

Solução N+1 para o uBR7200 com os cartões MC28C ou de MC16x

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Switch de RF](#)

[Cabos](#)

[uBR7200 com os cartões MC28C ou de MC16x](#)

[Cronômetros](#)

[Rastreamento](#)

[Manutenção de atividade](#)

[Períodos de failover](#)

[Revertime](#)

[Comandos sincronizados](#)

[Comandos NON-sincronizados](#)

[Testando modems para potencialidade de falha](#)

[Comandos hccp](#)

[Comandos exec de HCCP](#)

[Comandos de interface HCCP](#)

[O HCCP debuga](#)

[Comandos show HCCP](#)

[Teste e Troubleshooting do Command Quick Lookup](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento fornece a informação na instalação, na fiação, e na configuração da solução N+1 de acordo com o projeto recomendado de Cisco. Além do que os esquemas de fiação, estes componentes devem ser configurados:

- Conversor ascendente do VCom HD4040 com um módulo do Simple Network Management Protocol (SNMP) (HD4008) ou o conversor ascendente NON-SNMP
- interruptor do Radio Frequency (RF) UBR-RFSW
- uBR7200VXR

O uBR7200 pode ser setup como um chassi com os quatro cartões que protegem outros quatro chassis. Isto ajuda com economia, porque fornece a Disponibilidade 4+1, e igualmente passa

requisitos necessários para o PacketCable. Tecnicamente, esta será quatro 4+1 encenações separadas em um nível de interface ao usar os cartões 1x6, ou oito encenações separadas ao usar os cartões 2x8.

Recomenda-se espalhar grupos através do uBRs, caso um uBR inteiro for para baixo. O objetivo é ter cada cartão em um uBR protegido se este acontece. O uBR7200 começado com Cisco IOS® 12.1EC para a Redundância 1+1 para o Data-over-Cable Service Interface Specifications (DOCSIS) 1.0 e 1.0+. O N+1 para o uBR7200 para o DOCSIS 1.0 e os 1.1 está em 12.2(11)BC e mais tarde.

Dica: O lado de expedição de cabogramas é considerado a vista frontal no uBR7200, mas a vista traseira no outro equipamento. O projeto da referência é montar em nível todas as unidades à parte dianteira exceto o Switch RF. O conversor ascendente tem somente os suportes de fixação na parte dianteira, mas o uBR7200 e o Switch RF podem ser montados em nível do dianteiro ou traseiro. Veja o [uBR7200 com MC28C](#) ou seção dos [cartões do MC16x](#) deste documento para mais informação.

Pré-requisitos

Requisitos

O leitor deste documento deve ter a compreensão básica do protocolo DOCSIS, termos e conceitos RF, e familiaridade com a linha e a Alta disponibilidade de comando cisco ios.

Componentes Utilizados

Este documento é restringido ao uso específico de Cisco IOS® 12.1EC ou 12.2(11)BC e mais tarde o uBR7246VXR.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Switch de RF

O projeto da referência é prendido com um domínio MAC em um lado do encabeçamento, e o outro domínio MAC de um cartão 2x8 no outro lado do mesmo encabeçamento. O código de cores é muito importante porque os kit de cabo são pré-fabricados para o projeto da referência de Cisco para os cartões, o Switch RF, e o HD4040 uBR7200 2x8. Os cartões 2x8 instalam horizontal no uBR7200, assim que os cabos são cortados a um comprimento específico para prender. Os códigos de cores em ordem são vermelhos, brancos, azuis, verdes, amarelos, roxos, alaranjados, pretos, cinzentos, e marrom.

Quando o 2x8 é prendido acima com este esquema de cores, US 0, 1, 2, e 3 para o primeiro

domínio MAC seja vermelho, branco, azul, e verde, e o DS associado com ele será cinzento. Os US 0, 1, 2, e 3 do segundo domínio MAC serão amarelos, roxos, alaranjados, e pretos, e o DS associado com ele será marrom. Seja certo prender o encabeçamento do Switch RF com os quatro US à esquerda, e quatro à direita. Põe o fio cinzento à esquerda no segundo furo da parte inferior para o Switch RF 3x10. Põe o fio marrom sobre o lado direito do encabeçamento ao lado do cinza.

A imagem abaixo mostra que o conversor ascendente e o Switch RF protegem dentro o modo.

Os dois módulos conversor ascendente direitos distantes foram desabilitados, e os módulos 9 e 10 foram permitidos. Todos os diodos emissores de luz do Switch RF são ambarinos/amarelo, exceto os módulos que não foram usados nos bitmaps, que são o 5o módulo para baixo à esquerda, e os 5os e 7os módulos à direita.

