

# Redundância N+1 usando o switch Cisco RF

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Switch de RF](#)

[Configuração e operação do Switch RF](#)

[Informações Relacionadas](#)

## [Introduction](#)

Este documento fornece informações sobre redundância N+1 usando o Switch Cisco® RF.

## [Prerequisites](#)

## [Requirements](#)

Não existem requisitos específicos para este documento.

## [Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

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.

## [Conventions](#)

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

## [Informações de Apoio](#)

Para obter o máximo de valor por seu dinheiro, muitas operadoras de cabo decidiram fornecer redundância para sua rede de fibra óptica na forma de fontes de alimentação de reserva extra no nó de fibra, no UPS (Uninterruptible Power Supply [fonte de alimentação ininterrupta]) com gás

natural e bateria de reserva, e transmissores de fibra extras no nó. Fibras escuras extras também podem ser alocadas para cada nó no caso de falha de fibra.

Como explicado acima, o hardware é a primeira coisa a cobrir na fábrica externa. E os sinais upstream (US) e downstream (DS) reais que trafegam no meio de transporte? Em relação aos EUA, a Cisco implementou técnicas de gerenciamento de espectro avançado para manter os modems on-line e transmitindo da melhor forma. Algumas dessas técnicas são salto de frequência com capacidade "olhe antes de dar esse passo" avançada, através da placa-filha integrada analisadora de espectro na placa S. A Cisco também incorporou alterações de perfil de modulação e de largura de canal. Todos esses recursos permitem que o modem permaneça em uma parte limpa do espectro, utilize um perfil de modulação mais robusto e/ou mude a largura do canal para manter o serviço otimizado em relação à transferência e disponibilidade. Ao observar as frequências DS, você tem uma opção de 64 ou 256-QAM. Embora estes esquemas de modulação sejam muito menos robustos do que os EUA em QPSK ou 16-QAM, o espectro DS é muito mais previsível e está sob controle do que o espectro dos EUA.

A disponibilidade de hardware no fim de cabeçalho é o próximo fator lógico a ser focalizado. Se uma única fonte de CA ou CC falhar, o backup do gerador pode ser usado com fontes de alimentação redundantes, caso uma funcione mal.

