N+1 Redundantie met de Cisco RF-Switch

Inhoud

Inleiding

Dit document geeft informatie over N+1 redundantie met behulp van de Cisco® RF Switch.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Zie de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Om de meeste waarde voor hun geld te krijgen, hebben veel kabelexploitanten besloten redundantie te bieden voor hun glasvezelnetwerk in de vorm van extra back-upvoeding in het glasvezelknooppunt, ononderbrekbare voedingen (UPS) met aardgas en batterijen, en extra

glasvezelzenders in het knooppunt. Extra donkere vezels kunnen ook aan elk knooppunt worden toegewezen in geval van een vezelstoring.

Zoals hierboven is uitgelegd, is hardware het eerste wat in de externe fabriek wordt bedekt. Hoe zit het met de feitelijke upstream- (VS) en downstreamsignalen die op het transportmedium reizen? In de VS heeft Cisco Advanced Spectrum Management-technieken geïmplementeerd om de modems online te houden en optimaal te verzenden. Sommige van deze technieken zijn frequentieshoppen met geavanceerde 'kijk voor je lek'-mogelijkheid via de on-board spectrumanalyzer-dochterkaart op de S-kaart. Cisco heeft ook wijzigingen in het modulatieprofiel en wijzigingen in de kanaalbreedte opgenomen. Dankzij al deze functies kan de modem binnen het spectrum blijven, een robuuster modulatieprofiel gebruiken en/of de kanaalbreedte wijzigen om de service geoptimaliseerd te houden wat betreft doorvoersnelheid en beschikbaarheid. Wanneer je naar DS-frequenties kijkt, heb je een keuze uit 64 of 256-QAM. Hoewel deze modulatieregelingen veel minder robuust zijn dan de VS op QPSK of 16-QAM, is het DS-spectrum veel voorspelbaarder en onder controle dan het Amerikaanse spectrum.

De beschikbaarheid van hardware in het head-end is het volgende logische ding om je op te concentreren. Als één bron van AC of DC faalt, kan de back-up van de generator worden gebruikt met redundante voedingen voor het geval dat één bron slecht gaat.

Een ander hardware-of-fail-storing zou de Cable Modem Termination System (CMTS) voeding zijn. De uBR10K-voedingseenheid gebruikt een algoritme voor back-up en taakverdeling. Dit wordt soms N:1 genoemd, wat 1 betekent voor N back-up met taakverdeling. In dit geval zal het 1:1 zijn, en u zult merken dat het totale DC-vermogen iets meer is, met twee power entry modules (PEM's), dan als er één gebruikt werd voor de gehele lading. Geef de **sh cont klokreferentie** opdracht uit om deze informatie te bekijken.

```
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
```

Om zich op de beschikbaarheid van CMTS lijnkaarten te concentreren, heeft Cisco een protocol ontwikkeld om te specificeren hoe CMTSs in een hoog-beschikbaarheid scenario met elkaar zullen communiceren. Dit protocol wordt Hot Standby Connection-to-Connection Protocol (HCCP) genoemd. Dit protocol biedt een hartslag tussen het beveiligingsapparaat en de werkapparatuur(en) om de interfaces/apparaten gesynchroniseerd met de MAC-tabellen, -configuraties enzovoort te houden. Cisco heeft ook een RF-Switch ontwikkeld om een hoge beschikbaarheid op het MAC-domeinniveau te bieden in plaats van een chassis voor chassis. Een MAC-domein kan ook worden gezien als RF-SUBNET, dat één DS is en alle bijbehorende VS's.

Cisco heeft een paar jaar lang 1+1 redundantie op de uBR7200 Series chassis aangeboden, maar een volledig chassis moet leeg als een beschermd chassis. Het voordeel van 1+1 is dat er geen RF-Switch nodig is, maar minder schaalbaar. Dankzij het gebruik van een RF-Switch kan redundantie op interfaceniveau worden toegepast voor beschikbaarheid van N+1. Dit betekent 1 voor N back-up zonder taakverdeling of -verdeling. In plaats van een volledig chassis dat niets doet, kunt u één invalshoek/beveiligingskaart hebben of een interface die veel andere interfaces beschermt. UBR100012 kan worden ingesteld als één kaart die zeven anderen beschermt. Dit helpt met de economie omdat deze nu 7+1 beschikbaarheid biedt en ook de benodigde vereisten voor PacketCable doorgeeft.

Nadat deze punten zijn gedekt, wilt u zeker zijn dat u overtolligheid voor de backhaul-kant hebt, ook bekend als WAN of LAN-kant, afhankelijk van hoe u ernaar kijkt. Hot Standby Router Protocol (HSRP) is al jaren actief en maakt redundante paden tussen routers mogelijk om een niveau van beschikbaarheid te bieden dat nodig is voor dit single-point-of-fail. De werkelijke druk op deze functies is VoIP en toegenomen concurrentiedruk om de meest stabiele/beschikbare service aan de klant te leveren.

Operationele reeks gebeurtenissen

uBR10K-oplossing

HCCP gebeurt eerst tussen het chassis via de hartslag. Aangezien de uBR10K-oplossing allemaal in één chassis zit, is de hartslag mogelijk niet relevant. Als interne communicatie- en interfacewijzigingen succesvol zijn, zal HCCP een opdracht naar de RF-Switch blijven sturen om de juiste relais in te schakelen.

uBR7200 oplossing

HCCP gebeurt eerst tussen het chassis via de hartslag. Een opdracht wordt vervolgens vanuit de beveiliging 7200 naar de upconverter (UPx) verzonden om de frequentie te wijzigen. De UPx stuurt een ACK. De beveiliging 7200 stuurt een opdracht om de werkende UPx module uit te schakelen en wacht op een ACK. De beveiliging 7200 stuurt dan een opdracht om de security UPx module in te schakelen en wacht op een ACK. Als al dit werkt of geen ACK van de werkende UPx module wordt verzonden, dan zal het verder gaan en een opdracht naar de switch sturen om de aangewezen relais om te schakelen.