O Switch RF pode ser operado em dois modos separados, como um Switch RF 8+1 ou como dois 4+1 Switch RF. No caso do uBR7200, o modo de operação 4+1 é usado. No futuro, o Switch RF pode operar-se no modo 8+1 para mandar um proteger o chassi de trabalho da tampa oito do chassi.

Não há muito a programar no Switch RF próprio, exceto um endereço IP de Um ou Mais Servidores Cisco ICM NT e alguns nomes do grupo com os bitmaps correspondentes para indicar que portas pertencem aos grupos específicos. O modo do Switch RF do padrão é 8+1, e deverá ser mudado ao modo 4+1.

O tempo de failover é relativo ao tipo de falha, uma quantidade de Modems, e tipo de modem, contudo, realizou-se na ordem de 3-8 segundos. Os relés do Switch RF são milissegundos, mas provocar uma falha poderia ser 3-5 segundos. Toma mais tempo reiniciar transferência de dados em um modem devido às tabelas de MAC que precisam de ser refrescadas, ou à reconvergência do roteamento entre o uBRs. O código o mais atrasado deu a precedência ao Modems que faz a Voz sobre o tráfego IP (VoIP).

Cabos

Refira a tabela abaixo para as peças e os part numbers.

Peças	Part numbers
Cabeçalho Cisco Black para o interruptor N+1	Nº PEÇA MCXHEADERBK
Pino fixo MCX para terminação de campo	Nº PEÇA MCXFP
Conector de terminação de campo F	Nº PEÇA ASFP
Frisador para o MCXFP; .213 Encantar o friso	Nº PEÇA C47- 10120
Frisador para o conector ASFP F; .270 Encantar o friso	ACT-270 DO Nº PEÇA ~ \$35
Espadelador para o MCXFP; .230 x .125 tira da 2-fase	Nº PEÇA CPT- 7538-125
Espadelador para o ASFP; .250 x .250 tira de 2 fases	CPT-7538 DO Nº PEÇA ~ \$35
MCX Jack ao adaptador F Jack	Nº PEÇA 531-

	40137
Comute ao kit de cabo do cartão 2x8. MCX a FP 47.5"	Nº PEÇA 74-2765-02
Comute para plantar o jogo de expedição de cabogramas lateral MCXP a FP 10 m	Nº PEÇA 74-2961-01
Interruptor-à-planta; CAB-RFSW520TPMF, 3-meter	Nº PEÇA 74-2984-01 ou PN-78-147111-01

Você pode contactar CablePrep em 1-800-394-4046, ou visite seu site em <http://www.cableprep.com/>.

Cisco sugere obter os kit de cabo dos WhiteSands para todas as entradas, proteges, e saídas. O planejamento dos WhiteSands pode ser alcançado em <http://www.whitesandsengineering.com>. [Há um jogo de cabo de saída novo \(74-2984-01\) que contém dois conjuntos de cabo 3-meter de 10, de MCX a F, de um pacote 3-meter de 5, e de um saco de 25 conectores F extra. Os cabos podem ser pedidos dos WhiteSands com conectores F fêmeas igualmente.](#)

Dica: Teste o conector e a continuidade do cabeamento antes de pressionar o conector. Você pode precisar de testar através do Switch RF a menos que um adaptador (531-40137) for usado. Recorde testar portas DS do conversor ascendente output à saída do Switch RF, e portas E.U. do teste do CMTS à saída do Switch RF. Você não tem que instalar os cabos no encabeçamento para propósitos testando. Você pode querer usar uma varredura completa do espectro RF de 5-70 megahertz para portas E.U., e 50-870 megahertz para o DS movem.

Porque o conector F tem seu próprio pino, o condutor central do cabo de Belden deve ser cortado a um comprimento específico (condutor central de 1/4 de polegada e revestimento de 1/4 de polegada removido) para conectar corretamente dentro do conector F especial. A trança é dobrada então para trás e o dielétrico da ligado-folha é introduzido no mandrel do conector F. O condutor central é cobre contínuo, assim que não o dobra de medo da falha potencial. Comece sobre com a preparação do cabo se necessário.

Recomenda-se manter domínios MAC visivelmente separados, mas não necessários. Você pode prender os encabeçamentos com um domínio MAC em um lado do encabeçamento, e o outro domínio MAC de um cartão 2x8 no outro lado do mesmo encabeçamento. A fiação do domínio MAC deve ser a mesma em todas as entradas associadas, saídas, e protege que todos pertencem ao mesmo grupo. Para o fiação da placa 1x6, use o mesmo esquema acima, mas coloque as últimas duas portas E.U. no lado direito do encabeçamento. Isto facilitará promovendo a um cartão 2x8 no futuro.