Outro ponto de falha do hardware pode ser a alimentação do CMTS (Cable Modem Termination System). As fontes de alimentação uBR10K utilizam um algoritmo para backup e balanceamento de carga/compartilhamento. Às vezes isso é chamado de N:1, o que significa 1 para N backups com balanceamento de carga. Nesse caso, será 1:1, e você perceberá que a potência DC total é um pouco maior, com dois módulos de entrada de energia (PEMs), do que se um fosse usado para toda a carga. Emita o comando **sh cont clock-reference** para exibir essas informações.

```
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 se concentrar na disponibilidade de placas de linha CMTS, a Cisco desenvolveu um protocolo para especificar como os CMTSs se comunicarão entre si em um cenário de alta disponibilidade. Esse protocolo é chamado de Hot Standby Connection-to-Connection Protocol (HCCP). Esse protocolo fornece uma pulsação entre o dispositivo de proteção e os dispositivos em funcionamento para manter as interfaces/dispositivos sincronizados com tabelas MAC, configurações e assim por diante. A Cisco também desenvolveu o RF Switch para oferecer alta disponibilidade no nível de domínio MAC em vez de chassi para chassi. Um domínio MAC também pode ser considerado como uma sub-rede de RF, que é um DS e todos os USs associados.

A Cisco oferece redundância 1+1 no chassi da série uBR7200 por alguns anos, no entanto, um chassi inteiro deve permanecer ocioso como um chassi de proteção. A vantagem de fazer 1+1 é que nenhum Switch RF é necessário, mas menos escalável. O uso de um Switch RF permite que a redundância seja feita no nível da interface para disponibilidade N+1. Isso significa 1 para backup N sem balanceamento de carga/compartilhamento. Em vez de um chassi inteiro sentado em modo ocioso, você pode ter uma placa ou interface ociosa/protetora protegendo muitas outras interfaces. O uBR100012 pode ser configurado como uma placa que protege sete outras. Isso ajuda na economia porque agora oferece disponibilidade 7+1 e também passa os requisitos necessários para o PacketCable.

Depois que esses pontos forem abordados, você deve ter certeza de que possui redundância para o backhaul, também conhecido como WAN ou LAN side, dependendo de como você olha para ele. O Hot Standby Router Protocol (HSRP) existe há anos e permite caminhos redundantes entre roteadores para fornecer um nível de disponibilidade necessário para esse ponto único de falha. O verdadeiro impulso para esses recursos é o VoIP e o aumento das pressões competitivas para fornecer o serviço mais estável/disponível para o cliente.

## Seqüência Operacional de Eventos

### **Solução uBR10K**

O HCCP ocorre primeiro entre o chassi por meio do heartbeat. Como a solução uBR10K está toda contida em um chassi, a pulsação pode não ser relevante. Se a comunicação interna e as alterações de interface forem bem-sucedidas, o HCCP continuará a enviar um comando ao Switch RF para alternar os relés apropriados.

### **Solução uBR7200**

O HCCP ocorre primeiro entre o chassi por meio do heartbeat. Um comando é então enviado do 7200 de proteção para o conversor ascendente (UPx) para alterar a frequência. O UPx envia um ACK. O Protect 7200 envia um comando para desativar o módulo UPx em funcionamento e espera por um ACK. O Protect 7200 envia um comando para ativar o módulo UPx de proteção e espera por um ACK. Se tudo isso funcionar ou nenhuma ACK for enviada do módulo UPx em funcionamento, ele continuará e enviará um comando ao switch para alternar os relés apropriados.

Há dois tipos de mecanismos de pulsação que são relevantes para o HCCP. Eles estão listados abaixo.

1. helloACK entre o trabalho e a proteção — O LC de proteção envia uma mensagem de saudação para cada um dos LCs em funcionamento em seu grupo e espera um helloACK em resposta. A frequência de envio do hello e do helloACK é configurável no LC de proteção com CLI. Além disso, o tempo mínimo de saudação no 7200 é de 0,6 segundos, enquanto o mínimo no uBR10K é de 1,6 s.