Er zijn twee soorten hartslagmechanismen die relevant zijn voor HCCP. Ze staan hieronder vermeld.

1. HalloACK tussen de arbeiders en beveiligers — De beschermer LC stuurt een hallo bericht naar elk van de werkgroepen van de LC's in zijn groep, en verwacht een halloACK als reactie. De uitzendfrequentie van de hallo en halloACK is Configureerbaar op de bescherming van LC met CLI. Verder is de minimale hallo-tijd van de 7200 0,6 seconden, terwijl het minimum voor uBR10K 1,6 seconden is.
2. Sync pulse mechanism — Dit is een HCCP-data-plane hartslag mechanisme, en de frequentie ervan is niet Configureerbaar. De sync-pulsen worden door elk werkend LC naar zijn peer security LC verzonden. Deze sync-puls wordt één keer per seconde verzonden. Als drie sync-pulsen gemist zijn, wordt de peer uitgeschakeld. Cisco werkt aan een snel foutdetectiemechanisme om een werkende crash in de uitzonderingsgeleider te detecteren in minder dan 500 msec. De doelrelease is 12.2(15)BC. Bij de VXR kan echter door beide mechanismen een storing worden gedetecteerd, aangezien uBR10K alle interne HCCP is, is alleen het tweede relevante van belang.

RF-Switch

Cisco besloot een externe RF-Switch in plaats van een lijnkaart of interne bedrading die als RF-Switch zou werken vanwege toekomstige schaalbaarheid en complexiteit. De externe switch kan gestapeld worden en gebruikt worden voor meerdere scenario's, verschillende dichtheid en legacy-apparatuur.

Op de achterzijde van de switch staan 252 aansluitingen in een 3RU-pakket (rackeenheid). 1RU is 1,75 inch. De VCom HD4040-upconverter is 2RU.

Als de backplane op een bepaalde manier is geconfigureerd voor een interne switch, beperkt u de flexibiliteit om later langs de weg verschillende lijnkaartdichters te doen. Als een lijnkaart te dicht is dan worden te veel Amerikaanse havens getroffen door fouten die specifiek zijn voor één VS of DS en in het algemeen kaart. Daarom is er vanaf het begin een switch en redundantie nodig. Meer dichtheid is gelijk aan meer klanten die door één enkele gebeurtenis worden getroffen. Wat gebeurt er als pure DS-kaarten en pure Amerikaanse kaarten worden verkocht? In de toekomst zult u in staat zijn om Amerikaanse en DS-havens over de lijnkaarten te evenaren. Het externe ontwerp beschermt mijn investeringen in de toekomst verder.

U kunt nooit redundantie tussen chassis met een interne switch doen. Als je geld wilt besparen en er vier van 7200 uBR's door één willen laten ondersteunen, is er een externe RF-Switch nodig. Tenzij u denkt aan linecards in een chassis met een ander in hetzelfde chassis. Het enige probleem is dat als het hele chassis naar beneden gaat, je geen back-up hebt.

De beschikbaarheidsgetallen kunnen beter zijn voor een externe switch (ten minste met betrekking tot de elektronica, niet de bekabeling) vanwege minder actieve componenten. Aangezien de switch een volledig passief ontwerp heeft in het chassis, is de normale werkmodus operationeel, zelfs indien de actieve modules worden verwijderd. De informatiecentra bevinden zich alleen op het beveiligingspad met een volledig passief werkpad en kunnen worden gedraaid om de switch te testen zonder dat de werkmodus wordt beïnvloed. Dit betekent dat de normale werkmodus niet wordt beïnvloed door een stroomuitval op de switch, een uittrek van de switch of een storing van de switch. Het negatieve hiervan is het verlies van potentieel 6 tot 8 dB bij de hoogste DS-frequentie van 860 MHz.

Het externe ontwerp maakt het ook mogelijk de kabelmigratie en lijnkaartverwisselen mogelijk. Als iemand van een 2x8-kaart naar een 5x20-kaart wil upgraden, kan de lijnkaart worden gedwongen om in de beveiligingsmodus te springen. De lijnkaart kan worden vervormd in een tempo dat u bepaalt met de nieuwere, dikkere 5x20 kaart en wordt aangesloten voor toekomstige domeinen. De twee domeinen die in de beveiligingsmodus zaten, worden dan teruggezet naar de corresponderende interface/domeinen op de 5x20-kaart. Andere kwesties moeten worden aangepakt, zoals de 5x20-opdrachten voor converters en -aansluitingen.

Het voorpaneel heeft de LEDs, voedingskabel voor AC of DC, Ethernet connectiviteit, RS-232 connectiviteit, en een switch om AC, DC, of uit aan te wijzen. Er wordt bij elke switch ook een kabelextractiemiddel meegeleverd. Zorg ervoor dat u de rubberlaars verwijdert voor gebruik. De trekkracht kan met een schroevendraaier worden ingesteld door met de klok mee in te draaien op de achterzijde van het gereedschap.