Nota: Se fazendo o modo denso E.U. que combina no uBR, você pode fazê-lo na relação de cable modem termination system (CMTS), e salvar portas alguns E.U. no Switch RF. Cisco apoia somente uma configuração 3x10 e 2x12 DS-à-E.U., mas o Switch RF pode ser usuário configurável para encenações diferentes. É possível instalar um módulo extra DS no entalhe 14, e usa possivelmente os módulos DS nos entalhes 11 & 12 como os módulos US. Em caso afirmativo, você teria que instalar os módulos apropriados. Isto permitiria a 4+1 a Redundância usando as placas de linha 1x6 no uBR7200s com somente um Switch RF.

[uBR7200 com os cartões MC28C ou de MC16x](#)

A lista abaixo indica as situações que são seguidas para o início de failover. Esses são considerados os problemas mais comuns que poderiam deixar os modems off-line.

- Feche a interface de cabo ativa (trabalhos, mas não apoiado).
- Remoção de inserção on-line (OIR) da placa de linha ativa.
- Comandos baseados do software CLI (**interruptor g do hccp m**).
- Travamento de software da placa de linha ativa.
- Falha de expedição de cabogramas DS através dos recursos keepalive (manutenção de atividade).
- Restaurando a placa de linha (**hw-module slot x restaurado**).
- Falha de saída através do seguimento e recursos keepalive (manutenção de atividade).
- Interrupção de energia na placa em funcionamento (**sem energia do cabo x**).

No futuro, Cisco pode seguir as bases de informação de gerenciamento (MIBs) do conversor ascendente do VCom para indicar quando não há nenhuma frequência intermediária (SE) entrada ou uma falha no módulo. Neste tempo, Cisco segue uma falha DS através dos recursos keepalive (manutenção de atividade). Cisco oferece as placas de linha 2x8 e 1x6 com conversores ascendente internos, e o gerenciamento de espectro ajudar a facilitar a expedição de cabogramas e a confiança do conversor ascendente externo.

Uma falha DS podia ser de um conversor ascendente ruim ou de um cabo defeituoso entre o conversor ascendente e o uBR7200 ou o Switch RF. Os recursos keepalive (manutenção de atividade) seguem toda a comunicação em todas as portas E.U. de um domínio MAC particular. Quando não há nenhuma comunicação, um Failover iniciará, com base em alguns limiares configurável de usuário e temporizadores. Uma vez que a placa 2x8 é realmente dois domínios MAC 1x4, você pode comutar grupos com base em domínios MAC. Um domínio MAC é 1 DS e todos seus US associados.

Se você fecha o sinal DS, ainda gerará o seu SE output, mas o protocolo iniciará um failover através do arquivo de configuração. Um failover não é iniciado pelas relações E.U. que estão sendo fechadas. Puxar um cabo upstream de uma porta em uma placa de linha geralmente não é considerado um evento válido para causar um failover N+1 de placa de linha. É essencialmente impossível diferenciar isso de um atenuador desconectado em um nó de fibra ou amplificador (usado na manutenção operacional). Puxar o cartão fora do chassi, desligando o cabo a jusante entre a placa de linha e o conversor ascendente, desligando o módulo conversor ascendente, desligando a saída do conversor ascendente para o Switch RF, ou alguma falha no cartão própria é tudo do outro software ou do tipo de hardware eventos válidos considerados do Failover N+1.

Dica: Não se recomenda forçar um Failover através de fechar a relação. É o melhor emitir o **{member id} do interruptor do {group -} do hccp do** comando CLI do Failover. Você pode igualmente usar o comando down da potência da placa de linha, que corta a potência à placa de linha, e causa assim uma falha. O comando é o **entalhe do sem energia do cabo**, onde o **entalhe** é [3-6].

Um uBR será designado como um uBR da proteção, e todos os comandos serão configurados nesse backup do chassi todos os membros de funcionamento em seu grupo e nos conversores ascendentes que são relevantes a ele. Se uma placa de linha é removida, uns ou vários domínios MAC estarão removidos e uma placa de proteção será iniciada a suporta-a acima. A configuração no uBR da proteção fará o switchover apropriado dos relés do Switch RF e os conversores ascendentes associados para permitir e desabilitar igualmente.

Dica: Seja certo rever sempre sua configuração ao atualizar IO ao código o mais atrasado. Certifique-se de você configurar as interfaces de funcionamento antes das relações da proteção.

aviso: A frequência DS na configuração de uBR tem uma influência ao fazer a Redundância N+1. O conversor ascendente externo precisa de conhecer a frequência DS da configuração de uBR através do SNMP quando um failover ocorre. Se você o deixa vazio e a interruptor-sobre ocorre, o módulo conversor ascendente da proteção mudará sua frequência a uma frequência que possa estar incorreta. Era originalmente somente para o propósito informativo ou para a característica a jusante da ultrapassagem do cabo quando as frequências múltiplas DS estão na mesma planta.