2. Mecanismo de pulso de sincronização — Este é um mecanismo de pulsação do plano de dados HCCP e sua frequência não é configurável. Os pulsos de sincronização são enviados por cada LC em funcionamento para seu LC de proteção de peer. Este pulso de sincronização é enviado uma vez por segundo. Se três pulsos síncronos forem perdidos, o correspondente será declarado inativo. A Cisco está trabalhando em um mecanismo rápido de detecção de falhas para detectar um travamento em funcionamento no manipulador de exceções em menos de 500 ms. A versão desejada é 12.2(15)BC. No VXR, a falha pode ser detectada por ambos os mecanismos, entretanto, como o uBR10K é todo HCCP interno, apenas o segundo é relevante.

## Switch de RF

A Cisco decidiu usar um Switch RF externo em vez de uma placa de linha ou cabeamento interno que operaria como um Switch RF devido à escalabilidade e complexidade futuras. O switch externo pode ser empilhado e usado para vários cenários, densidades diferentes e equipamentos antigos.

Há 252 conexões na parte traseira do switch em um pacote de 3 unidades de rack (3RU). 1RU tem 1,75 polegadas. O conversor ascendente VCom HD4040 é de 2RU.

Se o backplane estiver configurado de uma certa maneira para um switch interno, você limitará a flexibilidade para fazer densidades de placa de linha diferentes posteriormente. Se uma placa de linha for muito densa, muitas portas US serão afetadas por falhas específicas a um único US ou DS e placa em geral. É por isso que um switch e uma redundância são necessários desde o início. Mais densidade equivale a mais clientes afetados por um único evento. O que acontece se placas DS puras e placas US puras forem vendidas? No futuro, você poderá combinar portas US e DS em placas de linha. O design externo protege ainda mais meu investimento no futuro.

Você nunca poderá fazer redundância entre os chassis com um switch interno. Para economizar dinheiro e ter quatro 7200 uBRs com backup de um, é necessário um Switch RF externo. A menos que você esteja pensando em ter placas de linha em um chassi com backup de outro no mesmo chassi. O único problema é que se o chassi inteiro cair, você não terá backup.

Os números de disponibilidade podem ser melhores para um switch externo (pelo menos no que diz respeito à eletrônica, não ao cabeamento) devido aos componentes menos ativos. Como o switch tem um design passivo total no chassi, o modo de funcionamento normal está operacional, mesmo que os módulos ativos sejam removidos. Os relés estão localizados apenas no caminho de proteção com um caminho de trabalho totalmente passivo e podem ser alternados para testar o switch sem afetar o modo de funcionamento real. Isso significa que o modo de funcionamento normal não será afetado por uma falha de energia no switch, por um módulo de switch sendo removido ou por uma falha no switch. O negativo disso é a perda de inserção de potencialmente 6 a 8 dB na maior frequência DS de 860 MHz.

O design externo também permite a migração de cabeamento e trocas de placas de linha. Se alguém quiser atualizar de uma placa 2x8 para uma placa 5x20, a placa de linha pode ser forçada a fazer failover para o modo de proteção. A placa de linha pode ser alterada no ritmo que você determinar com a placa 5x20 mais nova e mais densa e conectada para domínios futuros. Os dois domínios que estavam no modo de proteção serão então comutados de volta para a interface/domínios correspondentes na placa 5x20. Outros problemas devem ser abordados, como o 5x20 terá conversores internos e comandos de conector.

O painel frontal tem os LEDs, o cabo de alimentação para CA ou CC, a conectividade Ethernet, a conectividade RS-232 e um interruptor de alimentação para designar CA, CC ou desligado. Uma ferramenta de extração de cabos é enviada com cada switch também. Certifique-se de remover a inicialização de borracha antes do uso. A força de extração pode ser ajustada com uma chave de parafuso, parafusos no sentido horário na parte traseira da ferramenta.

A imagem abaixo é a vista frontal do Switch RF.

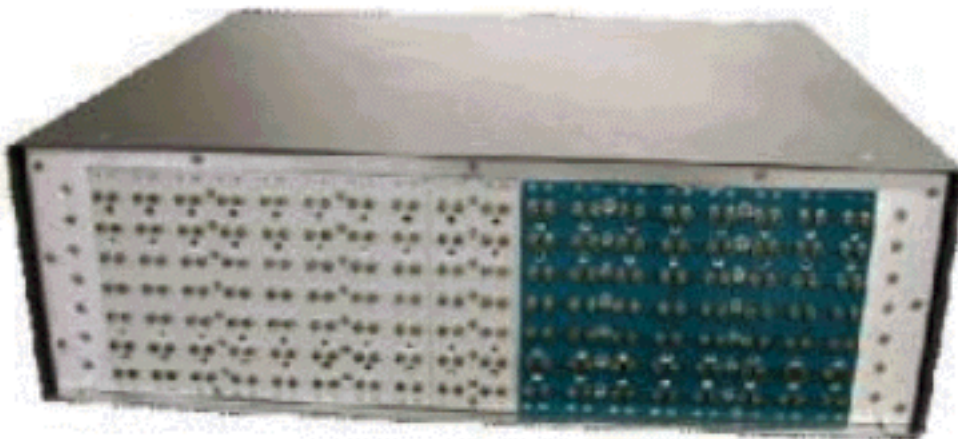


Há dez módulos US (mostrados em azul) e três DS (mostrados em cinza) instalados no Switch 3x10 RF. A parte inferior esquerda é conhecida como módulo N e está em branco. Os módulos na frente, começando do canto superior direito, são números de 1 a 13 e correlacionam-se às portas A-M. O Módulo de Upstream 1 tem todos os relés para a porta A nos slots de 1 a 8 e protege 1 e 2 na parte traseira. O módulo 2 está à esquerda e tem todos os relés para a porta H nos slots de 1 a 8 e protege 1 e 2.

