N+1-Redundanz mit dem Cisco RF-Switch

Inhalt

Einführung

Dieses Dokument enthält Informationen zur N+1-Redundanz mit dem Cisco® RF-Switch.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Hintergrundinformationen

Um den größtmöglichen Nutzen für ihr Geld zu erzielen, haben sich viele Kabelanbieter entschieden, Redundanz für ihr Glasfasernetzwerk in Form zusätzlicher Notstromversorgung im

Glasfaserknoten, unterbrechungsfreier Stromversorgungen (USV) mit Erdgas- und Batteriesicherung und zusätzlichen Glasfaser-Sendern im Knoten bereitzustellen. Bei einem Glasfaserausfall könnten jedem Knoten auch zusätzliche dunkle Fasern zugewiesen werden.

Wie bereits erläutert, ist Hardware das erste, das in der Außenanlage abgedeckt ist. Wie sieht es mit den tatsächlichen Upstream- (US) und Downstream-Signalen (DS) aus, die auf dem Transportmedium gesendet werden? Im Hinblick auf die USA hat Cisco Advanced Spectrum Management-Techniken implementiert, um die Modems online zu halten und optimal zu übertragen. Einige dieser Techniken sind Frequenzsprungverfahren mit erweiterten "Look before you Lep"-Funktionen über die integrierte Spectrum Analyzer-Tochterkarte auf der S-Card. Darüber hinaus wurden Modulationsprofiländerungen und Änderungen der Kanalbreite integriert. All diese Funktionen ermöglichen es dem Modem, in einem sauberen Teil des Spektrums zu bleiben, ein robusteres Modulationsprofil zu verwenden und/oder die Kanalbreite zu ändern, um den Service hinsichtlich Durchsatz und Verfügbarkeit zu optimieren. Bei DS-Frequenzen können Sie zwischen 64 und 256 QAM wählen. Obwohl diese Modulationsschemata bei QPSK oder 16-QAM viel weniger robust sind als die USA, ist das DS-Spektrum viel vorhersehbarer und kontrollierbarer als das US-Spektrum.

Die Hardwareverfügbarkeit im Headend ist die nächste logische Sache, auf die Sie sich konzentrieren sollten. Fällt eine einzelne Stromquelle aus, kann die Generatorsicherung mit redundanten Netzteilen verwendet werden, falls eine Stromquelle ausfällt.

Ein weiterer Hardwarepunkt für den Ausfall könnte die Stromversorgung des Cable Modem Termination System (CMTS) sein. Die uBR10K-Netzteile verwenden einen Algorithmus für die Sicherung und Lastverteilung. Dies wird manchmal auch als N:1 bezeichnet, d. h. 1 für N-Backup mit Lastenausgleich. In diesem Fall wird es 1:1 sein, und Sie werden feststellen, dass die DC-Gesamtleistung etwas größer ist, mit zwei Power Entry-Modulen (PEMs), als wenn eines für die gesamte Last verwendet wurde. Geben Sie den Befehl **sh cont clock-reference** ein, um diese Informationen anzuzeigen.

```
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
```

Um sich auf die Verfügbarkeit von CMTS-Linecards zu konzentrieren, hat Cisco ein Protokoll entwickelt, in dem festgelegt wird, wie CMTS in einem Hochverfügbarkeitsszenario miteinander kommunizieren. Dieses Protokoll wird als Hot Standby Connection-to-Connection Protocol (HCCP) bezeichnet. Dieses Protokoll bietet einen Heartbeat zwischen dem Sicherungsgerät und den Arbeitsgeräten, um die Schnittstellen/Geräte mit MAC-Tabellen, -Konfigurationen usw. synchronisieren zu lassen. Cisco hat außerdem einen RF-Switch entwickelt, um eine hohe Verfügbarkeit auf MAC-Domänenebene anstelle von Chassis für Chassis bereitzustellen. Eine MAC-Domäne kann auch als RF-Subnetz betrachtet werden, das ein DS und alle zugehörigen USA ist.

Cisco bietet bereits seit einigen Jahren 1+1-Redundanz für Chassis der Serie uBR7200. Ein gesamtes Chassis muss jedoch als Schutzgehäuse im Leerlauf sitzen. Der Vorteil von 1+1 besteht darin, dass kein RF-Switch erforderlich, aber weniger skalierbar ist. Die Verwendung eines RF-Switches ermöglicht Redundanz auf Schnittstellenebene für N+1-Verfügbarkeit. Dies bedeutet 1 für N-Backup ohne Lastenausgleich/Lastverteilung. Anstelle eines kompletten Chassis im Leerlauf kann eine Inaktiv/Schützenkarte oder eine Schnittstelle vorhanden sein, die viele andere

Schnittstellen schützt. Der uBR100012 kann als eine Karte eingerichtet werden, die sieben weitere schützt. Dies hilft bei der Wirtschaftlichkeit, da es jetzt 7+1-Verfügbarkeit bietet und auch die erforderlichen Anforderungen für PacketCable erfüllt.

Wenn diese Punkte abgedeckt sind, möchten Sie sicher sein, dass Sie je nach Betrachtung über Redundanz für Backhaul verfügen, die auch als WAN- oder LAN-Seite bezeichnet wird. Hot Standby Router Protocol (HSRP) ist bereits seit Jahren im Einsatz und ermöglicht redundante Pfade zwischen Routern, um eine für diesen Single-Point-of-Failure erforderliche Verfügbarkeit bereitzustellen. Die eigentliche Herausforderung für diese Funktionen sind VoIP und ein erhöhter Wettbewerbsdruck, um dem Kunden den stabilsten/verfügbaren Service bereitzustellen.

Operative Sequenz von Ereignissen

uBR10K-Lösung

HCCP findet zuerst zwischen den Chassis über den Heartbeat statt. Da die uBR10K-Lösung alle in einem Chassis enthalten ist, ist der Heartbeat möglicherweise nicht relevant. Wenn interne Kommunikation und Schnittstellenänderungen erfolgreich sind, sendet HCCP weiterhin einen Befehl an den RF-Switch, um die entsprechenden Relays auszuschalten.

uBR7200-Lösung

HCCP findet zuerst zwischen den Chassis über den Heartbeat statt. Ein Befehl wird dann vom protect 7200 an den upkonverter (UPx) gesendet, um die Frequenz zu ändern. Der UPx sendet ein ACK. Der Protect 7200 sendet einen Befehl, um das funktionierende UPx-Modul zu deaktivieren, und wartet auf ein ACK. Der Protect 7200 sendet dann einen Befehl zum Aktivieren des Protect UPx-Moduls und wartet auf eine ACK. Wenn all dies funktioniert oder kein ACK vom funktionierenden UPx-Modul gesendet wird, wird es fortgesetzt und ein Befehl an den Switch gesendet, um die entsprechenden Relays auszuschalten.

