CISCO

Ghid de configurare a software-ului routerului Cisco Catalyst IR1800 Rugged Series

Prima publicație:2020-08-13

Ultima modificare:23-12-2024

Sediu

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
SUA http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CUPRINS

CAPITOL 1

Prezentare generală

Această secțiune conține următoarele:

Introducere

Routerul Cisco Catalyst IR1800 Rugged Series este un router industrial modular. Seria IR1800 are patru platforme de bază cu module suplimentare conectabile care pot fi adăugate. Modulele conectabile oferă flexibilitatea de a adăuga diferite interfețe la platforma de bază.

Seria IR1800 ISR dispune de o platformă de bază cu modularitate care include:

- Modul de interfață conectabil (PIM)
- Modul mSATA (SSDM)
- Modul GPS (GNSS)
- Modul de interfață Wi-Fi (WIM)

Seria IR1800 constă din patru platforme de bază. Sunt:

- IR1821 - Lite
- IR1831 - Baza B
- IR1833 - Baza M
- IR1835 - Pro

Următorul tabel prezintă detalii despre diferențe:

Caracteristici	IR1821	IR1831	IR1833	IR1835
Procesor	600 MHz	600 MHz	600 MHz	1200MHz
Memorie	4GB	4GB	4GB	8 GB

Caracteristici	IR1821	IR1831	IR1833	IR1835
Sloturi PIM	1	2	2	2
Conectare WiFi Slot pentru modul	Da	Da	Da	Da
PoE	Nu	Nu	Da	Da
mSATA conectabil Modul	Nu	Nu	Da	Da
Conectabil GNSS Modul	Nu	Nu	Da	Da
GPIO	Nu	Nu	Nu	Da
Aprindere management	Da	Da	Da	Da
Autobuz CAN	Da	Da	Da	Da
Interfață serială	RS232 (1)	RS232 (2)	RS232 (2)	RS232 (1) RS232/RS485 (1)
Securitate avansată	Nu	Nu	Nu	Da,Umbrela Cisco Integrare

Nota Setul de documentație pentru acest produs se străduiește să utilizeze un limbaj fără părtinire. În sensul acestui set de documentație, lipsa de părtinire este definită ca limbaj care nu implică discriminare bazată pe vârstă, dizabilitate, sex, identitate rasială, identitate etnică, orientare sexuală, statut socioeconomic și intersecționalitate. În documentație pot fi prezente excepții din cauza limbii care este codificată în interfețele de utilizator ale software-ului produsului, a limbii utilizate pe baza documentației RFP sau a limbii care este utilizată de un produs terță parte la care se face referire.

Accesarea CLI folosind o consolă de router

Routerele Cisco IR1800 au un port de consolă cu doar suport USB.

Portul consolei este un conector USB micro-B care se află pe panoul frontal al șasiului. Rata de transmisie implicită este 9600.

Dacă laptopul sau PC-ul vă avertizează că nu aveți driverele adecvate pentru a comunica cu routerul, le puteți obține de la producătorul computerului sau accesați aici:

https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers

http://www.ftdichip.com/Support/Documents/InstallGuides/Mac_OS_X_Installation_Guide.pdf

Nota Cele mai recente drivere VCP nu funcționează cu MAC OS 10.14.x și mai departe. Dacă aveți nevoie de suport OS X 10.4, vă rugăm să instalați versiunea 3.1 a driverului VCP.

Pe un dispozitiv proaspăt venit din fabrică, sunteți întâmpinat cu un Dialog de configurare a sistemului unde răspundeți la întrebările de bază de configurare. Dacă routerul a fost comandat pentru utilizarea serviciilor Cisco PnP connect, în cazul furnizării centralizate, routerul omite dialogul inițial. Următorul este un exemplu:

- - - Dialog de configurare a sistemului ---

Doriți să intrați în dialogul de configurare inițială? [da/nu]:**Da**

În orice moment, puteți introduce un semn de întrebare „?" pentru ajutor.
Utilizați ctrl-c pentru a anula dialogul de configurare la orice solicitare.
Setările implicite sunt între paranteze drepte „[]".

Configurarea de bază de gestionare configurează doar suficientă conectivitate pentru gestionarea sistemului, configurarea extinsă vă va cere să configurați fiecare interfață a sistemului

Doriți să intrați în configurația de gestionare de bază? [da/nu]: da Configurarea parametrilor globali:

Introduceți numele gazdei [Router]:**<numele-gazdă>**

Secretul de activare este o parolă folosită pentru a proteja accesul la modurile EXEC și de configurare privilegiate. Această parolă, după ce este introdusă, devine criptată în configurație.
Introduceți secretul de activare:**<parola-voastra>**

Parola de activare este utilizată atunci când nu specificați o parolă secretă de activare, cu unele versiuni de software mai vechi și unele imagini de pornire.

Introduceți parola de activare:**<parola-voastra>**

Parola terminalului virtual este utilizată pentru a proteja accesul la router printr-o interfață de rețea. Introduceți parola terminalului virtual:**<parola-voastra>** Configurați contul pentru accesarea serverului HTTP? [Da]:**<întoarcere>**

Nume de utilizator [administrator]:**<numele de utilizator>** [cisco]:**<parola-voastra>**
Parolă
Parola este NESCRIPTATA.
Configurați managementul rețelei SNMP? [nu]:**<întoarcere>**

Rezumatul interfeței curente

Vreo interfață listată cu OK? valoarea „NU" nu are o configurație validă

Interfață	Adresa IP	BINE?	Starea	metodei	Protocol
GigabitEthernet0/0/0	nealocate	NU	dezactivat	Sus	Sus
GigabitEthernet0/1/0	nealocate	DA	dezactivat	jos	jos
GigabitEthernet0/1/1	nealocate	DA	dezactivat	jos	jos
GigabitEthernet0/1/2	nealocate	DA	dezactivat	jos	jos
GigabitEthernet0/1/3	nealocate	DA	dezactivat	Sus	Sus
Async0/2/0	nealocate	DA	dezactivat	Sus	jos
Vlan1	nealocate	DA	dezactivat	Sus	Sus

Nota Numele și adresele IP în această secțiune următoare sunt prezentate ca exemple.

Introduceți numele interfeței folosit pentru a vă conecta la rețeaua de management din rezumatul interfeței de mai sus:**vlan1**

Configurarea interfeței Vlan1:
Configurați IP-ul pe această interfață? [nu]:**Da**
Adresă IP pentru această interfață:**192.168.1.1**
Masca de subrețea pentru această interfață [255.255.255.0] :**<întoarcere>**
Rețeaua de clasă C este 192.168.1.0, 24 de biți de subrețea; masca este /24

Doriți să configurați DHCP? [da/nu]:**Da** Introduceți numele pool-ului DHCP:**wDHCPool** Introduceți rețeaua DHCP:**192.168.1.0** Introduceți masca de rețea DHCP:**255.255.255.0** Introduceți routerul implicit:**192.168.1.1**

A fost creat următorul script de comandă de configurare:

numele gazdă <numele-gazdă>
activați secretul 9 9Z6fl74fvoEdMgU$XZYs8l4phbqpXsb48l9bzCng3u4Bc2kh1STsoLoHNes activați
parola <vou-activați-parola>
linia vty 0 4
parola <parola-voastra>
username <your-username> privilegiu 15 parola <your-parola> nu snmp-server

!
!
închiderea interfeței
GigabitEthernet0/0/0
fara adresa ip
!
interfață GigabitEthernet0/1/0 !

interfață GigabitEthernet0/1/1 !

interfață GigabitEthernet0/1/2 !

interfață GigabitEthernet0/1/3 !

interfața Vlan1
nicio oprire
adresa ip 192.168.1.1 255.255.255.0 fără mop
activat
ip dhcp pool wDHCPool rețea 192.168.1.0
255.255.255.0 implicit-router 192.168.1.1

!
Sfârşit

[0] Accesați linia de comandă IOS fără a salva această configurație. [1] Reveniți la setare fără a salva această configurație.
[2] Salvați această configurație în nvram și ieșiți.

Introdu selecția ta [2]:**2** Configurația clădirii...

[BINE]

Utilizați comanda „configure” în modul activat pentru a modifica această configurație.

Apăsați RETURN pentru a începe!**<întoarcere>**

* 27 iulie 21:35:24.369: %CRYPTO_ENGINE-5-KEY_ADDITION: O cheie numită TP-self-signed-3211716068 a fost generată sau importată de cripto-motor
* 27 iulie 21:35:24.372: %SSH-5-ENABLED: SSH 1.99 a fost activat
* 27 iulie 21:35:24.448: %PKI-4-NOCONFIGAUTOSAVE: Configurația a fost modificată. Emiteți „memorie de scriere” pentru a salva noua configurație IOS PKI
* 27 iulie 21:35:24.532: %CRYPTO_ENGINE-5-KEY_ADDITION: O cheie numită TP-self-signed-3211716068.server a fost generată sau importată de numele de gazdă a motorului cripto>

Dispozitivul are acum o configurație de bază pe care o puteți construi.

Utilizarea interfeței consolă

Procedură

Pasul 1 Introduceți următoarea comandă:

Router > activare

Pasul 2 (Mergeți la Pasul 3 dacă parola de activare nu a fost configurată.) La solicitarea parolei, introduceți parola sistemului:

Parola: enablepass

Când parola este acceptată, se afișează promptul pentru modul EXEC privilegiat.

Router#

Acum aveți acces la CLI în modul EXEC privilegiat și puteți introduce comenzile necesare pentru a finaliza sarcinile dorite.

Pasul 3 Pentru a ieși din sesiunea consolei, introduceți**renunta**comanda:

Router#**renunta**

Securitate inițială la pornire

Această secțiune conține următoarele:

Aplicați modificarea parolei implicite

Când dispozitivul este pornit pentru prima dată după resetarea din fabrică sau proaspăt din fabrică, pe consolă se primește următoarea solicitare:

Doriți să intrați în dialogul de configurare inițială? [da/nu]:

În documentația anterioară, Cisco a recomandat utilizarea**activați secret**comanda în loc de**activați parola** comanda deoarece aceasta oferă un algoritm de criptare îmbunătățit.

Dialogul inițial forțează setarea unei noi parole de activare și, de asemenea, utilizarea**activați secret**comanda în schimb. Următorul este un exemplu:

```
Doriți să intrați în configurația de gestionare de bază? [da/nu]:Da Configurarea
parametrilor globali:

    Introduceți numele gazdei [Router]:router-1

    Secretul de activare este o parolă folosită pentru a proteja accesul la modurile EXEC
    și de configurare privilegiate. Această parolă, după ce este introdusă, devine
    criptată în configurație.
    Introduceți secretul de activare:********
    Confirmați secretul de activare: *******

    Parola de activare este utilizată atunci când nu specificați o parolă secretă de
    activare, cu unele versiuni de software mai vechi și unele imagini de pornire.

    Introduceți parola de activare:*********

Parola terminalului virtual este folosită pentru a proteja
    acces la router printr-o interfață de rețea. Introduceți parola
    terminalului virtual:********* Configurați managementul
    rețelei SNMP? [Da]:nu

Introduceți numele interfeței folosit pentru a vă conecta la
rețeaua de management din rezumatul interfeței de mai sus:Ethernet0/0

Configurarea interfeței Ethernet0/0:
    Configurați IP-ul pe această interfață? [Da]:nu

A fost creat următorul script de comandă de configurare: hostname
router-1
activați secretul 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg activați
parola parola-1
.
.
[0] Accesați linia de comandă IOS fără a salva această configurație. [1] Reveniți la
setare fără a salva această configurație.
[2] Salvați această configurație în nvram și ieșiți.

Introdu selecția ta [2]:2
.
.
router-1>ro
Parolă:
router-1#sh alerga | sec activare
activați secretul 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg activați
parola parola-1
```

Următorul este un exemplu de ceea ce se întâmplă dacă răspundeți**nu**la dialogul de configurare inițială:

```
Doriți să intrați în dialogul de configurare inițială? [da/nu]:nu Secretul de activare este o parolă
folosită pentru a proteja accesul la
    EXEC privilegiat și moduri de configurare. Această parolă, după ce este introdusă,
    devine criptată în configurație.
    Introduceți secretul de activare:********
    Confirmați activarea secretului:********
Doriți să opriți instalarea automată? [Da]:Da
```

.
.
router-1>**ro**
Parolă:
router-1#**sh alerga | sec activare**
activați secretul 9 9emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg

După ce secretul de activare este solicitat la prima conectare, iar administratorul introduce o parolă, parola introdusă de administrator va fi întotdeauna mascată. Dacă administratorul introduce o parolă slabă, i se va cere din nou să introducă o parolă puternică (adică amestecul standard de caractere majuscule/minuscule, caractere speciale, numere etc.). Solicitarea va continua până când administratorul introduce o parolă puternică. Administratorului i se va cere să introducă de două ori parola secretă puternică pentru a confirma că administratorul este sigur că este secretul pe care dorește să îl configureze.

Telnet și HTTP

A existat o schimbare în configurația de boot telnet și http începând cu versiunea 17.3.1. Când dispozitivul este pornit pentru prima dată după resetarea din fabrică sau proaspăt din fabrică, au loc următoarele:

- Dezactivați telnet
- Dezactivați serverul HTTP. Clientul HTTP funcționează.
- Activați SSH
- Activați serverul HTTPS

Accesarea CLI dintr-o consolă la distanță

Consola la distanță a IR1800 poate fi accesată prin Telnet sau SSH. Telnet este dezactivat în mod implicit și ar trebui utilizat SSH-ul mai sigur. Pentru detalii despre accesul SSH vezi capitolul SSH.

Următoarele subiecte descriu procedura de accesare a CLI de pe o consolă la distanță:

Se pregătește conectarea la consola routerului

Consultați ghidul de întărire Cisco IOS-XEDevice lahttps://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.htmlpentru detalii.

Configurarea bannerelor de diagnosticare și așteptare este opțională, dar recomandată. Bannerele sunt utile în special ca indicatori pentru utilizatori despre starea încercărilor lor Telnet sau SSH.

Pentru a accesa routerul de la distanță utilizând Telnet dintr-o rețea TCP/IP, configurați routerul să accepte linii terminale virtuale folosind**linia vty**comanda de configurare globală. Configurați liniile terminale virtuale pentru a solicita utilizatorilor să se conecteze și să specifice o parolă.

VeziReferință de comandă Cisco IOS Terminal Servicesdocument pentru mai multe informații despre linie**vty global** comanda de configurare.

Pentru a preveni dezactivarea autentificării pe o linie, specificați o parolă cu**parolă**comanda atunci când configurați**log in**comanda.

Dacă utilizați autentificare, autorizare și contabilitate (AAA), configurați**autentificare de conectare** comanda. Pentru a preveni dezactivarea conectării pe o linie pentru autentificarea AAA atunci când configurați o listă cu

comanda de autentificare login, trebuie să configurați și acea listă folosind**aaa autentificare autentificare**comanda de configurare globală.

Pentru mai multe informații despre serviciile AAA, consultațiGhid de configurare a securității Cisco IOS XE: Conectivitate sigurăiar celReferință pentru comenzile de securitate Cisco IOSdocumente. Pentru mai multe informații despre **configurarea liniei de conectare**comanda, veziReferință de comandă Cisco IOS Terminal Servicesdocument.

În plus, înainte de a realiza o conexiune Telnet la router, trebuie să aveți un nume de gazdă valid pentru router sau să aveți o adresă IP configurată pe router. Pentru mai multe informații despre cerințele pentru conectarea la router folosind Telnet, informații despre personalizarea serviciilor Telnet și despre utilizarea secvențelor de taste Telnet, consultațiGhid de configurare a noțiunilor fundamentale de configurare Cisco IOS.

Configurarea routerului pentru a rula SSH

Urmați procedura de mai jos pentru a configura dispozitivul să ruleze SSH:

Înainte de a începe

Configurați autentificarea utilizatorului pentru acces local sau de la distanță. Acest pas este necesar. Pentru mai multe informații, consultați Subiectele conexe de mai jos.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** router>**permite**	Activează modul EXEC privilegiat. • Introduceți parola dacă vi se solicită.
Pasul 2	**configura terminalul** **Exemplu:** router#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**nume de gazdă***nume de gazdă* **Exemplu:** router(config)#**nume de gazdă***numele_gazdă*	Configurați un nume de gazdă și un nume de domeniu IP pentru dispozitivul dvs. **Nota** Urmați această procedură numai dacă configurați dispozitivul ca server SSH.
Pasul 4	**IP nume-domeniu***nume_domeniu* **Exemplu:** router(config)#**IP nume-domeniu** *numele_domeniului_dvs*	Configurați un domeniu gazdă pentru dispozitivul dvs.

	Comanda sau Acțiune	Scop
Pasul 5	**cheie cripto genera rsa** **Exemplu:** router(config)#**cheie cripto genera rsa**	Activează serverul SSH pentru autentificare locală și de la distanță pe dispozitiv și generează o pereche de chei RSA. Generarea unei perechi de chei RSA pentru dispozitiv activează automat SSH. Vă recomandăm o dimensiune minimă a modulului de 1024 de biți. Când generați chei RSA, vi se solicită să introduceți o lungime a modulului. O lungime mai mare a modulului poate fi mai sigură, dar este nevoie de mai mult timp pentru a genera și a utiliza. **Nota** Urmați această procedură numai dacă configurați dispozitivul ca server SSH.
Pasul 6	**Sfârşit** **Exemplu:** router(config)#**Sfârşit**	Revine la modul EXEC privilegiat.
Pasul 7	**arată rularea-config** **Exemplu:** router#**arată rularea-config**	Vă verifică intrările.
Pasul 8	**copiați running-config startup-config** **Exemplu:** router#**copiați running-config startup-config**	(Opțional) Salvează intrările dvs. în fișierul de configurare.

Utilizarea Telnet pentru a accesa o interfață de consolă

Înainte de a începe

Telnet este considerat un risc de securitate și este dezactivat în mod implicit. Dacă trebuie să-l activați, vedețiConfigurarea Telnet

Procedură

Pasul 1 De pe terminal sau PC, introduceți una dintre următoarele comenzi:

- **conectați gazda***[port] [cuvânt cheie]*
- **gazdă telnet***[port] [cuvânt cheie]*

Aici,*gazdă*este numele de gazdă a routerului sau adresa IP,*port*este un număr de port zecimal (23 este valoarea implicită) și*cuvânt cheie* este un cuvânt cheie acceptat. Pentru mai multe informații despre aceste comenzi, consultațiReferință de comandă Cisco IOS Terminal Servicesdocument.

Următorul exemplu arată cum se utilizează**telnet**comandă pentru a vă conecta la un router numit**router**:

```
unix_host%router telnet
Încercând 172.20.52.40...
Conectat la 172.20.52.40. Caracterul
de evacuare este „^]”. unix_host%
connect
```

Pasul 2 Introduceți parola de conectare:

```
Parola de verificare a accesului
utilizatorului: parola mea
```

Nota
Dacă nu a fost configurată nicio parolă, apăsați**Reveni**.

Pasul 3 Din modul EXEC utilizator, introduceți**permite**comanda:

```
Router>permite
```

Pasul 4 La solicitarea parolei, introduceți parola sistemului:

```
Parolă:enablepass
```

Pasul 5 Când**permite**parola este acceptată, se afișează promptul pentru modul EXEC privilegiat:

```
Router#
```

Pasul 6 Acum aveți acces la CLI în modul EXEC privilegiat și puteți introduce comenzile necesare pentru a finaliza sarcinile dorite.

Pasul 7 Pentru a ieși din sesiunea Telnet, utilizați**Ieșire**sau**deconectare**comanda.

```
Router#deconectare
```

Managementul sesiunii CLI

Un timeout de inactivitate este configurabil și poate fi impus. Blocarea sesiunii oferă protecție împotriva suprascrierii a doi utilizatori a modificărilor pe care le-a făcut celălalt. Pentru a preveni ca un proces intern să utilizeze toată capacitatea disponibilă, o anumită capacitate de rezervă este rezervată pentru accesul la sesiunea CLI. De exemplu, acest lucru permite unui utilizator să acceseze de la distanță un router.

Informații despre gestionarea sesiunii CLI

Un timeout de inactivitate este configurabil și poate fi impus. Blocarea sesiunii oferă protecție împotriva suprascrierii modificărilor efectuate de doi utilizatori. Pentru a preveni ca un proces intern să utilizeze toată capacitatea disponibilă, o anumită capacitate de rezervă este rezervată pentru accesul la sesiunea CLI. De exemplu, acest lucru permite unui utilizator să acceseze de la distanță routerul.

Modificarea timpului de expirare a sesiunii CLI

Procedură

Pasul 1 **configura terminalul**

Intră în modul de configurare globală

Pasul 2 **consola de linie 0**

Pasul 3 **sesiune-timeout***minute*

Valoarea de*minute*setează perioada de timp pe care CLI-ul îl așteaptă înainte de expirarea timpului. Setarea timpului de expirare a sesiunii CLI crește securitatea unei sesiuni CLI. Specificați o valoare 0 pentru*minute*pentru a dezactiva expirarea sesiunii.

Pasul 4 **Afișați consola de linie 0**
Verifică valoarea la care a fost setată expirarea sesiunii, care este afișată ca valoare pentru"Sesiune inactivă ".

Blocarea unei sesiuni CLI

Înainte de a începe

Pentru a configura o parolă temporară într-o sesiune CLI, utilizați**blocare**comandă în modul EXEC. Înainte de a putea folosi**blocare**comanda, trebuie să configurați linia folosind**încuiat**comanda. În acest exemplu, linia este configurată ca**încuiat**, iar apoi**blocare**este utilizată comanda și este atribuită o parolă temporară.

Procedură

Pasul 1 Router#**configura terminalul**

Intră în modul de configurare globală.

Pasul 2 Introduceți linia pe care doriți să puteți utiliza**blocare**comanda.

Router(config)#**consola de linie 0**

Pasul 3 Router(config)#**încuiat**

Permite blocarea liniei.

Pasul 4 Router(config)#**Ieșire**

Pasul 5 Router#**blocare**
Sistemul vă solicită o parolă, pe care trebuie să o introduceți de două ori.

Parolă:**<parola>**
Din nou:**<parola>**
Blocat

CAPITOL 2

Caracteristici noi

Caracteristici noi pentru Cisco IOS XE 17.16.1a

Noile funcții din această versiune sunt enumerate mai jos:

- Accesați datele despre accelerometru și senzorul giroscop din IRM-GNSS, la pagina 240
- Configurați modulul DR folosind Cisco Catalyst SD-WAN Manager
- Configurarea serviciului EVPN VXLAN VLAN-Aware, la pagina 167
- Monitorizarea parametrilor semnalului radio și coordonatele GPS ale telemetriei celulare folosind mesaje Syslog
- Îmbunătățirea managementului rețelei P-LTE-450 prin obiecte MIB SNMP

Caracteristici noi pentru Cisco IOS XE 17.15.1a

Noile funcții din această versiune sunt enumerate mai jos:

- MACsec acceptat de software, la pagina 295
- Alocare mai mare pentru CPU și RAM pentru aplicațiile IOx

Caracteristici noi pentru Cisco IOS XE 17.14.1a

Noile funcții din această versiune sunt enumerate mai jos:

- Suport pentru modurile CAPWAP și WGB pe modulul de interfață Wi-Fi Cisco
- Suport suplimentar pentru modem pentru modulele celulare conectabile
- Suport pentru modulul de interfață conectabil P-LTE-450

Caracteristici noi pentru Cisco IOS XE 17.13.1

Acest capitol conține următoarele secțiuni:

- Modificare a furnizorului pentru modulul GNSS
- Acces IOX la accelerometrul și giroscopul de bord IR1800
- Apărarea unificată împotriva amenințărilor (UTD)
- vManage Support pentru modul EWC pe modulul de interfață Wi-Fi Cisco
- Suport suplimentar pentru modem pentru modulele conectabile celulare CAT 6 și CAT 7
- SD-WAN
- Modificare a ieșirii CLI pentru modemul FN980 5G

Caracteristici noi pentru Cisco IOS XE 17.12.1a

Noile funcții din această versiune sunt enumerate mai jos:

- Accesați datele despre accelerometru și senzorul giroscop de la IRM-GNSS
- Suport 5G Standalone Mode (SA).
- Implementarea licenței nelimitate

Caracteristici noi pentru Cisco IOS XE 17-11-1a

Noile funcții din această versiune sunt enumerate mai jos:

- Suport pentru modulul de interfață conectabil LoRaWAN
- Suport GNSS pe modulul GPS/Dead Reckoning (IRM-GNSS-ADR)
- Suport Galileo pentru modulele conectabile LTE
- Schimbați la Smart Licensing Packaging
- Suport Cisco IoT Operations Dashboard (OD) pentru configurarea și gestionarea modulului WP-WIFI6-x

Caracteristici noi pentru Cisco IOS XE 17.10.1a

Noile funcții din această versiune sunt enumerate mai jos:

- Suport SFP Digital Subscriber Line (DSL) pe IR1800
- Suport vManage pentru modulul WP-WIFI6-x
- Activați capabilitățile de ștergere sigură a datelor
- CLI de configurare Rawsocket Keepalive

Caracteristici noi pentru Cisco IOS XE 17.9.1

Noile funcții din această versiune sunt enumerate mai jos:

- Suport pentru modul de instalare
- Îmbunătățiri ale timpului de pornire celulară
- Avertisment de downgrade IOS XE
- Sondaj SNMP pentru OID de temperatură
- Modul GPS este activat implicit
- Suport de captură de pachete pentru CANBUS
- Suport GPS și Dead Reckoning pentru conectorul J1939

Caracteristici noi pentru Cisco IOS XE 17.8.1

- Îmbunătățirea caracteristicii prizei brute, la pagina 271
- Îmbunătățirea SCADA pentru TNB, la pagina 259
- Actualizarea interfeței de operațiuni de rețea gRPC, la pagina 393
- Actualizare GNMI Broker (GNMIB), la pagina 393

Îmbunătățiri ale funcționalității celulare

Au fost aduse îmbunătățiri pentru funcțiile celulare și GPS, după cum urmează:

Punctele de declanșare și codul de depanare pot fi activate prin intermediul CLI-urilor celulare ale controlerului pentru generarea și captarea automată a datelor de depanare, fără intervenție manuală. Sunt disponibile următoarele opțiuni CLI:

(controller de configurare)#**funcționalitate modem lte?**

GPS	Depanare GPS
resetarea interfeței	Resetare interfețe/Ștergere purtător
crash modem	Depanare prin blocare modem
resetarea modemului	IOS a inițiat resetări necunoscute ale modemului

Datele de depanare includ următoarele:

- Jurnalele de depanare bazate pe context (urmărire și locații GPS).
- Mesaje de depanare bine formatate.
- Date de depanare specifice furnizorului într-un interval mai larg.

Jurnalele de depanare se află în următoarea locație a flash:

router#**dir flash:servelogs** Directorul de
bootflash:/servelogs/

259340	-rw-	122	7 septembrie 2021 17:40:44 +00:00 7	gpslog-slot5-20210907-174044 celllog-
259339	-rw-	1734	septembrie 2021 12:14:07 +00:00	slot5-20210905-164628

Fișierele de jurnal GPS și celulare sunt create separat cu nume de fișiere folosind marcajul de timp din momentul creării. Aceste fișiere sunt create după cum urmează:

- Dacă fișierul existent a ajuns la 10Mb, va fi creat un fișier nou.
- Un fișier nou va fi creat dacă caracteristica (GPS sau mobil) este complet dezactivată și apoi reactivată.

Caracteristici noi pentru Cisco IOS XE 17.7.1

Suportă SFP-uri 1G

Versiunea 17.7.1 va adăuga suport pentru următoarele SFP-uri:

GLC-T-RGD

CWDM-SFP-1470=

CWDM-SFP-1610=

CWDM-SFP-1530=

DWDM-SFP-3033=

DWDM-SFP-3112=

GLC-BX-DI=

GLC-BX-UI=

GLC-TE

CAPITOL 3

Configurație CLI de bază a routerului

Acest capitol conține următoarele secțiuni:

Denumirea interfeței IR1800

Descrierile și graficele interfețelor routerului se găsesc înGhid de instalare hardware.

Interfețele hardware acceptate și convențiile lor de denumire sunt în următorul tabel:

Interfață hardware	Convenția de denumire
Port combo Gigabit Ethernet	GigabitEthernet0/0/0
Porturi Gigabit Ethernet	GigabitEthernet0/1/0 GigabitEthernet0/1/1 GigabitEthernet0/1/2 GigabitEthernet0/1/3
Interfață celulară	celular 0/4/0 celular 0/4/1 celular 0/5/0 celular 0/5/1

Interfață hardware	Convenția de denumire
Interfață serială asincronă	asincron 0/2/0 async 0/2/1 (când platforma de bază acceptă două interfețe seriale asincrone)
USB	usbflash0:
mSATA	msata
Intrare de alarmă	contact de alarma 0
GPIO	contact de alarmă 1-4

Configurație de bază

Configurația de bază este rezultatul intrărilor pe care le-ați făcut în timpul dialogului de configurare inițială. Aceasta înseamnă că routerul are cel puțin o interfață setată cu o adresă IP care să fie accesibilă, fie prin WebUI, fie pentru a permite procesului PnP să funcționeze. Utilizați**arată rularea-config**comandă pentru a vizualiza configurația inițială, așa cum se arată în exemplul următor:

```
Router#arată rularea-config
Configurația clădirii...

Configurație curentă: 7008 octeți!

! Ultima modificare a configurației la 00:01:55 GMT duminica 20 septembrie 2020!

versiunea 17.6
marcajele temporale ale serviciului depanare date și oră
msec marcajele temporale ale serviciului jurnal datetime
msec serviciu call-home
platformă qfp utilizare monitor încărcare 80 platformă
punt-keepalive disable-kernel-core !

numele gazdă IR1800
!
boot-start-marker
sistem de pornire bootflash:/ir1800-universalk9.17.06.01prd18.SPA.bin boot-end-
marker
!
!
!
nu aaa nou-model
fus orar ceas GMT -7 0 !

temporizator de oprire a contactului 120
!
prag de subtensiune la aprindere 9 600 !

fara sens de aprindere
!
fara activare a aprinderii
!
!
!
!
```

```
!
!
!
nume de domeniu ip cisco.com
ip dhcp excluded-address 10.0.0.1!

ip dhcp pool webui_int import
all
rețea 10.0.0.0 255.255.255.0 dns-server
10.0.0.1
default-router 10.0.0.1
închiriere 0 2
!
!
!
blocare autentificare-pentru 60 de încercări 3 în termen de 30 de
întârziere de conectare 3
login on-succes log
!
!
!
!
!
!
!
modelarea abonatului
!
!
!
!
!
!
Nume pachet multilink autentificat!

!
!
!
!
!
!
!
!
crypto pki trustpoint SLA-TrustPoint înscriere
pkcs12
revocare-verificare crl
!
crypto pki trustpoint TP-self-signed-2276770909 înregistrare
autosemnată
subiect-nume cn=IOS-Self-Signed-Certificate-2276770909 revocation-
check none
rsakeypair TP-auto-semnat-2276770909 !

!
Lanț de certificate crypto pki Certificat SLA-TrustPoint ca 01

30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030 32310E30
0C060355 040A16303 040A13903 040A13903 1E060355 04031317 43697363 6F204C69 63656E73
696E6720 526F6F74 20434130 1E170D31 33303533 3031833737 30353330 31393438 34375A30
32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363C 6597363
696E6720 526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
82010A02 82010A02 82013BDE0501 145EA72C 2CD686E6 17222EA1 F1EFF64D CBB4C798
212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E5940D 8A38E5940D78
C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
```

4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC 7390A3EB
2B5436AD C847A2C5 DAB553EB 6533EBCFA0932C930C93 58BD7188 68E69491 20F320E7
948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7 C7479096 B4CB2D62
EA2F5061D4 CC7B5062D4 E8250FC4 5D5D5FB8 8F27D191 C55F0D76 61F9A4CD 3D992327
A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44 DFC7C6FD011 01A34230 40300E06
03551D0F 0101FF04 04030201 06300F06 03551D13 0101FF04 05300301 01FF301D
0603501414904 4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01
010B0500 03820101 00507F24 D3932A658D0C 86F70D01 6D4DF6B0 49631C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
D98987CBD9C2E420CAE9C2011 8FA85686 CD98B646 5575B146 8DFC66A8 467A3DF4 4D565700
6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A92327CE671C767C 152E99B7 B1FCF9BB
E973DE7F 5BDDEB86 C71E3B49 1765308B 5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1
1A48A229 C9878C1F06 C98791F06 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A
B623CDBD 230E3AFB 418616A9 4093E049 4D10AB75 27E86F73 932E35B5FDA 8862751E
719BB2F0 D697DF7F 28

renunta
lanț de certificate crypto pki TP-auto-semnat-2276770909 certificat auto-
semnat 01
30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030 31312F30
2D060355 040391325624450362 2D536967 6E65642D 43657274 69666963 6174652D 32323736
37373039 3039301E 170D3230 30393230 31393230 31337303036A 39323031 34303630
365A3031 312F302D 06035504 03132649 4F532D53 656C662D 5369676E 65642D43 6576267463
32373637 37303930 39308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
0A028201 018782A4A93 0FCF6DB2 2794CC97 CF8DC253 D1CFB83B ACFA305A 28BA6174
2452EE0B C45E92EA BBA30235 C142D2D3 DA04C6FD A916507C BAFE6806 BBAB86BB50AC61
BBAB8655FB C5449A92 EFAA9519 9A2A084E 94A29BF5 B78604F2 76927505 371AD917 67D8EACF
CEBBA6A1 278F5647 DDDBE8AF 8E451772929704903 C2FA72E2 0C03C426 BB844F76 0BE65C37
60DFDA8E 38EBAFD8 9B3908BF 9B5A50B2 37539BF4 9D3256D9 B118DDF4 BC912DAA90
BCE912DAA990 4B594142 B46D7C93 13FF997B 2FECC956 2362A8CC A0CD51EF 5691A2C3
9EB200FE F4D341AE F35D3C06 8BCC1ACF 42E983FF F8C0B09065F8C7090F6 41CE9402 0572AE66
EF050203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603 551D23014
8173015 810530 030101FF 53C24775 8FC918B5 8059336C 12301D06 03551D0E 04160414
5C7DADE3 7AB19153 C247758F C918B580 59336C12 39086D08 F70D0101 05050003 82010100
673243D9 3BBC0321 1FAC5459 926E99BF 60E55344 123B8A22 359B5DA8 E98E0A4FFC
5BAF0479FFC 5BAF0479F E74BEC68 DF4D2116 9DBD58D0 F4ABEE17 D9155CAE DBB7E94E
7A058507 CFA8DFB2 90E44C50 F95AD87F 934F904D 8C07CE47 5AEBBCEB0794 EBAEBBCEB0794
CC4642B6 DE641222 E045CEF4 27625FD2 FE51853C 574CCCA8 F036874B 93C97278 3D3776F1
E6419A07 46065203 FB81BFFD52970BBE2452970B8 DF667257 DA97D96D 3E226378 28CE8460
2570D7D3 4D78C9E2 66FBA5B1 9A6E46AD E466D67F 425BFC40 FA717361 CBAA933361
9A6E46AD975 F1B6D193 12162EAA 6389A57C CF65AA08 53B07581 87A0C15A D5B6900B
E3F98713 F3918F89

renunta
!
!
fără licență hseck9
licență udi pid IR1835-K9 sn FHH2416P00V procesor fără
memorie low-watermark 47775 !

nivel de pornire de diagnostic minim!

spanning-tree extinde sistemul-id!

!
redundanţă
mod nici unul
!
!
controler GPS-Dr
!

```
!
politica internă de alocare vlan ascendentă!

!
interfață GigabitEthernet0/0/0 fără
adresă IP
închidere
negociere auto
!
închiderea interfeței
GigabitEthernet0/1/0
!
interfață GigabitEthernet0/1/1 acces în
modul switchport
!
închiderea interfeței
GigabitEthernet0/1/2
!
interfață GigabitEthernet0/1/3 !

interfață Wlan-GigabitEthernet0/1/4 !

interfața Vlan1
fara adresa ip
!
interfață Async0/2/0
fara adresa ip
încapsulare scada
!
interfață Async0/2/1
fara adresa ip
încapsulare scada
!
server ip http
ip http auth-retry 3 time-window 1 ip http
autentificare ip local http server securizat

ip forward-protocol nd
server ip dns
ip nat în interiorul listei sursă 197 supraîncărcare GigabitEthernet0/0/0!

!
!
ip access-list extins 197 10 permit ip
any any
!
!
!
!
planul de control
!
!
!
mgcp behavior rsip-range tgcp-only mgcp
behavior comedia-role niciunul
mgcp behavior comedia-check-media-src disable mgcp
behavior comedia-sdp-force disable !

profil mgcp implicit
!
!
!
!
!
```

```
!
linia con 0
opriri 1
linia 0/0/0 0/0/1
linia 0/2/0 0/2/1
linia vty 0 4
log in
transport de intrare toate
ieșire de transport toate
linia vty 5 15
log in
transport de intrare toate
ieșire de transport toate
!
sunați acasă
! Dacă adresa de e-mail de contact din call-home este configurată ca sch-smart-licensing@cisco.com ! adresa de e-mail configurată în Cisco Smart License Portal va fi utilizată ca adresă de e-mail de contact pentru a trimite notificări SCH.

contact-email-addr sch-smart-licensing@cisco.com profil
„CiscoTAC-1”
activ
destinație transport-metoda http !


Sfârșit
```

Configurarea parametrilor globali

Pentru a configura parametri globali pentru routerul dvs., urmați acești pași.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**configura terminalul** **Exemplu:** Router>**permite** Router#**configura terminalul** Router(config)#	Intră în modul de configurare globală când se utilizează portul de consolă. Utilizați următoarele pentru a vă conecta la router cu un terminal la distanță: nume sau adresa router telnet. Conectare: ID-ul de conectare Parola: ********* Router> activare
Pasul 2	**nume de gazdă***nume* **Exemplu:** Router(config)#**Nume gazdă Router**	Specifică numele routerului.
Pasul 3	**activați parola***parolă*sau**activați parola secretă***parolă* **Exemplu:** Router(config)#**activați parola cr1ny5ho**	Specifică o parolă pentru a preveni accesul neautorizat la router. **Nota** În această formă a comenzii, parola nu este criptat. Pentru a cripta parola utilizați activare

	Comanda sau Acțiune	Scop
		parola secretă, așa cum este menționată în Ghidul de întărire a dispozitivului menționat anterior.

Configurarea interfeței Gigabit Ethernet

Configurația implicită pentru interfața Gigabit Ethernet (GI0/0/0) de pe IR1800 este Layer 3 (L3). Interfața Gigabit Ethernet de pe IR1800 este un port combo, ceea ce înseamnă că este un conector RJ45+SFP. Dacă utilizați un SFP ca interfață, trebuie să setați tipul media pentru SFP.

Router(config-if)#**sfp de tip media**

Trebuie selectat conectorul corect, consultațiGhid de instalare hardware.

Pentru a defini manual interfața Gigabit Ethernet, urmați acești pași, începând de la modul de configurare globală.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**configura terminalul**	
Pasul 2	**IPv6 unicast-routing** **Exemplu:** Router#**IPv6 unicast-routing**	Permite redirecționarea pachetelor de date unicast IPv6.
Pasul 3	**interfață GigabitEthernet***slot/bay/port* **Exemplu:** Router(config)#**interfață GigabitEthernet 0/0/0**	Intră în modul de configurare pentru o interfață pe router.
Pasul 4	**adresa ip***masca cu adresa ip* **Exemplu:** Router(config-if)#**adresa ip 192.168.12.2 255.255.255.0**	Setează adresa IP și masca de subrețea pentru interfața specificată. Utilizați acest pas dacă configurați o adresă IPv4.
Pasul 5	**adresa ipv6***adresă/prefix ipv6* **Exemplu:** Router(config-if)#**adresa ipv6 2001.db8::ffff:1/128**	Setează adresa IPv6 și prefixul pentru interfața specificată. Utilizați acest pas în loc de Pasul 2, dacă configurați o adresă IPv6. Trebuie configurată și rutarea unicast IPv6, consultați informații suplimentare în**Ghid de configurare de bază pentru adrese IPv6 și conectivitate** situat aici:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-16-10/ip6b-xe-16-10-book/citește-mă-întâi.html

	Comanda sau Acțiune	Scop
Pasul 6	**nicio oprire** **Exemplu:** Router(config-if)#**nicio oprire**	Activează interfața și își schimbă starea de la administrativ în jos la administrativ sus.
Pasul 7	**Ieșire** **Exemplu:** Router(config-if)#**Ieșire**	Iese din modul de configurare al interfeței și revine la modul de configurare globală.

Suport pentru sub-interfață pe GigabitEthernet0/0/0

Cisco IOS-XE acceptă sub-interfețe și configurația dot1q pe interfața g0/0/0. De exemplu:

```
Router(config)#interfata g0/0/0 ?
  <1-4294967295> Număr interfață GigabitEthernet Router(config-
subif)#încapsulare?
  punct1Q                IEEE 802.1Q LAN virtuală
```

Configurarea unei interfețe Loopback

Înainte de a începe

Interfața loopback acționează ca un substituent pentru adresa IP statică și oferă informații implicite de rutare.

Pentru a configura o interfață loopback, urmați acești pași.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**configura terminalul**	
Pasul 2	**interfata***numărul de tip* **Exemplu:** Router(config)#**interfață Loopback 0**	Intră în modul de configurare pe interfața loopback.
Pasul 3	(Opțiunea 1)**adresa ip***masca cu adresa ip* **Exemplu:** Router(config-if)#**adresa ip 10.108.1.1 255.255.255.0**	Setează adresa IP și masca de subrețea pe interfața de loopback. (Dacă configurați o adresă IPv6, utilizați**adresa ipv6** *adresă/prefix ipv6*comanda descrisă mai jos.

	Comanda sau Acțiune	Scop
Pasul 4	(Opțiunea 2)**adresa ipv6***adresă/prefix ipv6* **Exemplu:** Router(config-if)#**adresa ipv6 2001:db8::ffff:1/128**	Setează adresa IPv6 și prefixul pe interfața de loopback.
Pasul 5	**Ieșire** **Exemplu:** Router(config-if)#**Ieșire**	Iese din modul de configurare pentru interfața loopback și revine la modul de configurare globală.

Exemplu

Verificarea configurației interfeței Loopback

Introduceți**arată loopback-ul interfeței**comanda. Ar trebui să vedeți o ieșire similară cu următorul exemplu:

```
Router#arată interfața loopback 0 Loopback0
este activ, protocolul de linie este activ
   Hardware-ul este Loopback
   Adresa de internet este 192.0.2.0/16
   MTU 1514 octeți, BW 8000000 Kbit, DLY 5000 usec,
       fiabilitate 255/255, txload 1/255, rxload 1/255 Encapsulare
   LOOPBACK, loopback nu setat
   Ultima intrare niciodată, ieșire niciodată, ieșire se blochează
   niciodată Ultima ștergere a contoarelor „afișați interfața” niciodată
   Strategia de așteptare: fifo
   Coada de ieșire 0/0, 0 picături; coadă de intrare 0/75, 0 picături 5
   minute rata de intrare 0 biți/sec, 0 pachete/sec Rată de ieșire 5 minute
   0 biți/sec, 0 pachete/sec
       0 pachete de intrare, 0 octeți, 0 fără buffer
       A primit 0 transmisii, 0 runt, 0 giganți, 0 throttles
       0 erori de intrare, 0 CRC, 0 cadru, 0 depășire, 0 ignorat, 0 anulare 0 ieșire pachete, 0
       octeți, 0 subîncărcări
       0 erori de ieșire, 0 coliziuni, 0 resetări de interfață 0 erori de buffer de
       ieșire, 0 tampon de ieșire schimbate
```

Alternativ, utilizați**ping**comandă pentru a verifica interfața de loopback, așa cum se arată în exemplul următor:

```
Router#ping 192.0.2.0
Tastați secvența de evacuare pentru a anula.
Trimiterea ecourilor ICMP de 5, 100 de octeți la 192.0.2.0, timeout este de 2 secunde: !!!!!

Rata de succes este de 100 la sută (5/5), dus-întors min/media/max = 1/2/4 ms
```

Activarea protocolului Cisco Discovery

Cisco Discovery Protocol (CDP) este activat implicit pe router. Poate fi dezactivat dacă este necesar din motive de securitate.

Pentru mai multe informații despre utilizarea CDP, consultațiGhid de configurare Cisco Discovery Protocol, Cisco IOS XE Release 3S.

Configurarea accesului la linia de comandă

Pentru a configura parametrii pentru a controla accesul la router, urmați acești pași.

Nota Intrarea de transport trebuie setată așa cum este explicat în secțiunile anterioare Telnet și SSH ale ghidului.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**linie [aux | consola | tty | vty]***număr-linie* **Exemplu:** Router(config)#**consola de linie 0**	Intră în modul de configurare a liniei și specifică tipul de linie. Exemplul oferit aici specifică un terminal de consolă pentru acces.
Pasul 2	**parolă***parolă* **Exemplu:** Router (linie de configurare) #**parola 5dr4Hepw3**	Specifică o parolă unică pentru linia terminalului consolei.
Pasul 3	**log in** **Exemplu:** Router (linie de configurare) #**log in**	Activează verificarea parolei la conectarea la sesiunea terminalului.
Pasul 4	**exec-timeout***minute*[*secunde*] **Exemplu:** Router (linie de configurare) #**exec-timeout 5 30** Router (linie de configurare) #	Setează intervalul în care interpretorul de comandă EXEC așteaptă până când este detectată intrarea utilizatorului. Valoarea implicită este 10 minute. Opțional, adaugă secunde la valoarea intervalului. Exemplul oferit aici arată un timeout de 5 minute și 30 de secunde. Introducerea unui timeout de**0 0** specifică să nu expire niciodată.
Pasul 5	**Ieșire** **Exemplu:** Router (linie de configurare) #**Ieșire**	Iese din modul de configurare linie pentru a reintra în modul de configurare globală.
Pasul 6	**linie [aux | consola | tty | vty]***număr-linie* **Exemplu:** Router(config)#**linia vty 0 4** Router (linie de configurare) #	Specifică un terminal virtual pentru accesul la consolă de la distanță.

	Comanda sau Acțiune	Scop
Pasul 7	**parolă***parolă* **Exemplu:** Router (linie de configurare) #**parola aldf2ad1**	Specifică o parolă unică pentru linia terminalului virtual.
Pasul 8	**log in** **Exemplu:** Router (linie de configurare) #**log in**	Activează verificarea parolei la autentificarea sesiunii de terminal virtual.
Pasul 9	**Sfârşit** **Exemplu:** Router (linie de configurare) #**Sfârşit**	Iese din modul de configurare a liniei și revine la modul EXEC privilegiat.

Exemplu

Următoarea configurație arată comenzile de acces la linia de comandă. Rețineți că introducerea de transport nu este implicită, dar dacă SSH este activat, acesta trebuie setat la ssh.

Nu trebuie să introduceți comenzile marcate**implicit**. Aceste comenzi apar automat în fișierul de configurare care este generat atunci când utilizați**arată rularea-config**comanda.

```
!
consola de linie 0
exec-timeout 10 0
parola 4youreyesonly
log in
intrare transport niciuna (implicit) biți de
oprire 1 (implicit) linia vty 0 4

parola secretă
log in
!
```

Configurarea rutelor statice

Rutele statice oferă căi fixe de rutare prin rețea. Acestea sunt configurate manual pe router. Dacă topologia rețelei se modifică, ruta statică trebuie actualizată cu o nouă rută. Rutele statice sunt rute private, cu excepția cazului în care sunt redistribuite printr-un protocol de rutare.

Pentru a configura rute statice, urmați acești pași.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	(Opțiunea 1)**ruta ip***masca de prefix*{*adresa ip* | *interfață-tip interfață-număr*[*adresa ip*]} **Exemplu:** Router(config)#**ruta IP 192.10.2.3 255.255.0.0 10.10.10.2**	Specifică o rută statică pentru pachetele IP. (Dacă configurați o adresă IPv6, utilizați **ruta ipv6**comanda descrisă mai jos.)
Pasul 2	(Opțiunea 2)**ruta ipv6***prefix/mască* {*adresa ipv6*| *interfață-tip interfață-număr* [*adresa ipv6*]} **Exemplu:** Router(config)#**ruta ipv6 2001:db8:2::/64 2001:db8:3::0**	Specifică o rută statică pentru pachetele IP. Vedeți informații suplimentare pentru IPv6 aici: https://www.cisco.com/c/en/us/td/docs/ios-xml/ ios/ipv6_basic/configuration/xe-16-10/ ip6b-xe-16-10-book/read-me-first.html
Pasul 3	**Sfârşit** **Exemplu:** Router(config)#**Sfârşit**	Iese din modul de configurare globală și intră în modul EXEC privilegiat.

În următorul exemplu de configurare, ruta statică trimite toate pachetele IP cu o adresă IP de destinație de 192.168.1.0 și o mască de subrețea de 255.255.255.0 pe interfața Gigabit Ethernet către un alt dispozitiv cu o adresă IP de 10.10.10.2. Mai exact, pachetele sunt trimise către PVC-ul configurat.

Nu trebuie să introduceți comanda marcată**implicit**. Această comandă apare automat în fișierul de configurare generat atunci când utilizați**arată rularea-config**comanda.

!
ip fără clasă (**implicit**)
ruta IP 2001:db8:2::/64 2001:db8:3::0

Verificarea configurației

Pentru a verifica dacă ați configurat corect rutarea statică, introduceți codul**arata ruta ip** comanda (sau **arată ruta ipv6**comanda) și căutați rutele statice marcate cu litera S.

Când utilizați o adresă IPv4, ar trebui să vedeți rezultate de verificare similare cu următoarea:

Router#**arata ruta ip**
Coduri: C - conectat, S - static, R - RIP, M - mobil, B - BGP
D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF inter zona N1 - OSPF NSSA extern tip 1, N2 - OSPF NSSA extern tip 2 E1 - OSPF extern tip 1, E2 - OSPF extern tip 2

i - IS-IS, su - IS-IS rezumat, L1 - IS-IS nivel-1, L2 - IS-IS nivel-2 ia - IS-IS inter zona, * - implicit candidat, U - rută statică per utilizator o - ODR, P - rută statică descărcată periodic

Poarta de ultimă instanță nu este setată

```
        10.0.0.0/24 este subrețea, 1 subrețea
C           10.108.1.0 este conectat direct, Loopback0
S*      0.0.0.0/0 este conectat direct, GigabitEthernet0
```

Când utilizați o adresă IPv6, ar trebui să vedeți rezultate de verificare similare cu următoarea:

```
Router#arată ruta ipv6
Tabel de rutare IPv6 - implicit - 5 intrări
Coduri: C - Conectat, L - Local, S - Static, U - Rută statică per utilizator
        B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
        I2 - ISIS L2, IA - interzonă ISIS, IS - rezumat ISIS, D - EIGRP EX - EIGRP extern, ND - ND
        Implicit, NDp - ND Prefix, DCE - Destinație

        NDr - Redirecționare, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1 OE2 - OSPF ext 2,
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2 ls - site LISP, ld - LISP dyn-EID, a -
        Aplicație

C    2001:DB8:3::/64 [0/0]
        prin GigabitEthernet0/0/2, conectat direct 2001:DB8:2::/64
S       [1/0]
        prin 2001:DB8:3::1
```

Configurarea rutelor dinamice

În rutarea dinamică, protocolul de rețea ajustează calea automat, pe baza traficului de rețea sau a topologiei. Modificările rutelor dinamice sunt partajate cu alte routere din rețea.

Toate ghidurile de configurare Cisco IOS-XE pot fi găsite aici:https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-amsterdam-17-3-1/model.html

Configurarea protocolului de informații de rutare

Pentru a configura RIP-ul pe un router, urmați acești pași.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**ruter rip** **Exemplu:** Router(config)#**ruter rip**	Intră în modul de configurare a routerului și activează RIP pe router.
Pasul 2	**versiune**{**1**|**2**} **Exemplu:** Router(config-router)#**versiunea 2**	Specifică utilizarea RIP versiunea 1 sau 2.

	Comanda sau Acțiune	Scop
Pasul 3	**reţea***adresa ip* **Exemplu:** Router(config-router)#**rețeaua 192.168.1.1** Router(config-router)#**rețeaua 10.10.7.1**	Specifică o listă de rețele pe care urmează să fie aplicat RIP, folosind adresa rețelei fiecărei rețele conectate direct.
Pasul 4	**fara auto-rezumat** **Exemplu:** Router(config-router)#**fara auto-rezumat**	Dezactivează rezumarea automată a rutelor de subrețea în rute la nivel de rețea. Acest lucru permite ca informațiile de rutare ale subprefixului să treacă peste granițele rețelei clasificate.
Pasul 5	**Sfârşit** **Exemplu:** Router(config-router)#**Sfârşit**	Iese din modul de configurare a routerului și intră în modul EXEC privilegiat.

Exemplu

Verificarea configurației

Pentru a verifica dacă ați configurat corect RIP, introduceți**arata ruta ip**comandă și căutați rutele RIP marcate cu litera R. Ar trebui să vedeți o ieșire similară cu cea prezentată în exemplul următor:

```
Router#arata ruta ip
Coduri: C - conectat, S - static, R - RIP, M - mobil, B - BGP
        D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF inter zona N1 - OSPF NSSA extern tip
        1, N2 - OSPF NSSA extern tip 2 E1 - OSPF extern tip 1, E2 - OSPF extern tip 2

        i - IS-IS, su - IS-IS rezumat, L1 - IS-IS nivel-1, L2 - IS-IS nivel-2 ia - IS-IS inter zona, * - implicit
        candidat, U - rută statică per utilizator o - ODR, P - rută statică descărcată periodic


Poarta de ultimă instanță nu este setată

      10.0.0.0/24 este subrețea, 1 subrețea
C        10.108.1.0 este conectat direct, Loopback0
R     3.0.0.0/8 [120/1] prin 2.2.2.1, 00:00:02, Ethernet0/0/0
```

Configurarea protocolului îmbunătățit de rutare a gateway-ului interior

Enhanced Interior Gateway Routing Protocol (EIGRP) este o versiune îmbunătățită a Interior Gateway Routing Protocol (IGRP) dezvoltat de Cisco. Proprietățile de convergență și eficiența operațională a EIGRP s-au îmbunătățit substanțial față de IGRP, iar IGRP este acum învechit.

Tehnologia de convergență a EIGRP se bazează pe un algoritm numit Diffusing Update Algorithm (DUAL). Algoritmul garantează o funcționare fără bucle în fiecare moment pe parcursul calculării rutei și permite sincronizarea tuturor dispozitivelor implicate într-o schimbare de topologie. Dispozitivele care nu sunt afectate de modificările topologiei nu sunt implicate în recalculări

Detalii despre configurarea protocolului EIGRP (Enhanced Interior Gateway Routing Protocol) se găsesc în următorul ghid:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-16-10/ire-xe-16-10-book/ire-enhanced-igrp.html

QoS modular (MQC)

Această secțiune oferă o prezentare generală a modular QoS CLI (MQC), care este modul în care sunt configurate toate caracteristicile QoS pe routerul pentru servicii integrate IoT. MQC este o abordare standardizată pentru a permite QoS pe platformele Cisco de rutare și comutare.

Urmați procedurile din Ghidul de configurare a interfeței pentru linia de comandă QoSModular QoS, ghidul Cisco IOS XE 17.

Configurarea interfeței seriale

Această secțiune descrie configurarea managementului interfeței seriale.

IR1800 acceptă protocoale de interfață serială asincronă utilizate pentru SCADA, Raw Socket sau Releu de încapsulare. În funcție de tipul de produs, routerul are una sau două interfețe seriale.

Tabelul 1: Convențiile de denumire

Interfață serială	Număr de linie	Cartografiere internă
Asincron 0/2/0 (DTE)	Linia 0/2/0 (50)	ttyS1
Asincron 0/2/1 (DCE)	Linia 0/2/1 (51)	ttyUSB0

IR1821

IR1821 are doar un singur port serial Async.

IR1831

IR1831 are două porturi, un port DTE și DCE doar cu RS232.

IR1833

IR1833 are două porturi, un port DTE și DCE doar cu RS232.

IR1835

IR1835 are două porturi, un DCE cu RS232/RS485 și un port DTE cu RS232. Cu RS485 de tip media, există suport atât pentru setări half cât și duplex.

Nota Cablarea serială asincronă este documentată înGhid de instalare hardware IR1800.

Specificarea unei interfețe seriale asincrone

Pentru a specifica o interfață serială asincronă și pentru a intra în modul de configurare a interfeței, utilizați una dintre următoarele comenzi în modul de configurare globală.

Comanda sau Acțiune	Scop
Router(config)# interfață asincronă 0/2/0	Intră în modul de configurare a interfeței.

Specificarea încapsulării seriale asincrone

Cele două interfețe seriale vor fi marcate ca asincron 0/2/0 și 0/2/1. Numărul compartimentului pentru asincron este 2.

Interfețele seriale asincrone acceptă următoarele metode de încapsulare serială:

- Priză brută
- Releu de linie
- Traducerea protocolului SCADA

Comanda sau Acțiune	Scop
Router(config-if)#**încapsulare** *{raw-tcp|raw-udp|scada|rele-line}*	Configurați încapsularea serială asincronă.

Metodele de încapsulare sunt setate în funcție de tipul de protocol sau de aplicație pe care o configurați în software-ul Cisco IOS.

Restul metodelor de încapsulare sunt definite în cărțile și capitolele respective care descriu protocoalele sau aplicațiile.

Configurarea portului serial

Dispozitivul IR1835 Pro are port DCE combinat RS232/RS485 Async 0/2/1. Dispozitivele rămase din seria IR1800 acceptă numai tipul media RS232.

Tabelul 2: Exemple de configurare

#**sh run int Async 0/2/1** Configurație clădire... Configurație curentă: 95 octeți! interfață Async0/2/1 fara adresa ip încapsulare scada tip media rs485 full-duplex Sfârșit	Port DCE cu RS485 de tip media

#sh run int Async 0/2/1 Configurație clădire... Configurație curentă: 64 de octeți! interfață Async0/2/1 fara adresa ip încapsulare raw-tcp Sfârșit	Port DCE cu RS232 de tip media [Configurație implicită]
sh run int Async 0/2/0 Configurație clădire... Configurație curentă: 64 de octeți! interfață Async0/2/0 fara adresa ip sfârșitul liniei de releu de încapsulare	Port DTE cu RS232 de tip media implicit. (RS485 nu este acceptat).

Următorul exemplu de configurare este pentru RS485 și RS232 de tip media.

IR1800#**sh rulează int asincron 0/2/1**
Configurație clădire... Configurație curentă:
100 de octeți!

interfață Async0/2/1
fara adresa ip
încapsulare-releu-line media-tip
rs485
semi-duplex
. . . . . IR1800#**sh rulează**
int asincron 0/2/0 Configurația
clădirii...

Configurație curentă: 64 de octeți!

interfață Async0/2/0
fara adresa ip
încapsulare scada
Sfârșit

Liniile care nu sunt în modul asincron -sau- fără suport hardware:

Tty Line Typ Tx/Rx A Modem Roty AccO AccI utilizează depășiri de zgomot Int1, 4-49, 52-73, 89-735

CAPITOL 4

Interfață cu utilizatorul web

Acest capitol conține următoarele secțiuni:

Introducere în interfața cu utilizatorul web

Interfața cu utilizatorul web (WebUI) oferă administratorilor de rețea o singură soluție pentru furnizarea, monitorizarea și optimizarea dispozitivelor. După ce finalizați instalarea hardware, trebuie să configurați dispozitivul cu o configurație necesară pentru a permite traficului să treacă prin rețea. În prima zi cu noul dispozitiv, puteți efectua o serie de sarcini pentru a vă asigura că dispozitivul este online, accesibil și ușor de configurat. Aceasta este denumită interfața Ziua 0.

Nota O configurație Ziua 0 este definită ca un dispozitiv care este proaspăt scos din cutie, fără configurație de pornire.

După configurarea inițială a Zilei 0, WebUI poate fi utilizată pentru configurarea zilnică.

Odată ce routerul pornește în ziua 0, computerul se poate conecta la rețeaua 192.168.1.x și poate accesa WebUI folosind adresa IP 192.168.1.1 cu orice browser. După ce configurația este aplicată prin WebUI, routerul va afișa mesajul „Day 0 config done. Stop autoinstall”.

Ziua 0 Modul celular

Cisco IOS XE ediția 17.9.1 oferă o nouă funcționalitate, permițând configurarea routerului în Ziua 0 prin modulul conectabil celular. Aceasta presupune că un modul conectabil celular este deja instalat.

Acest mod ajută la configurarea APN-ului celular, presupunând că clientul primește un APN privat (sau LTE/5G privat) ca backhaul WAN. Procedând astfel, valoarea APN este stocată în modem. Odată ce routerul repornește, acesta este resetat la valorile implicite din fabrică, permițând routerului să efectueze PnP peste Cellular atunci când este utilizat APN privat.

Nota Modul avansat este necesar pentru a configura WAN celular, inclusiv APN public sau privat. Acesta ar trebui să fie furnizat de furnizorul de servicii SIM.

Nota Interfața conectabilă nu poate fi schimbată la cald. Dacă doriți să schimbați un SIM, opriți routerul.

Urmează pașii de configurare prin modulul conectabil celular:

1.Selectați interfața celulară în**tip WAN**.

2.Introduceți numele APN.

3.Nu este nevoie să selectați un WAN de rezervă.

4.Reporniți routerul.

PnP va putea rula acum cu APN privat pentru a se conecta la IOS OD, vManage sau DNA-C.

Ziua 0 Interfața cu utilizatorul web

În vigoare cu IOS-XE Versiunea 17.1.1, interfața de utilizator web Day 0 (WebUI) va fi acceptată pe IR1101. Ziua 0 WebUI este acceptată numai pe porturile LAN. Acestea sunt porturile FastEthernet 0/0/1 – 0/0/4 pe IR1101. Conectați fie un PC/laptop Windows, Linux sau Mac la unul dintre porturile LAN ale IR1101 și porniți routerul în ziua 0. PC-ul/laptop-ul trebuie configurat pentru a obține o adresă IP prin DHCP.

Suport suplimentar pentru modem pentru modulele conectabile celulare CAT 6 și CAT 7

Această versiune oferă suport pentru modemuri suplimentare pe IR1101 și IR1800.

Modulele de interfață conectabile LTE Cat6 (PIM) vor fi actualizate cu modemuri Cat7. Următorul tabel arată tranziția produsului:

Tabelul 3: Tranziția Cat6 la Cat7

Cat6 (Actual)	**Cat7 (reîmprospătat)**
Sierra Wireless EM7455/7430	Sierra Wireless EM7411/7421/7431
Cat6 LTE Advanced	Cat7 LTE Advanced

Următoarele sunt noile PID-uri care vor fi disponibile:

- P-LTEA7-NA
- P-LTEA7-EAL
- P-LTEA7-JP
- P-5GS6-R16SA

Important Pentru noile PID-uri menționate mai sus, următoarele funcții celulare nu au fost testate și nu sunt acceptate cu IOS XE versiunea 17.13.1, deși comenzile CLI pot permite:

- GNSS/NMEA
- Celular Dying-Gasp
- Suport eSIM/eUICC

Nota Nu există nicio interfață de linie de comandă nouă sau modificată cu aceste modemuri noi.

Suport suplimentar pentru modem pentru modulele celulare conectabile

Cisco IOS-XE Versiunea 17.14.1 îmbunătățește opțiunile de conectivitate și debitul pe platformele IR1101 și IR1800 prin acceptarea modemurilor celulare suplimentare:

- Modemuri CAT 7:
  - P-LTEA7-NA
  - P-LTEA7-EAL
  - P-LTEA7-JP
- Modem 5G:
  - P-5GS6-R16SA-GL

Nota Modemurile CAT 7 acceptă streaming GNSS și NMEA, în timp ce în prezent modulul P-5GS6-R16SA-GL nu acceptă streaming GPS și NMEA.

Suport Galileo pentru modulele conectabile LTE

Cu Cisco IOS XE 17.11.1a și versiuni anterioare, singura constelație GNSS acceptată a fost GPS. Această versiune introduce suport pentru Galileo.

Nota O singură constelație poate fi activată la un moment dat.

Există noi opțiuni CLI disponibile pentru a sprijini noua constelație:

Comenzi de configurare

config#**controler celular** *<slot/port>*
(controller de configurare)#**<nu> lte gps constellation** *<GPS | galileo | gnss >*

Exemplu:

(controller de configurare)#**constelație GPS lte?**
galileo selectați Galileo ca constelație activă selectați GPS ca
GPS constelație activă selectați mai multe GNSS ca constelație
gnss activă

Nota Setarea implicită este modul GPS.

Noile opțiuni galileo și gnss din CLI de mai sus sunt utilizate pentru a configura Galileo și, respectiv, GNSS Multiplu/Simultan (GPS + Galileo etc).

Dacă dezactivați configurația GPS, asigurați-vă că nu există nicio constelație configurată, în concordanță cu configurația modului GPS. De exemplu:

config#**controler Cellular 0/1/0** (controller de configurare)#**nu lte**
gps constellation gps

Afișați comenzi

Următorul exemplu arată constelația GNSS actuală ca Galileo:

#afișați detaliile GPS 0/1/0 celular
Caracteristica GPS = activată
Modul GPS configurat = autonom Constelație curentă
configurată = Port GPS selectat = Port GPS dedicatgalileo | GPS | gnss
Stare GPS = achiziție GPS

Orice modificare adusă configurației va necesita repornirea routerului.

Mai multe informații sunt disponibile înGhid de configurare a modulului de interfață conectabilă celulară.

Modul GPS este activat implicit

În versiunile IOS XE anterioare 17.9.1, GPS a fost activat implicit, cu toate acestea, modul GPS a fost dezactivat implicit. Acest lucru a necesitat ca utilizatorul să efectueze un ciclu suplimentar de pornire a modemului după ce a apărut routerul pentru a utiliza GPS-ul.

Începând cu IOS XE 17.9.1, Modul GPS va fi activat în mod implicit și va fi setat în modul autonom. Acest lucru va ajuta la reducerea timpului de conectare celulară.

Nota Acest lucru se aplică numai GPS-ului bazat pe celular. Acest lucru nu se aplică modulului GPS/GNSS din IR1800 (modul DR), IR8140 (GPS nativ) și IR8340 (modul de sincronizare).

Utilizați următoarea comandă pentru a verifica starea GPS-ului celular:

Router#**afișați GPS-ul <slot> celular**
resetare automată Activați resetarea automată a modemului după configurarea modului sau activarea GPS

Orientări și limitări

Următoarele sunt linii directoare și limitări pentru IR1101 și IR1800:

IR1101

În vigoare cu IOS-XE Versiunea 17.3.1, interfața de utilizator web Day 0 (WebUI) va fi acceptată pe IR1101. Ziua 0 WebUI este acceptată numai pe porturile LAN. Acestea sunt porturile FastEthernet 0/0/1 – 0/0/4 pe IR1101. Conectați un computer la unul dintre porturile LAN ale IR1101 și porniți routerul în ziua 0. PC-ul poate fi configurat să utilizeze DHCP sau cu o adresă IP statică de 192.168.1.2/255.255.255.0.

Următoarele sunt limitări ale funcției Ziua 0:

- WebUI nu este suportat pe portul 1G deoarece această interfață este dedicată PnP. Este acceptat doar pe porturile 1-4 de 100M.
- Plug and Play (PNP) nu poate fi utilizat dacă routerul este utilizat pentru configurarea utilizând Day 0 WebUI, deoarece PNP va fi anulat odată ce configurația este aplicată prin Day 0 WebUI.
- Începând cu versiunea 17.1.2, un explicit**memorie de scriere**nu este necesar odată ce configurația este aplicată prin WebUI.

IR1800

Interfața utilizator Web Day 0 (WebUI) este acceptată pe IR1800. Ziua 0 WebUI este acceptată numai pe porturile LAN. Acestea sunt porturile GigabitEthernet 0/1/0 – 0/1/3 pe IR1800. Conectați un computer la unul dintre porturile LAN ale IR1800 și porniți routerul în ziua 0. PC-ul poate fi configurat să utilizeze DHCP sau cu o adresă IP statică de 192.168.1.2/255.255.255.0.

Următoarele sunt limitări ale funcției Ziua 0:

- WebUI nu este acceptat pe portul GigabitEthernet 0/0/0. Este acceptat numai pe porturile LAN GigabitEthernet0/1/0 prin GigabitEthernet0/1/3.

• Plug and Play (PNP) nu poate fi utilizat dacă routerul este utilizat pentru configurarea utilizând Day 0 WebUI, deoarece PNP va fi anulat odată ce configurația este aplicată prin Day 0 WebUI.

Configurarea computerului pentru a se conecta la router

Următoarea secțiune oferă îndrumări pentru configurarea computerului pentru a interfața corect cu IR1101.

Puteți accesa aplicația dintr-un browser web client. Asigurați-vă că sunt îndeplinite următoarele cerințe de client web:

• Hardware—Un laptop sau desktop Mac (versiunea OS 10.9.5) sau Windows (versiunea OS 10) compatibil cu unul dintre următoarele browsere testate și acceptate:

• Google Chrome 59 sau o versiune ulterioară

• Mozilla Firefox 54 sau o versiune ulterioară

• Apple Safari 10 sau o versiune ulterioară

• Browser Microsoft Edge

• Rezoluția afișajului — Vă recomandăm să setați rezoluția ecranului la 1280 x 800 sau mai mare.

Conectarea la router folosind DHCP

Configurați identificatorul de client DHCP pe client pentru a obține adresa IP de la router și pentru a vă putea autentifica cu acreditările de conectare din ziua 0.

Configurarea identificatorului de client DHCP pe client pentru Windows

1.Tip**regedit**în caseta de căutare Windows din bara de activități și apăsați**intra**.

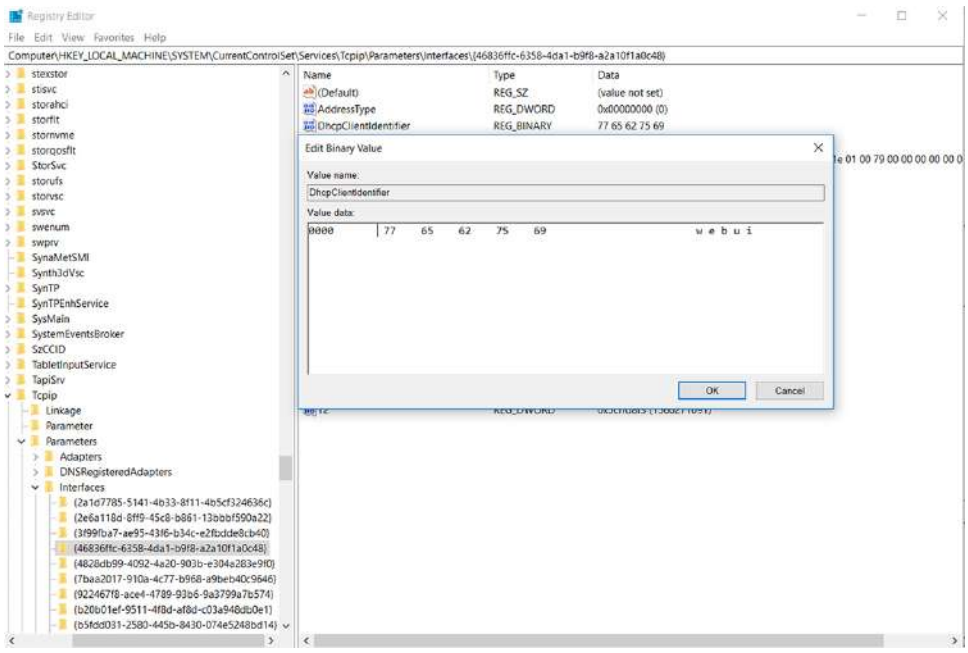
2.Dacă vi se solicită controlul contului utilizator, faceți clic**Da**pentru a deschide Editorul Registrului.

3.Navigați la

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces și localizați**Identificator unic global al interfeței Ethernet (GUID)**.

4.Adăugați un nou REG_BINARY**DhcpClientIdentifier**cu Date**77 65 62 75 69**pentru**webui**. Trebuie să introduceți manual valoarea.

Figura 1: Configurarea identificatorului de client DHCP pe Windows

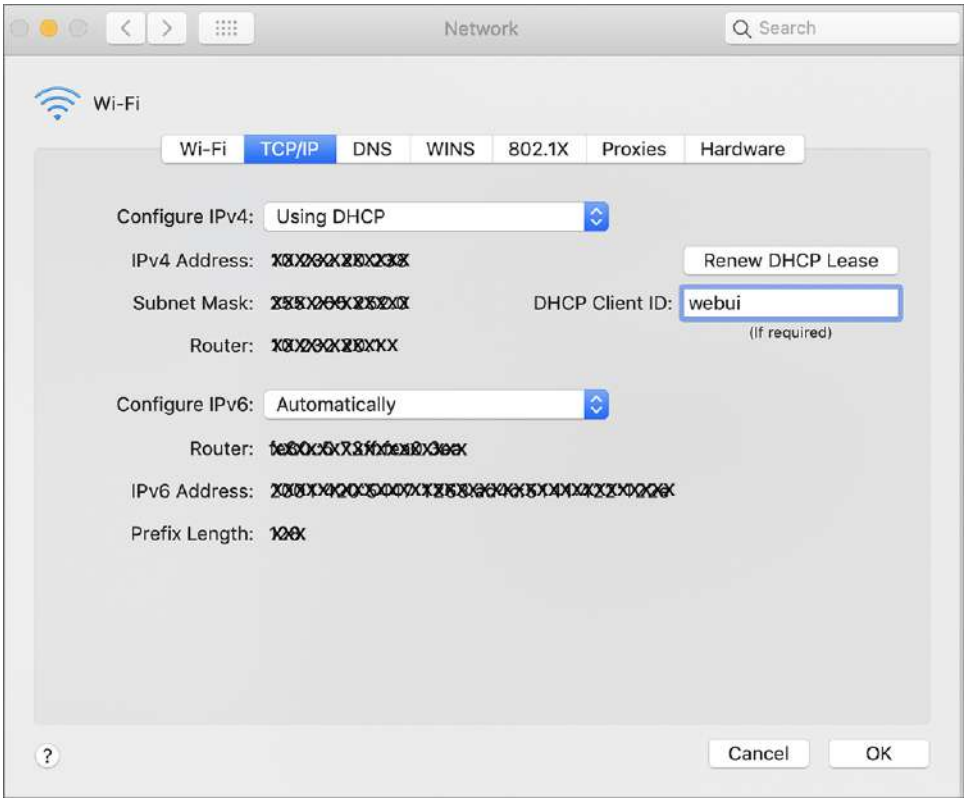


5.Reporniți computerul pentru ca configurația să aibă efect.

Configurarea identificatorului de client DHCP pe client pentru MAC

1.Du-te la**Preferințe de sistem > Rețea > Avansat > TCP > ID client DHCP:**si intra**webui**.

Figura 2: Configurarea identificatorului de client DHCP pe MAC



2.Clic**Bine**pentru a salva modificările.

Continuând cu Expertul de configurare

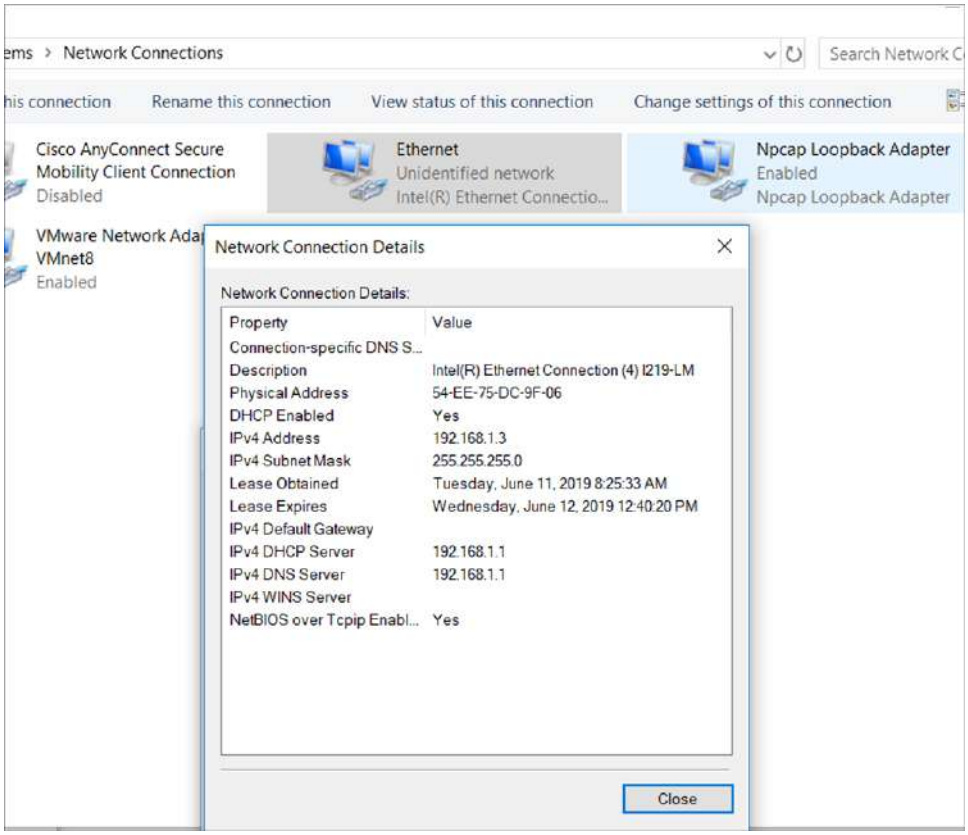
Scriptul de pornire rulează vrăjitorul de configurare, care vă solicită să introduceți configurația de bază: (**Doriți să intrați în dialogul de configurare inițială? [da/nu]:**).Pentru a configura setările Zilei 0 utilizând interfața de utilizare web, nu introduceți un răspuns. Efectuați în schimb următoarele sarcini:

1.Asigurați-vă că niciun dispozitiv nu este conectat la router.

2.Conectați un capăt al cablului ethernet la unul dintre porturile de downlink (non-management) de pe supervizorul activ și celălalt capăt al cablului ethernet la gazdă (PC/MAC).

3.Configurați computerul/MAC-ul ca client DHCP, pentru a obține automat adresa IP a routerului. Ar trebui să obțineți o adresă IP în intervalul 192.168.1.x/24.

Figura 3: Obținerea adresei IP



Poate dura până la trei minute. Trebuie să finalizați configurarea Zilei 0 prin interfața de utilizare web înainte de a utiliza terminalul routerului.

4.Lansați un browser web pe computer și introduceți adresa IP a routerului (**https://192.168.1.1**) în bara de adrese.

5.Introduceți numele de utilizator pentru Ziua 0**webui**si parola**cisco**.

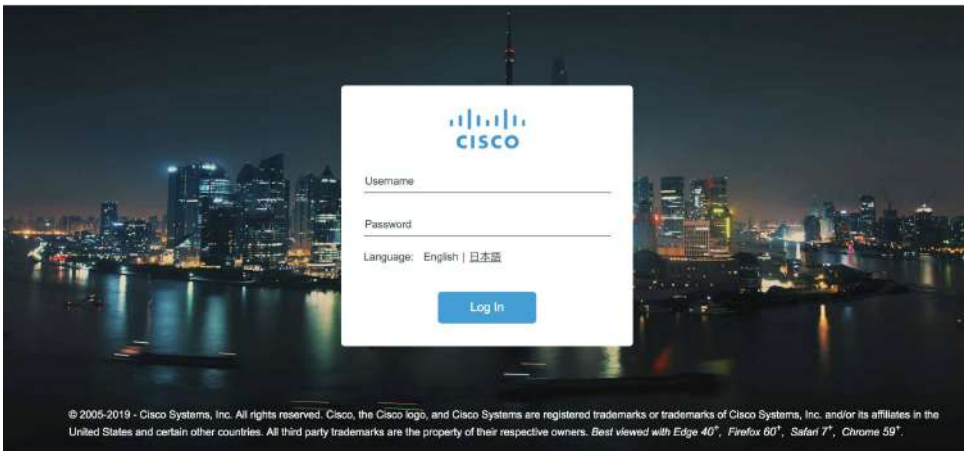
Configurarea modului de bază WebUI prin browser

Următorii pași vă ghidează prin procesul de utilizare a browserului pe PC/laptop pentru a configura WebUI.

Procedură

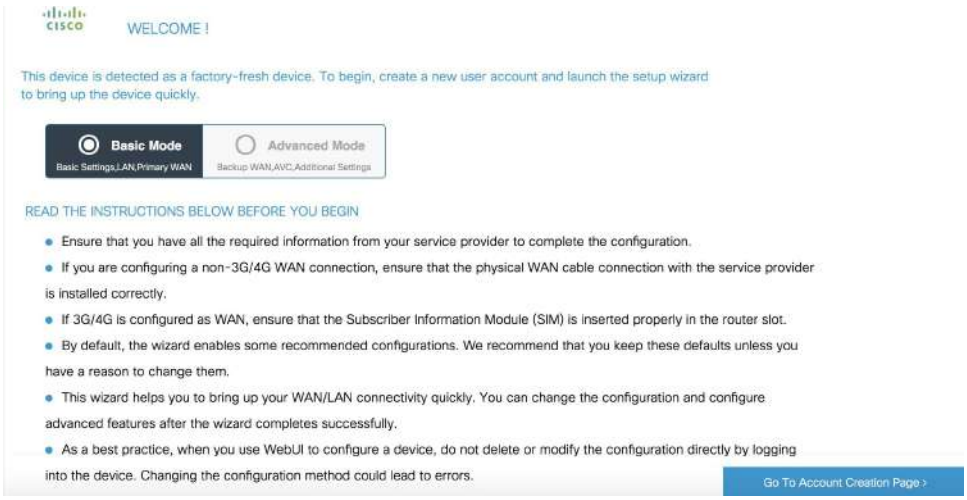
Pasul 1 Deschideți browserul și introduceți 192.168.1.1 în bara de adrese. Apare ecranul de conectare. Introduceți numele de utilizator **webui**și Parola**cisco**. Apoi faceți clic**Log in**.

Figura 4: Ecranul de conectare



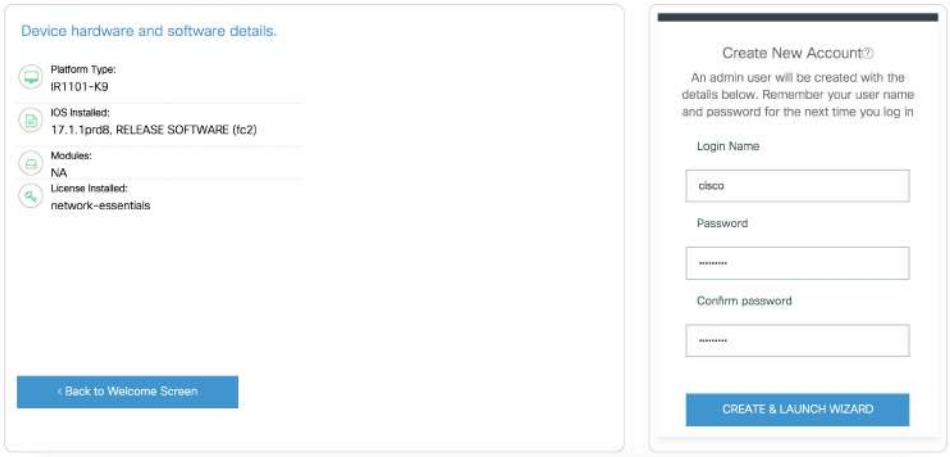
Pasul 2 Apare ecranul de bun venit. Selectați Modul avansat sau Modul de bază. Modul de bază permite configurarea setărilor de bază, a rețelei LAN și a unui WAN primar. Modul avansat vă permite să configurați un WAN de rezervă suplimentar, AVC, precum și setări suplimentare. În scopul acestei secțiuni, se utilizează Modul de bază. Selecta**Modul de bază**.