Os módulos podem ser trocados e removidos em operação, no entanto, a extração da placa é muito difícil. É extremamente apertado e os dois parafusos cativos devem ser soltos antes de serem puxados para fora. Talvez você precise abrir com uma chave de fenda ou mudar para a esquerda e para a direita enquanto puxa para fora.

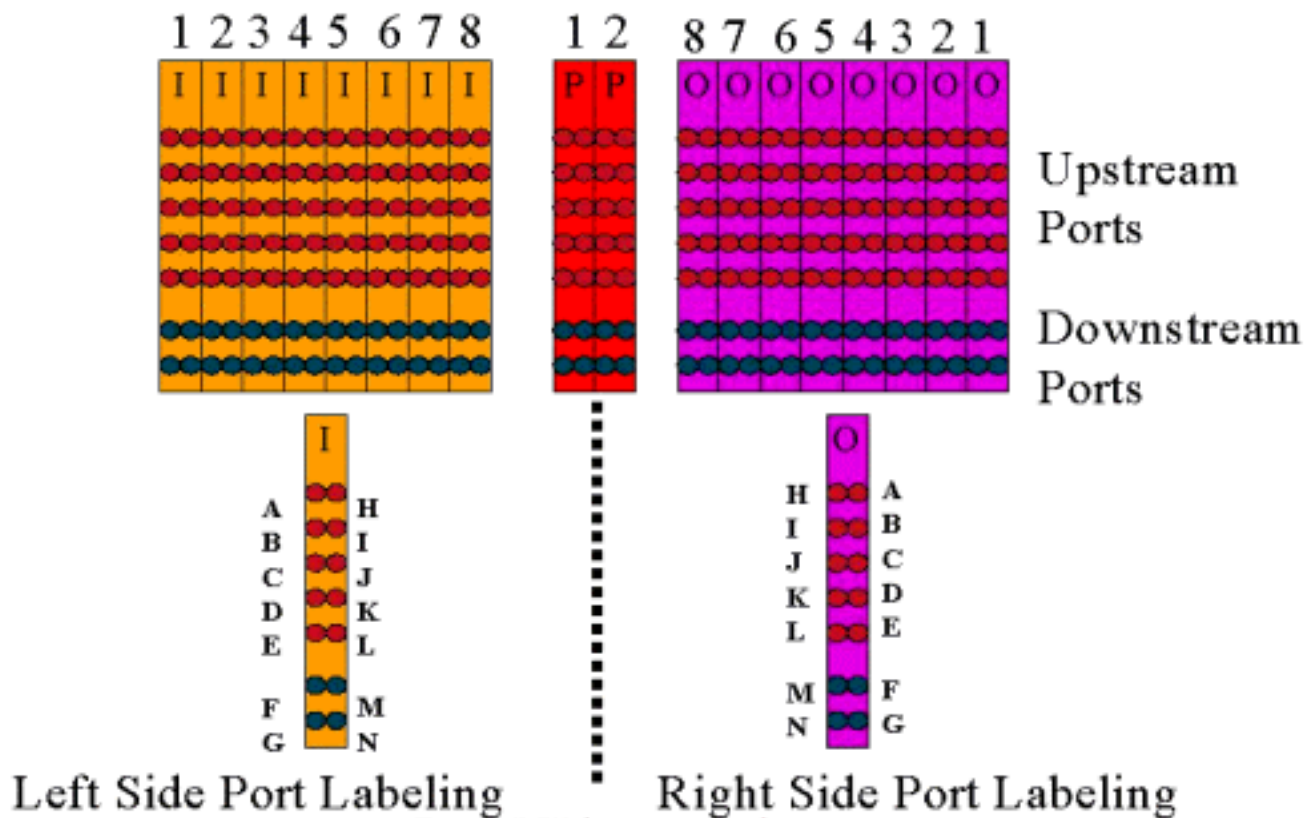
O painel traseiro tem etiquetas que dizem **CMTS**, **Protect** e **Cable Plant**. O lado **CMTS** é para as entradas de trabalho. O lado da **Fábrica de Cabos** contém todas as saídas para alimentar a fábrica de cabos.

A figura abaixo é a vista traseira do Switch RF.



As oito entradas de trabalho são numeradas da esquerda para a direita. As duas proteções estão no meio, e as 8 saídas estão à direita.

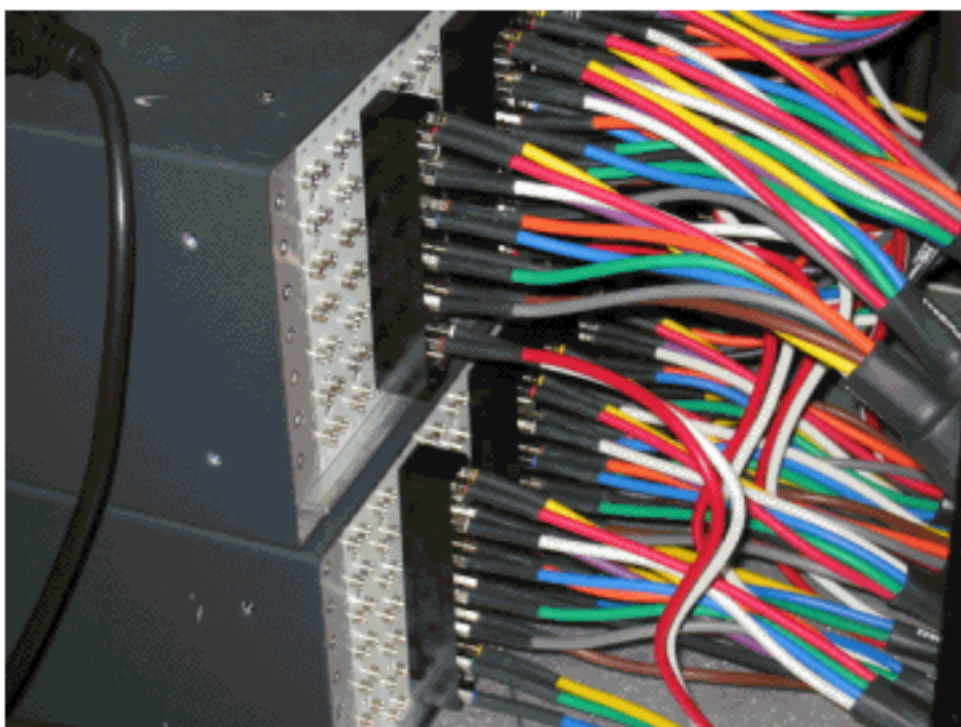
A figura abaixo é o esquema de numeração do Switch RF.



**Observação:** a porta N não é usada.

A saída (roxo colorido) representa a planta do cabo. A saída 1 está na extrema direita, enquanto a entrada 1 está na extrema esquerda. As portas também são espelhadas. Lembre-se de que a porta N não é usada. Apenas certifique-se de usar a consistência na fiação.

Esta imagem abaixo é a vista de trás do Switch RF com o cabeçalho de 14 portas e o cabo mini coaxial Belden especial com conectores MCX.



Os conectores MCX podem ser conectados diretamente ao switch, no entanto, você corre o risco de perder conexões, emissões e possíveis desconexões intermitentes. A Cisco desenvolveu um

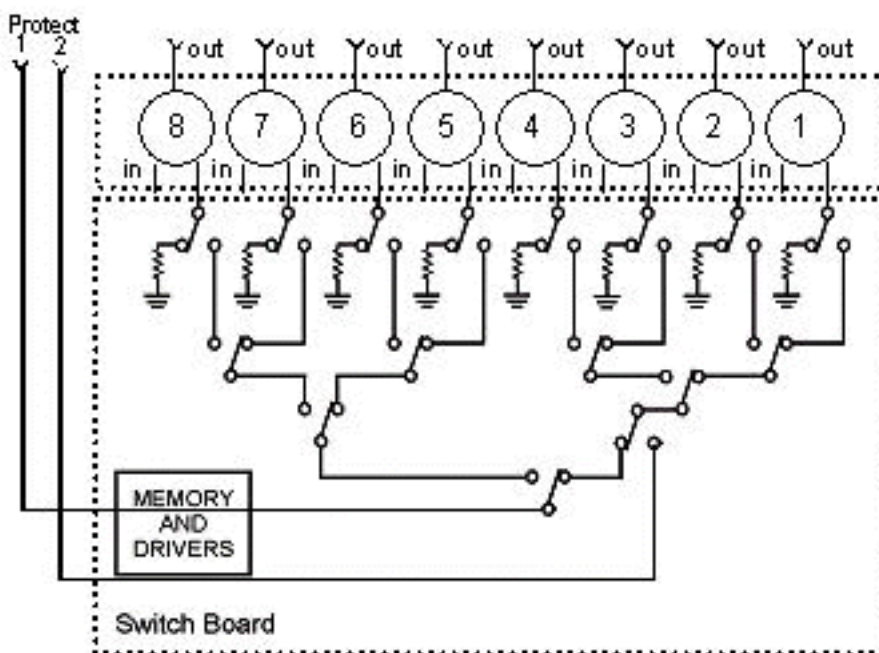
cabeçalho para resolver esses problemas.

Os conectores MCX se encaixam no cabeçalho e há uma ferramenta especial enviada com cada compra de switch para extração. O encabeçamento possui dois pinos guia e permite apenas um encaixe. Há um leve bisel na borda superior para indicar a parte superior do cabeçalho. Há dois parafusos de cabeça chata para conectar o conector ao switch. Um suporte de gerenciamento de cabos também é fornecido com cada Switch RF.

**Dica:** você também pode instalar o cabeçalho no switch e inserir os conectores MCX no cabeçalho. Isso pode facilitar a instalação. Não aperte o conector no switch até que todos os conectores estejam instalados.

## Configuração e operação do Switch RF

A figura abaixo é um diagrama de blocos do Switch RF.



Os componentes do combinador estão localizados no chassi do switch, mas os relés estão em cada módulo individual removível. Cada retransmissão termina com uma carga de 75 ohms, somente no caminho de proteção, não no caminho de entrada/funcionamento.

Configure a comunicação serial com o switch, fazendo um consolo com o HyperTerminal ou o TeraTerm, um cabo de console/rollover, o adaptador de 9 pinos para RJ-45 da Cisco e com uma taxa de baud de 9600.

Defina um endereço IP e uma máscara emitindo o comando **set ip addr ip add subnet mask**. Depois de fazer isso, será possível estabelecer uma sessão Telnet e definir uma senha Telnet. Em seguida, defina o esquema de proteção, seja 4+1 ou 8+1, emitindo o comando **set port 4/8**. O padrão é 8+1, onde o Protect 1 cobre todos os oito slots de entrada. No modo 4+1, proteja 1 cobre os slots de 5 a 8 e proteja 2 cobre os slots de 1 a 4.

A string de comunidade SNMP é **privada** e pode ser alterada, mas não é suportada no uBR10K.

### Configurando bitmaps

O próximo ponto importante a ser definido são os grupos de switch, que exigem bitmaps hexadecimais. O bitmap do Switch RF é um total de 32 bits (8 caracteres hexadecimais) de comprimento e é calculado conforme mostrado abaixo. Uma calculadora do Excel está disponível para uso.

Considere o grupo 1, que tem quatro cabos US conectados à esquerda de um cabeçalho de Switch RF no slot 1, e um DS conectado à esquerda desse mesmo cabeçalho. As portas usadas seriam ABCDF. Para cada porta envolvida na comutação, o bit correspondente é definido como 1. Se uma porta não estiver envolvida na comutação, esse bit de porta será definido como 0.

O grupo 1 é mostrado abaixo.