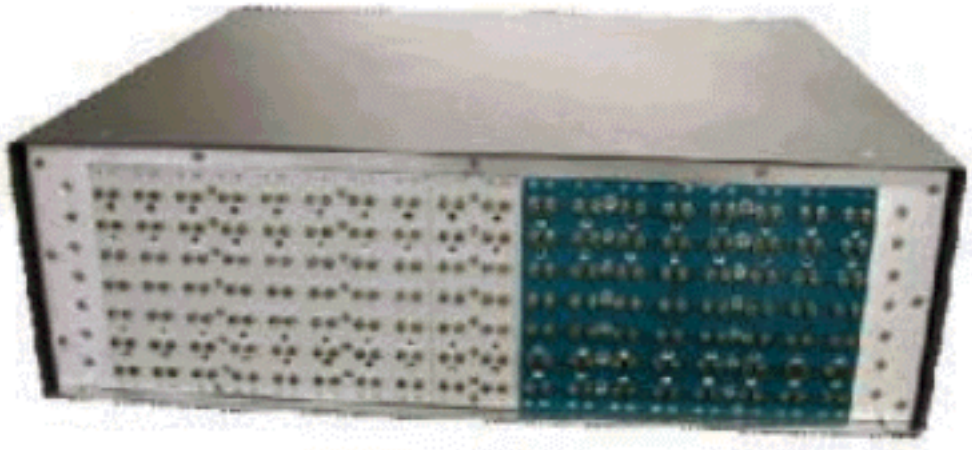
Het onderstaande beeld is het vooraanzicht van de RF-Switch.

Er zijn tien VS (weergegeven in blauw) en drie DS (weergegeven in grijs) modules geïnstalleerd in de 3x10 RF Switch. De linker onderkant is bekend als module N en is leeg. De modules aan de voorkant, die van de rechterbovenhoek beginnen, zijn nummers 1-13 en correëren met de poorten A-M. Upstream Module 1 heeft alle relais voor poort A in slots 1 tot en met 8 en beschermen 1 en 2 op de achterzijde. Module 2 is links en heeft alle relais voor poort H in slots 1 tot en met 8 en beschermt 1 en 2.

De modules kunnen echter worden omgedraaid, maar de extractie van de kaart is zeer moeilijk. Deze zijn zeer dicht en de twee in gevangenschap levende schroeven moeten worden losgelaten voordat zij zich aan de lijn trekken. U moet mogelijk met een schroevendraaier open prikken of naar links en rechts verschuiven terwijl u zich eruit trekt.

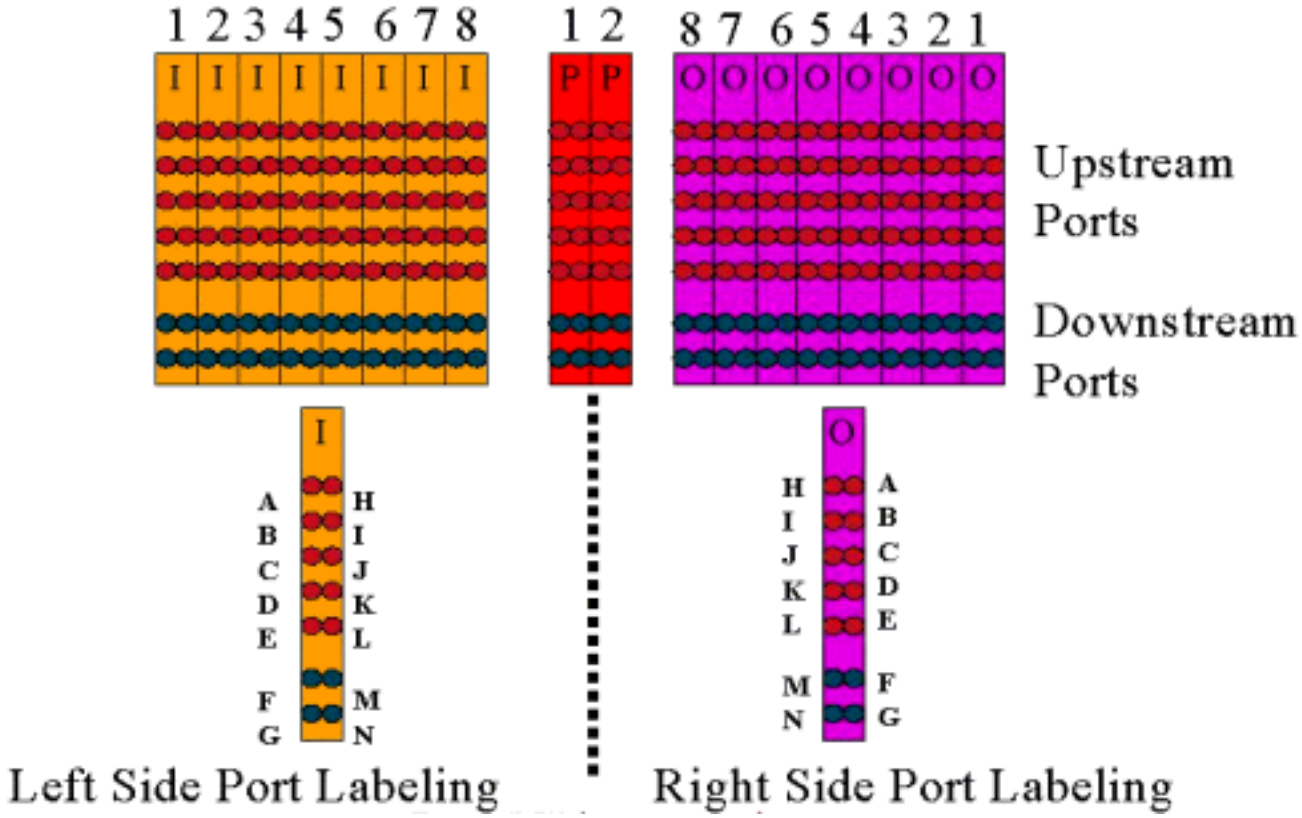
Het achterpaneel is voorzien van etiketten met **CMTS**, **Protect**, en **Cable Plant**. De **CMTS** kant is voor de werkende input. De zijde van de **kabelfabriek** bevat alle uitgangen om de kabelfabriek te voeden.

Het onderstaande beeld is het achteraanzicht van de RF-Switch.



De acht werkende 'inputs' zijn van links naar rechts genummerd. De twee bescherming zitten in het midden en de acht uitgangen rechts.