Figura 5: Ecranul de bun venit



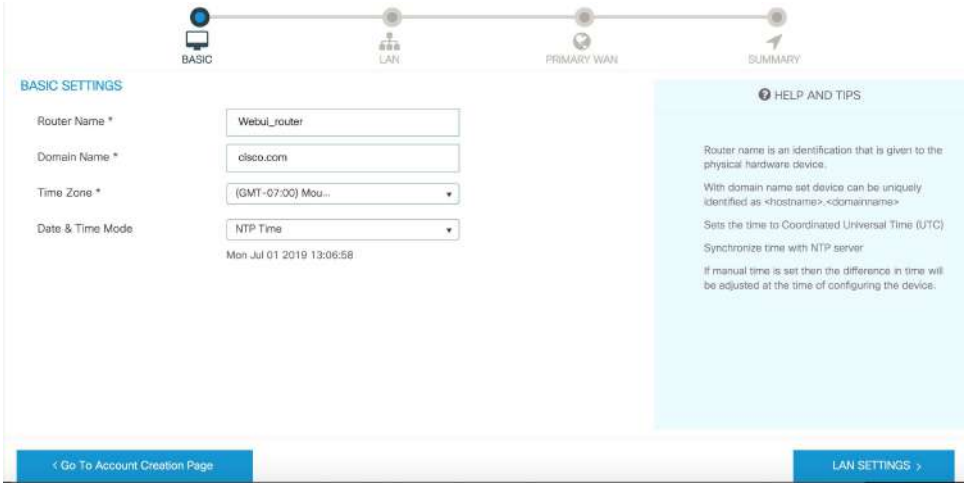
Pasul 3 Clic**Accesați pagina de creare a contului**. Apare ecranul Creare cont nou. Creați un nou nume de autentificare și parolă pentru a accesa WebUI.

Figura 6: Ecranul Creare cont nou



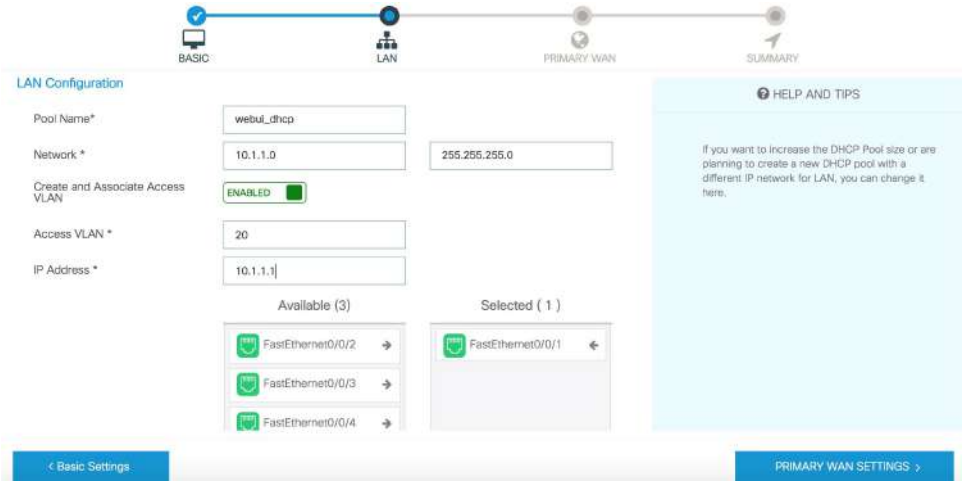
Pasul 4 Clic**CREATE & LUNCH WIZARD**. Apare ecranul Setări de bază. Furnizați un nume de router (nume de gazdă), un nume de domeniu, un fus orar și un mod de dată și oră.

Figura 7: Ecranul SETĂRI DE BAZĂ



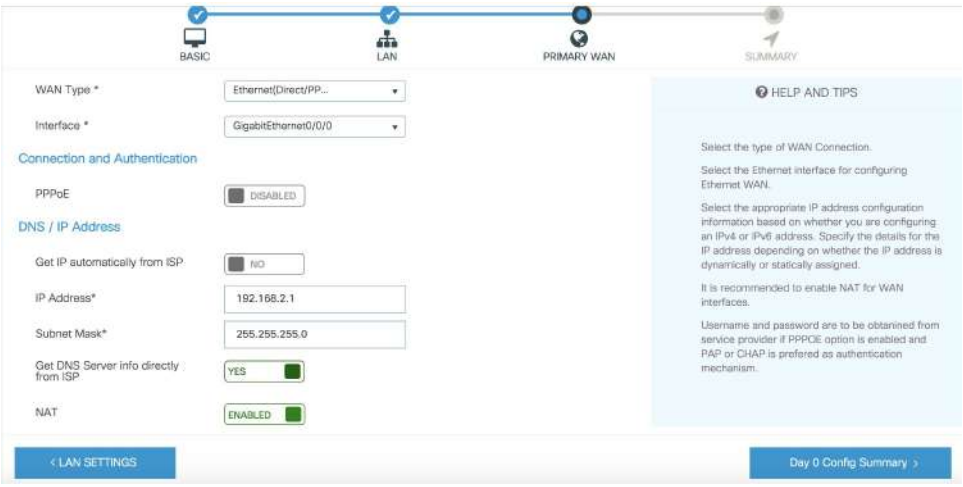
Pasul 5 Clic**SETĂRI LAN**. Apare ecranul de configurare LAN. Introduceți webui_dhcp Pool Name, adresa IP a interfeței VLAN și selectați interfața care este conectată la laptopul dvs. din lista de interfețe disponibile.

Figura 8: Ecranul de configurare LAN



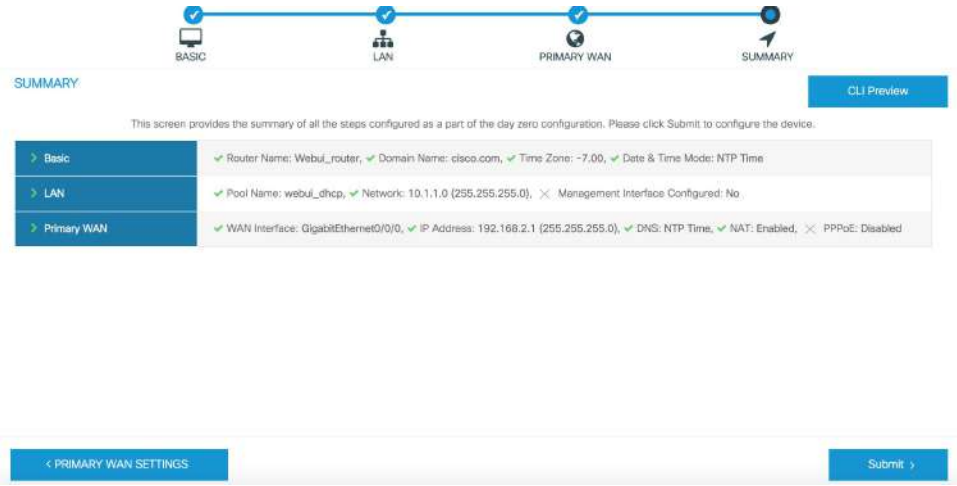
Pasul 6 Clic**SETĂRI PRIMAR WAN**. Apare ecranul SETĂRI WAN PRINCIPALE. Configurați interfața WAN selectând Tipul și Interfața WAN din opțiunile disponibile. Apoi introduceți informațiile despre adresa dvs. IP DNS și selectați Activare/Dezactivare NAT.

Figura 9: Ecranul interfeței WAN primară



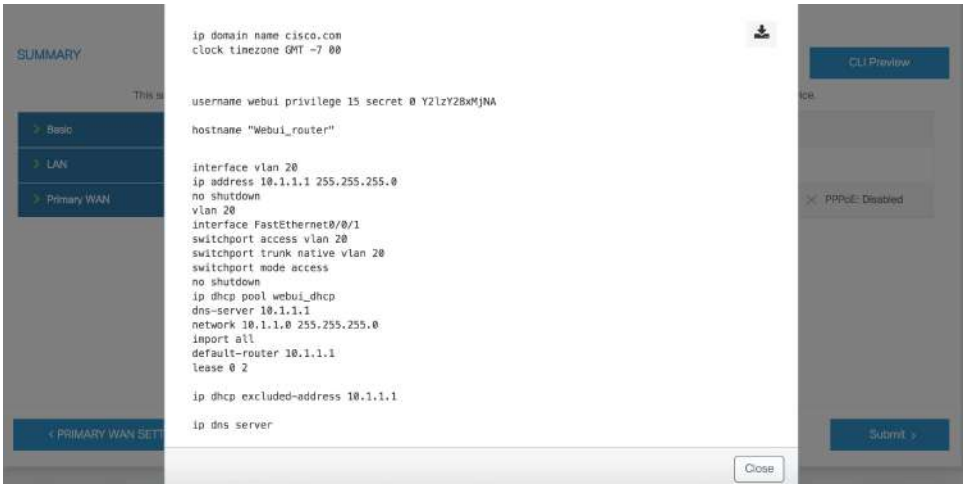
Pasul 7 Clic**Rezumatul config. Ziua 0**. Apare ecranul Rezumat revizuire. Verificați intrările înainte de a aplica configurația.

Figura 10: Ecranul Rezumat



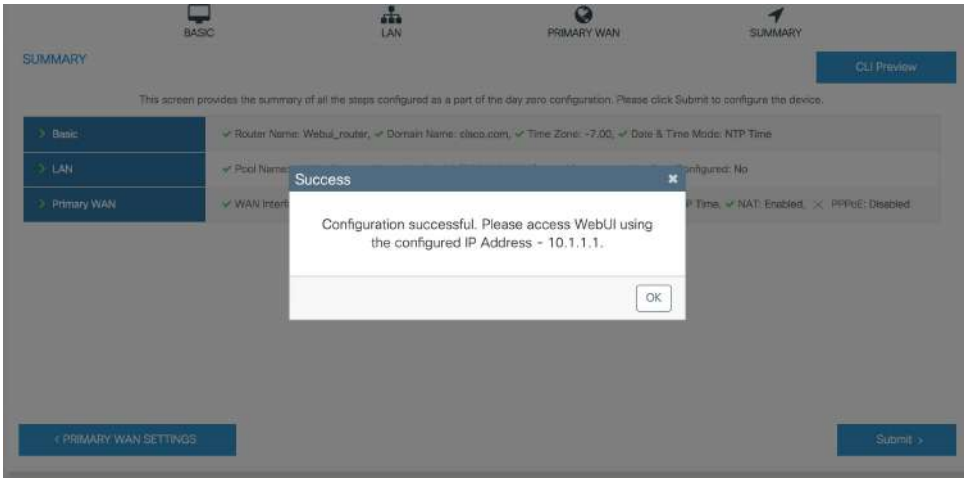
Pasul 8 (Opțional) Puteți da clic pe**Previzualizare CLI**pentru a vedea Configurația care este aplicată routerului. Închideți previzualizarea CLI și, dacă sunteți gata, faceți clic**Trimiteți**.

Figura 11: Ecranul de previzualizare CLI



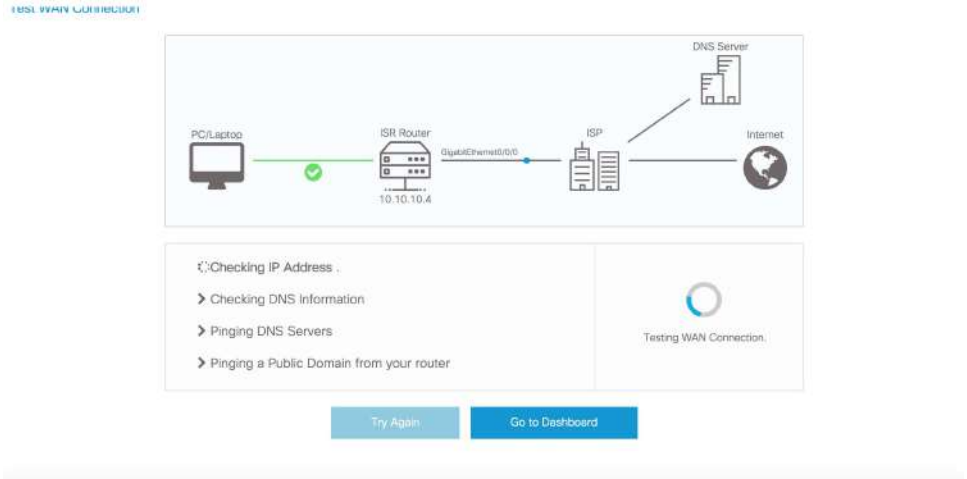
Pasul 9 După ce faceți clic pe**Trimiteți**, va apărea o casetă de dialog care vă informează că configurația a fost aplicată cu succes. Este prezentată și noua adresă IP WebUI.

Figura 12: Caseta de dialog Trimitere



Pasul 10 Dacă aveți conexiune web, dispozitivul va încerca să se conecteze. Se recomandă să închideți sesiunea de browser și să treceți la adresa IP WebUI nou configurată.

Figura 13: Ecranul de testare a conexiunii VLAN



Configurarea modului avansat WebUI prin browser

Următorii pași vă ghidează prin procesul de utilizare a browserului de pe computer pentru a configura WebUI.

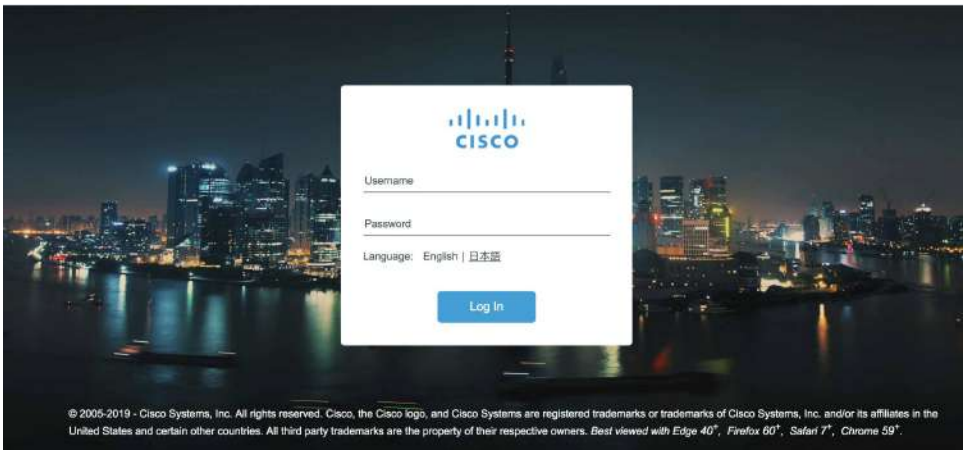
Asigurați-vă că laptopul dvs. este configurat pentru a obține o adresă IP prin DHCP sau atribuiți o adresă IP*nnnn* potrivirea subrețelei implicite.

Nota Modul avansat este necesar pentru a configura WAN celular, inclusiv APN public sau privat.

Procedură

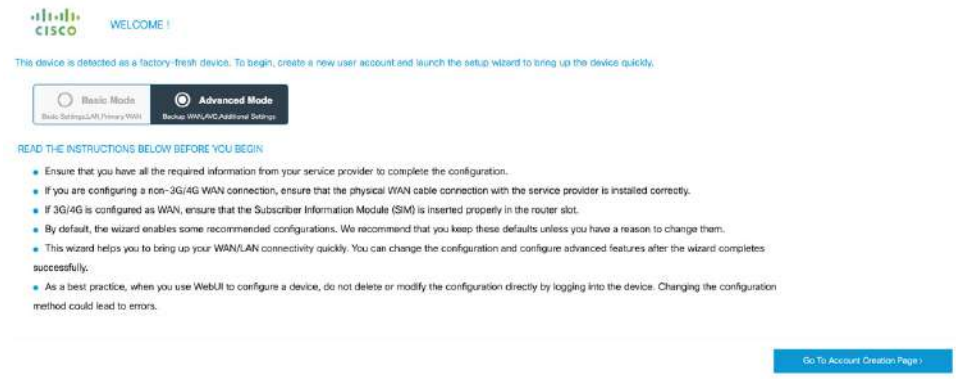
Pasul 1 Deschideți browserul și introduceți 192.168.1.1 în bara de adrese. Apare ecranul de conectare. Introduceți numele de utilizator **webui**și Parola**cisco**. Apoi faceți clic**Log in**.

Figura 14: Ecranul de conectare



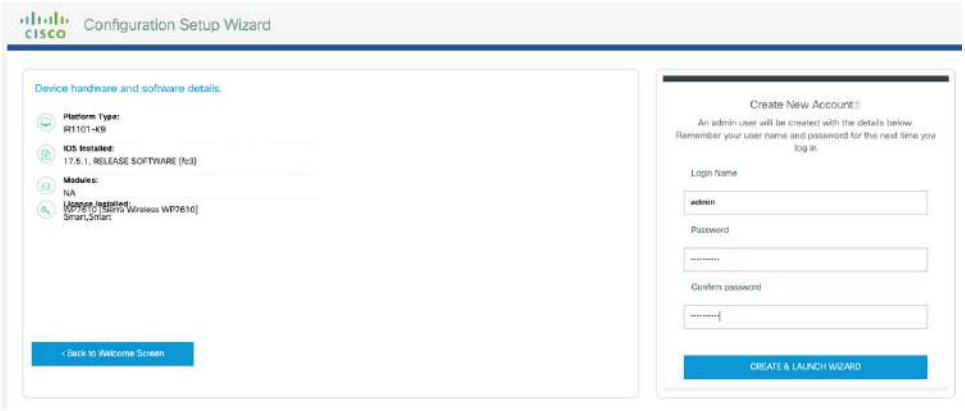
Pasul 2 Apare ecranul WELCOME. Selectați Modul avansat sau Modul de bază. Modul de bază permite configurarea setărilor de bază, a rețelei LAN și a unui WAN primar. Modul avansat vă permite să configurați un WAN de rezervă suplimentar, AVC, precum și setări suplimentare. În scopul acestei secțiuni, este utilizat Modul avansat.

Figura 15: Ecranul WELCOME



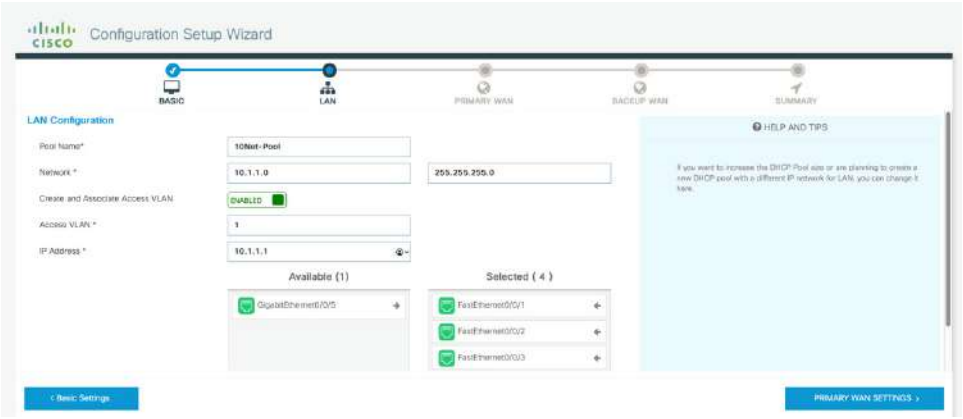
Pasul 3 Selecta**Modul avansat**, apoi faceți clic**Accesați pagina de creare a contului**. Apare ecranul Creare cont nou. Creați un nou nume de autentificare și parolă pentru a accesa WebUI.

Figura 16: Ecranul Creare cont nou



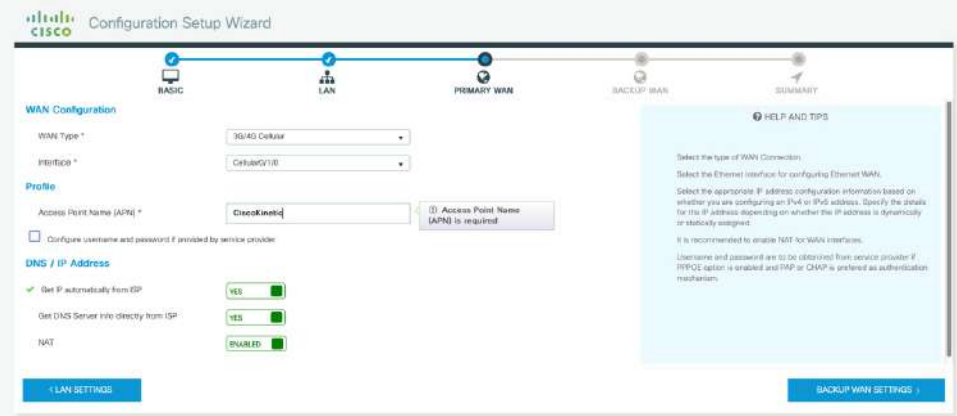
Pasul 4 Clic**CREATE & LUNCH WIZARD**Apare ecranul Configurare LAN. Furnizați un nume de grup, o adresă IP de rețea, o subrețea, un VLAN de acces și o adresă IP a dispozitivului. Se afișează o listă de interfețe disponibile din care puteți selecta.

Figura 17: Ecranul de configurare LAN



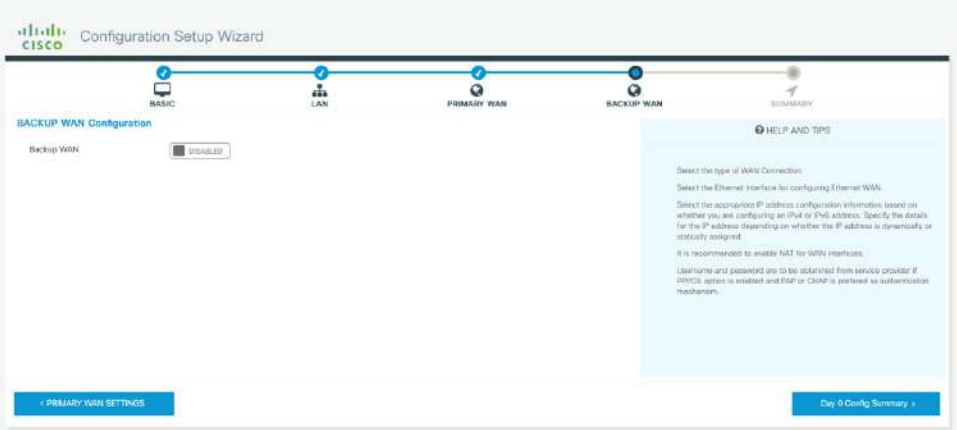
Pasul 5 Clic**SETĂRI PRIMAR WAN**. Apare ecranul Configurare WAN. Selectați tipul și interfața WAN din meniurile derulante. Furnizați un APN (nume punct de acces) de la furnizorul dvs. de servicii LTE, apoi selectați setările DNS și adresa IP pentru rețeaua dvs.

Figura 18: Ecranul de configurare WAN



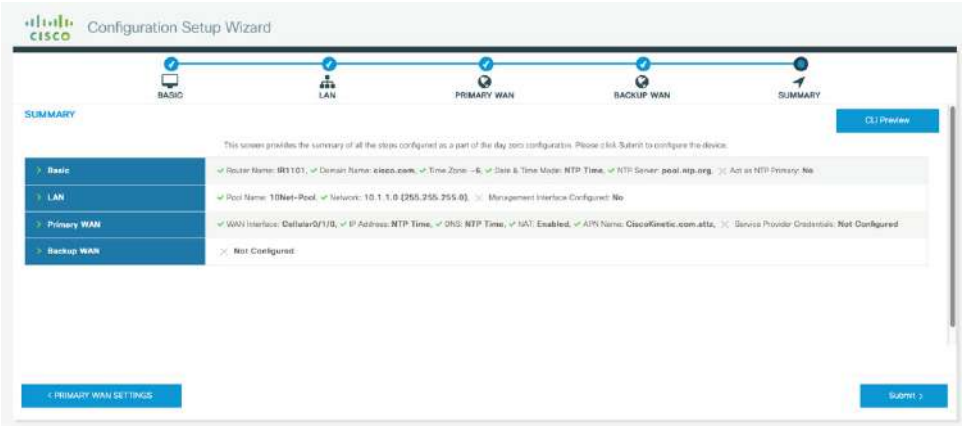
Pasul 6 Clic**SETĂRI BACKUP WAN**. Apare ecranul BACKUP WAN Configuration. Selectați butonul pentru a activa sau dezactiva un WAN de rezervă.

Figura 19: Configurare BACKUP WAN



Pasul 7 Clic**Rezumatul config. Ziua 0**. Apare ecranul REZUMAT. Verificați intrările înainte de a aplica configurația.

Figura 20: Ecranul Rezumat



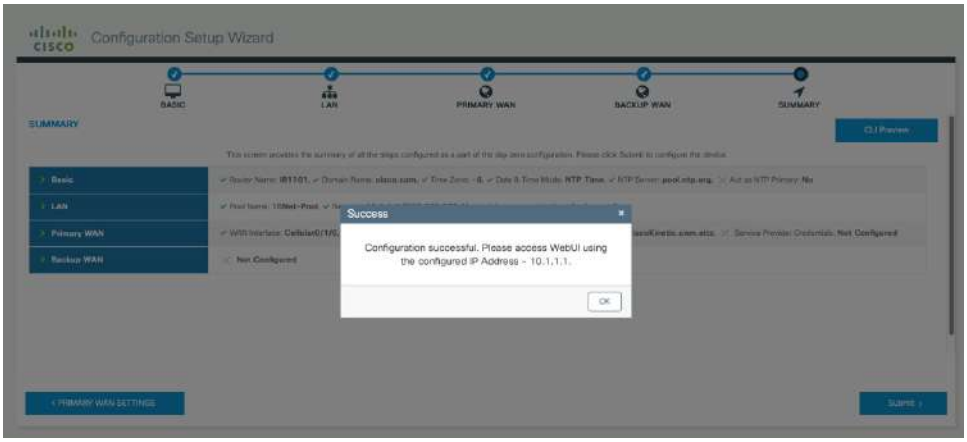
Pasul 8 (Opțional) Puteți da clic pe**Previzualizare CLI**pentru a vedea Configurația care este aplicată routerului. Închideți previzualizarea CLI și, dacă sunteți gata, faceți clic**Trimiteți**.

Nota

Un exemplu de previzualizare CLI este găsit la sfârșitul acestei secțiuni.

Pasul 9 După ce faceți clic pe**Trimiteți**, va apărea o casetă de dialog care vă informează că configurația a fost aplicată cu succes. Este prezentată și noua adresă IP WebUI.

Figura 21: Caseta de dialog Trimitere



Exemplu

Următorul este un exemplu de previzualizare CLI:

```
  nume de domeniu ip cisco.com
ceas fus orar GMT -6 00 server ntp
pool.ntp.org

nume de utilizator privilegiu de administrator 15 secret 0 Mjc1N0dsb2NrIQ==

numele gazdă „IR1101”
```

interfață vlan 1
adresa ip 10.1.1.1 255.255.255.0 fără oprire

vlan 1
interfață FastEthernet0/0/1 acces
switchport vlan 1 switchport trunk vlan
nativ 1 acces mod switchport

nicio oprire
interfață FastEthernet0/0/2 acces
switchport vlan 1 switchport trunk vlan
nativ 1 switchport mod acces

nicio oprire
interfață FastEthernet0/0/3 acces
switchport vlan 1 switchport trunk vlan
nativ 1 acces mod switchport

nicio oprire
interfață FastEthernet0/0/4 acces
switchport vlan 1 switchport trunk vlan
nativ 1 switchport mod acces

nicio oprire
ip dhcp pool 10Net-Pool dns-
server 10.1.1.1
rețea 10.1.1.0 255.255.255.0 import toate

default-router 10.1.1.1
închiriere 0 2

ip dhcp excluded-address 10.1.1.1

server ip dns
ip dns vizualizare implicit
implicit dns forwarder
redirecționare dns implicită
căutarea implicită a domeniului
Interfață implicită nume de
domeniu-server Cellular0/1/0
descriere adresa IP primary_wan
negociată
dialer în bandă
dialer-grup 1
timpul pulsului 1
închidere
nicio oprire
ip nat afara
Ieșire
dialer-list 1 protocol ip permis

controler Cellular 0/1/0
lte sim data-profile 2 attach-profile 2 slot 0

ruta ip 0.0.0.0 0.0.0.0 Cellular0/1/0

ip nat în lista sursă 197 interfață Cellular0/1/0 supraîncărcare lista de acces 197
permite ip orice

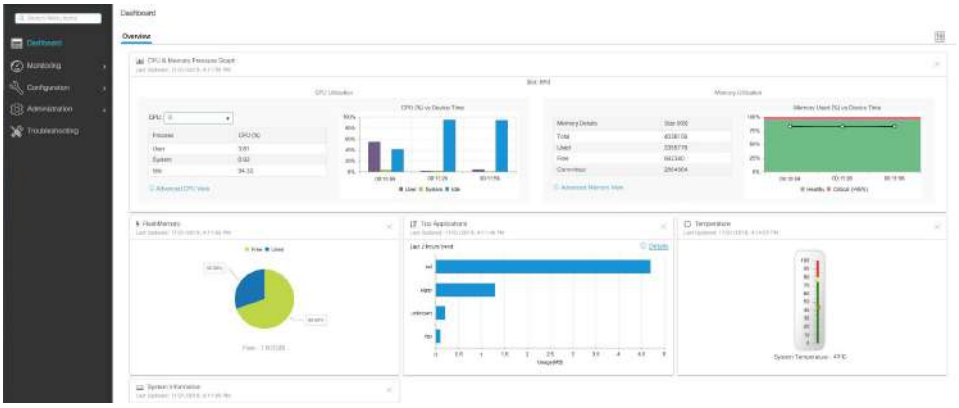
Tabloul de bord WebUI

După finalizarea configurării Zilei 0, WebUI poate fi acum utilizată pentru administrarea zilnică. WebUI se deschide către un tablou de bord ușor de utilizat.

Nota Suportul pentru funcția WebUI poate varia în funcție de licența și tipul de platformă a dispozitivului dvs.

Următoarea figură prezintă tabloul de bord:

Figura 22: Tabloul de bord



Următorul tabel oferă o prezentare generală a tabloului de bord.

Bord	Vizualizați dashlet-uri care vă oferă un instantaneu al procesului și al utilizării memoriei și informații despre sistem.
Monitorizare	Monitorizați-vă rețeaua zilnic și efectuați alte operațiuni ad-hoc legate de inventarul dispozitivelor din rețea și gestionarea configurației.
Configurare	Configurați-vă dispozitivul.
Administrare	Specificați setările de configurare a sistemului și setările de administrare a utilizatorilor.
Depanare	Depanați problemele de conectivitate și pierderile de pachete utilizând Ping și Traceroute și monitorizați starea și performanța dispozitivului folosind jurnalele de server web și jurnalele de sistem.

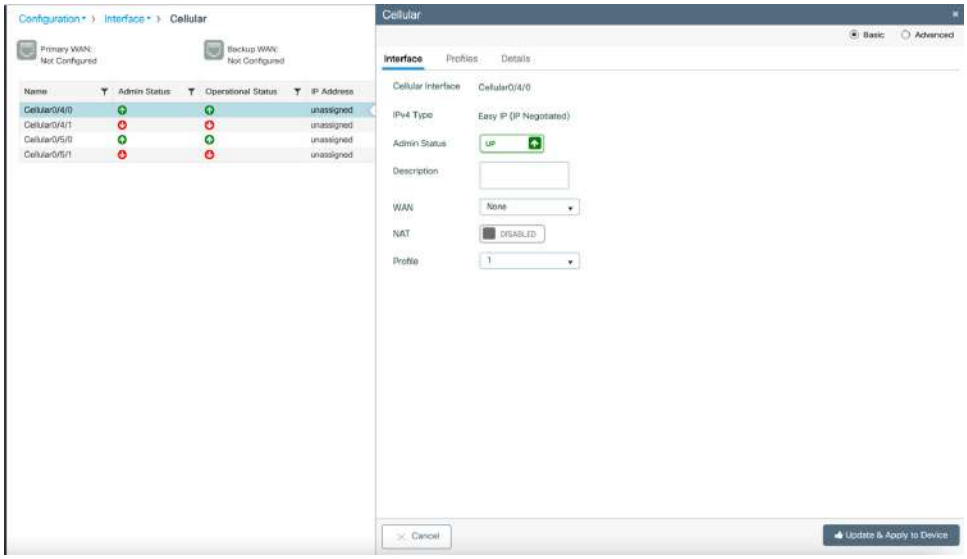
Nume punct de acces Cisco WebUI (APN)

IOS XE 17.9.1 a adăugat posibilitatea de a adăuga, edita sau șterge APN din interfața CiscoWebUI. Următoarele oferă o privire de ansamblu asupra modului în care se realizează această funcție.

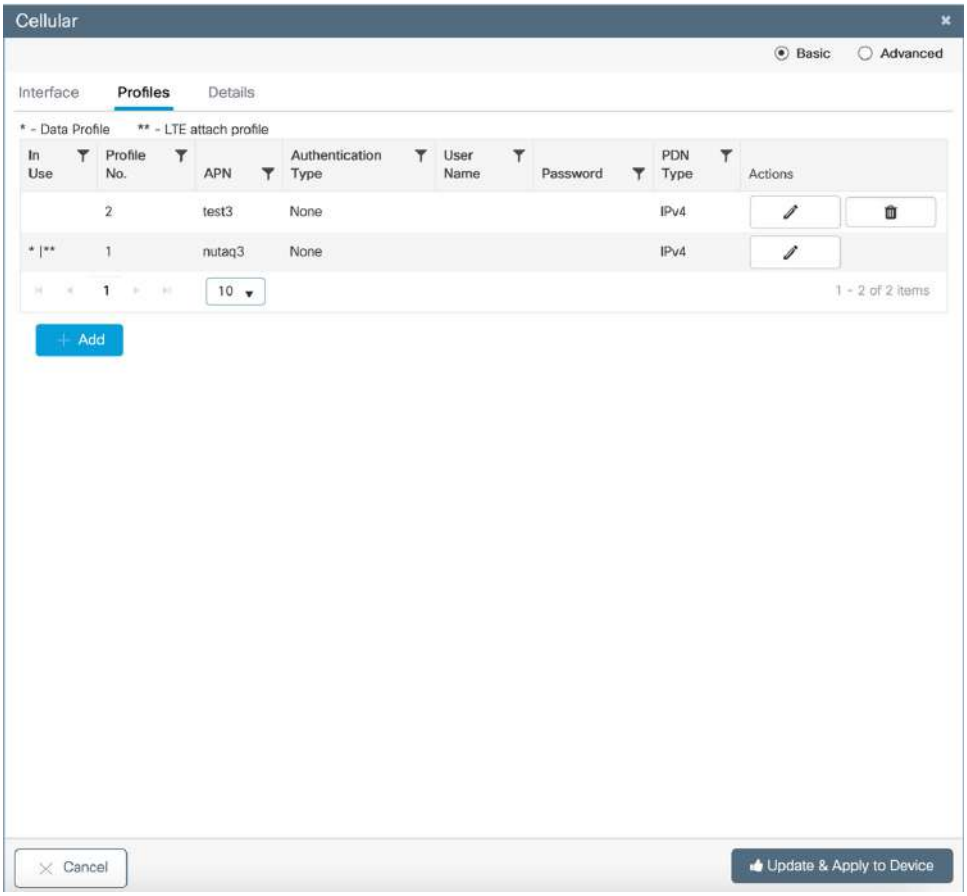
Nota Această secțiune descrie doar noi funcționalități și nu este o prezentare completă a WebUI.

Adăugarea APN-ului

Din WebUI, navigați la**Configurare > Interfață > Cellular**. Faceți dublu clic pe interfața celulară bazată pe platforma dvs.



În fereastra Cellular, faceți clic pe**Profiluri**fila.

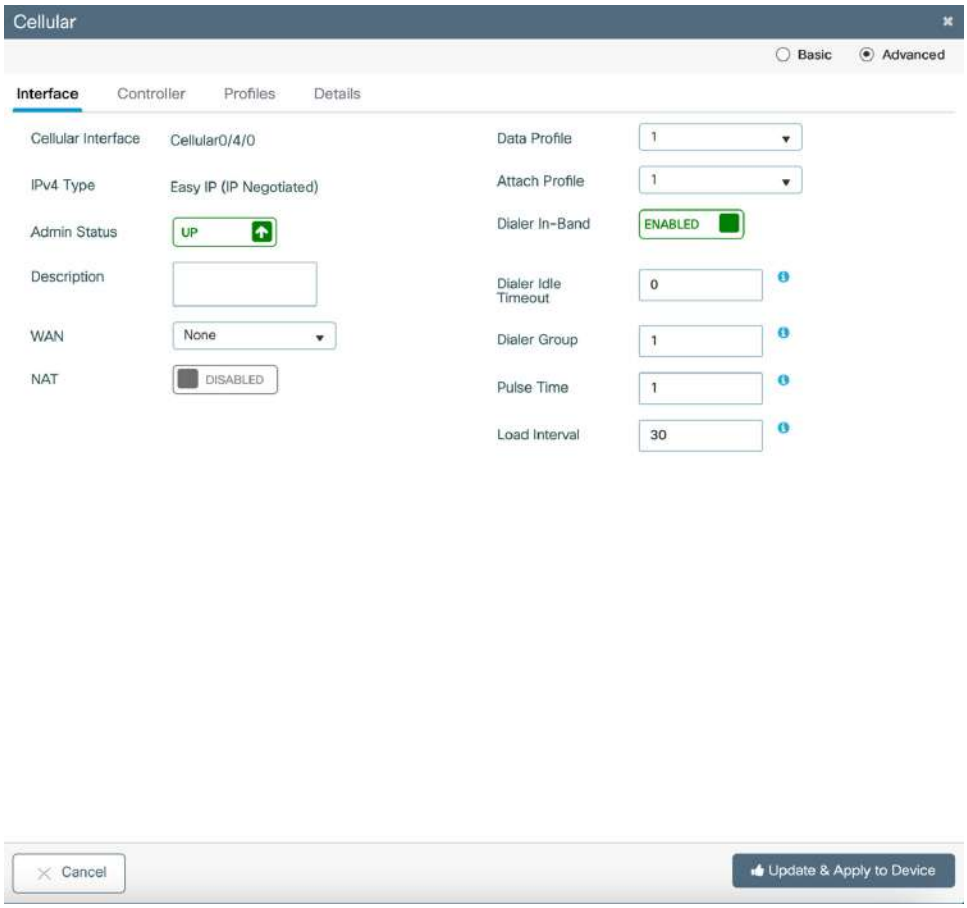


De la**Profiluri**fila, puteți adăuga, șterge sau edita APN. Odată ce profilul este modificat, faceți clic pe**Actualizați și aplicați pe dispozitiv**în partea de jos a ferestrei.

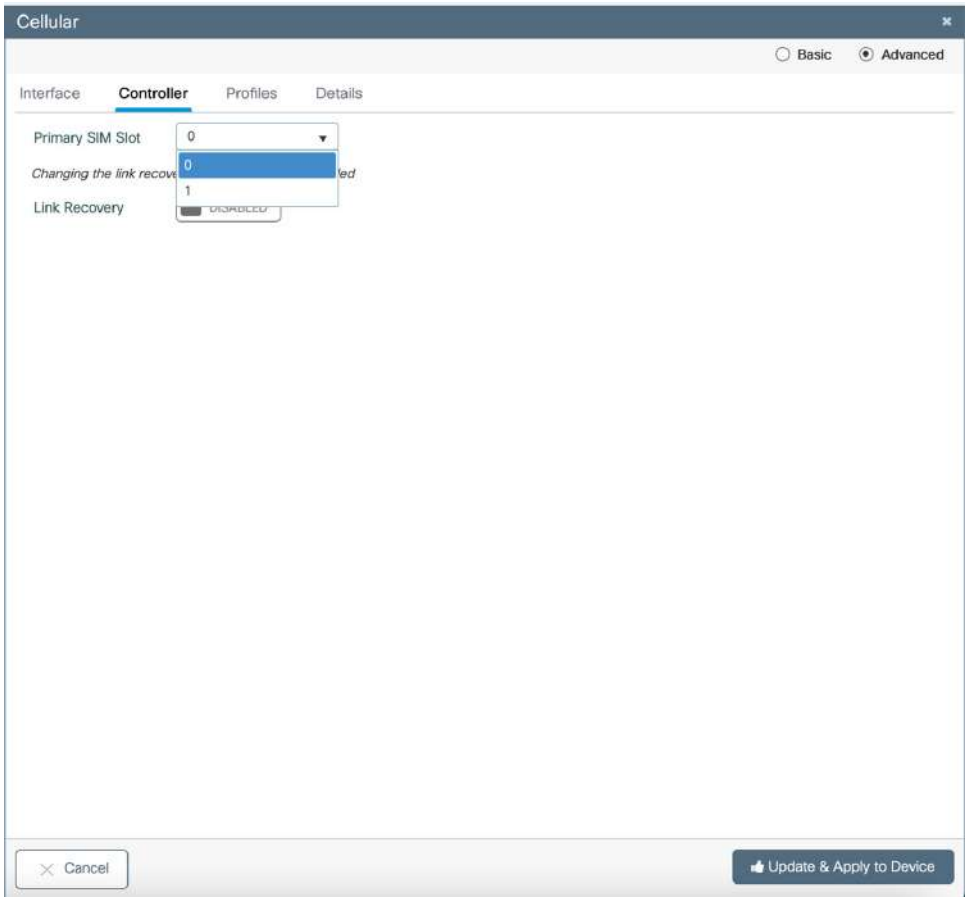
Schimbarea slotului SIM

În mod implicit, APN-ul este atașat la slotul SIM 0. Puteți schimba APN-ul în slotul SIM 1 utilizând WebUI.

Din WebUI, navigați la**Configurare > Interfață > Cellular**. Faceți clic pe**Avansat**butonul radio din partea de sus a ferestrei.



Faceți clic pe**Controlor**fila din partea de sus a ferestrei.



Faceți clic pe meniul derulant Primary SIMSlot și selectați slotul 1. Faceți clic pe**Actualizați și aplicați pe dispozitiv**în partea de jos a ferestrei.

CAPITOL 5

Shell Securizat

Această secțiune conține următoarele subiecte:

Informații despre Secure Shell

Secure Shell (SSH) este un protocol care oferă o conexiune sigură, la distanță, la un dispozitiv. SSH oferă mai multă securitate pentru conexiunile la distanță decât o face Telnet, oferind o criptare puternică atunci când un dispozitiv este autentificat. Această versiune de software acceptă SSH Versiunea 1 (SSHv1) și SSH Versiunea 2 (SSHv2).

Cerințe preliminare pentru configurarea Secure Shell

Următoarele sunt condițiile preliminare pentru configurarea dispozitivului pentru shell securizat (SSH):

- Pentru ca SSH să funcționeze, comutatorul are nevoie de o pereche de chei publice/private RSA.
- Serverul Secure Shell (SSH) necesită o imagine software de criptare IPsec (Data Encryption Standard [DES] sau 3DES); clientul SSH necesită o imagine software de criptare IPsec (DES sau 3DES).
- Configurați un nume de gazdă și un domeniu de gazdă pentru dispozitivul dvs. utilizând comenzile nume de gazdă și nume de domeniu ip în modul de configurare globală. Utilizați**nume de gazdă**și**IP nume-domeniu**comenzi în modul de configurare globală.

Restricții pentru configurarea Secure Shell

Următoarele sunt restricții pentru configurarea routerului pentru shell securizat.

- Routerul acceptă autentificarea RSA.
- SSH acceptă numai aplicația execution-shell.
- Serverul SSH și clientul SSH sunt acceptate numai pe software-ul de criptare a datelor Standard (DES) (56 de biți) și 3DES (168 de biți). În imaginile software DES, DES este singurul algoritm de criptare disponibil. În imaginile software 3DES, sunt disponibili atât algoritmii de criptare DES, cât și 3DES.

Nota Cisco recomandă cu căldură criptarea 3DES deoarece este mai puternică. Consultați ghidul de întărire a dispozitivului Cisco IOS-XE lahttps://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.htmlpentru detalii.

- Această versiune software acceptă IP Security (IPSec).
- Routerul acceptă algoritmul de criptare Advanced Encryption Standard (AES) cu o cheie de 128 de biți, o cheie de 192 de biți sau o cheie de 256 de biți. Cu toate acestea, cifrul simetric AES pentru a cripta cheile nu este acceptat.
- Bannerul de conectare nu este acceptat în Secure Shell Versiunea 1. Este acceptat în Secure Shell Versiunea 2, pe care Cisco îl recomandă datorită securității sale mai bune.
- Cuvântul cheie -l și userid :{number} {ip-address} delimitator și argumente sunt obligatorii la configurarea metodei alternative de Reverse SSH pentru accesul la consolă.

Acces SSH și router

Secure Shell (SSH) este un protocol care oferă o conexiune sigură, la distanță, la un dispozitiv. SSH oferă mai multă securitate pentru conexiunile la distanță decât o face Telnet, oferind o criptare puternică atunci când un dispozitiv este autentificat. Această versiune de software acceptă SSH Versiunea 1 (SSHv1) și SSH Versiunea 2 (SSHv2). SSH funcționează la fel în IPv6 ca și în IPv4. Pentru IPv6, SSH acceptă adrese IPv6 și permite conexiuni securizate, criptate cu noduri IPv6 la distanță printr-un transport IPv6.

Servere SSH, clienți integrați și versiuni acceptate

Caracteristica Secure Shell (SSH) Integrated Client este o aplicație care rulează prin protocolul SSH pentru a oferi autentificare și criptare a dispozitivului. Clientul SSH permite unui dispozitiv Cisco să realizeze o conexiune sigură, criptată la un alt dispozitiv Cisco sau la orice alt dispozitiv care rulează serverul SSH. Această conexiune oferă o funcționalitate similară cu cea a unei conexiuni Telnet de ieșire, cu excepția faptului că conexiunea este criptată. Cu autentificare și criptare, clientul SSH permite comunicarea sigură printr-o rețea nesecurizată.

Serverul SSH și clientul integrat SSH sunt aplicații care rulează pe comutator. Serverul SSH funcționează cu clientul SSH acceptat în această versiune și cu clienții SSH non-Cisco. Clientul SSH funcționează cu servere SSH disponibile public și comercial. Clientul SSH acceptă cifrurile Standardului de criptare a datelor (DES), 3DES și autentificarea prin parolă.

Nota Funcționalitatea client SSH este disponibilă numai atunci când serverul SSH este activat.

Autentificarea utilizatorului se realizează astfel în sesiunea Telnet către dispozitiv. SSH acceptă, de asemenea, următoarele metode de autentificare a utilizatorului:

- TACACS+
- RAZA
- Autentificare și autorizare locală

Ghid de configurare SSH

Urmați aceste instrucțiuni atunci când configurați dispozitivul ca server SSH sau client SSH:

- O pereche de chei RSA generată de un server SSHv1 poate fi utilizată de un server SSHv2 și invers.
- Dacă primiți mesaje de eroare CLI după introducerea**cheie cripto genera rsa global**comanda de configurare, o pereche de chei RSA nu a fost generată. Reconfigurați numele de gazdă și domeniul, apoi introduceți**cheie cripto genera rsa**comanda.
- Când se generează perechea de chei RSA, mesajul*Nu a fost specificat niciun nume de gazdă*ar putea apărea. Dacă se întâmplă, trebuie să configurați un nume de gazdă IP utilizând**nume de gazdă**comanda de configurare globală.
- La generarea perechii de chei RSA, poate apărea mesajul Niciun domeniu specificat. Dacă se întâmplă, trebuie să configurați un nume de domeniu IP utilizând**IP nume-domeniu**comanda de configurare globală.
- Când configurați metoda locală de autentificare și autorizare, asigurați-vă că AAA este dezactivat pe consolă.

Cum se configurează Secure Shell

Această secțiune conține următoarele:

Configurarea routerului pentru a rula SSH

Urmați procedura de mai jos pentru a configura dispozitivul să ruleze SSH:

Înainte de a începe

Configurați autentificarea utilizatorului pentru acces local sau de la distanță. Acest pas este necesar. Pentru mai multe informații, consultați Subiectele conexe de mai jos.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** router>**permite**	Activează modul EXEC privilegiat. • Introduceți parola dacă vi se solicită.
Pasul 2	**configura terminalul** **Exemplu:** router#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**nume de gazdă***nume de gazdă* **Exemplu:**	Configurați un nume de gazdă și un nume de domeniu IP pentru dispozitivul dvs.

	Comanda sau Acțiune	Scop
	router(config)#**nume de gazdă***numele_gazdă*	**Nota** Urmați această procedură numai dacă configurați dispozitivul ca server SSH.
Pasul 4	**IP nume-domeniu***nume_domeniu* **Exemplu:** router(config)#**IP nume-domeniu** *numele_domeniului_dvs*	Configurați un domeniu gazdă pentru dispozitivul dvs.
Pasul 5	**cheie cripto genera rsa** **Exemplu:** router(config)#**cheie cripto genera rsa**	Activează serverul SSH pentru autentificare locală și de la distanță pe dispozitiv și generează o pereche de chei RSA. Generarea unei perechi de chei RSA pentru dispozitiv activează automat SSH. Vă recomandăm o dimensiune minimă a modulului de 1024 de biți. Când generați chei RSA, vi se solicită să introduceți o lungime a modulului. O lungime mai mare a modulului poate fi mai sigură, dar este nevoie de mai mult timp pentru a genera și a utiliza. **Nota** Urmați această procedură numai dacă configurați dispozitivul ca server SSH.
Pasul 6	**Sfârşit** **Exemplu:** router(config)#**Sfârşit**	Revine la modul EXEC privilegiat.
Pasul 7	**arată rularea-config** **Exemplu:** router#**arată rularea-config**	Vă verifică intrările.
Pasul 8	**copiați running-config startup-config** **Exemplu:** router#**copiați running-config startup-config**	(Opțional) Salvează intrările dvs. în fișierul de configurare.

Configurarea serverului SSH

Urmați acești pași pentru a configura serverul SSH:

Nota Această procedură este necesară numai dacă configurați dispozitivul ca server SSH.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** router>**permite**	Activează modul EXEC privilegiat. • Introduceți parola dacă vi se solicită.
Pasul 2	**configura terminalul** **Exemplu:** router#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**versiunea ip ssh**[**2**] **Exemplu:** router(config)#**ip ssh versiunea 2**	(Opțional) Configura dispozitivul să ruleze SSH versiunea 2. Dacă nu introduceți această comandă sau nu specificați un cuvânt cheie, serverul SSH selectează cea mai recentă versiune SSH acceptată de clientul SSH. De exemplu, dacă clientul SSH acceptă SSHv1 și SSHv2, serverul SSH selectează SSHv2.
Pasul 4	**ip ssh**{**pauză***secunde*| **reîncercări de autentificare***număr*} **Exemplu:** router(config)#**ip ssh timeout 90 ip ssh autentificare-reîncercări 2**	Configurați parametrii de control SSH: • Specificați valoarea time-out-ului în secunde; valoarea implicită este de 120 de secunde. Intervalul este de la 0 la 120 de secunde. Acest parametru se aplică fazei de negociere SSH. După conexiunea este stabilită, dispozitivul utilizează valorile implicite de time-out ale sesiunilor bazate pe CLI. În mod implicit, sunt disponibile până la cinci conexiuni SSH simultane, criptate pentru mai multe sesiuni bazate pe CLI prin rețea (sesiunea 0 până la sesiunea 4). După ce pornește shell-ul de execuție, valoarea de expirare a sesiunii bazată pe CLI revine la valoarea implicită de 10 minute. • Specificați de câte ori un client se poate re-autentifica pe server. Valoarea implicită este 3; intervalul este de la 0 la 5.

	Comanda sau Acțiune	Scop
		Repetați acest pas când configurați ambii parametri.
Pasul 5	Utilizați unul sau ambele dintre următoarele: • **linia vty***line_number*[*numărul rândului final*] • **intrare de transport ssh** **Exemplu:** router(config)#**linia vty 1 10** sau router (linie de configurare) #**intrare de transport ssh**	(Opțional) Configurați setările liniei terminale virtuale. • Intră în modul de configurare a liniei pentru a configura setările liniei terminalului virtual. Pentru*line_number*și *număr_linie_terminală* argumente, intervalul este de la 0 la 15. • Specifică faptul că dispozitivul împiedică conexiunile Telnet non-SSH, limitând dispozitivul doar la conexiuni SSH.
Pasul 6	**Sfârşit** **Exemplu:** router (linie de configurare) #**Sfârşit**	Iese din modul de configurare a liniei și revine la modul EXEC privilegiat.
Pasul 7	**arată rularea-config** **Exemplu:** router#**arată rularea-config**	Vă verifică intrările.
Pasul 8	**copiați running-config startup-config** **Exemplu:** router#**copiați running-config startup-config**	(Opțional) Salvează intrările dvs. în fișierul de configurare.

Monitorizarea configurației și stării SSH

Tabelul 4: Comenzi pentru afișarea configurației și stării serverului SSH

Comanda	Scop
arata ip ssh	Afișează versiunea și informațiile de configurare pentru serverul SSH.
arată ssh	Afișează starea serverului SSH.

Configurarea routerului pentru autentificare și autorizare locală

Puteți configura AAA să funcționeze fără un server setând comutatorul pentru a implementa AAA în modul local. Routerul se ocupă apoi de autentificare și autorizare. Nu este disponibilă nicio contabilitate în această configurație.

Urmați acești pași pentru a configura AAA să funcționeze fără un server, setând routerul să implementeze AAA în modul local:

Nota Pentru a securiza routerul pentru acces HTTP prin utilizarea metodelor AAA, trebuie să configurați routerul cu comanda de configurare globală aaa ip http authentication. Configurarea autentificării AAA nu securizează routerul pentru acces HTTP prin utilizarea metodelor AAA.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** router>**permite**	Activează modul EXEC privilegiat. • Introduceți parola dacă vi se solicită.
Pasul 2	**configura terminalul** **Exemplu:** router#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**aaa nou-model** **Exemplu:** router(config)#**aaa nou-model**	Activează AAA
Pasul 4	**aaa autentificare locală implicită de conectare** **Exemplu:** router(config)#**aaa autentificare locală implicită de conectare**	Setează autentificarea de conectare pentru a utiliza baza de date locală de nume de utilizator. Cuvântul cheie implicit aplică autentificarea bazei de date a utilizatorului local la toate porturile.
Pasul 5	**aaa autorizare exec local** **Exemplu:** router (linie de configurare) #**aaa autorizare exec local**	Configurați autorizarea AAA a utilizatorului, verifică baza de date locală și permite utilizatorului să ruleze un shell EXEC.
Pasul 6	**aaa rețea de autorizare locală** **Exemplu:** router (linie de configurare) #**aaa rețea de autorizare locală**	Configurați autorizarea AAA a utilizatorului pentru toate solicitările de servicii legate de rețea.

	Comanda sau Acțiune	Scop
Pasul 7	**nume de utilizator***nume***privilegiu***nivel* **parolă** *parola de tip criptare* **Exemplu:** router (linie de configurare) #**nume de utilizator *numele_de_utilizator*privilegiu 1 parola 7 secret567**	Intră în baza de date locală și stabilește un sistem de autentificare bazat pe nume de utilizator. Repetați această comandă pentru fiecare utilizator. **o.**Pentru*nume*, specificați ID-ul utilizatorului ca un singur cuvânt. Spațiile și ghilimelele nu sunt permis. **b.**(Opțional) Pentru*nivel*, specificați nivelul de privilegii pe care îl are utilizatorul după obținerea accesului. Intervalul este de la 0 la 15. Nivelul 15 oferă acces privilegiat în modul EXEC. Nivelul 0 oferă utilizatorului acces în modul EXEC. **c.**Pentru tipul de criptare, introduceți 0 pentru a specifica că urmează o parolă necriptată. Introduceți 7 pentru a specifica că urmează o parolă ascunsă. **d.**Pentru parolă, specificați parola pe care trebuie să o introducă utilizatorul pentru a avea acces la comutator. Parola trebuie să aibă între 1 și 25 de caractere, poate conține spații încorporate și trebuie să fie ultima opțiune specificat în comanda nume de utilizator.
Pasul 8	**Sfârşit** **Exemplu:** router (linie de configurare) #**Sfârşit**	Iese din modul de configurare a liniei și revine la modul EXEC privilegiat.
Pasul 9	**arată rularea-config** **Exemplu:** router#**arată rularea-config**	Vă verifică intrările.
Pasul 10	**copiați running-config startup-config** **Exemplu:** router#**copiați running-config startup-config**	(Opțional) Salvează intrările dvs. în fișierul de configurare.

Informații despre Secure Copy

Caracteristica Secure Copy Protocol (SCP) oferă o metodă sigură și autentificată pentru copierea configurației routerului sau a fișierelor imagine a routerului. SCP se bazează pe Secure Shell (SSH), o aplicație și un protocol care oferă un înlocuitor sigur pentru Berkeley r-tools.

Cerințe preliminare pentru copiere securizată

Următoarele sunt condițiile preliminare pentru configurarea dispozitivului pentru shell securizat (SSH):

- Înainte de a activa SCP, trebuie să configurați corect SSH, autentificarea și autorizarea pe switch.
- Deoarece SCP se bazează pe SSH pentru transportul său securizat, routerul trebuie să aibă o pereche de chei RSA.
- SCP se bazează pe SSH pentru securitate.
- SCP necesită configurarea autorizației de autentificare, autorizare și contabilitate (AAA) astfel încât routerul să poată determina dacă utilizatorul are nivelul corect de privilegii.
- Un utilizator trebuie să aibă autorizația corespunzătoare pentru a utiliza SCP.
- Un utilizator care are autorizarea corespunzătoare poate utiliza SCP pentru a copia orice fișier din sistemul de fișiere Cisco IOS (IFS) către și de la un comutator, folosind**copie**comanda. Un administrator autorizat poate face acest lucru și de la o stație de lucru.

Restricții pentru configurarea copiei securizate

- Înainte de a activa SCP, trebuie să configurați corect SSH, autentificarea și autorizarea pe router.
- Când utilizați SCP, nu puteți introduce parola în**copie**comanda. Trebuie să introduceți parola când vi se solicită.

Configurarea copiei securizate

Pentru a configura routerul Cisco pentru funcționalitatea serverului Secure Copy (SCP), parcurgeți următorii pași.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** router> activare	Activează modul EXEC privilegiat. • Introduceți parola dacă vi se solicită.
Pasul 2	**configura terminalul** **Exemplu:** router# configura terminalul	Intră în modul de configurare globală.
Pasul 3	**aaa nou-model** **Exemplu:** router(config)# aaa nou-model	Setează autentificarea AAA la conectare.
Pasul 4	**aaa autentificare autentificare**{**implicit** | *nume-listă}*Activează sistemul de control al accesului AAA. *metoda 1 [metoda 2...*]	

	Comanda sau Acțiune	Scop
	Exemplu: router(config)# aaa autentificare autentificare grup implicit tacacs+	
Pasul 5	**nume de utilizator** *nume* [**privilegiu** *nivel*] **parolă** *parola criptată de tip criptare* **Exemplu:** router(config)# nume utilizator privilegiu superutilizator 2 parolă 0 superparolă	Stabilește un sistem de autentificare bazat pe nume de utilizator. **Nota** Puteți omite acest pas dacă a fost configurat un mecanism de autentificare bazat pe rețea, cum ar fi TACACS+ sau RADIUS.
Pasul 6	**activare server ip scp** **Exemplu:** router(config)# ip scp server activat	Activează funcționalitatea SCP pe partea serverului.
Pasul 7	**Ieșire** **Exemplu:** router(config)# exit	Iese din modul de configurare globală și revine la modul EXEC privilegiat.
Pasul 8	**arată rularea-config** **Exemplu:** router# show running-config	(Opțional) Afișează funcționalitatea serverului SCP.
Pasul 9	**depanare ip scp** **Exemplu:** router# depanare ip scp	(Opțional) Depanează problemele de autentificare SCP.

Exemplu

router#**copie scp***<un fișier>***your_username@remotehost:/***<unele/la distanță/director>**

Referințe suplimentare

Următoarele secțiuni oferă referințe legate de caracteristica SSH.

Subiect înrudit	Titlul documentului
Configurarea politicilor IdentityControl și a șabloanelor Identity Service pentru rețelele Session Aware.	SessionAwareNetworkingConfigurationGuide, Cisco IOSXEElease 3SE: https://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.pdf

Subiect înrudit	Titlul documentului
Configurarea RADIUS, TACACS+, Secure Shell, 802.1X și AAA.	Ghid de configurare Secure Shell, Cisco IOS XE Gibraltar 16.11.x: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-11/configuration_guide/sec/b_1611_sec_9500_cg/configuring_secure_shell__ssh_.html

CAPITOL 6

Cronometrare NTP bazată pe ceasul GPS

Acest capitol conține următoarele secțiuni:

Configurarea NTP folosind Ora GPS

Puteți configura ora GPS ca ceas de referință pentru NTP folosind comanda**ntp refclock gps**.

Nota Această caracteristică este disponibilă cu versiunea IOS XE 17.6.1. Mai multe informații pot fi găsite înSincronizarea ceasului NTP cu GPSînGhid de configurare a modulului de interfață conectabilă celulară.

Ora GPS acționează ca o sursă de strat 0, iar serverul Cisco IOS NTP acționează ca un dispozitiv de strat 1, care, la rândul său, oferă informații despre ceas clienților săi NTP (stratul 2 și 3).

Procedură

Pasul 1 Intrați în modul de configurare globală:

Exemplu:

Router#**configura terminalul**

Pasul 2 Configurați ceasul de referință NTP ca GPS:

Exemplu:

Router(config)#**ntp refclock gps**

Pasul 3 Pentru a verifica configurația, utilizați**spectacol**comenzi din exemplul următor:

Exemplu:

Router#
24 septembrie 19:58:43.046 GMT: %PKI-6-AUTHORITATIVE_CLOCK: Ceasul sistemului a fost setat. Router#**arată starea ntp**
Ceasul este sincronizat, stratul 1, referința este .GPS.
frecvența nominală este de 250,0000 Hz, frecvența reală este de 249,9970 Hz, precizia este de 2**10

Timpul de funcționare ntp este de 94000 (1/100 de secunde), rezoluția este de 4016. Timpul de referință este E31778F3.0B851ED8 (19:58:43.045 GMT Joi, 24 septembrie 2020) offset-ul ceasului este de 11,0000 msec, întârzierea rădăcină este de 0 ms.
Dispersia rădăcină este 3950,55 msec, dispersia peer este de 3938,47 msec starea filtrului buclă este „CTRL” (Bucla controlată normală), deriva este 0,000011995 s/s Intervalul de sondare a sistemului este 64, ultima actualizare a fost acum 7 secunde.
Router#
Router#
Router#**arata asociatii ntp**

adresa ref clock st când sondaj atinge întârziere offset disp
* ~127.127.5.1 .GPS. 0 38 64 7 0,000 11,000 1938,8
* sys.peer, # selectat, + candidat, - outlyer, x falseticker, ~ Router configurat#

Router#**arată ceasul**
20:00:43.660 GMT joi, 24 septembrie 2020
Router#

Pasul 4 Utilizați**depanare ntp refclock**comandă pentru depanarea configurației:

Exemplu:

Router#**depanare ntp?** ajustați
ajustările ceasului NTP toate NTP
toate depanarea pe mesajele de bază
NTP de bază
evenimente evenimente NTP
pachet NTP depanare pachet refclock
mesaje refclock NTP

Router#**depanare ntp refclock**
* 24 septembrie 19:58:43.045 GMT: GPS: Sondaj solicitat
* 24 septembrie 19:58:43.045 GMT: GPS (19:58:43.056 GMT joi, 24 septembrie 2020)
* 24 septembrie 19:58:43.045 GMT: rcvd oră validă de pe GPS: 24/09/2020 19:58:43.056 (frac = 0x0E560440)

* 24 septembrie 19:58:43.045 GMT: marcajul de timp al sondajului RTS (ceas local) a fost 0xE31778F3.0B851ED8
* 24 septembrie 19:58:43.045 GMT: marcajul de timp GPS este 0xE31778F3.0E560440
* 24 septembrie 19:58:43.045 GMT: NTP Core (OBSERVAT): ntpd PPM
* 24 septembrie 19:58:43.046 GMT: NTP Core (OBSERVAT): trans state: 5
* 24 septembrie 19:58:43.046 GMT: NTP Core (OBSERVAT): Ceasul este sincronizat.

CAPITOL 7

Gestionarea fișierelor de configurare

Acest capitol conține următoarele secțiuni:

Înțelegerea fișierelor de configurare

Fișierele de configurare conțin comenzile software Cisco IOS XE utilizate pentru a personaliza funcționalitatea dispozitivului de rutare Cisco (router, server de acces, comutator și așa mai departe). Comenzile sunt analizate (traduse și executate) de către software-ul Cisco IOS XE atunci când sistemul este pornit (din fișierul de pornire-configurare) sau când introduceți comenzi la CLI într-un mod de configurare.

Tipuri de fișiere de configurare

Fișierele de configurare de pornire (startup-config) sunt utilizate în timpul pornirii sistemului pentru a configura software-ul. Fișierele de configurare de rulare (running-config) conțin configurația curentă a software-ului. Cele două fișiere de configurare pot fi diferite. De exemplu, este posibil să doriți să modificați configurația pentru o perioadă scurtă de timp, mai degrabă decât definitiv. În acest caz, veți schimba configurația de rulare folosind comanda configure terminal EXEC, dar nu veți salva configurația folosind comanda copy running-config startup-config EXEC.

Pentru a modifica configurația de rulare, utilizați comanda configure terminal. Pe măsură ce utilizați modurile de configurare Cisco IOS XE, comenzile sunt în general executate imediat și sunt salvate în fișierul de configurare care rulează fie imediat după ce le introduceți, fie când părăsiți un mod de configurare.

Pentru a modifica fișierul de configurare de pornire, puteți fie să salvați fișierul de configurare care rulează în configurația de pornire utilizând comanda copy running-config startup-config EXEC, fie să copiați un fișier de configurare de pe un server de fișiere în configurația de pornire.

Locația fișierelor de configurare

Fișierele de configurare pot fi stocate în următoarele locații:

- Configurația de rulare este stocată în RAM.
- Configurația de pornire este stocată în locația specificată de variabila de mediu CONFIG_FILE.

  Variabila CONFIG_FILE este implicită la NVRAM și poate fi un fișier în următoarele sisteme de fișiere:

- nvram: (NVRAM)
- bootflash: (memorie flash internă)
- usbflash0: (media USB externă)

Găsirea versiunii software

Fișierele pachetului pentru software-ul Cisco IOS XE pot fi găsite pe dispozitivul flash de pe placa de sistem (flash:) sau pe unul dintre dispozitivele externe menționate anterior.

Puteți folosi**arata versiunea**comanda EXEC privilegiată pentru a vedea versiunea software care rulează pe dispozitivul dvs.

Nota Deși cel**arata versiunea**ieșirea arată întotdeauna imaginea software care rulează pe dispozitiv, numele modelului afișat la sfârșitul acestui afișaj este configurația din fabrică și nu se modifică dacă actualizați licența software.

De asemenea, puteți utiliza**dir***sistem de fișiere*: comandă EXEC privilegiată pentru a vedea numele directoarelor altor imagini software pe care le-ați putea stoca în memoria flash.

Gestionarea și configurarea unui pachet consolidat utilizând comenzile de copiere și pornire

Pentru a actualiza un pachet consolidat, copiați pachetul consolidat în directorul bootflash: de pe router. După ce faceți această copie a pachetului consolidat, configurați routerul să pornească folosind fișierul pachetului consolidat.

Următorul exemplu arată fișierul pachet consolidat care este copiat în sistemul de fișiere bootflash:. Registrul de configurare este apoi setat să pornească folosind comenzile sistemului de pornire, iar comenzile indică ruterului să pornească folosind pachetul consolidat stocat în sistemul de fișiere bootflash:. Noua configurație este apoi salvată folosind comanda copy running-config startup-config, iar sistemul este apoi reîncărcat pentru a finaliza procesul.

Afișați conținutul directorului bootflash.

```
Router#dir bootflash:
Directorul de bootflash:/ 13
          drwx          278528  19 mai 2022 05:20:04 +00:00 17 mai   tracelogs
11        drwx            4096  2022 14:24:54 +00:00 17 mai 2022     . instalator
84        drwx           20480  14:22:00 +00:00 17 mai 2022          license_evlog
83        -rw-              30  14:21:41 +00:04:00 17 mai 2022       throughput_monitor_params .
12        drwx            4096  +00:00 17 mai 2022 14:20:50 +00:00   prst_sync
22        -rw-             335  17 mai 2022 14:20:39 +00:00 17 mai   boothelper.log
14        - rwx          41040  2022 12:54:32 +00:00                 mode_event_log
259       -rw-       682679541
ir1800-universalk9.17.07.01.SPA.bin
```

Copiați noua imagine în directorul bootflash:.

Nota Pentru a utiliza copierea securizată (scp), trebuie mai întâi să configurați o configurație SSH. VedeaConfigurarea Secure Shell.

Router#**copie scp: bootflash:**
Adresa sau numele gazdei la distanță []? 192.168.1.2 Nume de
utilizator sursă [xxxxx]?**Intră**
Nume fișier sursă []? /auto/users/IR1800-universalk9.17.08.01.SPA.bin Nume fișier de
destinație [IR1800-universalk9.17.08.01.SPA.bin]?

Acesta este un dispozitiv gestionat de Cisco care poate fi utilizat numai în scopuri autorizate. Utilizarea
dvs. este monitorizată pentru securitate, protecția activelor și conformitatea cu politicile.

Parolă:**<parola-voastra>**
Moduri de trimitere fișier: C0644 208904396 IR1800-universalk9.17.08.01.SPA.bin . . . . . .

[OK - 208904396 octeți]
208904396 octeți copiați în 330,453 secunde (632176 octeți/sec)

Afișează conținutul directorului bootflash:.

Router#**dir bootflash:**
Directorul de bootflash:/ 13
drwx 278528 19 mai 2022 05:20:04 +00:00 17 mai tracelogs
11 drwx 4096 2022 14:24:54 +00:00 17 mai 2022 . instalator
84 drwx 20480 14:22:00 +00:00 17 mai 2022 license_evlog
83 -rw- 30 14:21:41 +00:04:00 17 mai 2022 throughput_monitor_params .
12 drwx 4096 +00:00 17 mai 2022 14:20:50 +00:00 prst_sync
22 -rw- 335 17 mai 2022 14:20:39 +00:00 17 mai boothelper.log
14 - rwx 41040 2022 12:54:32 +00:00 mode_event_log
259 -rw- 682679541
ir1800-universalk9.17.07.01.SPA.bin 12
-rw- 208904396 17 mai 2022 16:17:34 -07:00
ir1800-universalk9.17.08.01.SPA.bin

Configurați routerul să pornească folosind fișierul pachet consolidat.

Router#**configura terminalul**
Introduceți comenzile de configurare, una pe linie. Încheiați cu CNTL/Z. Router(config)#**sistem de pornire bootflash:ir1800-universalk9.17.08.01.SPA.bin** Router(config)#**Ieșire**

Verificați modificarea configurației.

Router#**show run | include boot** boot-
start-marker
sistemul de pornire bootflash:IR1800-universalk9.17.08.01.SPA.bin boot-end-
marker

Copiați configurația care rulează și salvați-o. Apoi, când reîncărcați routerul, acesta repornește cu configurația salvată.

Router#**copiați running-config startup-config** Nume fișier de
destinație [startup-config]?**<intra>** Configurare clădire... [OK]

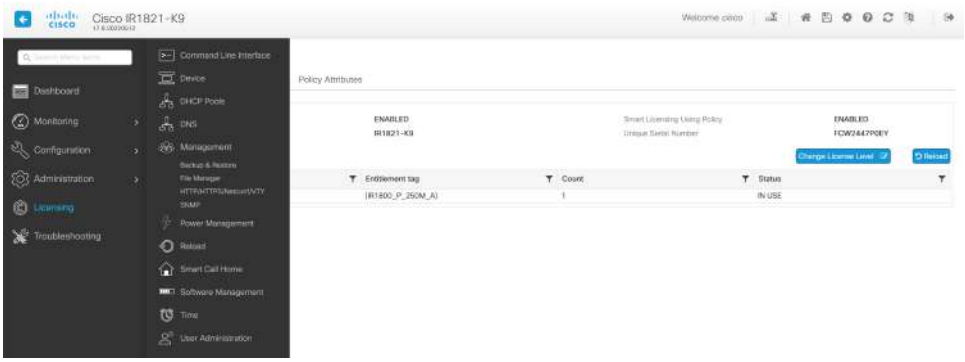
Router#**reîncărcați**
Continuați cu reîncărcarea? [confirma]**<intra>**
Dec 04 17:42:54.445 R0/0: %PMAN-5-EXITACTION: Managerul de proces iese: ieșirea procesului cu reîncărcare

Se inițializează hardware-ul...

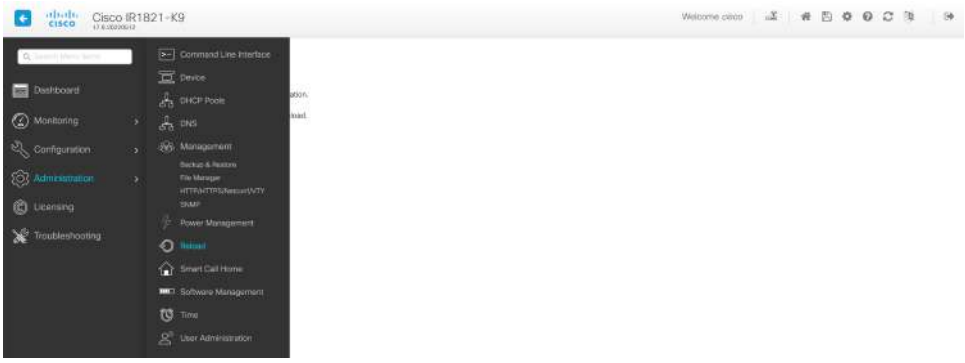
Actualizarea imaginii routerului prin WebUI

Routerul poate fi, de asemenea, actualizat prin interfața cu utilizatorul web (WebUI). Mai multe informații despre utilizarea WebUI pot fi găsite înInterfață cu utilizatorul web (WebUI)capitol.

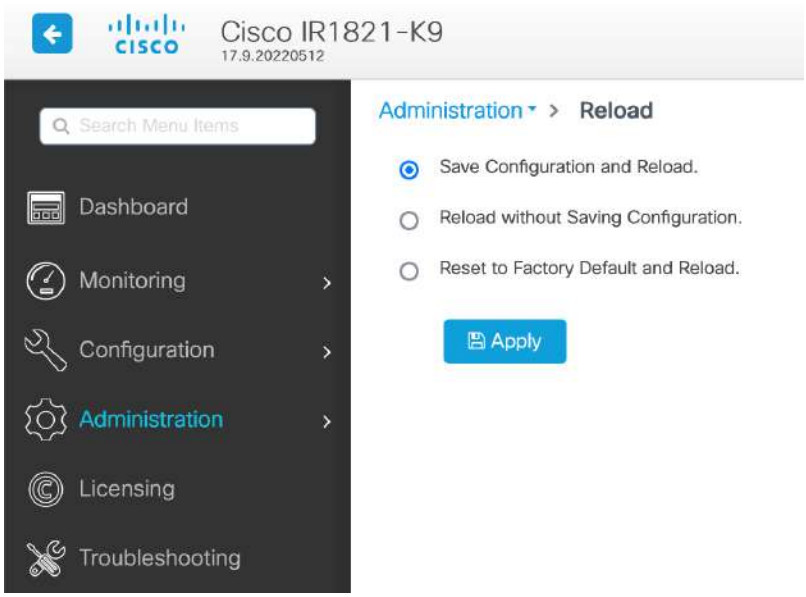
După ce lansați WebUI, accesați**Administrare**fila.



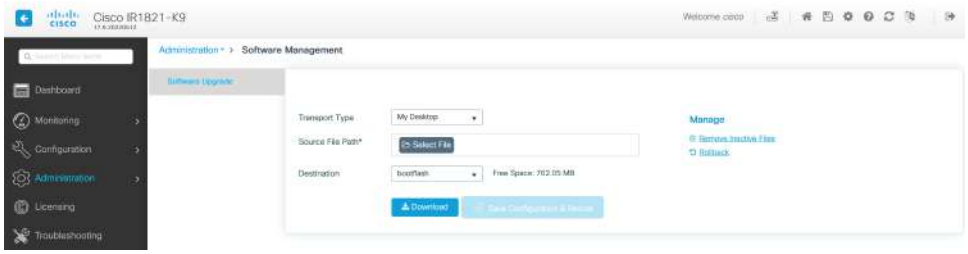
Reîncărcați routerul selectând**Administrare > Reîncărcare**.



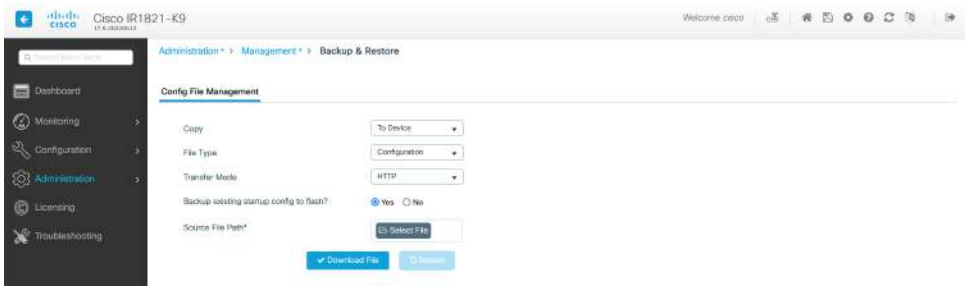
Selectați opțiunea dintre opțiuni, apoi faceți clic**Aplicați**.



Selecta**Management software**sub**Administrare**fila. Navigați la locația noului fișier imagine IOS XE de pe computer.



Selecta**Administrare > Management > Backup & Restore**. Copiați fișierul imagine de pe laptop pe router. Acest exemplu folosește HTTP ca transport.



Salvați configurația făcând clic pe pictograma unității de dischetă din partea de sus a WebUI.

CAPITOL 8

Utilizarea software-ului Cisco IOS XE

Acest capitol conține următoarele secțiuni:

Înțelegerea modurilor de comandă

Modurile de comandă disponibile în Cisco IOS XE sunt aceleași cu cele disponibile în Cisco IOS tradițional. Utilizați CLI pentru a accesa software-ul Cisco IOS XE. Deoarece CLI este împărțit în multe moduri diferite, comenzile disponibile pentru dvs. în orice moment depind de modul în care vă aflați în prezent. Introducerea unui semn de întrebare (**?**) la promptul CLI vă permite să obțineți o listă de comenzi disponibile pentru fiecare mod de comandă.

Când vă conectați la CLI, vă aflați în modul EXEC utilizator. Modul EXEC utilizator conține doar un subset limitat de comenzi. Pentru a avea acces la toate comenzile, trebuie să intrați în modul EXEC privilegiat, în mod normal folosind o parolă. Din modul EXEC privilegiat, puteți lansa orice comandă EXEC - utilizator sau modul privilegiat - sau puteți intra în modul de configurare globală. Majoritatea comenzilor EXEC sunt comenzi unice. De exemplu,**spectacol** comenzile afișează informații importante despre stare și**clar**comenzile șterg contoare sau interfețe. Comenzile EXEC nu sunt salvate când software-ul repornește.

Modurile de configurare vă permit să faceți modificări la configurația care rulează. Dacă mai târziu salvați configurația de rulare în configurația de pornire, aceste comenzi modificate sunt stocate atunci când software-ul este repornit. Pentru a intra în anumite moduri de configurare, trebuie să începeți din modul de configurare globală. Din modul de configurare globală, puteți intra în modul de configurare a interfeței și într-o varietate de alte moduri, cum ar fi modurile specifice protocolului.

Modul monitor ROM este un mod separat utilizat atunci când software-ul Cisco IOS XE nu se poate încărca corect. Dacă o imagine software validă nu este găsită la pornirea software-ului sau dacă fișierul de configurare este corupt la pornire, este posibil ca software-ul să intre în modul monitor ROM.

Următorul tabel descrie cum să accesați și să ieșiți din diferite moduri de comandă comune ale software-ului Cisco IOS XE. De asemenea, arată exemple de solicitări afișate pentru fiecare mod.

Tabelul 5: Accesarea și ieșirea modurilor de comandă

Modul de comandă	**Metoda de acces**	**Prompt**	**Metoda de ieșire**
Utilizator EXEC	Log in.	Router>	Utilizați**deconectare**comanda.
EXEC privilegiat	Din modul EXEC utilizator, utilizați **permite**comanda.	Router#	Pentru a reveni la modul EXEC utilizator, utilizați**dezactivați**comanda.
Configurație globală	Din modul EXEC privilegiat, utilizați**configurați terminarea** comand.	Router(config)#	Pentru a reveni la modul EXEC privilegiat din modul de configurare globală, utilizați**Ieșire**sau**Sfârşit** comanda.
Configurarea interfeței	Din modul de configurare globală, specificați o interfață folosind un **interfata**comanda.	Router(config-if)#	Pentru a reveni la modul de configurare globală, utilizați**Ieșire**comanda. Pentru a reveni la modul EXEC privilegiat, utilizați**Sfârşit**comanda.
Diagnostic	Routerul pornește sau accesează modul de diagnosticare în urmatoarele scenarii: • În unele cazuri, modul de diagnosticare va fi atins atunci când procesul sau procesele Cisco IOS eșuează. În majoritatea scenariilor, totuși, routerul se va reîncărca. • O politică de acces configurată de utilizator este configurată utilizând**transport-hartă** comandă care direcționează utilizatorul în modul de diagnosticare. • Un semnal de pauză (**Ctrl-C**, **Ctrl-Shift-6**, sau**trimite pauză**comanda) este introdus și routerul este configurat să acceseze modul de diagnosticare la recepționarea semnalului de întrerupere.	Router(diag)#	Dacă eșecul procesului Cisco IOS este motivul pentru a intra în modul de diagnosticare, problema Cisco IOS trebuie rezolvată și routerul trebuie repornit pentru a ieși din modul de diagnosticare. Dacă routerul este în modul de diagnosticare din cauza a transport-map, accesați routerul printr-un alt port sau folosind o metodă configurată pentru a se conecta la Cisco IOS CLI.

Modul de comandă	Metoda de acces	Prompt	Metoda de ieșire
monitor ROM	Din modul EXEC privilegiat, utilizați**reîncărcați**Comanda EXEC. Apăsați tasta**Pauză**tasta în primele 60 de secunde în timp ce sistemul pornește.	rommon#>	Pentru a ieși din modul monitor ROM, porniți manual o imagine validă sau efectuați o resetare cu autoboot setat, astfel încât să fie încărcată o imagine validă.

Utilizarea comenzilor rapide de la tastatură

Comenzile nu sunt sensibile la majuscule. Puteți abrevia comenzile și parametrii dacă abrevierile conțin suficiente litere pentru a fi diferite de orice alte comenzi sau parametri disponibile în prezent.

Următorul tabel listează comenzile rapide de la tastatură pentru introducerea și editarea comenzilor.