Es gibt zwei Arten von Heartbeat-Mechanismen, die für HCCP relevant sind. Sie sind unten aufgeführt.

1. helloACK zwischen Arbeit und Schutz - Der LC zum Schützen sendet eine Hello-Nachricht an alle funktionierenden LCs in seiner Gruppe und erwartet als Antwort ein helloACK. Die Sendefrequenz von hello und helloACK kann auf dem LC mit CLI für den Schutz konfiguriert werden. Darüber hinaus beträgt die minimale Hello-Zeit für den 7200 0,6 Sekunden, während der Mindestwert für den uBR10K 1,6 Sekunden beträgt.
2. Synchronisierungsimpuls - Dies ist ein Heartbeat-Mechanismus auf Datenebene mit HCCP, und seine Häufigkeit ist nicht konfigurierbar. Die Synchronimpulse werden von jedem funktionierenden LC an seinen Peer-Protect LC gesendet. Dieser Synchronimpuls wird einmal pro Sekunde gesendet. Wenn drei Synchronimpulse verpasst werden, wird der Peer für inaktiv erklärt. Cisco arbeitet an einem schnellen Fehlererkennungsmechanismus, um einen funktionierenden Absturz im Ausnahmehandler in weniger als 500 ms zu erkennen. Die Zielversion ist 12.2(15)BC. Auf dem VXR kann ein Ausfall von beiden Mechanismen erkannt werden. Da der uBR10K jedoch nur ein interner HCCP ist, ist nur der zweite relevant.

RF-Switch

Cisco entschied sich für einen externen RF-Switch anstelle einer Linecard oder internen Verkabelung, die aufgrund der zukünftigen Skalierbarkeit und Komplexität als RF-Switch fungieren würde. Der externe Switch kann im Stack verwendet werden und kann für verschiedene Szenarien, unterschiedliche Dichten und Legacy-Geräte verwendet werden.

An der Rückseite des Switches befinden sich 252 Anschlüsse in einem 3-HE-Gehäuse. 1 HE: Der VCom HD4040-Upper-Konverter ist eine 2 HE große Einheit.

Wenn die Rückwandplatine für einen internen Switch auf eine bestimmte Weise konfiguriert ist, können Sie später in der unteren Straßenseite die Flexibilität einschränken, verschiedene Linecard-Dichten zu erstellen. Wenn eine Linecard zu dicht ist, sind zu viele US-Ports von Ausfällen betroffen, die sich auf eine einzelne US-Karte oder DS und Karte im Allgemeinen beziehen. Aus diesem Grund sind Switch und Redundanz von Anfang an erforderlich. Eine höhere Dichte ist gleichbedeutend mit mehr Kunden, die von einer einzelnen Veranstaltung betroffen sind. Was passiert, wenn reine DS-Karten und reine US-Karten verkauft werden? In Zukunft können Sie die US- und DS-Ports auf allen Linecards abgleichen. Das externe Design schützt meine Investitionen in Zukunft weiter.

Eine Redundanz zwischen Chassis und einem internen Switch ist niemals möglich. Wenn Sie Kosten sparen und vier 7200 uBRs durch einen einzigen sichern möchten, ist ein externer RF-Switch erforderlich. Es sei denn, Sie denken darüber nach, Linecards in einem Chassis zu haben, das von einem anderen im selben Chassis gesichert wird. Das einzige Problem ist, wenn das gesamte Chassis ausfällt und Sie kein Backup haben.

Die Verfügbarkeitswerte sind für einen externen Switch möglicherweise besser (zumindest für die Elektronik, nicht für die Verkabelung), da weniger aktive Komponenten vorhanden sind. Da der Switch im Chassis ein vollständig passives Design aufweist, ist der normale Betriebsmodus auch dann aktiv, wenn die aktiven Module entfernt werden. Die Relays befinden sich nur auf dem Schutzpfad mit einem vollständig passiven Arbeitspfad und können zum Testen des Switches umgeschaltet werden, ohne den eigentlichen Arbeitsmodus zu beeinflussen. Dies bedeutet, dass der normale Betriebsmodus nicht durch einen Stromausfall am Switch, ein ausgebautes Switch-Modul oder einen Switch-Ausfall beeinträchtigt wird. Ein negatives Ergebnis ist der Einfügungsverlust von potenziell 6 bis 8 dB bei der höchsten DS-Frequenz von 860 MHz.

Das externe Design ermöglicht auch die Migration von Kabeln und den Austausch von Linecards. Wenn jemand von einer 2x8-Karte auf eine 5x20-Karte aktualisieren möchte, kann die Linecard gezwungen werden, ein Failover in den Schutzmodus durchzuführen. Die Linecard kann in einem Tempo ausgetauscht werden, das Sie mit der neueren, dichteren 5x20-Karte bestimmen und für zukünftige Domänen verkabelt werden. Die beiden Domänen, die sich im Schutzmodus befanden, werden dann auf der 5x20-Karte wieder zur entsprechenden Schnittstelle/Domäne/zu den Domänen zurückgeschaltet. Andere Probleme müssen behoben werden, z. B. die 5x20-Karte verfügt über interne Uplinks und Anschlussbefehle.

Die Vorderseite verfügt über LEDs, Netzkabel für Wechselstrom oder Gleichstrom, Ethernet-Konnektivität, RS-232-Konnektivität und einen Netzschalter für Wechselstrom, Gleichstrom oder Aus. Im Lieferumfang jedes Switches ist ebenfalls ein Kabelextraktionstool enthalten. Achten Sie darauf, den Gummiboot vor dem Gebrauch zu entfernen. Die Extraktionskraft kann mit einem Schraubenzieher eingestellt werden, indem man im Uhrzeigersinn auf der Rückseite des Werkzeuges schraubt.