```
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      0 - decimal
= A A 2 0 0 0 0 0 (in hexadecimal).
```

**Observação:** os bits 14 a 32 são "do not care" (X).

Para o grupo 2, o lado direito do cabeçalho está conectado e o mapa de bits é mostrado abaixo.

```
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)(0 0 0 0)
  5    5    1    0      0      0      0      0      0      0      0      0      0      0      0      0      0      0
= 5 5 1 0 0 0 0 0 (hex)
```

É necessário configurar grupos de switch ou o switch não entenderá quais portas e relés alternar. Ao configurar bitmaps, o número pode ser inserido como formato decimal ou deve ser inserido com 0x na frente do código hexadecimal para que o software reconheça que é hexadecimal. Emita o comando **set group2 0x55100000** para atribuir o bitmap. Group2 é uma sequência de palavras alfanumérica que deve começar com uma letra.

**Dica:** os dois bitmaps acima fazem parte do projeto de referência recomendado. O modo 4+1 é totalmente diferente e é recomendável usar a calculadora de bitmap. Se estiver fazendo um esquema de proteção 4+1, você terá quatro grupos HCCP. Os grupos de HCCP 1 e 2 na placa de proteção 2 e os grupos 3 e 4 de HCCP na placa de proteção 1. Além disso, proteger 1 cobre os slots 5-8 no switch, no entanto, na configuração do uBR esses slots são chamados de slots 1-4.

Se estiver alternando portas individuais em vez de domínios MAC, você deve saber qual esquema de proteção está executando e usar a tabela abaixo para saber qual número de grupo deve ser usado. Suponha que o switch esteja no modo 4+1. O comando é mostrado abaixo para o uBR10K.