Tabelul 6: Comenzi rapide de la tastatură

Nume cheie	Scop
Ctrl-Bsau cel**Săgeata stânga**cheie	Mutați cursorul înapoi cu un caracter.
Ctrl-Fsau cel**Săgeata dreapta**cheie	Mutați cursorul înainte cu un caracter.
Ctrl-A	Mutați cursorul la începutul liniei de comandă.
Ctrl-E	Mutați cursorul la sfârșitul liniei de comandă.
Esc B	Mutați cursorul înapoi cu un cuvânt.
Esc F	Mutați cursorul înainte cu un cuvânt.

Folosind formele de comenzi nu și implicite

Aproape fiecare comandă de configurare are un**nu**formă. În general, utilizați**nu**formular pentru a dezactiva o funcție. Utilizați comanda fără**nu**cuvânt cheie pentru a reactiva o funcție dezactivată sau pentru a activa o funcție care este dezactivată implicit. De exemplu, rutarea IP este activată în mod implicit. Pentru a dezactiva rutarea IP, utilizați**fara rutare ip**comanda; pentru a reactiva rutarea IP, utilizați**rutare ip**comanda. Publicațiile de referință pentru comenzile software Cisco IOS oferă sintaxa completă pentru comenzile de configurare și descriu ce**nu**forma unei comenzi face.

Multe comenzi CLI au, de asemenea, un**implicit**formă. Prin emiterea**<comandă> implicit**nume-comandă, puteți configura comanda la setarea implicită. Publicațiile de referință pentru comenzile software Cisco IOS descriu funcția de la a**implicit**forma comenzii atunci când**implicit**forma îndeplinește o altă funcție decât cea de câmpie și **nu**forme ale comenzii. Pentru a vedea ce comenzi implicite sunt disponibile pe sistemul dvs., introduceți**implicit?**în modul de comandă corespunzător.

Utilizarea memoriei tampon de istoric pentru a rechema comenzi

Bufferul istoric stochează ultimele 20 de comenzi pe care le-ați introdus. Înlocuirea istoricului vă permite să accesați aceste comenzi fără a le tasta din nou, folosind comenzi speciale prescurtate.

Următorul tabel listează comenzile de înlocuire a istoricului.

Tabelul 7: Comenzi de înlocuire a istoricului

Comanda	Scop
Ctrl-Psau cel**Săgeată sus**cheie	Amintește comenzile din memoria tampon de istoric, începând cu cea mai recentă comandă. Repetați secvența de taste pentru a rememora succesiv comenzi mai vechi.
Ctrl-Nsau cel**Săgeată în jos**cheie1	Revine la comenzile mai recente din memoria tampon de istoric după rechemarea comenzilor cu**Ctrl-P**sau cel**Săgeată sus**cheie.
Router# arată istoricul	În modul EXEC, listează ultimele comenzi pe care le-ați introdus.

Gestionarea fișierelor de configurare

Fișierul de configurare de pornire este stocat în sistemul de fișiere nvram: iar fișierele de configurare care rulează sunt stocate în sistem: sistem de fișiere. Această configurare de stocare a fișierelor de configurare este utilizată și pe mai multe alte platforme de routere Cisco.

IOS XE oferă criptarea fișierului de configurare. Criptarea este discutată pe larg în ghidul dispozitivului de întărire IOS XE, care poate fi găsit aici:https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

Ca o chestiune de întreținere de rutină a oricărui router Cisco, utilizatorii ar trebui să facă o copie de rezervă a fișierului de configurare de pornire prin copierea fișierului de configurare de pornire din NVRAM pe unul dintre celelalte sisteme de fișiere ale routerului și, în plus, pe un server de rețea. Copierea de rezervă a fișierului de configurare de pornire oferă o metodă ușoară de recuperare a fișierului de configurare de pornire dacă fișierul de configurare de pornire din NVRAM devine inutilizabil din orice motiv.

The**copie**comanda poate fi folosită pentru a face copii de rezervă ale fișierelor de configurare de pornire.

Pentru informații mai detaliate despre gestionarea fișierelor de configurare, consultați secțiunea „Gestionarea fișierelor de configurare” dinGhid de configurare a noțiunilor fundamentale de configurare Cisco IOS XE.

Salvarea modificărilor de configurare

Utilizați**copiați running-config startup-config**comandă pentru a salva modificările configurației în configurația de pornire, astfel încât modificările să nu se piardă dacă software-ul se reîncarcă sau are loc o întrerupere de curent. De exemplu:

Router#**copiați running-config startup-config** Nume fișier
de destinație [startup-config]?**intra** Configurare clădire...
[OK]

IR1101#
* 24 septembrie 08:50:26.666: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Fișier de configurare privat criptat cu succes

Nota Salvarea configurației poate dura câteva minute.

Această sarcină salvează configurația în NVRAM.

Ieșirea de filtrare din emisiune și mai multe comenzi

Puteți căuta și filtra rezultatul**spectacol**și**Mai mult**comenzi. Această funcționalitate este utilă dacă trebuie să sortați prin cantități mari de ieșiri sau dacă doriți să excludeți ieșirile pe care nu trebuie să le vedeți.

Pentru a utiliza această funcționalitate, introduceți a**spectacol**sau**Mai mult**comandă urmată de caracterul „pipe" (|); unul dintre cuvintele cheie**ÎNCEPE**,**include**, sau**exclude**; și o expresie regulată pe care doriți să căutați sau să filtrați (expresia este sensibilă la majuscule și minuscule):

spectacol*comandal***{anexează | începe | exclude | includ | redirecționare | sectiunea |** ***tricou}****expresie regulată*

Ieșirea se potrivește cu anumite linii de informații din fișierul de configurare.

Exemplu

În acest exemplu, un modificator al lui**arata interfata**comanda (**include protocolul**) este folosit pentru a furniza numai liniile de ieșire în care expresia**protocol**este afisat:

Router#**arata interfata | include protocolul**
GigabitEthernet0/0/0 este inactiv din punct de vedere administrativ, protocolul de linie este inactiv (dezactivat) 0 scăderi de protocol necunoscute
GigabitEthernet0/1/0 este oprit, protocolul de linie este oprit (nu se conectează) 0
scăderi de protocol necunoscute
GigabitEthernet0/1/1 este oprit, protocolul de linie este oprit (nu se conectează) 0 scăderi de protocol necunoscute
GigabitEthernet0/1/2 este oprit, protocolul de linie este oprit (nu se conectează) 0 scăderi de protocol necunoscute
GigabitEthernet0/1/3 este oprit, protocolul de linie este oprit (nu se conectează) 0 scăderi de protocol necunoscute
GigabitEthernet0/0/5 este activ, protocolul de linie este activat (conectat) 0
scăderi de protocol necunoscute
Cellular0/4/0 este activ, protocolul de linie a crescut 0
scăderi de protocol necunoscute
Cellular0/4/1 este inactiv din punct de vedere administrativ, protocolul de linie este oprit 0
scăderi de protocol necunoscute
Cellular0/5/0 este în sus, protocolul de linie este în sus 0
picături de protocol necunoscut
Cellular0/5/1 este inactiv din punct de vedere administrativ, protocolul de linie este oprit 0
scăderi de protocol necunoscute
Async0/2/0 este în sus, protocolul de linie este în jos 0
picături de protocol necunoscut
Vlan1 este activ, protocolul de linie este activ, Autostate Enabled 0
protocol necunoscut
Vlan172 este activ, protocolul de linie este inactiv, Autostate activat 0
protocol necunoscut
Vlan175 este oprit, protocolul de linie este oprit, Autostate Enabled 0 protocol
necunoscut
IR1800#

Utilizarea Cisco Feature Navigator

UtilizareCisco Feature Navigatorpentru a găsi informații despre suportul platformei și suportul imaginii software. Cisco Feature Navigator este un instrument care vă permite să determinați ce imagini software Cisco IOS XE acceptă o anumită versiune de software, set de caracteristici sau platformă. Pentru a utiliza instrumentul de navigare, nu este necesar un cont pe Cisco.com.

Găsirea informațiilor de asistență pentru platforme și imagini software Cisco

Software-ul Cisco IOS XE este împachetat în seturi de caracteristici constând din imagini software care acceptă platforme specifice.

Toate ghidurile de configurare Cisco IOS-XE pot fi găsite aici:https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/series.html.

Grupul de seturi de caracteristici care sunt disponibile pentru o anumită platformă depinde de ce imagini software Cisco sunt incluse într-o versiune. Pentru a identifica setul de imagini software disponibile într-o anumită versiune sau pentru a afla dacă o caracteristică este disponibilă într-o anumită imagine software Cisco IOS XE, puteți utilizaCisco Feature Navigatorsau vezihttps://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/series.html.

Obține ajutor

Introducerea unui semn de întrebare (**?**) la promptul CLI afișează o listă de comenzi disponibile pentru fiecare mod de comandă. De asemenea, puteți obține o listă de cuvinte cheie și argumente asociate oricărei comenzi folosind funcția de ajutor sensibilă la context.

Pentru a obține ajutor specific unui mod de comandă, unei comenzi, unui cuvânt cheie sau unui argument, utilizați una dintre următoarele comenzi.

Comanda	Scop
Ajutor	Oferă o scurtă descriere a sistemului de ajutor în orice mod de comandă.
abreviat-command-entry?	Oferă o listă de comenzi care încep cu un anumit șir de caractere. **Nota** Nu există spațiu între comandă și semnul întrebării.
abreviated-command-entry <Tab>	Completează un nume de comandă parțial.
?	Listează toate comenzile care sunt disponibile pentru un anumit mod de comandă.

Comanda	Scop
comanda?	Listează cuvintele cheie sau argumentele pe care trebuie să le introduceți în continuare pe linia de comandă. **Nota** Există un spațiu între comandă și semnul întrebării.

Găsirea opțiunilor de comandă: Exemplu

Această secțiune oferă informații despre cum să afișați sintaxa pentru o comandă. Sintaxa poate consta din cuvinte cheie și argumente opționale sau obligatorii. Pentru a afișa cuvinte cheie și argumente pentru o comandă, introduceți un semn de întrebare (**?**) la promptul de configurare sau după introducerea unei părți a unei comenzi urmată de un spațiu. Software-ul Cisco IOS XE afișează o listă și scurte descrieri ale cuvintelor cheie și argumentelor disponibile. De exemplu, dacă vă aflați în modul de configurare globală și doriți să vedeți toate cuvintele cheie și argumentele pentru**arap** comandă, ar trebui să tastați**arap ?**.

<**cr**> simbolul în ieșirea de ajutor pentru comandă reprezintă întoarcerea caruşului. Pe tastaturile mai vechi, tasta de întoarcere a căruciorului este**Reveni**cheie. Pe cele mai multe tastaturi moderne, tasta de întoarcere a căruciorului este **Intră**cheie. <**cr**> simbolul de la sfârșitul comenzii de ajutor indică faptul că aveți opțiunea de a apăsa**Intră**pentru a finaliza comanda și că argumentele și cuvintele cheie din lista care precede <**cr**> simbolurile sunt opționale. <**cr**> simbolul în sine indică faptul că nu mai sunt disponibile argumente sau cuvinte cheie și că trebuie să apăsați**Intră**pentru a finaliza comanda.

Următorul tabel prezintă exemple de utilizare a semnului întrebării (**?**) pentru a vă ajuta la introducerea comenzilor.

Tabelul 8: Găsirea opțiunilor de comandă

Comanda	Comentariu
Router> activare Parolă: <parolă> Router#	Introduceți**permite**comandă și parolă pentru a accesa comenzile EXEC privilegiate. Sunteți în modul EXEC privilegiat când promptul se schimbă la „ # ” din „ >”, de exemplu,**Router>**la**Router#**
Router# configura terminalul Introduceți comenzile de configurare, una pe linie. Sfârşitcomanda pentru a intra în modul de configurare globală. Tu cu CNTL/Z. Router(config)#	Introduceți**configura terminalul**EXEC privilegiat sunt în modul de configurare globală când promptul se schimbă în**Router (configurație)#**

Comanda	Comentariu
Router(config)# interfață GigabitEthernet ? <0-0> Numărul interfeței GigabitEthernet Router(config)# interfață GigabitEthernet 0/? <0-5> Numărul adaptorului de port Router (config)# interfață GigabitEthernet 0/0/?Intră**?**pentru a afișa <0-63> Numărul interfeței GigabitEthernet Router (config)# interfață GigabitEthernet 0/0/0? . <0-71> Router(config-if)#	Intrați în modul de configurare a interfeței specificând interfața pe care doriți să o configurați, folosind **interfață GigabitEthernet**comanda de configurare globală. ceea ce trebuie să introduceți în continuare pe linie de comandă. Când este afișat simbolul <cr>, puteți apăsa **Intră**pentru a finaliza comanda. Vă aflați în modul de configurare a interfeței când solicitarea se schimbă în**Router(config-if)#**
Router(config-if)#**?** Comenzi de configurare a interfeței: . . . ip Interfață Internet Protocol comenzile de configurare mentine in viata Activați keepalive lan-nume Comanda Nume LAN llc2 Subcomenzi de interfață LLC2 interval de încărcare Specificați intervalul pentru încărcare calcul pentru o interfață locaddr-prioritate Atribuiți un grup prioritar exploatare forestieră Configurați înregistrarea pentru interfata loopback Configurați intern loopback pe o interfata adresa mac Setați manual interfața adresa MAC mls sub/interfață router mls comenzi mpoa Interfață MPOA comenzi de configurare mtu Setați interfața Unitate de transmisie maximă (MTU) netbios Utilizați un NETBIOS definit lista de acces sau activați memorarea numelor în cache nu Anulați o comandă sau un set valorile sale implicite codificare nrzi Activați utilizarea NRZI codificare ntp Configurați NTP . . . Router(config-if)#	Intră**?**pentru a afișa o listă cu toate comenzile de configurare a interfeței disponibile pentru interfață. Acest exemplu arată doar câteva dintre comenzile de configurare a interfeței disponibile.

Comanda	Comentariu
Router(config-if)# ip? Subcomenzi de configurare IP a interfeței: acces-grup Specificați controlul accesului pentru pachete contabilitate Activați contabilitatea IP această interfață adresa Setați adresa IP a unui interfata autentificare subcomenzi de autentificare lățime de bandă-procent Setați limita de lățime de bandă EIGRP adresa-difuzare Setați adresa de difuzare a unei interfețe cgmp Activați/dezactivați CGMP regia-difuzare Activați redirecționarea emisiuni regizate dvmrp Comenzile interfeței DVMRP salut-interval Configurați IP-EIGRP salut interval ajutor-adresă Specificați o destinație adresa pentru emisiunile UDP timp de retinere Configurați reținerea IP-EIGRP timp . . . Router(config-if)#**ip**	Introduceți comanda pe care doriți să o configurați pentru interfață. Acest exemplu folosește**ip**comanda. Intră**?**pentru a afișa ceea ce trebuie să introduceți în continuare pe linia de comandă. Acest exemplu arată doar câteva dintre comenzile disponibile de configurare IP a interfeței.
Router(config-if)# adresa IP? ABCD adresa IP negociat Adresa IP a fost negociată PPP Router(config-if)# adresa ip	Introduceți comanda pe care doriți să o configurați pentru interfață. Acest exemplu folosește**adresa ip** comanda lui. Intră**?**pentru a afișa ceea ce trebuie să introduceți în continuare pe linia de comandă. În acest exemplu, trebuie să introduceți o adresă IP sau**negociat**cuvânt cheie. Returul de cărucior (<cr>) nu este afișat. Prin urmare, trebuie să introduceți cuvinte cheie sau argumente suplimentare pentru a finaliza comanda.
Router(config-if)# adresa IP 172.16.0.1? ABCD masca de subrețea IP Router(config-if)# adresa IP 172.16.0.1	Introduceți cuvântul cheie sau argumentul pe care doriți să îl utilizați. Acest exemplu folosește adresa IP 172.16.0.1. Intră**?**pentru a afișa ceea ce trebuie să introduceți în continuare pe linia de comandă. În acest exemplu, trebuie să introduceți o mască de subrețea IP. <cr> nu este afișat. Prin urmare, trebuie să introduceți cuvinte cheie sau argumente suplimentare pentru a finaliza comanda.

Comanda	Comentariu
Router(config-if)# adresa ip 172.16.0.1 255.255.255.0 ? secundar Faceți această adresă IP a adresa secundara <cr> Router(config-if)# adresa ip 172.16.0.1 255.255.255.0	Introduceți masca de subrețea IP. Acest exemplu folosește masca de subrețea IP 255.255.255.0. Intră**?**pentru a afișa ceea ce trebuie să introduceți în continuare pe linia de comandă. În acest exemplu, puteți introduce **secundar**cuvânt cheie sau puteți apăsa**Intră**. Se afișează <cr>. Presa**Intră**pentru a finaliza comanda sau introduceți un alt cuvânt cheie.
Router(config-if)# adresa ip 172.16.0.1 255.255.255.0 Router(config-if)#	Presa**Intră**pentru a finaliza comanda.

Utilizarea Software Advisor

Cisco menține instrumentul Software Advisor. VedeaInstrumente și resurse. Utilizați instrumentul Software Advisor pentru a vedea dacă o caracteristică este acceptată într-o versiune Cisco IOS XE, pentru a găsi documentul software pentru acea caracteristică sau pentru a verifica cerințele minime de software ale software-ului Cisco IOS XE cu hardware-ul instalat pe router. Trebuie să fiți un utilizator înregistrat pe Cisco.com pentru a accesa acest instrument.

Utilizarea notelor de lansare a software-ului

Consultați notele de lansare pentru informații despre următoarele:

- Prezentare generală a produsului
- Avertismentele de severitate 1 și 2 deschise și rezolvate
- Nume de imagini software
- Caracteristici noi
- Limitări cunoscute

Notele de lansare sunt destinate să fie specifice versiunii pentru cea mai recentă ediție, iar informațiile furnizate în aceste documente pot să nu fie cumulative în furnizarea de informații despre caracteristicile care au apărut pentru prima dată în versiunile anterioare. Pentru informații cumulate despre caracteristici, consultați Cisco Feature Navigator la: http://www.cisco.com/go/cfn/.

CAPITOL 9

Metode de instalare Cisco IOS XE

Acest capitol conține următoarele secțiuni:

Modul Bundle versus Modul Instalare

Cisco IOS XE care rulează pe routere IoT a folosit de obicei modul de pornire Bundle. Modul de pornire pachet este cunoscut și sub numele de pornire consolidată și folosește o singură imagine comprimată. Convenția tipică de denumire este <product>-universalk9.<release>.SPA.bin.

Acest mod oferă un proces de pornire consolidat, folosind imaginea .bin locală (hard disk, flash) sau la distanță (TFTP). Pornirea printr-o imagine .bin înseamnă că routerul ar trebui mai întâi să decomprima imaginea înainte de a porni de pe aceasta. Acest lucru a dus la o perioadă mai lungă de timp pentru pornirea routerului.

Pentru a actualiza routerul la o nouă versiune de IOS XE, ați indica „sistemul de pornire” către o nouă imagine software. Această metodă este bine cunoscută și detalii sunt disponibile în ghidul de configurare a produselor.

Începând cu versiunea 17.9.1 a IOS XE, la routerele IoT a fost adăugat un nou mod de pornire numit Modul de instalare. Modul de instalare folosește pachete încărcate în bootflash, care sunt citite de un fișier packages.conf. Această metodă oferă mai mult control asupra procesului de instalare a software-ului.

Modul de instalare necesită mai mult spațiu în bootflash: pentru fișiere. Pachetele sunt puțin mai mari decât imaginile .bin și variază în funcție de dimensiunea produsului.

Instalarea software-ului utilizând comenzile de instalare

Din Cisco IOS XE 17.9.1, routerele Cisco IoT sunt livrate implicit în modul de instalare. Utilizatorii pot porni platforma și pot face upgrade sau downgrade la versiunile software Cisco IOS XE folosind un set de**instala**comenzi.

Restricții pentru instalarea software-ului utilizând comenzile de instalare

- Modul de instalare necesită o repornire a sistemului.
- Instalarea SMU a fost acceptată atât în modul de pornire a pachetului, cât și în modul de instalare. Din versiunea Cisco IOS XE 17.9.x, instalarea SMU va fi oprită dacă routerul este pornit în modul pachet. Dacă routerul este pornit în modul de instalare, instalarea SMU va continua să funcționeze așa cum este în versiunile anterioare.

Suport pentru modul de instalare

Următorul tabel descrie diferențele dintre modul Bundle și modul Instalare:

Cisco IOS XE care rulează pe routere IoT a folosit de obicei modul de pornire Bundle. Modul de pornire pachet este cunoscut și sub numele de pornire consolidată și folosește o singură imagine comprimată. Convenția tipică de denumire este <product>-universalk9.<release>.SPA.bin.

Acest mod oferă un proces de pornire consolidat, folosind imaginea .bin locală (hard disk, flash) sau la distanță (TFTP). Pornirea printr-o imagine .bin înseamnă că routerul ar trebui mai întâi să decomprima imaginea înainte de a porni de pe aceasta. Acest lucru a dus la o perioadă mai lungă de timp pentru pornirea routerului.

Pentru a actualiza routerul la o nouă versiune de IOS XE, ați indica „sistemul de pornire” către o nouă imagine software. Această metodă este bine cunoscută și detalii sunt disponibile în ghidul de configurare a produselor.

Începând cu versiunea 17.9.1 a IOS XE, la routerele IoT a fost adăugat un nou mod de pornire numit Modul de instalare. Modul de instalare folosește pachete încărcate în bootflash, care sunt citite de un fișier packages.conf. Această metodă oferă mai mult control asupra procesului de instalare a software-ului.

Nota Instalarea SMU a fost acceptată atât în modul de pornire a pachetului, cât și în modul de instalare. Din Cisco IOS XE Release 17.9.x, instalarea SMU va fi oprită dacă routerul este pornit în modul pachet. Dacă routerul este pornit în modul de instalare, instalarea SMU va continua să funcționeze așa cum este în versiunile anterioare.

Tabelul 9: Modul Bundle vs Modul Instalare

Modul pachet	**Modul de instalare**
Acest mod oferă un proces de pornire consolidat, folosind imaginea .bin locală (hard disk, flash) sau la distanță (TFTP).	Acest mod folosește fișierul local (bootflash) packages.conf pentru procesul de pornire.
Acest mod folosește un singur fișier .bin.	. fișierul bin este înlocuit cu fișiere .pkg extinse în acest mod.
CLI: Router(config)#**sistemul de pornire bootflash:***<nume fișier>*	CLI: **#instalați adăugați fișierul bootflash: [activați comiterea]**
Pentru a face upgrade în acest mod, îndreptați sistemul de pornire către noua imagine.	Pentru a face upgrade în acest mod, utilizați**instala**comenzi.

Modul pachet	Modul de instalare
Actualizare automată a imaginii: Atunci când o nouă unitate înlocuibilă pe teren (FRU) este inserată într-un șasiu modular, este necesară intervenția manuală pentru ca noul FRU să funcționeze cu aceeași versiune ca și FRU-urile active.	Actualizare automată a imaginii: Când o nouă FRU este inserată într-un șasiu modular, FRU-ul care se alătură este actualizat automat la versiunea de imagine în sincronizare cu FRU-urile active.
Rollback: revenirea la imaginea anterioară cu mai multe actualizări de întreținere software (SMU) poate necesita mai multe reîncărcări.	Rollback: permite revenirea la o versiune anterioară a software-ului Cisco IOS XE, inclusiv mai multe corecții într-o singură reîncărcare.

Pentru informații suplimentare, consultațiMetode de instalare Cisco IOS XE.

Informații despre instalarea software-ului utilizând comenzile de instalare

Din versiunea Cisco IOS XE 17.9.1, routerele IoT vor fi livrate în modul de instalare în loc de modul pachet. Deci, orice router nou din fabrică se va porni în modul de instalare.

Instalările existente care utilizează versiunile anterioare ale IOS XE au opțiunea de a continua să-și folosească dispozitivul în modul Bundle dacă doresc. Sau își pot converti dispozitivul în modul Instalare.

Modul de instalare este aplicabil atât modului autonom, cât și modului controler.

O nouă versiune poate fi instalată în modul Instalare folosind vManage.

Următorul tabel descrie diferențele dintre modul Bundle și modul Instalare:

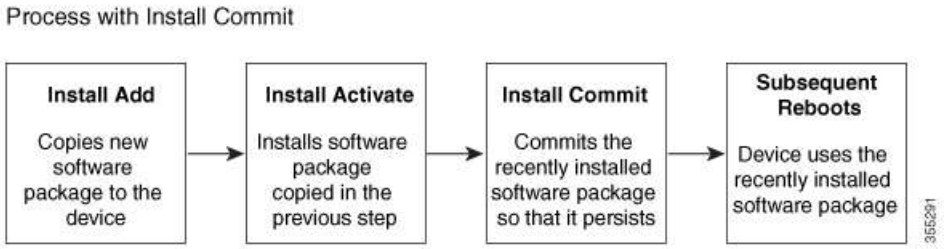
Tabelul 10: Modul Bundle vs Modul Instalare

Modul pachet	Modul de instalare
Acest mod oferă un proces de pornire consolidat, folosind imaginea .bin locală (hard disk, flash) sau la distanță (TFTP).	Acest mod folosește fișierul local (bootflash) packages.conf pentru procesul de pornire.
Acest mod folosește un singur fișier .bin.	. fișierul bin este înlocuit cu fișiere .pkg extinse în acest mod.
CLI: Router(config)#**sistemul de pornire bootflash:***<nume fișier>*	CLI: **#instalați adăugați fișierul bootflash: [activați comiterea]**
Pentru a face upgrade în acest mod, îndreptați sistemul de pornire către noua imagine.	Pentru a face upgrade în acest mod, utilizați**instala**comenzi.
Actualizare automată a imaginii: Când o nouă unitate de înlocuire pe câmp (FRU) este introdusă într-un șasiu modular, este necesară intervenția manuală pentru ca noul FRU să ruleze cu aceeași versiune ca și FRU-urile active.	Actualizare automată a imaginii: Când o nouă FRU este inserată într-un șasiu modular, FRU-ul care se alătură este actualizat automat la versiunea de imagine în sincronizare cu FRU-urile active.
Rollback: revenirea la imaginea anterioară cu mai multe actualizări de întreținere software (SMU) poate necesita mai multe reîncărcări.	Rollback: permite revenirea la o versiune anterioară a software-ului Cisco IOS XE, inclusiv mai multe corecții într-o singură reîncărcare.

Fluxul de proces al modului de instalare

Fluxul procesului în modul de instalare cuprinde trei comenzi pentru a efectua instalarea și actualizarea software-ului pe platforme –**install add**,**instalare activare,**şi**instalați commit**.

Următoarea diagramă de flux explică procesul de instalare cu**instala**comenzi:



The**install add**comanda copiază pachetul software dintr-o locație locală sau la distanță pe platformă. Comanda extrage componente individuale ale fișierului .package în subpachete și fișiere packages.conf. De asemenea, validează fișierul pentru a se asigura că fișierul imagine este specific platformei pe care este instalat.

Locația pachetului software poate fi în mai multe locuri, așa cum se arată în rezultatul următoarei comenzi:

IR1831#**instalați adăugați fișier?**
bootflash: Nume pachet crashinfo:
Nume pachet flash: Nume pachet

ftp: Numele pachetului
http: Numele pachetului
https: numele pachetului
cărucior: numele pachetului
rcp: Numele pachetului
scp: Numele pachetului
sftp: Numele pachetului
tftp: Numele pachetului
webui: Numele pachetului

The**instalare activare**comanda efectuează validările necesare și asigură pachetele adăugate anterior folosind**install add** comanda. De asemenea, declanșează o reîncărcare a sistemului.

The**instalarea comiterii**comanda confirmă pachetele activate anterior utilizând**instalare activare**comandă și face actualizările persistente peste reîncărcări.

Nota Instalarea unei actualizări înlocuiește orice imagine software instalată anterior. În orice moment, pe un dispozitiv poate fi instalată o singură imagine.

Următorul set de comenzi de instalare este disponibil:

Tabelul 11: Lista comenzilor de instalare

Comanda	Sintaxă	Scop
install add	**instalați adăugați fișier** *locație:filename.bin*	Copiază conținutul imaginii, pachetului și SMU-urilor în depozitul de software. Locația fișierului poate fi locală sau la distanță. Această comandă face următoarele: • Validează fișierul – suma de verificare, verificările de compatibilitate a platformei și așa mai departe. • Extras individual componentele pachetului în subpachete și pachete.conf • Copiază imaginea în inventarul local și o realizează disponibil pentru pașii următori.
instalare activare	**instalare activare**	Activează pachetul adăugat folosind**install add**comanda. • Utilizați**arată rezumatul instalării** comandă pentru a vedea ce imagine este inactivă. Această imagine va fi activată. • Sistemul se reîncarcă la executarea acestei comenzi. Confirmați dacă doriți să continuați cu activarea. Utilizați această comandă cu**la nivel prompt nici unul** cuvânt cheie pentru a ignora automat orice solicitare de confirmare.

Comanda	Sintaxă	Scop
(instalare activare) temporizator de întrerupere automată	**instalați activați temporizatorul de anulare automată** *<30-1200>*	The**temporizator de anulare automată**pornește automat, cu o valoare implicită de 120 de minute. Dacă**instalarea comiterii**comanda nu este executată în timpul prevăzut, procesul de activare este încheiat și sistemul revine la ultima stare comisă. • Puteți modifica valoarea timpului în timp ce executați**instalare activare**comanda. • Cel**instalarea comiterii**comanda oprește cronometrul și continuă procesul de instalare. • Cel**instalați activați oprirea temporizatorului de anulare automată** comanda oprește cronometrul fără să comite pachet. • Utilizați această comandă cu **la nivel prompt nici unul**cuvânt cheie pentru a ignora automat orice solicitare de confirmare. • Această comandă este valabilă numai în varianta de instalare în trei pași.
instalați commit	**instalați commit**	Commite pachetul activat folosind **instalare activare** comandă și o face persistentă peste reîncărcări. • Utilizați**arată rezumatul instalării** comandă pentru a vedea ce imagine este necommitată. Această imagine va primi comise.

Comanda	Sintaxă	Scop
avorta instalarea	**avorta instalarea**	Termină instalarea și readuce sistemul la ultima stare comisă. • Această comandă este aplicabilă numai atunci când pachetul este în starea activată (starea necommitată). • Dacă ați comis deja imaginea folosind**instalarea comiterii** comanda, utilizați **instalați rollback la**comandă pentru a reveni la versiunea preferată.
instalați eliminați	**install remove {fișier***<nume de fișier>***| inactiv}**	Șterge pachetele inactive din depozitul platformei. Utilizați această comandă pentru a elibera spațiu. • **fișier**: elimină fișierele specificate. • **inactiv**: elimină toate fișierele inactive.
instalați rollback la	**instalați rollback la {bază | etichetă | comis | id}**	Derulează înapoi setul de software la un punct de instalare salvat sau la ultimul punct de instalare comis. Următoarele sunt caracteristicile acestei comenzi: • Necesită reîncărcare. • Se aplică numai atunci când pachetul este în stare de comitere. • Utilizați această comandă cu **la nivel prompt nici unul**cuvânt cheie pentru a ignora automat orice solicitare de confirmare. **Nota** Dacă efectuați derularea instalării la o imagine anterioară, imaginea anterioară trebuie instalată în modul de instalare. Doar rollback-ul SMU este posibil în modul pachet.

Comanda	Sintaxă	Scop
instalare dezactivare	**instalați fișierul de dezactivare***<nume de fișier>*	Elimină un pachet din depozitul platformei. Această comandă este acceptată numai pentru SMU-uri. • Utilizați această comandă cu **la nivel prompt nici unul**cuvânt cheie pentru a ignora automat orice solicitare de confirmare.

Următoarele comenzi show sunt, de asemenea, disponibile:

Tabelul 12: Lista comenzilor show

Comanda	Sintaxă	Scop
arată jurnalul de instalare	**arată jurnalul de instalare**	Oferă istoricul și detaliile tuturor operațiunilor de instalare care au fost efectuate de la pornirea platformei.
arată pachetul de instalare	**arată pachetul de instalare***<nume de fișier>*	Oferă detalii despre fișierul .pkg/.bin care este specificat.
arată rezumatul instalării	**arată rezumatul instalării**	Oferă o prezentare generală a versiunilor de imagini și a stărilor de instalare corespunzătoare ale acestora.
arată instalarea activă	**arată instalarea activă**	Oferă informații despre pachetele active.
arată instalarea inactivă	**arată instalarea inactivă**	Oferă informații despre pachetele inactive.
arată instalarea comisă	**arată instalarea comisă**	Oferă informații despre pachetele comise.
arată instalarea necommitată	**arată instalarea necommitată**	Oferă informații despre pachetele necommitate.
afișează derularea instalării	**arată instalarea rollback {point-id | eticheta}**	Afișează pachetul asociat cu un punct de instalare salvat.
arata versiunea	**arată versiunea [rp-slot] [instalat [interfață utilizator] | aprovizionat | funcționare]**	Afișează informații despre pachetul curent, împreună cu informații despre hardware și platformă.

Pornirea platformei în modul de instalare

Puteți instala, activa și comite un pachet software folosind o singură comandă (instalare într-un singur pas) sau mai multe comenzi separate (instalare în trei pași).

Dacă platforma funcționează în modul pachet, procedura de instalare într-un singur pas trebuie utilizată pentru a converti inițial platforma din modul pachet în modul de instalare. Instalările și upgrade-urile ulterioare pe platformă se pot face fie cu variante cu un singur pas, fie cu trei pași.

Puteți vedea cum este configurat dispozitivul dvs. pentru a porni folosind**arata romvar**şi**arată bootvar**comenzi.

```
Router#arata romvar
Variabile ROMMON:
PS1 = rommon ! > CM
= IR1100
DEVICE_MANAGED_MODE = LICENSE_SUITE
autonom =
RET_2_RTS =
PUTERIE = 250
BOOT = flash:packages.conf,12; LICENSE_BOOT_LEVEL = avantajul
rețelei,toate:IR1101; BSI = 0

RET_2_RCALTS =
RANDOM_NUM = 212626522
Router#

Router#arată bootvar
Variabila BOOT = flash:packages.conf,12; Variabila
CONFIG_FILE nu există Variabila BOOTLDR nu există

Registrul de configurare este 0x2102

Standby nu este gata pentru a afișa bootvar

Router#
```

Instalare într-un singur pas SAU conversia de la modul Bundle la modul Instalare

Nota

- Toate acțiunile CLI (de exemplu, adăugare, activare și așa mai departe) sunt executate.
- Promptul de salvare a configurației va apărea dacă este detectată o configurație nesalvată.
- Solicitarea de reîncărcare va apărea după al doilea pas din acest flux de lucru. Utilizați**la nivel prompt nici unul**cuvânt cheie pentru a ignora automat solicitările de confirmare.
- Dacă nivelul prompt-ului este setat la Nici unul și există o configurație nesalvată, instalarea eșuează. Trebuie să salvați configurația înainte de a lansa din nou comanda.

Utilizați procedura de instalare într-un singur pas descrisă mai jos pentru a converti o platformă care rulează în modul de pornire pachet în modul de instalare. După ce comanda este executată, platforma repornește în modul de pornire de instalare.

Mai târziu, procedura de instalare într-un singur pas poate fi folosită și pentru a actualiza platforma.

Această procedură folosește**instalați adăugați fișier activați comiterea**comandă în modul EXEC privilegiat pentru a instala un pachet software și pentru a actualiza platforma la o versiune nouă.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** Dispozitiv>**permite**	Activează modul EXEC privilegiat. Introduceți parola, dacă vi se solicită.
Pasul 2	**instalați adăugarea locației fișierului:***nume de fișier*[**activați commit**] **Exemplu:** Dispozitiv#**instalați adăugați fișier bootflash:<image_router>.SSA.bin activați comiterea**	Copiază pachetul de instalare a software-ului dintr-o locație locală sau la distanță (prin FTP, HTTP, HTTP sau TFTP) pe platformă și extrage componentele individuale ale fișierului .package în subpachete și fișiere packages.conf. De asemenea, efectuează o verificare de validare și compatibilitate pentru platforma și versiunile de imagine, activează pachetul și commite pachetul pentru a-l face persistent pe parcursul reîncărcărilor. Platforma se reîncarcă după rularea acestei comenzi.
Pasul 3	**Ieșire** **Exemplu:** Dispozitiv#**Ieșire**	Iese din modul EXEC privilegiat și revine la modul EXEC utilizator.

Instalare în trei etape

Nota

- Toate acțiunile CLI (de exemplu, adăugare, activare și așa mai departe) sunt executate.
- Promptul de salvare a configurației va apărea dacă este detectată o configurație nesalvată.
- Solicitarea de reîncărcare va apărea după pasul de activare a instalării din acest flux de lucru. Utilizați**la nivel prompt nici unul** cuvânt cheie pentru a ignora automat solicitările de confirmare.

Procedura de instalare în trei pași poate fi utilizată numai după ce platforma este în modul de instalare. Această opțiune oferă clientului mai multă flexibilitate și control în timpul instalării.

Această procedură folosește individual**install add**,**instalare activare**, și**instalarea comiterii**comenzi pentru instalarea unui pachet software și pentru a actualiza platforma la o versiune nouă.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** Dispozitiv>**permite**	Activează modul EXEC privilegiat. Introduceți parola, dacă vi se solicită.

	Comanda sau Acțiune	Scop
Pasul 2	**instalați adăugarea locației fișierului:***nume de fișier* **Exemplu:** Dispozitiv#**instalați adăugați fișier bootflash:<image_router>.SSA.bin**	Copiază pachetul de instalare a software-ului dintr-o locație la distanță (prin FTP, HTTP, HTTP sau TFTP) pe platformă și extrage componentele individuale ale fișierului .package în subpachete și fișiere packages.conf.
Pasul 3	**arată rezumatul instalării** **Exemplu:** Dispozitiv#**arată rezumatul instalării**	(Opțional) Oferă o prezentare generală a versiunilor de imagini și a stării lor de instalare corespunzătoare.
Pasul 4	**instalați activați auto-abort-timer***<timp>* **Exemplu:** **Device# install activați auto-abort-timer 120**	Activează pachetul adăugat anterior și reîncarcă platforma. • Când efectuați o instalare completă a software-ului, nu furnizați un nume de fișier de pachet. • În varianta în trei trepte, **temporizator de anulare automată**începe automat cu**instalare activare**comanda; valoarea implicită pentru cronometru este de 120 de minute. Dacă **instalarea comiterii**comanda nu este rulată înainte de expirarea temporizatorului, procesul de instalare se încheie automat. Platforma se reîncarcă și pornește cu ultima versiune validată.
Pasul 5	**avorta instalarea** **Exemplu:** Dispozitiv#**avorta instalarea**	(Opțional) Termină activarea instalării software și readuce platforma la ultima versiune validată. • Utilizați această comandă numai când imaginea este în starea activată și nu atunci când imaginea este în starea confirmată.
Pasul 6	**instalați commit** **Exemplu:** Dispozitiv#**instalați commit**	Commite instalarea noului pachet și face modificările persistente în timpul reîncărcărilor.
Pasul 7	**instalați rollback la committed** **Exemplu:** Dispozitiv#**instalați rollback la committed**	(Opțional) Derulează înapoi platforma la ultima stare comisă.
Pasul 8	**instalați ștergeți**{**fișier***sistem de fișiere: nume de fișier*| **inactiv**} **Exemplu:** Dispozitiv#**install remove inactiv**	(Opțional) Șterge fișierele de instalare a software-ului. • **fișier**: Șterge un anumit fișier • **inactiv**: Șterge toate fișierele de instalare neutilizate și inactive.

	Comanda sau Acțiune	Scop
Pasul 9	**arată rezumatul instalării** **Exemplu:** Dispozitiv#**arată rezumatul instalării**	(Opțional) Afișează informații despre starea curentă a sistemului. Ieșirea acestei comenzi variază în funcție de**instala** comenzile rulează înainte de această comandă.
Pasul 10	**Ieșire** **Exemplu:** Dispozitiv#**Ieșire**	Iese din modul EXEC privilegiat și revine la modul EXEC utilizator.

Actualizare în modul de instalare

Utilizați fie instalarea într-un singur pas, fie instalarea în trei pași pentru a actualiza platforma în modul de instalare.

Trecerea la o versiune superioară în modul de instalare

Utilizați**instalați rollback**comandă pentru a downgrade platforma la o versiune anterioară, îndreptând-o către imaginea corespunzătoare, cu condiția ca imaginea la care faceți downgrade să fi fost instalată în modul de instalare.

The**instalați rollback**comanda reîncarcă platforma și o pornește cu imaginea anterioară.

Nota The**instalați rollback**comanda reușește numai dacă nu ați șters fișierul anterior folosind**install remove inactiv**comanda.

Alternativ, puteți face downgrade instalând imaginea mai veche folosind**instala**comenzi.

Încheierea unei instalări de software

Puteți opri activarea unui pachet software în următoarele moduri:

- Când platforma se reîncărcă după activarea unei noi imagini, se declanșează temporizatorul auto-abort (în varianta de instalare în trei pași). Dacă temporizatorul expiră înainte de a emite**instalarea comiterii**comandă, procesul de instalare este încheiat, iar platforma se reîncărcă și pornește cu ultima versiune validată a imaginii software.

  Alternativ, utilizați**instalați oprirea temporizatorului auto-abort**comandă pentru a opri acest temporizator, fără a utiliza **instalarea comiterii**comanda. Noua imagine rămâne neangajată în acest proces.

- Folosind**avorta instalarea**comanda readuce platforma la versiunea care rula înainte de instalarea noului software. Utilizați această comandă înainte de a lansa**instalarea comiterii**comanda.

Exemple de configurare

Această secțiune prezintă exemple de utilizare a comenzilor de instalare.

Instalare într-un pas

Următorul este un exemplu de instalare într-un singur pas sau de conversie din modul pachet în modul de instalare:

Router#**instalați adăugați fișierul flash:ir1101-universalk9.SSA.bin activați commit**
install_add_activate_commit: START Luni 30 mai 20:45:11 UTC 2022 install_add: Adăugarea IMG

- - - Se începe sincronizarea inițială a fișierului ---
Copierea flash:ir1101-universalk9.SSA.bin de la R0 la R0 Informații: Copierea
terminată în zona selectată
S-a încheiat sincronizarea inițială a fișierului

- - - Începeți adăugarea --- Efectuarea
adăugării pentru toți membrii [1] S-a
terminat Adăugarea pachetelor la R0
Verificarea stării Adăugării pe [R0]
Adăugare: transmisă la [R0]
Terminat Adăugați

Imagine adăugată. Versiune: 17.09.01.0.157857

install_activate: Activarea IMG Următoarele pachete
vor fi activate: /flash/ir1101-mono-
universalk9.SSA.pkg /flash/ir1101-rpboot.SSA.pkg

Această operațiune poate necesita o reîncărcare a sistemului. Doriți să continuați? [da/nu]**y**

- - - Se începe activarea --- Se execută activarea
pe toți membrii Configurarea construcției...

[OK] [1] Activare pachet(e) pe R0 [1] Terminat
Activare pe R0 Verificare starea Activare pe
[R0] Activare: Transmis pe [R0]

Activare terminată

- - - Pornirea comiterii --- Efectuarea
comiterii pentru toți membrii [1] Pachete de
comitere pe R0
[1] Terminat Commit on R0 Verificarea stării
Commit on [R0] Commit: Transmis pe [R0]

S-a încheiat operațiunea de comitere

SUCCES: install_add_activate_commit Luni 30 mai 20:48:01 UTC 2022 %PMAN-5-EXITACTION: R0/0: pvp:
Managerul de proces iese: acțiunea de reîncărcare solicitată watchdog: watchdog0: watchdog nu s-a oprit!

repornire: repornirea sistemului

System Bootstrap, Versiunea 3.3(REL), SOFTWARE DE LANSAREA
Copyright (c) 1994-2021 de către Cisco Systems, Inc.

Platformă IR1101-K9 cu 4169728 Kbytes de memorie principală

Versiune MCU - Bootloader: 4, Aplicație: 6 MCU
este în modul aplicație.

. . . . . .

```
Se încarcă: bootflash:packages.conf
#

##################################################################################################
##################################################################################################
################################

%BOOT-5-OPMODE_LOG: R0/0: binos: Sistemul a pornit în modul AUTONOM Apăsați
RETURN pentru a începe!

Router#arată rezumatul instalării
[ R0 ] Informații pachet(e) instalate:
Stare (St): I - Inactiv, U - Activat și Neangajat,
                    C - Activat și angajat, D - Dezactivat și neangajat
--------------------------------------------------------------------------- Tip St File
Nume/Versiune
--------------------------------------------------------------------------- IMG C
17.09.01.0.75

--------------------------------------------------------------------------- Temporizator de
întrerupere automată: inactiv
-----------------------------------------------------------------------------------------
```

Instalare în trei etape

Următorul este un exemplu de instalare în trei etape.

```
Instalați Adăugați

Router#instalați adăugați fișierul flash:ir1101-universalk9.17.09.01.SPA.bin
install_add: START marți 31 mai 01:35:40 UTC 2022 install_add: Adăugarea IMG

- - - Se începe sincronizarea inițială a fișierului ---
Copierea flash:ir1101-universalk9.17.09.01.SPA.bin de la R0 la R0 Informații: S-a terminat
de copiat în zona selectată
S-a încheiat sincronizarea inițială a fișierului

- - - Începeți adăugarea --- Efectuarea
adăugării pentru toți membrii [1] S-a
  terminat Adăugarea pachetelor la          R0
Verificarea stării Adăugării pe [R0]
Adăugare: transmisă la [R0]
Terminat Adăugați

Imagine adăugată. Versiune: 17.09.01.0.1

SUCCES: install_add /flash1/ir1101-universalk9.17.09.01.SPA.bin marți, 31 mai, 01:37:10 UTC 2022

Router#

Router#arată rezumatul instalării
[ R0 ] Informații pachet(e) instalate:
Stare (St): I - Inactiv, U - Activat și Neangajat,
                    C - Activat și angajat, D - Dezactivat și neangajat
--------------------------------------------------------------------------- Tip St File
Nume/Versiune
--------------------------------------------------------------------------- IMG I
17.09.01.0.1

-----------------------------------------------------------------------------------------
```

Temporizator de întrerupere automată: inactiv

Instalați Activați

Router#**instalare activare**
install_activate: START marți 31 mai 01:37:14 UTC 2022 install_activate:
se activează IMG
Următoarele pachete vor fi activate: /flash/ir1101-mono-
universalk9_iot.17.09.01.SPA.pkg /flash/ir1101-
rpboot.17.09.01.SPA.pkg

Această operațiune poate necesita o reîncărcare a sistemului. Doriți să continuați? [da/nu]**y**

- - - Începe activarea --- Efectuarea activării pe
toți membrii [1] Activare pachet(e) pe R0

[1] Terminat Activare pe R0 Verificare starea
Activare pe [R0] Activare: Transmis pe [R0]

Activare terminată

SUCCES: install_activate marți 31 mai 01:41:03 UTC 2022 Router#

31 mai 01:41:08.684: %PMAN-5-EXITACTION: R0/0: pvp: Managerul de proces iese: a fost solicitată o acțiune de reîncărcare

watchdog: watchdog0: watchdog nu sa oprit! repornire:
repornirea sistemului

System Bootstrap, Versiunea 3.3(REL), SOFTWARE DE LANSAREA
Copyright (c) 1994-2021 de către Cisco Systems, Inc.

Platformă IR1101-K9 cu 4169728 Kbytes de memorie principală

Versiune MCU - Bootloader: 4, Aplicație: 6 MCU
este în modul aplicație.

. . . . . .

Se încarcă: bootflash:packages.conf
#

##
##
######################

Apăsați RETURN pentru a începe!

Router#**arată rezumatul instalării**
[R0] Informații pachet(e) instalate:
Stare (St): I - Inactiv, U - Activat și Neangajat,
C - Activat și angajat, D - Dezactivat și neangajat
---Tip St File
Nume/Versiune
---IMG U
17.09.01.0.1

---Temporizator de
întrerupere automată: inactiv

Instalați Commit

```
Router#instalați commit
install_commit: START marți 31 mai 01:47:56 UTC 2022
- - - Pornirea comiterii --- Efectuarea
comiterii pentru toți membrii [1] Pachetele
  de comitere pe R0
  [1] Pachete(e) de comitere finalizate pe R0.
Verificarea stării de comitere pe [R0] Comitare:
transmisă pe [R0]
S-a încheiat operațiunea de comitere


SUCCES: install_commit marți 31 mai 01:48:04 UTC 2022

Router#arată rezumatul instalării
[ R0 ] Informații pachet(e) instalate:
Stare (St): I - Inactiv, U - Activat și Neangajat,
                    C - Activat și angajat, D - Dezactivat și neangajat
--------------------------------------------------------------------------------Tip St File
Nume/Versiune
--------------------------------------------------------------------------------IMG C
17.09.01.0.1

--------------------------------------------------------------------------------Temporizator de
întrerupere automată: inactiv
-------------------------------------------------------------------------------------------------
```

Afișarea pachetelor instalate

```
Router#arată pachetul de instalare flash:ir1101-universalk9.17.09.01.SPA.bin
  Pachet: ir1101-universalk9.17.09.01.SPA.bin
    Dimensiune: 674114352
    Marcaj temporal:
  Cale canonică: /flash1/ir1101-universalk9.17.09.01.SPA.bin

    Sumă SHA1 fișier brut disc:
      e54ba5a59824156af7515eaf4367ebe51b920316
  Dimensiunea antetului:  1148 octeți
  Tip pachet:             30000
  Steaguri de pachet:     0
  Versiunea antetului:    3

  Informații interne ale pachetului:
    Nume: rp_super
    BuildTime: 2022-04-27_00.47
    ReleaseDate: 2022-04-27_07.05
    BootArhitecture: arm64
    RouteProcessor: IR1101
    Platformă: IR1101
    Utilizator: mcpre
    PackageName: universalk9 Build:
    17.09.01
    Tipuri de card:

  Pachetul este bootabil de pe media și tftp. Continutul
  pachetului:

  Pachet: ir1101-mono-universalk9_iot.17.09.01.SPA.pkg
    Dimensiune: 673776700
    Marcaj temporal:

    Sumă SHA1 fișier brut disc:
```

```
Dimensiunea antetului:  1084 de octeți
Tip pachet:             30000
Steaguri de pachet:     0
Versiunea antetului:    3

Informații interne ale pachetului:
   Nume: mono
   BuildTime: 2022-04-27_00.47
   ReleaseDate: 2022-04-27_07.05
   BootArhitecture: arm64
   RouteProcessor: IR1101
   Platformă: IR1101
   Utilizator: mcpre
   PackageName: mono-universalk9_iot Build:
   17.09.01
   Tipuri de card:

Pachetul este bootabil de pe media și tftp. Continutul
pachetului:
```

Puteți determina ce pachet este activ utilizând**arată instalarea activă**comanda.

```
Router#arată instalarea activă
[ R0 ] Informații pachet(e) activ(e):
Stare (St): I - Inactiv, U - Activat și neangajat, C - Activat și angajat, D -
Dezactivat și neangajat
--------------------------------------------------------------------------------Tip St File
Nume/Versiune
--------------------------------------------------------------------------------IMG C
17.09.01.0.193

--------------------------------------------------------------------------------Temporizator de
întrerupere automată: inactiv
-------------------------------------------------------------------------------------------------
```

Se afișează pachetele angajate și neangajate

Aceste două comenzi show oferă informații despre pachetele care sunt comise și care nu sunt comise.

```
Router#arată instalarea comisă
[ R0 ] Informații pachet(e) angajat(e):
Stare (St): I - Inactiv, U - Activat și Neangajat,
                C - Activat și angajat, D - Dezactivat și neangajat
--------------------------------------------------------------------------------Tip St File
Nume/Versiune
--------------------------------------------------------------------------------IMG C
17.09.01.0.1

--------------------------------------------------------------------------------Temporizator de
întrerupere automată: inactiv
-------------------------------------------------------------------------------------------------

Router#arată instalarea necommitată
[ R0 ] Informații despre pachete neangajate:
Stare (St): I - Inactiv, U - Activat și Neangajat,
                C - Activat și angajat, D - Dezactivat și neangajat
--------------------------------------------------------------------------------Tip St File
Nume/Versiune
--------------------------------------------------------------------------------Fără pachete
neangajate
```

Eliminarea pachetelor inactive

Această comandă va elimina fișierele de instalare neutilizate (.conf/.pkg/.bin) din mediul de instalare.

Nota Această comandă este folosită pentru a curăța directorul de pornire al fișierelor de instalare neutilizate. Aceasta nu va elimina imaginea bootabilă.

```
Router#install remove inactiv install_remove: START marți 31 mai
01:49:10 UTC 2022 install_remove: eliminarea IMG

Curățarea fișierelor de pachete inutile
Nicio cale specificată, va folosi calea pornită /bootflash/packages.conf

Curățare/bliț
  Scanarea directorului de pornire pentru pachete... gata. Se
  pregătește lista de pachete pentru ștergere...
    [R0]: /flash/packages.conf Fișierul este în uz, nu se va șterge.
    [R0]: /flash/ir1101-mono-universalk9_iot.17.09.01.SPA.pkg Fișierul este în uz, nu se va șterge.

    [R0]: /flash/ir1101-universalk9.17.09.01.SPA.conf Fișierul este în uz, nu se va șterge. [R0]: /flash/ir1101-
    rpboot.17.09.01.SPA.pkg Fișierul este în uz, nu se va șterge.

Următoarele fișiere vor fi șterse:
    [R0]: /flash/ir1101-universalk9.17.09.01.SPA.bin [R0]: /flash/
    ir1101-mono-universalk9_iot.SSA.pkg [R0]: /flash/ir1101-
    universalk9.SSA.conf [R0]: /flash/ir1101-universalk9.SSA.conf
    [R0]: /flash/SSA.

Doriți să eliminați fișierele de mai sus? [da/nu]y


Ștergerea fișierului /flash/ir1101-universalk9.17.09.01.SPA.bin ... gata. Ștergerea fișierului /
flash/ir1101-mono-universalk9_iot.SSA.pkg ... gata. Ștergerea fișierului /flash/ir1101-
universalk9.SSA.conf ... gata. Ștergerea fișierului /flash/ir1101-rpboot.SSA.pkg ... gata.

Ștergerea /bootflash/.images/17.09.01.0.1.1651045630 ... gata. SUCCES: Fișierele au
fost șterse.

- - - Se începe Post_Remove_Cleanup --- Se efectuează
REMOVE_POSTCHECK pe toți membrii S-a terminat
Post_Remove_Cleanup
SUCCES: install_remove marți 31 mai 01:49:14 UTC 2022

Router#arată instalarea inactivă
[ R0 ] Informații pachet(e) inactiv(e):
Stare (St): I - Inactiv, U - Activat și Neangajat,
            C - Activat și angajat, D - Dezactivat și neangajat
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - Tip St File
Nume/Versiune
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - Nu există
pachete inactive
```

Depanarea instalării software-ului utilizând comenzile de instalare

ProblemăDepanarea instalării software-ului

SoluţieUtilizați următoarele comenzi show pentru a vizualiza rezumatul instalării, jurnalele și versiunile de software.

- **arată rezumatul instalării**
- **arată jurnalul de instalare**
- **arata versiunea**
- **arată versiunea care rulează**

ProblemăAlte probleme de instalare

SoluţieUtilizați următoarele comenzi pentru a rezolva problema de instalare:

- **dir <***directorul de instalare***>**
- **mai multe locatii:***pachete.conf*
- **Arată instalarea suportului tehnic**: această comandă rulează automat**spectacol**comenzi care afișează informații specifice instalării.
- **cerere platforma software trace arhiva target bootflash <***locaţie***>**: această comandă arhivează toate jurnalele de urmărire relevante pentru toate procesele care rulează pe sistem de la ultima reîncărcare și salvează aceste informații în locația specificată.

CAPITOL 10

Instalarea software-ului

Acest capitol conține următoarele secțiuni:

Instalarea software-ului

Instalarea software-ului pe router presupune instalarea unui pachet consolidat (imagine bootabilă). Acesta constă dintr-un pachet de subpachete (unități software modulare), fiecare subpachet controlând un set diferit de funcții.

Este mai bine să actualizați software-ul într-o perioadă planificată de întreținere, când o întrerupere a serviciului este acceptabilă. Routerul trebuie repornit pentru ca o actualizare de software să aibă efect.

Licențiere

Această secțiune conține următoarele:

Licențiere software Cisco

Licențiarea software Cisco constă în procese și componente pentru a activa seturile de caracteristici software Cisco IOS prin obținerea și validarea licențelor software Cisco.

Puteți activa funcțiile cu licență și puteți stoca fișiere de licență în bootflash-ul routerului. Licențele se referă la pachete consolidate, pachete tehnologice sau caracteristici individuale.

IR1800 folosește licențierea inteligentă îmbunătățită, care este discutată în detaliu în capitolul următor.

Pachete consolidate

Pentru a obține imagini software pentru router, accesați:https://software.cisco.com/download/home/286200112

Nota Este posibil ca toate caracteristicile IOS-XE să nu se aplice la IR1800. Este posibil ca unele funcții să nu fi fost implementate încă sau să nu fie adecvate pentru această platformă.

O licență bazată pe imagini este utilizată pentru a ajuta la afișarea tuturor subsistemelor care corespund unei licențe. Această licență este aplicată numai în momentul pornirii.

Una dintre următoarele licențe bazate pe imagini poate fi preinstalată pe routerul IR1800:

- Network-Essentials
- Rețea-Avantaj

Nota Detalii despre conținutul Network-Essentials și Network-Advantage pot fi găsite înfișa tehnică a produsului.

Network-Essentials

The**Network-Essentials**pachetul de tehnologie include caracteristicile de bază. De asemenea, acceptă funcții de securitate.

The**Network-Essentials_npe**pachetul tehnologic (npe = No Payload Encryption) include toate caracteristicile din pachetul tehnologic Network-Essentials fără funcționalitatea de criptare a încărcăturii utile. Acest lucru este pentru a îndeplini cerințele de restricție la export. Network-Essentials_npe este disponibil numai în imaginea Network-Essentials_npe. Diferența de caracteristici dintre pachetul Network-Essentials și pachetul Network-Essentials_npe este, prin urmare, setul de caracteristici de criptare a încărcăturii utile, cum ar fi IPsec și Secure VPN.

Rețea-Avantaj

The**Rețea-Avantaj**Pachetul de tehnologie include toate caracteristicile cripto.

The**Network-Advantage_npe**pachetul (npe = No Payload Encryption) include toate caracteristicile din **Rețea-Avantaj**pachet tehnologic fără funcționalitatea de criptare a sarcinii utile. Acest lucru este pentru a îndeplini cerințele de restricție la export. The**Network-Advantage_npe**pachetul este disponibil numai în **Network-Advantage_npe**imagine. Diferența de caracteristici dintre**Rețea-Avantaj**pachetul și**Network-Advantage_npe** pachetul este, prin urmare, un set de caracteristici care permit criptarea sarcinii utile, cum ar fi IPsec și Secure VPN.

Cum se instalează software-ul pentru Cisco IOS XE

Pentru a instala software-ul, utilizați una dintre următoarele metode descrise în această secțiune pentru a utiliza software-ul dintr-un pachet consolidat sau dintr-un pachet individual.

Instalarea versiunii Cisco IOS XE

Când dispozitivul pornește cu imaginea Cisco IOS XE pentru prima dată, dispozitivul verifică versiunea instalată a ROMMON și face upgrade dacă sistemul rulează o versiune mai veche. În timpul upgrade-ului, nu opriți dispozitivul. Sistemul pornește automat dispozitivul după ce este instalat noul ROMMON. După instalare, sistemul va porni cu imaginea Cisco IOS XE în mod normal.

Nota Când dispozitivul pornește pentru prima dată și dacă dispozitivul necesită o actualizare, întregul proces de pornire poate dura câteva minute. Acest proces va fi mai lung decât o pornire normală din cauza upgrade-ului ROMMON.

Următorul exemplu ilustrează procesul de boot al unui pachet consolidat:

Router#**configura terminalul**
Router(config)#**sistemul de pornire bootflash:/ir1800-universalk9.17.06.01prd18.SPA.bin**
Router(config)#**config-register 0x2102** Router(config)#**Ieșire**

* 7 noiembrie 00:07:06.784: %SYS-5-CONFIG_I: configurat din consolă de către consolă

Router#
Router#**show run | licență inc** licență udi pid IR1800-
K9 sn FCW2150TH0F licență nivel de încărcare avantaj
de rețea Router#

Router#**reincarca?**

/noverify	Nu verificați semnătura fișierului înainte de reîncărcare.
/verifica	Verificați semnătura fișierului înainte de reîncărcare.
la	Reîncărcați la o anumită oră/data
anula	Anulează în așteptarea reîncărcării
în	Reîncărcare după un interval de timp
pauză	Pauză în timpul reîncărcării
motiv	Reîncărcați motivul
<cr>	<cr>

Router#**reîncărcare/verificare**

Configurația sistemului a fost modificată. Salva? [da/nu]:**Da** Configurația
clădirii...

[BINE]
* nov 7 00:08:48.101: %SYS-2-PRIVCFG_ENCRYPT: Fișier de configurare privat criptat cu succes
Verificarea integrității fișierului bootflash:/ir1800-
universalk9.17.06.01prd18.SPA.bin..... . . . . .

Hash încorporat SHA1 : B0315BDC4F545D624BB128CE0FFAA468E6EF7587 SHA1 :
Hash calculat B0315BDC4F545D624BB128CE0FFAA468E6EF7587
Începe verificarea imaginii Hash
Computation: 100% gata!
Hash SHA2 calculat: 03febcc07fbeadeed664f2f5ef87f6c3
5b343e6f7aecdd70e50e5203909aec8f
3d276529d2a6af6859d4c77237f812d5
0da93678edc942c8874edca2d5224101

Hash încorporat SHA2: 03febcc07fbeadeed664f2f5ef87f6c3
5b343e6f7aecdd70e50e5203909aec8f
3d276529d2a6af6859d4c77237f812d5
0da93678edc942c8874edca2d5224101

Semnătură digitală verificată cu succes în fișierul bootflash:/ir1800-universalk9.16.10.01.SPA.bin Semnătură verificată

Continuați cu reîncărcarea? [confirma]**<Enter>**

* 9 iulie 06:43:37.910: %SYS-5-RELOAD: Reîncărcarea solicitată de consolă. Motiv pentru reîncărcare: Comanda de reîncărcare. 9 iulie 14:43:59.134: %PMAN-5-EXITACTION: R0/0: pvp: Managerul de proces se iese: ieșirea procesului cu codul șasiului de reîncărcare

watchdog watchdog0: watchdog nu sa oprit! repornire:
repornirea sistemului

Apăsați RETURN pentru a începe!

ROMMON Imagini

O imagine ROMMON este un pachet software utilizat de software-ul ROM Monitor (ROMMON) pe un router. Pachetul software este separat de pachetul consolidat utilizat în mod normal pentru pornirea routerului.

O imagine independentă ROMMON (pachet software) poate fi lansată ocazional, iar routerul poate fi actualizat cu noul software ROMMON. Pentru instrucțiuni detaliate, consultați documentația care însoțește imaginea ROMMON.

Nota O nouă versiune a imaginii ROMMON nu este neapărat lansată în același timp cu un pachet consolidat pentru un router.

Sisteme de fișiere

Următorul tabel oferă o listă de sisteme de fișiere care pot fi văzute pe routerul Cisco IR1800.

Tabelul 13: Sisteme de fișiere router

Sistem de fișiere	Descriere
bootflash:	Porniți sistemul de fișiere cu memorie flash.
flash:	Alias pentru sistemul de fișiere cu memoria flash de pornire de mai sus.
cns:	Directorul de fișiere Cisco Networking Services.
nvram:	Router NVRAM. Puteți copia configurația de pornire în NVRAM sau din NVRAM.
obfl:	Sistem de fișiere pentru fișierele Onboard Failure Logging (OBFL).
sistem:	Sistem de fișiere din memoria sistemului, care include configurația de rulare.
gudron:	Sistem de fișiere de arhivare.
tmpsys:	Sistem de fișiere temporare de sistem.
usbflash0:	Sistemele de fișiere ale unității flash USB (Universal Serial Bus). **Nota** Sistemul de fișiere al unității flash USB este vizibil numai dacă o unitate USB este instalată în portul USB. **Nota** Pot fi utilizate numai unități flash USB acceptate de Cisco. O listă de dispozitive acceptate se găsește înGhid de instalare hardware

Utilizați**?**opțiune de ajutor dacă găsiți un sistem de fișiere care nu este listat în tabelul de mai sus.

Opțiune pentru a activa sau dezactiva accesul USB

Unitățile flash USB oferă spațiu de stocare ușor și ieftin pentru routere pentru a stoca imaginile, fișierele de configurare și alte fișiere.

Nota IR1800 acceptă sisteme de fișiere ext2 și vfat pentru unitățile flash USB. Pot fi utilizate numai unități flash USB aprobate de Cisco.

IR1800 acceptă conectarea/deconectarea la cald a unităților flash USB. Pentru a accesa unitatea flash USB, introduceți dispozitivul în interfața USB a routerului. Odată ce USB-ul este recunoscut, pe consolă se vede un mesaj de alertă:

1 august 11:08:53.198 PDT: %IOSD_INFRA-6-IFS_DEVICE_OIR: Dispozitiv usbflash0 adăugat

După ce se vede acest mesaj, unitatea flash USB este accesibilă. Utilizatorii pot accesa conținutul USB utilizând **dir usbflash0:**comanda:

```
Dispozitiv#dir usbflash0:
Directorul usbflash0:/
    5   drwx          512   23 august 2019 10:42:18 -07:00 27   Informații despre volumul sistemului
    6   - rwx          35   august 2019 17:40:38 -07:00         test.txt
206472192 octeți în total (206470144 octeți gratuit)
Dispozitiv#
```

Conținutul poate fi copiat pe și de pe unitatea flash USB utilizând comanda copiere. Odată ce copia este finalizată, este afișat un mesaj de jurnal care arată numărul de octeți copiați.

```
Dispozitiv#copiere flash:test.txt usbflash0: Nume
fișier de destinație [test.txt]?<Intră> Copie în curs...C

35 octeți copiați în 0,020 secunde (1750 octeți/sec) Dispozitiv #
```

În timp ce conectarea/deconectarea la cald a unei unități flash USB este acceptată, funcționalitatea vine cu vulnerabilități de securitate. Pentru a împiedica utilizatorii să copieze informații sensibile pe unitatea flash USB, a fost adăugată funcționalitatea de activare/dezactivare USB.

În mod implicit, unitatea flash USB este activată. Dacă un utilizator dorește să dezactiveze USB, poate face acest lucru folosind comanda disable:

```
Dispozitiv#terminalul de configurare Dispozitiv
(config) #dezactivarea usb platformei

Dispozitiv (config) #Sfârşit
```

Odată ce unitatea flash USB a fost dezactivată, sistemul de fișiere nu este afișat pe Dispozitiv și mesajele syslog nu vor fi afișate atunci când USB este introdus. Utilizatorii nu vor putea accesa conținutul USB.

De exemplu:

```
Dispozitiv#dir usbflash0:
dir usbflash0:
     ^
% Intrare nevalidă detectată la marcatorul „^”.
Dispozitiv#
```

USB-ul este activat prin emiterea unui „**nu**' cu comanda dezactivare:

```
Dispozitiv#terminalul de configurare

Dispozitiv (config) #nicio platformă usb dezactivată
Dispozitiv (config) #Sfârşit
```

Starea USB poate fi afișată folosind următoarea comandă:

```
Dispozitiv#arată starea usb platformei
USB activat
Dispozitiv#
```

Portul USB ar putea fi considerat un potențial risc de securitate. Dacă doriți să dezactivați portul USB, urmați acești pași:

```
Configurați terminalul
dezactivarea usb platformei
Ieșire

arata platforma usb
```

Directoare și fișiere generate automat

Această secțiune discută fișierele și directoarele autogenerate care pot fi create și modul în care fișierele din aceste directoare pot fi gestionate.

Tabelul 14: Fișiere autogenerate

Fișier sau Director	Descriere
fișiere crashinfo	Fișierele Crashinfo pot apărea în sistemul de fișiere bootflash:. Aceste fișiere oferă informații descriptive despre un accident și pot fi utile în scopuri de reglare sau depanare. Cu toate acestea, fișierele nu fac parte din operațiunile routerului și pot fi șterse fără a afecta funcționarea routerului.
directorul de bază	Zona de stocare pentru fișierele .core. Dacă acest director este șters, se va regenera automat la pornire. Fișierele .core din acest director pot fi șterse fără a afecta funcționalitatea routerului, dar directorul în sine nu trebuie șters.
directorul administrat	Acest director este creat la pornire dacă se efectuează o verificare a sistemului. Aspectul său este complet normal și nu indică probleme cu routerul.
directorul tracelogs	Zona de stocare a fișierelor de urmărire. Fișierele de urmărire sunt utile pentru depanarea. Dacă procesul Cisco IOS eșuează, de exemplu, utilizatorii sau personalul de depanare pot accesa fișierele de urmărire folosind modul de diagnosticare pentru a aduna informații legate de defecțiunea Cisco IOS. Cu toate acestea, fișierele de urmărire nu fac parte din operațiunile routerului și pot fi șterse fără a afecta performanța routerului.

Note importante despre directoarele autogenerate Informațiile

importante despre directoarele autogenerate includ:

- Fișierele generate automat pe bootflash: directorul nu ar trebui să fie șters, redenumit, mutat sau modificat în niciun fel decât dacă este indicat de asistența pentru clienți Cisco.

Nota Modificarea fișierelor cu generare automată pe bootflash: poate avea consecințe imprevizibile asupra performanței sistemului.

- Fișierele Crashinfo și fișierele din directorul core și tracelogs pot fi șterse.

Stocare flash

Subpachetele sunt instalate pe stocarea media locală, cum ar fi flash. Pentru stocarea flash, utilizați**dir bootflash:** comandă pentru a lista numele fișierelor.

Nota Stocarea flash este necesară pentru funcționarea cu succes a unui router.

Indicatoare LED

Pentru informații despre LED-urile de pe router, consultați „Indicatori LED” din secțiunea „Prezentare generală a produsului” din Ghid de instalare hardware.

Pentru a monitoriza starea LED-urilor a sistemului, porturile de alarmă și de interfață, linia de comandă show LED este acceptată în modul IOS.

Router#**arată LED-ul**
LED SISTEM: verde

LED GigabitEthernet0/0/0: activat LED
GigabitEthernet0/1/0: oprit LED
GigabitEthernet0/1/1: oprit LED
GigabitEthernet0/1/2: oprit LED
GigabitEthernet0/1/3: oprit

* celular 0/4*
LED activare modul LTE: LED verde SIM
0 al modulului LTE: LED verde al
modulului LTE SIM 1: LED galben al
modulului LTE GPS: stins
LED modulul LTE RSSI 0 : pe
modulul LTE LED RSSI 1 : pe
modulul LTE LED RSSI 2 : pe
modulul LTE LED RSSI 3 : aprins

* celular 0/5*
LED activare modul LTE: LED verde SIM
0 al modulului LTE: LED verde al
modulului LTE SIM 1: oprit LED GPS al
modulului LTE: oprit
Modul LTE RSSI 0 LED : Aprins

LED modulul LTE RSSI 1 : pe modulul
LTE LED RSSI 2 : pornit modulul LTE
LED RSSI 3 : oprit router#

Documentație aferentă

Pentru mai multe informații despre licențele software, consultați capitolul Smart Licensing.

Avertisment de downgrade IOS XE

Această caracteristică va prezenta un avertisment la emiterea unui**sistemul de pornire flash**comanda urmată de un nume de fișier al unei imagini care are un număr de versiune mai mic decât cel al imaginii care rulează. Operația de downgrade va fi în continuare posibilă ignorând mesajul de avertizare prezentat utilizatorului. Pornirea unei imagini cu aceeași versiune sau o versiune superioară a imaginii care rulează este permisă fără avertisment. Caracteristica este destinată doar imaginilor deja încărcate pe bootflash-ul routerului, aceasta înseamnă doar pentru**sistemul de pornire flash***<nume_fișier>*CLI (excluzând alte surse/dispozitive precum ftp, mop, rpc, tftp, rom).

Următoarele sunt exemple de modul în care sistemul compară versiunile:

Când comparați două numere de versiune, după cum urmează:

- 17.7.1
- 17.7.1c

Versiunea cu litera (17.7.1c) va fi considerată cea mai actualizată.

Când comparați două numere de versiune, după cum urmează:

- 17.7.3a
- 17.7.3f

Comparația se va face ținând cont de ordinea alfabetică. În cazul de mai sus, 17.7.3f va fi considerat cel mai actualizat.

Activați capabilitățile de ștergere sigură a datelor

Ștergerea securizată a datelor este o inițiativă la scară largă a Cisco pentru a se asigura că dispozitivele de stocare de pe toate platformele bazate pe IOS XE vor fi curățate în mod corespunzător utilizând comenzile de ștergere securizată conforme NIST SP 800-88r1. Ori de câte ori este posibil, platformele IoT vor folosi proiectarea și implementarea ENG corespunzătoare disponibile până acum pe platformele lor.

Această caracteristică este acceptată pe următoarele platforme IoT:

- IR1101
- IR1800
- IR8140
- ESR6300

Când activarea ștergerii securizate a datelor este executată, următoarele vor fi șterse:

- IR1101, IR1800, IR8140: NVRAM, variabile rommon și bootflash
- ESR6300: NVARM, variabile rommon, bootflash

Routerul va fi în promptul rommon cu setările implicite din fabrică (rată de transmisie 9600) după ce comanda este executată. Flash-ul de boot nu va fi formatat până la pornirea cu imagine IOS prin usbflash sau descărcare tftp dacă platforma este acceptată.

Efectuarea unei ștergeri securizate de date

Pentru a activa funcția, efectuați următoarele:

Router#**resetarea din fabrică este sigură**
Operația de resetare din fabrică este ireversibilă pentru resetarea în siguranță a tuturor. esti sigur? [confirma]**Y**

Important Această operațiune poate dura ore. Vă rugăm să nu deconectați.

Pentru a verifica jurnalul după executarea comenzii și pornirea IOS XE, efectuați următoarele:

Router#**afișați jurnalul securizat de resetare din fabrică a software-ului platformei**
Jurnal de resetare din fabrică:
RAPORT CISCO DE SANITIZARE DATE: # IR1800 Purge
Cipul ACT2 la 12-08-2022, 15:17:28 Cipul ACT2 Purge realizat
la 12-08-2022, 15:17:29
mtd și ștergerea flash de rezervă încep la 12-08-2022, 15:17:29 mtd și
ștergerea flash de rezervă finalizată la 12-08-2022, 15:17:29.

CAPITOL 11

Upgrade de întreținere software (SMU)

Această secțiune conține următoarele:

Upgrade de întreținere software (SMU)

Actualizarea de întreținere software (SMU) este un pachet care poate fi instalat pe un sistem pentru a oferi o remediere a corecțiilor sau o rezoluție de securitate unei imagini lansate pentru un defect specific, pentru a răspunde la probleme imediate. Nu conține funcții noi.

Nota Instalarea SMU a fost acceptată atât în modul de pornire a pachetului, cât și în modul de instalare. Din Cisco IOS XE Release 17.9.x, instalarea SMU va fi oprită dacă routerul este pornit în modul pachet. Dacă routerul este pornit în modul de instalare, instalarea SMU va continua să funcționeze așa cum este în versiunile anterioare.

Unele dintre avertismentele SMU sunt:

- Furnizat pe o versiune, pe bază de componentă și este specific platformei. Versiunile SMU sunt sincronizate cu versiunile majore, minore și de întreținere ale pachetului pe care le actualizează.
- SMU-urile nu sunt o alternativă la versiunile de întreținere. Toate defectele remediate de SMU-uri sunt apoi integrate automat în versiunile de întreținere viitoare.
- Platforma Cisco IOS XE validează intern compatibilitatea SMU și nu vă permite să instalați SMU-uri necompatibile. Acest lucru se bazează pe reguli/limitări pentru un set de modificări SMU.
- Un SMU oferă un beneficiu semnificativ față de software-ul IOS clasic, deoarece vă permite să rezolvați rapid problema rețelei, reducând în același timp timpul și domeniul de aplicare al testării necesare.
- SMU este o metodă de remediere a erorilor dintr-o versiune existentă și permite aplicarea unei remedieri PSIRT într-o versiune existentă.
- SMU NU este o cale de actualizare de la versiunea X la versiunea de întreținere X.1

• SMU NU este o cale de actualizare de la versiunea X la versiunea Y

Dispozitivul acceptă doar „Hot Patching”. Acest lucru înseamnă:

• Imaginea care rulează este modificată la locul sau în serviciu

• Acest lucru evită timpul de nefuncţionare şi întreruperea serviciului

• Codul actualizat pentru a remedia defectul este scris într-o altă locație și unde patch-ul redirecționează rularea programului

Fluxul de lucru al SMU și cerințele de bază

Fluxul de lucru pentru corecție necesită să finalizați următoarea secvență de operare în modul exec:

1.Adăugarea SMU la sistemul de fișiere

2.Activarea SMU în sistem

3.Angajarea schimbării SMU

4.Îndepărtarea și dezinstalarea SMU-ului

Cerințele de bază pentru SMU sunt:

• Imaginea în care a fost descoperit defectul

• Fișierul de corecție care conține remedierea defectului trebuie să fie formatat ca ir1800-image_name.release_version.CSCxxyyyyy.SPA.smu.bin

Exemplu SMU

Această secțiune arată un exemplu de patch creat ca test. Patch-ul dvs. va avea un nume asociat cu un CDET pentru a fi instalat ca remediere.

Instalarea unei imagini de corecție

Efectuați următorii pași pentru a instala imaginea de corecție:

Procedură

Pasul 1 Afișați o comandă standard.

```
Router#arata putere
PSU principal:
    Putere totală consumată: 11,37 wați Mod
    configurat: N/A
    Starea curentă de rulare aceeași: N/A Sursă
    de alimentare: Modul extern PS POE:
```

Mod configurat: N/A Starea curentă de
rulare aceeași: N/A Putere totală
disponibilă: 30 Watt Router#

Pasul 2 Adăugați imaginea.

Router#**instalați adăugați fișier bootflash:ir1800-universalk9.2020-08-06_10.38.0.CSCxx12345.SSA.smu.bin** install_add: START Joi, 6 august 11:52:52 PDT 2020 cat: /tmp/patch/patch.sta: Nu există un astfel de fișier sau director
install_add: Adăugarea SMU

install_add: se verifică dacă noua adăugare este permisă...

- - - Pornirea operației SMU Add --- Efectuarea SMU_ADD pe Active/Standby
[1] Pachete SMU_ADD pe R0
[1] Terminat SMU_ADD pe R0 Verificarea stării SMU_ADD pe [R0] SMU_ADD: transmis pe [R0]
Operațiunea de adăugare SMU finalizată

SUCCES: install_add joi, 6 august 11:53:31 PDT 2020

Router#

Pasul 3 Activați imaginea patch-ului.

Router#**instalați fișierul de activare bootflash:ir1800-universalk9.2020-08-06_10.38.0.CSCxx12345.SSA.smu.bin** install_activate: START joi, 6 august 11:53:59 PDT 2020

Configurația sistemului a fost modificată.
Apăsați Da(y) pentru a salva configurația și continua. Apăsați Nu(n) pentru a continua fără a salva configurația.
Apăsați Ieșire (q) pentru a ieși, puteți salva configurația și reintroduceți comanda. [a/n/q]**y** Configurație clădire... [OK]Configurația modificată a fost salvată install_activate: Se activează SMU

Executarea pre-scripturilor....
Executarea pre-scripturilor gata.

- - - Pornirea operațiunii de activare SMU --- Efectuarea SMU_ACTIVATE pe Active/Standby /usr/sbin/kgv_update: kgv_update [/flash1/ir1800-universalk9.2020-08-06_10.38.0.CSCxx12345.SSA. smu este în continuare....binics, NU.smu local.

/usr/sbin/kgv_update: Semnătura validată pentru /flash1/ir1800-universalk9.2020-08-06_10.38.0.CSCxx12345.SSA.smu.bin /usr/sbin/kgv_update: TAM hash len:32
val:4407CBB447F0EEE3B12120D902F48FBA1C0D4900EED1FB614441198BE2302934 /usr/sbin/kgv_update: PCR8 înainte de extindere ctr:2
0817449B454BF036AF9D593D726D94D8942C50A9FFE93278FDA78EA62F2989F2 /usr/sbin/kgv_update: PCR8 după extindere ctr:3
EF5F579FCDFA989D044296F0584B99F719F2B6215895524B5E8AD55DF5671560 /usr/sbin/kgv_update: extinderea PCR cu succes
/usr/sbin/kgv_update: Chasfs actualizat pentru numele:ir1800-universalk9.2020-08-06_10.38.0.CSCxx12345.SSA.smu.bin hash:975352C1562A492D582D09D5BB91230863F6CC18E6F9C0EB512AF27CC0C77
E2C05F29596AD34AD7808C9B39EC23D4412F0D3AFA707BC906FE03D554A845E42D4 /usr/sbin/kgv_update: Actualizare reușită pentru
ir1800-universalk9.2020-08-06_10.38.0.CSCxx12345.SSA.smu.bin
[1] pachet(e) SMU_ACTIVATE pe R0

```
    [1] Terminat SMU_ACTIVATE pe R0 Verificarea stării
SMU_ACTIVATE pe [R0] SMU_ACTIVATE: transmis pe
[R0]
SMU terminat Activați operațiunea
SUCCES: install_activate /flash1/ir1800-universalk9.2020-08-06_10.38.0.CSCxx12345.SSA.smu.bin Joi 6 Aug 11:55:14 PDT
2020
Router#
```

Pasul 4 Angajați instalarea.

```
Router#instalați commit
install_commit: START Thu Aug         6 11:55:29 PDT 2020
install_commit: Se execută SMU
Executarea scripturilor preliminare...
Executarea scripturilor preliminare gata.
- - - Pornirea operațiunii SMU Commit --- Efectuarea
SMU_COMMIT pe Active/Standby
    [1] Pachete SMU_COMMIT pe R0
    [1] Terminat SMU_COMMIT pe R0 Verificarea
stării SMU_COMMIT pe [R0] SMU_COMMIT:
transmis pe [R0]
Operațiunea SMU Commit s-a încheiat

SUCCES: install_commit /flash1/ir1800-universalk9.2020-08-06_10.38.0.CSCxx12345.SSA.smu.bin Joi, 6 august 11:56:08 PDT
2020
Router#
```

Pasul 5 Afișați rezumatul stării procedurii de instalare.

```
Router#arată rezumatul instalării
[ R0 ] Informații pachet(e) instalate:
Stare (St): I - Inactiv, U - Activat și Neangajat,
                       C - Activat și angajat, D - Dezactivat și neangajat
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - Tip St File
Nume/Versiune
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - IMG
           C        17.04.01.0.118999
SMU     C        flash:ir1800-universalk9.2020-08-06_10.38.0.CSCxx12345.SSA.smu.bin

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - Temporizator de
întrerupere automată: inactiv
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - Router#
```

Pasul 6 Verificați rezultatul patch-ului afișând aceeași comandă.

```
Router#arata putere
PSU principal:
        Putere totală consumată: 11,04 wați
Dispozitivul HOT SMU funcționează!

        Mod configurat: N/A Starea curentă de
        rulare aceeași: N/A Sursă de alimentare:
        Modul extern PS POE:

        Mod configurat: N/A Starea curentă de
        rulare aceeași: N/A Putere totală
        disponibilă: 0 Watt Router#
```

Dezinstalarea imaginii de corecție

Există două metode de a elimina sau dezinstala imaginea de corecție.

