver
Controller firmware:
  RomMon: 1935033 V1.10
  Bootflash: 1935022E V2.20
  Flash: 1935030F V3.50
Slot      Model      Type      SerialNo  HwVer  SwVer  Config
  999      193-5001  10BaseT   1043      E      3.50
  1        193-5002  upstream  1095107   F      1.30  upstream
  2        193-5002  upstream  1095154   F      1.30  upstream
  3        193-5002  upstream  1095156   F      1.30  upstream
  4        193-5002  upstream  1095111   F      1.30  upstream
  5        193-5002  upstream  1095192   F      1.30  upstream
  6        193-5002  upstream  1095078   F      1.30  upstream
  7        193-5002  upstream  1095105   F      1.30  upstream
  8        193-5002  upstream  1095161   F      1.30  upstream
  9        193-5002  upstream  1095184   F      1.30  upstream
  10       193-5002  upstream  1095113   F      1.30  upstream
  11       193-5003  dnstream  1095361   J      1.30  dnstream
  12       193-5003  dnstream  1095420   J      1.30  dnstream
  13       193-5003  dnstream  1095417   J      1.30  dnstream
```

show module all

```
rfswitch>show module all
Module      Presence  Admin  Fault
  1          online   0      ok
  2          online   0      ok
  3          online   0      ok
  4          online   0      ok
  5          online   0      ok
  6          online   0      ok
  7          online   0      ok
  8          online   0      ok
  9          online   0      ok
  10         online   0      ok
  11         online   0      ok
  12         online   0      ok
  13         online   0      ok
```

show config

```
rfswitch>show config
IP addr: 10.10.3.3
Subnet mask: 255.255.255.0
MAC addr: 00-03-8F-01-04-13
Gateway IP: 10.10.3.170
TFTP host IP: 172.18.73.165
DHCP lease time: infinite
TELNET inactivity timeout: 600 secs
```

```
Password: xxxx
SNMP Community: private
SNMP Traps: Enabled
SNMP Trap Interval: 300 sec(s)
SNMP Trap Hosts: 1
    172.18.73.165
Card Protect Mode: 8+1
Protect Mode Reset: Disabled
Slot Config: 0x03ff 0x1c00 (13 cards)
Watchdog Timeout: 20 sec(s)
Group definitions: 5
ALL      0xffffffff
GRP1     0xaa200000
GRP2     0x55100000
GRP3     0x00c80000
GRP4     0x00c00000
```

Especificaciones del switch RF

La siguiente lista muestra las especificaciones del switch RF.

- Alimentación de entrada CA: de 100 a 240 V CA, 50/60 Hz, intervalo de funcionamiento: 90-254 V CA
- Alimentación de CC: tres bloques de terminales -48/-60 V CC, intervalo: de -40,5 a -72 V CC, onda/ruido de 200 mVpp
- Intervalo de temperatura: de 0 a +40 °C, intervalo de temperatura de funcionamiento: de -5 a +55 °C
- Control de unidad 10BaseT SNMP Ethernet y bus RS-232: D macho de 9 pines
- Conectores de RF: MCX, Impedancia: 75 ohmios
- Potencia de entrada máxima de radiofrecuencia: +15 dBm (63,75 dBmV)
- Tipo de switch: Electro-mech, absorbente para la trayectoria de trabajo, no absorbente en la trayectoria de protección
- Rango de frecuencia DS: de 54 a 860 MHz
- Pérdida máxima de inserción de DS: 5,5 dB de funcionamiento a salida, 8 dB de protección a salida
- Pérdida de inserción de DS: +1,1 dB de funcionamiento a salida, +2,1 dB de protección a salida
- Pérdida de retorno de salida de DS: superior a 15,5 dB
- Aislamiento de DS: más de 60 dB trabajando para trabajar, más de 20 dB trabajando para proteger respectivamente cuando está en modo de protección, y más de 60 dB trabajando para proteger cuando está en modo de funcionamiento
- Intervalo de frecuencia ascendente: de 5 a 70 MHz
- Pérdida máxima de inserción ascendente: 4,1 dB de entrada a funcionamiento, 5,2 dB de entrada para proteger
- Latencia de pérdida de inserción de US: + 0,4 dB de entrada a funcionamiento, + 0,6 dB de entrada para proteger
- Pérdida de retorno de entrada de US: superior a 16 dB
- Aislamiento de US: más de 60 dB trabajando para trabajar, más de 20 dB trabajando para proteger respectivamente cuando se encuentra en modo de protección y más de 60 dB trabajando para proteger cuando está en modo de funcionamiento
- Formato físico: 19 x 15,5 x 5,25 (482 mm x 394 mm x 133 mm), Peso: 36 libras

Información Relacionada

- [Cisco RF Switches](#)
- [Consejos y configuración de N+1 para uBR 10K con tarjetas MC28C](#)
- [Soporte Técnico - Cisco Systems](#)