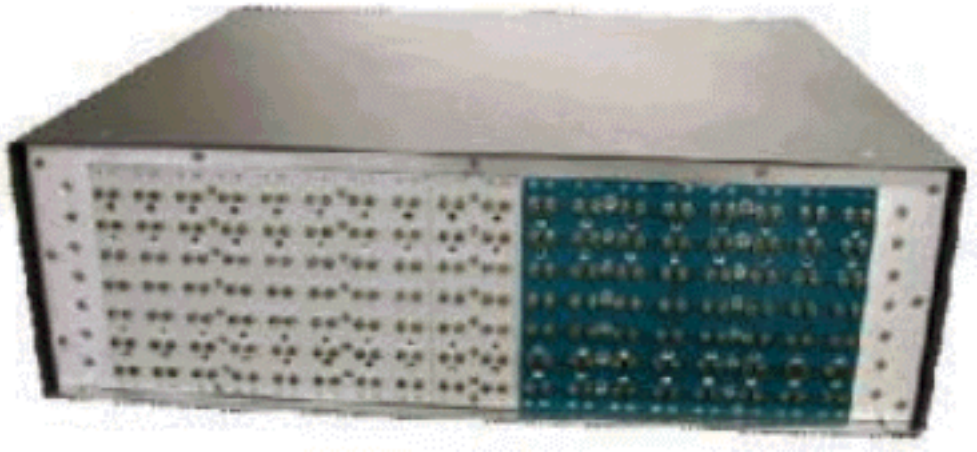
Die Abbildung unten zeigt die Vorderansicht des RF-Switches.

Der 3x10 RF-Switch verfügt über zehn US-Module (blau dargestellt) und drei DS-Module (grau dargestellt). Die untere linke Seite wird als Modul N bezeichnet und ist leer. Die Module auf der Vorderseite, beginnend in der oberen rechten Ecke, sind die Nummern 1-13 und korrelieren mit den Ports A-M. Upstream Module 1 enthält alle Relays für Port A in den Steckplätzen 1 bis 8 und schützen 1 und 2 auf der Rückseite. Modul 2 befindet sich auf der linken Seite und verfügt über alle Relays für Port H in den Steckplätzen 1 bis 8 und schützt 1 und 2.

Die Module können Hot-Swap-fähig sein, aber die Extraktion der Karte ist sehr schwierig. Sie ist extrem eng und die beiden unverlierbaren Schrauben müssen gelöst werden, bevor sie herausgenommen werden. Beim Herausziehen müssen Sie sich möglicherweise mit einem Schraubenzieher aufmachen oder nach links und rechts bewegen.

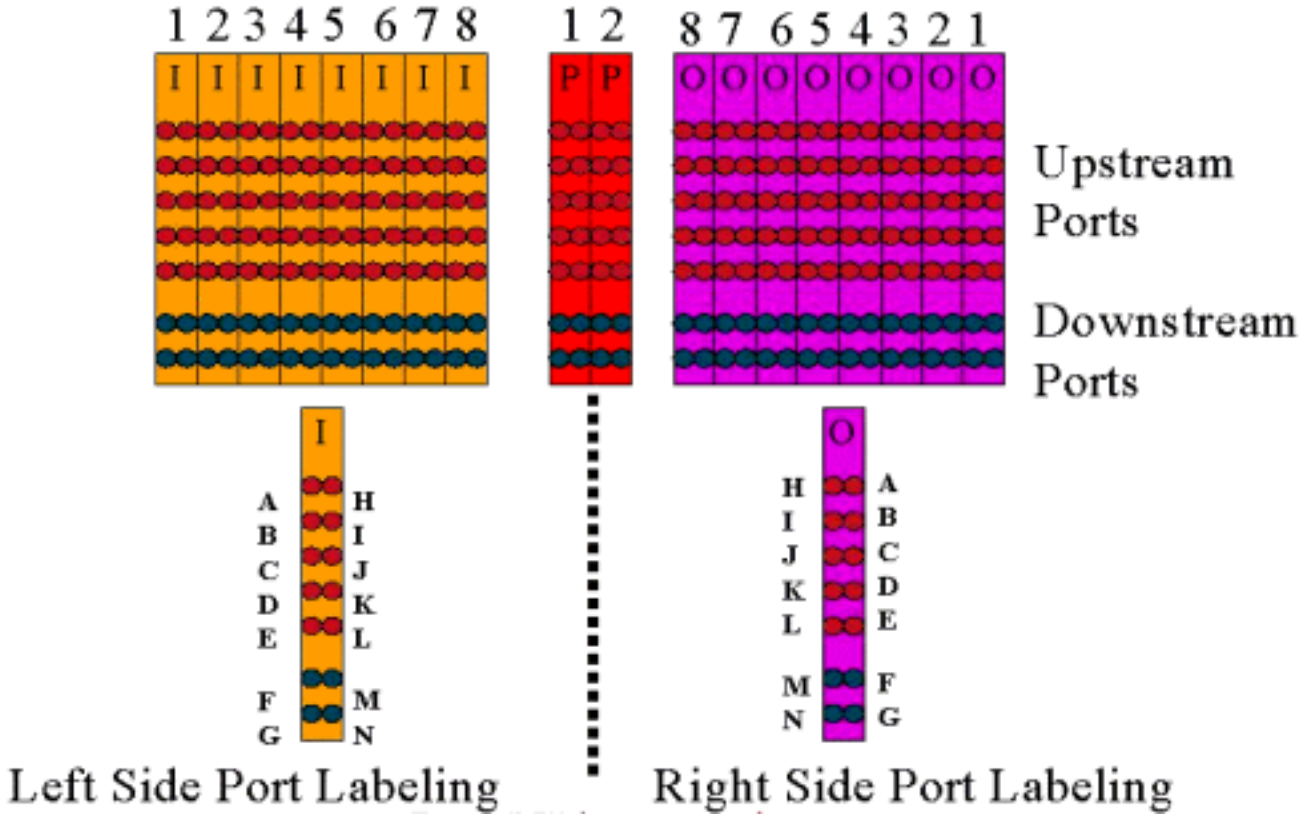
Auf der Rückseite sind Etiketten mit **CMTS**, **Protect** und **KabelPlant** vorhanden. Die **CMTS-**Seite dient zur Erfassung der funktionierenden Eingänge. Die Kabelseite enthält alle Ausgänge zur Versorgung der Kabelanlage.

Die nachfolgende Abbildung zeigt die Rückseite des RF-Switches.



Die acht funktionierenden Eingaben sind von links nach rechts nummeriert. Die beiden Schutzvorrichtungen befinden sich in der Mitte, und die acht Ausgänge befinden sich auf der rechten Seite.