- Restaurarea imaginii la versiunea sa originală utilizând următoarea comandă:
  - **instalați rollback la bază**
- Eliminarea specifică a unui patch prin utilizarea următoarelor comenzi în secvență:
  - **instalați dezactivați fișierul flash:***<fișier>*
  - **instalați commit**
  - **instalați șterge fișierul flash:***<fișier>*

Dezinstalarea imaginii de corecție utilizând Rollback

Această secțiune prezintă un exemplu de utilizare a metodei rollback.

Arată ce patch-uri sunt instalate:

```
Router#arată rezumatul instalării
[ R0 ] Informații pachet(e) instalate:
Stare (St): I - Inactiv, U - Activat și Neangajat,
                C - Activat și angajat, D - Dezactivat și neangajat
--------------------------------------------------------------------------------Tip St File
Nume/Versiune
--------------------------------------------------------------------IMG
        C       17.04.01.0.118999
SMU     C       flash:ir1800-universalk9.2020-08-06_10.38.0.CSCxx12345.SSA.smu.bin

--------------------------------------------------------------------------------Temporizator de
întrerupere automată: inactiv
--------------------------------------------------------------------------------Router#
```

Sunt disponibile următoarele comenzi:

```
Router#instala?
  avorta                    Anulați operațiunea de instalare curentă Activați
  activa                    un pachet instalat Instalați un fișier de pachet în
  adăuga                    sistem Instalați cronometrul auto-abort
  temporizator de anulare automată
  comite                    Commiteți modificările în calea de încărcare
  dezactivați               Dezactivați un pachet de instalare
  eticheta                  Adăugați un nume de etichetă la orice punct de instalare
  pregăti                   Pregătiți pachetul pentru funcționare
  elimina                   Eliminați pachetele instalate
  rollback                  Reveniți la un punct de instalare anterior
Router#instalați rollback la ?
  baza          Reveniți la imaginea de bază
  comise        Revenire la ultimul punct de instalare confirmat Revenire la un
  id            anumit ID punct de instalare
  eticheta      Reveniți la o etichetă de punct de instalare specifică
```

The**instalați rollback la bază**comanda elimină întregul patch și revine la versiunea de bază a imaginii cu defectul găsit.

```
Router#instalați rollback la bază install_rollback: START joi, 6 august
12:04:04 PDT 2020 install_rollback: derularea SMU

Executarea pre-scripturilor....
Executarea pre-scripturilor gata.

- - - Pornirea operațiunii SMU Rollback --- Efectuarea
SMU_ROLLBACK pe Activ/Standby
    [1] Pachetul(e) SMU_ROLLBACK pe R0
    [1] Terminat SMU_ROLLBACK pe R0 Verificarea
stării SMU_ROLLBACK pe [R0] SMU_ROLLBACK:
transmis pe [R0]
Operațiunea SMU Rollback finalizată

CSCxx12345:SUCCES
SUCCES: install_rollback /flash1/ir1800-universalk9.2020-08-06_10.38_shchang2.0.CSCxx12345.SSA.smu.bin Joi Aug
12:04:57 PDT 2020                                                                                         6

Router#
```

Arată ce patch-uri sunt instalate:

```
Router#arată rezumatul instalării
[ R0 ] Informații pachet(e) instalate:
Stare (St): I - Inactiv, U - Activat și Neangajat,
                        C - Activat și angajat, D - Dezactivat și neangajat
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - Tip St File
Nume/Versiune
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - IMG C
17.04.01.0.18

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - Temporizator de
întrerupere automată: inactiv
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - Router#
```

Nota În rezultatul comenzii de mai sus, patch-ul a fost eliminat și dispozitivul revine la versiunea de bază a imaginii înainte de actualizare.

Verificați rezultatul patch-ului afișând aceeași comandă.

```
Router#arata putere
PSU principal:
        Putere totală consumată: 11,98 wați Mod
        configurat: N/A
        Starea curentă de rulare aceeași: N/A Sursă
        de alimentare: Modulul extern PS POE:

        Mod configurat: N/A Starea curentă de
        rulare aceeași: N/A Putere totală
        disponibilă: 30 Watt Router#
```

Dezinstalarea imaginii de corecție utilizând Deactivate, Commit și Remove

În următoarea secvență, există două corecții instalate pe dispozitiv. CSCvq11111 și CSCvt22222 Numai CSCvt22222 va fi eliminat.

Arată ce patch-uri sunt instalate.

```
Router#arată rezumatul instalării
[ R0 ] Informații pachet(e) instalate:
Stare (St): I - Inactiv, U - Activat și Neangajat,
                    C - Activat și angajat, D - Dezactivat și neangajat
--------------------------------------------------------------------------------- Tip St File
Nume/Versiune
--------------------------------------------------------------------------- SMU
         C       /flash1/ir1800-universalk9.<lansare>.CSCvq11111.SPA.smu.bin /flash1/ir1800-
SMU      C       universalk9.<lansare>.CSCvt22222.SPA.smu.bin 17.04.1
IMG      C
```

Procedură

Pasul 1 Dezactivați patch-ul.

```
Router#instalați dezactivați fișierul flash:ir1800-universalk9.<release>.CSCvt22222.SPA.smu.bin install_deactivate:
START vineri, 24 apr 22:54:10 UTC 2020 install_deactivate: Se dezactivează SMU

Executarea pre-scripturilor....
Executarea pre-scripturilor gata.

- - - Pornirea operațiunii de dezactivare SMU --- Efectuarea
SMU_DEACTIVATE pe activ/standby
   [R0] Pachetul(e) SMU_DEACTIVATE pe R0 [R0]
   Terminat SMU_DEACTIVATE pe R0 Se verifică starea
SMU_DEACTIVATE pe [R0] SMU_DEACTIVATE: Transmis
pe [R0]
Operațiunea de dezactivare SMU terminată

SUCCES: install_deactivate /flash1/ir1800-universalk9.<release>.CSCvt22222.SPA.smu.bin Vine, 24 aprilie 22:54:49 UTC 2020
```

Arată ce patch-uri sunt instalate:

```
Router#arată rezumatul instalării
[ R0 ] Informații pachet(e) instalate:
Stare (St): I - Inactiv, U - Activat și Neangajat,
                    C - Activat și angajat, D - Dezactivat și neangajat
--------------------------------------------------------------------------------- Tip St File
Nume/Versiune
--------------------------------------------------------------------------- SMU
         C       /flash1/ir1800-universalk9.<lansare>.CSCvt11111.SPA.smu.bin /flash1/ir1800-
SMU      D       universalk9.<lansare>.CSCvt22222.SPA.smu.bin 17.01.1
IMG      C
```

Pasul 2 Angajați acțiunea.

```
Router#instalați commit
install_commit: START vineri, 24 apr 22:56:11 UTC 2020
install_commit: se angajează SMU
```

```
* 24 aprilie 22:56:15.169: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: S-a început instalarea commitExecutarea
  scripturilor prealabile....
Executarea pre-sript-urilor gata.
- - - Pornirea operațiunii SMU Commit --- Efectuarea
SMU_COMMIT pe Active/Standby
    [R0] Pachetul(e) SMU_COMMIT pe R0 [R0]
    Terminat SMU_COMMIT pe R0 Verificarea stării
SMU_COMMIT pe [R0] SMU_COMMIT: Transmis pe
[R0]
Operațiunea SMU Commit s-a încheiat

SUCCES: install_commit /flash1/ir1800-universalk9.<release>.CSCvt22222.SPA.smu.bin Vineri, 24 aprilie 22:56:32 UTC 2020


* 24 apr 22:56:33.342: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: SMU de comitere de instalare
finalizată
```

Arată ce patch-uri sunt instalate:

```
Router#arată rezumatul instalării
[ R0 ] Informații pachet(e) instalate:
Stare (St): I - Inactiv, U - Activat și Neangajat,
                        C - Activat și angajat, D - Dezactivat și neangajat
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - Tip St File
Nume/Versiune
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - SMU
            C       /flash1/ir1800-universalk9.<lansare>.CSCvt11111.SPA.smu.bin /flash1/ir1800-
SMU     eu      universalk9.<lansare>.CSCvt22222.SPA.smu.bin <lansare>
IMG     C
```

Pasul 3 Scoateți plasturele.

```
Router#instalați șterge fișierul flash:ir1800-universalk9.<release>.CSCvt22222.SPA.smu.bin install_remove:
START vineri, 24 apr 22:57:17 UTC 2020

* 24 aprilie 22:57:20.775: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Instalarea a început remove flash:ir1800-
  universalk9.<release>.CSCvt22222.SPA.smu.bininstall_remove: Eliminarea SMU

Executarea pre-scripturilor....
Executarea pre-scripturilor terminată.

- - - Pornirea operațiunii SMU Eliminare --- Efectuarea
SMU_REMOVE pe Activ/Standby
    [R0] Pachetul(e) SMU_REMOVE pe R0 [R0]
    Terminat SMU_REMOVE pe R0 Verificarea stării
SMU_REMOVE pe [R0] SMU_REMOVE: Transmis pe
[R0]
Operațiunea de eliminare a SMU terminată

SUCCES: install_remove /flash1/ir1800-universalk9.<release>.CSCvt22222.SPA.smu.bin Vineri, 24 aprilie 22:57:34 UTC 2020


* 24 apr 22:57:34.902: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Instalare finalizată eliminați
flash:ir1800-universalk9.<release>.CSCvt22222.SPA.smu.bin
```

Arată ce patch-uri sunt instalate:

```
Router#arată rezumatul instalării
[ R0 ] Informații pachet(e) instalate:
Stare (St): I - Inactiv, U - Activat și Neangajat,
                        C - Activat și angajat, D - Dezactivat și neangajat
```

```
---------------------------------------------------------------------------- Tip St File
Nume/Versiune
---------------------------------------------------------------------------- SMU
        C       /flash1/ir1800-universalk9.<lansare>.CSCvt11111.SPA.smu.bin <lansare>
IMG     C
```

CAPITOL 12

Politica de utilizare a licențelor inteligente

Acest capitol conține următoarele secțiuni:

Prezentare generală a SLP

Smart Licensing Using Policy (SLP), cunoscut anterior ca Smart Licensing Enhanced (SLE), este modul implicit pentru routerele IoT. SLE a înlocuit Smart Software Licensing.

Acest ghid acceptă toate routerele IoT și înlocuiește capitolele individuale din fiecare dintre ghidurile de configurare a software-ului.

Următoarele secțiuni arată caracteristicile și diferențele software dintre routerele IoT.

IR1800

Seria IR1800 acceptă doar SLP. Unele dintre diferențele de caracteristici sunt:

- Suportul a început cu versiunea IOS-XE 17.3.2
- Un cod de autorizare este necesar numai pentru cerința de control la export
- Debitul mai mare de 250 MB necesită o licență HSEC
- Nu mai sunt licențe EVAL. Starea de autorizat s-a schimbat în În uz sau Neutilizat cu o clasă Tip de aplicare.
- Cisco Smart Licensing Utility (CSLU) este un nou instrument de interfață între dispozitive și Cisco Smart Software Manager (CSSM) în anumite topologii ale clienților.

IR1101

Seria IR1100 acceptă doar SLP. Unele dintre diferențele de caracteristici sunt:

- Suportul a început cu versiunea IOS-XE 17.3.2

• Un cod de autorizare este necesar numai pentru cerința de control la export

• Nu mai sunt licențe EVAL. Starea de autorizat s-a schimbat în În uz sau Neutilizat cu o clasă Tip de aplicare.

• Cisco Smart Licensing Utility (CSLU) este un nou instrument de interfață între dispozitive și Cisco Smart Software Manager (CSSM) în anumite topologii ale clienților.

• Debitul este implicit și este limitat la 250 MB.

IR8100

Seria IR8100 acceptă doar SLP. Unele dintre diferențele de caracteristici sunt:

• Suportul a început cu versiunea IOS-XE 17.3.2

• Un cod de autorizare este necesar numai pentru cerința de control la export

• Debitul mai mare de 250 Mbps necesită o licență HSEC

• Nu mai sunt licențe EVAL. Starea de autorizat s-a schimbat în În uz sau Neutilizat cu o clasă Tip de aplicare.

• Cisco Smart Licensing Utility (CSLU) este un nou instrument de interfață între dispozitive și Cisco Smart Software Manager (CSSM) în anumite topologii ale clienților.

IR8300

Seria IR8300 acceptă doar SLP. Unele dintre diferențele de caracteristici sunt:

• Suportul a început cu versiunea IOS-XE 17.3.2

• Un cod de autorizare este necesar numai pentru cerința de control la export

• Debitul mai mare de 250 Mbps necesită o licență HSEC

• Nu mai sunt licențe EVAL. Starea de autorizat s-a schimbat în În uz sau Neutilizat cu o clasă Tip de aplicare.

• Cisco Smart Licensing Utility (CSLU) este un nou instrument de interfață între dispozitive și Cisco Smart Software Manager (CSSM) în anumite topologii ale clienților.

ESR6300

Routerul încorporat ESR6300 funcționează ușor diferit față de celelalte routere IoT. Unele dintre diferențele de caracteristici sunt:

• Suportul a început cu versiunea IOS-XE 17.4.1

• Un cod de autorizare este necesar numai pentru cerința de control la export

• Debitul mai mare de 250 Mbps necesită o licență HSEC

• Nu mai sunt licențe EVAL. Starea de autorizat s-a schimbat în În uz sau Neutilizat cu o clasă Tip de aplicare.

• Cisco Smart Licensing Utility (CSLU) este un nou instrument de interfață între dispozitive și Cisco Smart Software Manager (CSSM) în anumite topologii ale clienților.

Tipuri de aplicare a licențelor

O anumită licență aparține unuia dintre cele trei tipuri de aplicare. Tipul de aplicare indică dacă licența necesită autorizare înainte de utilizare sau nu.

- Neaplicat sau neaplicat

Marea majoritate a licențelor aparțin acestui tip de aplicare. Licențele neaplicate nu necesită autorizare înainte de a fi utilizate în rețele cu întrerupere sau de înregistrare în rețelele conectate. Termenii de utilizare pentru astfel de licențe sunt conform acordului de licență pentru utilizatorul final (EULA).

- Aplicat

Licențele care aparțin acestui tip de aplicare necesită autorizare înainte de utilizare. Autorizarea necesară este sub forma unui cod de autorizare, care trebuie instalat în instanța produsului corespunzătoare.

Un exemplu de licență impusă este licența Client Media Redundancy Protocol (MRP), care este disponibilă pe comutatoarele Industrial Ethernet.

- Export controlat

Licențele care aparțin acestui tip de aplicare sunt restricționate la export de legile SUA privind controlul comerțului și aceste licențe necesită autorizare înainte de utilizare. Codul de autorizare necesar trebuie instalat și în instanța de produs corespunzătoare și pentru aceste licențe. Cisco poate preinstala licențe controlate de export atunci când sunt comandate cu achiziționarea de hardware.

Un exemplu de licență controlată de export este licența de înaltă securitate (HSEC), care este disponibilă pe anumite routere Cisco.

Licență de înaltă securitate (HSEC).

Licența HSEC (High Security) este o licență de caracteristici care poate fi configurată în plus față de licența de rețea (NE/NA). O licență HSEC oferă controale la export pentru niveluri puternice de criptare. HSEC este disponibil pentru clienții din toate țările care nu sunt în prezent sub embargo, așa cum sunt enumerate de Departamentul de Comerț al SUA. Fără o licență HSEC, performanța SEC este limitată la un total de 250 Mbps de debit IPsec în fiecare direcție. O licență HSEC elimină această limitare.

Interfață de linie de comandă

Modul de configurare CLI pentru a activa HSEC pe IR1101 este următorul:

IR1101(config)#**caracteristica licenței hsec9**

Pentru a beneficia de licența HSEC, va fi disponibilă o nouă lățime de bandă. Noua lățime de bandă este numită **necapsulat**și este disponibil cu următorul CLI din modul de configurare:

IR1101(config)#**nivelul de debit hardware al platformei?** Debit de
250 M în bps Debit nelimitat în bps

IR1101#**Nivelul de debit hardware al platformei nelimitat**

După efectuarea comenzilor de mai sus, scrieți mem și reîncărcați routerul. Configurația va intra în vigoare când routerul revine.

Tipuri de licență

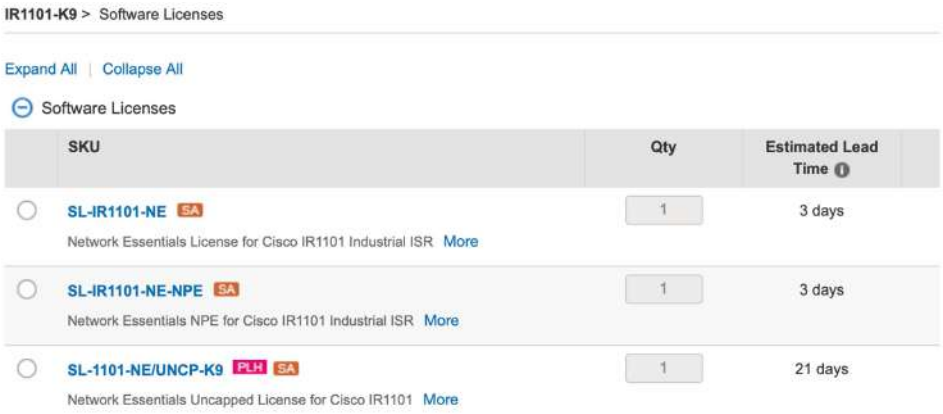
Cu această nouă caracteristică, IR1101 va accepta următoarele tipuri de lățime de bandă/licență:

- Rețea esențială 250 Mbps
- Avantaj de rețea 250 Mbps
- Elemente esențiale ale rețelei nelimitate
- Avantaj de rețea nelimitat
- HSEC

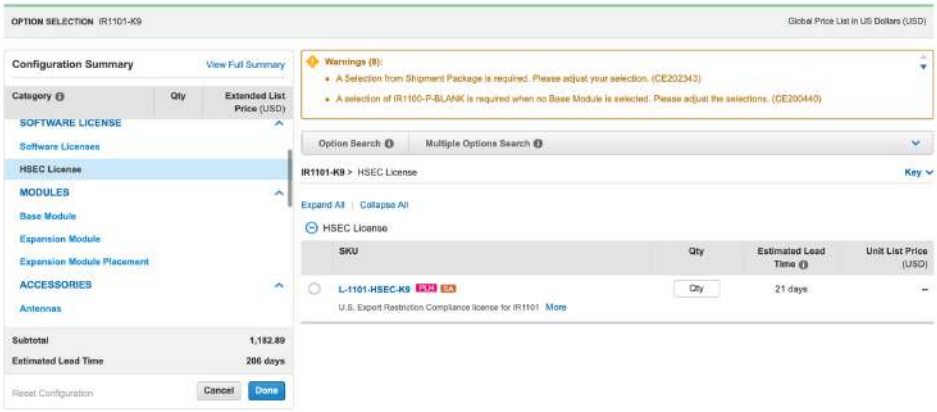
Comandă

Următorul este un exemplu de la IR1101-K9. Licența va fi disponibilă și pe IR1101-A-K9.

În exemplul următor, selectați SL-1101-NE/UNCP-K9 (Network Essentials Uncapped License):



Licența L-1101-HSEC-K9 va fi inclusă automat atunci când selectați licența nelimitată, după cum se arată în următoarele:



Cisco Software Central

Acest ghid oferă informații despre cum să comandați, să activați și să gestionați licențele Cisco Smart.

https://software.cisco.com/software/csws/ws/platform/home?locale=en_US&locale=en_US&locale=en_US#

Arhitectura SLP

Această secțiune explică diferitele componente care pot face parte din implementarea SLP.

Instanță de produs

O instanță de produs este o singură instanță a unui produs Cisco, identificată printr-un identificator unic de dispozitiv (UDI).

O instanță de produs înregistrează și raportează utilizarea licenței (rapoarte RUM) și oferă alerte și mesaje de sistem despre rapoartele restante, eșecuri de comunicare etc. Rapoartele RUM și datele de utilizare sunt, de asemenea, stocate în siguranță în instanța produsului.

Un raport de măsurare a utilizării resurselor (raport RUM) este un raport de utilizare a licenței, care îndeplinește cerințele de raportare specificate de politică. Rapoartele RUM sunt generate de instanța produsului și consumate de CSSM. Instanța produsului înregistrează informații despre utilizarea licenței și toate modificările de utilizare a licenței într-un raport RUM deschis. La intervale determinate de sistem, rapoartele RUM deschise sunt închise și noi rapoarte RUM sunt deschise pentru a continua înregistrarea utilizării licenței. Un raport RUM închis este gata pentru a fi trimis către CSSM.

O confirmare RUM (RUM ACK sau ACK) este un răspuns de la CSSM și oferă informații despre starea unui raport RUM. Odată ce ACK pentru un raport este disponibil pe instanța produsului, acesta indică faptul că raportul RUM corespunzător nu mai este necesar și poate fi șters.

CSSM afișează informații despre utilizarea licenței conform ultimului raport RUM primit.

Cisco Smart Software Manager (CSSM)

CSSM este un portal care vă permite să gestionați toate licențele software Cisco dintr-o locație centralizată. CSSM vă ajută să gestionați cerințele actuale și să revizuiți tendințele de utilizare pentru a planifica cerințele viitoare de licență.

Puteți accesa CSSM lahttps://software.cisco.com. Sub fila Licență, faceți clic pe linkul Smart Software Licensing.

În CSSM puteți:

- Creați, gestionați sau vizualizați conturi virtuale.
- Creați și gestionați jetoane de înregistrare a instanțelor de produs.
- Transferați licențe între conturi virtuale sau vizualizați licențe.
- Transferați, eliminați sau vizualizați instanțe de produs.
- Rulați rapoarte pentru conturile dvs. virtuale.
- Modificați setările de notificare prin e-mail.
- Vizualizați informații generale despre cont.

Înainte de a utiliza CSSM, vă rugăm să vizualizați un scurt videoclip despre cum să utilizați portalul, găsit aici:

https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html

Faceți clic pe**Vizualizați videoclipul**buton.

Cisco Smart Licensing Utility (CSLU)

CSLU este un utilitar de raportare bazat pe Windows care oferă fluxuri de lucru agregate de licențiere. Vă ajută să vă administrați toate licențele și instanțele de produse asociate acestora de la sediul dumneavoastră, în loc să vă conectați la CSSM.

Acest utilitar îndeplinește următoarele funcții cheie:

- Oferă opțiunile referitoare la modul în care sunt declanșate fluxurile de lucru. Fluxurile de lucru pot fi declanșate de CSLU sau de instanța produsului,
- Colectează rapoarte de utilizare din instanța produsului și încarcă aceste rapoarte de utilizare în contul inteligent sau contul virtual corespunzător – online sau offline, folosind fișiere. În mod similar, ACK-ul raportului RUM este colectat online sau offline și furnizat înapoi instanței produsului.
- Trimite cereri de coduri de autorizare către CSSM și primește coduri de autorizare1 de la CSSM.

CSLU poate face parte din topologia dvs. SLP în următoarele moduri:

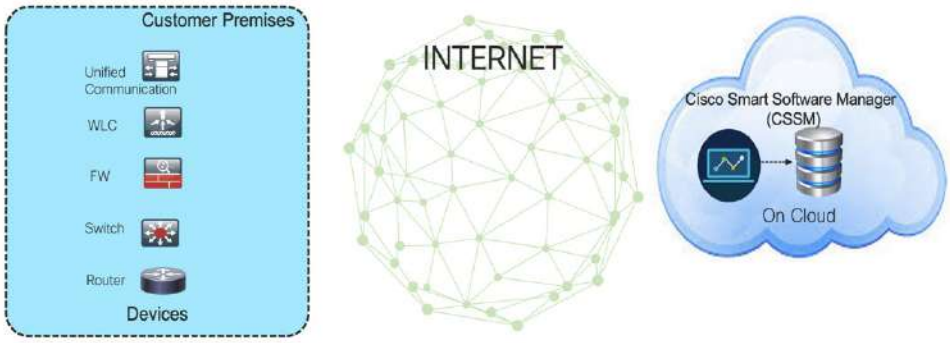
- Instalați aplicația Windows, pentru a utiliza CSLU ca unealtă autonomă și conectați-o la CSSM.
- Instalați aplicația Windows, pentru a utiliza CSLU ca unealtă autonomă și nu o conectați la CSSM. Cu această opțiune, informațiile de utilizare necesare sunt descărcate într-un fișier și apoi încărcate în CSSM. Acest lucru este potrivit pentru rețelele cu aer întrefier.
- Încorporați-l într-un controler, cum ar fi Cisco DNA Center.

Topologii client

Platformele de rutare IoT folosesc două topologii diferite.

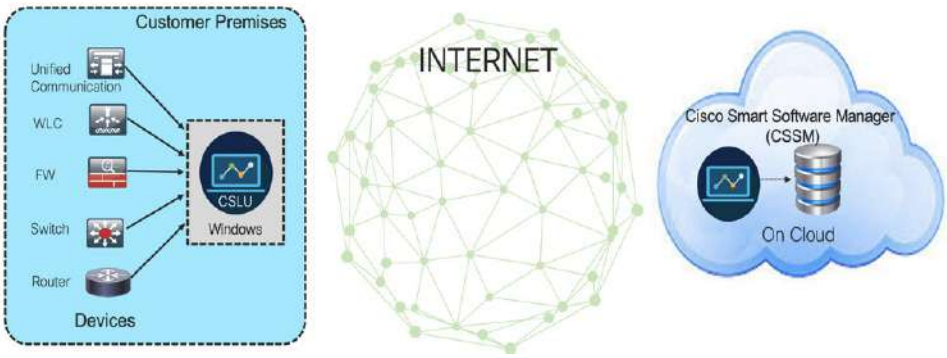
- Acces offline complet
- CSLU nu are acces la CSSM

Următoarea figură ilustrează accesul offline complet:



În această topologie, dispozitivele nu au conectivitate la CSSM (software.cisco.com). Utilizatorul trebuie să copieze și să insereze informații între produsele Cisco și CSSM pentru a verifica manual licențele.

Următoarea figură ilustrează CSLU care nu are acces la CSSM:



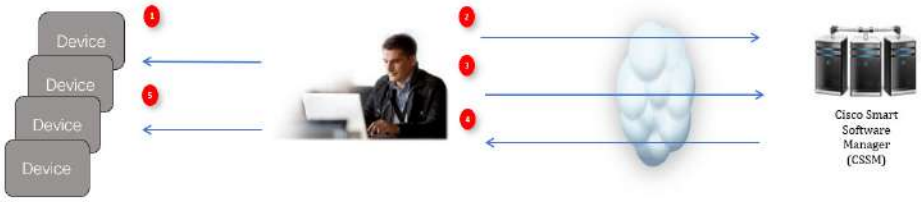
În această topologie, dispozitivele sunt conectate la controlerul CSLU, dar nu există conectivitate între CSLU și CSSM (Cisco Smart Software Manager – software.cisco.com).

Dispozitivele Cisco vor trimite informații de utilizare către un CSLU instalat local. Utilizatorul trebuie să copieze și să insereze informații între CSLU și CSSM pentru a face check-in și check-out manual licențe.

Procedura de instalare a licenței - Topologie completă de acces offline

Această procedură necesită un schimb manual de informații necesare între router și CSSM.

Consultați următorul grafic pentru fluxul de informații:



1.Generați un fișier de date de utilizare a licenței sau o solicitare de cod de autorizare

2.Exportați în CSSM

3.Încărcați datele de utilizare a licenței sau cererea de cod de autorizare

4.Exportați fișierul ACK/AuthRequest pe router

5.Încărcați fișierul ACK sau AuthRequestAuthCode

Această secțiune conține următoarele subiecte:

Procedura de înregistrare a instanței de produs în CSSM

Procedură

Pasul 1 Generați un fișier de utilizare a licenței de pe router.

În modul exec, efectuați următoarele:

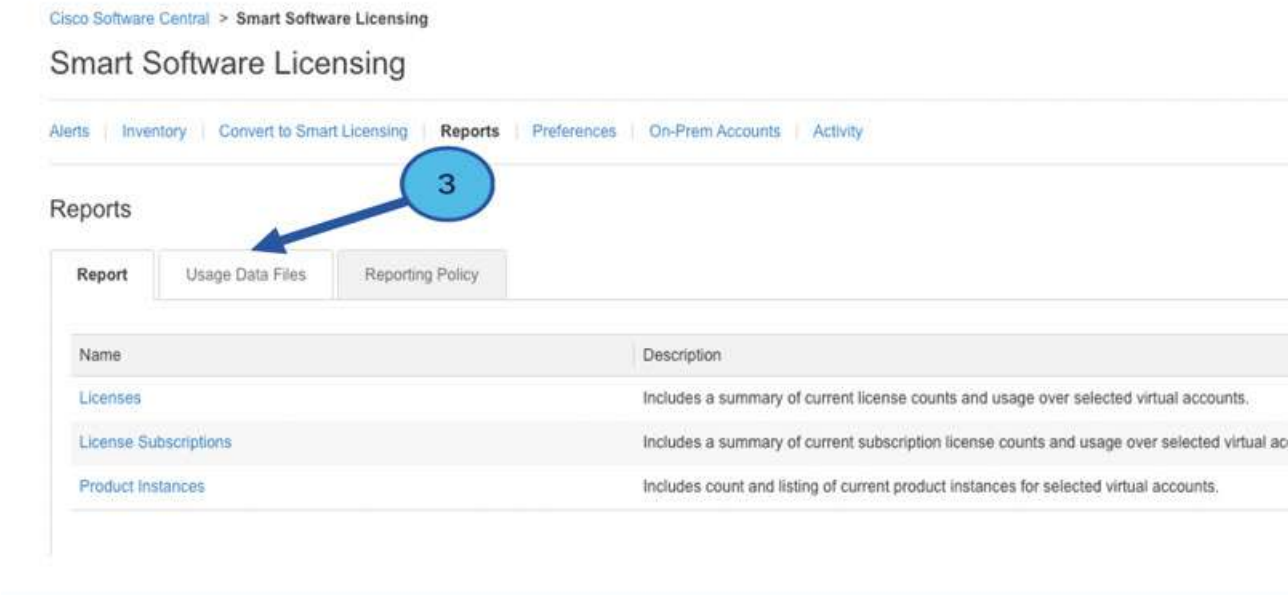
Exemplu:

Router#**licență inteligent salvare utilizare toate fișierele flash:slp**

Pasul 2 Exportați fișierul de utilizare a licenței (slp) pe laptopul/PC-ul gazdă.

Pasul 3 Importul fișierului de utilizare a licenței în CSSM on Cloud. Faceți clic pe**Fișiere de date de utilizare**fila.

Figura 23: Fișier de date de utilizare



Pasul 4 The**Încărcați date de utilizare**apare fereastra. Clic**Răsfoiește**și navigați până unde se află fișierul.

Pasul 5 Faceți clic pe**Încărcați date**.

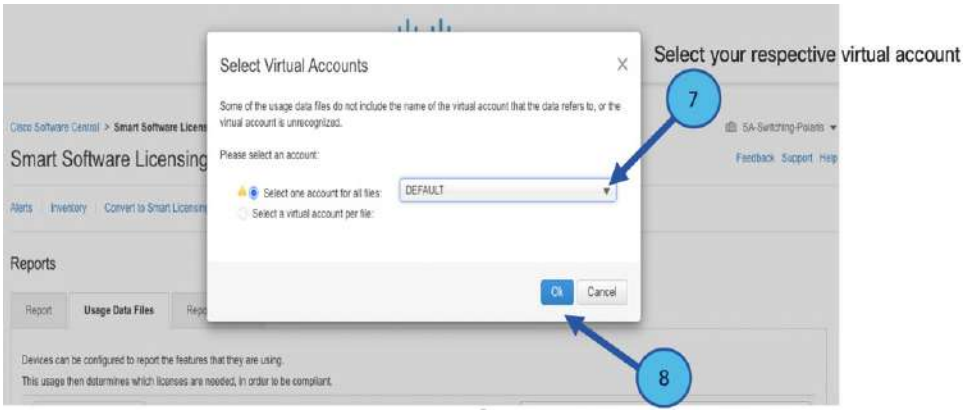
Figura 24: Răsfoiți și încărcați

Pasul 6 Selectați contul virtual.

Figura 25: Selectați cont

Pasul 7 Din meniul derulant, selectați contul virtual respectiv.

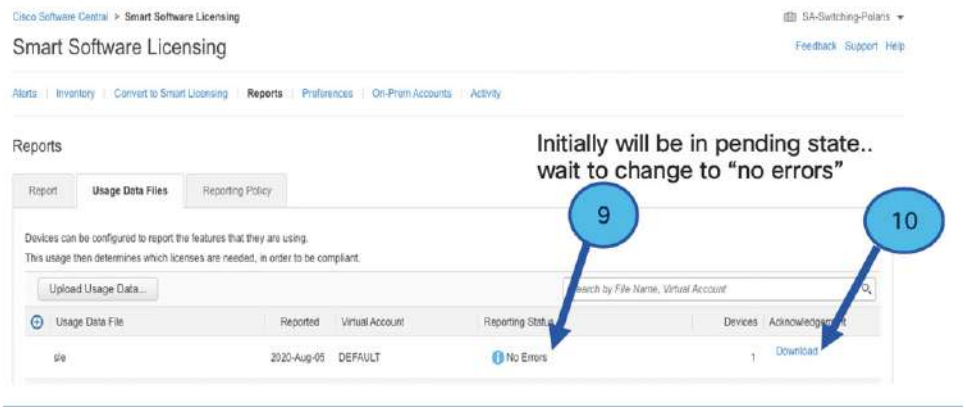
Figura 26: Selectați contul dvs



Pasul 8 Clic**Bine**.

Pasul 9 Observați fereastra Smart Software Licensing. Inițial, starea de raportare va fi**În așteptare**. Așteptați până când fereastra se reflectă**Fără erori**înainte de a continua.

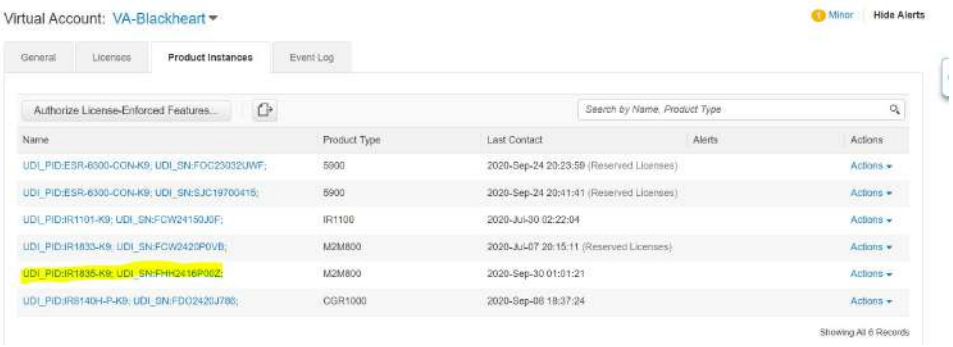
Figura 27: Starea raportării



Pasul 10 Clic**Descărcați**pentru a descărca fișierul ACK.

Pasul 11 Verificați sub**Instanțe de produs**pentru a verifica dispozitivul dvs. este listat.

Figura 28: Instanțe de produs



Nota
Acest exemplu arată un IR1835 evidențiat. Numele produsului dvs. poate fi diferit.

Pasul 12 Importați fișierul ACK din CSSM pe dispozitiv utilizând interfața de linie de comandă.

Importul fișierului ACK din CSSM pe dispozitiv

Procedură

Pasul 1 Copiați fișierul ACK din CSSM pe laptop-ul gazdă sau pe dispozitivul USB. În modul exec pe dispozitiv:

Exemplu:

```
Router#licență smart import <flash: | usbflash0:> ACK_slp Import de date
cu succes
Router#
* sept     1 21:12:58.576: %SIP-1-LICENSING: Serviciul SIP este activ. Raportul de licență a fost confirmat. 1 21:12:58.616:
* sept     %SMART_LIC-6-POLICY_INSTALL_SUCCESS: O nouă politică de licențiere a fost
instalat cu succes
```

Pasul 2 Verificați că Instanța produsului a importat datele.

a) Următorul exemplu este de la un IR1800:

Exemplu:

```
Router#arată utilizarea licenței
Autorizarea licenței:
    Stare: Nu se aplică
network-advantage_250M (IR1800_P_250M_A):
    Descriere: network-advantage_250M Număr: 1

    Versiune: 1.0
    Stare: ÎN UTILIZARE
    Stare export: NU RESTRICȚIONAT Nume
    caracteristică: network-advantage_250M
```

```
    Descrierea caracteristicii: network-advantage_250M Tip de
    aplicare: NU APLICAT
```

b) Următorul exemplu este de la un ESR6300:

Exemplu:

```
Router#arată utilizarea licenței
Autorizarea licenței:
    Stare: Nu se aplică
network-advantage_250M (ESR6300_P_250M_A):
    Descriere: network-advantage_250M Număr: 1

    Versiune: 1.0
    Stare: ÎN UTILIZARE
    Starea exportului: NU RESTRICȚIONAT Nume
    caracteristică: network-advantage_250M Descrierea
    caracteristicii: network-advantage_250M Tip de aplicare:
    NU APLICAT
```

Pasul 3 Verificați că licența este în uz.

a) Următorul exemplu este de la un IR1800:

Exemplu:

```
Router#arată rezumatul licenței
Utilizarea licenței:
    Licență                                    Eticheta de drept                    Conta
Stare
    ------------------------------------------------------------------------------------------------------------

    network-advantage_250M (IR1800_P_250M_A)          1          ÎN UTILIZARE

Router#
Router#arata licenta toate | implorați Raportarea utilizării:
Raportare de utilizare:
    Ultimul ACK primit: 01 septembrie 21:12:58 2020 UTC
    Următorul termen limită ACK: <niciun>
    Interval de raportare: 0 (fără raportare)
    Următoarea verificare push ACK: <niciun>
    Următorul raport push: <none> Ultimul
    raport push: <none> Ultimul raport fișier
    scris: <none>
Cod de încredere instalat: 01 septembrie 00:28:48 2020 UTC
```

b) Următorul exemplu este de la un ESR6300:

Exemplu:

```
Router#arată rezumatul licenței
Utilizarea licenței:
    Licență                                    Eticheta de drept                    Conta
Stare
    ------------------------------------------------------------------------------------------------------------

    network-advantage_250M (ESR6300_P_250M_A)         1          ÎN UTILIZARE

Router#
Router#arata licenta toate | Beg Raportare utilizare:
Raportare de utilizare:
    Ultimul ACK primit: 01 septembrie 21:12:58 2020 UTC
    Următorul termen limită ACK: <niciun>
    Interval de raportare: 0 (fără raportare)
    Următoarea verificare push ACK: <niciun>
```

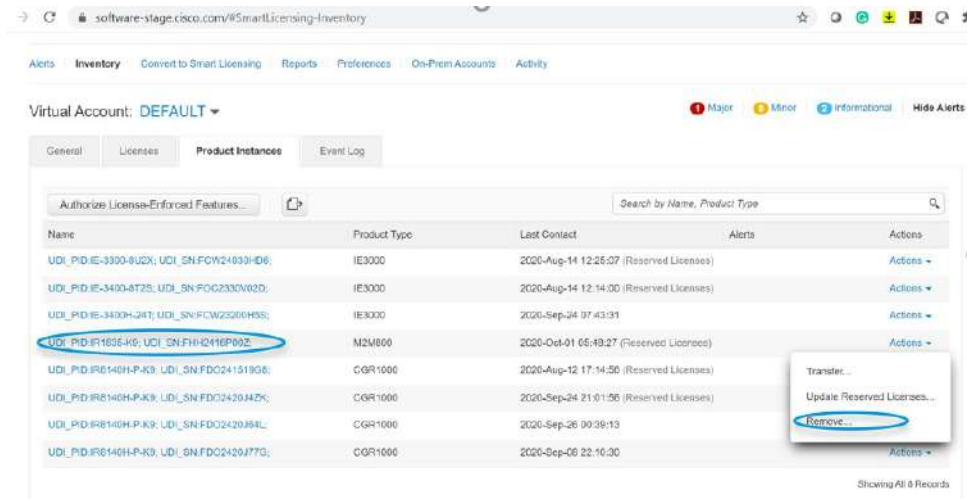
Următorul raport push: <none> Ultimul
raport push: <none> Ultimul raport fișier
scris: <none>
Cod de încredere instalat: 01 septembrie 00:28:48 2020 UTC

Eliminarea dispozitivului din CSSM

Procedură

Pasul 1 Navigați înapoi la fila Instanțe de produs. Găsiți dispozitivul dvs.

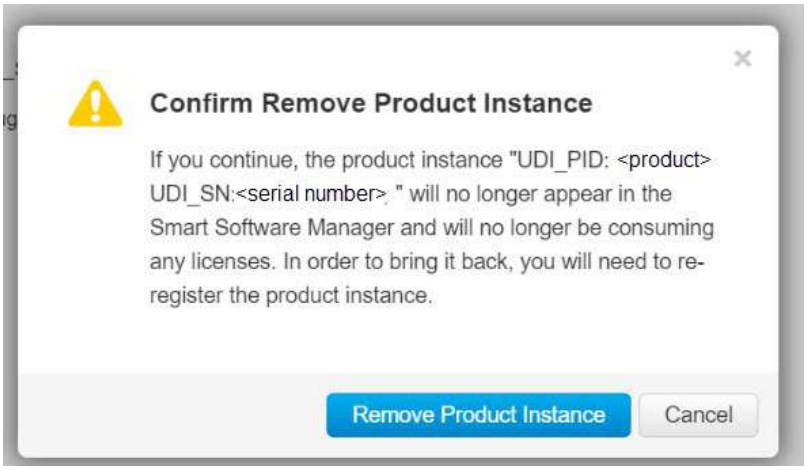
Figura 29: Instanțe de produs



Pasul 2 Faceți clic pe**Acțiuni**lângă dispozitivul dvs. și, din acele opțiuni, faceți clic**Elimina**.

Apare fereastra Confirm Remove Product Instance.

Figura 30: Confirmați eliminarea instanței produsului

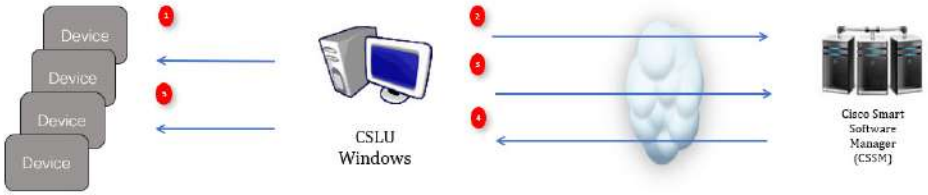


Pasul 3 Clic**Eliminați Instanța produsului**.

Procedura de instalare a licenței - CSLU nu are acces la CSSM

Această procedură realizează un schimb online de informații necesare între Router și CSLU.

Consultați următorul grafic pentru fluxul de informații:



Procedură

Pasul 1 În CSLU, identificați dispozitivele care necesită un AuthCode și inițiați solicitarea. Este creat un fișier AuthCode.

Pasul 2 Exportați fișierul AuthCode în CSSM.

Pasul 3 Încărcați AuthCode în contul CSSM SA/VA. Exportați

Pasul 4 fișierul AuthRequestAuthcode în CSLU. Încărcați

Pasul 5 fișierul ACK sau AuthRequestAuthCode.

Ce să faci în continuare

Această secțiune conține următoarele:

Procedura atunci când dispozitivele sunt conectate la CSLU

Mai întâi, efectuați acești pași pe router folosind CLI pentru a obține o licență UDI:

Exemplu dintr-un IR1800:

Router#**arată rezumatul licenței**
Rezervarea licenței este ACTIVATĂ
Utilizarea licenței:
Starea numărului de etichete de drepturi de licență
- Network-essentials_250M (IR1800M_P_E_E_2)

Router#**configura terminalul**
Introduceți comenzile de configurare, una pe linie. Încheiați cu CNTL/Z.
Router(config)#**nivel de debit hardware al platformei 2G** % Nivelul de debit 2G necesită licență hseck9! Router(config)#**Sfârşit**

Router#**sh licență udi**
UDI: PID:IR1835-K9,SN:FHH2416P00Z

Exemplu de la un ESR6300:

Router#**arată rezumatul licenței**
Rezervarea licenței este ACTIVATĂ Utilizarea licenței: Eticheta de drept al licenței Stare număr network-advantage_250M (ESR6300 _P_250M_A) 1 ÎN UTILIZARE

Router#**configura terminalul**
Introduceți comenzile de configurare, una pe linie. Încheiați cu CNTL/Z.
Router(config)#platform nivel de debit hardware 2G
% Nivelul de debit 2G necesită licență hseck9!

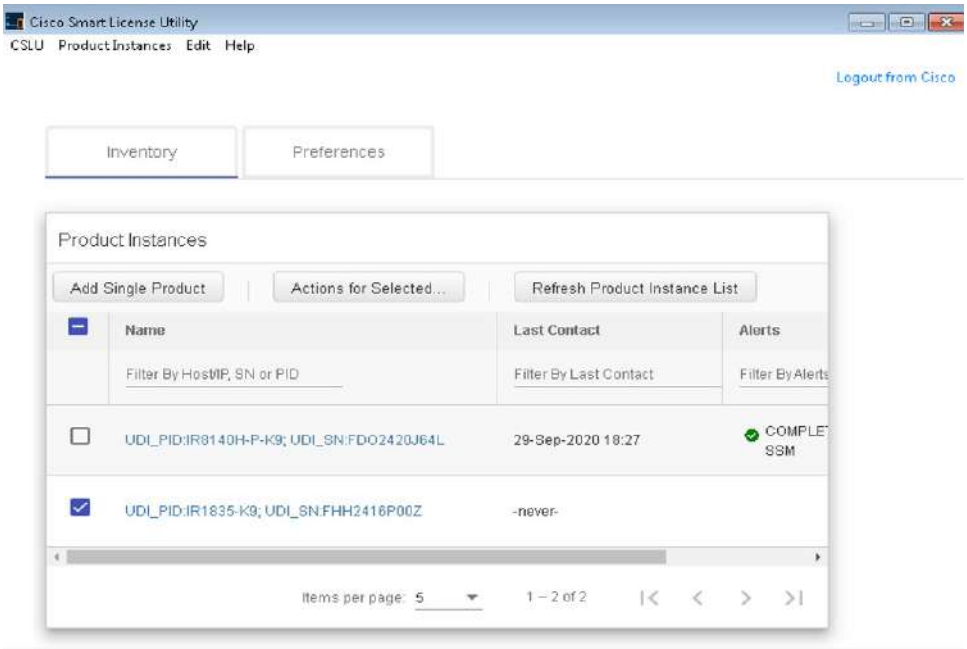
Router(config)#**Sfârşit**
Router#sh licență udi
UDI: PID:ESR-6300-CON-K9,SN:FOC23032UVB

Procedură

Pasul 1 Deschideți Cisco Smart License Utility (CSLU).

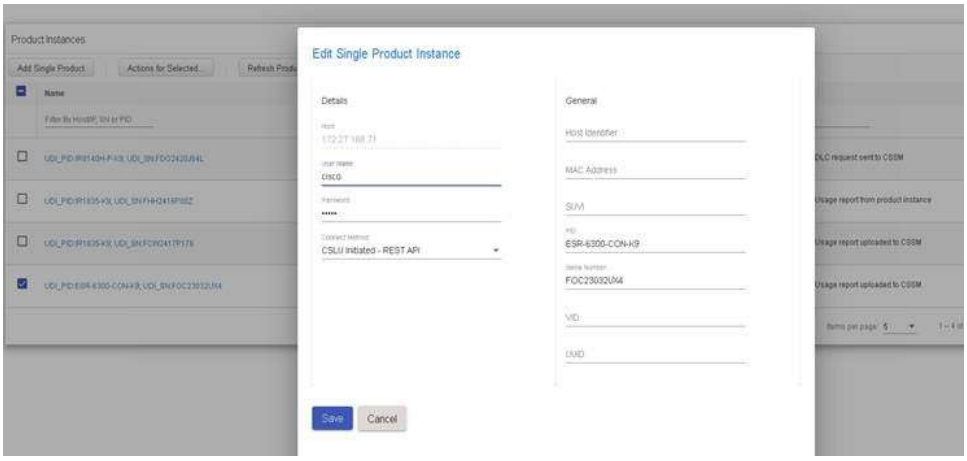
Pasul 2 Navigați la**Instanțe de produs**fila, apoi faceți clic pe UDI.

Figura 31: Selectați UDI - Exemplu IR1835



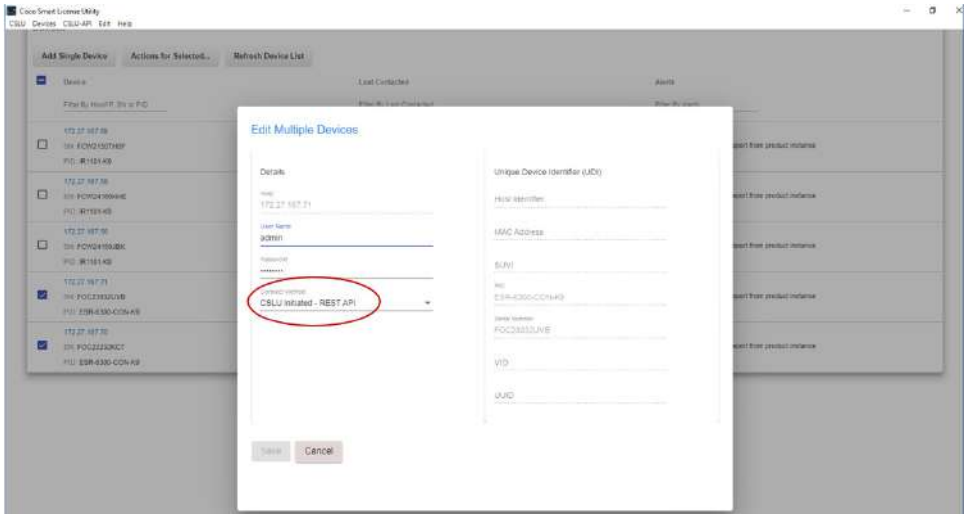
Pasul 3 The**Editați o singură instanță de produs**apare fereastra.

Figura 32: Editați o singură instanță de produs



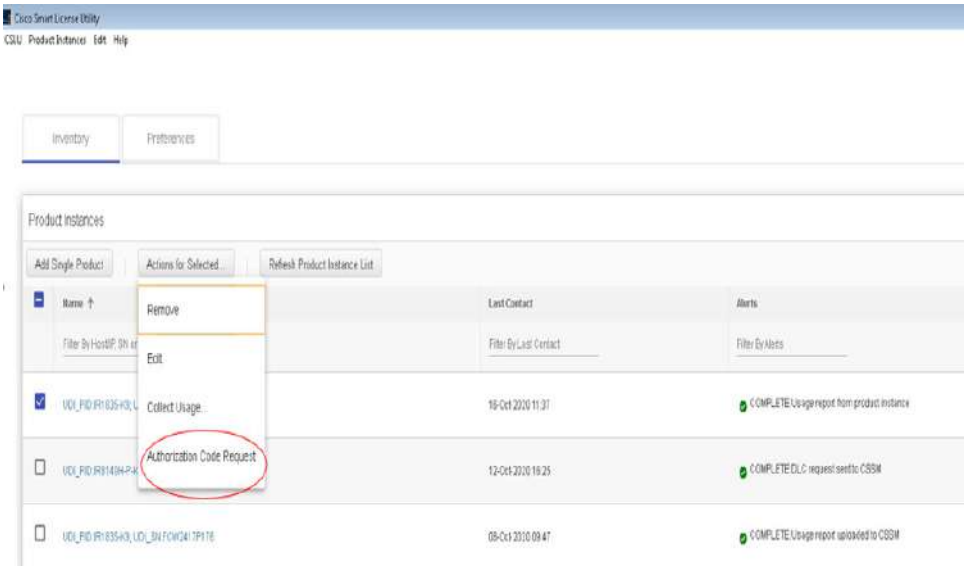
Pasul 4 The**Editați mai multe dispozitive**apare fereastra. Introduceți parola contului și faceți clic**Salva**.

Figura 33: Editați mai multe dispozitive



Pasul 5 În**Instanțe de produs**fereastra, faceți clic pe**Acțiuni pentru dispozitivele selectate**Tab.

Figura 34: Acțiuni pentru dispozitivele selectate



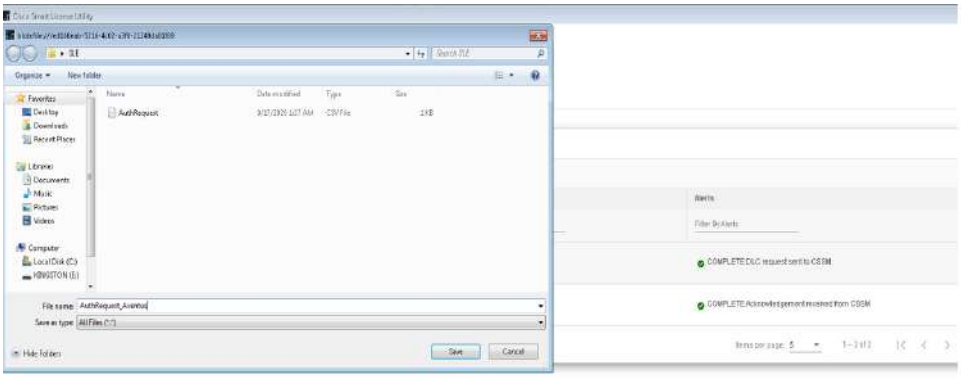
Pasul 6 Selecta**Solicitare cod de autorizare**.

Pasul 7 The**Informații privind cererea de autorizare**apare fereastra. Citiți conținutul și apoi faceți clic**Accepta**.

Figura 35: Informații privind cererea de autorizare

Pasul 8 CSLU descarcă un fișier de cerere de autorizare pe laptop. Clic**Salva**.

Figura 36: Fișier de cerere de autorizare



Exportarea fișierului AuthRequest în CSSM

Următorul pas este să luați fișierul Solicitare de autorizare pe care tocmai l-ați salvat și să-l exportați în Cisco Smart Software Manager (CSSM).

Lansați CSSM.

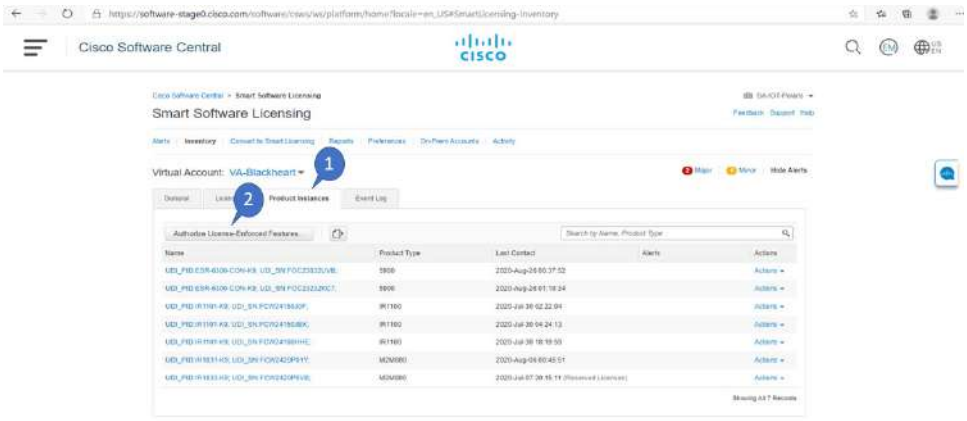
Faceți clic pe**Inventar**Tab, selectați contul dvs. virtual.

Procedură

Pasul 1 Faceți clic pe**Instanțe de produs**Tab.

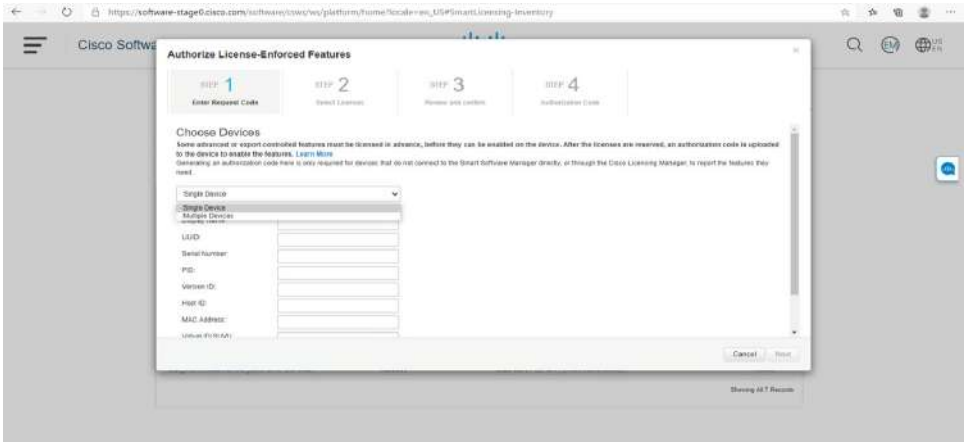
Pasul 2 Faceți clic pe**Autorizați funcțiile impuse de licență**.

Figura 37: Autorizarea funcțiilor impuse de licență



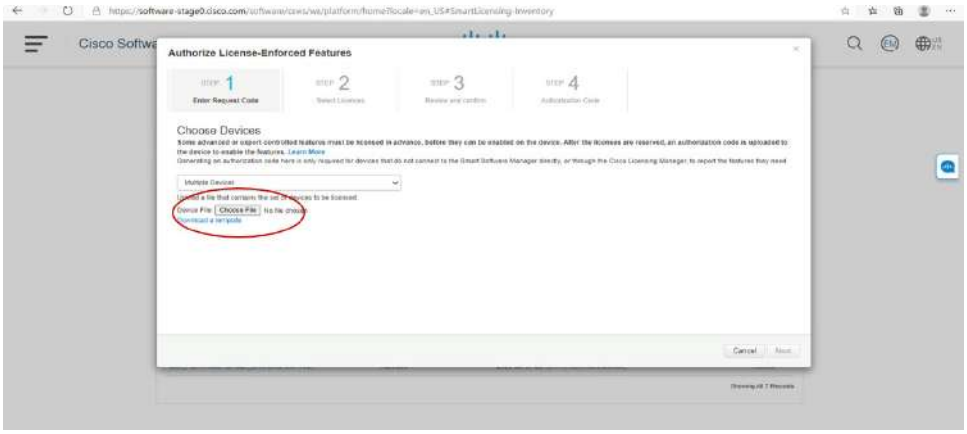
The**Autorizați funcțiile impuse de licență**apare fereastra.

Figura 38: Autorizarea funcțiilor impuse de licență



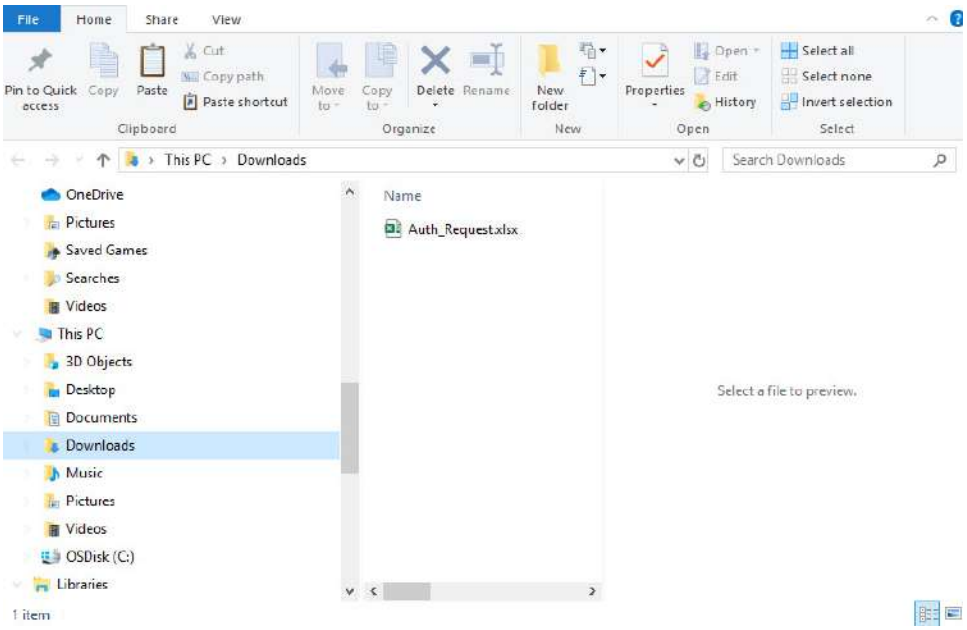
Pasul 3 Alege**Multiplu**sau**Singur**dispozitive din meniul derulant.

Pasul 4 Fereastra se schimbă într-o opțiune de selectare a fișierului dispozitivului. Faceți clic pe**Alegeți Fișier**.



Pasul 5 Se deschide o fereastră pop-up pentru a naviga la locul în care ați salvat fișierul Cerere de autorizare pe laptop.

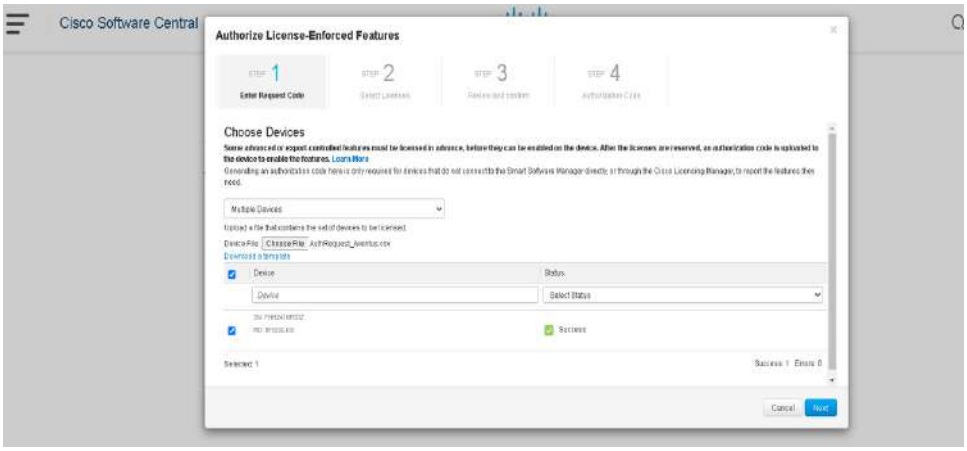
Figura 39: Deschideți fereastra de navigare a fișierelor



Pasul 6 Selectați fișierul, apoi faceți clic**Deschide**.

Pasul 7 Se încarcă fișierul de autorizare, iar fereastra se schimbă pentru a vă prezenta dispozitivele.

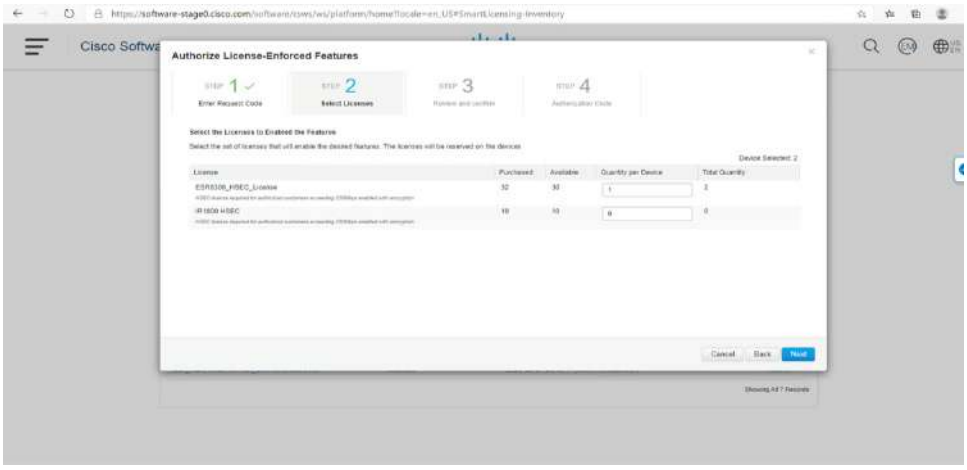
Figura 40: Dispozitive prezente



Pasul 8 Când a reușit, faceți clic**Următorul**.

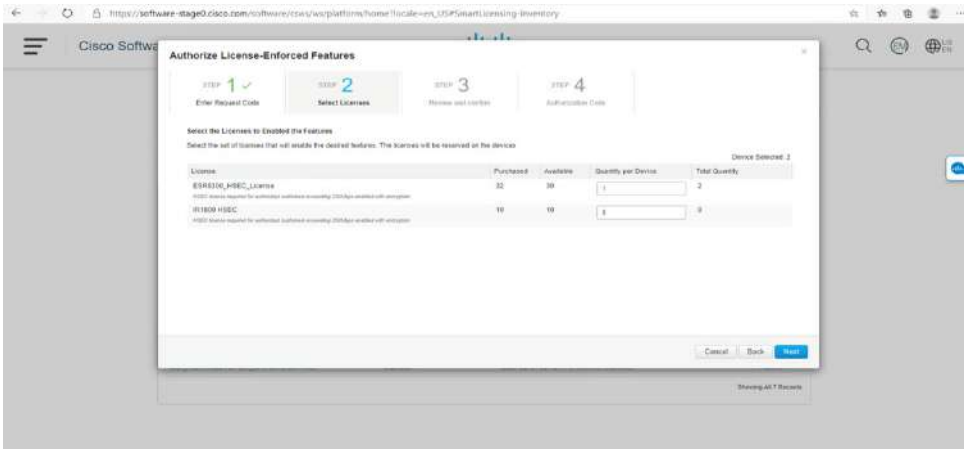
Pasul 9 The**Selectați Licențe**Se deschide fila.

Figura 41: Selectați licențe



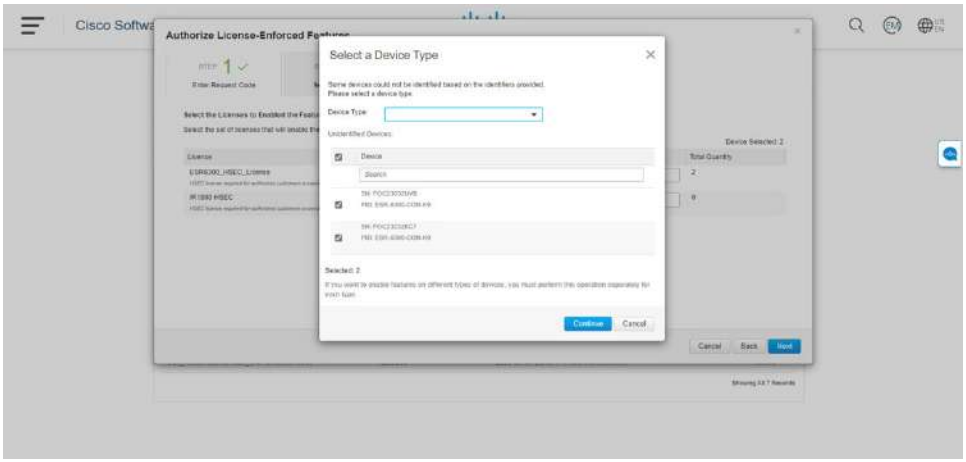
Pasul 10 Sub**Cantitate pe Dispozitiv**, introduceți numărul dorit.

Figura 42: Introduceți numărul



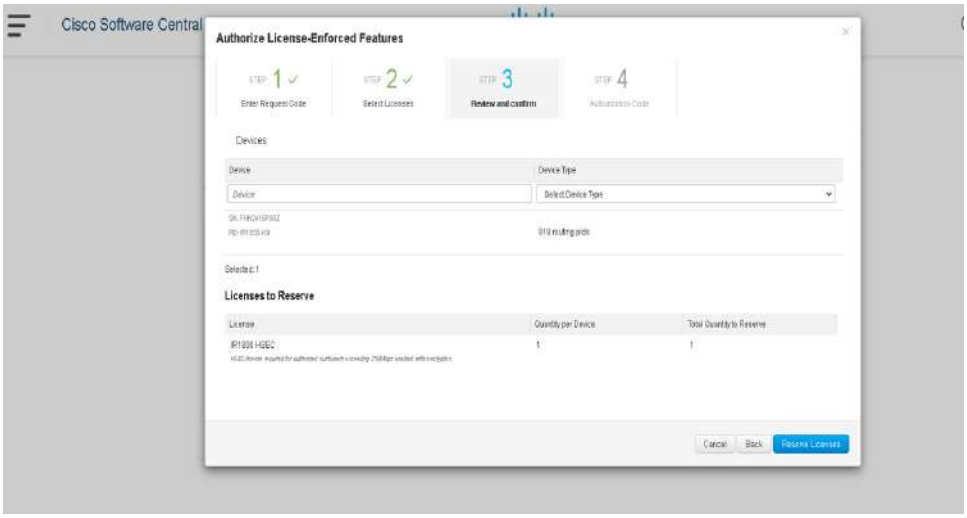
Pasul 11 Dacă CSSM nu vă poate identifica dispozitivul din informațiile de identificare, îl puteți selecta manual.

Figura 43: Selectați un tip de dispozitiv



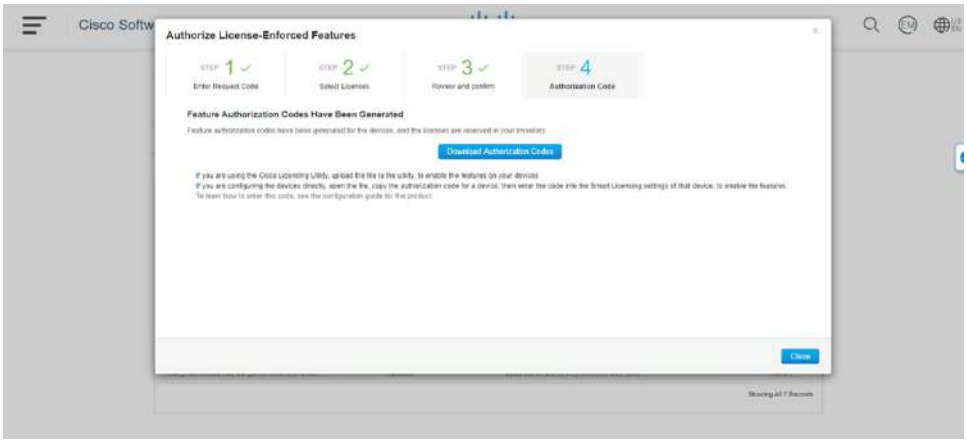
Pasul 12 Clic**Continua**, iar fereastra se schimbă în**Examinați și confirmați**.

Figura 44: Revizuire și confirmare



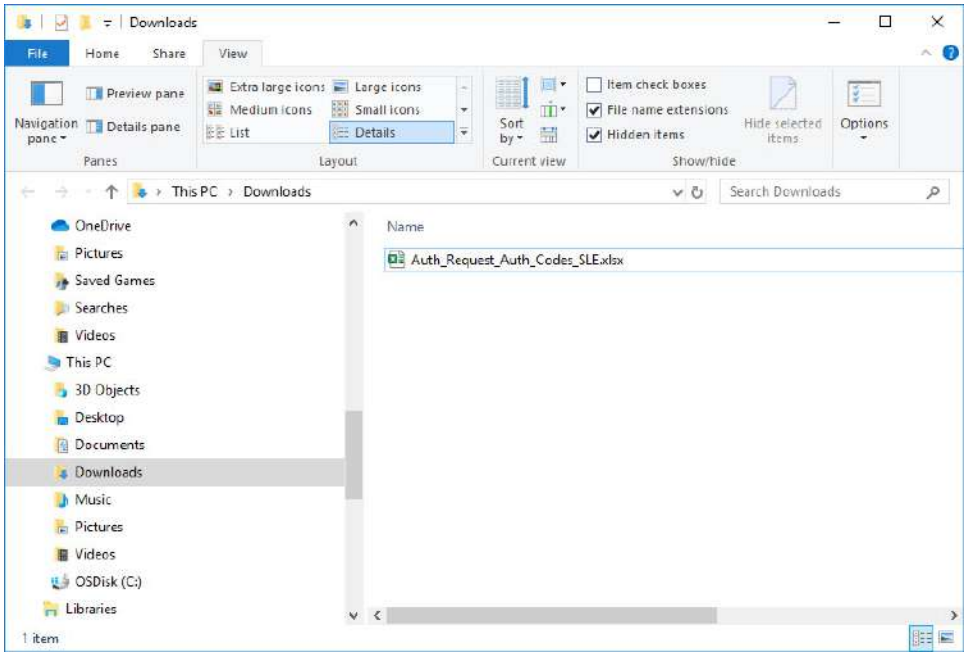
Pasul 13 Faceți clic pe**Licențe de rezervă**, iar CSSM generează coduri de autorizare a caracteristicilor.

Figura 45: Coduri de autorizare a caracteristicilor



Pasul 14 Clic**Descărcați coduri de autorizare**și se deschide o fereastră pentru a naviga unde doriți să salvați codurile.

Figura 46: Salvare cod de autorizare



Pasul 15 Clic**Bine**.

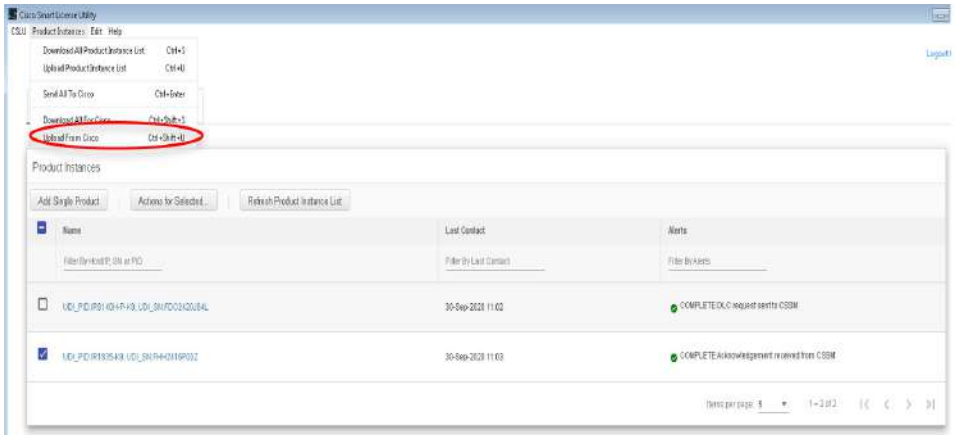
Încărcarea fișierului cod de solicitare de autorizare în CSLU

Procedură

Pasul 1 Deschideți Cisco Smart License Utility (CSLU).

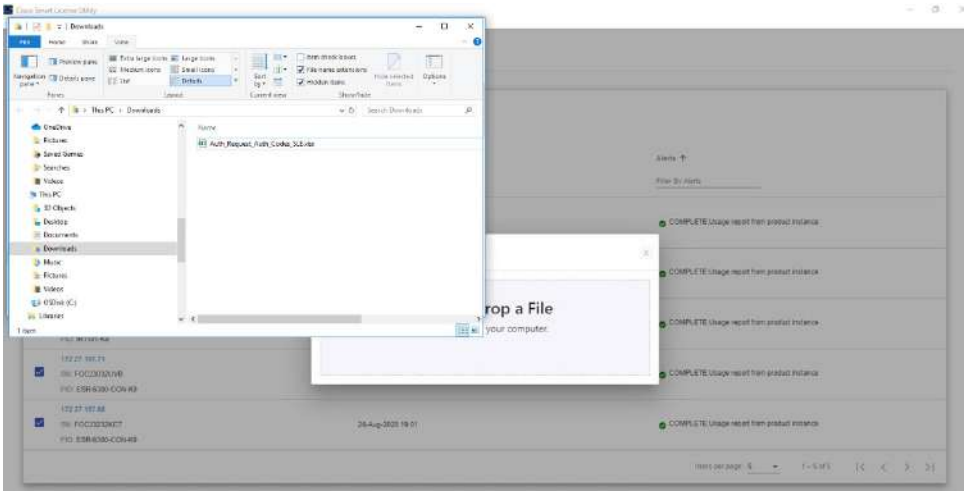
Pasul 2 Navigați la**Instanțe de produs**, apoi selectați**Încărcați de la Cisco**.

Figura 47: Încărcare de la Cisco



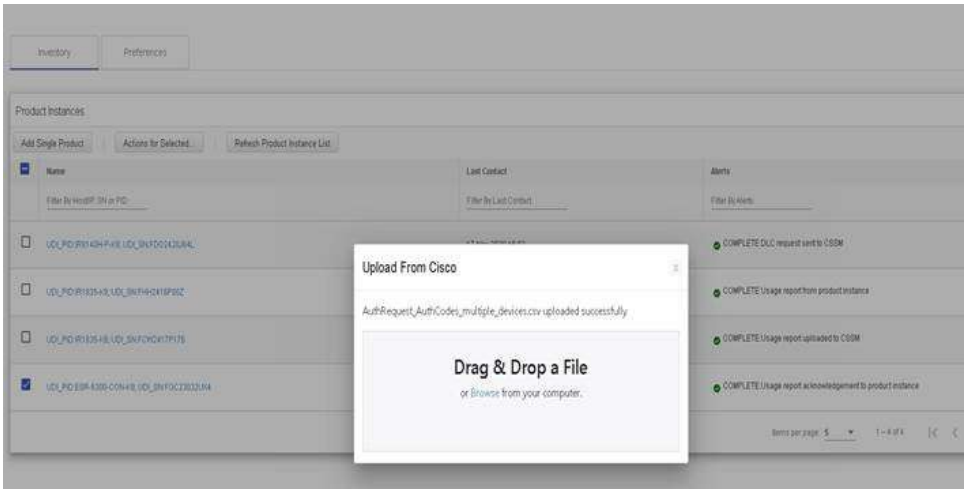
Pasul 3 Există două opțiuni pentru a vă încărca fișierul.**Trageți și plasați**, sau**Răsfoiește**unde ați salvat fișierul. Acest exemplu arată Browse.

Figura 48: Navigați la fișier



Pasul 4 Selectați fișierul cu codul de autorizare, apoi faceți clic**Deschide**. Sistemul încarcă fișierul cu codul de autorizare, apoi apare un mesaj de încărcare reușită.

Figura 49: Încărcare reușită



Procesul de instalare a licenței în router

Efectuați următoarele din interfața de linie de comandă.

IR1800 Exemplu

Efectuați următoarele din interfața de linie de comandă.

Router#**arată rezumatul licenței**
Rezervarea licenței este ACTIVATĂ
Utilizarea licenței:

Licență	Eticheta de drept	Stare numărare
network-essentials_250M (IR1800M_P_E)5		1 ÎN UTILIZARE
hseck9	(IR1800_HSEC)	1 ÎN UTILIZARE

Router#**arată utilizarea licenței**
Autorizarea licenței:
Stare: Nu se aplică
network-essentials_250M (IR1800_P_250M_E):
Descriere: network-essentials_250M Număr: 1

Versiune: 1.0
Stare: ÎN UTILIZARE
Starea exportului: NU RESTRICȚIONAT Nume caracteristică: network-essentials_250M Descrierea caracteristicii: network-essentials_250M Tip de aplicare: NU APLICAT

hseck9 (IR1800_HSEC):
Descriere: hseck9
Număr: 1
Versiune: 1.0
Stare: ÎN UTILIZARE
Stare export: RESTRICȚIONAT - PERMIS Nume caracteristică: hseck9
Descrierea caracteristicii: hseck9 Tip de aplicare: EXPORT RESTRICȚI
Router(config)#**nivel de debit hardware al platformei 2G** % Vă rugăm să scrieți mem și reîncărcați

% Configurația va avea efect la următoarea repornire
Router(config)#**Sfârşit**
Router#
* 30 septembrie 18:05:55.654: %SYS-5-CONFIG_I: Configurat din consolă de către Cisco pe consolă Router#**arată rezumatul licenței** Rezervarea licenței este ACTIVATĂ Utilizarea licenței:

Licență	Eticheta de drept	Stare numărare
network-essentials_250M (IR1800M_P_E)5		1 ÎN UTILIZARE
hseck9	(IR1800_HSEC)	1 ÎN UTILIZARE
network-essentials_2G	(IR1800_P_2G_E)	1 ÎN UTILIZARE

ESR6300 Exemplu

Efectuați următoarele din interfața de linie de comandă.

Router#**arată rezumatul licenței**
Rezervarea licenței este ACTIVATĂ
Utilizarea licenței:
Eticheta de drept al licenței Număr Stare network-advantage_250M (ESR6300_P_250M_E) 1 ÎN UTILIZARE hseck9 (ESR6300_HSEC) 1 ÎN UTILIZARE

Router#**arată utilizarea licenței**
Autorizarea licenței:
Stare: Nu se aplică
network-advantage_250M (ESR6300_P_250M_A):
Descriere: network-advantage_250M Număr: 1

Versiune: 1.0

Stare: ÎN UTILIZARE
Starea exportului: NU RESTRICȚIONAT Nume
caracteristică: network-advantage_250M Descrierea
caracteristicii: network-advantage_250M Tip de aplicare:
NU APLICAT
hseck9 (ESR6300_HSEC_License):
Descriere: hseck9
Număr: 1
Versiune: 1.0
Stare: ÎN UTILIZARE
Stare export: RESTRICȚIONAT - PERMIS Nume
caracteristică: hseck9
Descrierea caracteristicii: hseck9 Tip de aplicare:
EXPORT RESTRICȚIONAT

Router(config)#**nivel de debit hardware al platformei 2G** % Vă rugăm
să scrieți mem și reîncărcați
% Configurația va avea efect la următoarea repornire
Router(config)#**Sfârşit**
Router#
* 30 septembrie 18:05:55.654: %SYS-5-CONFIG_I: Configurat din consolă de către Cisco pe consolă Router#**arată rezumatul licenței**
Rezervarea licenței este ACTIVATĂ Utilizarea licenței:

Licență	Eticheta de drept	Conta	Stare
network-advantage_250M	(ESR6300_P_250M_A)	1	ÎN UTILIZARE
hseck9	(ESR6300_HSEC_License)	1	ÎN UTILIZARE
network-advantage_2G	(ESR6300_P_2G_A)	1	ÎN UTILIZARE

Instalare HSEC

Acest exemplu folosește routerul din seria IR8300.

Efectuați următoarele din interfața de linie de comandă.

Router#**licență cerere de autorizare inteligentă adăugați hseck9 local**
Router#
23 septembrie 05:29:37.894: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: Un nou cod de autorizare de licență a fost instalat cu succes pe PID:IR8340-K9,SN:FDO2523J6N1
Router#**configura terminalul**
Introduceți comenzile de configurare, una pe linie. Încheiați cu CNTL/Z.
Router(config)#**caracteristica licenței hseck9** Router(config)#**Sfârşit**

Router#**arată running-config | am licență**
caracteristica licenței hseck9
licență udi pid IR8340-K9 sn FDO2523J6N1 licență nivel
de încărcare avantaj de rețea
licență smart url https://smartreceiver-stage.cisco.com/licservice/license licență smart url smart https://smartreceiver-stage.cisco.com/licservice/license licență smart transport smart

Router#
Router#**arată rezumatul licenței**
Informații despre cont:
Cont inteligent: SA-IOT-Polaris Începând cu 23 septembrie 05:29:41 2021 UTC Cont
virtual: Router

Utilizarea licenței:

Licență	Etichetă de drept	Stare numărare
Network-advantage_T1	(IR8300_NA_T1_PERF)	1 ÎN UTILIZARE
hseck9	(IR8300_HSEC)	1 ÎN UTILIZARE

Router#

```
Router#arată utilizarea licenței
Autorizarea licenței:
    Stare: Nu se aplică
.
.
.
hseck9 (IR8300_HSEC):
    Descriere: hseck9
    Număr: 1
    Versiune: 1.0
    Stare: ÎN UTILIZARE
    Stare export: RESTRICȚIONAT - PERMIS Nume
    caracteristică: hseck9
    Descrierea caracteristicii: hseck9 Tip de aplicare:
    EXPORT RESTRICȚIONAT Tip de licență: Export
```

Schimbați la Smart Licensing Packaging

Această versiune aduce produsele de rutare IoT aliniate cu alte routere de servicii integrate (ISR).