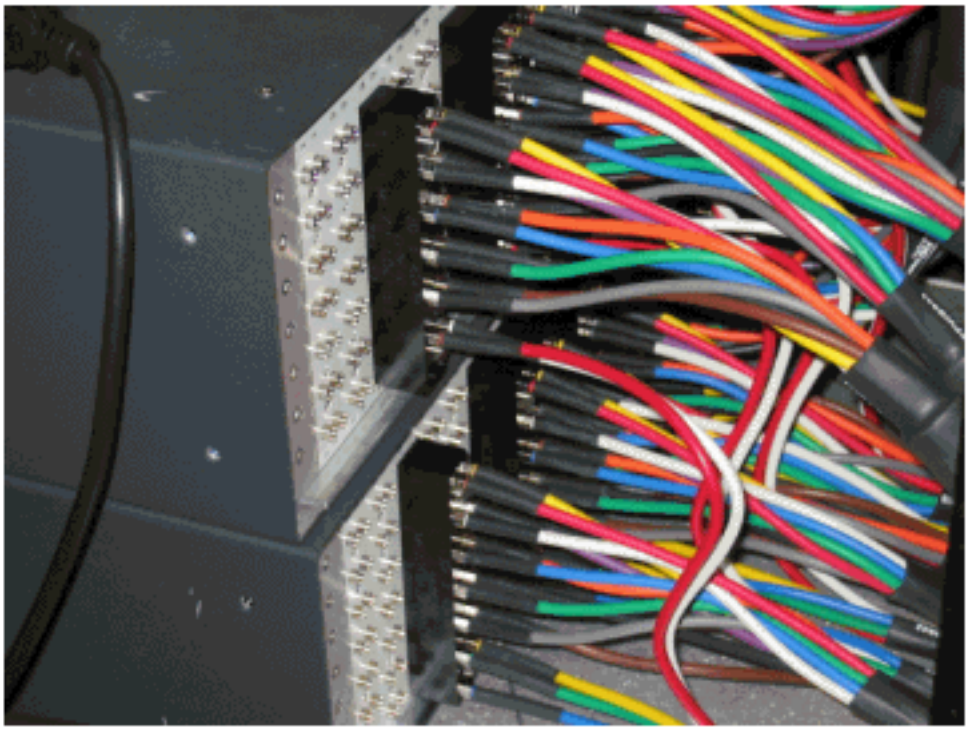
Het onderstaande beeld is het RF Switch nummeringsschema.



Opmerking: Port N is niet gebruikt.

De output (gekleurd paars) vertegenwoordigt de kabelfabriek. Uitvoer 1 staat linksboven, terwijl Input 1 linksonder is. Ook de havens worden gespiegeld. Vergeet niet dat poort N niet wordt gebruikt. Zorg er gewoon voor dat je consequent bent op de bedrading.

Dit beeld hieronder is het achteruitzicht van de RF-Switch met de 14-poorts header en speciale Belden mini-coax kabel met MCX-connectors.



De MCX-connectors kunnen rechtstreeks aan de switch worden bevestigd, maar u loopt het risico op losse aansluitingen, emissies en mogelijke onderbrekingen. Cisco heeft een header ontwikkeld

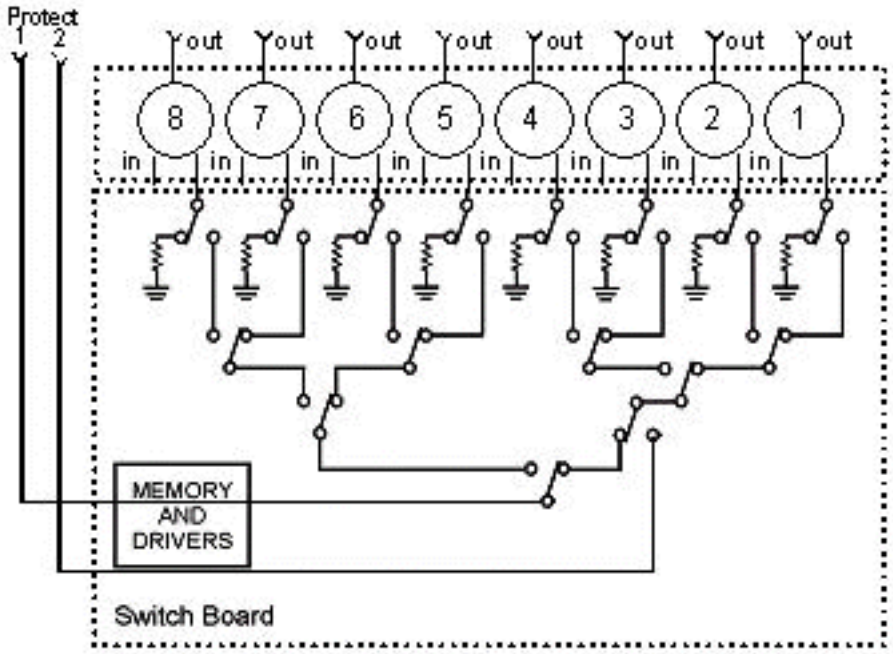
om deze problemen op te lossen.

De MCX-connectors klikken in de header en er is een speciaal gereedschap verzonden met elke switch die wordt aangeschaft voor extractie. De header heeft twee bedieningspennen die maar op één manier gaan. Er staat een lichte schuine rand op de bovenrand om de bovenkant van de kop aan te geven. Er zijn twee schroeven voor het bevestigen van de kop aan de switch. Er wordt ook een kabelbeheerbeugel meegeleverd bij elke RF-Switch.

Tip: U kunt de kop ook op de switch installeren en vervolgens de MCX-connectors in de header plaatsen. Hierdoor kan het gemakkelijker worden geïnstalleerd. Draai de kop niet aan de switch vast totdat alle connectors zijn geïnstalleerd.