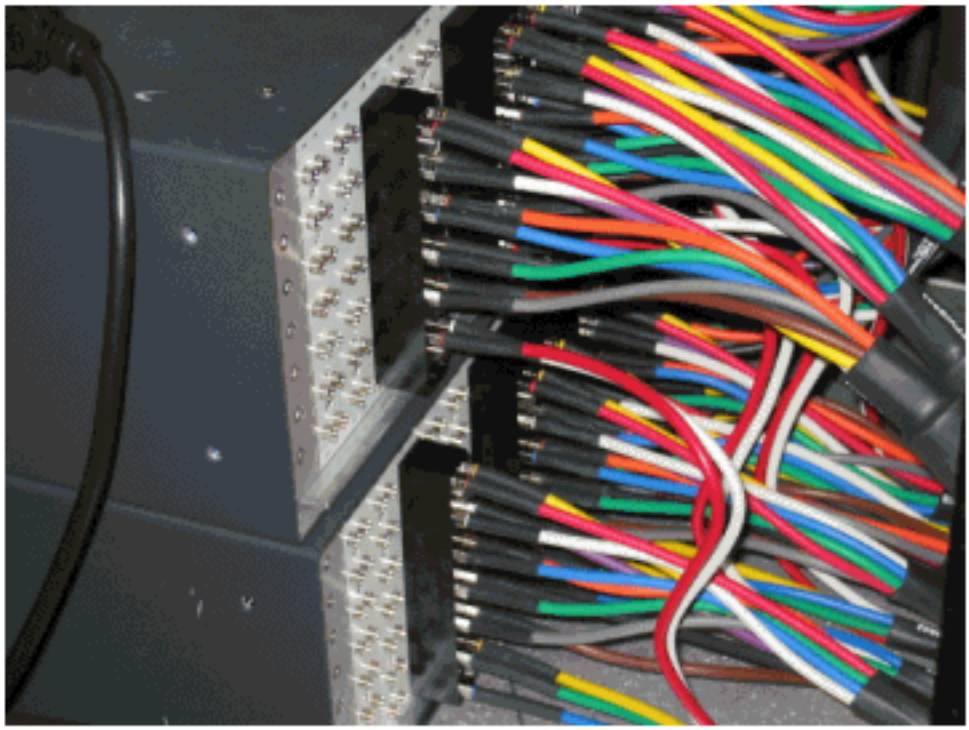
Die nachfolgende Abbildung zeigt das Nummerierungsschema für RF-Switch.



Hinweis: Port N wird nicht verwendet.

Die Ausgabe (farbig violett) stellt die Kabelanlage dar. Ausgabe 1 befindet sich ganz rechts, Eingabe 1 ganz links. Die Ports sind ebenfalls gespiegelt. Beachten Sie, dass Port N nicht verwendet wird. Vergewissern Sie sich, dass die Konsistenz bei der Verkabelung gegeben ist.

Dieses Bild unten zeigt die Rückseite des RF-Switches mit dem 14-Port-Header und dem speziellen Belden-Mini-Koaxialkabel mit MCX-Anschlüssen.



Die MCX-Anschlüsse können direkt an den Switch angeschlossen werden, es besteht jedoch das Risiko von losen Verbindungen, Emissionen und möglichen Unterbrechungen. Cisco hat einen

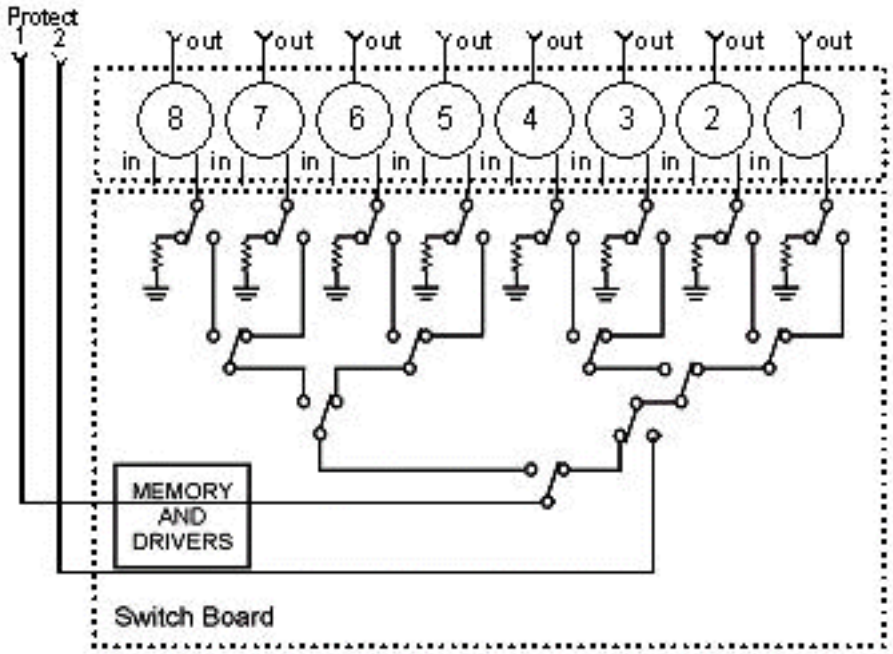
Header zur Behebung dieser Probleme entwickelt.

Die MCX-Steckverbinder lassen sich in den Header einstecken, und es ist ein spezielles Tool enthalten, das bei jedem Kauf eines Switches zur Extraktion geliefert wird. Der Header hat zwei Führungsstifte und geht nur in eine Richtung. An der oberen Kante befindet sich ein leichtes Kies, das den oberen Teil des Headers angibt. Es gibt zwei Schlitzschrauben, mit denen die Kopfzeile am Switch befestigt werden kann. Im Lieferumfang jedes RF-Switches ist außerdem eine Kabelmanagementhalterung enthalten.

Tipp: Sie können auch den Header auf dem Switch installieren und dann die MCX-Anschlüsse in den Header einfügen. Dies kann die Installation vereinfachen. Ziehen Sie den Header erst fest, wenn alle Anschlüsse installiert sind.

Konfiguration und Betrieb von RF-Switches

Die Abbildung unten zeigt ein Blockdiagramm des RF-Switches.



Die Combiner-Komponenten befinden sich im Switch-Chassis, die Relays befinden sich jedoch in jedem einzelnen, abnehmbaren Modul. Jedes Relay endet mit einer Last von 75 Ohm, nur im Protect-Pfad, nicht im Ein-/Arbeitspfad.