A imagem abaixo mostra o uBR7200 prendido acima com o cabo de Belden com conectores F e cabos cor-codificados.

Esta disposição da amostra é o projeto da referência de Cisco com placas de linha MC28C, dois Switch RF, e três HD4040 UPx mostrados da vista frontal. Nenhuma diferença é exigida entre os dispositivos, mas o roteamento de cabo é mais fácil com uma unidade de rack (RU) do espaço de rack entre os dois Switch RF e entre o primeiros Switch RF e uBR.

Os conjuntos de cabo de oito são usados para DS pelo VXR com F--f aos conectores para a placa de linha SE às entradas UPx. Os conjuntos de cabo de oito são usados com o F-à-MCX para o UPx output ao Switch RF. Os conjuntos de cabo de dez são usados para US com os acréscimos usados para uma elevação MC28U no futuro. Proteção e todos os cabos DS são cortados para endireitar com trabalho dos US cortados à esquerda.

A imagem abaixo das mostras dois Switch RF que estão sendo usados com cartões do MC16x porque os Switch RF são configurados como os Switch RF 3x10. Esta disposição da amostra usa cinco uBR7200s, dois Switch RF, e dois conversores ascendentes do VCom HD4040. Isto permite uma migração fácil aos cartões MC28U no futuro.

Nota: Os códigos de cores do cabo não podem ser relevantes para seu projeto.

A imagem abaixo é uma ideia da explosão do código de cores para o conversor ascendente e o Switch RF ao usar os cartões 1x6 com dois Switch RF.

A imagem abaixo é o projeto da referência usando um Switch RF.

Dica: Se as portas alguns E.U. são combinadas para um modo denso que combina a encenação, poderiam ser combinadas no CMTS para livrar acima portas alguns E.U. no Switch RF. Isto significa aquele em vez de tomar um reverso e rachando para alimentar duas portas E.U. antes do Switch RF, faça-o após o Switch RF e antes do CMTS.

Nota: Recomenda-se usar uma porta Ethernet separada para o tráfego SNMP para o protocolo Hot Standby Connection-to-Connection (HCCP) a não ser a porta do regresso que é usada para o tráfego do Internet.

aviso: As relações empacotadas querem o failover enquanto o pacote e os comandos global precisam PRE-de ser configurados no uBR da proteção. Também, os comandos cable interface NON-sincronizados precisam PRE-de ser configurados. Estes comandos devem ser os mesmos em todos os membros de um grupo de HCCP. Veja os [comandos section NON-sincronizados](#) deste documento para mais informação.

Cronômetros

O holdtime do hellotime dos temporizadores do {group -} do hccp do comando cable interface é para uma comunicação dos inter-chassis. O hellotime é o valor de temporizador do mensagem

heartbeat periódica que o HCCP troca entre o chassi pela Redundância N+1. O chassi da proteção mantém-se enviar o mensagem Hello Messages no *intervalo de hellotime nos* milissegundos para verificar a sanidade do chassi de trabalho. Se não há nenhum helloAck para mais do que um período de tempo igual ao *holdtime*, a seguir declara-se que o funcionamento falhou e inicia um switchover. O tempo de espera deve ser, no mínimo, três vezes maior do que o tempo de saudação. O padrão é 2000 para hello e 6000 ms para hold. O máximo é a Senhora 25000.

Rastreamento

Por padrão, uma interface HCCP rastreia ela própria. Quando um keepalive é permitido e não detecta nenhum pacote de upstream recebido, failover. O comando de rastreamento também pode ser usado para rastrear uma interface de uplink. Por exemplo, se trabalhar tem um uplink dedicado (por exemplo, o gigabit Ethernet) o trajeto e protege tem seus próprios, estas interfaces de uplink pode ser seguido. Quando um falha, a interface de cabo failover ao apoio.

Para comutar um cabeçalho inteiro, que pode suportar uma placa de linha, dois domínios MAC devem comutar ao usar os cartões 2x8. Emita o **comando track** de modo que cada relação aponte entre si. Emita o **comando hccp {Group -} track c3/0 na relação C3/1**, e a **trilha c3/1 do {group -} do hccp na relação C3/0**. Uma outra maneira é usar o empacotamento da relação. As relações empacotadas Failover como um grupo, mas não no uBR10K.

Dica: Cada placa em funcionamento pode igualmente seguir a porta de saída do Internet, assim que se algo acontece ao adaptador de backhaul ou à conexão, o chassi completo Failover. Se usando a relação que empacota para todas as quatro placas de linha, somente o mestre precisa de seguir a porta de saída. Ajuste o keepalive ao segundo na porta de saída.

Manutenção de atividade

A finalidade desta característica é cobrir o RF ruim output do conversor ascendente ou da expedição de cabogramas entre o Switch RF e o CMTS. A maneira de detectar uma falha do Hybrid Fiber Coaxial (HFC) é contar pacotes recebidos em todos os upstreams.