Configuratie en werking van RF-Switch

Het onderstaande beeld is een blokschema van de RF-Switch.



De combinatoronderdelen bevinden zich in het chassis van de switch, maar de relais bevindt zich in elke afzonderlijke, verwijderbare module. Elk relais eindigt met een lading van 75 ohm, slechts in het Beschermingspad, niet de in/het werk weg.

Stel seriële communicatie met de switch in door verbinding te maken met HyperTerminal of TeraTerm, een console/rollover-kabel, Cisco 9 pins tot RJ-45 adapter en met een basissnelheid van 9600.

Stel een IP-adres en -masker in door de opdracht uit te geven die **op ip-adres *is* ingesteld*, voegt u een subnetmasker toe*.** Zodra dit wordt gedaan, kunt u in Telnet en ook een wachtwoord van telnet instellen. Stel vervolgens het beveiligingssysteem in (of dit nu 4+1 of 8+1 is) door de opdracht uit te geven **ingesteld** op **poort 4/8**. De standaard is 8+1, waar bescherming 1 geldt voor alle acht invoersleuven. In de 4+1-modus beschermt u 1 "slots" 5-8 en beschermt u 2 "slots" 1-4.

De SNMP community string is **privé**, en kan worden gewijzigd, maar niet ondersteund in uBR10K.

Bitmaps instellen

Het volgende belangrijke om in te stellen is de switch-groepen, die hexadecimale bitmaps nodig hebben. De RF Switch bitmap is een totaal van 32 bits (8 hexadecimale tekens) in lengte, en wordt berekend zoals hieronder weergegeven. Er is een Excel-rekenmachine beschikbaar voor gebruik.

Neem groep 1, die vier Amerikaanse kabels heeft die links van een RF-Switch kop zijn aangesloten in sleuf 1, en 1 DS is aangesloten op de linkerkant van dezelfde header. De gebruikte poorten waren ABCDF. Voor elke poort die bij het overschakelen betrokken is, wordt het corresponderende bit ingesteld op 1. Als een poort niet bij het overschakelen betrokken is, wordt dat poortbit ingesteld op 0.

Groep 1 wordt hierna weergegeven.

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
= **A A 2 0 0 0 0 0** (in hexadecimal).

Opmerking: de bits 14 tot 32 geven "geen zorg" (X).

Voor groep 2 is de rechterkant van de header aangesloten en hieronder wordt de bitmap weergegeven.

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
= **5 5 1 0 0 0 0 0** (hex)

Er moeten switches-groepen worden ingesteld, anders begrijpt de switch niet welke havens en informatiecentra moeten worden ingericht. Wanneer u bitmaps maakt, kan het nummer worden ingevoerd als decimaal formaat, of moet het met 0x in de voorkant van de hexadecimale code worden ingevoerd om te erkennen dat het hex is. Geef de opdracht **set groep Group2 0x5100000 uit** om de bitmap toe te wijzen. Group2 is een alfanumerieke woordstring die moet beginnen met een letter.

Tip: de twee hierboven genoemde bitmaps maken deel uit van het aanbevolen referentieontwerp. De 4+1-modus is geheel anders en aanbevolen wordt om de bitmap calculator te gebruiken. Bij een 4+1-beveiligingssysteem hebt u vier HCCP-groepen. HCCP-groepen 1 en 2 in de beveiliging 2 kaarten en HCCP-groepen 3 en 4 in de beveiliging 1 kaart. Bescherm 1 heeft ook betrekking op slots 5-8 op de switch, maar in de uBR-configuratie worden deze slots aangeduid als slots 1-4.

Als u individuele poorten in plaats van MAC-domeinen verandert, moet u weten welke bescherming u biedt en gebruikt u de onderstaande tabel om te weten welk groepsnummer u wilt gebruiken. Stel dat de switch in de 4+1-modus staat. De opdracht wordt hierna weergegeven voor de uBR10K.

```
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
```

Dit geeft het IP-adres van de switch en module 26 aan, dat aangeeft dat kaart 2 een back-up van poort G in een 4+1-schema biedt, en module 10, die de beveiliging aangeeft van kaart 2 een back-up van poort C. Dit staat allemaal in sleuf 1 van de switch.

In de onderstaande tabel worden beide modi weergegeven en het nummer van de haven.

8+1-modus	4+1-modus
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)
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)

Configuratie instelsleuf

De nieuwe firmware stelt het chassis in voor elke mix van upstream-/downstreamkaarten. Dit wordt bereikt door gebruik te maken van de nieuwe CLI opdracht **set sleuf *USslots DS*.**

De ***US-slots*** en *DSslots-parameters zijn 16-bits hex integer-bit-bit-maskers die weergeven of de module is ingeschakeld/geconfigureerd voor dat type kaart, waarbij de meest rechtse bit module 1 vertegenwoordigt. Raadpleeg de nieuwe bitmap rekenmachine voor geautomatiseerde configuraties.*

Bijvoorbeeld, als u een chassis met vier lijnkaarten, upstream kaarten in modules 1-2, en downstream kaarten in modules 3-4 wilt instellen, zou u de **vastgestelde sleuf configuratie 0x003 0X000c** opdracht uitgeven.

De configuratie van de sleuf wordt opgeslagen op nvm, los van de applicatie firmware. Dit staat toekomstige upgrades aan de toepassingsfirmware toe zonder dat de gebruiker de configuratie van de sleuf hoeft te herprogrammeren en één toepassingscodedistributie mogelijk maakt voor alle RF-Switches configuraties.

Normaal gesproken zou de fabriek deze configuratie uitvoeren als de unit is gebouwd, maar dit zou u in staat stellen om de instelling in het veld desgewenst te wijzigen en elk aantal/elke mix kaarten te gebruiken die u in de toekomst nodig hebt.