Stellen Sie eine serielle Kommunikation mit dem Switch her, indem Sie HyperTerminal oder TeraTerm, ein Konsolen-/Rollover-Kabel, einen Cisco 9-poligen RJ-45-Adapter und eine Baudrate von 9600 verwenden.

Legen Sie eine IP-Adresse und eine Maske fest, indem Sie den Befehl **set ip addr** ***ip add subnet mask eingeben***. Anschließend können Sie Telnet hinzufügen und ein Telnet-Passwort festlegen. Als Nächstes legen Sie das Schutzschema fest, ob es 4+1 oder 8+1 ist, indem Sie den Befehl **set port 4/8** eingeben. Der Standardwert ist "8+1", wobei "Protect 1" alle acht Eingangssteckplätze abdeckt. Im 4+1-Modus ist der Schutz 1 für Steckplätze 5-8 und der Schutz 2 für Steckplätze 1-4 vorgesehen.

Der SNMP Community String ist **privat** und kann geändert werden, wird aber im uBR10K nicht unterstützt.

Festlegen von Bitmaps

Als Nächstes müssen die Switch-Gruppen festgelegt werden, die hexadezimale Bitmaps erfordern. Die Bitmap des RF-Switches hat eine Länge von insgesamt 32 Bit (8 Hexadezimalzeichen) und wird wie unten dargestellt berechnet. Es steht ein Excel-Rechner zur Verfügung.

Nehmen wir die Gruppe 1, bei der links neben einem RF-Switch-Header in Steckplatz 1 vier US-Kabel und links ein DS mit demselben Header verkabelt sind. Die verwendeten Ports sind ABCDF. Für jeden Port, der am Switching beteiligt ist, wird das entsprechende Bit auf 1 festgelegt. Wenn ein Port nicht an Switching beteiligt ist, wird dieses Port-Bit auf 0 gesetzt.

Gruppe 1 ist unten dargestellt.

```
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
(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     - decimal
=AA200000 (in hexadecimal).
```

Hinweis: Die Bits 14 bis 32 sind "nicht wichtig" (X).

Für Gruppe 2 ist die rechte Seite des Headers verkabelt, und die Bitmap wird unten angezeigt.

```
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
(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
=55100000 (hex)
```

Es muss Switch-Gruppen eingerichtet werden, oder der Switch erkennt nicht, welche Ports und Relays zum Umschalten verwendet werden. Bei der Einrichtung von Bitmaps kann die Zahl als Dezimalformat eingegeben werden oder muss sie mit 0x vor dem Hexadezimalcode eingegeben werden, damit die Software erkennt, dass sie Hexadezimalformat ist. Geben Sie die Befehlssatzgruppe **Group2 0x5510000** ein, um die Bitmap zuzuweisen. Group2 ist eine alphanumerische Zeichenfolge, die mit einem Buchstaben beginnen muss.

Tipp: Die beiden oben angegebenen Bitmaps sind Teil des empfohlenen Referenzdesigns. Der 4+1-Modus ist völlig anders, und es wird empfohlen, den Bitmaprechner zu verwenden. Bei einem 4+1-Schutzschema würden vier HCCP-Gruppen vorhanden sein. HCCP-Gruppen 1 und 2 in der "Protect 2"-Karte und HCCP-Gruppen 3 und 4 in der "Protect 1card". Schutz 1 deckt außerdem Steckplätze 5-8 am Switch ab. In der uBR-Konfiguration werden diese Steckplätze jedoch als Steckplätze 1-4 bezeichnet.

Wenn Sie statt MAC-Domänen einzelne Ports umschalten, müssen Sie wissen, welches Schutzschema Sie ausführen, und anhand der Tabelle unten wissen, welche Gruppennummer Sie verwenden sollen. Angenommen, der Switch befindet sich im 4+1-Modus. Der Befehl wird unten für den uBR10K angezeigt.

```
hccp 1 channel-switch 1 ds rfswitch-module 1.10.84.3 26 1
```

```
hccp 1 channel-switch 1 us rfswitch-module 1.10.84.3 10 1
```

Dies zeigt die IP-Adresse des Switches und des Moduls 26 an, das anzeigt, dass Karte 2 Sicherungskopien von Port G in einem Schema mit 4+1 anzeigt, und Modul 10, das anzeigt, dass Karte 2 Sicherungskopie von Port C anzeigt. All dies befindet sich in Steckplatz 1 des Switches.

Die nachfolgende Tabelle zeigt beide Modi und die Anzahl, die mit dem jeweiligen Port korreliert.

8+1-Modus	4+1-Modus
A(1) H(2)	A(1,2) H(3,4)
B Nummer 3 Teil I Nummer 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)

Festlegen der Steckplatzkonfiguration

Die neue Firmware ermöglicht die Konfiguration des Chassis für eine beliebige Mischung von Upstream-/Downstream-Karten. Dies wird mithilfe der neuen CLI-Befehlssatzsteckplatzkonfiguration **USlots DSlots** erreicht.

Die ***US-Steckplätze*** und die ***DS***-Steckplätze *sind 16-Bit-Ganzzahl-Bitmasken*, die angeben, ob das Modul für diesen Kartentyp aktiviert/konfiguriert ist, wobei das Bit rechts das Modul 1 darstellt. Automatisierte Konfigurationen finden Sie im neuen Bitmaprechner.

Wenn Sie beispielsweise ein Chassis mit vier Linecards, Upstream-Karten in den Modulen 1-2 und Downstream-Karten in den Modulen 3-4 einrichten möchten, geben Sie den Befehl **set slot config 0x003 0X000c ein**.

Die Steckplatzkonfiguration wird separat von der Anwendungs-Firmware auf nvmem gespeichert. Dies ermöglicht zukünftige Upgrades der Anwendungs-Firmware, ohne dass der Benutzer die Steckplatzkonfiguration neu programmieren muss, und ermöglicht die Verteilung des Anwendungscodes für alle RF-Switch-Konfigurationen.

Normalerweise würde die Fabrik diese Konfiguration bei der Installation der Einheit vornehmen. Dies würde Ihnen jedoch ermöglichen, die Konfiguration im Feld zu ändern, wenn Sie möchten, und eine beliebige Anzahl an Karten/eine beliebige Mischung von Karten zu verwenden, die Sie in Zukunft benötigen könnten.