Prezentare generală a licențelor inteligente

Cisco Smart Licensing este un model de licențiere flexibil care oferă utilizatorilor o modalitate mai simplă, mai rapidă și mai consistentă de a achiziționa și gestiona software în portofoliul Cisco și în organizația lor. Și este sigur. Cu ajutorul licențelor inteligente, utilizatorii obțin:

- Activare ușoară: Smart Licensing stabilește un grup de licențe software care pot fi utilizate în întreaga organizație – nu mai există chei de activare a produsului (PAK).
- Management unificat: Drepturile mele Cisco (MCE) oferă o vizualizare completă a tuturor produselor și serviciilor dumneavoastră Cisco într-un portal ușor de utilizat, astfel încât să știți întotdeauna ce aveți și ce utilizați.
- Flexibilitatea licenței: software-ul dvs. nu este blocat în nod pe hardware-ul dvs., astfel încât puteți utiliza și transfera cu ușurință licențele după cum este necesar.

Politica de utilizare a licențelor inteligente (SLP), anterior denumită Smart Licensing Enhanced (SLE) și este modul implicit, începând cu versiunea 17.3.2 Cisco IOS-XE. SLE a înlocuit Smart Software Licensing. Această modificare a caracteristicilor pentru Cisco IOS XE versiunea 17.11.1a se concentrează pe pachetul de licențiere.

Niveluri de licență

Următoarele sunt nivelurile de licență disponibile pentru toate dispozitivele Cisco IR.

Licențe de bază

- Elemente esențiale pentru rețea
- Network Advantage (include Network Essentials)

Nota Aceste licențe sunt comandate prin Cisco Commerce Workspace (CCW) și sunt permanente.

Licențe suplimentare—Acestea pot fi subscrise pe un termen fix de trei, cinci sau șapte ani.

- Elemente esențiale ale arhitecturii de rețele digitale (DNA).
- ADN Advantage (include DNA Essentials)

Nota Aceste licențe sunt comandate prin Cisco Commerce Workspace (CCW) și se referă la DNA-C și SDWAN. Pentru mai multe informații, consultațiCisco SD-WANșiCentrul Cisco DNApagini web.

Următoarele tabele oferă detalii despre nivelurile de licență:

Tabelul 15: Elemente esențiale de rețea (Licență perpetuă)

Capacități esențiale de comutare	Layer 2, Acces rutat (RIP, EIGRP Stub, OSPF (1000 de rute)), PBR, PIM Stub Multicast (1000 de rute) PVLAN, VRRP, PBR, CDP, QoS, FHS, 802.1x, Macsec-128, CoPP, SXP, IP SLA Responder SSO **Nota** Pentru ca dispozitivul să fie compatibil cu Licența DNA Essential, nu trebuie să depășească 1000 de rute în tabelul de rutare, indiferent de modul în care au fost învățate rutele.
Integrarea DevOps	• Netconf, Restconf, gRPC • Modele de date Yang • GuestShell (On-Box Python) • Agent PnP, ZTP

Tabelul 16: Network Advantage (Licență perpetuă) Conține toate elementele de bază ale rețelei plus următoarele:

IoT și mobilitate	CoAP
Funcționalitate completă de rutare	BGP, HSRP, OSPF, ISIS, GLBP
Segmentarea flexibilă a rețelei	VRF, VXLAN, LISP, SGT, MPLS
Disponibilitate ridicată și rezistență	NSF, GIR, Stackwise Virtual*, ISSU/eFSU, corecție (CLI)
Optimizați utilizarea lățimii de bandă cu Multicast	MSDP, mVPN, AutoRP, PIM-BIDIR

Tabelul 17: ADN-ul esențial (termeni de 3, 5, 7 ani)

Automatizare de bază	• Aplicație PnP • Automatizare LAN • Manager de evenimente încorporat
Asigurare de bază	• Tablouri de bord pentru sănătate – Rețea și Client • Monitorizarea stării de sănătate a dispozitivului de bază și a clienților cu fir

Tabelul 18: Avantajul ADN (termeni de 3, 5, 7 ani) Conține toate elementele esențiale ADN plus următoarele:

Automatizare avansată	• Analize de trafic criptate • Serviciul DNA pentru Bonjour
Asigurare și analiză	• Conformitate, Rapoarte personalizate • Switch 360 & Wired Client 360

Niveluri de debit al licențelor

Pe lângă configurarea nivelului de licență, este posibil să se configureze și nivelul de debit pe dispozitiv. Nivelul de debit determină limita lățimii de bandă care se aplică traficului criptat. Nu există nicio limită aplicată traficului necriptat (clear) care trece printr-un dispozitiv.

Important Pentru a respecta reglementările globale de export, dacă este necesar mai mult de 250 Mbs de trafic criptat, atunci o selecție „nelimitată” – dependentă de platformă – trebuie făcută pe CCW, precum și o licență HSEC.

Această limită este impusă bidirecțional. Aceasta înseamnă că, dacă limita de debit este setată la 250 Mbps, atunci până la 250 Mbps de trafic criptat pot circula prin dispozitiv în orice direcție. De exemplu, dispozitivul poate primi și transmite până la 250 Mbps de trafic criptat. Nu există nicio limită aplicată pentru traficul necriptat.

Când nivelul de transfer al dispozitivului este setat la „nelimitat”, nu există limite impuse atât pentru traficul criptat, cât și pentru cel necriptat care circulă prin acesta.

Nota Pentru a evita confuzia privind limitele de debit și versiunile software IOS XE, rețineți următoarele:

Cisco IOS XE versiunea 17.11.1a și anterioară care rulează pe platformele ESR6300, IR1800 și IR8140 acceptă licențe boost, nelimitate și nelimitate. Acestea sunt configurate folosind**nivel de debit hardware al platformei 2G**CLI.

Viitoarele versiuni Cisco IOS XE 17.12.1 și ulterioare care rulează pe ESR6300, IR1800 și IR8140 acceptă aceleași licențe, dar vor fi configurate folosind**Nivelul de debit hardware al platformei nelimitat**CLI.

Cu viitoarea versiune Cisco IOS XE 17.12.1 și ulterioare,**nivel de debit hardware al platformei 2G**iar cel **Nivelul de debit hardware al platformei nelimitat**CLI-urile vor oferi ambele același debit ca și licența nelimitată.

Următorul tabel arată limitele de debit (numite și licență Tier) acceptate pe dispozitivele IoT începând cu versiunea Cisco IOS XE 17.11.1a.

Platformă	**25 Mbps bidirectional** **(Nivelul 0)**	**50 Mbps bidirectional**	**Până la 200 Mbps bidirectional** **(Nivelul 1)**	**250 Mbps bidirectional**	**2 Gbps**	**Nelimitat (Nivelul 2)**
ESR 6300	N / A	Da	N / A	Da	Da	Pentru a fi susținut incepand cu 17.12.1

Platformă	25 Mbps bidirectional (Nivelul 0)	50 Mbps bidirectional	Până la 200 Mbps bidirectional (Nivelul 1)	250 Mbps bidirectional	2 Gbps	Nelimitat (Nivelul 2)
ESR-6300-LIC-K9	N / A	Da	N / A	N / A	N / A	Da
IR1101	N / A	N / A	N / A	Da	N / A	Sprijinit incepand cu 17.10.1.
IR1800	N / A	Da	N / A	Da	Da	Pentru a fi susținut incepand cu 17.12.1
IR8100	N / A	Da	Da	Da	Da	Pentru a fi susținut incepand cu 17.12.1
IR8300	Da	N / A	Da	N / A	N / A	Da

Interfață de linie de comandă

Sunt disponibile următoarele comenzi:

nivelul de pornire al licenței *<network-essentials/network-advantage>*

Nivelul de debit poate fi configurat folosind următorul CLI pe toate dispozitivele IR, cu excepția

IR8300: **nivelul de debit hardware al platformei** *<limită>*

Pe IR8300, nivelul de debit poate fi configurat folosind următorul CLI:

Debitul hardware al platformei cripto *<limită>*

Pentru a vedea debitul configurat pe dispozitiv, utilizați următorul

CLI: **arata versiunea | include debitul**
Nivelul curent de transfer criptografic este: 50000 kbps

Implementarea licenței nelimitate

Versiunea Cisco IOS XE 17.11.1 a introdus un nou nivel de debit numit „uncapped”. Această versiune extinde noul nivel de debit la toate platformele de rutare Cisco IoT. Următoarea este o recapitulare a implementării licenței nelimitate:

Niveluri de debit al licențelor

Nivelul de debit determină limita lățimii de bandă care se aplică traficului criptat. Nu există nicio limită aplicată traficului necriptat (clear) care trece printr-un dispozitiv.

Important Pentru a respecta reglementările globale de export, dacă este necesar mai mult de 250 Mbs de trafic criptat, atunci o selecție „nelimitată” – dependentă de platformă – trebuie făcută pe CCW, precum și o licență HSEC.

Această limită este impusă bidirecțional. Aceasta înseamnă că, dacă limita de debit este setată la 250 Mbps, atunci până la 250 Mbps de trafic criptat pot circula prin dispozitiv în orice direcție. De exemplu, dispozitivul poate primi și transmite până la 250 Mbps de trafic criptat. Nu există nicio limită aplicată pentru traficul necriptat.

Când nivelul de transfer al dispozitivului este setat la „nelimitat”, nu există limite impuse atât pentru traficul criptat, cât și pentru cel necriptat care circulă prin acesta.

Nota Pentru a evita confuzia privind limitele de debit și versiunile software IOS XE, rețineți următoarele:

Cisco IOS XE versiunea 17.11.1a și anterioară care rulează pe platformele ESR6300, IR1800 și IR8140 acceptă licențe boost, nelimitate și nelimitate. Acestea sunt configurate folosind**nivel de debit hardware al platformei 2G**CLI.

Viitoarea versiune Cisco IOS XE 17.12.1a și ulterioară care rulează pe ESR6300, IR1800 și IR8140 acceptă aceleași licențe, dar vor fi configurate folosind**Nivelul de debit hardware al platformei nelimitat**CLI.

Cu Cisco IOS XE versiunea 17.12.1a și ulterioară, versiunea**nivel de debit hardware al platformei 2G**iar cel**Nivelul de debit hardware al platformei nelimitat**CLI-urile vor oferi ambele același debit ca și licența nelimitată.

Următorul tabel arată limitele de debit (numite și licență Tier) acceptate pe dispozitivele IoT.

Platformă	**25 Mbps bidirectional** **(Nivelul 0)**	**50 Mbps bidirectional**	**Până la 200 Mbps bidirectional** **(Nivelul 1)**	**250 Mbps bidirectional**	**2 Gbps**	**Nelimitat (Nivelul 2)**
ESR 6300	N / A	Da	N / A	Da	Da	Sprijinit incepand cu 17.12.1a
ESR-6300-LIC-K9	N / A	Da	N / A	N / A	N / A	Da
IR1101	N / A	N / A	N / A	Da	N / A	Sprijinit incepand cu 17.10.1.
IR1800	N / A	Da	N / A	Da	Da	Sprijinit incepand cu 17.12.1a
IR8100	N / A	Da	Da	Da	Da	Sprijinit incepand cu 17.12.1a
IR8300	Da	N / A	Da	N / A	N / A	Nu

CAPITOL 13

Configurarea porturilor de comutare Ethernet

Acest capitol conține următoarele secțiuni:

Configurarea VLAN-urilor

Un VLAN este o rețea comutată care este segmentată logic după funcție, echipă de proiect sau aplicație, fără a ține cont de locațiile fizice ale utilizatorilor. VLAN-urile au aceleași atribute ca și LAN-urile fizice, dar puteți grupa stațiile finale chiar dacă nu sunt situate fizic pe același segment LAN. Orice port de comutare poate aparține unui VLAN, iar pachetele unicast, broadcast și multicast sunt redirecționate și inundate numai către stațiile terminale din VLAN. Fiecare VLAN este considerată o rețea logică, iar pachetele destinate stațiilor care nu aparțin VLAN-ului trebuie redirecționate printr-un router.

Nota Nu există suport pentru cadre Jumbo pe interfețele L2.

Următorul este un exemplu de configurație vlan:

```
IR1800#arată vlan
Nume VLAN                                        Stare    Porturi
---- -------------------------------------------------------------------- 1 implicit
                                                 activ    Ge0/1/0, Ge0/1/1, Ge0/1/2, Ge0/1/3
1002 fddi-implicit                               acționează/desupra
1003 token-ring-default 1004                     acționează/desupra
fddinet-default                                  acționează/desupra
1005 trnet-implicit                              acționează/desupra

Tip VLAN SAID       MTU   Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ------------------------------------------------------------------ 1 enet
      100001     1500  -      -      -        -    -        0      0
1002 fddi       101002     1500  -      -      -        -    -        0      0
```

```
1003 tr    101003     1500  -      -      -        -    -         0     0
1004 fdnet 101004     1500  -      -      -        ieee -         0     0
1005 trnet 101005     1500  -      -      -        ibm  -         0     0

Tip secundar primar                              Porturi
---------------------------------------------------------------------------------------

IR1800#
```

Puteți aloca un anumit port unui vlan urmând acești pași:

interfață GigabitEthernet0/1/0
switchport access vlan 4

interfață vlan 4
adresa ip v4 ... adresa ipv6
autoconf

VLAN Trunking Protocol (VTP)

VTP este un protocol de mesagerie de nivel 2 care menține consecvența configurației VLAN prin gestionarea adăugării, ștergerii și redenumirea VLAN-urilor la nivelul întregii rețele. VTP minimizează configurațiile greșite și inconsecvențele de configurare care pot cauza mai multe probleme, cum ar fi nume VLAN duplicate, specificații incorecte de tip VLAN și încălcări de securitate.

Înainte de a crea VLAN-uri, trebuie să decideți dacă utilizați VTP în rețea. Folosind VTP, puteți face modificări de configurare la nivel central pe unul sau mai multe switch-uri și puteți comunica automat acele modificări tuturor celorlalte switch-uri din rețea. Fără VTP, nu puteți trimite informații despre VLAN-uri către alte switch-uri. VTP este proiectat să funcționeze într-un mediu în care actualizările sunt făcute pe un singur switch și sunt trimise prin VTP către alte switch-uri din domeniu. Nu funcționează bine într-o situație în care mai multe actualizări ale bazei de date VLAN apar simultan pe comutatoarele din același domeniu, ceea ce ar duce la o inconsecvență în baza de date VLAN.

Mai multe informații despre configurarea VTP pot fi găsite aici:http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html#wp1046901

Configurarea autentificării 802.1x

Autentificarea bazată pe porturi IEEE 802.1x definește un protocol de autentificare și control al accesului bazat pe client-server pentru a preveni conectarea clienților neautorizați la o rețea LAN prin porturi accesibile public. Serverul de autentificare autentifică fiecare client conectat la un port de comutare înainte de a permite accesul la orice comutator sau servicii LAN. Până când clientul este autentificat, controlul accesului IEEE 802.1x permite doar traficul Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP) și Spanning Tree Protocol (STP) prin portul la care este conectat clientul. După autentificare, traficul normal trece prin port.

Cu autentificarea IEEE 802.1x, dispozitivele din rețea au roluri specifice:

- Supplicant—Dispozitiv (stație de lucru) care solicită acces la LAN și comută servicii și răspunde la solicitările de la router. Stația de lucru trebuie să ruleze un software client compatibil cu IEEE 802.1x, cum ar fi cel oferit în sistemul de operare Microsoft Windows XP. (Solicitantul este uneori numit client.)

- Server de autentificare—Dispozitiv care realizează autentificarea efectivă a solicitantului. Serverul de autentificare validează identitatea solicitantului și notifică ruterul dacă solicitantul este sau nu

autorizat să acceseze LAN și să comute serviciile. Dispozitivul de acces la rețea transmite în mod transparent mesajele de autentificare între solicitant și serverul de autentificare, iar procesul de autentificare este efectuat între solicitant și serverul de autentificare. Metoda EAP particulară utilizată va fi decisă între solicitant și serverul de autentificare (server RADIUS). Sistemul de securitate RADIUS cu extensii EAP este disponibil în Cisco Secure Access Control Server versiunea 3.0 sau mai recentă. RADIUS funcționează într-un model client și server în care informațiile de autentificare securizate sunt schimbate între serverul RADIUS și unul sau mai mulți clienți RADIUS.

- Authenticator—Router care controlează accesul fizic la rețea pe baza stării de autentificare a solicitantului. Routerul acționează ca un intermediar între solicitant și serverul de autentificare, solicitând informații de identitate de la solicitant, verificând acele informații cu serverul de autentificare și transmiterea unui răspuns către solicitant. Routerul include clientul RADIUS, care este responsabil de încapsularea și decapsularea cadrelor EAP și de interacțiunea cu serverul de autentificare.

Pentru informații detaliate despre cum să configurați autentificarea bazată pe port 802.1x, consultați următorul link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/15-mt/ sec-user-8021x-15-mt-book/config-ieee-802x-pba.html

Exemplu: Activarea IEEE 802.1x și AAA pe un port de comutare

Acest exemplu arată cum să configurați un router IR1800 ca autentificator 802.1x:

Router>**permite**
Router#**configura terminalul** Router(config)#**dot1x**
sistem-auth-control Router(config)#**aaa nou-model**

Router(config)#**aaa autentificare dot1x raza implicită a grupului** Router(config)#
interfață GigabitEthernet 0/1/0 Router(config-if)#**acces în modul switchport**
Router(config-if)#**acces-sesiune port-control automat** Router(config-if)#
autentificator dot1x pae Router(config-if)#**acces-sesiune închisă** Router(config-if)#**acces-sesiune gazdă-mod o singură gazdă** Router(config-if)#**Sfârşit**

Configurarea protocolului Spanning Tree

Spanning Tree Protocol (STP) este un protocol de gestionare a legăturilor de nivel 2 care oferă redundanță a căii, prevenind în același timp buclele în rețea. Pentru ca o rețea Ethernet de nivel 2 să funcționeze corect, poate exista o singură cale activă între oricare două stații. Mai multe căi active între stațiile finale provoacă bucle în rețea. Dacă există o buclă în rețea, stațiile finale pot primi mesaje duplicate. Switch-urile ar putea, de asemenea, să învețe adrese MAC ale stației finale pe mai multe interfețe Layer 2. Aceste condiții duc la o rețea instabilă. Operarea spanning-tree este transparentă pentru stațiile finale, care nu pot detecta dacă sunt conectate la un singur segment LAN sau la o LAN comutată de mai multe segmente.

STP utilizează un algoritm spanning-tree pentru a selecta un comutator al unei rețele conectate redundant ca rădăcină a arborelui spanning. Algoritmul calculează cea mai bună cale fără buclă printr-o rețea de strat 2 comutată prin atribuirea unui rol fiecărui port pe baza rolului portului în topologia activă:

- Root—Un port de redirecționare ales pentru topologia spanning-tree
- Designated—Un port de redirecționare ales pentru fiecare segment LAN comutat

- Alternate—Un port blocat care oferă o cale alternativă către puntea rădăcină din arborele de întindere
- Backup—Un port blocat într-o configurație loopback

Comutatorul care are toate porturile ca rol desemnat sau ca rol de rezervă este comutatorul rădăcină. Comutatorul care are cel puțin unul dintre porturile sale în rolul desemnat se numește comutator desemnat. Spanning Tree forțează căile de date redundante într-o stare de așteptare (blocata). Dacă un segment de rețea din spanning tree eșuează și există o cale redundantă, algoritmul spanning-tree recalculează topologia spanning-tree și activează calea de așteptare. Switch-urile trimit și primesc cadre de tip spanning-tree, numite bridge protocol data units (BPDU), la intervale regulate. Comutatoarele nu transmit aceste cadre, ci le folosesc pentru a construi o cale fără buclă. BPDU-urile conțin informații despre comutatorul care trimite și porturile acestuia, inclusiv adresele comutatorului și MAC, prioritatea comutatorului, prioritatea portului și costul căii. Spanning Tree utilizează aceste informații pentru a alege comutatorul rădăcină și portul rădăcină pentru rețeaua comutată și portul rădăcină și portul desemnat pentru fiecare segment comutat.

Când două porturi de pe un comutator fac parte dintr-o buclă, prioritatea porturilor din arborele de acoperire și setările de cost ale căii controlează care port este pus în starea de redirecționare și care este pus în starea de blocare. Valoarea priorității portului spanning-tree reprezintă locația unui port în topologia rețelei și cât de bine este amplasat pentru a trece traficul. Valoarea costului căii reprezintă viteza media.

Pentru informații detaliate despre configurarea STP, consultați următorul link:

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/NIM/software/configuration/guide/4_8PortGENIM.html#pgfId-1079138

Important Dacă routerul este setat din fabrică, scrierea ștearsă sau resetarea configurației, baza de date vlan este ștearsă. Chiar dacă configurația are efect, interfețele trebuie eliminate și aplicate din nou.

Exemplu: Configurarea protocolului Spanning Tree

Următorul exemplu arată configurarea priorității portului spanning-tree a unei interfețe Gigabit Ethernet. Dacă apare o buclă, spanning tree folosește prioritatea portului atunci când selectează o interfață pe care să o pună în starea de redirecționare.

Router#**configura terminalul** Router(config)#**interfață GigabitEthernet 0/1/0** Router(config-if)#**spanning-tree vlan 1 port-priority 64**
Router(config-if)#**Sfârşit**

Următorul exemplu arată cum să modificați costul portului spanning-tree al unei interfețe Gigabit Ethernet. Dacă apare o buclă, spanning tree folosește costul atunci când selectează o interfață pe care să o pună în starea de redirecționare.

Router#**configura terminalul**
Router(config)#**interfață GigabitEthernet 0/1/0** Router(config-if)#**spanning-tree costă 18** Router(config-if)#**Sfârşit**

Următorul exemplu arată configurarea priorității bridge-ului VLAN 10 la 33792:

Router#**configura terminalul**
Router(config)#**spanning-tree vlan 10 prioritate 33792**
Router(config)#**Sfârşit**

Următorul exemplu arată configurarea timpului de salut pentru VLAN 10 configurat la 7 secunde. Ora salută este intervalul dintre generarea mesajelor de configurare de către comutatorul rădăcină.

Router#**configura terminalul**
Router(config)#**spanning-tree vlan 10 hello-time 7** Router(config)#
Sfârşit

Următorul exemplu arată configurarea timpului de întârziere înainte. Întârzierea de transmitere este numărul de secunde pe care o interfață așteaptă înainte de a trece de la stările de învățare și ascultare din arborele de acoperire la starea de redirecționare.

Router#**configura terminalul**
Router(config)#**spanning-tree vlan 10 forward-time 21** Router(config)#
Sfârşit

Următorul exemplu arată configurarea intervalului maxim de vârstă pentru arborele de întindere. Timpul maxim de îmbătrânire este numărul de secunde pe care le așteaptă un comutator fără a primi mesaje de configurare spanning-tree înainte de a încerca o reconfigurare.

Router#**configura terminalul**
Router(config)#**spanning-tree vlan 20 max-varsta 36**
Router(config)#**Sfârşit**

Următorul exemplu arată că comutatorul este configurat ca punte rădăcină pentru VLAN 10, cu un diametru de rețea de 4.

Router#**configura terminalul**
Router(config)#**spanning-tree vlan 10 diametrul primar al rădăcinii 4**
Router(config)#**Ieșire**

Configurarea manipulării tabelului de adrese MAC

Tabelul de adrese MAC conține informații despre adrese pe care comutatorul le folosește pentru a redirecționa traficul între porturi. Toate adresele MAC din tabelul de adrese sunt asociate cu unul sau mai multe porturi. Tabelul de adrese include aceste tipuri de adrese:

- Adresă dinamică: o adresă MAC sursă pe care comutatorul o învață și apoi o renunță atunci când nu este utilizată. Puteți utiliza setarea timpului de îmbătrânire pentru a defini cât timp comutatorul păstrează adresele nevăzute în tabel.
- Adresă statică: o adresă unicast introdusă manual, care nu îmbătrânește și care nu se pierde la resetarea comutatorului.

Tabelul de adrese listează adresa MAC de destinație, ID-ul VLAN asociat și portul asociat cu adresa și tipul (static sau dinamic).

Securitatea porturilor este acceptată, la fel ca și adresele MAC lipicioase.

Consultați „Exemplu: Manipularea tabelului de adrese MAC” pentru exemple de configurații pentru activarea adresei MAC securizate, crearea unei intrări statistice, setarea numărului maxim de adrese MAC securizate și setarea timpului de vechime.

Pentru informații detaliate de configurare despre manipularea tabelului de adrese MAC, consultați următorul link:

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html#wp1048223

Exemplu: Manipularea tabelului de adrese MAC

Următorul exemplu arată crearea unei intrări statice în tabelul de adrese MAC.

Router#**configura terminalul**
Router(config)#**mac address-table static 0002.0003.0004 interfață GigabitEthernet 0/1/0**

vlan 3
Router(config)#**Sfârşit**

Următorul exemplu arată setarea temporizatorului de îmbătrânire.

Router#**configura terminalul**
Router(config)#**mac address-table aging-time 300**
Router(config)#**Sfârşit**

Configurarea Switch Port Analyzer

Cisco IR1800 acceptă numai SPAN local și până la o sesiune SPAN. Puteți analiza traficul de rețea care trece prin porturi utilizând SPAN pentru a trimite o copie a traficului către un alt port de pe switch sau pe un alt switch care a fost conectat la un analizor de rețea sau la alt dispozitiv de monitorizare sau securitate. SPAN copiează (sau oglindește) traficul primit sau trimis (sau ambele) pe porturile sursă către un port de destinație pentru analiză. SPAN nu afectează comutarea traficului de rețea pe porturile sursă. Trebuie să dedicați portul de destinație pentru utilizarea SPAN. Cu excepția traficului care este necesar pentru sesiunea SPAN sau RSPAN, porturile de destinație nu primesc sau redirecționează trafic.

Numai traficul care intră sau iese din porturile sursă sau traficul care intră sau iese din sursă poate fi monitorizat utilizând SPAN; traficul direcționat către o sursă nu poate fi monitorizat. De exemplu, dacă traficul de intrare este monitorizat, traficul care este direcționat din altă sursă nu poate fi monitorizat; cu toate acestea, traficul care este primit pe sursă și direcționat către alta poate fi monitorizat.

Pentru informații detaliate despre cum să configurați o sesiune de analizor de port comutat (SPAN), consultați următorul link web:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/15-0_2_se/configuration/guide/scg3750/swspan.html

Exemplu: Configurare SPAN

Următorul exemplu arată cum să configurați o sesiune SPAN pentru a monitoriza traficul bidirecțional de la o interfață sursă Gigabit Ethernet:

Router#**configura terminalul**
Router(config)#**monitorizați sesiunea 1 sursă GigabitEthernet 0/1/0**
Router(config)#**Sfârşit**

Următorul exemplu arată cum să configurați o interfață Gigabit Ethernet ca destinație pentru o sesiune SPAN:

Router#**configura terminalul**
Router(config)#**monitorizați sesiunea 1 destinație GigabitEthernet 0/1/0** Router(config)#
Sfârşit

Următorul exemplu arată cum să eliminați gigabit Ethernet ca sursă SPAN pentru sesiunea 1 SPAN:

Router#**configura terminalul**
Router(config)#**nicio sesiune de monitorizare 1 sursă GigabitEthernet 0/1/0**
Router(config)#**Sfârşit**

Afișați exemplu de monitor

Router(config)#**monitorizați interfața sursă sesiunea 1 gi0/1/0** Router(config)#
monitorizați sesiunea 1 interfața de destinație gi0/1/1 Router#**sh monitor**
sesiunea 1

```
Sesiunea 1
- - - - - - - - -
Tip: Porturi sursă sesiune
locală:
Ambele: Gi0/1/0
Porturi de destinație: Gi0/1/1
```

Exemplu de ERSPAN

```
Router#arată sesiunea de monitorizare
1 Sesiunea 1
- - - - - - - - -
Tip                             : Sesiune sursă ERSPAN :
Stare                           Administrator dezactivat
Porturi sursă                   :
    Numai RX                    : Gi0/0/0
Adresa IP de destinație         : 172.5.5.200
MTU                             : 1464
ID ERSPAN destinație            : 100
Adresa IP de origine            : 172.5.6.2
DSCP IPv6                       : 0
IPV6 TTL                        : 0
```

Configurarea IGMP Snooping

Snooping IGMP constrânge inundarea traficului multicast prin configurarea dinamică a interfețelor Layer 2, astfel încât traficul multicast este redirecționat numai către acele interfețe asociate cu dispozitivele IP multicast. După cum sugerează și numele, IGMP Snooping necesită ca comutatorul LAN să scruteze transmisiile IGMP dintre gazdă și router și să țină evidența grupurilor multicast și a porturilor membre. Când comutatorul primește un raport IGMP de la o gazdă pentru un anumit grup multicast, comutatorul adaugă numărul portului gazdă la intrarea tabelului de redirecționare; când primește un mesaj IGMP Leave Group de la o gazdă, elimină portul gazdă din intrarea tabelului. De asemenea, șterge periodic intrări dacă nu primește rapoarte de membru IGMP de la clienții multicast.

Routerul multicast trimite interogări generale periodice către toate VLAN-urile. Toate gazdele interesate de acest trafic multicast trimit cereri de alăturare și sunt adăugate la intrarea tabelului de redirecționare.

Utilizați**activare ip igmp snooping**comandă pentru a configura IGMP Snooping pe IR1800.

În mod implicit, IGMP Snooping este activat la nivel global în IR1800.

MLD snooping este, de asemenea, acceptat pe IR1800, iar informații suplimentare pot fi găsite în acest set de documentație:https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-1/configuration_guide/b_161_consolidated_3850_cg/b_161_consolidated_3850_cg_chapter_01100.html

Configurarea serviciului EVPN VXLAN VLAN-Aware

O instanță EVPN (EVI) compatibilă cu VLAN permite maparea mai multor subrețele (L2VNI) la un singur EVI. Când această caracteristică este configurată, MAC-VRF este identificat prin combinația dintre ruta-țintă și eticheta-ethernet. Rutele EVPN care necesită identificarea unui anumit tabel de punte în cadrul unui MAC-VRF vor face publicitate acestor rute cu câmpul Ethernet Tag setat la o valoare care permite o astfel de identificare. Această caracteristică îmbunătățește interoperabilitatea routerului.

Există două metode de a configura VLAN-Aware:

1.Configurație bazată pe profil

2.Configurare manuală

Orientări și limitări

- Puteți configura fie configurația bazată pe profil, fie metoda de configurare manuală pe un EVI. Ambele metode nu pot fi utilizate pentru a configura VLAN-aware pe același EVI de pe dispozitiv.
- Această caracteristică este acceptată numai pe Stratul 2. IRB și L3 nu sunt acceptate.

Configurație bazată pe profil a serviciului EVPN VXLAN VLAN-Aware

Configurați instanța EVPN VXLAN VLAN-Aware

Urmați această procedură pentru a configura o instanță EVPN (EVI) compatibilă cu VLAN:

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	configura terminalul **Exemplu:** Router#configure terminal	Intră în modul de configurare globală
Pasul 2	l2vpn evpn profile <nume-profil> <tip-serviciu> **Exemplu:** Router(config)#l2vpn evpn profile evpn_va vlan-aware	Configura un profil EVPN Vxlan Vlan-Aware.
Pasul 3	evi-id <id> **Exemplu:** Router(config-evpn-prof)#evi-id 1	Configurați id-ul instanței EVPN (EVI).
Pasul 4	etichetă-ethernet [auto-vni|auto-vlan] **Exemplu:** Router(config)#ethernet-tag auto-vlan	Permite generarea automată a etichetei Ethernet pe baza L2VNI sau pe valoarea VLAN. Valoarea implicită este*auto-vni*.
Pasul 5	(Opțional) l2vni-base <l2vni-base> **Exemplu:** Router(config-evpn-prof)#l2vni-base 50000	(Opțional) Configurați ID-ul de bază L2 Virtual Network Identifier (VNI).
Pasul 6	(Opțional) tip-replicare {*intrare*|*static* {[*ipv4_mcast_addr*|*ipv4_mcast_prefix*] **Exemplu:**	(Opțional) Configurați tipul de replicare.

	Comanda sau Acțiune	Scop
	Router(config-evpn-prof)#intrare tip replicare	
Pasul 7	(Opțional) încapsulare vxlan **Exemplu:** Router(config-evpn-prof)#capsulation vxlan	(Opțional) Configurați tipul de încapsulare.
Pasul 8	(Opțional) publicitate implicit-gateway {activare|dezactivare} **Exemplu:** Router(config)#default-gateway advertise enable	(Opțional) Activați sau dezactivați publicitatea gateway prestabilită.
Pasul 9	(Opțional) activarea publicității multicast **Exemplu:** Router(config)#multicast advertise enable	(Opțional) Activați sau dezactivați publicitatea multicast.
Pasul 10	(Opțional) ip local-learning {activare|dezactivare} **Exemplu:** Router(config)#ip activare local-learning	(Opțional) Activați sau dezactivați învățarea locală bazată pe IP.
Pasul 11	(Opțional) rezoluție-adresă de suprimare a inundațiilor {activare|dezactivare} **Exemplu:** Router(config)#flooding-suppression address-resolution enable	(Opțional) Activați sau dezactivați rezoluția adresei bazată pe suprimarea inundațiilor.
Pasul 12	(Opțional) re-originați ruta-type5 **Exemplu:** Router(config)#re-originate route-type5	(Opțional) Activați re-originarea rutelor de tip 5.

Aplicați configurația pe un domeniu Bridge

Urmați procedura pentru a aplica configurația pe un domeniu-punte pe dispozitivul dvs.:

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	bridge-domain <id> **Exemplu:** Router(config)#bridge-domain 12	Aplică configurația domeniului punte specificat.
Pasul 2	membru Vlan12 serviciu-instanță 12 **Exemplu:**	Specifică instanța de serviciu pentru membrul VLAN.

	Comanda sau Acțiune	Scop
	Router(config-bdomain)#member Vlan12 service-instance 12	
Pasul 3	membru evpn-instance profile <va-profile-name> **Exemplu:** Router(config-bdomain)#member evpn-instance profile evpn_va	Adăugați un membru EVI la domeniul-punte.

Configurarea manuală a serviciului EVPN VXLAN VLAN-Aware

Pentru a configura manual serviciul EVPN VXLAN VLAN-Aware pe dispozitivul dvs., finalizați aceste sarcini:

- Configurația statică a instanței EVPN VLAN-Aware VXLAN, la pagina 170
- Aplicarea configurației pe domeniul Bridge, la pagina 171
- Configurați replicarea intrării pentru EVPN VXLAN VLAN-Aware, la pagina 171
- Configurați replicarea statică pentru VLAN-Aware, la pagina 172

Configurația statică a instanței EVPN VXLAN VLAN-Aware

Urmați procedura pentru configurarea statică a instanței EVPN:

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	configura terminalul **Exemplu:** Router#configure terminal	Intră în modul de configurare globală
Pasul 2	l2vpn evpn instanță 1 vlan-aware **Exemplu:** Router(config)#l2vpn evpn instanță 1 vlan-aware	Configurați o instanță EVPN compatibilă cu VLAN.
Pasul 3	încapsulare vxlan **Exemplu:** Router(config-evpn-evi)#capsulation vxlan	Configurați tipul de încapsulare la VXLAN.

Exemplu

```
l2vpn evpn instanță 1 vlan-aware
  encapsulation vxlan
!
```

Aplicarea configurației pe domeniul Bridge

Urmați procedura pentru a aplica configurația pe domeniul bridge:

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	configura terminalul **Exemplu:** Router#configure terminal	Intră în modul de configurare globală
Pasul 2	domeniu-punte 12 **Exemplu:** Router(config)bridge-domain 12	Specifică domeniul punte pentru configurația care urmează să fie aplicată.
Pasul 3	membru Vlan12 serviciu-instanță 12 **Exemplu:** Router(config-bdomain)#member Vlan12 service-instance 12	Specifică instanța de serviciu pentru membrul VLAN.
Pasul 4	membru evpn-instance 1 vni <vni> ethernet-tag <etag> **Exemplu:** Router(config-bdomain)#member evpn-instance 1 vni 30012 ethernet-tag 20012	Configurați un membru EVI care știe VLAN în domeniul bridge-domain

Exemplu

```
domeniu-punte 12
  membru Vlan12 serviciu-instanță 12
  membru evpn-instance 1 vni 30012 ethernet-tag 20012
```

Configurați replicarea intrării pentru EVPN VXLAN VLAN-Aware

Urmați această procedură pentru a configura Ingress Replication pentru EVPN VXLAN VLAN-Aware:

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	configura terminalul **Exemplu:** Router#configure terminal	Intră în modul de configurare globală
Pasul 2	l2vpn evpn instanță 1 vlan-aware **Exemplu:**	Configurați o instanță EVPN compatibilă cu VLAN

	Comanda sau Acțiune	Scop
	Router(config)#l2vpn evpn instanță 1 vlan-aware	
Pasul 3	intrare de tip replicare **Exemplu:** Router(config-evpn-evi)#intrare tip replicare	Configurați tipul de replicare pentru replicarea de intrare.
Pasul 4	interfata nve1 **Exemplu:** Router(config)#interfață nve1	Configurați interfața NVE și intră în modul de configurare a interfeței.
Pasul 5	fara adresa ip **Exemplu:** Router(config-if)#fără adresă ip	Dezactivează procesarea IP pe interfață.
Pasul 6	sursă-interfață Loopback0 **Exemplu:** Router(config-if)#source-interface Loopback0	Specifică loopback-ul sursei pentru interfață.
Pasul 7	protocol de accesibilitate gazdă bgp **Exemplu:** Router(config-if)#protocol de accesibilitate gazdă bgp	Specifică protocolul BGP pentru accesibilitatea gazdei.
Pasul 8	membru vni 30000 replicare de intrare **Exemplu:** Router(config-if)#member vni 30000 replicare de intrare	Configurați membrul L2VNI cu replicarea intrării.

Exemplu

```
l2vpn evpn instanță 1 vlan-aware
  encapsulation vxlan
  intrare de tip replicare
!
interfata nve1
  fara adresa ip
  interfață-sursă Loopback0 protocol de
  accesibilitate gazdă membru bgp vni 30000
  membru de replicare de intrare vni 30012
  replicare de intrare
!
```

Configurați replicarea statică pentru VLAN-Aware

Urmați această procedură pentru a configura replicarea statică pentru VLAN-aware:

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	configura terminalul **Exemplu:** Router#configure terminal	Intră în modul de configurare globală
Pasul 2	l2vpn evpn instanță 1 vlan-aware **Exemplu:** Router(config)#l2vpn evpn instanță 1 vlan-aware	Activează VLAN-Aware pe instanța EVPN specificată.
Pasul 3	static de tip replicare **Exemplu:** Router(config)#replication-type static	Configurați tipul de replicare la replicare statică.
Pasul 4	interfata nve1 **Exemplu:** Router(config)#interfață nve1	Configurează interfața și intră în modul de configurare a interfeței.
Pasul 5	fara adresa ip **Exemplu:** Router(config-if)#fără adresă ip	Dezactivează procesarea IP pe interfață.
Pasul 6	sursă-interfață Loopback0 **Exemplu:** Router(config-if)#source-interface Loopback0	Specifică loopback-ul sursei pentru interfață.
Pasul 7	protocol de accesibilitate gazdă bgp **Exemplu:** Router(config-if)#protocol de accesibilitate gazdă bgp	Specifică protocolul BGP pentru accesibilitatea gazdei.
Pasul 8	membru vni 30000 mcast-group 209.165.1.1 **Exemplu:** Router(config-if)#member vni 30000 mcast-group 209.165.1.1	Configurați membrul VNI și grupul Multicast
Pasul 9	membru vni 30012 mcast-group 209.165.1.1 **Exemplu:** Router(config-if)#member vni 30012 mcast-group 209.165.1.1	Configurați membrul VNI și grupul Multicast

Exemplu

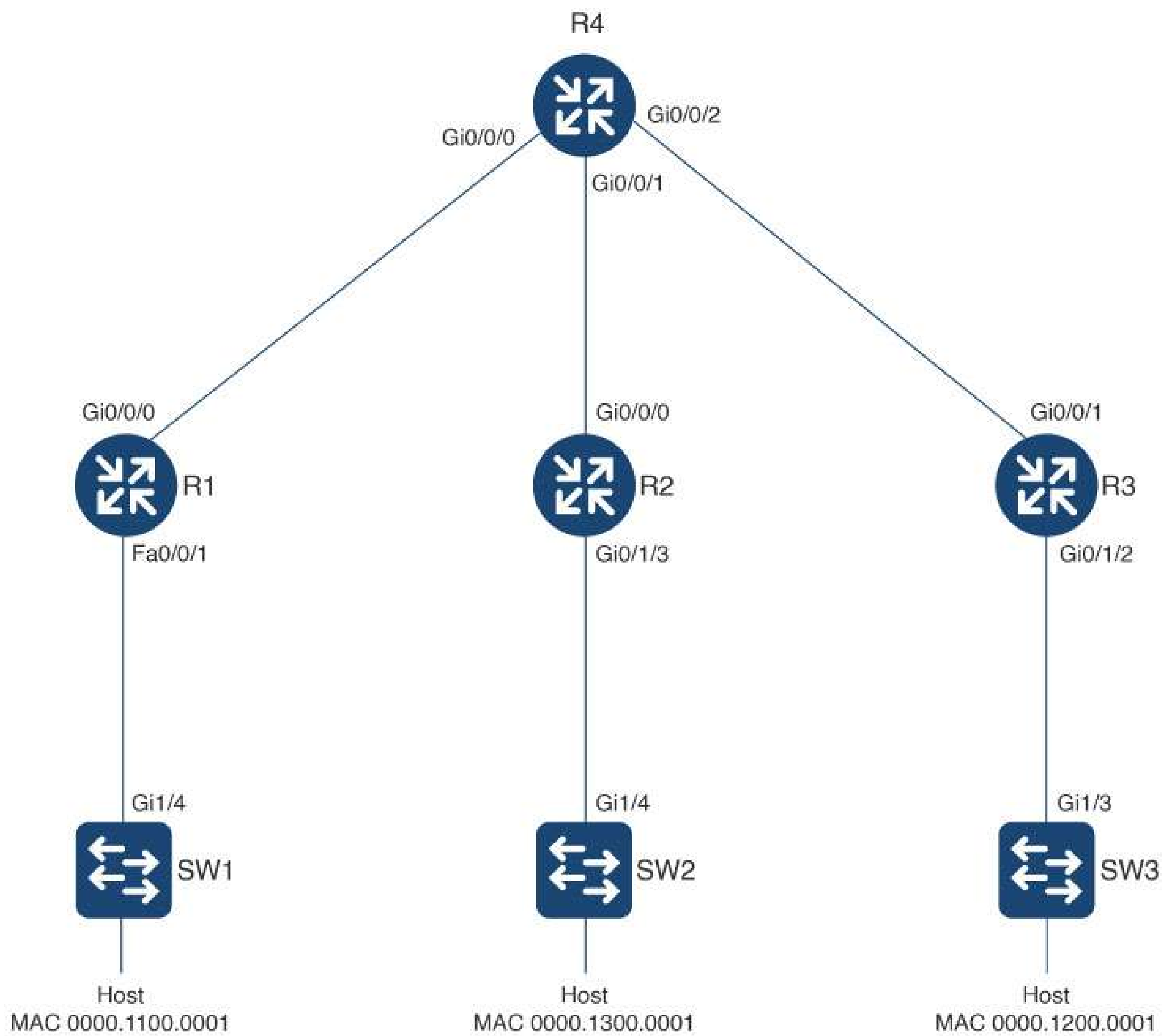
Exemplu:

```
l2vpn evpn instanță 1 vlan-aware
  encapsulation vxlan
  static de tip replicare
!
interfata nve1
  fara adresa ip
  sursă-interfață Loopback0 protocol de accesibilitate
  gazdă membru bgp vni 30000 mcast-group
  209.165.1.1 membru vni 30012 mcast-group
  209.165.1.1
!
```

Exemplu de configurare

Iată un exemplu de configurare a caracteristicii VLAN aware peste VXLAN EVPN într-o topologie de rețea cu trei routere (R1, R2 și R3) ca VTEP-uri (Virtual Tunnel Endpoint), conectate la trei porturi de comutare (SW1, SW2 și SW3) care sunt conectate la gazdă, în timp ce un router (R4) acționează ca*coloana vertebrală*așa cum se arată în figură.

Figura 50: Exemplu de configurare a topologiei cu 4 routere



Iată configurația de rulare pentru Router 1 (R1)

```
l2vpn evpn
  intrare de tip replicare
!
l2vpn evpn profile evpn_va vlan-aware evi-id 3

  l2vni-baza 50000
  ethernet-tag auto-vni
!
domeniu-punte 12
  membru Vlan12 service-instance 12 membru
  evpn-instance profil evpn_va
!
domeniu-punte 22
  membru Vlan22 service-instance 22 membru
  evpn-instance profil evpn_va

interfață Loopback0
  adresa ip 192.0.2.1 255.255.255.255
```

```
!
interfață GigabitEthernet0/0/0 adresa IP
  10.10.10.2 255.255.255.0
!
!
interfață FastEthernet0/0/1 trunk switchport
  permis vlan 12,22 trunk mod switchport

!
interfața Vlan12
  fara adresa ip
  instanță de serviciu 12 încapsulare
    ethernet dot1q 12
  !
!
interfața Vlan22
  fara adresa ip
  instanță de serviciu 22 încapsulare
    ethernet dot1q 22
  !
interfata nve1
  fara adresa ip
  sursă-interfață Loopback0 protocol de
  accesibilitate gazdă membru bgp vni 30000
  replicare de intrare
!
router ospf 1
  ID-ul routerului 192.0.2.1
  retea 10.10.10.0 0.0.0.255 zona 0 retea 192.0.2.1
  0.0.0.0 zona 0
!
router bgp 1
  bgp router-id 192.0.2.1 bgp log-neighbor-changes vecinul
  192.0.2.4 la distanță ca 1 vecin 192.0.2.4 update-source
  Loopback0 !


  adresa-familie ipv4
    vecin 192.0.2.4 activare vecin 192.0.2.4 trimitere-
    comunitate ambele exit-address-family

!
adresa-familie l2vpn evpn
    vecin 192.0.2.4 activare vecin 192.0.2.4 trimitere-
    comunitate ambele exit-address-family

!
```

Iată configurația de rulare pentru Router 2 (R2)

```
l2vpn evpn
  intrare de tip replicare
!
l2vpn evpn profile evpn_va vlan-aware evi-id 3

  l2vni-baza 50000
  ethernet-tag auto-vni
!
domeniu-punte 12
  membru Vlan12 service-instance 12 membru
  evpn-instance profil evpn_va
!
domeniu-punte 22
  membru Vlan22 service-instance 22 membru
  evpn-instance profil evpn_va
```

```
!
interfață Loopback0
  adresa ip 192.0.2.2 255.255.255.255
!
interfață GigabitEthernet0/0/0 adresa IP
  10.10.20.2 255.255.255.0
!
interfață trunchi GigabitEthernet0/1/3 switchport
  permis vlan 12,22 trunchi mod switchport

!
interfața Vlan12
  fara adresa ip
  instanță de serviciu 12 încapsulare
    ethernet dot1q 12
  !
!
interfața Vlan22
  fara adresa ip
  instanță de serviciu 22 încapsulare
    ethernet dot1q 22
  !
interfata nve1
  fara adresa ip
  sursă-interfață Loopback0 protocol de
  accesibilitate gazdă membru bgp vni 30000
  replicare de intrare
!
router ospf 1
  ID-ul routerului 192.0.2.2
  retea 10.10.20.0 0.0.0.255 zona 0 retea 192.0.2.2
  0.0.0.0 zona 0
!
router bgp 1
  bgp router-id 192.0.2.2 bgp log-neighbor-changes vecinul
  192.0.2.4 la distanță-ca 1 vecin 192.0.2.4 update-source
  Loopback0 !


  adresa-familie ipv4
    vecin 192.0.2.4 activare vecin 192.0.2.4 trimitere-
    comunitate ambele exit-address-family

!
adresa-familie l2vpn evpn
    vecin 192.0.2.4 activare vecin 192.0.2.4 trimitere-
    comunitate ambele exit-address-family

!
```

Iată configurația de rulare pentru Router 3 (R3)

```
l2vpn evpn
  intrare de tip replicare
!
l2vpn evpn profile evpn_va vlan-aware evi-id 3

  l2vni-baza 50000
  ethernet-tag auto-vni
!
domeniu-punte 12
  membru Vlan12 service-instance 12 membru
  evpn-instance profil evpn_va
!
domeniu-punte 22
```

```
  membru Vlan22 service-instance 22 membru
  evpn-instance profil evpn_va

interfață Loopback0
  adresa ip 192.0.2.3 255.255.255.255
!
interfață GigabitEthernet0/0/1 adresa IP
  10.10.30.2 255.255.255.0 interfață
GigabitEthernet0/1/2 trunk switchport permis
  vlan 12,22 trunk mod switchport

!
interfața Vlan12
  fara adresa ip
  instanță de serviciu 12 încapsulare
    ethernet dot1q 12
  !
!
interfața Vlan22
  fara adresa ip
  instanță de serviciu 22 încapsulare
    ethernet dot1q 22
  !
interfata nve1
  fara adresa ip
  sursă-interfață Loopback0 protocol de
  accesibilitate gazdă membru bgp vni 30000
  replicare de intrare
!
router ospf 1
  ID-ul routerului 192.0.2.3
  retea 10.10.30.0 0.0.0.255 zona 0 retea 192.0.2.3
  0.0.0.0 zona 0
!
router bgp 1
  bgp router-id 192.0.2.3 bgp log-neighbor-changes vecinul
  192.0.2.4 la distanță ca 1 vecin 192.0.2.4 update-source
  Loopback0 !


  adresa-familie ipv4
    vecin 192.0.2.4 activare vecin 192.0.2.4 trimitere-
    comunitate ambele exit-address-family

  !
  adresa-familie l2vpn evpn vecin 192.0.2.4 activare
    vecin 192.0.2.4 trimitere-comunitate ambele exit-
    address-family

!
```

Iată configurația de rulare pentru Router 4 (R4), care acționează ca *coloana vertebrală*.

```
interfață Loopback0
  adresa ip 192.0.2.4 255.255.255.255
!
interfață GigabitEthernet0/0/0 adresa IP
  10.10.10.1 255.255.255.0 negociere automată

!
interfață GigabitEthernet0/0/1 adresa IP
  10.10.20.1 255.255.255.0 negociere automată

!
```

```
interfață GigabitEthernet0/0/2 adresa IP
  10.10.30.1 255.255.255.0 negociere automată

!
router ospf 1
  ID-ul routerului 192.0.2.4
  retea 10.10.10.0 0.0.0.255 zona 0 retea
  10.10.20.0 0.0.0.255 zona 0 retea 10.10.30.0
  0.0.0.255 zona 0 retea 192.0.2.4 0.0.0.0 zona 0

!
router bgp 1
  bgp router-id 192.0.2.4 bgp log-neighbor-changes vecinul
  192.0.2.1 remote-as 1 vecin 192.0.2.1 update-source
  Loopback0 vecin 192.0.2.2 remote-as 1


  vecin 192.0.2.2 sursă de actualizare Loopback0 vecin
  192.0.2.3 la distanță ca 1
  vecin 192.0.2.3 sursă de actualizare Loopback0 !

adresa-familie l2vpn evpn
    vecin 192.0.2.1 activare vecin 192.0.2.1 trimitere-
    comunitate ambele vecin 192.0.2.1 route-reflector-client
    vecin 192.0.2.2 activare

    vecin 192.0.2.2 trimitere-comunitate ambele vecin
    192.0.2.2 route-reflector-client vecin 192.0.2.3 activare

    vecin 192.0.2.3 trimite-comunitate ambele exit-
  adresa-familie
!
```

Iată configurația de rulare pentru switchport-ul SW1, conectat la Router-ul R1.

```
interfață trunchi GigabitEthernet1/4 switchport
  permis vlan 12,22 trunchi mod switchport

!
interfață trunchi GigabitEthernet1/7 switchport
  permis vlan 12,22 trunchi mod switchport

!
```

Iată configurația de rulare pentru switchport SW2, conectat la Router R2.

```
interfață trunchi GigabitEthernet1/4 switchport
  permis vlan 12,22 trunchi mod switchport

!
interfață trunchi GigabitEthernet1/7 switchport
  permis vlan 12,22 trunchi mod switchport

!
```

Iată configurația de rulare pentru switchport SW3, conectat la Router R3.

```
  trunchiul switchport permis vlan 12,22 trunk
  mod switchport
!
interfață trunchi GigabitEthernet1/7 switchport
  permis vlan 12,22 trunchi mod switchport

!
```

Verificați configurația serviciului EVPN VXLAN VLAN-Aware

Verificați configurația pe routerul R1

Utilizați**arată l2vpn evpn evi 3 detaliu**comandă pentru a verifica configurația EVI și a domeniului punte și pentru a se asigura că valoarea etichetei ethernet este configurată.

```
Router1#arată l2vpn evpn evi 3 detaliu
Instanță EVPN:              3 (conștient VLAN)
  Profil:                   evpn_va
  RD:                       10.10.10.2:32770 (automat) 1:3
  Import-RT-uri:
  Export-RT-uri:            1:3
  Etichetă per-EVI:         nici unul
  Stat:                     Stabilit
  Tip de replicare:         Intrare (profil)
  Încapsulare:              vxlan (profil)
  IP Local Learn:           Activat (global)
  Adv. Def. Gateway: Dezactivat (global) Re-originați
  RT5: Dezactivat (profil) Suprimarea inundațiilor AR:
  Activat (global) Domeniu Bridge:
                            12
    Etichetă Ethernet:      50012
    Stat:                   Stabilit
    Suprimarea inundațiilor: Ataşat
    De bază dacă:
    Acces dacă:
    NVE dacă:               nve1
    RMAC:                   0000,0000,0000
    Core BD:                0
    L2 VNI:                 50012
    L3 VNI:                 0
    IP VTEP:                192.0.2.1
    Pseudoporturi:
      Instanța 12 a serviciului Vlan12
        Rute: 0 MAC, 0 MAC/IP Peers:

      192.0.2.2
        Rute: 0 MAC, 0 MAC/IP, 1 IMET, 0 EAD
      192.0.2.3
        Rute: 1 MAC, 0 MAC/IP, 1 IMET, 0 EAD Bridge
        Domain:             22
    Etichetă Ethernet:      50022
    Stat:                   Stabilit
    Suprimarea inundațiilor: Ataşat
    De bază dacă:
    Acces dacă:
    NVE dacă:               nve1
    RMAC:                   0000,0000,0000
    Core BD:                0
    L2 VNI:                 50022
    L3 VNI:                 0
    IP VTEP:                192.0.2.1
    Pseudoporturi:
      Instanța 22 a serviciului Vlan22
        Rute: 0 MAC, 0 MAC/IP Peers:

      192.0.2.2
        Rute: 0 MAC, 0 MAC/IP, 1 IMET, 0 EAD
      192.0.2.3
        Rute: 0 MAC, 0 MAC/IP, 1 IMET, 0 EAD
```

Utilizați**arata l2route evpn imet**comanda pentru verificarea rutelor IMET.

```
Router1#arata l2route evpn imet EVI
          ETAG    Prod                                Adresa IP router     Tip      Eticheta
                  Proxy multicast ID tunel
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------3
          50012     BGP                                10.10.20.2         6        50012
                    192.0.2.2                 Nu
      3   50012     BGP                                10.10.30.2         6        50012
                    192.0.2.3                 Nu
      3   50012   L2VPN                                10.10.10.2         6        50012
                    192.0.2.1                 Nu
      3   50022     BGP                                10.10.20.2         6        50022
                    192.0.2.2                 Nu
      3   50022     BGP                                10.10.30.2         6        50022
                    192.0.2.3                 Nu
      3   50022   L2VPN                                10.10.10.2         6        50022
                    192.0.2.1                 Nu
```

Utilizați**arată ip bgp l2vpn evpn all**comanda pentru a verifica configurația.

```
Router1#arată ip bgp l2vpn evpn all
Versiunea tabelului BGP este 31, ID-ul routerului local este 192.0.2.1
Coduri de stare: s suprimat, d amortizat, h istoric, * valid, > cel mai bun, i - intern,
                 r RIB-failter, S Stale, m multipath, b backup-path, f RT-Filter, x best-external, a
                 additional-path, c RIB-compressed,
                 t cale secundară, L longeviv-învechit,
Coduri de origine: i - IGP, e - EGP, ? - coduri de validare RPKI incomplete: V
valid, I invalid, N Nu a fost găsit

     Rețea                Următorul Hop          Calea ponderii LocPrf metric
Distingere traseu: 192.0.2.1:32770
 * >   [2][192.0.2.1:32770][50012][48][000011000001][0][*]/20
                           0.0.0.0                                  32768 ?
 * > i [2][192.0.2.1:32770][50012][48][000012000001][0][*]/20
                           192.0.2.3                0 100           0 ?
 * > i [2][192.0.2.1:32770][50012][48][000013000001][0][*]/20
                           192.0.2.2                0 100           0 ?
 * > i [2][192.0.2.1:32770][50012][48][04BD9708512B][0][*]/20
                           192.0.2.3                0 100           0 ?
 * >   [2][192.0.2.1:32770][50022][48][000011000002][0][*]/20
                           0.0.0.0                                  32768 ?
 * > i [2][192.0.2.1:32770][50022][48][000012000002][0][*]/20
                           192.0.2.3                0 100           0 ?
 * > i [2][192.0.2.1:32770][50022][48][000013000002][0][*]/20
                           192.0.2.2                0   100         0 ?
Distingere traseu: 192.0.2.2:32770
 * > i [2][192.0.2.2:32770][50012][48][000013000001][0][*]/20
                           192.0.2.2                0 100           0 ?
 * > i [2][192.0.2.2:32770][50022][48][000013000002][0][*]/20
                           192.0.2.2                0   100         0 ?
Distingere traseu: 192.0.2.3:32770
 * > i [2][192.0.2.3:32770][50012][48][000012000001][0][*]/20
                           192.0.2.3                0 100           0 ?
 * > i [2][192.0.2.3:32770][50012][48][04BD9708512B][0][*]/20
                           192.0.2.3                0 100           0 ?
 * > i [2][192.0.2.3:32770][50022][48][000012000002][0][*]/20
                           192.0.2.3                0   100         0 ?
Distingere traseu: 192.0.2.1:32770
 * >   [3][192.0.2.1:32770][50012][32][192.0.2.1]/17
                           0.0.0.0                                  32768 ?
 * > i [3][192.0.2.1:32770][50012][32][192.0.2.2]/17
                           192.0.2.2                0 100           0 ?
 * > i [3][192.0.2.1:32770][50012][32][192.0.2.3]/17
                           192.0.2.3                0 100           0 ?
 * >   [3][192.0.2.1:32770][50022][32][192.0.2.1]/17
```

```
                                    0.0.0.0                                32768 ?
 * > i    [3][192.0.2.1:32770][50022][32][192.0.2.2]/17
                                    192.0.2.2              0 100           0 ?
 * > i    [3][192.0.2.1:32770][50022][32][192.0.2.3]/17
                                    192.0.2.3              0    100        0 ?
Distingere traseu: 192.0.2.2:32770
 * > i    [3][192.0.2.2:32770][50012][32][192.0.2.2]/17
                                    192.0.2.2              0 100           0 ?
 * > i    [3][192.0.2.2:32770][50022][32][192.0.2.2]/17
                                    192.0.2.2              0    100        0 ?
Distingere traseu: 192.0.2.3:32770
 * > i    [3][192.0.2.3:32770][50012][32][192.0.2.3]/17
                                    192.0.2.3              0 100           0 ?
 * > i    [3][192.0.2.3:32770][50022][32][192.0.2.3]/17
                                    192.0.2.3              0 100           0 ?
```

Utilizați**arată nve peers**comanda pentru a verifica configurația.

```
Router1#arată nve peers
„M” – indicatorul de descărcare a intrării MAC „A” – indicatorul de descărcare
adiacentă „4” - steag IPv4 „6” - steag IPv6

Interfață  VNI    Tastați Peer-IP      RMAC/Num_RTs   eVNI    steaguri de stat UP
nve1       50012  L2CP 192.0.2.2   1                 50012   SUS  N/A  00:38:47
nve1       50012  L2CP 192.0.2.3   1                 50012   SUS  N/A  00:38:47
nve1       50022  L2CP 192.0.2.2   1                 50022   SUS  N/A  00:38:47
nve1       50022  L2CP 192.0.2.3   1                 50022   SUS  N/A  00:38:47
```

Utilizați**arată l2vpn evpn mac**comanda pentru a verifica configurația.

```
Router1#arată l2vpn evpn mac
Adresa MAC EVI BD                ESI                                Ether Tag Următorul hop(e)
-------------------------------------------------------------------------------- 0000.1100.0001 3
                         12      0000.0000.0000.0000.0000 50012          Vl12:12
0000.1200.0001 3         12      0000.0000.0000.0000.0000 50012          192.0.2.3
0000.1300.0001 3         12      0000.0000.0000.0000.0000 50012          192.0.2.2
04bd.9708.512b 3         12      0000.0000.0000.0000.0000 50012          192.0.2.3
0000.1100.0002 3         22      0000.0000.0000.0000.0000 50022          Vl22:22
0000.1200.0002 3         22      0000.0000.0000.0000.0000 50022          192.0.2.3
0000.1300.0002 3         22      00.000.000.000.000. 50022               192.0.2.2
```

Verificați configurația pe routerul R2

Utilizați**arată l2vpn evpn evi 3 detaliu**comandă pentru a verifica configurația EVI și a domeniului punte și pentru a se asigura că valoarea etichetei ethernet este configurată.

```
Router2#arată l2vpn evpn evi 3 detaliu

Instanță EVPN:              3 (conștient VLAN)
  Profil:                   evpn_va
  RD:                       10.10.20.2:32770 (automat) 1:3
  Import-RT-uri:
  Export-RT-uri:            1:3
  Etichetă per-EVI:         nici unul
  Stat:                     Stabilit
  Tip de replicare:         Intrare (profil)
  Încapsulare:              vxlan (profil)
  IP Local Learn:           Activat (global)
  Adv. Def. Gateway: Dezactivat (global) Re-originați
  RT5: Dezactivat (profil) Suprimarea inundațiilor AR:
  Activat (global) Domeniu Bridge:
                            12
    Etichetă Ethernet:      50012
    Stat:                   Stabilit
    Suprimarea inundațiilor: Ataşat
```

```
De bază dacă:
Acces dacă:
                    NVE dacă:       nve1
                    RMAC:           0000,0000,0000
                    Core BD:        0
                    L2 VNI:         50012
                    L3 VNI:         0
                    IP VTEP:        192.0.2.2
    Pseudoporturi:
      Instanța 12 a serviciului Vlan12
        Rute: 0 MAC, 0 MAC/IP Peers:

      192.0.2.1
        Rute: 0 MAC, 0 MAC/IP, 1 IMET, 0 EAD 192.0.2.3
        Rute: 1 MAC, 0 MAC/IP, 1 IMET, 0 EAD Bridge
                        Domain:         22
                    Etichetă Ethernet:  50022
                    Stat:               Stabilit
                    Suprimarea inundațiilor: Atașat
De bază dacă:
Acces dacă:
                    NVE dacă:       nve1
                    RMAC:           0000,0000,0000
                    Core BD:        0
                    L2 VNI:         50022
                    L3 VNI:         0
                    IP VTEP:        192.0.2.2
  Pseudoporturi:
  Instanța 22 a serviciului Vlan22
  Rute: 0 MAC, 0 MAC/IP Peers:

        192.0.2.1
          Rute: 0 MAC, 0 MAC/IP, 1 IMET, 0 EAD
        192.0.2.3
          Rute: 0 MAC, 0 MAC/IP, 1 IMET, 0 EAD
```

Utilizați**arata l2route evpn imet**comanda pentru verificarea rutelor IMET.

```
Router2#arata l2route evpn imet EVI
                ETAG Prod                                   Adresa IP router Tip Eticheta
                        Proxy multicast ID tunel

---------------------------------------------------------------------------------------------------- 3
                50012       BGP                                 10.10.10.2      6       50012
                            192.0.2.1               Nu
  3             50012       BGP                                 10.10.30.2      6       50012
                            192.0.2.3               Nu
  3             50012   L2VPN                                   10.10.20.2      6       50012
                            192.0.2.2               Nu
  3             50022       BGP                                 10.10.10.2      6       50022
                            192.0.2.1               Nu
  3             50022       BGP                                 10.10.30.2      6       50022
                            192.0.2.3               Nu
  3             50022   L2VPN                                   10.10.20.2      6       50022
                            192.0.2.2               Nu
```

Utilizați**arată ip bgp l2vpn evpn all**comanda pentru a verifica configurația.

```
Router2#sh ip bgp l2vpn evpn all
Versiunea tabelului BGP este 27, ID-ul routerului local este 192.0.2.2
Coduri de stare: s suprimat, d amortizat, h istoric, * valid, > cel mai bun, i - intern,
                 r RIB-failter, S Stale, m multipath, b backup-path, f RT-Filter, x best-external, a additional-
                 path, c RIB-compressed,
```

```
                    t cale secundară, L longeviv-învechit,
Coduri de origine: i - IGP, e - EGP, ? - coduri de validare RPKI incomplete: V
valid, I invalid, N Nu a fost găsit

     Reţea                Următorul Hop          Calea ponderii LocPrf metric
Distingere traseu: 192.0.2.1:32770
 * > i   [2][192.0.2.1:32770][50012][48][000011000001][0][*]/20
                           192.0.2.1                0 100              0 ?
 * > i   [2][192.0.2.1:32770][50022][48][000011000002][0][*]/20
                           192.0.2.1                0      100         0 ?
Distingere traseu: 192.0.2.2:32770
 * > i   [2][192.0.2.2:32770][50012][48][000011000001][0][*]/20
                           192.0.2.1                0 100              0 ?
 * > i   [2][192.0.2.2:32770][50012][48][000012000001][0][*]/20
                           192.0.2.3                0 100              0 ?
 * >     [2][192.0.2.2:32770][50012][48][000013000001][0][*]/20
                           0.0.0.0                                     32768 ?
 * > i   [2][192.0.2.2:32770][50012][48][04BD9708512B][0][*]/20
                           192.0.2.3                0 100              0 ?
 * > i   [2][192.0.2.2:32770][50022][48][000011000002][0][*]/20
                           192.0.2.1                0 100              0 ?
 * > i   [2][192.0.2.2:32770][50022][48][000012000002][0][*]/20
                           192.0.2.3                0 100              0 ?
 * >     [2][192.0.2.2:32770][50022][48][000013000002][0][*]/20
                           0.0.0.0                                     32768 ?
Distingere traseu: 192.0.2.3:32770
 * > i   [2][192.0.2.3:32770][50012][48][000012000001][0][*]/20
                           192.0.2.3                0 100              0 ?
 * > i   [2][192.0.2.3:32770][50012][48][04BD9708512B][0][*]/20
                           192.0.2.3                0 100              0 ?
 * > i   [2][192.0.2.3:32770][50022][48][000012000002][0][*]/20
                           192.0.2.3                0      100         0 ?
Distingere traseu: 192.0.2.1:32770
 * > i   [3][192.0.2.1:32770][50012][32][192.0.2.1]/17
                           192.0.2.1                0 100              0 ?
 * > i   [3][192.0.2.1:32770][50022][32][192.0.2.1]/17
                           192.0.2.1                0      100         0 ?
Distingere traseu: 192.0.2.2:32770
 * > i   [3][192.0.2.2:32770][50012][32][192.0.2.1]/17
                           192.0.2.1                0 100              0 ?
 * >     [3][192.0.2.2:32770][50012][32][192.0.2.2]/17
                           0.0.0.0                                     32768 ?
 * > i   [3][192.0.2.2:32770][50012][32][192.0.2.3]/17
                           192.0.2.3                0 100              0 ?
 * > i   [3][192.0.2.2:32770][50022][32][192.0.2.1]/17
                           192.0.2.1                0 100              0 ?
 * >     [3][192.0.2.2:32770][50022][32][192.0.2.2]/17
                           0.0.0.0                                     32768 ?
 * > i   [3][192.0.2.2:32770][50022][32][192.0.2.3]/17
                           192.0.2.3                0      100         0 ?
Distingere traseu: 192.0.2.3:32770
 * > i   [3][192.0.2.3:32770][50012][32][192.0.2.3]/17
                           192.0.2.3                0 100              0 ?
 * > i   [3][192.0.2.3:32770][50022][32][192.0.2.3]/17
                           192.0.2.3                0 100              0 ?
```

Utilizați**arată nve peers**comanda pentru a verifica configurația.

```
Router2#arată nve peers
„M” – indicatorul de descărcare a intrării MAC „A” – indicatorul de descărcare
adiacentă „4” - steag IPv4 „6” - steag IPv6

Interfață  VNI     Tastați Peer-IP    RMAC/Num_RTs   eVNI     steaguri de stat UP
nve1       50012   L2CP 192.0.2.1     2              50012    SUS  N/A 00:05:28
nve1       50012   L2CP 192.0.2.3     3              50012    SUS  N/A 00:05:28
```

nve1	50022	L2CP 192.0.2.1	2	50022	SUS	N / A	00:05:28
nve1	50022	L2CP 192.0.2.3	2	50022	SUS	N / A	00:05:28

Utilizați**arată l2vpn evpn mac**comanda pentru a verifica configurația

```
Router2#arată l2vpn evpn mac
Adresa MAC EVI BD                ESI                                Ether Tag Următorul(e) hop(e)
-------------------------------------------------------------------------------- 0000.1100.0001 3
                      12         0000.0000.0000.0000.0000 50012     192.0.2.1
0000.1200.0001 3      12         0000.0000.0000.0000.0000 50012     192.0.2.3
0000.1300.0001 3      12         0000.0000.0000.0000.0000 50012     Vl12:12
04bd.9708.512b 3      12         0000.0000.0000.0000.0000 50012     192.0.2.3
0000.1100.0002 3      22         0000.0000.0000.0000.0000 50022     192.0.2.1
0000.1200.0002 3      22         0000.0000.0000.0000.0000 50022     192.0.2.3
0000.1300.0002 3      22         00.000.000.000.000. 50022          Vl22:22
```

Verificați configurația pe routerul R3

Utilizați**arată l2vpn evpn evi 3 detaliu**comandă pentru a verifica configurația EVI și a domeniului punte și pentru a se asigura că valoarea etichetei ethernet este configurată.

```
Router3#arată l2vpn evpn evi 3 detaliu
Instanță EVPN:                  3 (conștient VLAN)
  Profil:                       evpn_va
  RD:                           10.10.30.2:32770 (automat) 1:3
  Import-RT-uri:
  Export-RT-uri:                1:3
  Etichetă per-EVI:             nici unul
  Stat:                         Stabilit
  Tip de replicare:             Intrare (profil)
  Încapsulare:                  vxlan (profil)
  IP Local Learn:               Activat (global)
  Adv. Def. Gateway: Dezactivat (global) Re-originați
  RT5: Dezactivat (profil) Suprimarea inundațiilor AR:
  Activat (global) Domeniu Bridge:
                                12
    Etichetă Ethernet:          50012
    Stat:                       Stabilit
    Suprimarea inundațiilor:    Ataşat
    De bază dacă:
    Acces dacă:
    NVE dacă:                   nve1
    RMAC:                       0000,0000,0000
    Core BD:                    0
    L2 VNI:                     50012
    L3 VNI:                     0
    IP VTEP:                    192.0.2.3
    Pseudoporturi:
      Instanța 12 a serviciului Vlan12
        Rute: 1 MAC, 0 MAC/IP Peers:

      192.0.2.1
        Rute: 0 MAC, 0 MAC/IP, 1 IMET, 0 EAD
      192.0.2.2
        Rute: 0 MAC, 0 MAC/IP, 1 IMET, 0 EAD Bridge
        Domain:                 22
    Etichetă Ethernet:          50022
    Stat:                       Stabilit
    Suprimarea inundațiilor:    Ataşat
    De bază dacă:
    Acces dacă:
    NVE dacă:                   nve1
    RMAC:                       0000,0000,0000
    Core BD:                    0
```

```
  L2 VNI:                 50022
  L3 VNI:                 0
  IP VTEP:                192.0.2.3
  Pseudoporturi:
    Instanța 22 a serviciului Vlan22
      Rute: 0 MAC, 0 MAC/IP Peers:

    192.0.2.1
      Rute: 0 MAC, 0 MAC/IP, 1 IMET, 0 EAD
    192.0.2.2
      Rute: 0 MAC, 0 MAC/IP, 1 IMET, 0 EAD
```

Utilizați**arata l2route evpn imet**comanda pentru verificarea rutelor IMET.

```
Router3#arata l2route evpn imet
  EVI        ETAG     Prod                                Adresa IP router      Tip      Eticheta
                      Proxy multicast ID tunel
------------------------------------------------------------------------------------------------
------------------------------------------------------------------3
             50012      BGP                                10.10.10.2            6        50012
                        192.0.2.1                 Nu
    3        50012      BGP                                10.10.20.2            6        50012
                        192.0.2.2                 Nu
    3        50012    L2VPN                                10.10.30.2            6        50012
                        192.0.2.3                 Nu
    3        50022      BGP                                10.10.10.2            6        50022
                        192.0.2.1                 Nu
    3        50022      BGP                                10.10.20.2            6        50022
                        192.0.2.2                 Nu
    3        50022    L2VPN                                10.10.30.2            6        50022
                        192.0.2.3                 Nu
```

Utilizați**arată ip bgp l2vpn evpn all**comanda pentru a verifica configurația.

```
Router3#sh ip bgp l2vpn evpn all
Versiunea tabelului BGP este 30, ID-ul routerului local este 192.0.2.3
Coduri de stare: s suprimat, d amortizat, h istoric, * valid, > cel mai bun, i - intern,
                 r RIB-failter, S Stale, m multipath, b backup-path, f RT-Filter, x best-external, a
                 additional-path, c RIB-compressed,
                 t cale secundară, L longeviv-învechit,
Coduri de origine: i - IGP, e - EGP, ? - coduri de validare RPKI incomplete: V
valid, I invalid, N Nu a fost găsit

     Rețea                Următorul Hop          Calea ponderii LocPrf metric
Distingere traseu: 192.0.2.1:32770
 * > i  [2][192.0.2.1:32770][50012][48][000011000001][0][*]/20
                           192.0.2.1                0 100             0 ?
 * > i  [2][192.0.2.1:32770][50022][48][000011000002][0][*]/20
                           192.0.2.1                0      100        0 ?
Distingere traseu: 192.0.2.2:32770
 * > i  [2][192.0.2.2:32770][50012][48][000013000001][0][*]/20
                           192.0.2.2                0 100             0 ?
 * > i  [2][192.0.2.2:32770][50022][48][000013000002][0][*]/20
                           192.0.2.2                0      100        0 ?
Distingere traseu: 192.0.2.3:32770
 * > i  [2][192.0.2.3:32770][50012][48][000011000001][0][*]/20
                           192.0.2.1                0 100             0 ?
 * >    [2][192.0.2.3:32770][50012][48][000012000001][0][*]/20
                           0.0.0.0                                    32768 ?
 * > i  [2][192.0.2.3:32770][50012][48][000013000001][0][*]/20
                           192.0.2.2                0 100             0 ?
 * >    [2][192.0.2.3:32770][50012][48][04BD9708512B][0][*]/20
                           0.0.0.0                                    32768 ?
 * > i  [2][192.0.2.3:32770][50022][48][000011000002][0][*]/20
                           192.0.2.1                0 100             0 ?
```

```
 * >     [2][192.0.2.3:32770][50022][48][000012000002][0][*]/20
                                0.0.0.0                                32768 ?
 * > i   [2][192.0.2.3:32770][50022][48][000013000002][0][*]/20
                                192.0.2.2                0    100      0 ?
Distingere traseu: 192.0.2.1:32770
 * > i   [3][192.0.2.1:32770][50012][32][192.0.2.1]/17
                                192.0.2.1                0 100         0 ?
 * > i   [3][192.0.2.1:32770][50022][32][192.0.2.1]/17
                                192.0.2.1                0    100      0 ?
Distingere traseu: 192.0.2.2:32770
 * > i   [3][192.0.2.2:32770][50012][32][192.0.2.2]/17
                                192.0.2.2                0 100         0 ?
 * > i   [3][192.0.2.2:32770][50022][32][192.0.2.2]/17
                                192.0.2.2                0    100      0 ?
Distingere traseu: 192.0.2.3:32770
 * > i   [3][192.0.2.3:32770][50012][32][192.0.2.1]/17
                                192.0.2.1                0 100         0 ?
 * > i   [3][192.0.2.3:32770][50012][32][192.0.2.2]/17
                                192.0.2.2                0 100         0 ?
 * >     [3][192.0.2.3:32770][50012][32][192.0.2.3]/17
                                0.0.0.0                                32768 ?
 * > i   [3][192.0.2.3:32770][50022][32][192.0.2.1]/17
                                192.0.2.1                0 100         0 ?
 * > i   [3][192.0.2.3:32770][50022][32][192.0.2.2]/17
                                192.0.2.2                0 100         0 ?
 * >     [3][192.0.2.3:32770][50022][32][192.0.2.3]/17
                                0.0.0.0                                32768 ?
```

Utilizați**arată nve peers**comanda pentru a verifica configurația.

```
Router3#arată nve peers
„M” – indicatorul de descărcare a intrării MAC „A” – indicatorul de descărcare
adiacentă „4” - steag IPv4 „6” - steag IPv6

Interfață  VNI      Tastați Peer-IP          RMAC/Num_RTs   eVNI     steaguri de stat UP
nve1       50012    L2CP 192.0.2.1           2              50012    SUS  N/A 00:07:48
nve1       50012    L2CP 192.0.2.2           2              50012    SUS  N/A 00:05:23
nve1       50022    L2CP 192.0.2.1           2              50022    SUS  N/A 00:07:48
nve1       50022    L2CP 192.0.2.2           2              50022    SUS  N/A 00:05:23
```

Utilizați**arată l2vpn evpn mac**comanda pentru a verifica configurația

```
Router3#arată l2vpn evpn mac Adresa
MAC EVI BD ESI                                                  Ether Tag Următorul(e) hop(e)
-------------------------------------------------------------------------- 0000.1100.0001 3
                    12      0000.0000.0000.0000.0000 50012              192.0.2.1
0000.1200.0001 3    12      0000.0000.0000.0000.0000 50012              Vl12:12
0000.1300.0001 3    12      0000.0000.0000.0000.0000 50012              192.0.2.2
0000.1100.0002 3    22      0000.0000.0000.0000.0000 50022              192.0.2.1
0000.1200.0002 3    22      0000.0000.0000.0000.0000 50022              Vl22:22
0000.1300.0002 3    22      0000.0000.0000.0000.0000 50022              192.0.2.2
```

CAPITOL 14

Alimentare prin Ethernet (PoE)

Această secțiune conține următoarele:

Power over Ethernet Prezentare generală

Power over Ethernet (PoE) este de obicei folosit pentru a alimenta dispozitive precum punctele de acces, camerele IP și telefoanele IP conectate la porturile Ethernet ale dispozitivului. Puterea totală disponibilă PoE este de 30 W, care va fi partajată de cele 4 porturi LAN.

Alocarea puterii este următoarea:

- 1 x port POE+ (AT Type2, Clasa 4) (25,5 W)
- 1 x porturi POE (AT Type1 sau AF-Class 0/3) (15,4 W)
- 4 x porturi POE (AF, Clasa 1, Clasa 2) (3,84 W sau 6,49 W)

Detectarea dispozitivului și alocarea puterii

Routerul va detecta un Cisco Pre-standard sau un PD compatibil cu IEEE atunci când PoE este activat și dispozitivul conectat nu este alimentat de un adaptor de curent alternativ.

După detectarea dispozitivului, routerul va determina cerințele de alimentare pe baza clasei de clasificare a puterii. În funcție de puterea disponibilă în bugetul de putere, routerul determină dacă un port poate fi alimentat. Routerul alocă inițial această putere atunci când detectează și alimentează dispozitivul. Negocierea de putere folosind protocoalele CDP/LLDP are loc ulterior. Protocoalele acceptate pentru negocierea puterii sunt CDP pentru Cisco PD și LLDP pentru non-Cisco PD. Bugetul maxim de putere pentru 4 porturi LAN combinate în orice moment este de 30,8 W. La reîncărcare, porturile PoE sunt oprite până când unitatea repornește.

Interfață de linie de comandă

Această secțiune descrie CLI-ul de utilizat pentru configurarea și afișarea PoE.

Pentru a configura automat sau oprit:

putere în linie*auto* | *nu*

Exemplu de configurare:

Router#**terminal de configurare** Router#**interfață g0/1/ <0,1,2,3>** Router(config-if)#**putere în linie {auto| niciodată}**

Pentru a vă verifica configurația:

Router#**arată puterea în linie**
Disponibil:30,0(w) Folosit:22,5(w) Rest:7,5(w)

Interfață	Admin	Opera	Putere (Wați)	Dispozitiv	Clasa	max
- Gi0/1/0						
	auto	pe	15.4	Ieee PD	4	30,0
Gi0/1/1	auto	oprit	0,0	N / A	N / A	30,0
Gi0/1/2	auto	oprit	0,0	N / A	N / A	30,0
Gi0/1/3	auto	pe	7.1	Telefon IP 8845	2	30,0

Router#

Pentru a afișa puterea pe o anumită interfață:

Router#**arată puterea în linie {interfață-id}**

Afișează starea PoE pentru un router pentru interfața specificată.

arată puterea în linie*ID-ul interfeței*detaliu

Pentru a afișa consumul de energie:

Router#**arata putere**
PSU principal:
Putere totală consumată: 20,99 wați Mod configurat: N/A
Starea curentă de rulare aceeași: N/A Sursă de alimentare: Modul extern PS POE:

Mod configurat: N/A Starea curentă de rulare aceeași: N/A Putere totală disponibilă: 30 Watt Router#

Lista de comenzi pentru depanarea PoE este următoarea:

Comanda	**Descriere**
Depanați controlerul ilpower	Afișează mesajele de depanare a controlerului PoE
Depanați evenimentul ilpower	Afișează mesajele de depanare a evenimentelor PoE
Depanați portul ilpower	Afișează mesajele de depanare a managerului de porturi PoE
Depanați ilpower powerman	Afișează mesajele de depanare de gestionare a alimentării PoE
Depanați ilpower cdp	Afișează mesajele de depanare PoE CDP
Depanați registrele ilpower	Afișează mesajele de depanare a registrelor PoE

Comanda	Descriere
Depanați ilpower scp	Afișează mesajele de depanare PoE scp

CAPITOL 15

Distribuție vCPU și RAM

Introducere

Acest capitol oferă informații despre cum să distribuiți nucleele unității centrale de procesare virtuală (vCPU) și resursele RAM pentru aplicațiile Cisco IOx pe routerul Cisco Catalyst IR1835.

Nota vCPU este cunoscut și ca procesor fizic.

Distribuția resurselor vCPU și RAM pentru aplicațiile Cisco IOx

Distribuirea eficientă a resurselor disponibile vă permite să rulați mai multe aplicații IOx simultan.

Utilizați aceste șabloane pentru a distribui resursele vCPU și RAM:

- **Avion de date grele—**Se referă la o configurație de router în care majoritatea resurselor de sistem sunt dedicate planului de date, care este responsabil pentru procesarea și redirecționarea pachetelor de rețea.