Se dentro de três períodos de keepalive não há nenhum pacote recebido (pedidos da escala/resposta, manutenção de estação, dados, e assim por diante) em todos os upstreams, o protocolo de linha estará para baixo, e o HCCP supõe que algo é errado nesse canal e switchover. Recorde, se há um problema real com o HFC, o switchover ocorrerá, mas não fará nenhum bom desde que está ainda na mesma fábrica HFC ruim. Esta característica é significada cobrir falhas nos componentes que não são comuns entre a proteção e as interfaces de funcionamento tais como conversores ascendentes e determinada expedição de cabogramas.

Os recursos keepalive (manutenção de atividade) são desligados à revelia em interfaces de cabo com os IO mais velhos, mas optados um valor de dez segundos no código mais novo. Ajuste o keepalive o mais baixo possível, que seria segundo, mas somente depois que a relação estabilizou.

Pode ser vantajoso não emitir **nenhum keepalive nas** relações da proteção de modo que não falhe de volta à interface de funcionamento se todo o Modems vai off line.

Dica: Se a manutenção de rotina estará ocorrendo na planta de cabos (amplificadores de equilíbrio, e assim por diante) e a perda de sinal é eminente que afetará todas as portas E.U. de um domínio MAC, fechamento que a relação até o trabalho está feita. Se usado conjuntamente

com o Agrupamento de cabos de interface IP, então todas as relações associadas no pacote devem ser travadas para fora também.

Períodos de failover

O DOCSIS 1.0 especifica a Senhora 600 como a perda de sincronização DS, mas não especifica o que o modem a cabo deve fazer após a perda de sincronização. A maioria de Modems a cabo não registrar novamente imediatamente depois da perda de sincronização.

A manutenção de estação para o Modems é segundo por modem, até que você obtenha a 20 Modems, a seguir é cada 20 segundos quando há 20 ou mais Modems no domínio MAC. Antes de 15BC1, este era 25 segundos. Quando o HCCP é configurado, o número superior é 15 segundos para uma probabilidade maior de failover bem-sucedido. Isto é devido ao temporizador do T4 no Modems que é ajustado em 30 segundos. Se um modem era experimentar um Failover mesmo antes de sua manutenção de estação 20-second programada, teria somente dez segundos deixados de seu temporizador do T4. O Failover poderia tomar levemente mais por muito tempo do que este, e o modem iria off line. Fazendo à manutenção de estação cada 15 segundos, o cenário do pior caso dará 15 segundos para que um Failover ocorra antes de um intervalo do T4.

Revertime

O revertime é configurado em interfaces de funcionamento, e é para que a proteção reverta automaticamente para trás de modo que tenha a capacidade servir uma outra falha caso que o usuário esquece a comutar manualmente para trás. O padrão é 30 minutos. Emita o **comando no revertime** ajustar o padrão de 30 minutos. Para não reverter, emita o comando no `hccp {Group -} revertive` na relação da proteção.

Se você ajusta o revertime a um minuto na configuração da interface de funcionamento, ainda toma três minutos para que o trabalho retroceda para trás dentro. Há dois minutos de suspende o tempo antes do revertime. Esse tempo suspenso é usado para definir uma falha singular. Qualquer dupla de switchovers que ocorram dentro deste tempo de suspensão é considerada falha dupla. O HCCP é recomendado na falha dobro, e o serviço sem interrupções não é garantido. Se o revertime é demasiado curto, o usuário não pode poder fixar um problema da terceira, e a proteção pode comutar para trás se a placa se está operando corretamente. As falhas que ocorrem devido às falhas do keepalive não reverterem para trás automaticamente.

Nota: Uma vez o tempo da suspensão acaba-se, toda a falha na relação da proteção comutará para trás se a interface de funcionamento se está operando corretamente, nenhuma matéria se o revertime é sobre ou não. Se você OIR a placa de proteção, o tempo da suspensão é, contudo, introdução contorneada o cartão tomará dois minutos para recarregar. Uma outra maneira de falhar de protege de volta ao trabalho imediatamente seria emitir o **comando cable power off slot**, a seguir a potência do cabo no **entalhe na** relação da proteção.

Você pode emitir o **comando show hccp brief** ver quanto hora é deixada no contador. Emita este comando na proteção e no uBRs de trabalho.

```
uBR # sh hccp brief Interface Config Grp Mbr Status WaitToResync WaitToRestore C3/0 Working 1 1
active 00:01:45.792 C4/0 Working 2 1 active 00:00:45.788 00:01:45.788
```

Após um minuto, o static sync acontece e as sincronizações à espera até o active. Se você usa o encerramento/não-encerramento, OIR, ou emite o **comando hw-module reset** provocar um

Failover, você pode fazer assim right after o static sync está completo.