Nachfolgend finden Sie eine Beispielkonfiguration.

```
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
```

Testen der RF-Switch-Relays

Cisco empfiehlt, die Relays einmal pro Woche und mindestens einmal pro Monat zu testen. Konsole oder Telnet in den Switch einstecken und geben Sie das Befehl-**Testmodul aus**. Wenn im RF-Switch ein Kennwort festgelegt ist, geben Sie den **Befehl password *password name* ein, um den Testbefehl zu verwenden.** Dadurch werden alle Relays auf einmal getestet und der normale Arbeitsmodus wiederhergestellt. Verwenden Sie diesen Testbefehl nicht, wenn Sie sich im Schutzmodus befinden. **Verwenden Sie diesen Testbefehl nicht, wenn Sie sich im Schutzmodus befinden.**

Tipp: Sie können die Relays auf dem Switch umschalten, ohne den Umrichter oder eines der Modems zu beeinflussen. Dies ist wichtig, wenn die Relays getestet werden, ohne dass tatsächlich eine der Linecards oder die entsprechenden Upkonverter gewechselt werden müssen. Wenn ein Relay auf dem Switch aktiviert ist und ein Failover erfolgt, wechselt er in den richtigen Zustand und wechselt nicht nur zwischen den Zuständen.

Geben Sie den Befehl **switch 13 1** ein, um Port G an Steckplatz 1 des Switches zu testen. Sie können eine gesamte Bitmap testen, indem Sie den Befehl **switch *group name* 1** eingeben. Geben Sie den Befehl **switch *group name* 0** (oder **idle**) ein, um die Relays für den normalen Arbeitsmodus zu deaktivieren.

Zusätzlich sollte der Kunde einen CLI-Failover-Test einer HCCP-Gruppe (Ausgabe des Befehls **hccp *g* switch *m***) vom CMTS durchführen, um die Schutzkarte zu testen und den Pfad zu schützen. Dieser Failover-Typ kann 4-6 Sekunden dauern und dazu führen, dass ein kleiner Prozentsatz der Modems offline geht. Daher sollte dieser Test weniger häufig und nur außerhalb der Spitzenzeiten durchgeführt werden. Die oben genannten Tests tragen zur Verbesserung der allgemeinen Systemverfügbarkeit bei.

Aktualisieren des RF-Switch-Codes

Befolgen Sie die unten aufgeführten Schritte.

1. Laden Sie die neuen Images in den uBR mit einer Flash-Diskette in Steckplatz 0.
2. Konfigurieren Sie die folgenden Befehle im uBR.

```
tftp-server disk0: rfsw330-bf-1935022g alias rfsw330-bf-1935022g
tftp-server disk0: rfsw330-fl-1935030h alias rfsw330-fl-1935030h
```

3. Schließen Sie den Switch an, und geben Sie den Befehl **set tftp-host {ip-addr}** aus. Verwenden Sie die IP-Adresse des uBR für TFTP-Übertragungen.
4. Stellen Sie die **Kopie an ftp:rfsw330-bf-1935022g bf:** -Befehl, um den Bootflash zu laden, und **kopieren Sie tftp:rfsw330-fl-1935030h fl:** um den Flash zu laden.
5. Starten oder neu laden, sodass der neue Code ausgeführt wird. Geben Sie **PASS SYSTEM** und **Save Config** ein, um die neuen nvmem-Felder zu aktualisieren. Starten Sie den

Computer erneut, damit dies alles in Kraft tritt.

Warnung: Möglicherweise müssen Sie einige Konfigurationen nach dem erneuten Laden zurücksetzen, z. B. die IP-Adresse des Switches. Überprüfen Sie die Switch-Konfiguration nach dem erneuten Laden zur Überprüfung. Nach dem Upgrade auf Version 3.5 kann dem Switch eine Standard-Gateway-Adresse hinzugefügt werden, und neue Upgrades für den Switch können remote über Subnetze vorgenommen werden. Beim Laden von Unix-Stationen darf der neue Bildname nur in Kleinbuchstaben verwendet werden. Dieses neue Image fügt außerdem eine DHCP-Client-Option und eine Chassis-/Modulkonfigurationseinstellung hinzu.

DHCP-Betrieb

Diese Version bietet vollständige Unterstützung für einen DHCP-Client. Der DHCP-Vorgang ist standardmäßig aktiviert, es sei denn, der Benutzer hat eine statische IP-Adresse aus der CLI festgelegt. Befehle wurden hinzugefügt/erweitert, um den DHCP-Betrieb zu unterstützen.

Wenn der RF-Switch hochgefahren wird, prüft er, ob DHCP aktiviert wurde. Dies erfolgt auf verschiedene Weise über die CLI. Sie können einen der folgenden Befehle verwenden, um DHCP zu aktivieren:

```
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.
```

Der RF-Switch geht nicht mehr von einer statischen IP-Adresse von 10.0.0.1 aus, wie dies in Versionen vor 3.00 der Fall war.

Wenn diese Funktion aktiviert ist, installiert der RF-Switch den DHCP-Client und versucht, einen DHCP-Server zu finden, um eine Lease anzufordern. Der Client fordert standardmäßig eine Leasingzeit von 0xffffff (unendlicher Leasing) an. Dies kann jedoch durch den **Befehl set dhcp leasetime _*secs*** geändert werden. Da die tatsächliche Leasedauer vom Server gewährt wird, wird dieser Befehl hauptsächlich für Debug/Tests verwendet und sollte für den normalen Betrieb nicht erforderlich sein.

Wenn sich ein Server befindet, fordert der Client Einstellungen für IP-Adresse und Subnetzmaske, eine Gateway-Adresse und den Speicherort eines TFTP-Servers an. Die Gateway-Adresse wird aus Option 3 (Routeroption) übernommen. Die TFTP-Serveradresse kann auf verschiedene Weise angegeben werden. Der Client überprüft die Next-Server-Option (Sid), Option 66 (TFTP-Servername) und Option 150 (TFTP-Serveradresse). Wenn alle drei oben genannten Adressen nicht vorhanden sind, wird für die Adresse des TFTP-Servers standardmäßig die DHCP-Serveradresse verwendet. Wenn der Server ein Lease gewährt, zeichnet der DHCP-Client die angebotene Leasedauer für die Verlängerung auf und fährt mit dem Bootvorgang fort, indem er die anderen Netzwerkanwendungen (Telnet und SNMP) und die CLI installiert.

Wenn sich ein Server nicht innerhalb von 20-30 Sekunden befindet, wird der DHCP-Client ausgesetzt und die CLI ausgeführt. Der DHCP-Client wird im Hintergrund ausgeführt und versucht, ungefähr alle fünf Sekunden einen Server zu kontaktieren, bis sich ein Server befindet, eine statische IP über die CLI zugewiesen wird oder das System neu gestartet wird.