  Șablonul Data Plane Heavy maximizează debitul și asigură transferul de pachete de mare viteză, care este esențial pentru cerințele de trafic de rețea. Acest lucru asigură mai multă putere de procesare și memorie pentru a face față sarcinii crescute pe planul de date, îmbunătățind capacitatea routerului de a muta eficient volume mari de date.

Nota Data Plane Heavy este șablonul implicit pentru distribuția vCPU și RAM în routerul IR1835.

- **Avion de serviciu greu—**Se referă la o configurație de router în care majoritatea resurselor de sistem sunt alocate planului de servicii, care este responsabil pentru furnizarea de servicii de rețea, cum ar fi calitatea serviciului (QoS), funcții de securitate și echilibrarea sarcinii.

  Șablonul Service Plane Heavy alocă vCPU și RAM suplimentar aplicațiilor IOx. Cu toate acestea, reduce debitul de date (lățimea de bandă).

Nota Routerele cu 2 GB RAM și un singur nucleu vCPU (resurse IOx) nu pot rula mai multe aplicații IOx, cum ar fi Unified Threat Defense și Cisco Cyber Vision.

Alocare mai mare pentru CPU și RAM pentru aplicațiile IOx

Din Cisco IOS XE Versiunea 17.15.1, routerul IR1835 cu 8 GB RAM acceptă șabloanele de distribuție Data Plane Heavy și Service Plane Heavy. Puteți aloca 3 GB RAM și două nuclee vCPU routerului IR1835 pentru găzduirea aplicațiilor Cisco IOx. Vă recomandăm șablonul Service Plane Heavy pentru a aloca resurse pentru găzduirea aplicațiilor IOx.

Configurați șablonul greu pentru planul de date

Procedură

Pasul 1 Introduceți comanda de configurare pentru a activa șablonul greu pentru planul de date:

Router(config)#platform resource data-plane-heavy

Pasul 2 Introduceți comanda de reîncărcare pentru a reporni routerul și a activa șablonul greu pentru planul de date:

Router#reîncărcare

Ce să faci în continuare

Verificați distribuția vCPU și RAM activă.

Verificați vCPU-ul activ și distribuția RAM

Utilizați**spectacol**comandă pentru a verifica alocarea nucleelor vCPU pentru aplicațiile IOx.

Router# arata platforma software alocarea CPU
Informații de alocare CPU:
Planul de control cpu alloc: 0-1 Plan de date cpu
alloc: 2-3 Plan de service cpu alloc:**0-1** Planul de
control lent cpu alloc: Șablon utilizat:**CLI-**
data_plane_heavy

Utilizați**spectacol**comandă pentru a verifica alocarea RAM pentru aplicațiile IOx.

Router#show app-host resource
Alocarea resurselor:
Cota procesor: 33%
Cotă de memorie:**2048 MB**
Stocare totală: 6350 MB
Stocare disponibilă: 1404 MB

Utilizați**spectacol**comandă pentru a verifica alocarea resurselor unităților CPU pentru aplicațiile IOx.

Router#show app-host infra
Versiunea IOX: 2.11.0.3
Verificarea semnăturii aplicației: dezactivată CAF
Health: Stabil
Director de lucru intern: /vol/harddisk/iox CPU:

Cota: 33%
Disponibil: 33%
Cota:**1617 (unități)**
Disponibil: 1617 (Unități)

Configurați șablonul pentru avionul de service

Procedură

Pasul 1 Introduceți comanda de configurare pentru a activa șablonul greu pentru planul de service:

Router(config)#platform resource service-plane-heavy

Pasul 2 Introduceți comanda de reîncărcare pentru a reporni routerul și pentru a activa șablonul greu pentru planul de service:

Router#reîncărcare

Ce să faci în continuare

Verificați distribuția vCPU și RAM activă.

Verificați vCPU-ul activ și distribuția RAM

Utilizați**spectacol**comandă pentru a verifica alocarea nucleelor vCPU pentru aplicațiile IOx.

Router# arata platforma software alocarea CPU
Informații de alocare CPU:
Planul de control cpu alloc: 0-1 Plan de date cpu
alloc: 3 Plan de service cpu alloc:**0-2** Șablon
folosit:**CLI-service_plane_heavy**

Utilizați**spectacol**comandă pentru a verifica alocarea RAM pentru aplicațiile IOx.

Router#show app-host resource
Alocarea resurselor:
Cota CPU: 38%
Cotă de memorie:**3072 MB**
Stocare totală: 6350 MB
Stocare disponibilă: 1403 MB

Utilizați**spectacol**comandă pentru a verifica alocarea resurselor unităților CPU pentru aplicațiile IOx.

Router#show app-host infra
Versiunea IOX: 2.11.0.3
Verificarea semnăturii aplicației: dezactivată CAF
Health: Stabil
Director de lucru intern: /vol/harddisk/iox CPU:

Cota: 38%
Disponibil: 38%
Cota:**1862 (unități)**
Disponibil: 1862 (Unități)

CAPITOL 16

Ghid de configurare a modulului de interfață conectabilă celulară

Capitolul Cisco 4G LTE-Configurație avansată a fost înlocuit cu un nou ghid autonom numit Ghid de configurare a modulului de interfață conectabilă celulară. Acest ghid conține informații actualizate despre toate aspectele utilizării Cisco Cellular PIM.

Important Modulul conectabil nu poate fi schimbat la cald. Routerul trebuie reîncărcat după ce este instalat un nou modul.

Suport pentru modulul conectabil P-5GS6-GL pe ESR6300

Suportul pentru modulul conectabil P-5GS6-GL funcționează la fel pe ESR6300 ca și pe celelalte routere IoT. Pentru detalii, veziModul de interfață conectabil 5G sub-6 GHzşiGhid de configurare a modulului de interfață conectabilă celulară.

Suport Galileo pentru modulele conectabile LTE

Cu Cisco IOS XE 17.11.1a și versiuni anterioare, singura constelație GNSS acceptată a fost GPS-ul. Această versiune introduce suport pentru Galileo.

Nota O singură constelație poate fi activată la un moment dat.

Există noi opțiuni CLI disponibile pentru a sprijini noua constelație:

Comenzi de configurare

config#**controler celular***<slot/port>*
(controller de configurare)#**<nu> lte gps constellation***<GPS | galileo | gnss >*

Exemplu:

(controller de configurare)#**constelație GPS lte?**
galileo selectați Galileo ca constelație activă selectați GPS ca
GPS constelație activă selectați mai multe GNSS ca constelație
gnss activă

Nota Setarea implicită este modul GPS.

Noile opțiuni galileo și gnss din CLI de mai sus sunt utilizate pentru a configura Galileo și, respectiv, GNSS Multiplu/Simultan (GPS + Galileo etc).

Dacă dezactivați configurația GPS, asigurați-vă că nu există nicio constelație configurată, în concordanță cu configurația modului GPS. De exemplu:

config#**controler Cellular 0/1/0** (controller de configurare)#**nu lte**
gps constellation gps

Afișați comenzi

Următorul exemplu arată constelația GNSS actuală ca Galileo:

#afișați detaliile GPS 0/1/0 celular
Caracteristica GPS = activată
Modul GPS configurat = autonom Constelație curentă
configurată = Port GPS selectat = Port GPS dedicatgalileo | GPS | gnss
Stare GPS = achiziție GPS

Orice modificare adusă configurației va necesita repornirea routerului.

Mai multe informații sunt disponibile înGhid de configurare a modulului de interfață conectabilă celulară.

Monitorizarea parametrilor semnalului radio și coordonatele GPS ale telemetriei celulare folosind mesaje Syslog

Prezentare generală a telemetriei celulare

Telemetria celulară permite monitorizarea și analiza în timp real a performanței conexiunii celulare prin jurnalele de sistem. Ajută la depanarea, optimizarea performanței rețelei și asigurarea unei conexiuni fiabile. Funcția de telemetrie celulară colectează parametrii de frecvență radio (RF) și coordonatele sistemului de poziționare globală (GPS) din rețeaua celulară și le afișează la un interval fix de 60 de secunde.

Parametrii de telemetrie celulară care pot fi monitorizați includ:

- Indicator de putere a semnalului primit (RSSI)
- Puterea recepționată a semnalului de referință (RSRP)
- Calitatea semnalului de referință recepționat (RSRQ)

- Identitatea fizică a celulei (PCI)
- Raport semnal/zgomot (SNR)
- Coordonatele sistemului de poziţionare globală (GPS).

Prescripţie

Cisco Catalyst WAN Manager nu acceptă telemetria celulară.

Activați telemetria celulară

Pentru a activa caracteristica de telemetrie celulară în interfața celulară controler 0/x/0 folosind CLI.

Înainte de a începe

- Introduceți modulul de interfață conectabil celular (PIM) în dispozitivul IR.
- Activați GPS în controler pentru ca coordonatele GPS să fie afișate în syslogs.

Procedură

Pasul 1 Intrați în modul de configurare globală.

Exemplu:

Router#**configura terminalul**

Pasul 2 Intrați în modul de configurare celulară.

Exemplu:

Router (configurație)#**controler celular 0/1/0**

Pasul 3 Activați parametrii RF și coordonatele GPS.

Exemplu:

Router (controller de configurare)#**parametrii de semnal de funcționare a modemului lte** Router (controller de configurare)#**Sfârşit**

Dezactivați telemetria celulară

Pentru a dezactiva caracteristica de telemetrie celulară, utilizați forma no a**parametrii de semnal de funcționare a modemului lte** comandă, așa cum se arată în exemplu:

Router#**Configurați terminalul** Router(config)#**controler celular 0/1/0** Router (config-controller) #**nu există parametri de semnal de funcționare a modemului lte** Router (config-controller) #**Sfârşit**

Monitorizați telemetria celulară

Pentru a vizualiza parametrii RF și coordonatele GPS pentru interfețele celulare, puteți utiliza fie**afișează înregistrarea**comanda sau verifica ieșirea consolei.

Următorul exemplu afișează parametrii RF și coordonatele GPS la fiecare interval de un minut:

```
Router#afișează înregistrarea
* 3 septembrie 17:08:42.081: %CELLWAN-2-MODEM_SIGNAL_PARAM: Cellular0/1/0: 4G: RSSI = -54 dBm RSRP = -76 dBm
  RSRQ = -9 dB PCI = 1 SNR = 27,4 dB
Latitudine =       12 grade 56 min 8,9260 sec nord 77 grade
Longitudine =      41 min 44,1641 sec est

* 3 septembrie 17:09:42.080: %CELLWAN-2-MODEM_SIGNAL_PARAM: Cellular0/1/0: 4G: RSSI = -54 dBm RSRP = -76 dBm
  RSRQ = -9 dB PCI = 1 SNR = 29,0 dB
Latitudine =       12 grade 56 min 8,8989 sec nord 77 grade
Longitudine =      41 min 44,1570 sec est
```

Următorul exemplu afișează numai parametrii RF și nu coordonatele GPS, deoarece GPS-ul nu este activat în controler:

```
Router#afișează înregistrarea
* 3 septembrie 17:08:42.081: %CELLWAN-2-MODEM_SIGNAL_PARAM: Cellular0/1/0: 4G: RSSI = -54 dBm RSRP = -76 dBm
  RSRQ = -9 dB PCI = 1 SNR = 27,4 dB

* 3 septembrie 17:09:42.080: %CELLWAN-2-MODEM_SIGNAL_PARAM: Cellular0/1/0: 4G: RSSI = -54 dBm RSRP = -76 dBm
  RSRQ = -9 dB PCI = 1 SNR = 29,0 dB
```

CAPITOL 17

Modulul de interfață Wi-Fi Cisco (WIM)

Acest capitol conține următoarele secțiuni:

Prezentare generală a modulului de interfață Wi-Fi Cisco (WIM).

Acest capitol al ghidului de configurare a fost transformat într-o carte de sine stătătoare numităGhid de configurare Cisco Wi-Fi Interface Module (WIM).pentru a oferi mai multe detalii despre configurarea WIM-ului.

Suport Cisco IoT Operations Dashboard (OD) pentru configurarea și gestionarea modulului WP-WIFI6-x

Cisco IOS XE versiunea 17.11.1a oferă capabilități suplimentare pentru Modulul de interfață Wi-Fi (WIM) Cisco.

Această secțiune conține următoarele:

CAPITOL 18

I/O digitală, aprindere și conectivitate magistrală CAN

Această secțiune conține următoarele:

Prezentare generală

Această secțiune acoperă configurația I/O digitale și detaliile CAN Bus.

IR1835 acceptă patru porturi de intrare/ieșire de uz general (GPIO), denumite și porturi I/O digitale. Un port GPIO poate fi configurat ca alarmă de intrare SAU de ieșire. Poate funcționa ca contact uscat sau umed, protejat până la + 60V.

Bus-ul Controller Area Network (CAN) permite ECU (unitatea de control electronică) dintr-un vehicul să comunice cu toate celelalte ECU. Este format din două fire, magistrală CAN High și Low, care acceptă o rată de date de până la 1 Mbs.

Caracteristicile CAN Bus 2.0B de mare viteză sunt stratul de legătură de date ISO 11898-1, stratul fizic ISO 11898-2 și ISO-11898-5 cu o rată de date de până la 1 Mbs (dependent de software).

IO digitală

Sunt acceptate un total de patru IO-uri digitale cu un randament comun. Digital IO este similar cu ALARM IN și ALARM OUT acceptate în comutatoarele IE și routerele IR. Diferențele sunt că ALARM IN este o intrare dedicată, ALARM OUT este o ieșire dedicată, în timp ce Digital IO poate fi de intrare sau de ieșire. ALARM OUT include un releu pentru a furniza bornele Normal deschis (NO) sau Normal închis (NC). Digital IO implementează o caracteristică de releu similară cu portul de alarmă.

Sunt disponibile următoarele comenzi de configurare:

contact de alarmă atașat la-iox contact de
alarmă <1-4> activare activare contact de
alarmă <1-4> aplicație contact de alarmă
<1-4> descriere contact de alarmă <1-4>
severitate
contact de alarmă <1-4> prag <1600-2700> contact de
alarmă <1-4> declanșare
contact de alarmă <1-4> ieșire <1 | 0>
contact de alarmă <1-4> releu de ieșire contact de alarmă
temperatură <1-4> releu de ieșire intrare-alarma <0-4>

Toate comenzile de configurare vin și cu a**nu**prefixul acestora.

Bus de rețea a rețelei de controler (CAN).

Detaliile despre busul CAN și conexiunea la diagnosticul de bord al vehiculului (OBD-II) sunt tratate în Ghid de instalare hardware al routerului Cisco Catalyst IR1800 Rugged Series.

Interfața CAN Bus poate fi vizualizată folosind interfața de linie de comandă. Unele dintre CLI sunt:

IR1800#**termenul conf**
Introduceți comenzile de configurare, una pe linie. Încheiați cu CNTL/Z.
IR1800(config)#**baudrate canbus?**
<125000-1000000> introduceți viteza baud între 125000 și 1000000

IR1800#**arată platforma hardware canbus?**
interfata Afișează interfața CAN Bus
legătură Afișează legătura CAN Bus

IR1800#**afișează link-ul canbus hardware al platformei**
8: can0: <NOARP,UP,LOWER_UP,ECHO> mtu 16 qdisc pfifo_fast state UP mode DEFAULT grup implicit qlen 10

link/poate promiscuitate 0
poate indica ERROR-ACTIVE restart-ms 100
rata de biți 125000 punct de eșantionare 0,875
tq 500 prop-seg 6 fază-seg1 7 fază-seg2 2 sjw 1 mcp251x: tseg1 3..16 tseg2 2..8
sjw 1..4 brp 1..64 brp-inc 1 ceas 10000000

repornit magistrală-erori arbit-pierdut eroare-avertizare eroare-pass magistrală-off
000000

numtxqueues 1 numrxqueues 1 gso_max_size 65536 gso_max_segs 65535

RX: octeți pachete erori eliminate depășire mcast 0
0 0000
TX: octeți pachete erori eliminate collsns de transportator 0
0 0000

```
IR1800#

IR1800#afișează interfața canbus hardware a platformei
can0      Link cap: UNSPEC        HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 MTU:16
          UP RUNNING NOARP        Metric:1
          Pachete RX:0 erori:0 scăpat:0 depășiri:0 cadru:0 Pachete TX:0 erori:0
          scăpat:0 depășiri:0 transportator:0 coliziuni:0 txqueuelen:10

          Octeți RX: 0 (0,0 B) Octeți TX: 0 (0,0 B)
```

Suport IOx CAN Bus

Un tunel vxcan este creat între Linux și IOx, iar apoi CAN_GW din interiorul linux este configurat pentru a redirecționa traficul CANBus de la/la interfața reală de magistrală (adică can0) la/de la punctul final al tunelului vxcan.

Un tunel vxcan este stabilit în mod implicit, traficul CANBus va fi trimis prin tunel după cum urmează:

CANBus: [Linux] vxcan-ap și vxcan0 [IOx]

Exemplu de ieșire de la vxcan0 [IOx]

```
vxcan0    Link cap: UNSPEC        HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 MTU:16
          UP RUNNING NOARP        Metric:1
          Pachete RX:715 erori:0 scăpat:0 depășiri:0 cadru:0 Pachete TX:530 erori:0
          scăpat:0 depășiri:0 transportator:0
```

Note importante

- Caracteristica poate suporta mai multe containere, o pereche de vxcan va fi configurată pentru un container, prin urmare, două perechi de vxcan vor fi configurate pentru două containere.
- Într-un singur container, dacă mai multe aplicații trebuie să acceseze vxcan, este responsabilitatea aplicației clientului să includă CAN_GW în software-ul lor.

Suport de captură de pachete pentru CANBUS

Când este activată, această caracteristică va capta pachetele trimise și primite pe CANBUS seria IR1800. Odată capturate, datele vor fi exportate ca fișier de captură de pachete (PCAP) pentru a permite o examinare ulterioară. Caracteristica este configurată în modul exec și este doar temporară, ceea ce înseamnă că nu este permanentă la o repornire/reîncărcare.

Pentru captură este necesar un nume de fișier. Locația implicită pentru fișierul de captură este la bootflash:/canbus_dumplogs. Dacă capturarea este pornită fără a specifica fișierul inițial sau după ce routerul este reîncărcat, veți primi următorul mesaj când verificați starea:

fișierul canbus packetdump calea pcapfile bootflash:/canbus_dumplogs/pcapfile nu a pornit

După oprirea capturii, dacă doriți să reporniți captura fără a specifica numele fișierului, vechiul nume specificat va fi suprascris.

Utilizați următoarea comandă pentru a specifica numele fișierului de captură:

Router#**monitorizați fișierul canbus packetdump***<nume de fișier>*

Nota Nu trebuie să specificați calea, singura cale acceptată este calea implicită**bootflash:/canbus_dumplogs**

Utilizați următoarea comandă pentru a porni captura folosind <filename> specificat din comanda de mai sus:

Router#**monitorizați pornirea packetdump canbus**

Utilizați următoarea comandă pentru a opri captura:

Router#**monitorizați oprirea packetdump canbus**

Utilizați următoarea comandă pentru a verifica starea monitorizării:

Router#**arată canbus packetdump**

Exemple de comenzi

Router#**monitorizați canbus packetdump?**
fișier CAN Bus interfață pachet de captură destinație pornire fișier CAN
Bus interfață CAN Packet capture start stop oprire CAN Bus interfață
pachet pachet oprire

Router#**monitorizați fișierul canbus packetdump canbusfile**
Router#**arată canbus packetdump**
fișierul canbus packetdump calea fișierului canbus bootflash:/canbus_dumplogs/canbusfile nu a pornit

Router#**monitorizați pornirea packetdump canbus**
Router#**arată canbus packetdump**
fișier canbus packetdump calea fișierului canbus bootflash:/canbus_dumplogs/canbusfile a început

Router#**monitorizați oprirea packetdump**
canbus Router#**arată canbus packetdump**
fișierul canbus packetdump calea fișierului canbus bootflash:/canbus_dumplogs/canbusfile nu a pornit

Configurarea IO digitală

Pentru a configura caracteristica, efectuați următoarele:

Router(config)#**activare contact de alarmă 2** Router(config)#**Ieșire implicită contact de alarmă 2** Router(config)#**severitatea contactului de alarmă implicit 2** Router(config)#**contact de alarmă implicit 2 prag** Router(config)#**declanșarea contactului de alarmă implicit 2** Router(config)#**aplicație de contact de alarmă implicită 2** Router(config)#**descrierea contactului de alarmă implicit 2** Router(config)#**Sfârşit**

Pentru a vizualiza ieșirea alarmei, efectuați următoarele:

Router#**arata alarma | secțiunea I/O digitală 2** I/O
digitală 2:
Descriere: Portul I/O digital extern 2 Stare: Neafirmat

Aplicare: uscat
Severitate: minoră
Declanșator: închis
Tensiune: 3300mV
Prag: 1600mV

Mod: Intrare
Router#

Privire de ansamblu asupra managementului puterii de aprindere

Această secțiune oferă o descriere și instrucțiuni pentru configurarea funcției Ignition Power Management a routerului IR1800. Ignition Power Management împiedică routerul să epuizeze încărcarea bateriei în aplicațiile auto. De asemenea, menține routerul în funcțiune în timp ce vehiculul este oprit. Prin urmare, utilizatorii nu trebuie să aștepte ca routerele să se reîncarce de fiecare dată când vehiculul este oprit.

Când motorul este pornit, generează energie și reîncarcă bateria. Când contactul este oprit, routerul poate rămâne operațional pentru o perioadă de timp predeterminată.

Pe seria IR1800, există două moduri de a efectua Ignition Power Management. Toate routerele din serie pot folosi senzorul de tensiune bazat pe software controlat de MCU. IR1835 poate folosi, de asemenea, semnalul de semnal/aprindere, disponibil de la pinul de aprindere din conectorul GPIO cu 6 pini.

Informațiile despre cablarea aprinderii se găsesc înGhid de instalare hardware.

Caracteristici ale managementului puterii de aprindere

Managementul puterii de aprindere este controlat prin MCU încorporat în router. MCU oferă detectarea automată a puterii de intrare pentru a detecta dacă contactul este pornit sau oprit. Aprinderea este detectată dacă semnalul de aprindere este pornit sau oprit sau prin detectarea nivelului de intrare a puterii.

Cablurile și conectorul de gestionare a puterii de aprindere sunt acoperite aici:https://www.cisco.com/c/en/us/td/docs/routers/access/IR1800/hig/b-ir1800-hig/m-GPIO.html

Software-ul de sistem încearcă să prevină descărcarea bateriei cu următoarele:

- Oprirea routerului dacă vehiculul are contactul oprit pentru o perioadă de timp (programabil).
- Oprirea routerului dacă tensiunea bateriei scade la un anumit nivel (programabil).
- Încercarea de a proteja routerul prin oprirea routerului dacă tensiunea bateriei crește peste un anumit nivel (perioada de timp fixă).

Software-ul de sistem înregistrează următoarele evenimente în jurnalul de sistem:

- Când utilizatorul pornește sau oprește funcția de gestionare a aprinderii cu CLI
- Când contactul este pornit sau oprit
- Când cronometrul de oprire a contactului expiră și sistemul se oprește
- Când utilizatorul activează sau dezactivează caracteristica prin CLI
- Înregistrează provizoriu evenimentele de subtensiune și supratensiune

Toate pragurile de intrare a aprinderii pornite, oprite, scăzute și ridicate pot fi stocate în memoria nevolatilă. Când dispozitivul pornește, pragurile vor fi preluate din memorie în registru. Când CPU detectează butonul de pe panoul frontal, memoria nevolatilă se va reseta la valoarea implicită.

Prezentare generală a sensului de aprindere

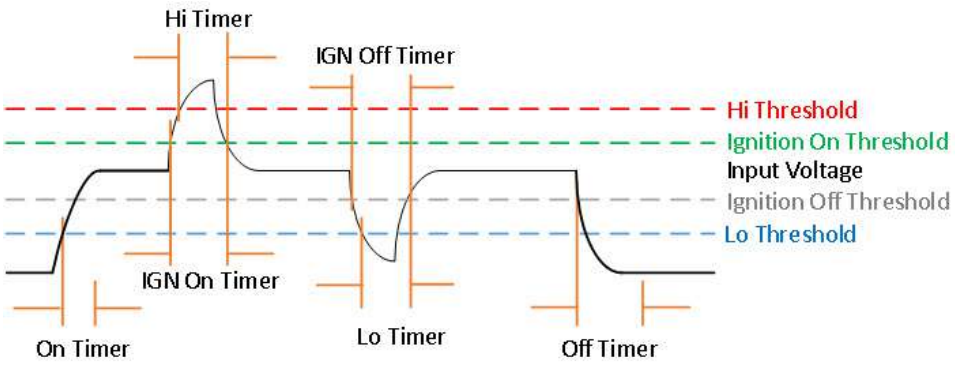
Pe IR1800, Ignition Power Management adaugă sensul de aprindere prin software. Sensul de aprindere poate fi determinat fie prin monitorizarea pinului semnalului de aprindere, fie a nivelului de tensiune a bateriei. Pinul de aprindere și nivelul tensiunii sunt monitorizate continuu. Această intrare va fi semnalul principal pentru pornirea mașinii de stare. Dacă semnalul de aprindere nu este activ, atunci va fi utilizat sensul nivelului de tensiune. Există o opțiune pentru utilizator de a dezactiva detectarea nivelului de tensiune prin ștergerea registrului de activare a senzorului de tensiune de aprindere.

Consultați următorul tabel:

Bypass de aprindere	Activare detecție tensiune aprindere	Sens de aprindere
0	0	Semnal de aprindere
0	1	Nivel de tensiune
1	x	Aprinderea dezactivată

Următorul grafic ilustrează Sensul aprinderii:

Figura 51: Aprindere în funcție de tensiune (intrare analogică)



Următoarele tabele oferă detalii despre tensiune:

Tabel 19: Tensiune de intrare (DC)

Minim	9,6 V
Maxim	36V
Nominal	12V sau 24V

Tabelul 20: Tensiunea de detectare a aprinderii

	Baterie 12V	Baterie 24V
Pe	13V + 2%	26V + 2%
Off	13V -2%	26V - 2%

Tabelul 21: Tensiunea bateriei

	Baterie 12V	Baterie 24V
Subtensiune	11,5 V	23V
Supratensiune	36V	36V

Vedeți următorul exemplu de ieșire a comenzii:

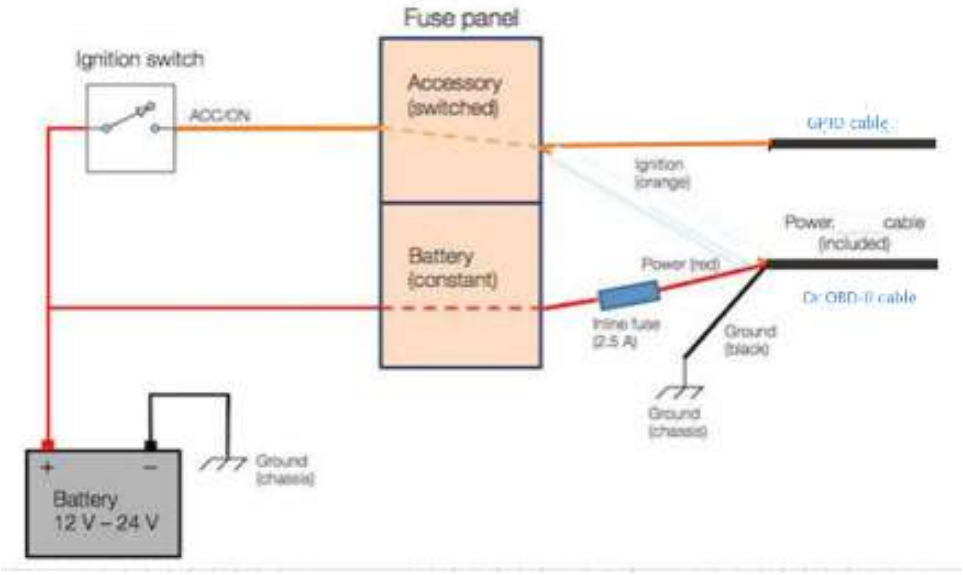
```
IR1800#show run | s aprindere
cronometru de oprire a contactului 300
prag de subtensiune de aprindere 9 000 aprindere
tip baterie 12v
sens de aprindere-prag de tensiune 13 000 sens de
aprindere
activare aprindere

IR1800#arată starea de aprindere
Stare:
   Gestionarea aprinderii: Activat
   Tensiune de intrare:          11.953 V
   Starea aprinderii:            Aprinderea sincronizată oprită oprită
   Sensul aprinderii:            Activată
   Temporizator de oprire:       242,0 s până la oprire [va începe oprirea la ~100 sec] 12v
   Baterie configurată:
Praguri:
   Subtensiune:                  9.000 V
   Supratensiune:                37.000 V
   Sentiment pe:                 13.000 V
   Sense off:                    12.800 V
   Temporizator de subtensiune:  20,0 s
   Temporizator de supratensiune: 1,0 s
   Temporizator aprindere-oprire: 300,0 s
```

IR1835 Comutator de aprindere

IR1835 este singurul model din seria IR1800 care oferă monitorizarea aprinderii prin semnalul Semnal/ Aprindere, disponibil din pinul de aprindere din conectorul GPIO cu 6 pini.

Consultați următoarea figură:

Figura 52: Aprindere bazată pe semnal/comutator de aprindere (intrare digitală)



Există două moduri de a alimenta routerul:

- Putere CANBUS
- Prin cablu CAB-PWR-15-MF4

Există două praguri:

- 12V — Setarea implicită a pragului de tensiune de detectare a aprinderii 13
- 24V — Setarea implicită a pragului de tensiune de detectare a aprinderii 26

Vedeți următorul exemplu de ieșire a comenzii:

IR1835#**show run | s aprindere***!Configurare* temporizator
de oprire a contactului 120
prag de subtensiune aprindere 9 600 aprindere tip
baterie 12v
sens de aprindere-prag de tensiune 13 000 fără sens
de aprindere
activare aprindere

IR1835#**arată starea aprinderii***!Monitorizare*
Gestionarea aprinderii: Activat Tensiune de intrare:
13.999 V
Starea aprinderii: Porniți
Sensul aprinderii: Dezactivat
Temporizator de oprire: 0,0 s până la oprire [va începe oprirea la ~100 sec] 12v
Baterie configurată:
Praguri:
Subtensiune: 9.600 V
Supratensiune: 37.000 V
Sentiment pe: 13.200 V
Sense off: 12.800 V
Temporizator de subtensiune: 20,0 s
Temporizator de supratensiune: 1,0 s
Temporizator aprindere-oprire: 120,0 s

IR1800 Tensiune de aprindere și baterie

IR1800 poate fi configurat cu o baterie de 12V sau 24V. Nivelul tensiunii de detectare a aprinderii se va modifica în consecință.

- Baterie de 12 volți
  - Dacă tensiunea de intrare > 13.200 V pentru mai mult de 1 secundă, aprinderea este**PE**
  - Dacă tensiunea de intrare < 12.800 V pentru mai mult de 20 de secunde, aprinderea este**OFF**
- Baterie de 24 volți
  - Dacă tensiunea de intrare > 26.200V pentru mai mult de 1 secundă, aprinderea este**PE**
  - Dacă tensiunea de intrare < 25.800V pentru mai mult de 20 de secunde, aprinderea este**OFF**

Utilizați următoarea comandă pentru a determina tipul bateriei dvs.:

IR1800#**termenul conf**
Introduceți comenzile de configurare, una pe linie. Încheiați cu CNTL/Z.
IR1800(config)#**tip baterie de aprindere?**
12v Bateria este 12v Bateria
24v este 24v

Interfață de linie de comandă (CLI)

Funcția de gestionare a puterii de aprindere a seriei IR1800 utilizează o interfață de linie de comandă.

Activarea managementului puterii la aprindere

Caracteristica este dezactivată implicit și activată folosind următoarea comandă:

Router(config)#**activare aprindere**
Router(config)#
* 15 septembrie 16:08:27.697: %IGNITION-5-IGN_ENABLE_CMD: Ignition Power Management este activat Router(config)#
Sfârşit

Opțiunile pentru comanda de activare a aprinderii sunt:

Router(config)#**activare aprindere?**
permite Activați funcția de gestionare a puterii la aprindere
temporizator de oprire Întârziere de oprire
sens Activați funcția de detectare a puterii de aprindere
subtensiune Setați parametrii de subtensiune pentru oprirea sistemului

- Valoarea temporizatorului de oprire a aprinderii. După ce contactul este oprit, routerul va rămâne operațional pentru această perioadă de timp, apoi se oprește dacă contactul este încă oprit:

Router#**cronometru de oprire a aprinderii <valoare>**

- Valoarea sensului de aprindere. Pornirea acestei funcții permite routerului să detecteze dacă contactul este pornit sau oprit.

Router(config)#**sensul de aprindere**
* 15 septembrie 16:08:14.391: %IGNITION-5-IGN_SENSE_CMD: Sensul tensiunii de aprindere este activat
Router(config)#**Sfârşit**

- Subtensiune la aprindere. Această comandă vă permite să setați parametrii pentru închiderea routerului.

Router(config)#**pragul de subtensiune la aprindere ?** <0-999>
Introduceți milivolți (mV), dacă există

- Prag de supratensiune. Această comandă vă permite să setați parametrii pentru închiderea routerului.

Router#**pragul de supratensiune la aprindere** *<valoare>*

Exemple de comenzi

Configurație implicită fără setări de gestionare a aprinderii:

Router#**arată aprinderea**
Stare:
Gestionarea aprinderii: Dezactivat
Tensiune de intrare: 17,672 V
Stare aprindere: Pornire Sens
aprindere: Dezactivat
Temporizator de oprire: 0,0 s până la oprire [va începe oprirea la ~100 sec] Baterie
configurată: 12v
Praguri:
Subtensiune: 9.000 V
Supratensiune: 37.000 V
Sens activat: 13,200 V Sens oprit:
12,800 V Temporizator subtensiune:
20,0 s Temporizator supratensiune:
1,0 s Temporizator aprindere-oprire:
300,0 s

Configurați managementul aprinderii:

Router(config)#**activare aprindere**
Router(config)#
* 15 septembrie 16:08:27.697: %IGNITION-5-IGN_ENABLE_CMD: Gestionarea puterii aprinderii este activată

Router(config)#**sensul de aprindere**
***** 15 septembrie 16:08:14.391: %IGNITION-5-IGN_SENSE_CMD: Sensul tensiunii de aprindere este activat
Router(config)#**Sfârşit**

Verificați modificările:

Router#**arată aprinderea**
Stare:
Gestionare aprindere: Activat
Tensiune de intrare: 17,656 V Stare
aprindere: Pornire Sens aprindere:
Activat
Temporizator de oprire: 0,0 s până la oprire [va începe oprirea la ~100 sec] Baterie
configurată: 12v
Praguri:
Subtensiune: 9.000 V
Supratensiune: 37.000 V
Sens activat: 13,200 V Sens oprit:
12,800 V Temporizator subtensiune:
20,0 s Temporizator supratensiune:
1,0 s Temporizator aprindere-oprire:
300,0 s Router#

Afișează starea aprinderii

Următoarele comenzi sunt utilizate pentru a afișa starea caracteristicii:

Router#**arată aprinderea**
Stare:

Gestionarea aprinderii: Dezactivat
Tensiune de intrare: 17,672 V
Stare aprindere: Pornire Sens
aprindere: Dezactivat
Temporizator de oprire: 0,0 s până la oprire [va începe oprirea la ~100 sec] Baterie
configurată: 12v
Praguri:
Subtensiune: 9.000 V
Supratensiune: 37.000 V
Sens activat: 13,200 V Sens oprit:
12,800 V Temporizator subtensiune:
20,0 s Temporizator supratensiune:
1,0 s Temporizator aprindere-oprire:
300,0 s

Router#**arată running-config | sec aprindere** cronometru
de oprire a contactului 300
prag de subtensiune de aprindere 9 000 aprindere
tip baterie 12v
sens de aprindere-prag de tensiune 13 000 fără sens
de aprindere
fara activare a aprinderii

Valori implicite

Următoarele setări implicite se aplică pentru gestionarea puterii de aprindere:

Setare	**Valoare implicită**
Funcția de gestionare a puterii aprinderii	Dezactivat
Sens de aprindere	Dezactivat
Temporizator de oprire	300 de secunde
Sub pragul de tensiune	9.000 volți
Temporizator oprire sub tensiune	20 de secunde
Temporizator de oprire la supratensiune	1,0 secunde
Sens de aprindere activat	13.200 volți (26.200 volți)
Sens aprindere oprit	12.800 volți (25.800 volți)
Baterie configurată	12 volți (24 volți)

Managementul puterii de aprindere Model Yang

Un model Yang este disponibil pentru modelul de configurare de gestionare a puterii de aprindere (model de configurare) și comanda de afișare a managementului puterii de aprindere (model de funcționare).

CLI-urile de configurare a aprinderii pentru modelul de configurare sunt după cum urmează:

- **[nu] activare aprindere**–Activați/dezactivați gestionarea puterii la aprindere.
- **temporizator de oprire a aprinderii** *<valoare>*–După ce contactul este oprit, routerul va rămâne operațional pentru această perioadă de timp, apoi se oprește dacă contactul este încă oprit.
- **[nu] sens de aprindere**– Activați/dezactivați sensul de tensiune
- **pragul de subtensiune la aprindere** *<valoare>*–Dacă tensiunea de intrare scade la niveluri sub acest prag, routerul se va opri.

Nodurile frunzelor pentru acest model sunt după cum urmează:

- activare
- temporizator de oprire
- simţ
- prag-valoare-volt
- valoare-prag-mili-volt

Un fișier model Yang, Cisco-IOS-XE-ignition.yang este disponibil pentru modelul de configurare.

CLI-urile pentru aprinderea pentru modelul oper sunt următoarele:

arată aprinderea–Afișează toți parametrii legați de aprindere

Un fișier model Yang, Cisco-IOS-XE-ignition-oper-transform.yang este disponibil în acest scop.

Suport SNMP MIB pentru managementul puterii de aprindere

Următorul este un exemplu de ieșire din**arată aprinderea**CLI:

```
Stare:
Gestionarea aprinderii: Dezactivat
Tensiune de intrare: 17,672 V
Stare aprindere: Pornire Sens
aprindere: Dezactivat
Temporizator de oprire: 0,0 s până la oprire [va începe oprirea la ~100 sec] Baterie
configurată: 12v
Praguri:
Subtensiune: 9.000 V
Supratensiune: 37.000 V
Sens activat: 13,200 V Sens oprit:
12,800 V Temporizator subtensiune:
20,0 s Temporizator supratensiune:
1,0 s Temporizator aprindere-oprire:
300,0 s
```

Un fișier MIB, CISCO-IGNITION-MIB.my, este disponibil pentru a sprijini**arată aprinderea**CLI.

Fișierul MIB are următoarele câmpuri:

- IgnitionManagement (1=adevărat; 2=fals, boolean)
- Tensiune de intrare (milivolt, întreg fără semn)
- Stare aprindere (încărcător/pornire/închidere la tensiune joasă sincronizare..., indice de stare)

- Bootloader (0)
- Pornire (1)
- Întârziere scăzută (2)
- Întârziere la oprire (3)
- Întârziere mare (4)
- La întârziere (5)
- Monitor (6)
- Somn (7)
- Necunoscut (8)

- IgnitionSense (1=adevărat; 2=fals, boolean)
- ShutdownTimer (milisecunde, întreg nesemnat)
- ConfigBattery (volți, Interger)
- Subtensiune (milivolt, întreg fără semn)
- Supratensiune (milivolt, întreg fără semn)
- SenseOn (milivolți, întreg fără semn)
- SenseOff (milivolți, întreg fără semn)
- UndervoltageTimer (milisecunde, întreg fără semn)
- OvervoltageTimer (milisecunde, întreg fără semn)
- IgnitionOffTimer (milisecunde, întreg fără semn)

CAPITOL 19

Configurarea GPS

Acest capitol conține următoarele:

Prezentare generală GPS

Există două moduri de a primi informații GPS. Există GPS modem celular disponibil în modulele LTE care acceptă GPS și există un modul dedicat GPS/Dead Reckoning (IRM-GNSS-ADR) care oferă capabilități mai robuste.

IR1833 și IR1835 au un slot pentru un modul dedicat de unitate de înlocuire pe teren (FRU) GPS, care va fi folosit în plus față de cel integrat în modulul LTE, pentru performanțe mai precise de calcul. Numărul piesei este IRM-GNSS-ADR.

Hardware-ul IRM-GNSS-ADR este capabil să suporte diverse constelații GNSS. Vă rugăm să întrebați reprezentantul dvs. de vânzări pentru o foaie de parcurs de suport pentru constelații suplimentare pe modulul IRM-GNSS-ADR.

GPS-ul bazat pe modem nu poate furniza coordonatele atunci când nu există sateliți în linia vizuală. Modulul GPS cu capabilități DR furnizează coordonatele chiar și atunci când nu există sateliți în linia de vedere.

Odată cu adăugarea modulului dedicat GPS/Dead Reckoning, împreună cu modulul Cellular, vor exista două surse de informații despre locația GPS. Acestea două sunt independente și pot fi preluate folosind CLI-uri diferite:

- Informațiile GPS ale modemului celular pot fi văzute utilizând**arată celular***<numărul slotului>***GPS**comanda.
- Modulul GPS/DR Informațiile GPS utilizează**afișează detaliile gps hardware ale platformei**comanda.

Următorul tabel oferă o comparație între GPS-ul bazat pe modem și GPS-ul bazat pe modulul GPS/Dead Reckoning.

Parametrii	**GPS bazat pe modem**	**Modul GPS/Dead Reckoning**
Tip	GPS bazat pe modem celular	GPS bazat pe FRU
PID-uri acceptate	Toate din seria IR1800	Doar pe IR1835 și IR1833
Moduri de configurare	Modul autonom	Nu este disponibilă nicio configurație pentru selectarea modurilor. Dispozitivul selectează automat fie independent | modul de calcul bazat pe recepția sateliților.
Numărul de sateliți necesari pentru coordonate	Modul autonom - 4	Dacă un semnal este primit de la 4 sau mai mulți sateliți, coordonatele GPS autonome vor furniza coordonatele, altfel calculul nedeterminat va furniza coordonatele GPS.
Sateliți acceptați în comanda show	Coordonatele văzute în afișarea comenzilor se bazează numai pe GPS.	Coordonatele văzute în rezultatul comenzilor show se bazează numai pe sateliți GPS. Cu toate acestea, traficul nmea va afișa GPS, Gallileo și Glonass.
Este necesară calibrarea inițială	Nu	Da
Coordonate în absența satelitului	Nicio coordonată nu va fi dobândită și rămâne în stare de achiziție.	Dispozitivul trece fără probleme în modul Dead-reckoning și oferă coordonate pe baza calculelor efectuate de FRU. FRU ia în considerare viteza vehiculului, direcția, ultimele coordonate achiziționate de la satelitul GPS, accelerometru și giroscop. Pentru ca neapărat să funcționeze, dispozitivul ar fi trebuit să obțină coordonatele cel puțin o dată înainte de pierderea semnalului de la satelit după pornirea routerului.
Numele dispozitivului controlerului de utilizat pentru configurare	**controler celular***<slot>*	**controler gps-dr**
CLI pentru a activa funcția	**activare lte gps** **modul lte GPS autonom** **Nota** Este necesar un ciclu de pornire a modemului după activarea configurației.	**activare dead-reckoning**
CLI pentru a configura nmea	**lte gps nmea**	nmea este activat automat odată ce „activarea dead-reckoning” este configurată

Parametrii	GPS bazat pe modem	Modul GPS/Dead Reckoning
CLI pentru a configura socketul nmea udp	**lte gps nmea ip udp** *<ip_sursă> <ip_destinație> <port_destinație>*	**dead-reckoning nmea udp** *<ip_sursă> <ip_destinație> <port_destinație>*
CLI pentru a verifica configurația sub show running-config	**show run | sec controller celular** *<slot>*	**show run | sec controller gps-dr**
Afișați comenzi pentru a verifica ieșirea GPS	**arată celular** *<slot>***GPS** **arată controlerul celular** *<slot>***|inc GPS**	**afișează detaliile gps hardware ale platformei** **afișează modul hardware al platformei GPS** **afișează starea GPS-ului hardware al platformei** **arătați platforma hardware gps neapărat**
Acces la traficul GPS nmea pe partea IOx	Sprijinit	Sprijinit
Comanda de depanare	**depanare celulară** *<slot>***mesaje gps** **depanare celulară** *<slot>***mesaje nmea**	**hardware-ul platformei de depanare gps_dr** *toate | dr | GPS | nmea*
Suport pentru modelul Yang	Da	Da

GPS bazat pe modem celular

GPS bazat pe modem celular este acoperit înGhid de configurare a modulului de interfață conectabilă celulară.

Modul GPS/Dead Reckoning (IRM-GNSS-ADR)

Această secțiune descrie caracteristica atunci când utilizați modulul GPS bazat pe GPS/Dead Reckoning.

Nota Calcul de socoteală GPS este disponibil numai pe modulul conectabil GPS.

Dead Reckoning GPS

Funcția de estimare prin GPS este acceptată pe SKU-urile 1835-K9 și 1833-K9.

Dead Reckoning Prezentare generală

Dead Reckoning este o funcție de rezervă GPS care oferă utilizatorilor informații despre locație în timpul întreruperii semnalului satelitului, calculând poziția curentă folosind o poziție determinată anterior și avansând acea poziție pe baza vitezelor cunoscute sau estimate în timpul și cursul scurs.

IR18xx 3D Automotive Dead Reckoning (3D ADR) oferă servicii GPS de calitate auto prin utilizarea algoritmilor inteligenți care combină datele de navigație prin satelit cu datele despre viteza roții, giroscopul și accelerometrul pentru a oferi o poziționare precisă, chiar și atunci când semnalele satelitului sunt blocate parțial sau complet.

Tranziția de la serviciul de localizare prin satelit la serviciul de localizare bazat pe date interne este transparentă și automată, bazată pe calitatea și prezența semnalelor satelitare.

Caracteristica este dezactivată în mod implicit și sunt furnizate CLI pentru a activa și configura această caracteristică. Activarea funcției activează automat GPS-ul, DR și magistrala CAN. Caracteristica arată starea, configurația și datele despre locație. Datele de locație sunt transmise în flux de la modulul GPS și vor fi redirecționate către aplicație prin priză.

Interfață de linie de comandă

Această secțiune oferă o descriere a diferitelor CLI utilizate cu Dead Reckoning GPS.

Comanda	Descriere
controler gps-dr	GPS-Dead Reckoning poate fi configurat sub comanda controler gps-dr.
activare dead-reckoning	Activează caracteristica GPS-DR.
nicio activare a calculului mort	Dezactivează funcția GPS-Dead Reckoning.
afișează detaliile gps hardware ale platformei	Afișează următoarea ieșire: • Caracteristica este activată/dezactivată • Coordonatele GPS • Marcaje temporale • Informații din satelit cu SNR
afișează starea GPS-ului hardware al platformei	Afișează dacă caracteristica este activată sau dezactivată și starea coordonatelor dacă sunt achiziționate sau în curs de achiziție.
arata platforma hardware gps mode	Afișează dacă funcția este activată sau dezactivată și dacă Dead Reckoning este în uz pentru remedierea locației sau nu.
arătați platforma hardware gps neapărat	Afișează următoarea ieșire: • Firmware care rulează pe modulul GPS • Număr de transmisii/recepții CAN • Citirea kilometrajului • Accelerometru • Citirile giroscopului • Dacă Dead Reckoning este utilizat sau nu pentru remedierea locației

Comanda	Descriere
hardware platformă de depanare gps_dr gps | nmea | dr	Activează jurnalele de depanare pentru GPS | NMEA | DR **Nota** Consola este inundată dacă jurnalele sunt activate. Configurați**fără consolă de logare** și apoi activați această comandă pentru a evita inundarea consolei. Apoi executați**arată jurnalul**pentru a vedea rezultatul. Efectua**depana toate**pentru a dezactiva depanarea. Asigurați-vă că activați înregistrarea pe consolă odată ce depanarea este dezactivată, dacă este necesar.

Comenzi de configurare

Pentru a activa funcția GPS Dead Reckoning, efectuați următoarele:

Router#**conf t**
Introduceți comenzile de configurare, una pe linie. Încheiați cu CNTL/Z.
Router(config)#**controler gps-dr**

Router (config-controller) #**activare dead-reckoning** Informații:
[]: Procesul DR a fost activat cu succes.

Pentru a dezactiva funcția GPS Dead Reckoning, efectuați următoarele:

Router#**conf t**
Introduceți comenzile de configurare, una pe linie. Încheiați cu CNTL/Z. Router(config)#
controler gps-dr Router (config-controller) #**nicio activare a calculului mort** Informații: []: caracteristica GPS/DR a fost dezactivată cu succes

Comenzi de depanare

Sunt disponibile următoarele comenzi de depanare:

Router#**hardware-ul platformei de depanare gps_dr ?**
toate GPS DR toate depanare
dr GPS DR dr depanare
GPS Depanare GPS DR GPS
nmea Depanare mesaje GPS NMEA

Afișați comenzi

Utilizați următoarele comenzi pentru a vizualiza starea modulului și detaliile GPS:

Router#**arata inventarul**
+ +
+ + + + INFORMAȚII: Utilizați „afișați licența UDI” pentru a obține numărul de serie pentru licențiere.
+ +
+ + + + + + + NUME: „Șasiu”, DESCRIERE: „Cisco Catalyst IR1835 Rugged Series IR1835 PID”89
, VID: V00 , SN: FHH2416P00W
NAME: „Modul de alimentare 0”, DESCR: „Sursă de alimentare CC Cisco IR1800” PID: PWR-12V
, VID: , SN:
NAME: „Modul GE-POE”, DESCR: „Modul POE pentru GE la bord pentru Cisco IR183X” PID: IR-183X-POE
, VID: , SN:
NAME: „modul 0”, DESCR: „Controler NIM Cisco IR-1835-K9 încorporat” PID: IR-1835-K9
, VID: , SN:
NAME: „NIM subslot 0/0”, DESCR: „Modul Gigabitethernet pe panoul frontal 1 port” PID: IR1835-1x1GE
, VID: V01 , SN:

NAME: „NIM subslot 0/1”, DESCR: „IR1835-ES-4” PID: IR1835-
ES-4 , VID: V01 , SN:
NAME: „modulul F0”, DESCR: „Procesor de redirecționare Cisco IR1835-K9” PID: IR1835-
K9 , VID: , SN:
**NAME: „Gps-Dr”, DESCR: „Modul GNSS/GPS/DR dedicat” PID: IRM-
GNSS , VID:V03, SN:FOC243645DJ**

Când coordonatele GPS sunt achiziționate de la satelit, următoarea este rezultatul din comenzile show:

Router#**afișează detaliile gps hardware ale platformei**
Caracteristica GPS = activat
Stare GPS = Coordonatele GPS achiziționate
Latitudine = 37 grade 25 min 4,7460 sec nord 121 grade
Longitudine = 55 min 11,1840 sec vest
Marca temporală (GMT) = Tue Nov 24 03:03:55 2020 0,
Fix tip index = Înălțime = 40 m
HDOP = 4.1, Modul GPS utilizat = GPS autonom
Informații satelit
- - - - - - - - - - - - - - - -
Satelitul #30, cota 72, azimut 43, SNR 0 Satelit #28, cota 68,
azimut 277, SNR 0 Satelit #7, cota 49, azimut 89, SNR 0 Satelit #13,
cota 37, azimut 30, cota 2 SNR 30, cota 2 azimut 185, SNR 25
Satelit #8, cota 21, azimut 43, SNR 0 Satelit #9, cota 15, azimut
160, SNR 17 Satelit #5, cota 11, azimut 260, SNR 26 Satelit #107,
cota SNR 160, altitudine #19, cota 7, azimut 194, SNR 24 Satelit
#1, cota 7, azimut 103, SNR 0 Satelit #15, cota 6, azimut 322, SNR
0 Router#show platform hardware gps dead-reckoning
==========

Informații despre furnizor GPS/DR: TELIT
Modul GPS/DR Versiune FW: V33-1.0.5-CLDR-4.7.10-N115R115-003291-3 Stare magistrală
CAN:
Contor CAN Bus Tx: 0
Contor CAN Bus Rx: 0
Număr CAN NULL Bus RX: 0 Număr CAN
Bus TX către DR: 0
Eroare CAN Bus TX la DR Număr: 0 DR
Sample TimeStamp în uz: 0 DR număr
odometru: 0
Stare inversă DR: 0
DR în uz pentru remedierea locației: Nu
durata de timp pentru pierderea liniei de vedere: distanța
călătoriei pentru pierderea liniei de vedere: eroare de
direcție la ieșire:
eroare de rotație la ieșire: eroare de câștig
al giroscopului de călătorie la ieșire:
eroare de poziție la ieșire:
raport de eroare de poziție la ieșire:
eroare de zgomot de poziție la ieșire:
date brute de accelerare în X: - 2360
Date brute de accelerare în 16130
Y: Date brute de accelerare 0
în Z: Date brute Gyro în X: 38
Date brute Gyro în Y: Date 0
brute Gyro în Z: Router# 0

Router#**afișează starea GPS-ului hardware al platformei**
Caracteristica GPS = activat
Stare GPS = Coordonatele GPS achiziționate

Router#

Router#**afișează modul hardware al platformei GPS**
Caracteristica GPS = activată
DR în uz pentru remedierea locației: fără
router#

Când antena nu poate primi un semnal satelit, va comuta în modul Dead Reckoning. În acest mod, numai ieșirea de la următoarele comenzi show se va schimba. Restul comenzilor de afișare a ieșirii rămâne același.

Router#**afișează modul hardware al platformei GPS**
Caracteristica GPS = activată
DR în uz pentru remedierea locației: da
Router#

Router#**afișează detaliile gps hardware ale platformei**
Caracteristica GPS = activat
Stare GPS = Coordonatele GPS achiziționate
Latitudine = 37 grade 25 min 4,7460 sec nord 121 grade
Longitudine = 55 min 11,1840 sec vest
Marca temporală (GMT) = Tue Nov 24 03:03:55 2020 0,
Fix tip index = Înălțime = 40 m
HDOP = 4,1,**Modul GPS utilizat = GPS bazat pe DR**

Informații prin satelit
- - - - - - - - - - - - - - - -
Satelitul #30, cota 72, azimut 43, SNR 0 Satelit #28, cota 68, azimut 277, SNR 0 Satelit #7, cota 49, azimut 89, SNR 0 Satelit #13, cota 37, azimut 30, cota 2 SNR 30, cota 2 azimut 185, SNR 12 Satelit #8, cota 21, azimut 43, SNR 0 Satelit #9, cota 15, azimut 160, SNR 14 Satelit #5, cota 11, azimut 260, SNR 10 Satelit #10, cota SNR 20, altitudine 160 #19, cota 7, azimut 194, SNR 8 Satelit #1, cota 7, azimut 103, SNR 0 Satelit #15, cota 6, azimut 322, SNR 0 Router#

Când GPS-Dead Reckoning este dezactivat, rezultatul comenzilor de afișare apare după cum urmează:

Router#**afișează detaliile gps hardware ale platformei**
Caracteristica GPS = **dezactivat**
Stare GPS = Modul GPS nu este activat

Router#**afișează modul hardware al platformei GPS**
Caracteristica GPS =**dezactivat**

Router#**afișează starea GPS-ului hardware al platformei**
Caracteristica GPS = **dezactivat**
Stare GPS = Modul GPS nu este activat

Router#**arătați platforma hardware gps neapărat**
========== Informații despre furnizorul GPS/DR:
Modul GPS/DR Versiune FW: CAN
Bus Stare:
Contor CAN Bus Tx: 0
Contor CAN Bus Rx: 0
Număr CAN NULL Bus RX: 0 Număr CAN
Bus TX către DR: 0
Număr de erori CAN Bus TX to DR: 0

DR Sample TimeStamp în uz: 0 DR număr
de odometru: 0
Stare inversă DR: 0
DR în uz pentru remedierea locației: Nu
durata de timp pentru pierderea liniei de vedere: distanța
călătoriei pentru pierderea liniei de vedere: eroare de
direcție la ieșire:
eroare de rotație la ieșire: eroare de câștig
al giroscopului de călătorie la ieșire:
eroare de poziție la ieșire:
raport de eroare de poziție la ieșire:
eroare de zgomot de poziție la ieșire:
date brute de accelerare în X: 0
Date brute de accelerație în Y: 0
Date brute de accelerație în Z: 0
Date brute de giroscop în X: 0
Date brute de giroscop în Y: 0
Date brute de giroscop în Z: 0

Limitări ale caracteristicilor

Următoarele sunt limitări ale caracteristicilor:

- Pentru a obține un marcaj temporal inițial, este necesar ca antena să primească un semnal de la satelit atunci când dispozitivul este pornit. Odată achiziționat, marcajul de timp va fi actualizat în fiecare secundă. În plus, pentru ca DR să afișeze coordonatele, este necesar ca antena să obțină coordonatele de la satelit cel puțin o dată după ce dispozitivul este pornit și DR este activat. Dacă dispozitivul a dobândit coordonate înainte de oprire și dispozitivul este pornit din nou mai târziu, dispozitivul poate încerca să afișeze coordonatele pe baza ultimei locații cunoscute.

- Cisco recomandă utilizarea acestei caracteristici numai dacă magistrala CAN al vehiculului este conectată la acest IR18xx. Conexiunea CAN Bus asigură calibrarea corectă a modulului GPS înainte ca caracteristica DR să fie complet funcțională, iar fixarea locației poate fi obținută chiar și fără linia vizuală a sateliților.

- Atâta timp cât sunt primite suficiente semnale de satelit, coordonatele vor fi achiziționate ca un modul GPS autonom, indiferent dacă este conectat la vehicul prin magistrala CAN sau nu. Cu toate acestea, dacă nu există semnale suficiente (sau deloc semnale), remedierea locației folosind DR va începe și va fi precisă numai dacă interfața sa CAN este conectată la vehicul prin magistrala CAN și primește toate datele necesare vehiculului.

- În cazul instalării inițiale a unui modul GPS pe teren, dacă magistrala CAN nu este conectată și nu este primit semnalul satelitului, coordonatele nu pot fi achiziționate.

- În cazul în care un modul GPS a obținut coordonatele anterior, dacă semnalul satelitului nu este primit, coordonatele vor fi achiziționate cu valoarea obținută anterior prin DR, indiferent dacă magistrala CAN nu este conectată sau nu. Precizia depinde de dacă locația a fost mutată sau nu de la ultima remediere a locației cu semnale de satelit.

Calibrarea modulului GPS DR IR1800

Modulul GPS DR IR1800 oferă caracteristica Automotive Dead Reckoning (ADR) care permite navigarea pe o platformă auto chiar și atunci când nu există un număr suficient de semnale satelit GPS disponibile. Acest lucru este foarte frecvent în aplicațiile IoT, cum ar fi în canioanele urbane, tunelurile subterane sau în orice zonă în care linia de vedere a sateliților este blocată.

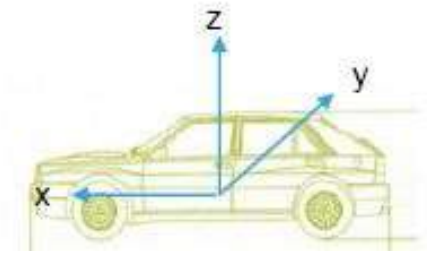
Pentru a oferi un astfel de serviciu în 3-D, modulul trebuie să utilizeze senzorii giroscopi și accelerometru cu trei axe încorporați ai chipset-ului pentru a obține date pentru schimbarea direcției, precum și orientarea și elevația chipset-ului.

În plus, pentru a oferi servicii de calitate auto, permite, de asemenea, introducerea datelor despre viteza și direcția vehiculului obținute direct din interfața magistrală CAN pe IR1800.

Pentru a permite modulului să interpreteze corect datele primite de la senzorii cu trei axe, este necesar să se furnizeze informațiile care descriu orientarea acestor senzori încorporați în raport cu vehiculul, astfel încât să se calibreze corect modulul, odată ce IR1800 este instalat în vehicul.

Cerințe de calibrare

Orientarea vehiculului este utilizată în calibrarea modulului ca referință de bază. Este aranjat așa cum este ilustrat în următorul grafic:



- Axa X: indică către direcția înainte a vehiculului
- Axa Y: indică spre partea dreaptă a vehiculului când privitorul privește înainte
- Axa Z: indică în sus în raport cu planul de mișcare al vehiculului.

Procesul de calibrare DR necesită obținerea informațiilor de orientare a senzorilor în raport cu această referință de bază. Orientarea implicită pentru acest modul, așa cum este utilizată de algoritmul DR este descrisă după cum urmează:

- IR1800 este instalat și fixat pe o bază stabilă. Panoul său frontal este orientat spre partea dreaptă a vehiculului, de exemplu, la 90 de grade în sensul acelor de ceasornic, față de direcția înainte a vehiculului. Panoul frontal este partea cu conectorul de alimentare și porturile ethernet.
- Cu orientarea implicită, nu este nevoie să introduceți date de orientare a senzorului în modul pentru calibrare. Datele implicite vor fi preluate de modul pentru întregul proces de calibrare.

Versiunea 17.6.1 nu acceptă calibrarea cu orientare care nu este implicită. Cisco va oferi o astfel de asistență dacă apar cerințe viitoare. Pentru moment, clienții trebuie să urmeze aceste instrucțiuni pentru orientarea implicită pentru calibrarea modulului.

Procesul de calibrare

Începeți cu routerul instalat așa cum este descris anterior și cu modulul GPS instalat. Configurați modulul din linia de comandă:

Procedură

Pasul 1 Acest pas este necesar numai dacă caracteristica DR nu este încă activată. În caz contrar, treceți direct la pasul 2.

Exemplu:

Router(config)#**controler gps** Router (config-controller) #**nicio activare a calculului mort**

Informații: []: Caracteristica GPS/DR a fost dezactivată cu succes Router(config-controller)#**Sfârşit**

Pasul 2 Activați caracteristica DR (ștergeți datele vechi de calibrare)

Exemplu:

Router#**conf t**
Introduceți comenzile de configurare, una pe linie. Încheiați cu CNTL/Z.
Router(config)#**controler gps** Router (config-controller) #**activare dead-reckoning** Informații: Procesul DR a fost activat cu succes.

Pasul 3 Setați viteza de transmisie a magistralei CAN. Vă rugăm să verificați manualul de utilizare al vehiculului pentru valoarea baudrate. De obicei, 500 kbps este cel mai frecvent, dar poate varia între diferiții producători de vehicule.

Exemplu:

Router (config-controller) #**Ieșire**
Router(config)#**baudrate canbus?**
<125000-1000000> introduceți rata baud între 125000 și 1000000 Router(config)#**baudrate canbus**<*baudrate a interfeței CAN/OBDII a vehiculului*>

Pasul 4 Reîncărcați sau porniți routerul și așteptați până când routerul termină repornirea.

Executarea calibrarii

De obicei, este nevoie de un vehicul care conduce pentru a calibra modulul DR. Acest proces este necesar o singură dată, atâta timp cât orientarea modulului în raport cu vehiculul nu este schimbată. Acest lucru este valabil atâta timp cât routerul sau modulul nu sunt niciodată repoziționați în interiorul acestui vehicul.

Urmați acești pași pentru calibrare:

Procedură

Pasul 1 Alegeți o locație în care există cer deschis pe parcursul întregului test pentru un semnal GPS bun. Calibrarea va necesita ca vehiculul să fie în mișcare.

Pasul 2 Așteptați aproximativ 2 minute într-o poziție oprită cu routerul și vehiculul pornite. Acest lucru permite modulului să inițializeze offset-ul ratei de rotire cu valori sigure.

Pasul 3 Conectați-vă în consolă și executați următoarea comandă pentru a vă asigura că locația GPS este obținută:

Exemplu:

Router#**afișează detaliile gps hardware ale platformei**
Caracteristica GPS = activat
Stare GPS = Coordonatele GPS achiziționate
Latitudine = 37 grade 25 min 5,8200 sec nord 121
Longitudine = grade 55 min 9,1020 sec vest
Marca temporală (GMT) = Mar 9 Mar 02:36:00 2021 0,
Fix tip index = Înălțime = 1 m
HDOP = 1.0, Modul GPS utilizat = GPS autonom
Informații satelit
- - - - - - - - - - - - - - - -
Satelitul #12, cota 70, azimut 147, SNR 22 Satelitul #25, cota 63, azimut 305, SNR 25

Satelitul #2, cota 51, azimut 43, SNR 23 Satelit #5, cota 41, azimut 139, SNR 20 Satelit #29, cota 33, azimut 294, SNR 26 Satelit #6, cota 13, azimut 1, cota 1, 46, cota SNR 1, 46 azimut 317, SNR 14 Satelit #24, cota 7, azimut 195, SNR 0 Satelit #18, cota 4, azimut 230, SNR 0 Satelit #82, cota 58, azimut 326, SNR 22 Satelit 5NR 22, cota 5NR 88, azimut 581, azimut Satelitul #79, cota 41, azimut 190, SNR 22 Satelit #81, cota 34, azimut 37, SNR 25 Satelit #83, cota 28, azimut 267, SNR 0 Satelit #66, cota 19, azimut # NR7, cota 3079 azimut 330, SNR 18 Satelit #67, cota 8, azimut 129, SNR 0 Satelit #65, cota 4, azimut 21, SNR 16

Pasul 4 După ce ați așteptat 2 minute, conduceți în linie dreaptă timp de cel puțin cinci minute la o viteză constantă. Viteza ar trebui să fie mai mare de 35 km/h (aproximativ 22 mph).

Pasul 5 Urmând conducerea în linie dreaptă, faceți mai multe viri la stânga și la dreapta de cel puțin 90 de grade, permițând sistemului să calculeze câștigul vitezei de rotație a giroscopului.

Important

Calibrarea va fi îmbunătățită cu mai multe ture finalizate. Se recomandă minim 10 ture. Calibrarea trebuie efectuată într-un mediu cu cer deschis. Evitați canioanele urbane, tunelurile, garajele de parcare, frunzișul dens etc.

Pasul 6 Pentru a finaliza calibrarea, vehiculul trebuie să se oprească și să rămână staționar timp de cel puțin 10 secunde. Pentru ca o calibrare completă să aibă succes, trebuie urmată procedura de mai sus.

Pasul 7 Utilizați următoarea comandă pentru a verifica dacă calibrarea este efectuată:

Exemplu:

Router#**arată platforma hardware gps mort**

========== Informații
despre furnizorul GPS/DR: TELIT
Modul GPS/DR Versiune FW: V33-1.0.5-CLDR-4.7.10-N115R115-003291-3 Stare calibrare
DR:
DR este calibrat
Odometrul este calibrat
Câștigul este calibrat
Offset-ul este calibrat
Stare magistrală CAN:
CAN Bus Tx Count: 6856 CAN Bus Tx Count: 0 CAN
Bus Rx Count: 12724 CAN NULL Pachete Bus RX
Count: 0 CAN Bus Rx neacceptat Packet Count: 0
CAN Bus TX to DR Count: 12601

Eroare CAN Bus TX la DR Număr: 123 Date
DR:
DR Sample TimeStamp în usec: 0
Contorul de parcurs DR primit de la modul: 54597690 Contorul de
parcurs DR trimis către modul: 54597697
Contorul de parcurs DR este valid de la modulul
Contorul de parcurs DR din modul: 220 Stare inversă
DR: 0

Pasul 8 Pentru a șterge calibrarea (în scopuri de testare), urmați pașii 1 și 2 din Procesul de calibrare.

Dead Reckoning pentru streaming de date GPS NMEA

Caracteristica de streaming de date NMEA permite utilizatorului să redirecționeze fluxurile NMEA prin Internet către orice dispozitiv care rulează o aplicație terță parte pentru serviciul de localizare GPS.

CLI-urile pentru socket-urile IPv4 UDP vor fi acceptate ca paritate de caracteristici cu funcționalitatea GPS existentă bazată pe modem 4G. În acest moment, nu este acceptat niciun suport pentru portul IPv6 UDP pentru fluxul de date NMEA în modemul GPS existent 4G.

Interfață de linie de comandă

(controller de configurare)#**dead-reckoning nmea ?**
interfață ip NMEA peste IP

Router (config-controller) #**dead-reckoning nmea udp ?**
ABCD Adresă sursă

(controller de configurare)#**dead-reckoning nmea udp 10.3.4.5 ?**
ABCD Adresă de destinație

(controller de configurare)#**dead-reckoning nmea udp 10.1.1.1 10.3.4.5 ?**
Port de destinație

(controller de configurare)#**dead-reckoning nmea udp 10.1.1.1 10.3.4.5 3456**

Suport GPS și Dead Reckoning pentru conectorul J1939

Automotive Dead-Reckoning (DR) se referă la capacitatea unui receptor GNSS de a continua să navigheze pe o platformă auto atunci când există un număr insuficient de semnale de satelit GNSS disponibile. Pentru a face acest lucru, receptorul folosește informațiile furnizate de senzori externi privind starea vehiculului pentru a propaga soluția de navigație.

Automotive DR necesită informații cu privire la schimbarea direcției de direcție a vehiculului, care sunt furnizate de un giroscop digital cu trei axe. Automotive DR necesită, de asemenea, informații despre viteza și direcția vehiculului. Viteza este furnizată de un contor de kilometraj (ticul roții), care este introdus în modulul conectabil IRM-GNSS-ADR.

Caracteristica DR auto acceptă și date de la un accelerometru digital cu trei axe, care oferă informații care pot fi utilizate pentru a determina orientarea giroscopului atunci când este instalat la un unghi de înclinare. Aceste informații sunt folosite și pentru estimarea altitudinii. Accelerometrul este integrat în senzorul inclus în modulul conectabil.

Înainte de lansarea 17.9.1, era disponibil doar modul obdii. În 17.9.1, modul j1939 este adăugat cu modul implicit obdii existent.

Conectorul J1939 este acceptat pe camioanele grele, care furnizează date despre viteză și starea inversă pentru a fi introduse în modulul GPS/DR folosind protocolul J1939. Este configurat prin interfața de linie de comandă sub controler.

Configurare

Următoarele CLI sunt disponibile.

Pentru a arăta ceea ce este disponibil pentru estimare:

Router (config-controller) #**socoteala?** enable enable
enable GPS feature mode DR mode configuration nmea
NMEA Configuration

Pentru a configura modul j1939:

Router(config)#**controler GPS-Dr** Router (config-controller) #**modul
de estimare j1939**

Pentru a vedea starea:

Router#**arătați platforma hardware gps neapărat**
============================== DR Mod interfață vehicul:
J1939 GPS/DR Informații furnizor: TELIT

Modul GPS/DR Versiune FW: V33-1.0.5-CLDR-4.7.10-N115R115-003291-3 Stare calibrare
DR:
DR nu este calibrat Odometrul nu
este calibrat Câștigul nu este
calibrat Offset-ul nu este calibrat

Stare magistrală CAN:
CAN Bus Tx Count: 1874 CAN Bus
Tx Count: 0

Număr de recepții CAN Bus: 571
Număr RX de pachete CAN NULL: 0
Număr de pachete neacceptate CAN Bus Rx: 448

CAN Bus TX to DR Count: 123 CAN Bus TX
to DR Count: 0

Date DR:
DR Sample TimeStamp în usec: 0
Contorul de parcurs DR primit de la modul: 0 Contorul
de parcurs DR trimis către modul: 1353 Contorul de
parcurs DR nu este valid de la modul
Număr delta contorului DR de la modul: 0 Stare
inversă DR: 0

DR în uz pentru remedierea locației: Nu
durata de timp pentru pierderea liniei de vedere: distanța
călătoriei pentru pierderea liniei de vedere: eroare de
direcție la ieșire:
eroare de rotație la ieșire: eroare de câștig
al giroscopului de călătorie la ieșire:
eroare de poziție la ieșire:
Raport de eroare de poziție la ieșire:
eroare de zgomot de poziție la ieșire:
Date brute de accelerare în X: 0
Date brute de accelerare în Y: 0 Date
brute de accelerație în Z: 0 Date brute
pentru giroscop în X: 0 Date brute
pentru giroscop în Y: 0 Date brute
pentru giroscop în Z: 0

Suport IOx al Asociației Naționale de Electronică Marină (NMEA).

Din linux sau containerul IOx, următorul tty este disponibil pentru traficul NMEA:

- /dev/ttyTun9
- /dev/ttyS2

Suport socket NMEA UDP

Pentru a configura suportul pentru socket NMEA UDP, trebuie să activați mai întâi caracteristica de dead reckoning, apoi să configurați suportul pentru socket NMEA UDP. Pentru a dezactiva suportul pentru socket NMEA UDP, trebuie să dezactivați mai întâi suportul pentru socket NMEA UDP, apoi să dezactivați caracteristica de dead reckoning.

Vezi următoarele exemple.

Activați caracteristica

GPS-ul este dezactivat:

Router#**afișează detaliile gps hardware ale platformei**
Caracteristica GPS = dezactivat
Stare GPS = Modul GPS nu este activat

Router#**afișează starea GPS-ului hardware al platformei**
Caracteristica GPS = dezactivat
Stare GPS = Modul GPS nu este activat

Router#**afișează modul hardware al platformei GPS**
Caracteristica GPS = dezactivată

Router#**arătați platforma hardware gps neapărat**
========== Informații despre furnizorul
GPS/DR:
Modul GPS/DR Versiune FW: DR
Stare Calibrare:
DR nu este calibrat Odometrul nu
este calibrat Câștigul nu este
calibrat Offset-ul nu este calibrat

Stare magistrală CAN:
Număr CAN Bus Tx: 0 Număr de
erori CAN Bus Tx: 0

Contor CAN Bus Rx: 0
Număr de pachete CAN NULL Bus RX: 0 CAN Bus Rx
Număr de pachete neacceptate: 0

Număr de erori CAN Bus TX către DR: 0
Număr de erori CAN Bus TX către DR: 0

Date DR:
DR Sample TimeStamp în usec: 0
Numărul contorului DR primit de la modul: 0 Numărul
contorului DR trimis către modul: 0
Contorul DR nu este valid din modul

Număr delta contorului DR de la modul: 0 Stare inversă DR: 0
DR în uz pentru remedierea locației: Nu
durata de timp pentru pierderea liniei de vedere: distanța călătoriei pentru pierderea liniei de vedere: eroare de direcție la ieșire:
eroare de rotație la ieșire: eroare de câștig al giroscopului de călătorie la ieșire:
eroare de poziție la ieșire:
raport de eroare de poziție la ieșire:
eroare de zgomot de poziție la ieșire:
date brute de accelerare în X: 0
Date brute de accelerație în Y: 0
Date brute de accelerație în Z: 0
Date brute de giroscop în X: 0
Date brute de giroscop în Y: 0
Date brute de giroscop în Z: 0

Configurați Dead Reckoning GPS:

Router#**termenul de configurare**
Introduceți comenzile de configurare, una pe linie. Încheiați cu CNTL/Z.

Router(config)#**controler GPS-Dr**

Router (config-controller) #**activare dead-reckoning** Informații:
Procesul DR a fost activat cu succes.

Configurați Dead Reckoning NMEA UDP:

Router (config-controller) #**dead-reckoning nmea udp 192.0.2.163 192.0.2.240 11111** Conectarea soclului NMEA UDP cu succes.

Router (config-controller) #**Sfârşit**

Verificați starea:

Router#**show run | sec controller Gps-Dr** controler
GPS-Dr
activare dead-reckoning
dead-reckoning nmea udp 192.0.2.163 192.0.2.240 11111 Router#show platform hardware gps detail
Funcția GPS = soclul NMEA UDP
activat este în uz
Starea operațională a soclului NMEA UDP: stare GPS
activă = achizitie GPS
Latitudine = 0 Grad 0 Min 0 Sec Nord 0 Grad
Longitudine = 0 Min 0 Sec Est
Marca temporală (GMT) = Duminica 6 ianuarie 00:00:00 1980

Index de tip fix = 0
HDOP = , Modul GPS utilizat = neconfigurat

Informații prin satelit
- - - - - - - - - - - - - - - -

Router#**afișează starea GPS-ului hardware al platformei** Funcția GPS = soclul NMEA UDP activat
este în uz
Stare operațională a soclului NMEA UDP: stare GPS activă = achiziție GPS

Router#**afișează modul hardware al platformei GPS**
Caracteristica GPS = activată
DR în uz pentru remedierea locației: Nu

Router#**arătați platforma hardware gps neapărat**
========== Informații despre furnizorul
GPS/DR:
Modul GPS/DR Versiune FW: DR
Stare Calibrare:
DR nu este calibrat Odometrul nu
este calibrat Câștigul nu este
calibrat Offset-ul nu este calibrat

Stare magistrală CAN:
Număr CAN Bus Tx: 135 Număr de
erori CAN Bus Tx: 0

Contor CAN Bus Rx: 0
Număr de pachete CAN NULL Bus RX: 0 CAN Bus Rx
Număr de pachete neacceptate: 0

Număr de erori CAN Bus TX către DR: 0
Număr de erori CAN Bus TX către DR: 0

Date DR:
DR Sample TimeStamp în usec: 0
Numărul contorului DR primit de la modul: 0 Numărul
contorului DR trimis către modul: 0
Contorul de parcurs DR nu este valid de la modul
Contor de contor de kilometraj DR din modul: 0
Stare inversă DR: 0

DR în uz pentru remedierea locației: Nu
durata de timp pentru pierderea liniei de vedere: distanța
călătoriei pentru pierderea liniei de vedere: eroare de
direcție la ieșire:
eroare de rotație la ieșire: eroare de câștig
al giroscopului de călătorie la ieșire:
eroare de poziție la ieșire:
raport de eroare de poziție la ieșire:
eroare de zgomot de poziție la ieșire:
date brute de accelerare în X: 0
Date brute de accelerație în Y: 0
Date brute de accelerație în Z: 0
Date brute de giroscop în X: 0
Date brute de giroscop în Y: 0
Date brute de giroscop în Z: 0

Dezactivați caracteristica

Inversați procedura pentru a dezactiva suportul NMEA UDP. Vedeți următoarele exemple:

Router#**termenul de configurare**
Introduceți comenzile de configurare, una pe linie. Încheiați cu CNTL/Z.

Router(config)#**controler GPS-Dr**

Router (config-controller) #**fără dead-reckoning nmea udp 192.0.2.163 192.0.2.240 11111** Socketul NMEA UDP a fost dezactivat cu succes.

Router (config-controller) #**nicio activare a calculului mort**
Informații: caracteristica GPS/DR a fost dezactivată cu succes

Router (config-controller) #**Sfârşit**

Verificați starea:

Router#**afișează detaliile gps hardware ale platformei**
Caracteristica GPS = dezactivat
Stare GPS = Modul GPS nu este activat

Router#**afișează starea GPS-ului hardware al platformei**
Caracteristica GPS = dezactivat
Stare GPS = Modul GPS nu este activat

Router#**afișează modul hardware al platformei GPS**
Caracteristica GPS = Router dezactivat#

Router#**arătați platforma hardware gps neapărat**
========== Informații despre furnizorul GPS/DR:
Modul GPS/DR Versiune FW: DR
Stare Calibrare:
DR nu este calibrat Odometrul nu este calibrat Câștigul nu este calibrat Offset-ul nu este calibrat

Stare magistrală CAN:
Număr CAN Bus Tx: 0 Număr de erori CAN Bus Tx: 0

Contor CAN Bus Rx: 0
Număr de pachete CAN NULL Bus RX: 0 CAN Bus Rx
Număr de pachete neacceptate: 0

Număr de erori CAN Bus TX către DR: 0
Număr de erori CAN Bus TX către DR: 0

Date DR:
DR Sample TimeStamp în usec: 0
Numărul contorului DR primit de la modul: 0 Numărul contorului DR trimis către modul: 0
Contorul de parcurs DR nu este valid de la modul
Contor de contor de kilometraj DR din modul: 0
Stare inversă DR: 0

DR în uz pentru remedierea locației: Nu
durata de timp pentru pierderea liniei de vedere: distanța călătoriei pentru pierderea liniei de vedere: eroare de direcție la ieșire:
eroare de rotație la ieșire: eroare de câștig al giroscopului de călătorie la ieșire:
eroare de poziție la ieșire:
raport de eroare de poziție la ieșire:
eroare de zgomot de poziție la ieșire:
date brute de accelerare în X: 0
Date brute de accelerare în Y: Date brute de accelerare în Z: Date brute Gyro în X: 0
Date brute Gyro în Y: Date brute Gyro în Z: Router# 0

Configurație NMEA UDP cu Yang

Modelul Yang poate fi folosit pentru a activa caracteristica în același mod ca și linia de comandă. Se aplică aceleași reguli:

Pentru a configura suportul pentru socket NMEA UDP, trebuie să activați mai întâi caracteristica de dead reckoning, apoi să configurați suportul pentru socket NMEA UDP. Pentru a dezactiva suportul pentru socket NMEA UDP, trebuie să dezactivați mai întâi suportul pentru socket NMEA UDP, apoi să dezactivați caracteristica de dead reckoning.

Activați Dead Reckoning:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
   <edit-config>
      <țintă>
         <alergare/>
      </target>
      <config>
         <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
            <controller>
               <Gps-Dr xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-controller">
                  <la socoteală>
                     <activare/>
                  </dead-calcul>
               </Gps-Dr>
            </controller>
         </nativ>
      </config>
   </edit-config>
</rpc>
```

Activați soclul UDP:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
   <edit-config>
      <țintă>
         <alergare/>
      </target>
      <config>
         <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
            <controller>
               <Gps-Dr xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-controller">
                  <la socoteală>
                     <nmea>
                        <udp>
                           <source-address>172.27.169.162</source-address> <destination-
                           address>172.27.169.140</destination-address> <destination-port>11111</
                           destination-port>
                        </udp>
                     </nmea>
                  </dead-calcul>
               </Gps-Dr>
            </controller>
         </nativ>
      </config>
   </edit-config>
</rpc>
```

Obține stare:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
   <obține>
```

```
      <filtru>
         <gnss-dr-oper-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-gnss-dr-oper">
            <gnss-dr-data/>
         </gnss-dr-oper-data>
      </filter>
   </get>
</rpc>
```

Ștergeți soclul UDP:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
   <edit-config>
      <țintă>
         <alergare/>
      </target>
      <config>
         <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
            <controller>
               <Gps-Dr xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-controller">
                  <la socotealã>
                     <nmea>
                     <udp xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0" nc:operation="delete">

                           <source-address>172.27.169.162</source-address> <destination-
                           address>172.27.169.240</destination-address> <destination-port>11111</
                           destination-port>
                        </udp>
                     </nmea>
                  </dead-calcul>
               </Gps-Dr>
            </controller>
         </nativ>
      </config>
   </edit-config>
</rpc>
```

Ștergeți configurația Dead Reckoning:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
   <edit-config>
      <țintă>
         <alergare/>
      </target>
      <config>
         <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
            <controller>
               <Gps-Dr xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-controller">
                  <la socotealã>
                     <enable xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
nc:operation="delete"/>
                  </dead-calcul>
               </Gps-Dr>
            </controller>
         </nativ>
      </config>
   </edit-config>
</rpc>
```

Suport pentru modelul de date Yang

Modelul yang de controler este prezent sub controlerul Cisco-IOS-XE - Cisco-IOS-XE-native:

Următorul este un exemplu XML pentru a activa funcția GPS-Dead Reckoning:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
    <edit-config>
        <țintă>
            <alergare/>
        </target>
        <config>
            <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
                <controller>
                    <Gps-Dr xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-controller">
                        <la socotealã>
                            <activare/>
                        </dead-calcul>
                    </Gps-Dr>
                </controller>
            </nativ>
        </config>
    </edit-config>
</rpc>
```

Următorul este un exemplu XML pentru a dezactiva caracteristica GPS-Dead Reckoning:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
    <edit-config>
        <țintă>
            <alergare/>
        </target>
        <config>
            <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
                <controller>
                    <Gps-Dr xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-controller">
                        <la socotealã>
                            <enable xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
nc:operation="delete"/>
                        </dead-calcul>
                    </Gps-Dr>
                </controller>
            </nativ>
        </config>
    </edit-config>
</rpc>
```

Comenzile operaționale GPS-Dead Reckoning sunt prezente sub modelul Cisco-IOS-XE-gnss-dr-oper:

Următorul este un exemplu de XML pentru modelul de comandă opera yang al GPS-Dead Reckoning:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <obține>
    <filtru>
      <gnss-dr-oper-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-gnss-dr-oper">
        <gnss-dr-data/>
      </gnss-dr-oper-data>
    </filter>
  </get>
</rpc>
```

Suportul pentru datele operaționale și de configurare YANG va fi furnizat și pentru CLI-urile menționate anterior.