Se você desliga o DS de uma placa, a proteção retrocederá dentro corretamente depois que três Keepalives expiraram. Uma falha DS não será seguida se o keepalive está. Uma vez que o reverttime e os dois que o minuto suspende o tempo estão acima, ele irá para trás ao trabalho se não há nada erradamente com a placa. Você pode escolher não reverter ao trabalho emitindo o **comando no hccp {Group -} revertive** na relação da proteção. Se você ainda permite que a proteção reverta, você pode configurar um maior reverte o tempo na interface de funcionamento (até os minutos 65k), e emite manualmente o **comando hccp {Group -} switch {Member -}** quando você quer comutar para trás.

aviso: Observou-se que forçar um Failover através de uma porta de saída falhada ou pôr fora do chassi de trabalho uma vez a porta de saída de trabalho e/ou trabalhar o chassi são funcional outra vez, a proteção comuta de volta ao trabalho, mesmo que **não reversivo** foi configurado na proteção. Isto pode ser considerado uma causa rara para um Failover no primeiro lugar, e não pode causar nenhuma edições, mas deve ser compreendido e explicado.

Comandos sincronizados

Esta é uma lista de comandos interface que são sincronizados entre a relação da proteção e todas as interfaces de funcionamento que são parte de seu grupo HCCP.

```
[no] ip address <ip address> <subnet mask> [secondary] [no] ip helper-address <address> [no] ip vrf forwarding <vrf name> [no] mac-address <mac address> [no] interface <type><optional-whitespace><unit> [no] cable arp [no] cable proxy-arp [no] cable ip-multicast-echo [no] cable ip-broadcast-echo [no] cable source-verify ["dhcp"] [no] cable dhcp-giaddr [ policy | primary ] [no] cable resolve-sid [no] cable reset cable dci-response [ ignore | reject-permanent | reject-temporary | success ] [no] cable intercept {mac-addr} {dst-ip} {dst-port} [no] cable downstream frequency <f> [no] cable downstream channel-id <id> [no] cable downstream rf-power <dbmv> [no] cable downstream rf-shut [no] cable insertion-interval <interval> [no] cable insertion-interval automatic <min-interval> <max-interval> [no] cable helper-address <ip-address> ["cable-modem" | "host"] [no] bundle <n> [ master ] [no] upstream <n> shutdown [no] upstream <n> frequency <f> [no] upstream <n> power-level <dbmv> [no] upstream <n> concatenation [no] upstream <n> minislotsize <2-128> [no] upstream <n> fragmentation [no] upstream <n> modulation-profile <1st-choice> [<2nd-choice>] [no] upstream <n> channel-width <hz> <hz-opt2> [no] ip access-group [<n>| <WORD>] ["in" | "out"] [no] cable spectrum-group <grp num> [no] cable upstream <n> spectrum-group <grp num> [no] cable upstream <n> hopping blind [no] cab up<#> threshold cnr-profile1 <5-35> cnr-profile2 <5-35> Corr-Fec <0-30> Uncorr-Fec <0-30> [no] cable upstream <#> hop-priority [frequency | modulation] [frequency | modulation | channel-width] [no] ip pim sparse-dense-mode
```

Comandos NON-sincronizados

Além do que **todos os comandos global**, estes comandos devem PRE-ser configurados na relação da proteção:

```
cable map-advance dynamic/static cable downstream modulation [256qam | 64qam] cable downstream interleave-depth [128|64|32|16|8] [no] keepalive <0-32767> power-adjust threshold, power-adjust continue, & power-adjust noise tftp enforce (mark only) shared secret arp timeout cable source-verify lease timer ip policy route-map load balance configs no shut
```

Todas as configurações serão sincronizadas no código 15BC2 e acima, mas a modulação DS, o modo do anexo, e a intercalação ainda precisam de ser a mesma em todos os membros de um grupo HCCP.

O código IOS mais novo (depois que código EC1 & 4BC de 12.10) permite que o usuário ponha em um número do duro-grupo para dinâmico e o avanço do mapa de estática. Refira o [avanço de](#)

[mapa de cabo \(dinâmico ou estático?\)](#) para uma explicação detalhada deste comando. Com isto em mente, cada relação podia ter um ajuste diferente do avanço map. Se o funcionamento falha sobre a uma proteção com um ajuste diferente, o Modems pode ter a dificuldade que sincroniza mapas. Os deslocamentos de tempo da manutenção inicial de cada modem acabar-se-ão sincronizados no código IOS 12.2(8)BC2 e mais tarde. Recomenda-se usar as configurações padrão na proteção. Emita o **Cable Map-Advance Dynamic 1000 1800** para as configurações padrão.

aviso: Ao adicionar e ao remover configurações das placas em funcionamento vivas, a arquitetura N+1 não pode proteger a configuração nova até que estiver estaticamente sincronizado à placa de proteção. Se a interruptor-sobre ocorre antes do static sync, o aplicativo, que foi invocado pela configuração nova, poderia ter o comportamento imprevisível.