```
hccp 1 channel-switch 1 ds rfs witch-module 1.10.84.3 26 1
hccp 1 channel-switch 1 us rfs witch-module 1.10.84.3 10 1
```

Indica o endereço IP do switch e o módulo 26, que indica que a placa de proteção 2 está fazendo backup da porta G em um esquema 4+1, e o módulo 10, que indica que a placa de proteção 2



está fazendo backup da porta C. Tudo isso no slot 1 do switch.

A tabela abaixo mostra os dois modos e qual número corresponde à respectiva porta.

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)

### [Configurando a configuração do slot](#)

O novo firmware permite que o chassi seja configurado para qualquer combinação de placas upstream/downstream. Isso é feito usando o novo comando CLI **set slot config USslots DS**.

Os parâmetros de **slots US** e **DSslots** são máscaras de bit hex integer de 16 bits que representam se o módulo está ativado/configurado para esse tipo de placa, com o bit mais à direita representando o módulo 1. Consulte a nova calculadora de bitmap para obter configurações automatizadas.

Por exemplo, se você quisesse configurar um chassi com quatro placas de linha, placas upstream nos módulos 1-2 e placas downstream nos módulos 3-4, você executaria o comando **set slot config 0x0003 0X000c**.

A configuração do slot é armazenada em nvmem, separada do firmware do aplicativo. Isso permite futuras atualizações do firmware do aplicativo sem exigir que o usuário re programe a configuração do slot e permite uma única distribuição de código de aplicativo para todas as configurações do Switch RF.

Normalmente, a fábrica faria essa configuração quando a unidade fosse construída, no entanto, isso permitiria que você alterasse a configuração no campo, se desejar, e usasse qualquer número/combinção de placas que você precisasse no futuro.

Uma configuração de exemplo é fornecida a seguir.