Modelul YANG va permite utilizatorului să configureze priza UDP (adresă IP, portul UDP etc, sub controlerul XE), precum și să afișeze starea operațională a acestei caracteristici (sub XE-gnss-dr-oper), prin intermediul aplicației software YANG.

Exemplu: Conectarea la un server care găzduiește o aplicație GPS

Puteți transmite datele NMEA unui server la distanță care găzduiește aplicația GPS. Serverul poate fi conectat la router fie direct folosind un cablu Ethernet, fie printr-o rețea LAN sau WAN. Dacă aplicația acceptă portul serial, rulați un program de emulare a portului serial pentru a crea un port serial virtual prin conexiunea LAN sau WAN.

Nota Microsoft Streets & Trips este un software licențiat pe care îl puteți descărca de pe site-ul web Microsoft.

Pentru a conecta un Cisco 4G LTE-Advanced prin IP la un PC care rulează Microsoft Streets & Trips, parcurgeți următorii pași:

1.Conectați computerul la router folosind un cablu Ethernet.

2.asigurați-vă că computerul și routerul pot face ping.

3.Lansați redirectorul portului serial pe computer.

4.Creați un port serial virtual care se conectează la portul NMEA de pe router.

5.Lansa**Microsoft Streets & Trips**pe computerul dvs.

6.Selectați meniul GPS.

7.Faceți clic pe Începeți urmărirea.

8.Dacă ați obținut o remediere a locației de la**afișează gps-ul celular 0/3/0**ieșirea comenzii pe router, locația curentă este reprezentată pe grafic și pe hartă se vede un cursor cu puncte maro roșiatic cu un cerc în jurul său.

Nota Dacă nu ați obținut o remediere a locației, aplicația Microsoft expiră și se deconectează.

Suport GNSS pe modulul GPS/Dead Reckoning (IRM-GNSS-ADR)

Înainte de lansarea Cisco IOS XE 17.11.1a, singura constelație GNSS acceptată era GPS. Această versiune introduce suport pentru GPS și Galileo.

Nota O singură constelație poate fi activată la un moment dat.

Există noi opțiuni CLI disponibile pentru a sprijini noua constelație:

Comenzi de configurare:

(controller de configurare)#**controler gps**
<nu> constelație de nerăbdare <gps | galileo |gnss >

Nota Setarea implicită este modul GPS. Noile opțiuni galileo și gnss din exemplul CLI de mai sus sunt utilizate pentru a configura Galileo și, respectiv, GNSS Multiplu/Simultan (GPS + Galileo etc).

Afișați comenzi

afișează GPS-ul hardware al platformei*<modul | stare | detalii>*
. . . .
Constelația curentă configurată = gps | galileo | gnss . . . .

Orice modificare adusă configurației va necesita repornirea routerului.

Mai multe informații sunt disponibile înConfigurarea GPScapitolul Ghidului de configurare software IR1800.

Suport Galileo pentru modulele conectabile LTE

Cu Cisco IOS XE 17.11.1a și versiuni anterioare, singura constelație GNSS acceptată a fost GPS-ul. Această versiune introduce suport pentru Galileo.

Nota O singură constelație poate fi activată la un moment dat.

Există noi opțiuni CLI disponibile pentru a sprijini noua constelație:

Comenzi de configurare

config#**controler celular** *<slot/port>*
(controller de configurare)#**<nu> lte gps constellation** *<GPS | galileo | gnss >*

Exemplu:

(controller de configurare)#**constelație GPS lte?**
galileo selectați Galileo ca constelație activă selectați GPS ca
GPS constelație activă selectați mai multe GNSS ca constelație
gnss activă

Nota Setarea implicită este modul GPS.

Noile opțiuni galileo și gnss din CLI de mai sus sunt utilizate pentru a configura Galileo și, respectiv, GNSS Multiplu/Simultan (GPS + Galileo etc).

Dacă dezactivați configurația GPS, asigurați-vă că nu există nicio constelație configurată, în concordanță cu configurația modului GPS. De exemplu:

config#**controler Cellular 0/1/0** (controller de configurare)#**nu lte**
gps constellation gps

Afișați comenzi

Următorul exemplu arată constelația GNSS actuală ca Galileo:

#afișați detaliile GPS 0/1/0 celular
Caracteristica GPS = activată
Modul GPS configurat = autonom Constelație curentă
configurată = Port GPS selectat = Port GPS dedicatgalileo | GPS | gnss
Stare GPS = achiziție GPS

Orice modificare adusă configurației va necesita repornirea routerului.

Mai multe informații sunt disponibile înGhid de configurare a modulului de interfață conectabilă celulară.

Accesați datele despre accelerometru și senzorul giroscop de la IRM-GNSS

Această caracteristică permite transmiterea în flux a datelor accelerometrului și senzorului giroscop din modulul IRM-GNSS (GPS DR) către IOX printr-un TTY în IR1800. Înainte de această lansare, modulul IRM-GNSS a împins datele senzorului către gazdă în NMEA prin portul /dev/ttyS2. Versiunile anterioare de IOS XE au analizat și stocat deja în cache datele.

Caracteristica va transmite datele senzorului către IOX prin TTY ori de câte ori datele sunt primite de la NMEA. În prezent, nu există control asupra frecvenței în care datele sunt trimise de la modul, care se bazează în totalitate pe modulul în sine.

Nu există comenzi noi pentru această caracteristică. Este activat în mod prestabilit odată ce este activată dead reckoning. CLI-urile existente pot fi utilizate pentru a vizualiza datele senzorului, de exemplu:

Router#**arătați platforma hardware gps neapărat**

DR Mod interfață vehicul: OBDDII GPS/DR
Informații furnizor: TELIT
Modul GPS/DR Versiune FW: V33-1.0.5-CLDR-4.7.10-N115R115-003291-3 ...

Date brute de accelerare în X: - 542
date brute de accelerare în Y: 538
date brute de accelerare în Z: 16964
date brute de giroscop în X: 153
date brute de giroscop în Y: - 80
date brute de giroscop în Z: 99

Cele existente**platforma de depanare hardware gps dead-reckoning**comanda a fost îmbunătățită pentru a oferi mesaje suplimentare de depanare pentru o mai bună funcționare. Mesajele de depanare vor acoperi următoarele:

- Cât de des sunt transmise datele senzorului de la modul în IOS, trebuie să fie cel puțin o dată pe secundă.
- Cele mai recente date de senzor primite de la modul.

Modificare a furnizorului pentru modulul GNSS

Această caracteristică se aplică numai IR1833 și IR1835. A existat o schimbare a producătorilor de cipuri pe modulul conectabil IRM-GNSS-ADR. Nu au existat modificări ale funcționalității, totuși veți vedea o schimbare în afișarea informațiilor despre furnizor și a versiunii de firmware.

Vezi următorul exemplu:

Router#**arătați platforma hardware gps neapărat** DR Mod
interfață vehicul: OBDDII GPS/DR Informații furnizor: VIC3DA

Modul GPS/DR Versiune FW: 4.6.18.11 Stare
Calibrare DR:
DR nu este calibrat Odometrul nu
este calibrat Câștigul nu este
calibrat Offset-ul nu este calibrat

Stare magistrală CAN:
Număr CAN Bus Tx: 11
Număr de erori CAN Bus Tx: 150930

Acces IOX la accelerometrul și giroscopul de bord IR1800

Această caracteristică permite transmiterea în flux a datelor de la senzorul accelerometrului și al giroscopului la bord către IOX printr-un TTY. Această caracteristică este dezactivată în mod implicit și va păstra paritatea caracteristică cu accelerometrul IR829 și caracteristica de date a senzorului giroscopului. CLI-urile pentru această caracteristică sunt definite mai jos.

Comenzi de configurare

Sunt disponibile următoarele comenzi:

Router(config)#**acc-gyro ?**
  permite Permite
  frecvenţă Frecvența în citire

Router(config)#**frecvență acc-gyro?**
  patru/sec Citirea de 4 ori pe secundă Citirea
  unu/min de 1 ori pe minut
  unu/sec Citire de 1 dată pe secundă (valoare implicită) Citire de
  zece/min 10 ori pe minut

Afișați comenzi

Următoarea comandă este disponibilă:

Router#**arată platforma hardware acc-gyro senzor-date**

Data Timp GX GY GZ XL-X XL-Y XL-Z
2022:10:26:16:58:13.855143 1137.50 -297.50 621.25 -18.056 -3.111 -966.057
2022:10:26:16:58:14.86362.50 -18.056 -3.111 -966.057 735,00 -17.629 -2.989 -965.996
2022:10:26:16:58:15.869117 1207.50 -140.00 726.25 -18.361 -3.294 -965.813
2022:10:26:16:58:16.874036 1268.75 -192.50 717.50 -18.178 -3.050 -965.874
2022:10:26:16:58:17.8846760.50 -18.178 717,50 -18.056 -2.989 -965.813 2022:10:26:16:58:18.894063
1347.50 -148.75 708.75 -18.117 -3.477 -965.935 2022:10:26:16:58:19,900830 1137,50 -315,00 577,50
-18,239 -3,599 -965,935 2022:10:26:16:58:20,9083765 -18,239 -3,599 -965,935 726,25 -17,873 -3,538
-965,813 2022:10:26:16:58:21,916674 1137,50 -262,50 726,25 -18,361 -2,867 -965,935
2022:10:26:16:58:22,927371 1137,50 -323,75 516,25 -17,934 -3,477 -965,569
2022:10:26:16:58:23,9342075 -17,934 -3,477 -965,569 516,25 -18,361 -3,416 -965,752
2022:10:26:16:58:24,940819 1111,25 -262,50 743,75 -18,422 -2,989 -965,386
2022:10:26:16:58:25,947471 1190,00 -201,25 673,75 -17,995 -3,416 -966,057
2022:10:26:16:58:26,95318,75 -17,995 -3,416 -966,057 577,50 -17,995 -3,233 -965,874
2022:10:26:16:58:27,961469 1137,50 -428,75 551,25 -18,117 -2,745 -965,996
2022:10:26:16:58:28,971354 1050,00 -271,25 717,50 -18,361 -3,233 -965,508
2022:10:26:16:58:29,981728,705 18,361 -3,233 -965,508 -18.117 -3.538 -965.386

Alte

Cele existente**depanare hardware acc-gyro senzor-date**comanda a fost îmbunătățită pentru a oferi mesaje suplimentare de depanare pentru o mai bună funcționare. Mesajele de depanare vor acoperi următoarele:

- Cât de des sunt transmise datele senzorului de la modul în IOS, trebuie să fie cel puțin o dată pe secundă.
- Cele mai recente date de senzor primite de la modul.

Configurați modulul DR folosind Cisco Catalyst SD-WAN Manager

Routerele IR1833 și IR1835 încorporează un modul Dead Reckoning (DR) care calibrează datele pentru a estima locația unui vehicul atunci când semnalul GPS este slab sau indisponibil. Cisco Catalyst SD-WAN Manager facilitează utilizarea comenzilor DR CLI prin șablonul CLI pentru a estima coordonatele GPS.

Cisco Catalyst SD-WAN Manager folosește modelele de date YANG pentru a configura modulul DR. Traduce aceste comenzi DR CLI în modele YANG și, ulterior, le împinge către dispozitiv.

Exemplu de configurare

Puteți configura dispozitivul care acceptă modulul DR prin șablonul CLI.

Aceasta este configurația eșantion, așa cum se vede în șablonul CLI Cisco Catalyst SD-WAN Manager.

controler GPS-Dr
activare dead-reckoning
dead-reckoning nmea udp 192.168.1.1 192.168.2.1 1111 mod dead-
recknoning j1939
dead-reckoning can-filter extins dead-reckoning
constelație gnss dead-reckoning iox-acc-frecvență zece/
min dead-reckoning iox-giro-frecvență patru/sec dead-
reckoning tty-baudrate 115200

Sfârşit
canbus baudrate 500000

Verificare

Verificați starea modulului DR

Router#**arătați platforma hardware gps neapărat** DR Mod
interfață vehicul: OBDDII GPS/DR Furnizor:

Informații despre furnizor GPS/DR:
Modul GPS/DR Versiune FW: 4.6.18.11 Stare
Calibrare DR:
DR este calibrat în modul DRUM-DRAW
  Contorul de parcurs este calibrat
  Câștigul este calibrat
  Offset-ul este calibrat

Stare magistrală CAN:
  CAN Bus Tx Count: 8621 CAN Bus Tx
  Count: 0 CAN Bus Rx Count: 38519 CAN
  Bus Rx Missed Count: 0 CAN NULL Packet
  NULL Bus RX Count: 0

  Număr de pachete neacceptate CAN Bus Rx: 2841 CAN
  Bus TX to DR Count: 8634
  Număr de erori CAN Bus TX to DR: 0

CAPITOL 20

Informații despre SCADA

Această secțiune conține următoarele subiecte:.

Prezentare generală privind controlul de supraveghere și achiziția de date (SCADA).

SCADA se referă la un sistem de control și management folosit în industrii precum managementul apei, energia electrică și producția. Un sistem SCADA colectează date de la diferite tipuri de echipamente din sistem și transmite acele informații înapoi către un Centru de control pentru analiză. În general, persoanele aflate la Centrul de Control monitorizează activitatea pe sistemul SCADA și intervin atunci când este necesar.

Unitatea terminală de la distanță (RTU) acționează ca sistem de control principal în cadrul unui sistem SCADA. RTU-urile sunt configurate pentru a controla funcții specifice din cadrul sistemului SCADA, care pot fi modificate după cum este necesar printr-o interfață cu utilizatorul.

Pe IR1800, linia este 0/2/0 sau 0/2/1, la fel ca interfața Async.

Rolul IR1800

În rețea, Centrul de control servește întotdeauna ca maestru în rețea atunci când comunică cu IR1800. IR1800 servește ca stație principală proxy pentru Centrul de control atunci când comunică cu RTU.

IR1800 oferă traducere de protocol pentru a servi ca gateway SCADA pentru a face următoarele:

- Primiți date de la RTU și transmiteți comenzile de configurare de la Centrul de control către RTU.
- Primiți comenzi de configurare de la Centrul de control și transmiteți datele RTU către Centrul de control
- Terminați cererile primite de la Centrul de control, atunci când un RTU este offline

IR1800 efectuează traducerea protocolului pentru următoarele protocoale:

- IEC 60870 T101 la/de la IEC 60870 T104.
- DNP3 serial la DNP3 IP

Termeni cheie

Următorii termeni sunt relevanți atunci când configurați stivele de protocoale T101 și T104 pe IR1800:

- Canal – Un canal este configurat pe fiecare interfață de port serial IR1800 pentru a oferi o conexiune la un singur RTU pentru fiecare conexiune IP la un centru de control la distanță. Fiecare conexiune transportă o singură stivă de protocoale T101 (RTU) sau T104 (Centrul de control).
- Link Adresă – Se referă la adresa dispozitivului sau a stației.
- Link Mode (Echilibrat și Dezechilibrat) – Se referă la modurile de transfer de date.
  - O setare Dezechilibrat se referă la un transfer de date inițiat de la master.
  - O setare Echilibrat se poate referi fie la un transfer de date inițiat de master sau slave.
- Sector – Se referă la un singur RTU dintr-un site la distanță.
- Sesiuni – Reprezintă o singură conexiune la un site la distanță.

Următorii termeni sunt relevanți atunci când configurați stivele de protocol DNP3 pe IR1800:

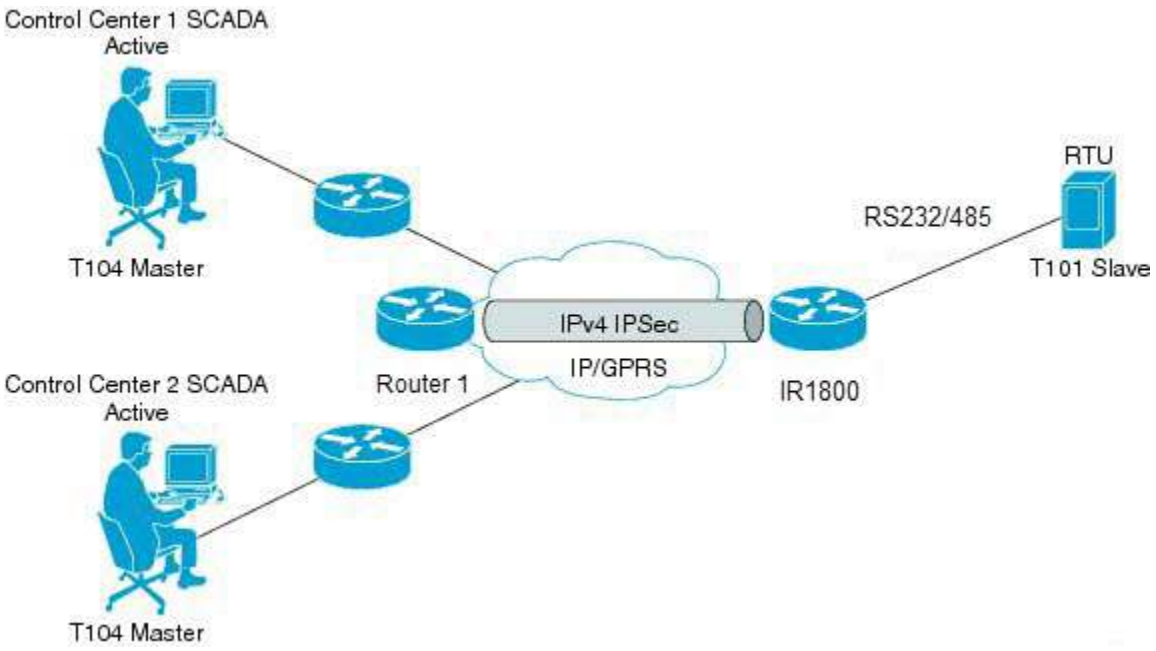
- Canal – Un canal este configurat pe interfața portului serial IR1800 pentru a oferi o conexiune la un singur RTU pentru fiecare conexiune IP la un Centru de control de la distanță. Fiecare conexiune transportă o singură stivă de protocol DNP3 serial (RTU) sau DNP3 IP (Control Center).
- Link Adresă – Se referă la adresa dispozitivului sau a stației.
- Sesiuni – Reprezintă o singură conexiune la un site la distanță.

Aplicația de traducere a protocolului

ÎnFigura 53: Routere În cadrul unui sistem SCADAS, la pagina 245IR1800 (instalat într-o substație secundară a rețelei de utilități) utilizează Protocol Translation pentru a oferi conectivitate securizată, de la capăt la capăt, între Centrele de control și RTU-urile din cadrul unui sistem SCADA.

IR1800 se conectează la RTU (subordonat) printr-o conexiune RS232/RS485. Pentru a proteja traficul atunci când este transmis prin infrastructuri publice (de exemplu, celulare), IR1800 transmite datele SCADA de la RTU către Centrul de control din sistemul SCADA printr-un tunel IPSec (FlexVPN site-to-site sau hub and spoke). Tunelul IPSec protejează întregul trafic dintre IR1800 și routerul de agregare Head-end. Traficul SCADA poate fi inspectat printr-un dispozitiv IPS poziționat în calea traficului SCADA înainte de a fi redirecționat către Centrul de control corespunzător.

Figura 53: Routere în cadrul unui sistem SCADA



Cerințe preliminare

RTU-urile trebuie să fie configurate și să funcționeze în rețea.

Pentru fiecare RTU care se conectează la IR1800, veți avea nevoie de următoarele informații pentru T101/T104:

- Informații despre canal
  - Numele canalului
  - Tip conexiune: serial
  - Setarea procedurii de transmisie prin link: dezechilibrat sau echilibrat
  - Câmpul de adresă al legăturii (număr exprimat în octeți)
- Informații despre sesiune
  - Numele sesiunii
  - Mărimea adresei comune a unității de date pentru serviciul aplicației (ASDU) (număr exprimat în octeți)
  - Mărimea cauzei transmisiei (COT) (număr exprimat în octeți)
  - Mărimea adresei obiectului de informare (IOA) (număr exprimat în octeți)
- Informații sectoriale
  - Denumirea sectorului
  - Adresă ASDU, (număr exprimat în octeți)

Pentru fiecare RTU care se conectează la IR1800, veți avea nevoie de următoarele informații pentru DNP3:

- Informații despre canal
  - Numele canalului
  - Tip conexiune: serial
  - Adresă link
- Informații despre sesiune
  - Numele sesiunii

Orientări și limitări

- Fiecare canal acceptă o singură sesiune.
- Fiecare sesiune acceptă un singur sector.
- Tipurile de obiect 8, 17, 18, 19, 20, 38, 39 și 40 nu sunt acceptate pentru traducerea protocolului IEC.

Setări implicite

T101/T104 Parametrii	**Implicit**
Rol pentru T101	Maestru
Rol pentru T104	Sclav

Parametrii DNP3	**Implicit**
Răspuns nesolicitat (DNP3-serial)	Nu Activat
Trimite mesaj nesolicitat (DNP3-IP)	Activat

Configurarea traducerii protocolului

Această secțiune include următoarele subiecte:

Nota Înainte de a face modificări de configurare la un IR1800 care funcționează cu Protocol Translation, vă rugăm să consultați secțiunea desprePornirea și oprirea motorului de traducere a protocolului, la pagina 259.

Activarea portului serial IR1800 și a încapsulării SCADA

Înainte de a putea activa și configura Protocol Translation pe IR1800, trebuie mai întâi să activați portul serial pe IR1800 și să activați încapsularea SCADA pe acel port.

Înainte de a începe

Determinați disponibilitatea unui port serial pe IR1800.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**configura terminalul**	Intră în modul de configurare globală.
Pasul 2	**interfață asincronă***slot/port/interfață*	Intră în modul de comandă a interfeței pentru slotul/portul/interfața asincron. *slot*–valoare de 0 *port*–valoare de 2 *interfata*–valoare 0 sau 1
Pasul 3	**nicio oprire**	Aduce portul, administrativ.
Pasul 4	**încapsulare scada**	Permite încapsularea pe portul serial pentru traducerea protocolului și alte protocoale SCADA.

Activați Exemplul de port serial

Acest exemplu arată cum să activați portul serial 0/2/0 și cum să activați încapsularea pe acea interfață pentru a suporta protocoalele SCADA.

router#**configura terminalul** router(config)#
interfață asincronă 0/2/0 router (config-if)#**nicio oprire** router (config-if)#**încapsulare scada**

Configurarea stivelor de protocol T101 și T104

Puteți configura stivele de protocoale T101 și T104, care permit comunicarea end-to-end între Centrele de Control (T104) și RTU-uri (T101) în cadrul unui sistem SCADA.

- Configurarea stivei de protocol T101, la pagina 248
- Configurarea stivei de protocol T104, la pagina 252
- Pornirea și oprirea motorului de traducere a protocolului, la pagina 259

Cerințe preliminare pentru stiva de protocol

Asigurați-vă că ați adunat toate informațiile de configurare necesare.

Activați portul serial și încapsularea SCADA.

Configurarea stivei de protocol T101

Configurați parametrii de canal, sesiune și sector pentru stiva de protocoale T101.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**configura terminalul**	Intră în modul de configurare globală.
Pasul 2	**protocolul scada-gw t101**	Intră în modul de configurare pentru protocolul T101.
Pasul 3	**canal***nume_canal*	Intră în modul de configurare a canalului pentru protocolul T101. *nume_canal*–Identifică canalul pe care portul serial al IR1800 comunică cu RTU. **Nota** Când numele canalului introdus nu există deja, routerul creează un nou canal. Intrând în**nu**forma acestei comenzi șterge un canal existent. Cu toate acestea, toate sesiunile trebuie șterse înainte de a putea șterge un canal.
Pasul 4	**maestru de rol**	Atribuie rolul de master canalului de protocol T101 (implicit).
Pasul 5	**modul de legătură***{echilibrat | dezechilibrat}*	Configurați modul de legătură ca echilibrat sau neechilibrat. dezechilibrat – Se referă la un transfer de date inițiat de la master. echilibrat – Se referă la un transfer de date master sau slave.
Pasul 6	**link-addr-size {niciunul | unul | două}**	Definește dimensiunea adresei de legătură în octeți.
Pasul 7	**asincron legat de interfață***slot/port/interfață*	Definește interfața serială IR1800 pe care sistemul își trimite traficul protocolului T101. *slot*–Valoarea 0 *port*–Valoarea de 2 *interfata*–Valoarea 0 sau 1

	Comanda sau Acțiune	Scop
Pasul 8	**Ieșire**	Încheie configurarea canalului și iese din modul de configurare a canalului. Salvează toate setările.
Pasul 9	**sesiune***nume_sesiune*	Intră în modul de configurare a sesiunii și atribuie un nume sesiunii.
Pasul 10	**atașare la canal***nume_canal*	Atașează sesiunea la canal. Introduceți același nume de canal pe care l-ați introdus Pasul 3. *nume_canal*–Identifică canalul.
Pasul 11	**dimensiune-adresă-comună***{unul | doi | trei}*	Definește dimensiunea comună a adresei în octeți.
Pasul 12	**dimensiunea pătuțului***{unul | doi | trei}*	Definește cauza transmisiei, cum ar fi schemele de date spontane sau ciclice în octeți.
Pasul 13	**info-obj-adr-size***{unul | doi | trei}*	Definește dimensiunea adresei elementului de informație în octeți.
Pasul 14	**link-adr-size***{unul | doi | trei}*	Definește dimensiunea adresei de legătură în octeți.
Pasul 15	**link-adr***adresa_link*	Se referă la adresa de link a RTU. **Nota** Adresa de legătură introdusă aici trebuie să se potrivească cu valoarea setată pe RTU la care se conectează portul serial. *adresa_link*–Interval de 0-65535.
Pasul 16	**Ieșire**	Iese din modul de configurare a sesiunii.
Pasul 17	**sector***nume_sector*	Intră în modul de configurare a sectorului și atribuie un nume sectorului pentru RTU. *nume_sector*–Identifică sectorul.
Pasul 18	**atașare la sesiune***nume_sesiune*	Atașează sectorul RTU la sesiune. Introduceți același nume de sesiune în care l-ați introdusPasul 9. *nume_sesiune*-Identifică sesiunea.
Pasul 19	**asdu-addr***adresa_asdu*	Se referă la adresa structurii ASDU a RTU.
Pasul 20	**Ieșire**	Iese din modul de configurare sector.
Pasul 21	**Ieșire**	Iese din modul de configurare a protocolului.

Exemplu de stivă de protocol T101

Acest exemplu arată cum să configurați parametrii pentru stiva de protocoale T101 pentru *RTU_10*.

router#**configura terminalul** router(config)#**protocolul scada-gw t101** router(config-t101)#**canal rtu_canal** router(config-t101-channel)#**maestru de rol** router(config-t101-channel)#**modul de legătură dezechilibrat** router(config-t101-channel)#**link-adr-size unul**

router(config-t101-channel)#**legare la interfață asincronă 0/2/0** router(config-t101-channel)#**Ieșire** router(config-t101)#**sesiune rtu_session** router(config-t101-session)#**atașare la canal rtu_channel** router(config-t101-session)#**comun-adresă-mărimea doi** router(config-t101-session)#**unul de mărimea pătuțului** router(config-t101-session)#**info-obj-addr-size two** router(config-t101-session)#**link-adr 3** router(config-t101-session)#**Ieșire** router(config-t101)#**sector rtu_sector** router(config-t101-sector)#**atașare la sesiune rtu_session** router(config-t101-sector)#**asdu-addr 3** router(config-t101-sector)#**Ieșire** router(config-t101)#**Ieșire** router(config)#

Exemplu de configurare T101

Următorul exemplu arată cum să configurați interfața portului serial pentru conexiunea T101, să configurați stivele de protocoale T101 și T104 și să porniți Motorul de traducere a protocolului pe IR1800.

router#**configura terminalul** router(config)#**interfață asincronă 0/2/0** router (config-if)#**nicio oprire** router (config-if)#**încapsulare scada** router (config-if)#**Ieșire** router(config)#**protocolul scada-gw t101** router(config-t101)#**canal rtu_canal** router(config-t101-channel)#**maestru de rol** router(config-t101-channel)#**modul de legătură dezechilibrat** router(config-t101-channel)#**link-adr-size unul** router(config-t101-channel)#**legare la interfață asincronă 0/2/0** router(config-t101-channel)#**Ieșire** router(config-t101)#**sesiune rtu_session** router(config-t101-session)#**atașare la canal rtu_channel** router(config-t101-session)#**comun-adresă-mărimea doi** router(config-t101-session)#**unul de mărimea pătuțului** router(config-t101-session)#**info-obj-addr-size two** router(config-t101-session)#**link-adr 3** router(config-t101-session)#**Ieșire** router(config-t101)#**sector rtu_sector** router(config-t101-sector)#**atașare la sesiune rtu_session** router(config-t101-sector)#**asdu-addr 3** router(config-t101-sector)#**Ieșire** router(config-t101)#**Ieșire** router(config)#**protocolul scada-gw t104** router(config-t104)#**canalul cc_master1** router(config-t104-channel)#**valoarea k 12** router(config-t104-channel)#**valoarea w 8**

router(config-t104-channel)#**t0-timeout 30** router(config-t104-channel)#**t1-timeout 15** router(config-t104-channel)#**t2-timeout 10** router(config-t104-channel)#**t3-timeout 30** router(config-t104-channel)#**tcp-connection 0 local-port 2050 remote-ip orice** router(config-t104-channel)#**tcp-connection 1 local-port 2051 remote-ip orice** router(config-t104-channel)#**Ieșire** router(config-t104)#**sesiune cc_master1** router(config-t104-session)#**atașare la canal cc_master1** router(config-t104-session)#**pătuț de mărimea doi** router(config-t104-session)#**Ieșire** router(config-t104)#**sector cc_master1-sector** router(config-t104-sector)#**atașare la sesiune cc_master1** router(config-t104-sector)#**asdu-adr 3** router(config-t104-sector)#**map-to-sector rtu_sector** router(config-t104)#**Ieșire** router(config-t104)#**sesiune cc_master2** router(config-t104-session)#**atașare la canal cc_master2** router(config-t104-session)#**pătuț de mărimea doi** router(config-t104-session)#**Ieșire** router(config-t104)#**sector cc_master2-sector** router(config-t104-sector)#**atașare la sesiune cc_master2** router(config-t104-sector)#**asdu-adr 3** router(config-t104-sector)#**map-to-sector rtu_sector** router(config-t104-sector)#**Ieșire** router(config-t104)#**Ieșire** router(config)#**activare scada-gw**

Acest exemplu configurează comunicația end-to-end între Centrele de control și RTU-urile dintr-un sistem SCADA utilizând stivele de protocoale DNP3 și pornește Motorul de traducere a protocolului pe IR1800:

router#**configura terminalul** router(config)#
interfață asincronă 0/2/0 router (config-if)#**nicio oprire** router (config-if)#**încapsulare scada** router (config-if)#**Ieșire**

router(config)#**protocol scada-gw dnp3-serial** router(config-dnp3s)#**canal rtu_canal** router(config-dnp3s-channel)#**legare la interfață asincronă 0/2/0** router(config-dnp3s-channel)#**sursa link-addr 3** router(config-dnp3s-channel)#**activarea răspunsului nesolicitat** router(config-dnp3s-channel)#**Ieșire** router(config-dnp3s)#**sesiune rtu_session** router(config-dnp3s-session)#**atașare la canal rtu_channel** router(config-dnp3s-session)#**link-addr dest 3** router(config-dnp3s-session)#**Ieșire** router(config-dnp3s)#**Ieșire** router(config)#**protocolul scada-gw dnp3-ip** router(config-dnp3n)#**canalul cc_channel** router(config-dnp3n-channel)#**link-addr dest 3** router(config-dnp3n-channel)#**tcp-connection local-port default remote-ip any** router(config-dnp3n-channel)# ieșire din router(config-dnp3n)#**sesiune cc_session** router(config-dnp3n-session)#**atașare la canal cc_channel** router(config-dnp3n-session)#**sursa link-addr 3** router(config-dnp3n-session)#**map-to-session rtu_session** router(config-dnp3n)#**Ieșire** router(config)#**Ieșire**

router(config)#**activare scada-gw**

Configurarea stivei de protocol T104

Urmați pașii de mai jos pentru fiecare Centru de control la care doriți să vă conectați printr-un protocol T104.

Înainte de a începe

Asigurați-vă că ați adunat toate informațiile de configurare necesare. (VedeaCerințe preliminare, la pagina 245)

Activați portul serial și încapsularea SCADA. (VedeaActivarea portului serial IR1800 și a încapsulării SCADA, la pagina 247)

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**configura terminalul**	Intră în modul de configurare.
Pasul 2	**protocolul scada-gw t104**	Intră în modul de configurare pentru protocolul T104.
Pasul 3	**canal***nume_canal*	Intră în modul de configurare a canalului pentru protocolul T104. *nume_canal*–Identifică canalul pe care routerul comunică cu Centrul de control. **Nota** Când numele canalului introdus nu există deja, routerul creează un nou canal. Intrând în**nu**forma acestei comenzi șterge un canal existent. Cu toate acestea, toate sesiunile trebuie șterse înainte de a putea șterge un canal.
Pasul 4	**valoarea k***valoare*	Setează numărul maxim de unități de date pentru protocolul de aplicație (APDU) restante pentru canal. **Nota** Un APDU încorporează ASDU și un antet de control. *valoare*–Interval de valori de la 1 la 32767. Valoarea implicită este 12 APDU.
Pasul 5	**valoarea w***valoare*	Setează numărul maxim de APDU-uri pentru canal. *valoare*–Interval de valori de la 1 la 32767. Valoarea implicită este 8 APDU-uri.

	Comanda sau Acțiune	Scop
Pasul 6	**t0-timeout***valoare*	Definește valoarea t0-timeout pentru stabilirea conexiunii canalului T104.
Pasul 7	**t1-timeout***valoare*	Definește valoarea t1-timeout pentru trimiterea sau testarea APDU-urilor pe canalul T104.
Pasul 8	**t2-timeout***valoare*	Definește valoarea t2-timeout pentru confirmări atunci când routerul nu primește niciun mesaj de date. **Nota** Valoarea t2 trebuie întotdeauna setată la o valoare mai mică decât valoarea t1 pe canalul T104.
Pasul 9	**t3-timeout***valoare*	Definește valoarea t3-timeout pentru trimiterea de cadre s în cazul unei stări de inactivitate lungă pe canalul T104. **Nota** Valoarea t3 trebuie întotdeauna setată la o valoare mai mare decât valoarea t1 pe canalul T104.
Pasul 10	**tcp-connection {0|1} local-port**{*port_number* | **implicit} remote-ip**{*ABCD* / *ABCD/LEN* | **orice**} [**vrf***CUVÂNT*]	Într-o configurație în care există Centre de control redundante, setează valoarea conexiunii pentru Centrul de control secundar, așa cum este definit în Centrul de control principal. *număr-port*–valoare între 2000 și 65535. valoarea implicită de 2404. *ABCD*–o singură gazdă. *ABCD/nn*–subrețeaua ABCD/LEN. orice – orice gazdă la distanță 0.0.0.0/0. WORD – nume VRF.
Pasul 11	**Ieșire**	Iese din modul de configurare a canalului.
Pasul 12	**sesiune***nume_sesiune*	Intră în modul de configurare a sesiunii și atribuie un nume sesiunii. *nume_sesiune*–Folosiți același nume pe care l-ați atribuit canalului înPasul 3.
Pasul 13	**atașare la canal***nume_canal*	Definește numele canalului care transportă traficul de sesiune.
Pasul 14	**dimensiunea pătuțului***{unul / doi / trei}*	Definește cauza transmisiei (cot), cum ar fi schemele de date spontane sau ciclice în octeți.
Pasul 15	**Ieșire**	Iese din modul de configurare a sesiunii.

	Comanda sau Acțiune	Scop
Pasul 16	**sector***nume_sector*	Intră în modul de configurare a sectorului și atribuie un nume sectorului pentru Centrul de control.
Pasul 17	**atașare la sesiune***nume_sesiune*	Atașează sectorul Centrului de control la canal. *nume_sesiune*–Folosiți același nume pe care l-ați atribuit canalului înPasul 3.
Pasul 18	**asdu-addr***adresa_asdu*	Se referă la adresa structurii ASDU. Valoarea introdusă aici trebuie să se potrivească cu valoarea ASDU de pe RTU. *adresa_asdu*–*adresa_asdu*–Valoarea 1 sau 2.
Pasul 19	**hartă la sector***nume_sector*	Mapează sectorul Centrului de control (T104) cu sectorul RTU (T101).
Pasul 20	Întoarce-te laPasul 1.	Repetați toți pașii din această secțiune pentru fiecare Centru de control activ în rețea.

Configurați exemplul de stivă de protocol T104

Acest exemplu arată cum să configurați parametrii pentru protocolul T104*Centrul de control 1*și *Centrul de control 2,*ambele sunt configurate ca*stăpâni*,și cum să mapați sectorul T104 cu sectorul T101.

Pentru a configura Centrul de control 1 (*cc_master1*),introduceți următoarele comenzi.

router#**configura terminalul** router(config)#**protocolul scada-gw t104** router(config-t104)#**canalul cc_master1** router(config-t104-channel)#**valoarea k 12** router(config-t104-channel)#**valoarea w 8** router(config-t104-channel)#**t0-timeout 30** router(config-t104-channel)#**t1-timeout 15** router(config-t104-channel)#**t2-timeout 10** router(config-t104-channel)#**t3-timeout 30**

router(config-t104-channel)#**tcp-connection 0 local-port 2050 remote-ip 209.165.200.225** router(config-t104-channel)#**tcp-connection 1 local-port 2051 remote-ip 209.165.201.25** router(config-t104-channel)#**Ieșire** router(config-t104)#**sesiune cc_master1**

router(config-t104-session)#**atașare la canal cc_master1** router(config-t104-session)#**pătuț de mărimea doi** router(config-t104-session)#**Ieșire** router(config-t104)#**sector cc_master1-sector** router(config-t104-sector)#**atașare la sesiune cc_master1** router(config-t104-sector)#**asdu-adr 3** router(config-t104-sector)#**map-to-sector rtu_sector** router(config-t104)#**Ieșire** router(config)#

Pentru a configura Control Center 2 (*cc_master2*),introduceți următoarele comenzi.

router(config)#**protocolul scada-gw t104** router(config-t104)#**canalul cc_master2** router(config-t104-channel)#**valoarea k 12** router(config-t104-channel)#**valoarea w 8** router(config-t104-channel)#**t0-timeout 30** router(config-t104-channel)#**t1-timeout 15** router(config-t104-channel)#**t2-timeout 10** router(config-t104-channel)#**t3-timeout 30**

router(config-t104-channel)#**tcp-connection 0 local-port 2060 remote-ip 209.165.201.237** router(config-t104-channel)#**tcp-connection 1 local-port 2061 remote-ip 209.165.200.27** router(config-t104-channel)#**Ieșire** router(config-t104)#**sesiune cc_master2** router(config-t104-session)#**atașare la canal cc_master2** router(config-t104-session)#**pătuț de mărimea doi** router(config-t104-session)#**Ieșire** router(config-t104)#**sector cc_master2-sector** router(config-t104-sector)#**atașare la sesiune cc_master2** router(config-t104-sector)#**asdu-adr 3** router(config-t104-sector)#**map-to-sector rtu_sector** router(config-t104-sector)#**Ieșire** router(config-t104)#**Ieșire** router(config)#

Configurarea stivelor de protocol DNP3

Puteți configura stivele de protocol DNP3 serial și DNP3 IP, care permit comunicarea end-to-end între Centrele de Control și RTU-urile din cadrul unui sistem SCADA.

Configurarea DNP3 Serial

Configurați parametrii de canal și de sesiune pentru comunicația serială DNP cu un RTU.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**configura terminalul**	Intră în modul de configurare globală.
Pasul 2	**protocol scada-gw dnp3-serial**	Intră în modul de configurare pentru protocolul serial DNP3.
Pasul 3	**canal***nume_canal*	Intră în modul de configurare a canalului pentru protocolul serial DNP3. *nume_canal*–Identifică canalul pe care portul serial al routerului comunică cu RTU. **Nota** Când numele canalului introdus nu există deja, routerul creează un nou canal Intrând în**nu**forma acestei comenzi șterge un canal existent. Cu toate acestea, toate sesiunile

	Comanda sau Acțiune	Scop
		trebuie șters înainte de a putea șterge un canal.
Pasul 4	**bind-to-interface async0/2/0**	Definește interfața asincronă a routerului pe care sistemul își trimite traficul protocolului DNP3.
Pasul 5	**sursa link-addr***adresa_sursă*	Se referă la adresa de legătură a masterului. *adresa_sursă*–Interval de valori de la 1 la 65535.
Pasul 6	**activarea răspunsului nesolicitat**	(Opțional) Permite răspunsuri nesolicitate. Intrând în**nu**forma acestei comenzi dezactivează răspunsurile nesolicitate. Valoarea implicită este dezactivată.
Pasul 7	**Ieșire**	Încheie configurarea canalului și iese din modul de configurare a canalului. Salvează toate setările.
Pasul 8	**sesiune***nume_sesiune*	Intră în modul de configurare a sesiunii și atribuie un nume sesiunii. **Nota** Când numele de sesiune introdus nu există deja, routerul creează o nouă sesiune. Intrând în**nu**forma acestei comenzi șterge o sesiune existentă.
Pasul 9	**atașare la canal***nume_canal*	Atașează sesiunea la canal. **Nota** Introduceți același nume de canal pe care l-ați introdus la Pasul 3 de mai sus. *nume_canal*–Identifică canalul.
Pasul 10	**link-addr dest***adresa_destinație*	Se referă la adresa link-ului slave. *adresa_destinație*–Interval de valori de la 1 la 65535.
Pasul 11	**Ieșire**	Iese din modul de configurare a sesiunii.
Pasul 12	**Ieșire**	Iese din modul de configurare a protocolului.

Exemplu de stivă de protocol serial DPN3

Acest exemplu arată cum să configurați parametrii pentru stiva de protocol serial DPN3:

router#**configura terminalul** router(config)#**protocol scada-gw dnp3-serial** router(config-dnp3s)#**canal rtu_canal** router(config-dnp3s-channel)#**legare la interfață asincronă 0/2/0** router(config-dnp3s-channel)#**sursa link-addr 3**

router(config-dnp3s-channel)#**activarea răspunsului nesolicitat** router(config-dnp3s-channel)#**Ieșire** router(config-dnp3s)#**sesiune rtu_session** router(config-dnp3s-session)#**atașare la canal rtu_channel** router(config-dnp3s-session)#**link-addr dest 3** router(config-dnp3s-session)#**Ieșire** router(config-dnp3s)#**Ieșire** router(config)#

Configurarea IP DNP3

Urmați pașii de mai jos pentru Centrul de control la care doriți să vă conectați prin IP DNP3. Pentru redundanță, puteți crea mai multe conexiuni care partajează aceeași configurație de sesiune în aceeași sesiune.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**configura terminalul**	Intră în modul de configurare.
Pasul 2	**protocolul scada-gw dnp3-ip**	Intră în modul de configurare pentru protocolul DNP-IP.
Pasul 3	**canal***nume_canal*	Intră în modul de configurare a canalului pentru protocolul DNP-IP. *nume_canal*–Identifică canalul pe care routerul comunică cu Centrul de control. **Nota** Când numele canalului introdus nu există deja, routerul creează un nou canal. Intrând în**nu**forma acestei comenzi șterge un canal existent. Cu toate acestea, toate sesiunile trebuie șterse înainte de a putea șterge un canal.
Pasul 4	**link-addr dest***adresa_destinație*	Se referă la adresa de legătură a masterului. *adresa_destinație*–Interval de valori de la 1 la 65535.
Pasul 5	**activare send-unsolicited-msg**	(Opțional) Permiteți mesajele nesolicitate. Valoarea implicită este activată.
Pasul 6	**tcp-conexiune local-port**[**implicit**| *port_local*] **la distanţă-ip**[**orice**| *remote_ip*| *subrețea_la distanță*]	Configurați numărul portului local și adresa IP la distanță pentru conexiunea TCP: • **implicit** – 20000. • *port_local*–Interval de valori de la 2000 la 65535.

	Comanda sau Acțiune	Scop
		• orice–Orice gazdă la distanță 0.0.0.0/0 • *remote_ip*–Gazdă unică: ABCD • *subrețea_la distanță*–Subrețea: ABCD/LEN Dacă este specificat remote_subnet, atunci când două canale au aceleași porturi locale, subrețelele la distanță nu se pot suprapune. **Nota** Fiecare <local-port, remote-ip>trebuie să fie unic pe canal. Dacă este specificat remote_subnet, atunci când două canale au aceleași porturi locale, subrețelele la distanță nu se pot suprapune.
Pasul 7	**Ieșire**	Iese din modul de configurare a canalului.
Pasul 8	**sesiune***session_name*	Intră în modul de configurare a sesiunii și atribuie un nume sesiunii. **Nota** Când numele de sesiune introdus nu există deja, routerul creează o nouă sesiune. Intrând în**nu**forma acestei comenzi șterge o sesiune existentă.
Pasul 9	**atașare la canal***nume_canal*	Atașează sesiunea la canal. Introduceți același nume de canal pe care l-ați introdus la Pasul 3. *nume_canal*–Identifică canalul.
Pasul 10	**sursa link-addr***adresa_sursă*	Se referă la adresa link-ului slave. *adresa_sursă*–Valoarea 1-65535.
Pasul 11	**hartă la sesiune***nume_sesiune*	Mapează sesiunea dnp3-ip la o sesiune dnp3-serial existentă. **Nota** O sesiune dnp3-ip poate fi mapată la o singură sesiune dnp3-serial.
Pasul 12	**Ieșire**	Iese din modul de configurare a sesiunii.
Pasul 13	**Ieșire**	Iese din modul de configurare a protocolului.

Exemplu de parametri IP DNP3

Acest exemplu arată cum să configurați parametrii IP DNP3:

router#**configura terminalul** router(config)#
protocolul scada-gw dnp3-ip

router(config-dnp3n)#**canalul cc_channel** router(config-dnp3n-channel)#**link-addr dest 3** router(config-dnp3n-channel)#**tcp-connection local-port default remote-ip any** router(config-dnp3n-channel)# ieșire din router(config-dnp3n)#**sesiune cc_session** router(config-dnp3n-session)#**atașare la canal cc_channel** router(config-dnp3n-session)#**sursa link-addr 4** router(config-dnp3n-session)#**map-to-session rtu_session** router(config-dnp3n)#**Ieșire** router(config)#**Ieșire**

Pornirea și oprirea motorului de traducere a protocolului

Înainte de a porni motorul de traducere a protocolului pe router pentru prima dată, asigurați-vă că ați completat următoarele elemente:

Activarea portului serial IR1800 și a încapsulării SCADA, la pagina 247

Configurarea stivelor de protocol T101 și T104, la pagina 247

Trebuie să porniți Motor Translation Protocol pentru a utiliza Protocol Translation pe IR1800.

Pornire– După ce activați încapsularea SCADA pe portul serial IR1800 și configurați protocoalele T101 și T104 pe IR1800, puteți porni Motorul de traducere a protocolului.

Oprire– Înainte de a putea face modificări de configurare la Protocol Translation pe IR1800 cu un Protocol Translation Engine activ, trebuie să opriți motorul.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**configura terminalul**	Intră în modul de configurare globală.
Pasul 2	**activare scada-gw**	Începe (**activare scada-gw**) sau se oprește (**nicio activare scada-gw**) Motorul de traducere a protocolului de pe IR1800.

Porniți exemplu de motor de traducere a protocolului

Pentru a porni motorul de traducere a protocolului pe router, introduceți următoarele comenzi:

router#**configura terminalul**
router(config)#**activare scada-gw**

Pentru a opri motorul de traducere a protocolului pe router, introduceți următoarele comenzi:

router#**configura terminalul**
router(config)#**nu**
activare scada-gw

Îmbunătățirea SCADA pentru TNB

Această îmbunătățire oferă compatibilitate cu RTU-urile WG ale TNB, inclusiv următoarele:

- RTU-urile TNB necesită ca mesajul Reset-Link să fie trimis împreună cu mesajul Link-Status pentru a asigura inițializarea corectă a seriei. Caracteristica poate fi activată selectiv folosind noul CLI de configurare **protocolul scada-gw forță resetarea-link.**
- Când trecerea ceasului este activată și dacă routerul nu a primit marcajul de timp de la masterul DNP3-IP, ora hardware a routerului va fi trimisă în aval către RTU. La primirea unui nou marcaj temporal de la DNP3-IP master, routerul va începe să trimită noul timestamp provenit de la DNP3-IP master la RTU.
- Numărul de evenimente DNP3 tamponabile din memorie va fi crescut de la 600 la 10000.
- Cel**interblocarea protocolului scada-gw**comanda va fi acceptată pentru DNP3. Anterior, suportul exista doar pentru T101/T104. Cu această nouă îmbunătățire, routerul va deconecta legătura serială dacă masterul DNP3-IP nu este sau nu este accesibil. În mod similar, când legătura serială la RTU este oprită, conexiunea TCP la master DNP3-IP va fi deconectată.
- „Solicitările” personalizate vor fi comandate automat în funcție de prioritate, astfel încât utilizatorul să le poată specifica în orice ordine pe care ar dori să o facă.

Verificarea configurației

Comanda	Scop
spectacol **rulare-config**	Afișează configurația routerului, inclusiv funcțiile active și setările acestora.
arată scada baza de date	Afișează detalii în baza de date SCADA.
arată scada statistici	Afișează statistici pentru gateway-ul SCADA, inclusiv numărul de mesaje trimise și primite, expirări și erori.
arată scada tcp	Afișează conexiunile TCP asociate cu gateway-ul SCADA.

Acest exemplu arată rezultatul din comenzile show scada tcp și show scada statistics:

```
router#arată scada tcp
Canal de rețea DNP3 [test]: max. 4 conexiuni simultane conexiune: local-ip:
3.3.3.21                    local-port 20000        remote-ip 3.3.3.15          priza de date
  1
Total:
    1 conexiuni client curente 0 total
    conexiuni închise router# arată
statisticile scada DNP3 canal canal [test]:

    5 mesaje trimise, 2 mesaje primite 0 timeouts, 0
    anulări, 0 respingeri
    2 erori de protocol, 2 erori de legătură, 0 erori de adresă Canal serial
DNP3 [test]:
    152 de mesaje trimise, 152 de mesaje primite 1
    timeout, 0 anulări, 0 respingeri
    0 erori de protocol, 0 erori de legătură, 0 erori de adresă
```

Comenzi de depanare SCADA

Această secțiune listează câteva comenzi de depanare care sunt utile la depanare.

Tabelul 22: Comenzi de depanare la nivel de funcție SCADA

Comanda	Scop
depanare funcția scada config	Configurare urmă
depanare controlul funcției Scada	Urmă de control
depanare fișierul funcției scada	Urmă fișier
funcția de depanare scada freeze	Urme înghețate
depanare funcția scada fizică	Urmă fizică
depanare funcția scada sondaj	Urmă sondaj
depanare stiva de funcții scada	Urmă stivă
depanare funcția scada umode	Urmă Umode

CAPITOL 21

Transport cu priză brută

Această secțiune conține următoarele subiecte:

Prezentare generală a transportului de prize brute

Raw Socket Transport transportă fluxuri de caractere de la o interfață serială la alta printr-o rețea IP pentru aplicații utilitare.

Acest document descrie Raw Socket Transport pentru IR1800 și oferă o secțiune de referință care descrie comenzile Raw Socket Transport.

Informații despre transportul de prize brute

Raw Socket este o metodă de transport de date seriale printr-o rețea IP. Caracteristica poate fi utilizată pentru a transporta date SCADA (control de supraveghere și achiziție de date) de la unități terminale la distanță (RTU). Această metodă este o alternativă la protocolul Block Serial Tunnel (BSTUN).

Raw Socket Transport acceptă TCP sau UDP ca protocol de transport. O interfață poate fi configurată să utilizeze oricare dintre protocoluri, dar nu ambele în același timp. Transportul TCP este potrivit pentru aplicații precum aplicațiile de control care necesită livrarea confirmată și secvențială a datelor. Pentru aplicațiile sensibile la latență, cum ar fi releele SEL de linie, transportul UDP oferă un transport mai rapid de date seriale decât TCP.

Raw Socket Transport acceptă următoarele pentru interfața serială asincronă:

- TCP ca protocol de transport, cu mecanism de reîncercare a conexiunii automate TCP încorporat.
- Până la 32 de sesiuni TCP.

- Configurarea interfeței ca server, client sau o combinație a ambelor.
- O interfață de server, dar mai mulți clienți.
- Conștientizarea VRF, care permite routerului să trimită trafic Raw Socket Transport către o gazdă de server conectată printr-o interfață Virtual Private Network (VPN) Virtual Routing and Forwarding (VRF).

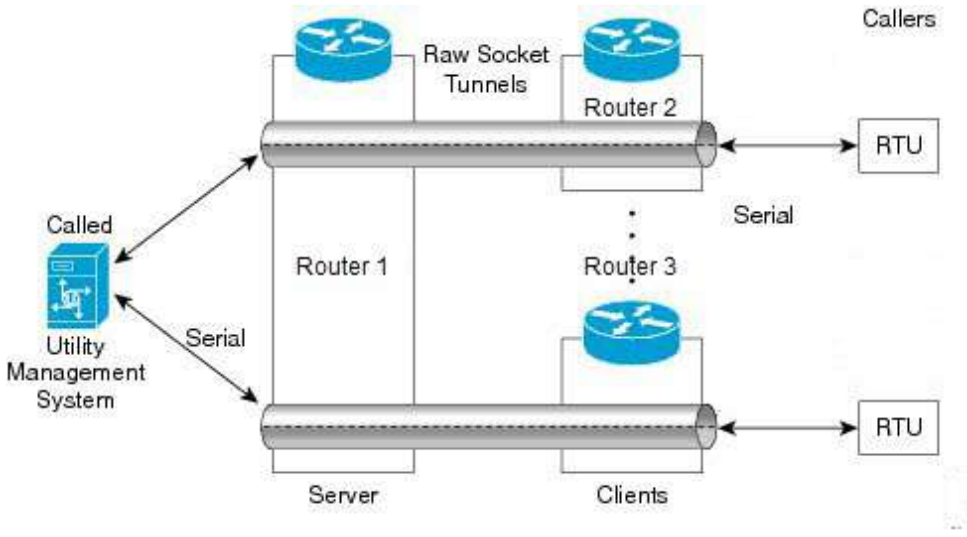
Această secțiune include următoarele subiecte:

Transport TCP

Transportul TCP Raw Socket utilizează un model client-server. Cel mult un server și mai mulți clienți pot fi configurați pe o singură linie serială asincronă. În modul client, IR1800 poate iniția până la 32 de sesiuni TCP pe serverele Raw Socket, care pot fi alte routere IR1800 sau dispozitive terțe.

Următoarea figură prezintă un exemplu de configurare Raw Socket TCP. În acest exemplu, datele seriale sunt transferate între RTU-uri și un sistem de management al utilităților printr-o rețea IP care include mai multe routere IR1800. Un router IR1800 (Router 1) acționează ca un server Raw Socket, ascultând cererile de conexiune TCP de la celelalte routere IR1800 (Router 2 și Router 3), care sunt configurate ca clienți Raw Socket.

Un client Raw Socket primește fluxuri de date seriale de la RTU și acumulează aceste date în buffer-ul său, apoi plasează datele în pachete, pe baza criteriilor de pachetizare specificate de utilizator. Clientul Raw Socket inițiază o conexiune TCP cu serverul Raw Socket și trimite datele pachetizate prin rețeaua IP către serverul Raw Socket, care preia datele seriale din pachete și le trimite la interfața serială și la sistemul de management al utilităților.



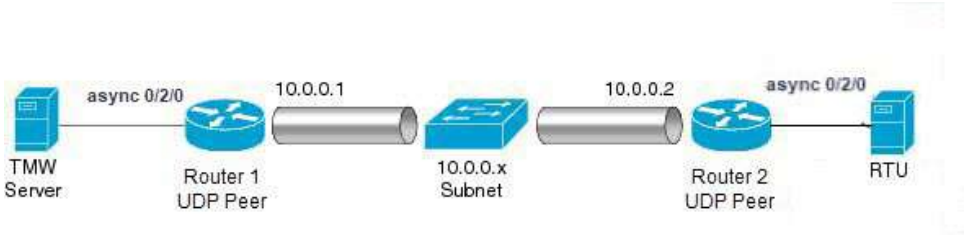
Nota Când configurați interfața de legătură serială de pe router ca server, peer-ul interfeței este interfața de legătură serială de pe routerul client și invers.

Transport UDP

Transportul UDP utilizează un model peer-to-peer. Pot fi configurate mai multe conexiuni UDP pe o linie serială asincronă.

Următoarea figură prezintă un exemplu de configurare Raw Socket UDP. În acest exemplu, datele seriale sunt transferate între RTU-uri și un sistem de management al utilităților printr-o rețea IP care include două routere (Routerul 1, care este un IR1800 și Router-ul 2, care este un IR807), care sunt configurate ca egali Raw Socket UDP.

În acest exemplu, peer-ul Raw Socket UDP primește fluxuri de date seriale de la RTU și acumulează aceste date în buffer-ul său, apoi plasează datele în pachete, pe baza criteriilor de pachete specificate de utilizator. Peer-ul Raw Socket UDP trimite datele pachetizate prin rețeaua IP către peer-ul Raw Socket de la celălalt capăt, care preia datele seriale din pachete și le trimite la interfața serială și la sistemul de management al utilităților.



Prelucrarea datelor în serie

Când se utilizează protocolul serial implicit, Protocolul de comunicare asincronă, fluxurile de date seriale primite de un peer Raw Socket pot fi pachetizate pe baza următoarelor criterii:

- **Lungimea pachetului**–Puteți specifica o lungime de pachet care declanșează IR1800 să transmită datele seriale către peer. Odată ce IR1800 colectează atât de multe date în buffer-ul său, pachetează datele acumulate și le transmite către peer-ul Raw Socket.
- **Valoarea pachet-timer**–Temporizatorul de pachete specifică perioada de timp pe care IR1800 așteaptă să primească următorul caracter dintr-un flux. Dacă un caracter nu este primit până la expirarea temporizatorului de pachete, datele pe care IR1800 le-a acumulat în buffer-ul său sunt pachetizate și transmise către peer-ul Raw Socket.
- **Caracter special**–Puteți specifica un caracter care va declanșa IR1800 să pacheteze datele acumulate în buffer-ul său și să le trimită către peer-ul Raw Socket. Când caracterul special (de exemplu, un CR/LF) este primit, IR1800 pachetează datele acumulate și le trimite către peer-ul Raw Socket.

VeziProcedura „Configurarea opțiunilor comune pentru linia de priză brută” la pagina 6pentru informații despre configurarea opțiunilor de procesare.

Priză Raw Aware VRF

Caracteristica Raw Socket Transport care știe VRF vă permite să izolați traficul Raw Socket folosind un VRF pentru gestionarea și controlul eficient al datelor seriale. După configurarea unui VRF, puteți asocia interfața serială configurată pentru Raw Socket Transport cu VRF. VeziRaw Socket VRF, la pagina 275pentru un exemplu de configurare.

Cerințe preliminare

Stabiliți cum doriți să fie transportat traficul Raw Socket în rețeaua dvs., inclusiv dispozitivele și interfețele de rețea pe care să le utilizați, modul în care routerul pachetează datele seriale și dacă să utilizați VRF.

Orientări și limitări

De obicei, traficul UDP este blocat de firewall-urile din rețea. Dacă rețeaua are astfel de firewall-uri, asigurați-vă că ați configurat găuri pentru a permite traficul UDP de soclu brut.

Setări implicite

Caracteristică	Setare implicită
Priză brută Transport	Dezactivat.
Lungimea pachetului	Nu este configurată nicio lungime de pachet.
Protocol serial	Protocol de comunicare asincronă
Timp de expirare a pachetului	15 ms.
Caracter special	Nu este configurat niciun caracter special.
Modul Raw Socket	Modul cel mai bun efort este dezactivat, nu este acceptat pe IR1801.
Timp de inactivitate TCP	5 minute.

Configurarea Raw Socket Transport

Această secțiune include următoarele subiecte:

Activarea transportului de soclu brut pe interfața serială

Pentru a activa Raw Socket Transport pe routerul IR1800, trebuie mai întâi să activați un port serial asincron și să activați încapsularea Raw Socket TCP sau UDP pentru acel port.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**configura terminalul**	Intră în modul de configurare globală.

	Comanda sau Acțiune	Scop
Pasul 2	**interfață async0***/slot/port*	Intră în modul de comandă a interfeței pentru slotul/portul asincron.
Pasul 3	**fara adresa ip**	Dezactivează procesarea IP pe interfață.
Pasul 4	Efectuați una dintre următoarele: • **încapsulare raw-tcp** • **încapsulare raw-udp**	Activează încapsularea RawSocket TCP sau încapsularea UDP pentru portul serial.

Activați Exemplul de port serial

Acest exemplu arată cum să activați portul serial 0/2/0 și cum să activați încapsularea Raw Socket TCP pe acel port.

router#**configura terminalul** router(config)#
interfață async0/2/0 router(config-if)#**fara adresa ip**
router(config-if)#**încapsulare raw-tcp** router(config-if)#**Ieșire**

Configurarea opțiunilor comune pentru linia de priză brută

Puteți configura opțiuni comune tuturor conexiunilor de pe o linie. Opțiunile comune se aplică atât pentru TCP, cât și pentru UDP.

Înainte de a începe

Activați Raw Socket Transport așa cum este descris înActivarea transportului de soclu brut pe interfața serială, la pagina 266.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**configura terminalul**	Intră în modul de configurare globală.
Pasul 2	**linia 0***/slot/port*	Intră în modul de comandă linie pentru slotul/portul serial.
Pasul 3	**raw-socket-lungimea pachetului***lungime*	Specifică dimensiunea pachetului care declanșează IR1800 să transmită datele către peer. Când IR1800 acumulează atât de multe date în buffer-ul său, el pachetează datele și le transmite către peer-ul Raw Socket. *lungime*-2 până la 1400 de octeți. În mod implicit, declanșatorul pentru lungimea pachetului este dezactivat.
Pasul 4	**temporizator de pachete cu priză brută***pauză*	Specifică timpul maxim în milisecunde pe care IR1800 îl așteaptă pentru a primi următorul caracter

	Comanda sau Acțiune	Scop
		într-un pârâu. Dacă un caracter nu este primit până la expirarea temporizatorului de pachete, datele acumulate sunt pachetate și transmise către peer-ul Raw Socket. *pauză*—3 până la 1000 ms. Valoarea implicită este de 15 ms.
Pasul 5	**raw-socket spec-char***ascii_char*	Specifică un caracter care va declanșa IR1800 să pacheteze datele acumulate în buffer-ul său și să le trimită către peer-ul Raw Socket. *ascii_char*—de la 0 la 255. În mod implicit, declanșarea caracterelor speciale este dezactivată.

Ce să faci în continuare

Utilizați**nu**forma acestor comenzi pentru a reveni la valorile implicite.

Exemplu de configurare Common Raw Socket Line Options

router#**configura terminalul** router(config)#**linia 0/2/0** router
(linie de configurare) #**lungimea pachetului raw-socket-ul 32**
router (linie de configurare) #**raw-socket packet-timer 500**
router (linie de configurare) #**raw-socket special-char 3**

Configurarea Raw Socket TCP

După ce activați încapsularea Raw Socket TCP, configurați serverul și/sau clienții TCP.

Configurarea serverului Raw Socket TCP

Înainte de a începe

Activați un port serial și încapsularea Raw Socket TCP pentru acel port, așa cum este descris înActivarea transportului de soclu brut pe interfața serială, la pagina 266.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**configura terminalul**	Intră în modul de configurare.
Pasul 2	**linia 0***/slot/port*	Intră în modul de comandă linie pentru slotul/portul serial.
Pasul 3	**server raw-socket tcp***port*[*adresa_ip*]	Pornește serverul Raw Socket Transport TCP pentru o interfață de linie asincronă. În priză brută

	Comanda sau Acțiune	Scop
		modul server, IR1800 ascultă cererile de conectare primite de la clienții Raw Socket. *port*–Numărul de port pe care ascultă serverul. *adresa_ip*– (Opțional) Adresă IP locală pe care serverul ascultă cererile de conectare.
Pasul 4	**raw-socket tcp idle-timeout***session_timeout*	Setează timpul de expirare a sesiunii TCP Raw Socket Transport pentru interfața de linie asincronă. Dacă nu sunt transferate date între client și server în acest interval, atunci sesiunea TCP se închide. Clientul încearcă apoi automat să restabilize sesiunea TCP cu serverul. Această setare de timeout se aplică tuturor sesiunilor TCP Raw Socket Transport din această linie specială. *session_timeout*–Timpul de inactivitate al sesiunii configurat în prezent, în minute. Valoarea implicită este de 5 minute.

Ce să faci în continuare

Pentru a elimina un server Raw Socket TCP, utilizați**fără server tcp cu socket brut**comanda.

Exemplu de configurare Common Raw Socket TCP Server

Acest exemplu arată cum să configurați un server TCP Raw Socket pentru o linie serială asincronă. Serverul TCP ascultă cererile de conectare a clientului TCP pe portul local 4000 și pe adresa IP locală 10.0.0.1. Dacă nu se fac schimb de date între serverul Raw Socket TCP și unul dintre clienții TCP timp de 10 minute, atunci sesiunea TCP se închide și clientul Raw Socket încearcă să restabilească sesiunea cu serverul Raw Socket.

router#**configura terminalul**

router(config)#**linia 0/2/0**
router (linie de configurare) #**server tcp raw-socket 4000 10.0.0.1** router (linie de configurare) #**raw-socket tcp idle-timeout 10** router (linie de configurare) #**Ieșire** router(config)#

Configurarea clientului Raw Socket TCP

Înainte de a începe

Activați un port serial și încapsularea Raw Socket TCP pentru acel port, așa cum este descris înActivarea transportului de soclu brut pe interfața serială, la pagina 266.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**configura terminalul**	Intră în modul de configurare.
Pasul 2	**linia 0***/slot/port*	Intră în modul de comandă linie pentru slotul/portul serial.
Pasul 3	**client tcp raw-socket***dest_ip_address dest_port [local_ip_address] [local_port]*	Specifică setările pentru sesiunile client TCP Raw Socket Transport. *adresa_ip_dest*–Adresa IP de destinație a serverului Raw Socket de la distanță. *dest_port*–Numărul portului de destinație de utilizat pentru conexiunea TCP la serverul de la distanță. *adresa_ip_locală*– (Opțional) Adresă IP locală la care se poate lega și clientul. *port_local*– (Opțional) Număr de port local la care se poate lega și clientul.
Pasul 4	**raw-socket tcp idle-timeout***session_timeout*	Setează timpul de expirare a sesiunii TCP Raw Socket Transport pentru interfața de linie asincronă. Dacă nu sunt transferate date între client și server în acest interval, atunci sesiunea TCP este închisă. Clientul încearcă apoi automat să restabilize sesiunea TCP cu serverul. Această setare de timeout se aplică tuturor sesiunilor TCP Raw Socket Transport din această linie specială. *session_timeout*–Timpul de inactivitate al sesiunii configurat în prezent, în minute. Valoarea implicită este de 5 minute.
Pasul 5	**tcp keepalive***interval*	Setează intervalul de menținere a sesiunii TCP Raw Socket Transport pentru interfața de linie asincronă. Routerul trimite mesaje keepalive pe baza intervalului configurat. Poate fi necesar să configurați acest interval, de exemplu, când trimiteți trafic TCP brut printr-o interfață celulară. *interval*–Interval de menținere configurat în prezent în secunde. Intervalul este 1-864000 secunde. Valoarea implicită este de 1 secundă.

Ce să faci în continuare

Pentru a elimina un client TCP Raw Socket, utilizați**nici un client tcp raw-socket**comanda.

Raw Socket TCP Client Exemplu

Acest exemplu arată cum să configurați un client TCP Raw Socket pentru o linie serială asincronă. IR1800 (routerul), care servește ca client Raw Socket, inițiază sesiuni TCP cu un server Raw Socket și îi transmite date seriale pachetizate. Routerul colectează fluxuri de date seriale în buffer-ul său; când acumulează 827 de octeți în buffer-ul său, routerul pachetează datele și le transmite către serverul Raw Socket. Dacă routerul și serverul Raw Socket nu fac schimb de date timp de 10 minute, atunci sesiunea TCP cu serverul Raw Socket se închide și routerul încearcă să restabilească sesiunea cu serverul Raw Socket.

router#**configura terminalul**
router(config)#**linia 0/2/0**
router (linie de configurare) #**client tcp raw-socket 10.0.0.1 4000** router (linie de configurare) #**Lungimea pachetului de priză brută 827** router (linie de configurare) #**raw-socket tcp idle-timeout 10** router (linie de configurare) #**Ieșire** router(config)#

Îmbunătățirea caracteristicii prizei brute

Această îmbunătățire permite utilizatorului să introducă numărul maxim de încercări disponibile pentru soclul de scriere. Intervalul numărului de reîncercări variază de la 1 la 1000. Numărul implicit de reîncercări este 10. Pentru a permite această caracteristică, a fost creat un nou CLI,**raw-socket tcp max-retry <1-1000>**. <1-1000> este numărul maxim de încercări.

Configurarea unei conexiuni peer-to-peer UDP cu soclu brut

După ce activați încapsularea Raw Socket UDP și opțiunile comune de linie, configurați conexiunea peer-to-peer de Raw Socket UDP. Portul local de la un capăt al conexiunii ar trebui să fie portul de destinație de la celălalt capăt.

Înainte de a începe

Activați un port serial și încapsularea Raw Socket UDP pentru acel port, așa cum este descris înActivarea transportului de soclu brut pe interfața serială, la pagina 266.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**configura terminalul**	Intră în modul de configurare.
Pasul 2	**linia 0***/slot/port*	Intră în modul de comandă linie pentru slotul/portul serial.
Pasul 3	**conexiune raw-socket udp***dest_ip_address dest_port local_port [local_ip_address]*	Specifică setările pentru conexiunile UDP Raw Socket Transport. *adresa_ip_dest*–Adresă IP de destinație de utilizat pentru conexiunea UDP. *dest_port*–Numărul portului de destinație de utilizat pentru conexiunea UDP.

	Comanda sau Acțiune	Scop
		port_local–Număr de port local pentru conexiunea UDP. *adresa_ip_locală*– (Opțional) Adresă IP locală pentru conexiunea UDP.

Ce să faci în continuare

Pentru a elimina o conexiune Raw Socket UDP, utilizați**nicio conexiune udp raw-socket**comanda.

Exemplu de conexiune UDP priză brută

Acest exemplu arată cum să configurați o conexiune Raw Socket UDP între routerul A (adresa IP locală 192.168.0.8) și routerul B (adresa IP locală 192.168.0.2).

Routerul A

router#**configura terminalul**
router(config)#**linia 0/2/0**
router (linie de configurare) #**conexiune udp raw-socket 192.168.0.2 5000 7000** router (linie de configurare) #**Ieșire** router(config)#

Routerul B

router#**configura terminalul**
router(config)#**linia 0/2/0**
router (linie de configurare) #**conexiune udp raw-socket 192.168.0.8 7000 5000** router (linie de configurare) #**Ieșire** router(config)#

CLI de configurare Rawsocket Keepalive

Rawsocket keepalive pentru interfețele asincrone este o caracteristică care a existat în platformele clasice IOS. Ca parte a versiunii 17.10.1a, caracteristica va fi extinsă la platformele bazate pe IOS-XE. Un nou CLI cu următoarea sintaxă va fi adăugat sub rawsocket.

Router (linie de configurare) #**raw-socket tcp keepalive***interval*

Modificări CLI

Pe platformele IOS-XE începând cu 17.10.1a, există o corecție CLI și a fost adăugat un CLI suplimentar ca parte a raw-socket.

Corecția este pentru**raw-socket inactiv timeout**comanda. Acum există o opțiune de configurare a timeout-ului pe baza minutelor și secundelor, în timp ce configurația anterioară folosea doar minute.

Router (linie de configurare) #**raw-socket tcp idle-timeout***[0-1440] [<0-59> | cr]*

CLI-ul suplimentar este pentru ștergerea clienților TCP raw-socket. Sintaxa comenzii este**linie clară de priză brută** *[1-145 | tty | x/y/z]*de exemplu:

Router#**linie raw-socket clară 0/2/0**

Nota La inițierea liniei de socket raw-socket clar, sesiunile de socket raw vor fi șterse pentru clienții raw-socket din **arată sesiunile tcp cu socket brut**comanda. Conexiunile vor fi restabilite după o strângere de mână TCP, care se poate face făcând închidere/neînchidere pe interfața de conexiune TCP.

Verificarea configurației

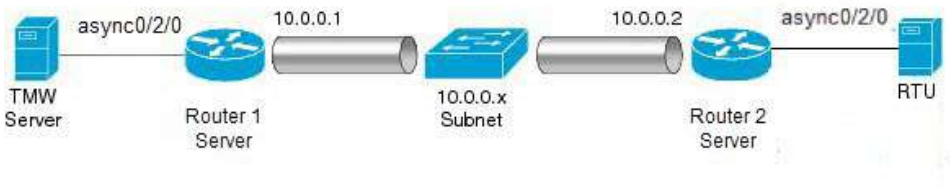
Comanda	Scop
arată rularea-config	Afișează configurația IR1800, inclusiv acele caracteristici care sunt active și setările acestora.
afișează detaliile tcp de priză brută	Afișează informații despre activitatea TCP Raw Socket Transport.
arată sesiunile tcp cu socket brut	Afișează informații despre sesiunile TCP Raw Socket Transport.
afișează statisticile raw-socket tcp	Afișează statisticile TCP Raw Socket Transport pentru fiecare linie serială asincronă.
arată detaliile udp prize brute	Afișează informații despre activitatea UDP Raw Socket Transport.
afișează sesiunile udp raw-socket	Afișează informații despre sesiunile UDP Raw Socket Transport.
afișează statisticile raw-socket udp	Afișează statisticile UDP Raw Socket Transport pentru fiecare linie serială asincronă.
statistici clare de priză brută	Șterge statisticile Raw Socket Transport pentru o anumită interfață TTY sau pentru toate liniile seriale asincrone.

Exemple de configurare a transportului de prize brute

Următoarele secțiuni includ exemple de configurare Raw Socket Transport:

Raw Socket TCP

Următorul exemplu arată o configurație Raw Socket Transport în care un router IR1800 (Router 1) acționează ca server, iar un alt IR809 (Router 2) acționează ca client.



Următorul tabel afișează configurația serverului și a clientului IR1800s evidențiate în figura de mai sus:

Configurare server IR1800	Configurare client IR807
. . . interfață async0/2/0 fara adresa ip **încapsulare raw-tcp** ! . . . linia 0/2/0 **server tcp raw-socket 5000 10.0.0.1** **raw-socket packet-timer 3 raw-socket tcp idle-timeout 5** . . .	. . . interfață async0 fara adresa ip **încapsulare raw-tcp** ! interfață asincronă1 fara adresa ip **încapsulare raw-tcp** ! . . . linia 1 **client tcp raw-socket 10.0.0.1 5000 10.0.0.2 9000 raw-socket lungime-pachet 32** **raw-socket tcp idle-timeout 5** linia 2 **client tcp raw-socket 10.0.0.1 5000 10.0.0.2 9001 raw-socket lungime-pachet 32** **raw-socket tcp idle-timeout 5**

Exemplu de priză brută UDP

Acest exemplu arată configurația pentru o conexiune Raw Socket UDP între două routere IR1800:

De la Router1

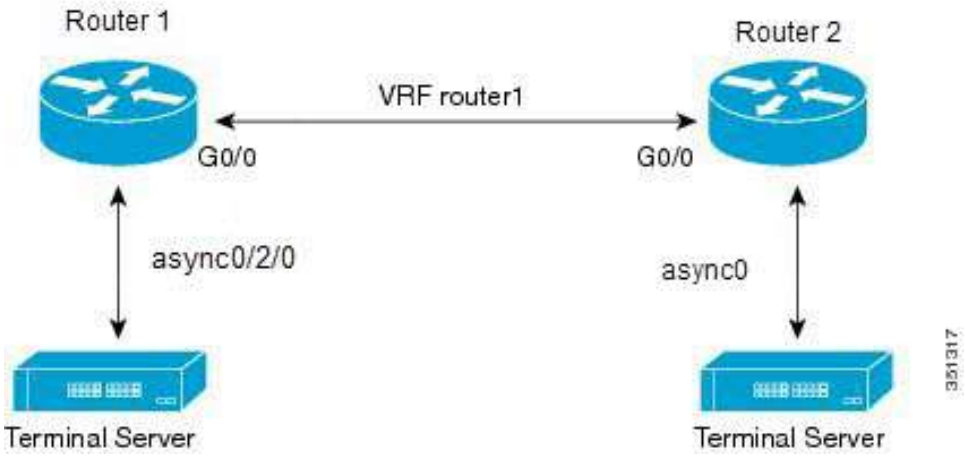
interfață GigabitEthernet0/1
adresa ip 192.168.0.8 255.255.255.0 duplex automat
viteza automata
interfață async0/2/0
fara adresa ip
încapsulare raw-udp
linia 0/2/0
conexiune udp raw-socket 192.168.0.2 2 2

De la Router2

interfață GigabitEthernet0/1
adresa ip 192.168.0.2 255.255.255.0 interval de încărcare 60
duplex automat
viteza automata
fara mentinere in viata
interfață async0/2/0
fara adresa ip
încapsulare raw-udp
linia 0/2/0
raw-socket udp connection 192.168.0.8 2 2

Raw Socket VRF

Următorul exemplu arată o configurație Raw Socket VRF în care două routere, configurate pentru Raw Socket Transport, se conectează printr-un VRF. Router1 este un IR1800, servește ca server Raw Socket TCP, iar Router2 este un IR807 servește drept client TCP Raw Socket.



Următoarele sunt configurațiile Router1 și Router2, așa cum se arată în figura de mai sus:

Configurație Router1

Definirea VRF pe router:

```
router de definiție vrf1
 rd 100:1
 export rută-țintă 100:3 import
 rută-țintă 100:3 !

 adresa-familie ipv4
 ieșire-adresă-familie
```

Aplicarea configurației VRF pe interfață:

```
interfață GigabitEthernet0/0 router de
 redirecționare vrf1
 adresa ip 100.100.100.2 255.255.255.0 duplex
 automat
 viteza automata
```

Aplicarea raw-tcp pe interfața serială:

```
interfață async0/2/0
 router de redirecționare vrf1
 fara adresa ip
 încapsulare raw-tcp
```

Aplicarea raw-tcp pe linie:

```
linia 0/2/0
 server tcp raw-socket 5000 4.4.4.4
```

Configurație Router2

Definirea VRF pe router:

```
router de definiție vrf1
  rd 100:1
  export rută-țintă 100:3 import
  rută-țintă 100:3 !

  adresa-familie ipv4
  ieșire-adresă-familie
```

Aplicarea configurației VRF pe interfață:

```
interfață GigabitEthernet0/0 router de
  redirecționare vrf1
  adresa ip 100.100.100.1 255.255.255.0 duplex
  automat
  viteza automata
```

Aplicarea raw-tcp pe interfața serială:

```
interfață async0
  router de redirecționare vrf1
  fara adresa ip
  încapsulare raw-tcp
```

Aplicarea raw-tcp on-line:

```
linia 1
   client tcp raw-socket 4.4.4.4 5000
```

CAPITOL 22

Gazduire aplicatie IOx

Această secțiune conține următoarele subiecte:

Gazduire aplicatie

O aplicație găzduită este o soluție software ca serviciu și poate fi rulată de la distanță folosind comenzi. Găzduirea aplicațiilor oferă administratorilor o platformă pentru a-și folosi propriile instrumente și utilități.

Acest modul descrie caracteristica de găzduire a aplicației și cum să o activați.

Informații despre găzduirea aplicației

Această secțiune conține următoarele:

Nevoia de găzduire a aplicațiilor

Trecerea către mediile virtuale a dat naștere nevoii de a construi aplicații care să fie reutilizabile, portabile și scalabile. Găzduirea aplicațiilor oferă administratorilor o platformă pentru a-și folosi propriile instrumente și utilități. O aplicație, găzduită pe un dispozitiv de rețea, poate servi pentru o varietate de scopuri. Aceasta variază de la automatizare, monitorizarea managementului configurației și integrarea cu lanțurile de instrumente existente.

Dispozitivele Cisco acceptă aplicații disponibile de la terți, construite folosind lanțuri de instrumente Linux. Utilizatorii pot rula aplicații personalizate compilate încrucișat cu kitul de dezvoltare software oferit de Cisco.

Prezentare generală IOx

IOx este un cadru de aplicații end-to-end dezvoltat de Cisco, care oferă capabilități de găzduire a aplicațiilor pentru diferite tipuri de aplicații pe platformele de rețea Cisco.

Arhitectura IOx pentru IR1800 este diferită în comparație cu alte platforme Cisco care utilizează abordarea hypervisor. În alte platforme, IOx rulează ca o mașină virtuală. IOx rulează ca proces pe IR1800.

Prezentare generală a găzduirii aplicațiilor Cisco

IR1800 permite utilizatorului să implementeze aplicația folosind CLI-urile de găzduire a aplicației. Aceste CLI de găzduire a aplicațiilor nu sunt disponibile pe celelalte platforme mai vechi. Există modalități suplimentare de a implementa aplicațiile utilizând Managerul Local și Directorul de ceață.

Gazduirea aplicatiei ofera urmatoarele servicii:

- Lansează aplicații desemnate în containere.
- Verifică resursele disponibile (memorie, CPU și stocare) și le alocă și le gestionează.
- Oferă suport pentru înregistrarea în consolă.
- Oferă acces la servicii prin intermediul API-urilor REST.
- Oferă un punct final CLI.
- Oferă o infrastructură de găzduire a aplicațiilor denumită Cisco Application Framework (CAF).
- Ajută la configurarea unei rețele specifice platformei (packet-path) prin VirtualPortGroup și interfețe de gestionare.

Containerul este denumit mediu de virtualizare furnizat pentru a rula aplicația invitat pe sistemul de operare gazdă. Serviciile de virtualizare Cisco IOS-XE oferă manevrabilitate și modele de rețea pentru rularea aplicațiilor invitate. Infrastructura de virtualizare permite administratorului să definească o interfață logică care specifică conectivitatea dintre gazdă și oaspete. IOx mapează interfața logică în placa de interfață de rețea virtuală (vNIC) pe care o folosește aplicația invitată.

Aplicațiile care urmează să fie implementate în containere sunt ambalate ca fișiere TAR. Configurația care este specifică acestor aplicații este, de asemenea, ambalată ca parte a fișierului TAR.