Para impedir isto, o fechamento a placa em funcionamento emitindo o **comando hccp {Group -} lockout {Member -}**, e configurar os comandos new. Quando terminado, destrave a placa emitindo o **comando hccp {Group -} unlockout {Member -}**. Isto força um sincronismo estático imediato. As resincronizações ocorrerão automaticamente após ter deixado o modo de configuração da interface de cabo com a versão do IOS 12.2(11)BC1 e mais tarde.

Dica: As resincronizações ocorrerão automaticamente após ter deixado o modo de configuração da interface de cabo com 12.2(11) a versão do IOS BC1 e mais tarde. Após toda a alteração de configuração em uma placa em funcionamento, o **comando hccp {group} resync {member}** deve ser emitido nessa placa, ou em saída do modo de configuração assim que é feito automaticamente.

Éigualmente possível fechar a relação da proteção até que a configuração esteja terminada, a seguir emite o **comando no shut**, contudo, você deve esperar um minuto antes que um resync ocorrerá. O problema com fechamento da relação da proteção não é lá será nenhuma proteção para todas as relações que restantes pode proteger quando for fechada. O problema com fechamento é que você pode precisar iniciá-lo para todas as interfaces.

Testando modems para potencialidade de falha

Siga estas etapas para testar a duração da perda de sincronização de downstream, para que um modem permanece em linha.

1. Emita o **comando test cable synch delay msec**. Isto especifica a duração da perda de sincronização nos milissegundos.
2. Do modo exec uBR7200, emita o **comando test cable atp mac 16**.

O **comando test cable atp mac 16** sibila o modem primeiramente, a seguir para a mensagem de sincronização para a duração especificada, e reinicia a emissão da sincronização na duração da Senhora 10. Ele realiza um ping no modem novamente para verificar a conectividade. Se este ping for bem sucedido, o teste é considerado um sucesso.

Observe que se o ping falhar, o teste ATP continuará ativo até o modem se recuperar. **A passagem** final do teste da saída ATP não é uma indicação do que você precisa de verificar. O teste falha se a sessão do sibilo após o reinício da sincronização falha.

Siga os passos a seguir para testar a duração da perda da portadora downstream, para a qual um modem permanece on-line.

1. Emita o **comando show cable modem** verificar se o modem dado é em linha.

2. Quando consolado dentro, estabeleça uma sessão do sibilo do uBR7200 ao modem a cabo.
3. De uma sessão de Telnet com o uBR7200, emita o comando **test hccp {group} {member} modem-test ds-signal name string of the upx mac-address of the modem duration in msec of carrier loss time.**

Verifique se a sessão de ping continua após a conclusão do teste (sucesso). Se a sessão do sibilo termina, o teste falhou. Este teste instrui o UPx fechar para uma quantidade de tempo especificada.

Dica: Datilografe **Control+Alt** ou **Shift+6** para parar caso necessário o sibilo. Uma outra maneira fácil testar o modem a cabo é puxar o cabo para o modem por ~6 segundos para considerar se pode segurar a perda DS que por muito tempo.

Comandos hccp

Comandos exec de HCCP

```
hccp 1 ? -bypass Enter bypass operation -check Exit bypass operation -lockout Lockout switchover
on teaching worker -resync Re-sync member's database -switch Switchover -unlockout Release
lockout on teaching worker
```

Comandos de interface HCCP

```
(config-if)#hccp 1 ? -authentication Authentication -channel-switch Specify channel switch
-protect Specify Protect interface -revertive Specify revert operation on Protect interface
-reverttime Wait before revert switching takes place -timers Specify "hello" & "hold" timers on
Protect interface -track Enable failover based on interface state -working Specify Working
interface
```

O HCCP debuga

```
debug hccp ? authentication Authentication channel-switch Channel switch events Events inter-db
inter database plane inter-plane communication sync SYNC/LOG message timing Timing Measurement
```