Hieronder vindt u een voorbeeldconfiguratie.

```
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
```

RF-Switch relay testen

Cisco raadt aan de informatiecentra eens per week en ten minste eens per maand te testen. Console of telnet in de switch en geeft de opdracht **testmodule** uit. Als er een wachtwoord is ingesteld in de RF-Switch, geeft u de opdracht *Wachtwoord* en *Wachtwoord* ***in om de testopdracht te gebruiken.*** Hierdoor worden alle informatiecentra tegelijkertijd getest en gaan ze terug naar de normale werkmodus. Gebruik deze testopdracht niet in de beveiligingsmodus. **Gebruik deze testopdracht niet in de beveiligingsmodus.**

Tip: U kunt de relais op de switch draaien zonder dat dit de converter of een van de modems beïnvloedt. Dit is belangrijk als het testen van de informatiecentra zonder dat er daadwerkelijk een van de lijnkaarten of corresponderende upconverters is veranderd. Als een relais op de switch wordt geactiveerd en een failover gebeurt, zal het naar de juiste staat gaan en niet slechts van de ene staat naar de andere overschakelen.

Geef de opdrachtregel **switch 13 1** uit om poort G te testen op sleuf 1 van de Switch. U kunt een volledige bitmap testen door de *naam van de* ***switch*** uit te geven **1** opdracht. Geef de *opdracht* ***switch*** *groepsnaam* ***0*** (of **los**) uit om de relais voor de normale werkmodus uit te schakelen.

Daarnaast dient de klant een CLI-failover-test van een HCCP-groep uit te voeren (**hccp** ***g*** **switch** ***m*** **opdracht** geven) van de CMTS om de beveiligingskaart te testen en pad te beschermen. Dit type failover kan 4-6 seconden in beslag nemen en kan een klein percentage modems veroorzaken om offline te gaan. Daarom moet deze test minder vaak en alleen tijdens de uren buiten de piek worden uitgevoerd. Bovenstaande tests zullen de algemene beschikbaarheid van het systeem verbeteren.

Besturing van de RF-Switch

Volg de onderstaande stappen.

1. Laad de nieuwe afbeeldingen in de uBR met een Flash-schijf in sleuf 0.
2. Configureer de onderstaande opdrachten in de uBR.

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

3. console in de switch en geeft de **set tftp-host {ip-addr}** opdracht uit. Gebruik het IP-adres van uBR voor TFTP-overdrachten.
4. Geef het **exemplaar tftp:rfsw330-bf-1935022g af.** Opdracht om de flitser te laden en **kopie te ftp:rfsw330-fl-1935030h fl:** om de Flash te laden.
5. Herstart of opnieuw laden zodat de nieuwe code kan worden uitgevoerd. Typ **PASS-SYSTEEM** en **Save Config** om de nieuwe NVIM-velden te uploaden. Herstart het programma zodat dit allemaal van kracht wordt.

Waarschuwing: het kan nodig zijn om een deel van de configuratie opnieuw in te stellen nadat u het opnieuw hebt geladen, zoals het IP-adres van de switch. Bekijk de configuratie van uw switch na het opnieuw laden om het te controleren. Zodra u bent bijgewerkt naar versie 3.5 kan er een standaard gateway-adres worden toegevoegd aan de switch en kunnen er nieuwe upgrades aan

de switch worden uitgevoerd via subnetten die u extern kunt gebruiken. De enige limiet is indien het laden van Unix stations de nieuwe beeldnaam kleine letters is. Dit nieuwe beeld voegt ook een DHCP-clientoptie en een configuratie-instelling voor chassis/modules toe.

DHCP-werking

Deze release omvat volledige ondersteuning voor een DHCP-client. DHCP-handeling wordt standaard ingeschakeld, tenzij de gebruiker een statische IP vanuit de CLI heeft ingesteld. Er zijn opdrachten toegevoegd of uitgebreid om de DHCP-werking te ondersteunen.

Wanneer de RF Switch start, controleert het of DHCP is ingeschakeld. Dit gebeurt op verschillende manieren via de CLI. U kunt een van de volgende opdrachten gebruiken om DHCP in te schakelen:

```
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.
```

De RF-Switch gaat niet langer uit van een statische IP van 10.0.0.1, zoals in versies vóór 3.0.

Als deze optie ingeschakeld is, installeert de RF-Switch de DHCP-client en probeert u een DHCP-server te vinden om een lease-overeenkomst aan te vragen. Standaard vraagt de client een leasetijd van 0xffffffff (oneindige lease), maar deze kan worden gewijzigd door de **set dhcp lease** ***leasetime_secs*** **opdracht** uit te geven. Aangezien de eigenlijke leasetijd van de server is toegekend, wordt deze opdracht in de eerste plaats gebruikt voor debug/testen en is deze opdracht niet nodig voor normaal gebruik.

Als een server zich bevindt, vraagt de client om instellingen voor IP adres en subnetmasker, een toegangs adres en de locatie van een TFTP-server. Het adres van de gateway is afkomstig van optie 3 (routeroptie). Het TFTP-serveradres kan op verschillende manieren worden gespecificeerd. De client controleert de next-server optie (siaddr), optie 66 (TFTP-servernaam) en optie 150 (TFTP-serveradres). Als alle drie de bovenstaande punten niet aanwezig zijn, wordt het TFTP-serveradres standaard ingesteld op het DHCP-serveradres. Als de server een huur verleent, registreert de DHCP-client de aangeboden leasetijd voor vernieuwing en gaat deze door met het laarsproces, het installeren van de andere netwerktoepassingen (telnet en SNMP) en de CLI.

Als een server niet binnen 20-30 seconden geplaatst is, wordt de DHCP-client geschorst en de CLI loopt. De DHCP-client wordt op de achtergrond uitgevoerd in een poging om elke vijf seconden contact op een server op te nemen totdat een server zich bevindt, er wordt een statische IP toegewezen via de CLI of het systeem wordt herstart.