```
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
```

## [Testando os relés do switch RF](#)

A Cisco recomenda testar os relés uma vez por semana e pelo menos uma vez por mês. Use o console ou Telnet no switch e emita o comando **test module**. Se uma senha for definida no Switch RF, emita o comando **password *password name*** para usar o comando test. Isso testará todos os relés de uma só vez e voltará ao modo de trabalho normal. Não use esse comando de teste enquanto estiver no modo de proteção. **Não use esse comando de teste enquanto estiver no modo de proteção.**

**Dica:** você pode alternar os relés no switch sem afetar o conversor ascendente ou qualquer um dos modems. Isso é importante se você testar os relés sem realmente trocar qualquer uma das placas de linha ou os conversores ascendentes correspondentes. Se um relé estiver ativado no switch e ocorrer um failover, ele entrará no estado correto e não apenas alternar de um estado para outro.

Emita o comando **switch 13 1** para testar a porta G no slot 1 do Switch. Você pode testar um bitmap inteiro emitindo o comando **switch *group name* 1**. Emita o comando **switch *group name* 0** (ou **idle**) para desativar os relés para o modo de trabalho normal.

Além disso, o cliente deve executar um teste de failover CLI de um grupo HCCP (emita o comando **hccp *g switch m***) do CMTS para testar a placa de proteção e proteger o caminho. Esse tipo de failover pode levar de 4 a 6 segundos e pode fazer com que uma pequena porcentagem de modems fique off-line. Assim, este teste deve ser realizado com menor frequência e apenas durante os horários fora de pico. Os testes acima ajudarão a melhorar a disponibilidade geral do sistema.

## [Atualizando o código do switch RF](#)

Siga as etapas abaixo.

1. Carregue as novas imagens no uBR com um disco Flash no slot 0.
2. Configure os comandos abaixo no uBR.

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

3. Use o console para se conectar ao switch e execute o comando **set tftp-host {ip-addr}**. Use o endereço IP do uBR para transferências TFTP.
4. Emita a **cópia tftp:rfs330-bf-1935022g bf:** para carregar o flash de inicialização e **copiar tftp:rfs330-fl-1935030h fl:** para carregar o Flash.
5. Reinicialize ou recarregue para que o novo código seja executado. Digite **PASS SYSTEM** e **Save Config** para atualizar os novos campos nvram. Reinicialize novamente para que tudo entre em vigor.

**Aviso:** talvez seja necessário redefinir algumas configurações após o recarregamento, como o endereço IP do switch. Revise a configuração do switch após o recarregamento para verificar. Depois de atualizado para a versão 3.5, um endereço de gateway padrão pode ser adicionado ao switch e novas atualizações para o switch podem ser feitas remotamente em sub-redes. O único limite é que se estiver carregando de estações Unix, o novo nome da imagem deverá ser letras minúsculas. Essa nova imagem também adiciona uma opção de cliente DHCP e uma configuração de chassi/módulo.

## Operação do DHCP

Esta versão inclui suporte total para um cliente DHCP. A operação DHCP é habilitada por padrão, a menos que o usuário tenha definido um IP estático a partir da CLI. Os comandos foram adicionados/aprimorados para suportar a operação DHCP.

Quando o Switch RF é inicializado, ele verifica se o DHCP foi ativado. Isso é feito via CLI de várias maneiras. Você pode usar qualquer um dos seguintes comandos para ativar o DHCP:

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

O Switch RF não assume mais um IP estático de 10.0.0.1 como nas versões anteriores à 3.00.

Se habilitado, o Switch RF instala o cliente DHCP e tenta localizar um servidor DHCP para solicitar um aluguel. Por padrão, o cliente solicita um tempo de leasing de 0xffffffff (leasing infinito), mas isso pode ser alterado com a emissão do comando **set dhcp lease leasetime\_secs**. Como o tempo real de aluguel é concedido a partir do servidor, esse comando é usado principalmente para depuração/teste e não deve ser necessário para a operação normal.

Se um servidor estiver localizado, o cliente solicitará configurações para endereço IP e máscara de sub-rede, um endereço de gateway e a localização de um servidor TFTP. O endereço do gateway é retirado da opção 3 (opção do roteador). O endereço do servidor TFTP pode ser especificado de várias maneiras. O cliente verifica a opção do próximo servidor (siaddr), a opção 66 (nome do servidor TFTP) e a opção 150 (endereço do servidor TFTP). Se as três opções acima estiverem ausentes, o endereço do servidor TFTP assumirá como padrão o endereço do servidor DHCP. Se o servidor conceder um leasing, o cliente DHCP registra o tempo de leasing oferecido para renovação e continua com o processo de inicialização, instalando os outros aplicativos de rede (Telnet e SNMP) e a CLI.

Se um servidor não estiver localizado dentro de 20 a 30 segundos, o cliente DHCP será suspenso e a CLI será executada. O cliente DHCP será executado em segundo plano tentando entrar em contato com um servidor aproximadamente a cada cinco segundos até que um servidor seja localizado, um IP estático seja atribuído via CLI ou o sistema seja reinicializado.

A CLI permite que o usuário substitua qualquer configuração de rede que possa ser recebida pelo servidor e atribua valores estáticos para essas configurações. Todos os parâmetros do comando **set xxx** são armazenados em nvmem e são usados em reinicializações. Como as configurações de rede atuais agora podem vir do DHCP ou da CLI, algumas alterações/novos comandos foram implementados. O comando **show config** existente foi alterado para mostrar as configurações de todos os parâmetros nvmem, que não são necessariamente os que estão em vigor no momento.

Para obter os parâmetros de rede atuais em uso, o novo comando **show ip** foi adicionado. Além das configurações de rede, esse comando também mostra o modo IP atual (estático versus DHCP), o status do cliente DHCP e o status dos aplicativos Telnet e SNMP (que são iniciados somente se houver um IP válido).

Um comando adicional, **show dhcp**, foi adicionado para fins informativos. Esse comando mostra os valores recebidos do servidor DHCP, bem como o status do tempo de concessão. Os valores de tempo mostrados estão no formato HH:MM:SS e são relativos à hora atual do sistema, que

também é exibida.

A atribuição de valores estáticos para qualquer um dos parâmetros de rede configuráveis deve entrar em vigor imediatamente e substituir a configuração atual sem nenhuma ação adicional. Isso permite que alguns dos parâmetros permaneçam dinâmicos, enquanto corrigem outros. Por exemplo, o DHCP pode ser usado para obter o endereço IP, enquanto mantém a configuração do servidor TFTP definida via CLI. A única exceção a isso é quando vamos usar um IP estático para DHCP. Como o cliente DHCP só é instalado na inicialização conforme necessário, a transição de um IP estático para o DHCP exige que o sistema seja reinicializado para que o DHCP tenha efeito.

## LEDs

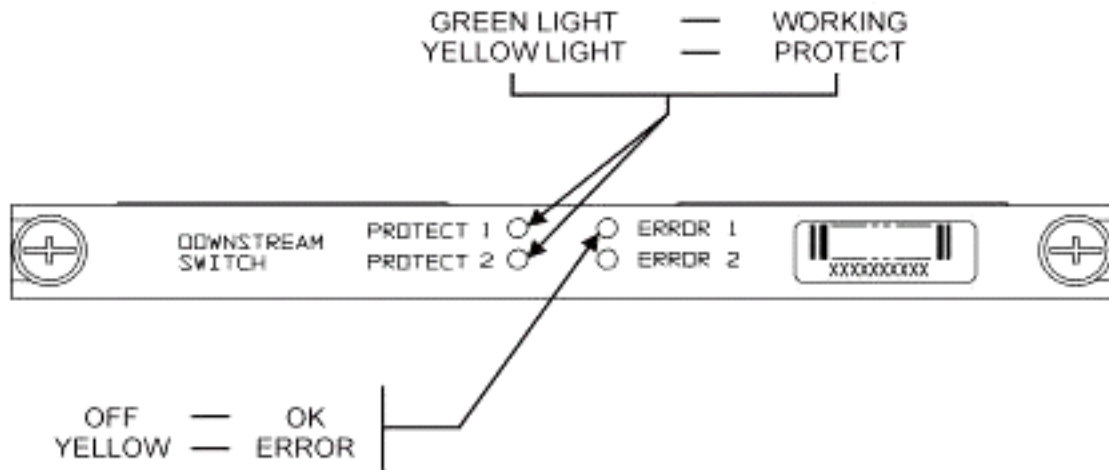
Os LEDs do módulo correspondente mudarão de verde para âmbar/amarelo. O layout é oposto do verso, o que significa que se o switch-group à esquerda do cabeçalho no slot 1 do switch falhar em um modo 8+1, os LEDs de proteção 1 à direita vão de verde a âmbar para mostrar que os relés alternaram.

A figura abaixo mostra as diferenças de cor nos LEDs e não representa um failover específico.



- LED nº 1 verde/amarelo para indicar funcionamento/proteção 1
- LED nº 2 verde/amarelo para indicar funcionamento/proteção 2
- LED #3 desligado/amarelo para indicar um problema no canal 1
- LED nº 4 desligado/amarelo para indicar um problema no canal 2

O diagrama do módulo é mostrado abaixo.



A figura abaixo mostra os indicadores do 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 |
| <b>Power Supply:</b> |           |                            |
| -OFF/ON              |           | Off/Green                  |



### [Questões e aplicativos do cliente](#)

Alguns pontos que podem ser considerados problemas são o custo, a utilização de todos os componentes, a perda de inserção, o layout físico, pequenos conectores e cabos e a disponibilidade e suporte desses componentes.

A perda de inserção de 6 dB no modo de trabalho pode ser um problema. Há também mais perda de inserção (cerca de 1 a 2 dB) quando o switch entra no modo de proteção. Isso depende da frequência que você está usando para o DS. A perda de inserção de US é de cerca de 4,5 dB.

A aceitação do setor pode levar tempo em relação aos conectores MCX menores e ao cabo coaxial menor sendo usado para a solução. A AOL Time Warner decidiu comprar 10.000 pés desse estilo de cabo para religar alguns dos cabeamentos norte-americanos em suas centrais de recepção. A Charter também está usando esse cabeamento agora. Se eles começarem a usar o cabo, será apenas uma questão de tempo até que eles e outros fabricantes comecem a usar o novo conector menor também. O novo conversor ascendente do VCom usa conectores MCX agora.

A WhiteSands Engineering produz os kits de cabos para a Cisco. A Cisco deve ter um estilo mínimo de kits de cabo para satisfazer nosso projeto recomendado. Você pode ir diretamente para WhiteSands para pedidos especiais de cabo. Você pode obter as ferramentas necessárias para a conexão a partir de CablePrep ou WhiteSands.

O número de peça do Switch RF diferencia maiúsculas e minúsculas. Você precisa inserir **uBR-RFSW** para solicitar o switch.

## Problemas operacionais

Considere as situações descritas abaixo.

Uma placa de linha 5x20 fica com defeito e a placa de linha de proteção assume o controle. Você desconecta a placa de linha defeituosa e o sinal DS da placa de linha de proteção de back-feeds até a extremidade do cabo desconectado que costumava estar conectado à outra placa de linha e agora não está terminado.

Isso causará uma incompatibilidade de impedância e energia refletiva que será cerca de 7 dB abaixo do sinal original. Isso ocorre porque o divisor no chassi do switch terá apenas cerca de 7 dB de isolamento quando a porta comum não for terminada. As frequências afetadas estarão relacionadas ao comprimento físico do cabo que foi desconectado.

Essa ideia ajudará a reduzir o risco potencial de alteração do nível DS em até 3 dB:

- Termine os cabos DS com terminadores de 75 ohm. Podem ser necessários terminadores MCX especiais.

Em outra situação, o acesso Telnet do switch RF do console uBR10K cria entradas duplas ao digitar. Uma solução é desativar o eco local. Por exemplo, na CLI, emita **telnet ip address /noecho**. Você precisa pressionar **control break** para sair ou **control ]** para o modo de comando Telnet e digitar **quit** ou **send break**. Outra maneira de desconectar é pressionar **Control+shift+6+x** e digitar **disco 1** na linha de comando uBR. Para algumas sequências de break padrão, consulte [Combinções de Sequência de Chave de Break Padrão Durante a Recuperação de Senha](#).

## Aplicações indefinidas

Considere a situação descrita abaixo.

A proteção dos cabos US na uBR pode ser usada para testar a intensidade do sinal para o correspondente funcionamento. Por exemplo, suponha que você tenha o switch no modo 8+1, um blade em funcionamento no slot 8/0 do uBR, um blade de proteção no slot 8/1 e o switch esteja conectado até o slot 1 do switch. Para testar o nível de energia US em US0 da placa 8/0, execute Telnet ou console no switch e emita o comando **switch 1 1**. Isso ativará a retransmissão do slot 1 do switch para o Módulo 1, também conhecido como porta A do switch. Desconecte o cabo em US0 da lâmina de proteção e conecte-o a um analisador de espectro. Você poderá testar o sinal dos EUA que realmente vai para o US0 em funcionamento.

## comandos show

Use os comandos abaixo para solucionar 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
```