Comandos show HCCP

```
sh hccp ? | Output modifiers <1-255> Group number brief Brief output channel-switch Channel
switch summary detail Detail output interface Per interface summary
show hccp channel-switch Grp 1 Mbr 1 Working channel-switch: "uc" - enabled, frequency 453000000
Hz "rfswitch" - module 2, normal module 6, normal module 10, normal module 14, normal module 18,
normal module 22, normal module 26, normal Grp 1 Mbr 2 Working channel-switch: "uc" - enabled,
frequency 453000000 Hz "rfswitch" - module 4, normal module 8, normal module 12, normal module
16, normal module 20, normal module 24, normal module 28, normal uBR7246P#sh hccp channel-switch
Grp 1 Mbr 1 Protect channel-switch: "uc" - disabled, frequency 453000000 Hz "rfswitch" - module
2, normal module 6, normal module 10, normal module 14, normal module 18, normal module 22,
normal module 26, normal Grp 1 Mbr 2 Protect channel-switch: "uc" - disabled, frequency
453000000 Hz "rfswitch" - module 4, normal module 8, normal module 12, normal module 16, normal
module 20, normal module 24, normal module 28, normal
show hccp brief Interface Config Grp Mbr Status WaitToResync WaitToRestore Ca3/0 Working 1 1
active 00:01:45.792 Ca4/0 Working 2 1 active Each module should have a set of objectives.
show hccp detail HCCP software version 3.0 Cable3/0 - Group 1 Working, enabled, forwarding
authentication none hello time 2000 msec, hold time 6000 msec, revert time 120 min track
interfaces: Cable3/0 sync time 1000 msec, suspend time 120000 msec switch time 240000 msec
retries 5 local state is Teach, tran 80 in sync, out staticsync, start static sync in never last
switch reason is internal data plane directly sends sync packets statistics: standby_to_active
```

```

5, active_to_standby 4 active_to_active 0, standby_to_standby 0 Member 1 active target ip
address: protect 192.168.1.7, working 192.168.1.5 channel-switch "uc" (wavecom-hd,
192.168.1.2/1, 192.168.1.2/16) enabled channel-switch "rfswitch" (rfswitch-group,
192.168.1.4/0xAA880800/1) enabled tran #: SYNC 72, last SYNC_ACK 4, last HELLO_ACK 5790 hold
timer expires in 00:00:11.532 interface config: mac-address 0005.00e1.9908 cmts config: bundle 1
master, resolve sid, dci-response success, downstream - frequency 453000000, channel id 0
downstream - insertion_invl auto min = 25, max = 500 upstream 0 - frequency 24000000, power
level 0 upstream 0 - modulation-profile 2, channel-width 3200000 !--- Minislot does not show up,
but it is synchronized. upstream 0 - cnr-profile1 25, cnr-profile2 15 corr-fec 1, uncorr-fec 1
upstream 0 - hop-priority frequency modulation channel-width sub-interface master config: ip
address 192.168.2.5 255.255.255.0 ip address 24.51.24.1 255.255.255.0 secondary ip pim sparse-
dense-mode cable helper-address 192.168.2.165 cable arp, proxy-arp, cable ip-multicast-echo,
cable dhcp-giaddr policy,
uBR7246P#sh hccp 1 1 ? H.H.H MAC address channel-switch Channel switch summary host Host
information modem Cable Modem information qosparam Qos Parameter information service-flow
Service Flow information sid SID information
uBR7246P#sh hccp 1 1 modem !--- This is used to see the modem inter-database on the protect uBR.
Cable3/0: MAC Address IP Address MAC Prim Timing Num BPI Prio State Sid Offset CPEs Enbld
0090.837c.0acb 192.168.3.1 online 6 1243 0 no 4 0090.837c.0ac9 192.168.3.2 online 7 1243 0 no 2
0000.39d7.004a 192.168.3.3 online 9 1667 0 no 0 0090.8336.030d 192.168.3.6 online 11 1242 0 no 1

```

Teste e Troubleshooting do Command Quick Lookup

Use os comandos abaixo para o uBR7200.

```

test hccp {Group #}{Worker's member id} channel-switch {name} snmp/front-panel test hccp {Group
#}{Worker's member id}{working/protect }fault 1 (simulates an Iron bus fault) test hccp {Group
#}{Worker's member id}{working/protect } failover test hccp {Group #}{Worker's member id} modem-
test ds-signal{name}{mac-addr}{msec} test cable synch delay {msec delay} test cable atp {CMTS
interface}{mac-addr} mac {test_id} show hccp; show hccp (brief ; detail; channel-switch) show ip
interface brief; show hccp{Group #}{Worker's member id} modem hccp {Group #} switch; lockout;
resync {Worker's member id} hw-module {slot}/{subslot} reset debug hccp authentication; channel-
switch; events; plane; sync; timing

```

Use os comandos abaixo para o Switch RF.

```

test module config card count{1-14} !--- Removed in 3.3 RF Switch firmware. sh conf or sh cf sh
mod all sh dhcp sh ip sh switch status {mod #} or sh sw st {mod #} switch {mod #}{slot #} switch
{group name}{slot #} switch {group name} 0

```

Informações Relacionadas

- [Solução N+1 para o uBR10012](#)
- [Redundância N+1 usando o Cisco RF Switch](#)
- [Suporte Técnico - Cisco Systems](#)