Mit der CLI kann der Benutzer alle Netzwerkeinstellungen überschreiben, die über den Server empfangen werden können, und statische Werte für diese Einstellungen zuweisen. Alle **festgelegten xxx**-Befehlsparameter werden in nvmem gespeichert und für Neustarts verwendet.

Da die aktuellen Netzwerkeinstellungen nun entweder von DHCP oder der CLI übernommen werden können, wurden einige Änderungen/neue Befehle implementiert. Der bestehende Befehl **show config** wurde geändert, um die Einstellungen aller nvmem-Parameter anzuzeigen, die nicht unbedingt die zu diesem Zeitpunkt gültigen Parameter sind.

Um die aktuell verwendeten Netzwerkparameter abzurufen, wurde der neue Befehl **show ip** hinzugefügt. Neben den Netzwerkeinstellungen zeigt dieser Befehl auch den aktuellen IP-Modus (statisch im Vergleich zu DHCP), den Status des DHCP-Clients und den Status der Telnet- und SNMP-Anwendungen (die nur gestartet werden, wenn eine gültige IP vorhanden ist).

Ein zusätzlicher Befehl, **show dhcp**, wurde zu Informationszwecken hinzugefügt. Dieser Befehl zeigt die vom DHCP-Server empfangenen Werte sowie den Status der Leasedauer an. Die angezeigten Zeitwerte haben das Format HH:MM:SS und beziehen sich auf die aktuelle Systemzeit, die ebenfalls angezeigt wird.

Die Zuweisung statischer Werte für alle konfigurierbaren Netzwerkparameter sollte sofort wirksam werden und die aktuelle Einstellung ohne weitere Maßnahmen überschreiben. So können einige Parameter dynamisch bleiben und andere korrigiert werden. Beispielsweise kann DHCP zum Abrufen der IP-Adresse verwendet werden, wobei die Einstellung für den TFTP-Server über die CLI beibehalten wird. Eine Ausnahme bildet hierbei der Wechsel von einer statischen IP-Adresse zu DHCP. Da der DHCP-Client nur bei Bedarf beim Hochfahren installiert wird, muss das System neu gestartet werden, damit DHCP wirksam wird.

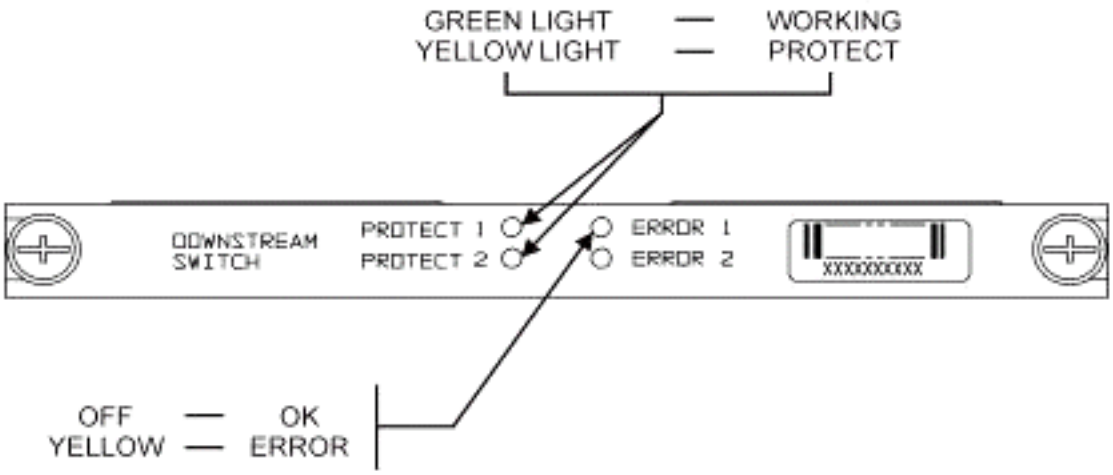
LEDs

Die entsprechenden Modul-LEDs leuchten von grün zu orange/gelb. Das Layout ist von der Rückseite anders, d. h. wenn die Switch-Gruppe links im Header in Steckplatz 1 des Switches in einem 8+1-Modus ausfällt, werden die Protect 1-LEDs auf der rechten Seite von grün in orange geändert, um anzuzeigen, dass die Relays umgeschaltet wurden.

Die Abbildung unten zeigt die Farbunterschiede bei den LEDs und stellt kein spezielles Failover dar.

- LED Nr. 1 Grün/Gelb zeigt an, dass sie funktioniert/schützt 1
- LED Nr. 2 Grün/Gelb zeigt an, dass sie funktioniert/schützt 2
- LED Nr. 3 Aus/Gelb zeigt ein Problem an Kanal 1 an
- LED Nr. 4 Aus/Gelb zeigt ein Problem an Kanal 2 an

Das Moduldiagramm ist unten dargestellt.



Die folgende Abbildung zeigt die Ethernet-Controller-Anzeigen.

-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

Kundenprobleme und -anwendungen

Einige Punkte, die als Probleme angesehen werden können, sind die Kosten, die Nutzung aller Komponenten, Einfügeverlust, physisches Layout, kleine Steckverbinder und Kabel sowie die Verfügbarkeit und Unterstützung dieser Komponenten.

Der Einfügungsverlust von 6 dB im Arbeitsmodus kann ein Problem sein. Bei Wechseln des Switches in den geschützten Modus treten außerdem weitere Einfügedämpfungen (etwa 1-2 dB) auf. Dies hängt von der Häufigkeit ab, mit der Sie DS verwenden. Die Einfügungsdämpfung in den USA liegt bei etwa 4,5 dB.

Die Akzeptanz in der Branche kann sich im Hinblick auf die kleineren MCX-Anschlüsse und das kleinere Koaxialkabel, das für die Lösung verwendet wird, als zeitaufwendig erweisen. AOL Time Warner entschied sich für den Kauf von 3.000 m Kabeln dieser Art, um einige der US-Kabel an den Kopfenden neu zu verkabeln. Die Charta nutzt diese Kabel jetzt auch. Wenn sie das Kabel

verwenden, ist es nur eine Frage der Zeit, bis sie und andere Hersteller auch den neuen kleineren Steckverbinder verwenden. Der neue Upper-Konverter von VCom verwendet jetzt MCX-Connectors.