Met CLI kan de gebruiker een van de netwerkinstellingen omzeilen die via de server ontvangen kunnen worden, en statische waarden voor deze instellingen toewijzen. Alle **ingestelde xxx** opdrachtparameters worden opgeslagen in nvm en gebruikt bij herstart. Aangezien de huidige netwerkinstellingen nu van DHCP of de CLI kunnen komen, zijn er een aantal wijzigingen/nieuwe opdrachten geïmplementeerd. Het bestaande bevel **show** software is veranderd om de instellingen van alle nvm parameters te tonen, die niet noodzakelijk de op het ogenblik van kracht zijn.

Om de huidige in gebruik zijnde netwerkparameters te verkrijgen, **toont** de nieuwe opdracht **ip** is toegevoegd. Naast de netwerkinstellingen toont deze opdracht ook de huidige IP-modus (statisch

versus DHCP), de status van de DHCP-client en de status van de telnet- en SNMP-toepassingen (die alleen gestart worden als een geldige IP bestaat).

Er is een aanvullende opdracht toegevoegd, **die** het **dhcp laat zien**. Deze opdracht toont de waarden die van de DHCP-server zijn ontvangen, evenals de status van de leasetijd. De weergegeven tijdwaarden zijn in het formaat HH:MM:SS weergegeven en zijn relatief ten opzichte van de huidige systeemtijd, die ook wordt weergegeven.

Toewijzing van statische waarden voor een van de configureerbare netwerkparameters moet onmiddellijk van kracht worden en zonder verdere actie de huidige instelling omzeilen. Hierdoor kunnen sommige parameters dynamisch blijven, terwijl andere worden gerepareerd. DHCP kan bijvoorbeeld worden gebruikt om het IP-adres te verkrijgen, terwijl de instelling voor de TFTP-server via de CLI behouden blijft. De enige uitzondering hierop is wanneer je van een statische IP naar DHCP gaat. Aangezien de DHCP-client alleen bij de start-up is geïnstalleerd zoals vereist, moet de overdracht van een statische IP naar DHCP worden herstart zodat DHCP van kracht wordt.

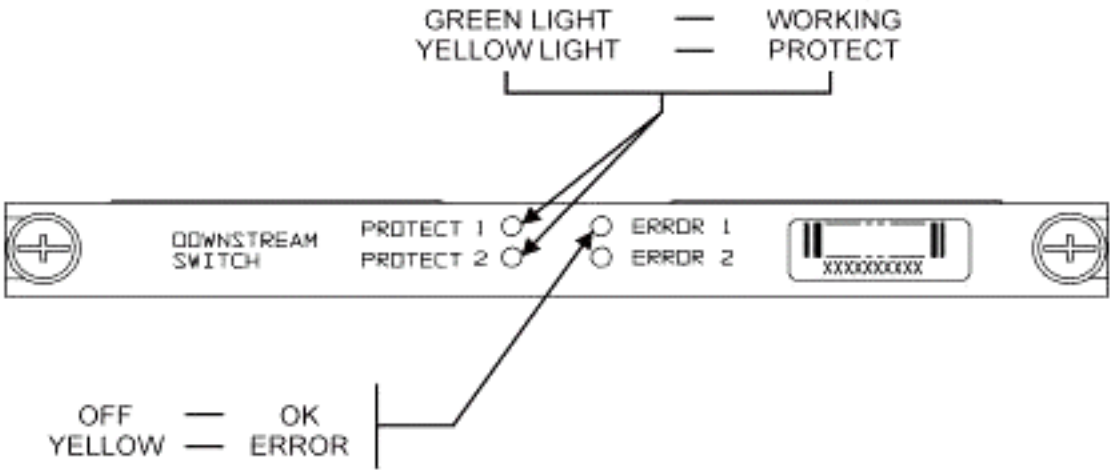
LEDs

De corresponderende module LEDs worden van groen naar amber/geel. De lay-out is tegenovergesteld van de rug, wat betekent dat als de switch-groep links van de header in sleuf 1 van de switch in sleuf 1 in een 8+1-modus uitvalt, de beveiliging van 1 LEDs rechts van groen naar amber gaat om de relais te tonen.

Het beeld hieronder toont de kleurverschillen op LEDs en geeft geen specifieke failover weer.

- LED #1 Groen/Geel om aan te geven dat je werkt/beschermt 1
- LED #2 Groen/Geel om aan te geven dat je werkt/beschermt 2
- LED #3 Off/Yellow om een probleem op kanaal 1 aan te geven
- LED #4 Off/Yellow om een probleem op kanaal 2 aan te geven

Het moduldiagram wordt hierna weergegeven.



Het onderstaande beeld toont de Ethernet-controller-indicatielampjes.

-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

Problemen en toepassingen voor klanten

Sommige punten die als problemen kunnen worden beschouwd zijn de kosten, het gebruik van alle componenten, het inbrengen, het fysieke indeling, kleine connectors en kabel, en de beschikbaarheid en ondersteuning van deze componenten.

Het inbrengen van een verlies van 6 dB in de werkmodus zou een probleem kunnen zijn. Er is ook meer inzetverlies (ongeveer 1-2 dB) wanneer de switch in de beveiligingsmodus komt. Dit hangt af van de frequentie die u voor DS gebruikt. In de VS is het inplantingsverlies ongeveer 4,5 dB.

De aanvaarding door de industrie kan enige tijd in beslag nemen voor de kleinere MCX-connectors en de kleinere coaxiale kabel die voor de oplossing wordt gebruikt. AOL Time Warner besloot om 10.000 meter van deze kabelstijl te kopen om een deel van de Amerikaanse bekabeling via hun hoofd te bedraden. Het Handvest maakt nu ook gebruik van deze bekabeling. Als ze de kabel gaan gebruiken, is het net een kwestie van tijd voordat ze en andere fabrikanten ook de nieuwe kleinere connector gaan gebruiken. De nieuwe upconverter van VC gebruikt nu MCX-connectors.