## Especificações do RF Switch

A lista abaixo mostra as especificações do Switch RF.

- Potência de entrada AC — 100 a 240 Vac, 50/60 Hz, Faixa de operação — 90-254 Vac
- Alimentação DC — Três Bloco De Terminal -48/-60 Vdc, Faixa - -40,5 a -72 Vdc, 200 mVpp ondulação/ruído
- Faixa de temperatura — 0 a +40 °C, faixa de temperatura operacional — de -5 a +55 °C
- Controle da unidade 10BaseT SNMP Ethernet e barramento RS-232 — D macho de 9 pinos
- Conectores RF — MCX, impedância — 75 ohms
- Potência de entrada máxima RF — +15 dBm (63,75 dBmV)
- Tipo de switch — Eletro-mecânico, absorvente para caminho de trabalho, não absorvente no caminho de proteção
- Faixa de frequência DS — 54 a 860 MHz
- Perda máxima de inserção DS — 5,5 dB de trabalho para saída, 8,0 dB de proteção para saída
- Lentidão de perda de inserção DS — +1,1 dB desde o trabalho até a saída, +2,1 dB desde a proteção até a saída
- Perda de retorno de saída DS — maior que 15,5 dB
- Isolamento de DS — superior a 60 dB trabalhando para trabalhar, superior a 20 dB do trabalho para a respectiva proteção quando no modo de proteção e superior a 60 dB do funcionamento para proteção quando no modo de funcionamento
- Faixa de frequência upstream — 5 a 70 MHz
- Perda máxima de inserção upstream — 4,1 dB da entrada para o funcionamento, 5,2 dB da entrada para proteger
- Latência de perda por inserção dos EUA — + 0,4 dB da entrada para o funcionamento, + 0,6 dB da entrada para proteger
- Perda de retorno de entrada US — maior que 16 dB
- Isolamento dos EUA — maior que 60 dB trabalhando para trabalhar, maior que 20 dB do trabalho para proteção respectiva quando no modo de proteção e maior que 60 dB do trabalho para proteger quando no modo de funcionamento
- Fator de forma física — 19 x 15,5 x 5,25 (482 mm x 394 mm x 133 mm), Peso — 36 lbs

## Informações Relacionadas

- [Cisco RF Switches](#)
- [N+1 Dicas e configuração do uBR 10K com placas MC28C](#)
- [Suporte Técnico - Cisco Systems](#)