WhiteSands Engineering stellt die Kabelkits für Cisco her. Cisco muss ein Mindestformat an Kabelkits vorrätig halten, um unser empfohlenes Design zu erfüllen. Sie können WhiteSands direkt für spezielle Kabelbestellungen aufrufen. Sie können die erforderlichen Werkzeuge für die Anbindung über CablePrep oder WhiteSands erhalten.

Bei der Teilenummer des RF-Switches wird zwischen Groß- und Kleinschreibung unterschieden. Sie müssen **uBR-RFSW** eingeben, um den Switch zu bestellen.

Betriebliche Probleme

Berücksichtigen Sie die unten beschriebenen Situationen.

Eine 5 x 20 Line Card ist defekt, und die Linecard zum Schutz übernimmt die Sicherung. Sie trennen die fehlerhafte Linecard, und das DS-Signal von der Linecard für den Schutz, die Rückfeeds zum Ende des nicht angeschlossenen Kabels, das zuvor an die andere Linecard angeschlossen war und jetzt nicht terminiert wurde, wird abgeschaltet.

Dies führt zu einem Impedanzungleichgewicht und reflektierender Energie, die etwa 7 dB vom ursprünglichen Signal entfernt ist. Der Grund hierfür ist, dass der Splitter im Switch-Chassis nur etwa 7 dB Isolation aufweist, wenn der gemeinsame Port nicht terminiert wird. Die betroffenen Frequenzen hängen mit der physischen Länge des Kabels zusammen, das getrennt wurde.

Diese Idee wird helfen, das potenzielle Risiko einer Änderung des DS-Levels um bis zu 3 dB zu verringern:

- Schließen Sie die DS-Kabel mit 75 Ohm-Abschlusswiderständen an. Möglicherweise sind spezielle MCX-Terminatoren erforderlich.

In einer anderen Situation werden beim Tippen durch den RF-Switch-Telnet-Zugriff von der uBR10K-Konsole doppelte Einträge erstellt. Eine Problemumgehung besteht darin, lokales Echo zu deaktivieren. Beispiel: In der CLI wird **telnet** ***ip address*** **/noecho** ausgegeben. Sie müssen **Strg-Break** drücken, um die Verbindung herzustellen, oder **steuern** Im Telnet-Befehlsmodus**. Geben Sie quit** oder **send break ein**. Eine andere Möglichkeit, die Verbindung zu trennen, besteht darin, **Strg+Shift+6+x zu** drücken und **disk 1** aus der uBR-Befehlszeile einzugeben. Informationen zu einigen standardmäßigen Unterbrechungssequenzen finden Sie unter Standardkombinationen für Break Key Sequence während der Kennwortwiederherstellung.

Verdeckte Anwendungen

Betrachten Sie die unten beschriebene Situation.

Die US-Schutzkabel am uBR können zum Testen der Signalstärke für die entsprechende Arbeit verwendet werden. Nehmen Sie beispielsweise an, der Switch befindet sich im 8+1-Modus, ein funktionierendes Blade in Steckplatz 8/0 des uBR, ein geschütztes Blade in Steckplatz 8/1 und das funktionsfähige bis zu Steckplatz 1 des Switches. So testen Sie den US-Stromversorgungszustand auf US0 der Karte 8/0, Telnet oder Konsole im Switch und geben den Befehl **switch 1 1** aus. Dadurch wird das Relay aus Steckplatz 1 des Switches für Modul 1 aktiviert, das auch als Port A des Switches bezeichnet wird. Trennen Sie das Kabel an US0 des

geschützten Blades, und schließen Sie es an einen Spektrumanalysator an. Sie können das US-Signal testen, das tatsächlich an die funktionsfähigen US0 gesendet wird.

Befehle anzeigen

Verwenden Sie zur Fehlerbehebung die folgenden Befehle.

Anzeigeversion

```
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
```

Anzeigemodul für alle

```
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
```

RF-Switch-Spezifikationen

In der folgenden Liste sind die RF-Switch-Spezifikationen aufgeführt.

- Eingangsleistung Wechselstrom - 100 bis 240 V Wechselstrom, 50/60 Hz, Betriebsbereich - 90 bis 254 V Wechselstrom
- Gleichstrom - Drei Terminalbaustein - 48/60 V Gleichstrom, Bereich - -40,5 bis -72 V Gleichstrom, 200 mVPP-Blende/Geräusch
- Temperaturbereich: 0 bis +40° C, Betriebstemperatur: -5 bis +55° C
- Einheitensteuerung 10BaseT SNMP Ethernet und RS-232 Bus - 9-poliger Stecker D
- RF-Anschlüsse - MCX, Impedance - 75 Ohm
- Max. RF-Eingangsleistung: +15 dBm (63,75 dBmV)
- Switch-Typ - Elektromech, absorbierend für Arbeitspfad, nicht absorbierend auf Schutzpfaden
- DS-Frequenzbereich - 54 bis 860 MHz
- Max. DS-Einfügungsverlust - 5,5 dB bei der Verarbeitung zur Ausgabe, 8,0 dB beim Schutz zur Ausgabe
- DS Insertion Loss Flatness - +1,1 dB von der Arbeit bis zur Ausgabe, +2,1 dB vom Schutz bis zur Ausgabe
- DS-Ausgangsverlust - größer als 15,5 dB
- DS-Isolierung - mehr als 60 dB bei Betrieb, mehr als 20 dB bei Betrieb zum entsprechenden Schutz im Schutzmodus und mehr als 60 dB bei der Arbeit im Arbeitsmodus
- Upstream-Frequenzbereich - 5 bis 70 MHz
- Maximaler Upstream-Einfügungsverlust - 4,1 dB von Eingang zu Betrieb, 5,2 dB von Eingang zum Schutz
- Verlustfreiheit bei Einfügung in den USA - + 0,4 dB vom Eingang zum Betrieb, + 0,6 dB vom Eingang zum Schutz
- Rückflussdämpfung bei US-Eingang: mehr als 16 dB
- US-Isolierung - mehr als 60 dB bei Betrieb, mehr als 20 dB bei Betrieb zum entsprechenden Schutz im Schutzmodus und mehr als 60 dB bei der Arbeit im Arbeitsmodus
- Formfaktor: 19 x 15,5 x 5,25 (482 mm x 394 mm x 133 mm), Gewicht: 36 lbs

Zugehörige Informationen

- Cisco RF-Switches
- N+1 Tipps und Konfiguration für uBR 10K mit MC28C-Karten
- Technischer Support - Cisco Systems