WhiteSands Engineering produceert de kabelsets voor Cisco. Cisco moet een minimum stijl kabelsets opslaan om aan ons aanbevolen ontwerp te voldoen. Je kunt rechtstreeks naar WhiteSands gaan voor speciale kabelorders. U kunt de benodigde gereedschappen voor connectorisatie verkrijgen via CablePrep of WhiteSands.

Het nummer van het RF-onderdeel van de Switch is hoofdlettergevoelig. U moet **uBR-RFSW** invoeren om de switch te bestellen.

Operationele kwesties

Neem de situaties die hieronder worden beschreven.

Een lijnkaart van 5 x 20 is slecht en de lijnkaart neemt het over. U koppelt de defecte lijnkaart los, en het DS-signaal van de beschermlijnrugvoer naar het eind van de losaangesloten kabel die aan de andere lijnkaart werd bevestigd en nu niet beëindigd is.

Dit zal een impedantie mismatch veroorzaken, en reflecterende energie die ongeveer 7 dB lager zal zijn dan het oorspronkelijke signaal. Dit komt doordat de splitter in het chassis van de switch slechts ongeveer 7 dB geïsoleerd zal hebben wanneer de gemeenschappelijke poort niet wordt afgesloten. De aangetaste frequenties zijn gerelateerd aan de fysieke lengte van de losgekoppelde kabel.

Dit idee zal helpen om het potentiële gevaar van het DS-niveau te verminderen door tot 3 dB te veranderen:

- Beëindiging van de DS-kabels met 75 ohm terminatoren. Mogelijk zijn er speciale MCX-terminators nodig.

In een andere situatie, creëert RF Switch Telnet toegang van de uBR10K console dubbele ingangen wanneer het typen. Een werk rond is om lokale echo uit te schakelen. Bijvoorbeeld, van het CLI **geeft telnet *ip adres*/noecho uit**. U moet op **controle pauze** drukken om uit te komen, of **controle** voor de bevelmodus van het telnet, en **stop** of **verstuur pauze**. Een andere manier om de verbinding te verwijderen is door op **Control+Shift+6+x** te drukken en **schijf 1** van de uBR-opdrachtregel te typen. Raadpleeg voor sommige standaardbreuksequenties de standaarddoorbraaksleutelcombinaties tijdens wachtwoordherstel.

Obscure-toepassingen

Neem de onderstaande situatie.

De beveiligingskabels op uBR kunnen worden gebruikt om de signaalsterkte te testen voor het corresponderende werk. Ga er bijvoorbeeld vanuit dat u de switch in 8+1-modus hebt, een werkblad in sleuf 8/0 van de uBR, een beveiligingsmes in sleuf 8/1 en de werkdraad tot sleuf 1 van de switch. Om het Amerikaanse elektriciteitsniveau op US0 kaart 8/0 te testen, telnet of console in de switch en geeft u de opdracht **switch 1 1** uit. Dit activeert het relais vanaf sleuf 1 van de switch voor module 1, dat ook bekend staat als haven A van de switch. Koppel de kabel op US0 van het beschermde blad los en bevestig aan een spectrumanalyzer. U zult het Amerikaanse signaal kunnen testen dat in feite naar de werkende Amerikaanse0 gaat.

Opdrachten weergeven

Gebruik de onderstaande opdrachten om een oplossing te vinden.

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
```

volledige module tonen

```
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
```

toonconfiguratie

```
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-specificaties

In de onderstaande lijst worden de specificaties voor de RF-Switch weergegeven.

- Invoervoeding AC — 100 tot 240 Vac, 50/60 Hz, exploitatiebereik — 90-254 Vac
- DC-voeding — Drie terminal Blok -48/60 Vdc, bereik — 40,5 tot -72 Vdc, 200 mVpp rimpel/ruis
- Temperatuurbereik — 0 tot +40° C, temperatuurbereik — 5 tot +55° C
- Unity Control 10BaseT SNMP Ethernet en RS-232 Bus — 9-pins mannelijk D
- RF-connectors — MCX, impedantie — 75 ohm
- Max RF-ingangsvoeding — +15 dBm (63,75 dBmV)
- Type switch — Elektrotechnische apparatuur, absorberend voor werkpad, niet-absorberend op beschermingspad
- DS-frequentiebereik — 54 tot 860 MHz
- Max DS insertion Loss: 5,5 dB van werken naar uitvoer, 8,0 dB van beveiliging naar uitvoer
- DS insertieverlies Flatness - +1.1 dB van werken naar uitvoer, +2.1 dB van bescherming naar uitvoer
- DS-uitgang — meer dan 15,5 dB
- DS-isolatie: meer dan 60 dB aan het werk, meer dan 20 dB aan de respectievelijke bescherming onttrokken in de beveiligingsmodus, en meer dan 60 dB aan de bescherming onttrokken in de werkmodus
- Upstream frequentiebereik — 5 tot 70 MHz
- Maximaal upstreamingverlies — 4,1 dB van input naar werk, 5,2 dB van invoer ter bescherming van
- US insertion Loss Flatness — + 0,4 dB van input naar werk, + 0,6 dB van input ter bescherming van
- VS Input Return Loss — groter dan 16 dB
- US-isolatie: meer dan 60 dB aan het werk, groter dan 20 dB aan de respectievelijke bescherming in de beveiligingsmodus, en groter dan 60 dB aan de bescherming tijdens de werkmodus
- Fysieke formulierfactor — 19 x 15,5 x 5,25 (482 x 394 x 133 mm), Gewicht — 36 lbs

Gerelateerde informatie

- Cisco RF-Switches
- N+1 Tips en configuratie voor uBR 10K met MC28C-kaarten
- Technische ondersteuning - Cisco-systemen