Interfața de management de pe dispozitiv conectează rețeaua de găzduire a aplicației la interfața de management IOS. Interfața Layer 3 a aplicației primește traficul Layer 2 prin punte de la interfața IOSmanagement. Interfața de management se conectează prin puntea de management la interfața container/aplicație. Adresa IP a aplicației trebuie să fie pe aceeași subrețea cu adresa IP a interfeței de gestionare.

IOXMAN

IOXMAN este un proces care stabilește o infrastructură de urmărire pentru a oferi servicii de înregistrare sau urmărire pentru aplicațiile invitate, cu excepția Libvirt, care emulează dispozitivele seriale. IOXMAN se bazează pe ciclul de viață al aplicației oaspete pentru a activa și dezactiva serviciul de urmărire, pentru a trimite date de înregistrare la IOS syslog, pentru a salva datele de urmărire în IOx tracelog și pentru a menține IOx tracelog pentru fiecare aplicație invitată.

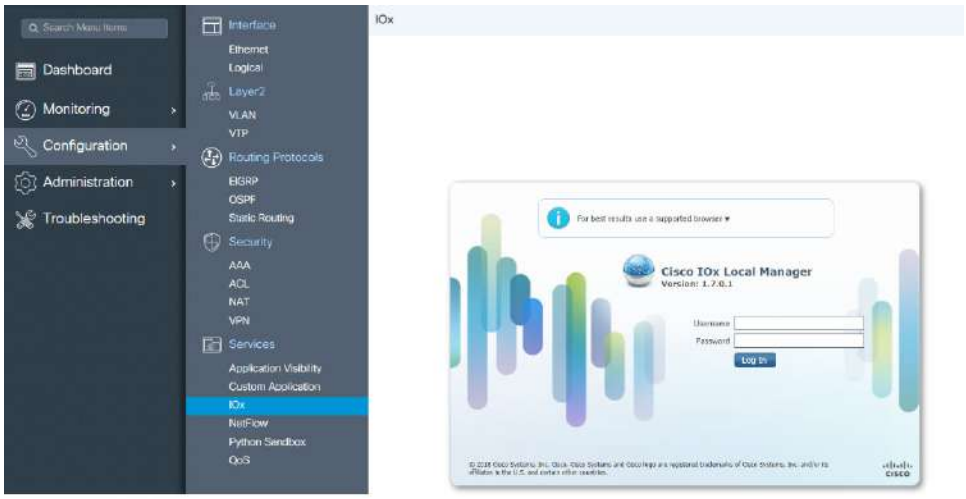
Găzduire de aplicații pe routerul de servicii integrate industriale IR1800

Această secțiune descrie caracteristicile de găzduire a aplicației specifice routerului pentru servicii integrate industriale IR1800.

Nota CPU IR1800 nu se bazează pe arhitectura x86 ca alte routere. Prin urmare, acest lucru necesită ca aplicația să respecte arhitectura ARM pe 64 de biți.

Găzduirea aplicației poate fi realizată folosind cli-urile de găzduire a aplicației, precum și folosind Managerul local și Directorul de ceață. Găzduirea aplicației folosind Local Manager se face prin WebUI. Pentru a implementa aplicațiile folosind Local Manager, WebUI ar trebui să fie activat și apoi să vă conectați la Local Manager.

Figura 54: Manager local



1. Din WebUI, faceți clic pe**Configurare > Servicii > IOx**

2. Conectați-vă folosind numele de utilizator și parola configurate.

3. Urmați pașii pentru ciclul de viață al aplicației din**Ghid de referință pentru Cisco IOx Local Manager**folosind acest link:https://www.cisco.com/c/en/us/td/docs/routers/access/800/software/guides/iox/lm/reference-guide/ 1-7/b_iox_lm_ref_guide_1_7/b_iox_lm_ref_guide_1_7_chapter_011.html

Următoarea secțiune explică implementarea unei aplicații folosind cli-urile de găzduire a aplicației.

VirtualPortGroup

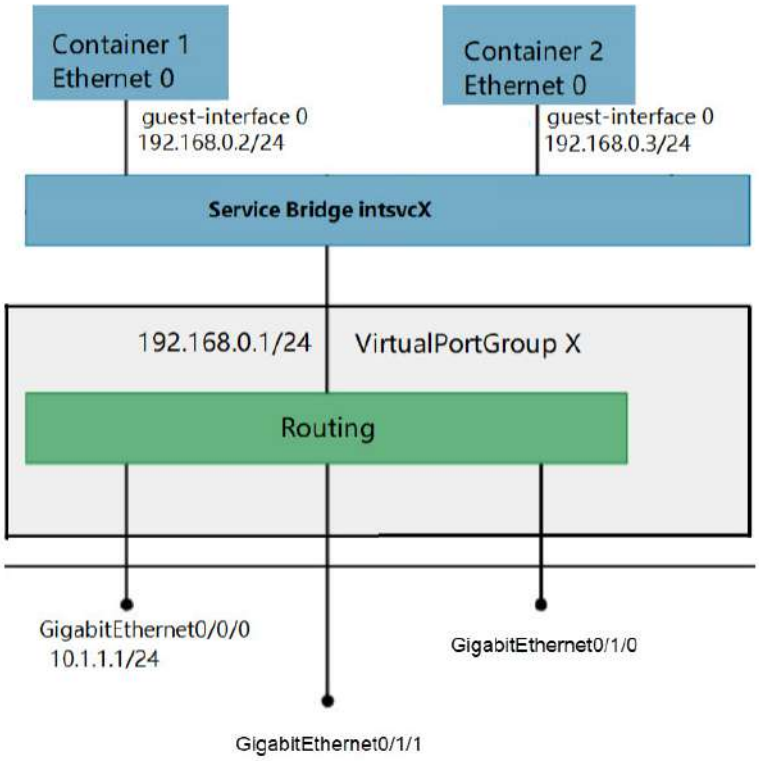
VirtualPortGroup este o construcție software pe Cisco IOS care se mapează la o adresă IP de punte Linux. Ca atare, VirtualPortGroup reprezintă interfața virtuală de comutare (SVI) a containerului Linux. Fiecare punte poate conține mai multe interfețe; fiecare mapare la un container diferit. Fiecare container poate avea, de asemenea, mai multe interfețe.

Interfețele VirtualPortGroup sunt configurate utilizând comanda interfață virtualportgroup. Odată ce aceste interfețe sunt create, adresa IP și alte resurse sunt alocate.

Interfața VirtualPortGroup conectează rețeaua de găzduire a aplicației la domeniul de rutare IOS. Interfața Layer 3 a aplicației primește trafic direcționat de la IOS. Interfața VirtualPortGroup se conectează prin SVC Bridge la interfața container/aplicație.

Următorul grafic ajută la înțelegerea relației dintre VirtualPortGroup și alte interfețe, deoarece este diferită de routerele IR8x9.

Figura 55: Maparea grupului de porturi virtuale



vNIC

Pentru gestionarea ciclului de viață al containerului, este utilizat modelul de rutare Layer 3 care acceptă un container per interfață logică internă. Aceasta înseamnă că o pereche Ethernet virtuală este creată pentru fiecare aplicație; și o interfață a acestei perechi, numită vNIC, face parte din containerul aplicației. Cealaltă interfață, numită vpgX face parte din sistemul gazdă.

NIC este interfața Ethernet standard din interiorul containerului care se conectează la planul de date al platformei pentru trimiterea și primirea pachetelor. IOx este responsabil pentru gateway (interfața VirtualPortGroup), adresa IP și atribuirea adresei MAC unice pentru fiecare vNIC din container.

VNIC-urile din interiorul containerului/aplicației sunt considerate interfețe Ethernet standard.

Cum să configurați găzduirea aplicației

Această secțiune conține următoarele:

Activarea IOx

Efectuați această sarcină pentru a activa accesul la IOx Local Manager. IOx Local Manager oferă o interfață de utilizator bazată pe web pe care o puteți utiliza pentru a gestiona, administra, monitoriza și depana aplicațiile de pe sistemul gazdă și pentru a efectua o varietate de activități conexe

Nota În pașii următori, comenzile IP HTTP nu activează IOX, dar permit utilizatorului să acceseze WebUI pentru a conecta IOX Local Manager.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** Dispozitiv>**permite**	Activează modul EXEC privilegiat. Introduceți parola dacă vi se solicită.
Pasul 2	**configura terminalul** **Exemplu:** Dispozitiv#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**iox** **Exemplu:** Dispozitiv (config) #**iox**	Activează IOx.
Pasul 4	**server ip http** **Exemplu:** Dispozitiv (config) #**server ip http**	Activează serverul HTTP pe sistemul dumneavoastră IP sau IPv6.
Pasul 5	**ip http server securizat** **Exemplu:** Dispozitiv (config) #**ip http server securizat**	Activează un server HTTP (HTTPS) securizat.
Pasul 6	**nume de utilizator***nume***privilegiu***nivel***parolă**{ **0 | 7**| *parola-utilizator* }*parolă-criptată* **Exemplu:** Dispozitiv (config) #**nume de utilizator privilegiu cisco 15 parolă 0 cisco**	Stabilește un sistem de autentificare bazat pe nume de utilizator și un nivel de privilegii pentru utilizator. Nivelul de privilegiu al numelui de utilizator trebuie configurat ca 15.

	Comanda sau Acțiune	Scop
Pasul 7	**Sfârşit** **Exemplu:** Dispozitiv (config-if)#**Sfârşit**	Iese din modul de configurare a interfeței și revine la modul EXEC privilegiat

Configurarea unui VirtualPortGroup la un Port de date Layer 3

Mai multe porturi de date Layer 3 pot fi direcționate către unul sau mai multe VirtualPortGroups sau containere. VirutalPortGroups și porturile de date Layer 3 trebuie să fie pe subrețele diferite.

Activați**rutare ip**comandă pentru a permite rutarea externă pe portul de date Layer 3.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** Dispozitiv>**permite**	Activează modul EXEC privilegiat. Introduceți parola dacă vi se solicită.
Pasul 2	**configura terminalul** **Exemplu:** Dispozitiv#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**rutare ip** **Exemplu:** Dispozitiv (config) #**rutare ip**	Activează rutarea IP. The**rutare ip**comanda trebuie să fie activată pentru a permite rutarea externă pe porturile de date Layer 3.
Pasul 4	**interfata***numărul de tip* **Exemplu:** Dispozitiv (config) #**interfață gigabitethernet 0/0/0**	Configura o interfață și intră în modul de configurare a interfeței.
Pasul 5	**fara switchport** **Exemplu:** Dispozitiv (config) #**fara switchport**	Plasează interfața în modul Layer 3 și o face să funcționeze mai degrabă ca o interfață de router decât ca un port de comutare.
Pasul 6	**adresa ip***masca cu adresa ip* **Exemplu:** Dispozitiv (config) #**adresa ip 10.1.1.1 255.255.255.0**	Configurați o adresă IP pentru interfață.
Pasul 7	**Ieşire** **Exemplu:** Dispozitiv (config-if)#**Ieșire**	Iese din modul de configurare a interfeței și revine la modul de configurare globală.

	Comanda sau Acțiune	Scop
Pasul 8	**interfata***numărul de tip* **Exemplu:** Dispozitiv (config) #**interfață virtualportgroup 0**	Configura o interfață și intră în modul de configurare a interfeței.
Pasul 9	**adresa ip***masca cu adresa ip* **Exemplu:** Dispozitiv (config-if)#**adresa ip 192.168.0.1 255.255.255.0**	Configurați o adresă IP pentru interfață.
Pasul 10	**Sfârşit** **Exemplu:** Dispozitiv (config-if)#**Sfârşit**	Iese din modul de configurare a interfeței și revine la modul EXEC privilegiat
Pasul 11	**configura terminalul** **Exemplu:** Dispozitiv#**configura terminalul**	Intră în modul de configurare globală.
Pasul 12	**app-hosting app***app_number* **Exemplu:** Dispozitiv (config) #**app-hosting appd app1**	Configurează aplicația și intră în modul de configurare a aplicației.
Pasul 13	**app-vnic gateway0 virtualportgroup 0 interfață pentru oaspeți 0** **Exemplu:** Dispozitiv(config-app-hosting)#**app-vnic gateway0 virtualportgroup 0 interfață pentru oaspeți 0**	Configurați interfața aplicației și gateway-ul aplicației.
Pasul 14	**invitat-adresă-ipad***adresa_ip***mască de rețea***mască de rețea* **Exemplu:** Dispozitiv(config-app-hosting-gateway0)#**guest-ipaddress 192.168.0.2 netmask 255.255.255.0**	Configurați adresa IP a interfeței Ethernet aplicației.
Pasul 15	**app-default-gateway***adresa_ip* **interfață pentru oaspeți 0** **Exemplu:** Dispozitiv(config-app-hosting-gateway0)#**app-default-gateway 192.168.0.1 guest-interfață 0**	Configurați gateway-ul implicit pentru aplicație.
Pasul 16	**Sfârşit** **Exemplu:** Dispozitiv#**Sfârşit**	Iese din modul de configurare a interfeței și revine la modul EXEC privilegiat

Instalarea și dezinstalarea aplicațiilor

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** Dispozitiv>**permite**	Activează modul EXEC privilegiat. Introduceți parola dacă vi se solicită.
Pasul 2	**configura terminalul** **Exemplu:** Dispozitiv#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**app-hosting install *appid****nume-ap/icație*** *pachet****ca/ea pachetului*** **Exemplu:** Dispozitiv#**app-hosting install appid lxc_app package flash:my_iox_app.tar**	Instalează o aplicație din locația specificată. Aplicația poate fi instalată din orice locație de stocare locală, cum ar fi flash, bootflash și usbflashO.
Pasul 4	**app-hosting start appid** *nume-ap/icație* **Exemplu:** Dispozitiv#**app-hosting porniți aplicația appl**	Pornește aplicația. Scripturile de pornire a aplicației sunt activate.
Pasul 5	**app-hosting stop *appid****nume-ap/icație* **Exemplu:** Dispozitiv#**app-hosting opriți aplicația appl**	Oprește aplicația.
Pasul 6	**app-hosting dezactivați appid** *nume-ap/icație* **Exemplu:** Dispozitiv#**app-hosting dezactivați aplicația appl**	Dezactivează toate resursele alocate pentru aplicație.
Pasul 7	**app-hosting uninstall *appid****nume-ap/icație*** **Exemplu:** Dispozitiv#**app-hosting dezinstalează aplicația appl**	Dezinstalează aplicația. Dezinstalează toate ambalajele și imaginile stocate. Toate modificările și actualizările aplicației sunt, de asemenea, eliminate.

Suprascrierea configurației resurselor aplicației

Modificările resurselor vor avea efect numai după configurarea comenzii de activare a găzduirii aplicației.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** Dispozitiv>**permite**	Activează modul EXEC privilegiat. Introduceți parola dacă vi se solicită.
Pasul 2	**configura terminalul** **Exemplu:** Dispozitiv#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**app-hosting app***nume* **Exemplu:** Dispozitiv(config-app-hosting)#**profil de resurse de aplicație personalizat**	Activează găzduirea aplicației și intră în modul de configurare a găzduirii aplicației.
Pasul 4	**profil de resurse de aplicație***nume* **Exemplu:** Dispozitiv#**app-hosting porniți aplicația app1**	Configurați profilul personalizat de resurse de aplicație și intră în modul de configurare a profilului personalizat de resurse de aplicație. Numai numele profilului personalizat este acceptat.
Pasul 5	**CPU***unitate* **Exemplu:** Dispozitiv(config-app-resource-profile-custom)# **CPU 800**	Modifică alocarea implicită a CPU pentru aplicație. Valorile resurselor sunt specifice aplicației și orice ajustare a acestor valori trebuie să asigure că aplicația poate rula fiabil cu modificările.
Pasul 6	**memorie***memorie* **Exemplu:** Dispozitiv(config-app-resource-profile-custom)# **memorie 512**	Modifică alocarea implicită de memorie.
Pasul 7	**vcpu***număr* **Exemplu:** Dispozitiv(config-app-resource-profile-custom)# **vcpu 2**	Modifică alocarea CPU virtuală (vCPU) pentru aplicație.
Pasul 8	**Sfârşit** **Exemplu:** Dispozitiv(config-app-resource-profile-custom)# **Sfârşit**	Iese din modul de configurare a profilului resurselor aplicației personalizate și revine la modul EXEC privilegiat.

Verificarea configurației de găzduire a aplicației

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** Dispozitiv>**permite**	Activează modul EXEC privilegiat. Introduceți parola dacă vi se solicită.
Pasul 2	**configura terminalul** **Exemplu:** Dispozitiv#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**arata iox-service** **Exemplu:** Dispozitiv (config) #**arata iox-service** Rezumatul infrastructurii IOx: – - Serviciu IOx (CAF) 1.8.0.2 : Rulează serviciul IOx (HA) : Serviciul IOx neacceptat (IOxman) : Rulează Libvirtd 1.3.4 : Rulează Dispozitiv#	Afișează starea tuturor serviciilor IOx.

Pasul 4	**afișați detaliile despre găzduirea aplicației**
	
	Exemplu:
	
	Dispozitiv#**afișați detaliile despre găzduirea aplicației** ID
	aplicație : app1
	Proprietar : iox
	Stat : ALLERARE
	Aplicație
	  Tip : lxc
	  Nume : nt08-stres
	  Versiune : 0,1
	  Descriere : Testarea de stres
	 Aplicație
	  Cale : usbflash0:
	my_iox_app.tar
	Nume profil activat: rezervare personalizată a resurselor
	  Memorie : 64 MB
	  Disc : 2 MB
	  CPU : 500 de unități
	Dispozitive atașate
	  Tip Nume
	Alias
	
	--- 	
	
	  serial/shell iox_console_shell
	serial0
	  serial/aux iox_console_aux
	serial1
		Afișează informații detaliate despre aplicație.

	Comanda sau Acțiune	Scop
	serial/syslog iox_syslog serial2 serial/urmă iox_trace serial3 Interfețe de rețea ---------- eth0: adresa MAC : 52:54:dd:fa:25:ee	
Pasul 5	**arată lista de găzduire a aplicațiilor** **Exemplu:** Dispozitiv#**arată lista de găzduire a aplicațiilor** ID aplicație Stat ---------- ------- app1 FUNCȚIONARE	Afișează lista aplicațiilor și starea acestora.

Exemple de configurare pentru găzduirea aplicațiilor

Vedeți următoarele exemple:

Exemplu: Activarea IOx

Dispozitiv>**permite**
Dispozitiv#**configura terminalul**
Dispozitiv (config) #**iox**
Dispozitiv (config) #**server ip http** Dispozitiv
(config) #**ip http server securizat**
Dispozitiv (config) #**nume de utilizator privilegiu cisco 15 parolă 0 cisco**
Dispozitiv (config) #**Sfârşit**

Exemplu: Configurarea unui VirtualPortGroup la un Port de date Layer 3

Dispozitiv>**permite**
Dispozitiv#**configura terminalul** Dispozitiv (config) #**rutare ip** Dispozitiv
(config) #**interfață gigabitethernet 0/0/0** Dispozitiv (config-if)#**fara switchport** Dispozitiv (config-if)#**adresa ip 10.1.1.1 255.255.255.0**
Dispozitiv (config-if)#**Ieșire** Dispozitiv (config) #**interfață virtualportgroup 0** Dispozitiv (config-if)#**adresa ip 192.168.0.1 255.255.255.0** Dispozitiv
(config-if)#**Sfârşit**

Exemplu: Instalarea și dezinstalarea aplicațiilor

Dispozitiv>**permite**

Dispozitiv#**app-hosting instalează appid app1 pachet flash:my_iox_app.tar** Dispozitiv# **app-hosting activați aplicația app1** Dispozitiv#**app-hosting porniți aplicația app1** Dispozitiv#**app-hosting opriți aplicația app1** Dispozitiv#**app-hosting dezactivați aplicația app1** Dispozitiv#**app-hosting dezinstalează aplicația app1**

Exemplu: suprascrierea configurației resurselor aplicației

Dispozitiv#**configura terminalul** Dispozitiv (config) #**app-hosting appd app1** Dispozitiv(config-app-hosting)#**profil de resurse de aplicație personalizat** Dispozitiv(config-app-resource-profile-custom)#**CPU 800** Dispozitiv(config-app-resource-profile-custom)#**memorie 512** Dispozitiv(config-app-resource-profile-custom)#**vcpu 2** Dispozitiv(config-app-resource-profile-custom)#**Sfârşit**

Suport nativ pentru docker

Asistența Native Docker permite utilizatorilor să implementeze aplicațiile docker pe IR1800. Procesul ciclului de viață al aplicației este similar cu procedura din secțiunea Instalarea și dezinstalarea aplicațiilor. Pentru aplicațiile Docker, configurarea punctului de intrare este necesară ca parte a configurației aplicației. Vă rugăm să consultați următorul exemplu pentru configurarea punctului de intrare.

Router#**conf t**
Introduceți comenzile de configurare, una pe linie. Încheiați cu CNTL/Z.
Router(config)#**app-hosting appd app3**
Router(config-app-hosting)#**app-vnic gateway0 virtualportgroup 0 interfață pentru oaspeți 0** Router(config-app-hosting-gateway0)#**guest-ipaddress 192.168.0.7 netmask 255.255.255.0** Router(config-app-hosting-gateway0)# **app-default-gateway 192.168.0.1 guest-interfață 0** Router(config-app-hosting)#**aplicație-resurse docker** Router(config-app-hosting-docker)#**run-opts 1 "--entrypoint '/bin/sleep 10000'"** Router(config-app-hosting-docker)#**Sfârşit** Router#

Ieșirea pentru aplicațiile docker este afișată în următorul exemplu:

Router#**afișați detaliile despre găzduirea aplicației** ID aplicație: app1
Proprietar: iox
Stare: RUNNING
Aplicație
Tip: docker
Nume: aarch64/busybox
Versiune: ultima
Descriere:
Cale: bootflash:busybox.tar Nume profil activat: rezervare personalizată a resurselor
Memorie: 431 MB
Disc: 10 MB
CPU: 577 de unități
VCPU: 1
Dispozitive atașate
Tastați Nume Alias
- serial/shell iox_console_shell serial0 serial/aux iox_console_aux serial1

serial/syslog iox_syslog serial2 serial/trace
iox_trace serial3 Interfețe de rețea

- eth0:

Adresă MAC: 52:54:dd:e9:ab:7a Adresă
IPv4: 192.168.0.7 Nume rețea: VPG0

Docher
- - - - - -
Informații despre timpul de execuție
Comanda:
Punct de intrare: /bin/sleep 10000
Rulați opțiunile în uz: --entrypoint '/bin/sleep 10000' Informații despre
sănătatea aplicației
Stare: 0
Eroare ultima sondă:
Ieșire ultima sondă:
Router#

Digital IO pentru aplicații container IOx

Aplicațiile container IOx pot accesa IO-ul digital. Există un CLI pentru comanda contactului de alarmă.

Router(config)#**contact de alarma?**

<0-4>	Număr de contact pentru alarmă (0: port de alarmă, 1-4: I/O digitală)
atașați-la-iox	Activați accesul la porturile IO digitale de la IOX

Router (configurație)#**contact de alarmă atașat la iox**

Activarea**atașați-la-iox**comanda va oferi control complet al tuturor porturilor digitale IO către IOx. Porturile vor fi expuse ca dispozitive cu patru caractere /dev/dio-[1-4] la aplicațiile IOX. Puteți utiliza funcțiile de citire/scriere pentru a obține/setare valori ale porturilor Digital IO.

Dacă doriți să actualizați modul, puteți scrie valoarea modului în fișierul dispozitivului de caractere. Acest lucru este realizat prin apeluri IOCTL pentru a citi/scrie starea, a schimba modul și a citi adevărata tensiune analogică a portului. Urmând această metodă, puteți atașa senzori analogici la IR1800. Toate porturile sunt setate inițial pe modul de intrare cu tensiunea ridicată la 3,3 V.

Următoarele sunt exemple de apeluri IOCTL:

Citiți portul digital IO:

cat /dev/dio-1

Scrieți pe portul digital IO:

echo 0 > /dev/dio-1 echo
1 > /dev/dio-1

Schimbarea modului:

echo out > /dev/dio-1 echo
in > /dev/dio-1

Lista IOCTL acceptate:

DIO_GET_STATE = 0x1001
DIO_SET_STATE = 0x1002
DIO_GET_MODE = 0x1003
DIO_SET_MODE_OUTPUT = 0x1004
DIO_SET_MODE_INPUT = 0x1005

DIO_GET_THRESHOLD 0x1006
DIO_SET_THRESHOLD = 0x1007
DIO_GET_VOLTAGE = 0x1009

Citiți starea folosind IOCTL:

import fcntl, array
fișier = deschis("/dev/dio-1","rw") stare =
array.array('L',[0]) fcntl.ioctl(fișier,
DIO_GET_STATE, stare) print(stare[0])

Schimbați modul folosind IOCTL:

import fcntl
fișier = deschis("/dev/dio-1","rw") fcntl.ioctl(fișier,
DIO_SET_MODE_OUTPUT, 0)

Asistență pentru aplicații semnate

Aplicațiile Cisco Signed sunt acum acceptate pe IR1800. Pentru a instala o aplicație semnată, verificarea semnată trebuie să fie activată pe dispozitiv. Verificarea semnată poate fi activată urmând următoarele instrucțiuni.

Router#**configura terminalul**
Introduceți comenzile de configurare, una pe linie. Încheiați cu CNTL/Z.
Router(config)#
Router(config)#**verificarea semnată a găzduirii aplicației**
Router(config)#
Router(config)#**Ieșire**

După activarea verificării semnate, urmați instrucțiunile din secțiunea Instalare și dezinstalare aplicații din IOx Application Hosting pentru a instala aplicația.

CAPITOL 23

Serviciul Releu Serial

Acest capitol conține următoarele:

Serviciu de releu serial IOx

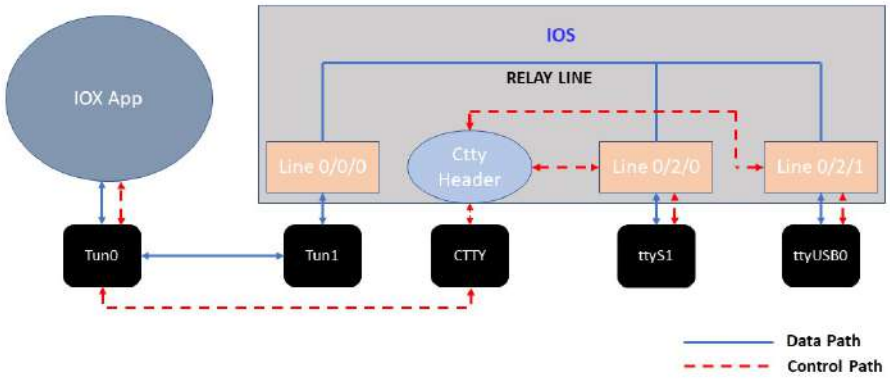
Serviciul IOx Serial Relay de pe IR1800 permite aplicațiilor IOx să comunice cu portul Serial Async (/dev/ttyS1 sau /dev/ttyUSB0 sub IOS-XE). Configurația serviciului IOx Serial Relay este similară cu cea a IR800.

Căile de date

Pe IR1800, IOS-XE are control complet asupra căii de date și a căii de control a portului serial asincron. Acest aspect este esențial pentru alte încapsulări acceptate pe portul Aysnc, cum ar fi PPP, raw-socket, SCADA etc. Aplicației IOx nu i se permite niciodată să exercite control deplin asupra dispozitivului. Toate datele și configurațiile sunt transmise prin IOS-XE înainte de a merge la dispozitiv.

În loc să expună portul serial real la aplicațiile IOx, serviciul de releu serial creează un dispozitiv serial emulat prin software enumerat ca /dev/ttyTun0 (arat mai jos). Perechea de dispozitive /dev/ttyTun0 și /dev/ttyTun1 reprezintă un tunel de date a cărui funcție principală este de a acționa ca un gateway de trecere în timpul oricărui transfer de date. /dev/ttyTun1 este deschis de IOS-XE și toate datele de intrare/ieșire din IOS către aplicație utilizează acest dispozitiv în timpul transferului de date. Linia 0/0/0 este folosită pentru a comunica cu /dev/ttyTun1. Serviciul de releu serial trebuie configurat în prealabil pentru a permite conexiunea între două linii.

Figura 56: Căi de date



Calea datelor:

1.Când aplicația IOx trimite un caracter la /dev/ttyTun0, driverul de tunel împinge automat datele în /dev/ttyTun1.

2.IOS citește datele pe care apoi le transmite serviciului de releu serial.

3.Serviciul de releu serial preia informații despre celălalt capăt al serviciului de releu (linia 0/2/0 sau linia 0/2/1 în acest caz) și transmite datele către buffer-ul liniei.

4.Driverul de linie împinge în mod activ datele în dispozitivul serial real (/dev/ttyS1 sau /dev/ttyUSB0) în funcție de disponibilitatea tamponului.

5.Calea inversă funcționează la fel cu rolurile /dev/ttyS1 sau /dev/ttyUSB0 și /dev/tun0 inversate.

Calea de control:

1.Când aplicația IOx efectuează apelul ioctl TCGETS pe /dev/ttyTun0, driverul de tunel folosește /dev/cttyTun pentru a trimite cererea către serviciul de gestionare CTTY care rulează în IOS.

2.Serviciul de gestionare CTTY și driverul de kernel utilizează o arhitectură client-server pentru a comunica obiectele de configurare.

3.La primirea cererii despre TCGETS de la /dev/cttyTun, handlerul CTTY examinează cererea și solicită conducătorului de linie să completeze datele necesare în structurile de date de control.

4.La primirea structurilor de date de control, handlerul CTTY trimite un răspuns către /dev/cttyTun care se întoarce în cele din urmă la /dev/ttyTun0.

5./dev/ttyTun0 transmite datele de control către aplicația IOx așa cum este solicitat.

6. Cale similară poate fi extrapolată pentru TCSETS, unde handlerul CTTY solicită driverului de linie să actualizeze setările driverului /dev/ttyS1 sau /dev/ttyUSB0 de sub.

7. Driverul de linie al liniei 0/2/0 sau al liniei 0/2/1 și configurația driverului de pe /dev/ttyTun0 sunt întotdeauna sincronizate unul cu celălalt. Orice modificare a configurației, cum ar fi modificarea vitezei de transmisie, este transmisă în mod transparent driverului de linie, fără nicio suprasarcină suplimentară de configurare. Aceasta emulează caracteristica de propagare a releului serial pe seria IR800, unde portul serial virtual poate configura parametrii portului serial real.

Comenzi de configurare

IR1800#**configura terminalul** IR1800(config)#**interfață asincronă 0/2/0** IR1800(config-if)#**linie releu de încapsulare** IR1800(config-if)#**Ieșire** IR1800(config)#**linie de releu 0/2/0 0/0/0** IR1800(config)#**Ieșire**

IR1800#

CAPITOL 24

Suport pentru MACsec

Software acceptat MACsec

Toate routerele existente Cisco IOSXE folosesc transceiver speciale pentru a efectua criptarea și decriptarea MACsec. Software-ul MACsec utilizează infrastructura CDAL în QFP pentru a efectua operațiuni cripto. În comparație cu MACsec suportat hardware, procesul de configurare, stare și calea datelor este efectuat, este diferit ceea ce creează anumite limitări în funcționalitate atunci când este utilizat.

MACsec este acceptat numai pe interfețele L2. Portul MACsec trebuie pus în modul de acces. Pe măsură ce criptarea are loc pe interfața virtuală a comutatorului de ieșire (SVI), VLAN-ul utilizat pentru port ar trebui să fie unic și nicio altă interfață nu trebuie să folosească acel VLAN. Acest lucru se datorează faptului că QFP nu are informații despre tabelul MAC.

Nota

- Deoarece MACsec este realizat prin software, performanța nu este rata de linie pe interfețele L2.
- Cisco acceptă numai*ar trebui să se asigure*Modul MACsec pentru IR1800, care permite trafic necriptat chiar și într-o stare securizată.

  IR1800 nu acceptă*trebuie să se asigure*modul.

Pentru un pachet de ieșire, SVI-ul este conștient de faptul că pachetul trebuie trimis pe un VLAN fără informații despre nicio interfață specifică. Cipul de comutare este cel care decide în ce port îl trimite. Toate pachetele fără eticheta MACsec sunt procesate fără nicio modificare. Pachetele L2 de ieșire vor ieși, de asemenea, fără criptare sau modificare.

Pentru această caracteristică, licența Network Essentials și Network Advantage acceptă GCM-AES-128. Această caracteristică nu este disponibilă rulând imaginea NPE.

Limitări

- MACsec nu este acceptat în modul controler.
- Trebuie să existe un ID vlan unic pentru o interfață MACsec.
- Numai gcm-aes-128 este acceptat

- Atât SCI explicit, cât și non-explicit sunt acceptate pe partea de intrare. IR1800 trimite doar pachete SCI explicite, deoarece nu este un sistem final.
- IR1800 nu acceptă compensarea confidenţialităţii.
- Numai integritatea nu este acceptată.
- Pentru gcm-aes-128, la un pachet criptat sunt adăugați până la 32 de octeți în comparație cu un pachet simplu. Deci, configurația MTU ar trebui să adauge 32 pentru ca acesta să funcționeze corect.
- Cheia MACsec este gestionată de modulul MKA. Pentru acel dispozitiv, necesită o cheie statică pentru ca MKA să negocieze cheia MACsec.
- Nu există suport MIB.
- Cadrul Jumbo nu este acceptat.
- MACsec nu este acceptat pe portul WAN.
- Urmărirea dispozitivului IP (IPDT) nu este acceptată pe gazdă pentru a comuta MACsec

CAPITOL 25

Prezentare generală a monitorului ROM

Prezentare generală a monitorului ROM

The *Monitor ROM* este un program de bootstrap care inițializează hardware-ul și pornește software-ul Cisco IOS XE atunci când porniți sau reîncărcați un router. Când conectați un terminal la routerul care se află în modul ROM Monitor, este afișat promptul ROM Monitor (rommon 1>).

În timpul funcționării normale, utilizatorii nu utilizează modul ROM Monitor. Modul ROM Monitor este utilizat numai în circumstanțe speciale, cum ar fi reinstalarea întregului set de software, resetarea parolei routerului sau specificarea unui fișier de configurare care să fie utilizat la pornire.

The *Software-ul ROM Monitor* este cunoscut sub multe nume. Se numește uneori *ROMMON* din cauza promptului CLI în modul ROM Monitor. Software-ul ROM Monitor se mai numește și *software de pornire*, *imaginea de boot*, sau *ajutor de boot*. Deși este distribuit cu routere care utilizează software-ul Cisco IOS XE, ROM Monitor este un program separat de software-ul Cisco IOS XE. În timpul pornirii normale, monitorul ROM inițializează routerul și apoi controlul trece la software-ul Cisco IOS XE. După ce software-ul Cisco IOS XE preia controlul, monitorul ROM nu mai este utilizat.

Atenţie Pe routerele din seria IR1800, dacă alimentarea este pierdută de 20 de ori la rând în timpul pornirii, routerul va intra în ROM Monitor.

Variabilele de mediu și Registrul de configurare

Există două conexiuni principale între ROM Monitor și software-ul Cisco IOS XE: variabilele de mediu ROM Monitor și registrul de configurare.

Variabilele de mediu ROMMonitor definesc locația software-ului Cisco IOS XE și descriu cum să-l încărcați. După ce ROM Monitor a inițializat routerul, acesta utilizează variabilele de mediu pentru a localiza și încărca software-ul Cisco IOS XE.

The*registrul de configurare*este o setare software care controlează modul în care pornește un router. Una dintre utilizările principale ale registrului de configurare este de a controla dacă routerul pornește în modul ROM Monitor sau în modul Administration EXEC. Registrul de configurare este setat fie în modul ROM Monitor, fie în modul Administration EXEC, după cum este necesar. De obicei, setați registrul de configurare folosind promptul software Cisco IOS XE atunci când trebuie să utilizați modul ROM Monitor. Când întreținerea în modul ROM Monitor este completă, modificați registrul de configurare, astfel încât routerul să repornească cu software-ul Cisco IOS XE.

Accesarea modulului de monitorizare ROM cu o conexiune la terminal

Când routerul este în modul ROM Monitor, puteți accesa software-ul ROM Monitor doar de la un terminal conectat direct la portul de consolă al cardului. Deoarece software-ul Cisco IOS XE (mod EXEC) nu funcționează, interfețele care nu sunt de gestionare nu sunt accesibile. Practic, toate resursele software Cisco IOS XE nu sunt disponibile. Hardware-ul este disponibil, dar nu există nicio configurație pentru a utiliza hardware-ul.

Acces la managementul rețelei și modul monitor ROM

Este important să rețineți că modul ROM Monitor este un mod router, nu un mod în cadrul software-ului Cisco IOS XE. Cel mai bine este să rețineți că software-ul ROM Monitor și software-ul Cisco IOS XE sunt două programe separate care rulează pe același router. În orice moment, routerul rulează doar unul dintre aceste programe.

O zonă care poate fi confuză atunci când utilizați ROM Monitor și software-ul Cisco IOS XE este zona care definește configurația IP pentru interfața Ethernet de gestionare. Majoritatea utilizatorilor se simt confortabil cu configurarea interfeței Management Ethernet în software-ul Cisco IOS XE. Cu toate acestea, când routerul este în modul ROMMonitor, routerul nu rulează software-ul Cisco IOS XE, astfel încât configurația interfeței Ethernet de management nu este disponibilă.

Când doriți să accesați alte dispozitive, cum ar fi un server TFTP, în modul ROM Monitor pe router, trebuie să configurați variabilele ROM Monitor cu informații de acces IP.

Nota Variabilele de acces TFTP nu sunt acceptate în prezent pe platforma IR1800.

Accesați modul monitor ROM

Următoarele secțiuni descriu cum să intrați în modul ROMMON și conțin următoarele secțiuni:

Verificarea versiunii curente ROMMON

Pentru a afișa versiunea ROMmon care rulează pe un router, utilizați**arata rom-monitor**comanda. Pentru a afișa toate variabilele care sunt setate în ROMmon, utilizați**arata romvar**comanda.

```
Router#arată rom-monitorul r0
============================================================

System Bootstrap, versiunea 3.9(REL), LANSAREA SOFTWARE-ului
Copyright (c) 1994-2021 de către cisco Systems, Inc.
```

```
Router#arata romvar
Variabile ROMMON:
PS1 = rommon ! >
THRPUT =
LICENSE_BOOT_LEVEL =
RET_2_RTS =
DEVICE_MANAGED_MODE = autonom
BOOT = bootflash:/ir1800-universalk9.17.06.01prd18.SPA.bin,12; BOOT_STAGED =
bootflash:ir1800-universalk9.17.06.01prd18.SPA.bin BSI = 0

RET_2_RCALTS =
RANDOM_NUM = 231998661

Router#
```

Dacă registrul de configurare a fost setat la valoarea hex 0x0 sau 0x1820, operația de reîncărcare vă va aduce la promptul de comandă al modulului ROMmon (rommon 1>). Invocarea comenzii set la prompt (rommon 1> set) va afișa aceleași informații ca „show romvar” de mai sus în modul exec IOS/XE.

```
rommon 1 >set
PS1=rommon ! >
THRPUT=
LICENSE_BOOT_LEVEL=
RET_2_RTS=
DEVICE_MANAGED_MODE=BOOT autonom=bootflash:/ir1800-
universalk9.17.06.01prd18.SPA.bin,12; BOOT_STAGED=bootflash:ir1800-
universalk9.17.06.01prd18.SPA.bin BSI=0

RANDOM_NUM=231998661
RET_2_RCALTS=1626821700
```

Comenzile de monitorizare ROM utilizate în mod obișnuit

Următorul tabel rezumă comenzile utilizate în mod obișnuit în ROM Monitor. Pentru instrucțiuni specifice despre utilizarea acestor comenzi, consultați procedura relevantă din acest document.

Tabelul 23: Comenzile de monitorizare ROM utilizate în mod obișnuit

Comandamentul ROMMON	Descriere
imaginea de boot	Pornește manual o imagine software Cisco IOS XE.
imagine de pornire –o cale-fișier-config	Pornește manual software-ul Cisco IOS XE cu un fișier alternativ temporar de configurare de administrare.
confreg	Modifică setarea registrului de configurare.
dev	Afișează dispozitivele de stocare locale disponibile.
dir	Afișează fișierele de pe un dispozitiv de stocare.
resetare	Resetează nodul.
set	Afișează setările de mediu ale monitorului ROM setate în prezent.
sincronizare	Salvează noile setări de mediu ale monitorului ROM.
neasezat	Elimină o setare variabilă de mediu.

Exemple

Următorul exemplu arată ce apare când introduceți**?**comanda pe un router:

```
rommon 1 >?
alias                 setați și afișați aliasuri comanda pornire
cizme                 un proces extern de configurare registru
confreg               utilitar listează tabelul dispozitivelor
dev
dir                   listează fișiere în sistemul de fișiere
Ajutor                monitorizează comanda încorporată ajută la
istorie               monitorizarea istoricului comenzii
meminfo               informațiile din memoria principală repetă o
repeta                comandă de monitorizare resetarea
resetare              sistemului
set                   Afișează variabilele monitorului Afișează monitorul
showmon               ROM selectat în prezent scrierea mediului de
sincronizare          monitorizare pe identificatorul unic de simbol al plăcii
jeton                 de afișare NVRAM dezactivați un alias
unalias
neasezat              dezactivați o variabilă de monitor
```

Modificarea promptului monitorului ROM

Puteți modifica solicitarea în modul Monitor ROM folosind**PS1=**comandă așa cum se arată în exemplul următor:

```
rommon 8 > PS1="IR1800 rommon ! > " IR1800
rommon 9 >
```

Modificarea promptului este utilă dacă lucrați cu mai multe routere în ROM Monitor în același timp. Acest exemplu specifică că promptul ar trebui să fie „IR1800 rommon”, urmat de numărul liniei și apoi urmat de „ > “ de numărul liniei.

Afișarea setării registrului de configurare

Pentru a afișa setarea curentă a registrului de configurare, introduceți**confreg**comandă fără parametri după cum urmează:

```
rommon >confreg
Rezumatul configurației
(Registrul de configurare virtuală: ) activate
sunt:
[ 0 ] break/abort are efect [ 1 ] baud
console: 9600 boot:..... the ROM
Monitor
vrei sa schimbi configuratia? y/n                    [n]:
```

Setarea registrului de configurare este etichetată*Registrul de configurare virtuală*. Introduceți**nu**comandă pentru a evita modificarea setării registrului de configurare.

Setări variabile de mediu

Variabilele de mediu ROMMonitor definesc atributele ROMMonitor. Variabilele de mediu sunt introduse ca și comenzi și sunt întotdeauna urmate de semnul egal (=). Setările variabilelor de mediu sunt introduse cu majuscule, urmate de o definiție. De exemplu:

IP_ADDRESS=10.0.0.2

În condiții normale de funcționare, nu este necesar să modificați aceste variabile. Acestea sunt șterse sau setate numai atunci când trebuie să faceți modificări în modul în care funcționează ROM Monitor.

Această secțiune include următoarele subiecte:

Variabile de mediu utilizate frecvent

Următorul tabel prezintă principalele variabile de mediu ROM Monitor. Pentru instrucțiuni despre cum să utilizați aceste variabile, consultați instrucțiunile relevante din acest document. Încărcătorul de pornire IR1800 nu acceptă pornirea prin net, deci nu se utilizează nicio setare precum următoarele variabile de mediu:

- IP_ADDRESS
- IP_SUBNET_MASK
- DEFAULT_GATEWAY
- TFTP_SERVER
- TFTP_FILE

Tabelul 24: Variabilele de mediu utilizate frecvent ROM Monitor

Variabila de mediu	Descriere
BOOT=cale/fișier	Identifică software-ul de pornire pentru un nod. Această variabilă este de obicei setată automat când routerul pornește.

Afișarea setărilor variabilelor de mediu

Pentru a afișa setările curente ale variabilei de mediu, introduceți**set**comanda:

rommon 1 >**showmon**
System Bootstrap, versiunea 3.9(REL), LANSAREA SOFTWARE-ului
Copyright (c) 1994-2021 de către cisco Systems, Inc.

Platformă IR1833-K9 cu 4194304 Kbytes de memorie principală

Versiune MCU - Bootloader: 22, Aplicație: 4D MCU
este în modul aplicație.

Introducerea setărilor pentru variabilele de mediu

Setările variabilelor de mediu sunt introduse cu majuscule, urmate de o definiție. Următorul exemplu arată variabilele de mediu care pot fi configurate în modul ROMmon.

rommon 1 >**confreg 0x0** rommon 1>**BOOT_WDOG = DEZACTIVAT** rommon 1>**BOOT = IR1800-K9_image_name**

Salvarea setărilor variabilelor de mediu

Pentru a salva setările curente ale variabilei de mediu, introduceți**sincronizare**comanda:

rommon >**sincronizare**

Nota Valorile de mediu care nu sunt salvate cu**sincronizare**comanda sunt eliminate ori de câte ori sistemul este resetat sau pornit.

Ieșire din modul monitor ROM

Pentru a ieși din modul ROM Monitor, trebuie să modificați registrul de configurare și să resetați routerul.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**confreg** **Exemplu:** rommon 1>**confreg**	Inițiază solicitările de configurare a registrului de configurare.
Pasul 2	Răspundeți la fiecare solicitare conform instrucțiunilor.	Consultați exemplul care urmează această procedură pentru mai multe informații.
Pasul 3	**resetare** **Exemplu:** rommon 2>**resetare**	Resetează și inițializează routerul.

Exemplu de configurare ROMMON

```
rommon 3 >confreg
Rezumatul configurației
(Registrul de configurare virtuală: 0x0) activate
sunt:
  [ 0 ] break/abort are efect [ 1 ] baud
  console: 9600 boot: ..... monitorul
  ROM
vrei sa schimbi configuratia? activați y/n                    [n]:    y
                „modul de diagnosticare”? y/n [n]: „utilizați
  permite       rețeaua în adresa IP bcast”? y/n „încărcare rom  [n]:
  permite       după ce netboot eșuează”? y/n „utilizați toate   [n]:
  permite       emisiunile zero”? y/n                            [n]:
  dezactivați „break/abort are effect”? y/n activați             [n]:
  „ignorați informațiile de configurare a sistemului”? da/n      [n]:
  schimba viteza de transmisie a consolei? y/n [n]:
schimbați caracteristicile boot-ului? y/n [n]: Rezumatul
configurației
(Registrul de configurare virtuală: 0x0) activate
sunt:
  [ 0 ] break/abort are efect [ 1 ] baud
  console: 9600 boot: ..... monitorul
  ROM
vrei sa schimbi configuratia? y/n                              [n]:
```

Actualizarea ROMmon pentru un router

Upgrade-ul ROMmon pe routerul IR1800-K9 se face automat când imaginea este pornită. Cea mai recentă versiune a ROMmon este inclusă cu imaginea IOSXE. Un algoritm detectează dacă versiunea curentă care rulează este mai veche decât versiunea inclusă, dacă da, este actualizată automat. Dacă versiunea curentă care rulează este egală cu versiunea inclusă, nu se execută nicio actualizare. Pentru fiecare actualizare reușită, routerul este repornit automat pentru ca noua versiune să fie încărcată și executată.

Procedură

Pasul 1 (Opțional) Rulați**arata rom-monitor***slot*comanda de pe router pentru a vedea numerele de ediție curente ale ROMmon pe hardware. VeziVerificarea versiunii curente ROMMON, la pagina 298pentru informații despre interpretarea rezultatului comenzii pe care o executați.

Pasul 2 Dacă autoboot nu a fost activat utilizând**config-register 0x2102**comanda, rulează**cizme** *sistem de fișiere://locație-fișier* comanda la promptul ROMmon pentru a porni imaginea Cisco IOS XE, unde *sistem de fișiere://locație-fișier*este calea către fișierul pachet consolidat. Actualizarea ROMmon nu este permanentă pentru nicio piesă hardware până când imaginea Cisco IOS XE nu este pornită.

Pasul 3 Rulați**permite**comanda la promptul utilizatorului pentru a intra în modul EXEC privilegiat după finalizarea pornirii.

Pasul 4 Rulați**arata rom-monitor***slot*comandă pentru a verifica dacă ROMmon a fost actualizat.

CAPITOL 26

Suport pentru agent NMS de rețea conectată (CGNA).

Acest capitol conține următoarele secțiuni:

Suport pentru agent NMS de rețea conectată (CGNA).

CGNA este un subsistem care rulează pe IOS care oferă conectivitate și manevrabilitate cu un sistem de gestionare a rețelei precum FND și IOT Operations Dashboard. Seturi complete de documentație pentru IoT Field Network Director și IoT Industrial Network Director pot fi găsite în următoarele link-uri:

https://www.cisco.com/c/en/us/support/cloud-systems-management/iot-field-network-director/series.html

https://www.cisco.com/c/en/us/support/cloud-systems-management/industrial-network-director/series.html#%7Etab-documents

Prezentare generală CGNA

Majoritatea caracteristicilor sunt implementate pe IR1800, inclusiv profilul de bază, profilul de execuție, profilul bătăilor inimii și descărcarea firmware-ului. Unele caracteristici precum bspatch nu vor fi importate pe IR1800 din cauza limitării imaginii IOS.

CGNA are patru profiluri diferite pentru diferite cazuri de utilizare. Sunt:

- Profil - Acesta este profilul de bază. Poate fi configurat să accepte furnizarea de tunel, înregistrarea și actualizarea periodică.
- Profil de execuție - Acesta poate fi configurat pentru a executa comenzi CLI
- Profil ritm cardiac - Acesta poate fi configurat pentru a trimite mesaje ritm cardiac
- Profil de transport - Acesta poate fi configurat pentru a oferi un protocol de transport diferit pentru profilul de bază de utilizat. În prezent, acceptă doar WebSocket.

CGNA oferă, de asemenea, CLI pentru preluarea imaginilor reluabile din sistemul de management al rețelei și un server SNMP simplu pentru redirecționarea evenimentelor către conexiunea WebSocket.

Suport WebSocket

IOS tradițional a furnizat serviciul WebSocket în nucleul IOSd. Polaris IOS-XE mută serviciul WebSocket din nucleul IOSd pentru o performanță îmbunătățită. Versiunea websocket va fi actualizată la 3.2.3.

CAPITOL 27

Ieșire CLI pentru modemul FN980 5G

Modificare a ieșirii CLI pentru modemul FN980 5G

Această versiune are o ieșire diferită de cea a**arată banda radio celulară 0/x/0**comanda. Modulul nu va mai afișa informațiile despre banda 5G-SA în mod implicit. Cu toate acestea, odată ce 5G-SA a fost activat, informațiile despre bandă vor fi afișate.

Vedeți următoarele exemple de comandă folosind un IR1101 care rulează IOS XE 17.13.1 cu un modem FN980:

IR1101#**arată banda radio celulară 0/1/0**

Benzile LTE acceptate de modem:
- Benzi 2 4 5 12 14 26 29 30 46 48 66.
Setări de preferință pentru banda LTE pentru sim activ (slot 1):
- Benzi 2 4 5 12 14 26 29 30 46 48 66.

Benzile NR5G NSA acceptate de modem:
- Benzi 2 5 12 66 77.
NR5G NSA band Setări de preferință pentru sim activ (slot 1):
- Benzi 2 5 12 66 77.

Benzile 3G acceptate de modem:
Index: <niciun>
Setări de preferință pentru banda 3G pentru sim activ (slot 1): Index:
<niciun>

========== Lista de
referință pentru indexul benzilor:

Pentru LTE și 5G, indicii 1-128 corespund benzilor 1-128.

Pentru 3G, indicii 1-64 se corelează cu benzile 3G menționate față de fiecare mai sus.

IR1101#

IR1101#**arata mobil 0/1/0 greu**

* 8 noiembrie 12:13:31.969: Modem Graphit 5G RSRP/RSRQ LTE:[1] Versiune
firmware modem = M0H.030202
Versiune firmware gazdă = A0H.000302 ID
model dispozitiv = FN980
International Mobile Subscriber Identity (IMSI) = 001010123456789 International Mobile
Equipment Identity (IMEI) = 359661100035795

ID card de circuit integrat (ICCID) = 89860000502000180722 Servicii integrate
pentru abonat mobil
Digital Network-Number (MSISDN) = Stare
modem = Modem online Temperatura curentă a
modemului = 40 grade C
Versiunea PRI = 1080-114, Carrier = Versiune GCF OEM PRI
generică = 1080-114
IR1101#

IR1101#**arată banda radio celulară 0/1/0**

Benzile LTE acceptate de modem:
- Benzi 1 2 3 4 5 7 8 12 13 14 17 18 19 20 25 26 28 29 30 32 34 38 39 40 41 42 43 46 48 66 71.
Setări de preferință pentru banda LTE pentru sim-ul activ (slot 0):
- Benzi 1 2 3 4 5 7 8 12 13 14 17 18 19 20 25 26 28 29 30 32 34 38 39 40 41 42 43 46 48 66 71.

Benzile NR5G NSA acceptate de modem:
- Benzi 1 2 3 5 7 8 12 20 25 28 38 40 41 48 66 71 77 78 79. Banda NR5G NSA Setări de preferință pentru sim activ (slot 0):
- Benzi 1 2 3 5 7 8 12 20 25 28 38 40 41 48 66 71 77 78 79.

Benzile NR5G SA acceptate de modem:
- Benzi <niciuna>
Setări de preferință pentru banda NR5G SA pentru sim activ (slot 0):
- Benzi <niciuna>

Benzile 3G acceptate de modem:
Index:
23 - Banda UMTS 1: 2100 MHz (IMT) 24 - Banda UMTS 2: 1900 MHz (PCS AF) 26 - Banda UMTS 4: 1700 MHz (AWS AF) 27 - Banda UMTS 5: US 850 MHz (CLR) 50 - Banda UMTS 08 MHz (UMTS 1:-9SM) Banda 9: Japonia 1700 MHz 61 - UMTS Banda 19: 800 MHz (800 Japonia)

Setări de preferință pentru banda 3G pentru sim activ (slot 0): Index:

23 - Banda UMTS 1: 2100 MHz (IMT) 24 - Banda UMTS 2: 1900 MHz (PCS AF) 26 - Banda UMTS 4: 1700 MHz (AWS AF) 27 - Banda UMTS 5: US 850 MHz (CLR) 50 - Banda UMTS 08 MHz (UMTS 1:-9SM) Banda 9: Japonia 1700 MHz 61 - UMTS Banda 19: 800 MHz (800 Japonia)

==========

Lista de referințe pentru indexul benzilor:

Pentru LTE și 5G, indicii 1-128 corespund benzilor 1-128.

Pentru 3G, indicii 1-64 se corelează cu benzile 3G menționate față de fiecare mai sus.

IR1101#

CAPITOL 28

Apărarea unificată împotriva amenințărilor

Apărarea unificată împotriva amenințărilor (UTD)

Unified Threat Defense (UTD) este soluția principală de securitate a rețelei Cisco, care oferă o suită cuprinzătoare de caracteristici de securitate, cum ar fi:

- Firewall Enterprise
- IPS/IDS
- Protecție avansată împotriva programelor malware
- Filtrare URL
- Securitate DNS

UTD este disponibil pe routerul IR1835.

Limitări IR1835

Următoarele sunt limitări specifice produsului:

- Containerul UTD necesită un spațiu minim de 1,8 GB.
- UTD este acceptat atât în modul autonom, cât și în modul controler, dar în modul autonom, sunt acceptate doar funcțiile IPS/IDS.
- Configurația UTD acceptă numai profilul Cloud-Low.
- Baza de date cu filtrare web On-Box nu este acceptată.
- Proxy-ul SSL nu este acceptat.

Licență și caracteristici acceptate

Pentru a activa funcțiile UTD, este necesară licența DNA Essentials, pe lângă Network Essentials. Licența este necesară doar în sd-router (mod autonom).

Dacă se dorește și Cisco Secure Malware Analytics, atunci este necesară licența DNA Advantage, pe lângă Network Advantage.

Configurare caracteristică

Configurația pe IR1835 este aceeași ca la alte produse. Pentru informații vă rugăm să consultați:

- Sistem de prevenire a intruziunilor
- Filtrare URL
- Protecție avansată împotriva programelor malware

CAPITOL 29

Suport pentru modurile CAPWAP și WGB pe modulul de interfață Wi-Fi Cisco

Suport pentru modurile CAPWAP și WGB pe modulul de interfață Wi-Fi Cisco

Modulul de interfață Wi-Fi Cisco (WIM) este un modul de interfață conectabil disponibil pentru toate modelele din seria IR1800. Identificatorul de produs (PID) este WP-WIFI6-x unde x înseamnă domeniul de reglementare. Pentru mai multe informații despre WIM, consultațiGhid de configurare Cisco Wi-Fi Interface Module (WIM)..

Cisco IOS XE versiunea 17.14.1 acceptă:

1.Comutați modul de funcționare între Controlul și furnizarea punctelor de acces fără fir (CAPWAP) și Workgroup Bridge (WGB).

2.Resetarea din fabrică și ștergerea configurației.

3.Configurați radiourile pentru operațiunile WGB uplink și mod concomitent Root AP.

Următorul tabel rezumă suportul de gestionare pentru operațiunile Modulului Wi-Fi în IR1800:

Moduri	**WIM IOS XE Eliberare**	**Router IOSXE Eliberare**	**Sprijin**
Controlul și furnizarea punctelor de acces wireless (CAPWAP) Modul	17.11.0.155 și mai târziu	17.13.1 și mai târziu	Controler LAN wireless Cisco.
Wireless încorporat Modul controler (EWC).	17.11.0.155 și mai târziu	17.13.1 și mai târziu	IOS XE CLI vManage (mod controler SDWAN).
Modul Work Group Bridge (WGB).	17.11.0.155 și mai târziu	17.13.1	Tabloul de bord Cisco IoT Operations.
		17.14.1	Tabloul de bord Cisco IoT Operations. IOS XE CLI vManage (modurile SDWAN și SD-Routing).

Suport pentru modurile CAPWAP și WGB pe modulul de interfață Wi-Fi Cisco

Suport de management pentru Cisco WIM în modul CAPWAP

- Când funcționează în modul CAPWAP, modulul funcționează ca un punct de acces gestionat de un controler LAN fără fir Cisco IOS XE extern, dobândind o adresă IP prin DHCP și descoperind controlerul folosind Layer 3, DHCP, DNS sau transmisie subrețea IP.
- Configurarea serverului DHCP și Switch Virtual Interface (SVI) pe router pentru WIM este necesară pentru ca modul CAPWAP pentru ca WIM să descopere și să comunice cu controlerul LAN fără fir.

Nota Schimbarea modului de la modul CAPWAP la modul WGB este acceptată numai atunci când modulul este în configurația implicită din fabrică.

Pentru mai multe informații, veziControlul și furnizarea punctelor de acces fără fir (CAPWAP).

Suport de management pentru Cisco WIM în modul EWC

- Modulul Wi-Fi acționează ca un controler LAN fără fir Cisco IOS XE în modul Controler fără fir încorporat (EWC), acceptând configurarea din versiunea IOS XE 17.13.1.

Nota Modulul Wi-Fi în modul EWC nu acceptă trecerea la modul CAPWAP sau WGB.

Pentru mai multe informații, veziControler LAN fără fir.

Pentru mai multe informații, veziModul EWC.

Suport IPv6

Din Versiunea 17.16.1a, modelul vManage și Yang acceptă atât configurația IPv6 statică, cât și dinamică în modul WGB.

Puteți configura IPv6 pe WIM în modul WGB de la router la:

- obțineți adrese IPv6,
- colectați valori și
- vizualizați detaliile de configurare.

Utilizațiafișează clienții wireless-bridge,arată interfața wireless-bridge ipv4, șispectacol interfață wireless-bridge ipv6comenzi de pe router pentru a vizualiza detaliile de configurare IPv4 și IPv6 client.

Pentru mai multe informații despre configurarea adresei IPv6, consultațiConfigurați adresa IPv6.

Suport de management pentru Cisco WIM în modul WGB

Următoarea secțiune descrie noile opțiuni de configurare disponibile pe IR1800 pentru implementarea modulului de interfață CiscoWi-Fi în modul WGB.

Configurarea IR1800 pentru implementarea WGB

Următoarea secțiune arată cum să configurați IR1800 pentru implementarea WGB:

Configurarea unui profil QoS

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** router#**permite**	Activează modul EXEC privilegiat.
Pasul 2	**configura terminalul** **Exemplu:** router#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**submod wireless-bridge** **Exemplu:** router(config)#**punte fără fir**	Intră în modul de configurare wireless-bridge.
Pasul 4	**qos-profil***qos-profile-name***{bronz | aur | platină | argint }** **Exemplu:** router(config-wl-bridge)#**qos-profile test-qos-profile bronz**	Creați un profil QoS cu unul dintre nivelurile politicii QoS.
Pasul 5	**Sfârşit** **Exemplu:** router(config-wl-bridge)#**Sfârşit**	Iese din modul de configurare a podului wireless și revine la modul EXEC privilegiat.

Configurarea unui profil SSID cu autentificare deschisă fără un profil QoS mapat

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:**	Intră în modul EXEC privilegiat.

	Comanda sau Acțiune	Scop
	router#**permite**	
Pasul 2	**configura terminalul** **Exemplu:** router#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**submod wireless-bridge** **Exemplu:** router(config)#**punte fără fir**	Intră în modul de configurare wireless-bridge.
Pasul 4	**ssid-profil***nume-profil-ssid***ssid***nume-ssid* | **autentificare deschisă** **Exemplu:** router(config-wl-bridge)#**ssid-profile test-ssid-profile ssid test-ssid autentificare deschisă**	Creați un profil SSID cu autentificare deschisă.
Pasul 5	Sfârşit **Exemplu:** router(config-wl-bridge)#**Sfârşit**	Iese din modul de configurare a podului wireless și revine la modul EXEC privilegiat.

Configurarea unui profil SSID cu autentificare deschisă cu un profil QoS mapat

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** router#**permite**	Intră în modul EXEC privilegiat.
Pasul 2	**configura terminalul** **Exemplu:** router#**configura terminalul**	Intră în modul de configurare globală.

	Comanda sau Acțiune	Scop
Pasul 3	**submod wireless-bridge** **Exemplu:** router(config)#**punte fără fir**	Intră în modul de configurare wireless-bridge.
Pasul 4	**ssid-profil***nume-profil-ssid***ssid***nume-ssid* **qos-profil***qos-profile-name***autentificare deschisă** **Exemplu:** router(config-wl-bridge)#**ssid-profile test-ssid-profile ssid test-ssid qos-profile test-qos-profile** **autentificare deschisă**	Creați un profil SSID cu autentificare deschisă cu un profil QoS mapat.
Pasul 5	Sfârşit **Exemplu:** router(config-wl-bridge)#**Sfârşit**	Iese din modul de configurare a podului wireless și revine la modul EXEC privilegiat.

Configurarea unui profil SSID cu autentificare personală WPA2 fără un profil QoS mapat

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** router#**permite**	Intră în modul EXEC privilegiat.
Pasul 2	**configura terminalul** **Exemplu:** router#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**submod wireless-bridge** **Exemplu:** router(config)#**punte fără fir**	Intră în modul de configurare wireless-bridge.

	Comanda sau Acțiune	Scop
Pasul 4	**ssid-profil***nume-profil-ssid***ssid***nume-ssid* **autentificare psk key-management wpa2 cheie secretă {0 | 6 | 7}***cheie secretă* **Exemplu:** router(config-wl-bridge)#**ssid-profile test-ssid-profile ssid test-ssid autentificare psk key-management wpa2 secret-key 0 testkey123!**	Creați un profil SSID cu autentificare PSK. • 0: Specifică o cheie secretă necriptată va urma. • 6: Specifică o cheie secretă criptată care va urma. • 7: Specifică o cheie secretă ascunsă care va urma.
Pasul 5	Sfârşit **Exemplu:** router(config-wl-bridge)#**Sfârşit**	Iese din modul de configurare a podului wireless și revine la modul EXEC privilegiat.

Configurarea unui profil SSID cu autentificare personală WPA2 cu un profil QoS mapat

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** router#**permite**	Intră în modul EXEC privilegiat.
Pasul 2	**configura terminalul** **Exemplu:** router#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**submod wireless-bridge** **Exemplu:** router(config)#**punte fără fir**	Intră în modul de configurare wireless-bridge.
Pasul 4	**ssid-profil***nume-profil-ssid***ssid***nume-ssid***autentificare** **psk key-management wpa2 cheie secretă {0 | 6 | 7}***cheie secretă* **Exemplu:** router(config-wl-bridge)#**ssid-profile test-ssid-profile ssid test-ssid**	Creați un profil SSID cu autentificare PSK **qos-profil***qos-profile-name***autentificare**cu profilul QoS mapat. • 0: Specifică o cheie secretă necriptată urmează. • 6: Specifică o cheie secretă criptată urmează.

	Comanda sau Acțiune	Scop
	qos-profile qos-profile-test autentificare psk key-management wpa2 secret-key 0 testkey123!	• 7: Specifică o cheie secretă ascunsă care va urma.
Pasul 5	Sfârşit **Exemplu:** router(config-wl-bridge)#**Sfârşit**	Iese din modul de configurare a podului wireless și revine la modul EXEC privilegiat.

Configurarea unei radio Dot11 în modul WGB și configurarea diferiților parametri

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** router#**permite**	Intră în modul EXEC privilegiat.
Pasul 2	**configura terminalul** **Exemplu:** router#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**submod wireless-bridge** **Exemplu:** router(config)#**punte fără fir**	Intră în modul de configurare wireless-bridge.
Pasul 4	**dot11radio {0|1} modul {wgb } ssid-profile** *nume de profil ssid* **Exemplu:** router(config-wl-bridge)#**dot11radio 1 mod wgb ssid-profile test-ssid-profile**	Configurați un Dot11Radio ca WGB.
Pasul 5	**dot11radio {0|1} {activați | dezactivare }** **Exemplu:** router(config-wl-bridge)#**activare dot11radio 1**	Activarea Dot11Radio.

	Comanda sau Acțiune	Scop
Pasul 6	**canalul dot11radio {0|1}***număr canal canal-lățime* **Exemplu:** router(config-wl-bridge)#**dot11radio 1 canal 40 40**	Configurați detaliile unui canal Dot11Radio.
Pasul 7	Sfârşit **Exemplu:** router(config-wl-bridge)#**Sfârşit**	Iese din modul de configurare a podului wireless și revine la modul EXEC privilegiat.

Configurarea unui Dot11Radio în modul uWGB și configurarea diferiților parametri

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** router#**permite**	Activează modul EXEC privilegiat.
Pasul 2	**configura terminalul** **Exemplu:** router#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**submod wireless-bridge** **Exemplu:** router(config)#**punte fără fir**	Intră în modul de configurare wireless-bridge.
Pasul 4	**dot11radio {0|1} mod {uwgb }***HHH* **ssid-profil***nume de profil ssid* **Exemplu:** router(config-wl-bridge)#**dot11radio 1 mod uwgb E462.C49F.9AA0 ssid-profile test-ssid-profile**	Configurați un Dot11Radio ca uWGB.
Pasul 5	**dot11radio {0|1} {activați | dezactivare }** **Exemplu:**	Activarea Dot11Radio.

	Comanda sau Acțiune	Scop
	router(config-wl-bridge)#**activare dot11radio 1**	
Pasul 6	**canalul dot11radio {0|1}***număr canal canal-lățime* **Exemplu:** router(config-wl-bridge)#**dot11radio 1 canal 40 40**	Configurați detaliile unui canal Dot11Radio.
Pasul 7	**Sfârşit** **Exemplu:** router(config-wl-bridge)#**Sfârşit**	Iese din modul de configurare a podului wireless și revine la modul EXEC privilegiat.

Configurarea unei radio Dot11 în modul Root AP și configurarea diferiților parametri

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** router#**permite**	Activează modul EXEC privilegiat.
Pasul 2	**configura terminalul** **Exemplu:** router#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**submod wireless-bridge** **Exemplu:** router(config)#**punte fără fir**	Intră în modul de configurare wireless-bridge.
Pasul 4	**dot11radio {0|1} mod {root-ap}** **Exemplu:** router(config-wl-bridge)#**dot11radio 0 mod root-ap**	Configurați un Dot11Radio ca Root AP. Root AP plasează puntea în modul punct de acces. În acest mod, bridge-ul emulează un punct de acces Cisco Aironet seria 1100 și acceptă asocieri de la dispozitivele client.
Pasul 5	**dot11radio {0|1} {activați | dezactivare }** **Exemplu:** router(config-wl-bridge)#**dot11radio 0 activare**	Activarea Dot11Radio.

	Comanda sau Acțiune	Scop
Pasul 6	**dot11radio {0|1} wlan***wlan-profile-name wlan-id (2-16)***vlan***vlan-id (2-4094)* **Exemplu:** router(config-wl-bridge)#**dot11radio 0 wlan test-wlan-profile 4 vlan 400**	Mapați un profil WLAN la Dot11Radio în modul Root AP.
Pasul 7	**canalul dot11radio {0|1}***număr canal canal-lățime* **Exemplu:** router(config-wl-bridge)#**dot11radio 0 canal 5 20**	Configurați detaliile unui canal Dot11Radio.
Pasul 8	**Sfârşit** **Exemplu:** router(config-wl-bridge)#**Sfârşit**	Iese din modul de configurare a podului wireless și revine la modul EXEC privilegiat. **Nota** 1. Comanda de mai sus face legătura între crearea VLAN-ului în clientul care servește radio la wired0, redirecționarea traficului clientului wireless direct către router. 2. ID-urile WLAN variază de la 2 la 16 (suportă maxim 15 WLAN-uri). Configurațiile legate de Root AP vor intra în vigoare numai după comutarea radioului Root AP. 3. Activarea etichetării Broadcast în WGB va împiedica AP-ul rădăcină să accepte conexiuni client wireless. Configurația de etichetare a difuzării este dezactivată în mod implicit.

Configurați adresa IPv4

Utilizați această sarcină pentru a configura adresa IPv4 pe WIM în modul WGB de la router.

Procedură

Pasul 1 Utilizați**permite**comanda pentru a activa modul EXEC privilegiat.

router#**permite**

Pasul 2 Utilizați**configura terminalul**comanda pentru a intra în modul de configurare globală.

router#**configura terminalul**

Pasul 3 Utilizați**punte fără fir**comanda pentru a intra în modul de configurare a podului fără fir.

router(config)#**punte fără fir**

Pasul 4 Utilizați**adresa wgb ipv4 static***ipaddress netmask gateway*comandă pentru a configura o adresă IPv4 statică împreună cu masca de rețea și gateway-ul implicit.

router(config-wl-bridge)#**adresa wgb ipv4 static 10.10.10.2 255.255.255.0 10.10.10.1**

Pasul 5 Utilizați**adresa wgb ipv4 dhcp**comandă pentru a configura adresa IPv4 DHCP.

router(config-wl-bridge)#**adresa wgb ipv4 dhcp**

Configurați adresa IPv6

Utilizați această sarcină pentru a configura adresa IPv6 pe WIM în modul WGB de la router.

Procedură

Pasul 1 Utilizați**permite**comanda pentru a activa modul EXEC privilegiat.

router#**permite**

Pasul 2 Utilizați**configura terminalul**comanda pentru a intra în modul de configurare globală.

router#**configura terminalul**

Pasul 3 Utilizați**punte fără fir**comanda pentru a intra în modul de configurare a podului fără fir.

router(config)#**punte fără fir**

Pasul 4 Utilizați**adresa wgb ipv6 static***ipaddress netmask gateway*comandă pentru a configura o adresă IPv6 statică împreună cu masca de rețea și gateway-ul implicit.

router(config-wl-bridge)#**adresa wgb ipv6 static 2000:100::10 64 2000:100::1**

Pasul 5 Utilizați**adresa wgb ipv6 dhcp**comandă pentru a configura adresa DHCP IPv6.

router(config-wl-bridge)#**adresa wgb ipv6 dhcp**

Verificați configurația modulului WGB, monitorizarea stării operaționale

Utilizați următoarele comenzi pentru a verifica starea configurației:

Comanda: arată run-config | sec wireless-bridge

Exemplu:

router#**arată run-config | sec wireless-bridge**

Utilizați următoarele comenzi pentru monitorizarea stării de funcționare:

Comanda: arată starea podului wireless

Exemplu:

router#**arată starea podului wireless** Modul
de operare: modul WGB Stare modul
: Modul stare gata

Versiune software : 17.11.0.155
Starea sesiunii de modul: Conectare reușită

Comanda: afișează rețelele WLAN wireless-bridge

Exemplu:

```
router#afișează rețele wireless-bridge
 wlan band oper vlan #client wlan-mode SSID
 ------------------------------------------------------------------
    2 2,4 g în sus          2          1 downlink myssid
```

Comanda: arată clienții wireless-bridge

Exemplu:

Din Versiunea 17.16.1a, Cisco WIM introduce suport pentru IPv6, iar adresele IPv4 și IPv6 sunt vizibile în ieșire.

```
router#afișați clienții wireless-bridge Client-
 MAC-Addr adresa de stare a benzii          wlan  DeviceType  SSID       adresa IPV4      IPV6

 ------------------------------------------------------------------------------------------
---------------------- E4:62:C4:9F:68:CF
 5g Asociat FE80::EDA6:F758:9C25:8539       3     fără fir    000_bba    30.30.30.2
```

Nota vManage nu acceptă vizualizarea detaliilor de configurare IPv4 și IPv6 client.

Comanda: Folosiți**arată interfața wireless-bridge ipv4**comandă pentru a vizualiza detaliile interfeței IPv4.

Exemplu:

```
router#arata interfata wireless-bridge Interfata ipv4
                  Adresa IP       Metodă      Stare       Protocol    Viteză
 Duplex
cu fir0           nealocate       neasezat    Sus         Sus         1000
 deplin
auxiliar-client   20.20.20.5      DHCP        Sus         Sus         N / A
 N / A
service-vlan      N / A           N / A       Sus         Sus         N / A
 N / A
apr0v0            N / A           N / A       Sus         Sus         N / A
 N / A
apr1v0            N / A           N / A       Sus         Sus         N / A
 N / A
```

Comanda: Folosiți**arată interfața wireless-bridge ipv6**comandă pentru a vizualiza detaliile interfeței IPv6.

Exemplu:

```
router#arată interfața wireless-bridge ipv6 srcr2
          Capacitate link: Ethernet      HWaddr E4:62:C4:9F:52:40 Bcast:20.20.20.255
          inet adresa:20.20.20.5         Masca:255.255.255.0
          inet6 addr: 3000:100::9d98:c2e:5a8f:1351/128 Domeniu de aplicare:Global
          inet6 addr: 3000:100::c132:d20b:b520:3537/128 Domeniu de aplicare:Global
          inet6 addr: fe80::18c:5b82:4cef:c56c/64 Domeniu de aplicare:Link inet6
          addr: 3000:100::5996:1093:a134:ea8c/128 Domeniu de aplicare:RUNARE
          GLObal UP BROADCAST MULTICAST MTU:1500
          Pachete RX:5042 erori:0 scăpat:0 depășiri:0 cadru:0 Pachete TX:4841
          erori:0 scăpat:0 depășiri:0 transportator:0
```

coliziuni:0 txqueuelen:0
Octeți RX: 565722 (552,4 KiB) Octeți TX: 556927 (543,8 KiB)

Comanda: Folosiți**arată configurația de rulare a podului fără fir**comanda pentru a vizualiza configurația și starea operațională

Exemplu:

router#**arată configurația de rulare a podului fără fir**
 # # # WGB Running config - Nume gazdă: dispozitiv ###

configurați managementul apei adăugați numele de utilizator Parola Cisco1 $1$$r0JYqf7z0bIzm/v2jcqVp/ secret 1 $cN9KzIWhwzaBqoL.xelgi1
configurați adresa ap ipv6 dhcp configurați
profilul qos qos-profile1 gold
configura ssid-profile wlan2 ssid 000_aab autentificare deschis configura ssid-profile wlan3 ssid 000_bba autentificare deschis configura dot11Radio 0 mod wgb ssid-profile wlan2 configura dot11Radio 0 activare

configurați dot11Radio 1 activați configurați dot11Radio 1 mod root-ap configurați dot11Radio 1 wlan adăugați wlan3 3 vlan 30 configurați dot11Radio 1 canal 36 80

configurați dot11Radio 1 tx-power 1

Pentru informații suplimentare despre configurația WGB și Universal Workgroup Bridge (uWGB), consultați următoarele documente:

- Podul grupului de lucru (WGB)
- Ghid de implementare Cisco Industrial Wireless Workgroup Bridge și Universal WGB

Comenzi suplimentare

Ștergeți configurația

Pentru a șterge configurația pe modulul Wi-Fi, utilizați următoarea comandă:

router#**ștergere wireless-bridge**

Resetare din fabrică

Pentru a efectua o resetare din fabrică a modulului, utilizați următoarea comandă:

router#**resetarea din fabrică a podului wireless*config/implicit***

Conversie de mod

Pentru a schimba modul de operare al modulului între modurile WGB și CAPWAP, utilizați următoarea comandă:

router#**modul de pornire wireless-bridge*capwap/wgb***

Actualizare firmware

Actualizarea firmware-ului este acceptată de la Unified Client Image versiunea 17.11 și mai sus atunci când rulează în modul WGB. Pentru a actualiza firmware-ul, IR1800 necesită ca serverul TFTP să fie activat pentru ca modulul să obțină imaginea.

Procesul de actualizare a firmware-ului durează aproximativ 5-6 minute. După actualizarea cu succes, modulul Wi-Fi este reîncărcat automat cu noua imagine.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** router#**permite**	Intră în modul EXEC privilegiat.
Pasul 2	**copie** **rcp://***local-server***/ap1g8t-k9c1-tar-k9c1-tar** **Exemplu:** router#**copie** **rcp:// netadmin@172.16.101.101 /ap1g8t-k9c1-tar** **bootflash:ap1g8t-k9c1-tar**	Copiați imaginea client unificată (ap1g8t-k9c1-tar) în IR1800. Imaginea va fi descărcată în modul din această locație.
Pasul 3	**configura terminalul** **Exemplu:** router#**configura terminalul**	Intră în modul de configurare globală.
Pasul 4	**tftp-server***director*:*imagine* **Exemplu:** router#**tftp-server** **bootflash:ap1g8t-k9c1-tar** **router# end**	Configurați locația imaginii pe serverul TFTP al IR1800 și ieșiți din modul de configurare globală.
Pasul 5	**upgrade de firmware-punte fără fir** *ap1g8t-k9c1-tar IP netmask gateway* **Exemplu:** router(config)#**upgrade-firmware-punte fără fir ap1g8t-k9c1-tar 10.10.10.1 255.255.255.0 10.10.10.1**	Porniți actualizarea firmware-ului.
Pasul 6	**mai mult bootflash:/od_status**	Actualizarea firmware-ului durează aproximativ 5 până la 6 minute. Verificați**od_status**jurnalele pentru a monitoriza progresul.

CAPITOL 30

Suport suplimentar pentru modem pentru modulele celulare conectabile

Suport suplimentar pentru modem pentru modulele conectabile celulare CAT 6 și CAT 7

Această versiune oferă suport pentru modemuri suplimentare pe IR1101 și IR1800.

Modulele de interfață conectabile LTE Cat6 (PIM) vor fi actualizate cu modemuri Cat7. Următorul tabel arată tranziția produsului:

Tabelul 25: Tranziția Cat6 la Cat7

Cat6 (Actual)	**Cat7 (reîmprospătat)**
Sierra Wireless EM7455/7430	Sierra Wireless EM7411/7421/7431
Cat6 LTE Advanced	Cat7 LTE Advanced

Următoarele sunt noile PID-uri care vor fi disponibile:

- P-LTEA7-NA
- P-LTEA7-EAL
- P-LTEA7-JP
- P-5GS6-R16SA

Suport suplimentar pentru modem pentru modulele celulare conectabile

Important Pentru noile PID-uri menționate mai sus, următoarele funcții celulare nu au fost testate și nu sunt acceptate cu IOS XE versiunea 17.13.1, deși comenzile CLI pot permite:

- GNSS/NMEA
- Celular Dying-Gasp
- Suport eSIM/eUICC

Nota Nu există nicio interfață de linie de comandă nouă sau modificată cu aceste modemuri noi.

Suport suplimentar pentru modem pentru modulele celulare conectabile

Cisco IOS-XE Versiunea 17.14.1 îmbunătățește opțiunile de conectivitate și debitul pe platformele IR1101 și IR1800 prin acceptarea modemurilor celulare suplimentare:

- Modemuri CAT 7:
  - P-LTEA7-NA
  - P-LTEA7-EAL
  - P-LTEA7-JP
- Modem 5G:
  - P-5GS6-R16SA-GL

Nota Modemurile CAT 7 acceptă streaming GNSS și NMEA, în timp ce în prezent modulul P-5GS6-R16SA-GL nu acceptă streaming GPS și NMEA.

Suport 5G Standalone Mode (SA).

Această caracteristică oferă suport pentru modul 5G Standalone (SA) pe modulul conectabil P-5GS6-GL. Suportul modului 5G SA va permite afișarea configurației celulare 5G folosind comenzile Cisco IOS-XE CLI.

Această caracteristică oferă un mecanism în CLI pentru a selecta un set de benzi pentru modul SA, spre deosebire de o singură bandă din versiunile software anterioare. Următoarele CLI-uri IOS-XE au fost modificate pentru suport 5G SAmode:

- arată radioul celular
- afișați detaliile radioului celular (fără agregarea operatorului)
- afișați rețeaua celulară

Există, de asemenea, un CLI de selecție a benzilor pentru a selecta benzile celulare.

Afișați exemple de comandă

Router#**arată radioul celular 0/2/0** Modul
de putere radio = Număr canal 5G Rx online
= 632544 Număr canal 5G Tx = 632544
Banda 5G-SA = 78

Lățimea de bandă = 20 MHz
Curent 5G RSSI = -60 dBm Curent
5G RSRP = -71 dBm Curent 5G
RSRQ = -11 dB Curent 5G SNR =
34,5 dB Id-ul fizic al celulei = 500

Tehnologia de acces radio (RAT) Preferință = AUTO Tehnologia
de acces radio (RAT) selectată = 5GNR-SA

Router#**arată detaliile radio 0/4/0 celular** Modem
Radio este online Principal 0 Detalii antenă: RSSI =
-38 dBm

RSRP = -48 dBm
Diversitate 0 Detalii antenă: RSSI = -47
dBm
RSRP = -58 dBm

Router#**arată rețeaua celulară 0/4/0** Ora curentă a
sistemului = Sun Jan 6 0:4:36 1980 Stare curentă a
serviciului = Normal
Serviciu curent = Comutare de pachete Stare
curentă de roaming = Mod selecție rețea de
domiciliu = Rețea automată = Test PLMN 1-1

Codul de țară mobil (MCC) = 1 Cod de
rețea mobilă (MNC) = 1
Starea domeniului de comutare de pachete (PS) = Codul
zonei de urmărire atașat (TAC) = 1
ID celulă = 1024
MTU de rețea negociat = 1500

Exemplu de comandă de selecție a benzii

The**lte modem band-select**CLI poate fi folosit pentru a activa benzile pe care utilizatorul dorește să le folosească și la care dorește să se aboneze. În mod implicit, benzile SA nu sunt disponibile.

Important Dacă doriți să utilizați benzi SA,**lte modem band-select**comanda**NECESITATE**să fie utilizat ca parte a configurației.

Următorul este un exemplu de comandă:

conf t
controler celular 0/2/0
lte modem band-select indexes umts3g all lte4g all nr5g-NSA all nr5g-SA 78 slot 0 exit

Următoarele arată un exemplu de utilizare a benzii nr5g-sa 48:

Indicii de selectare a benzii modem lte umts3g "23" lte4g "7" nr5g-nsa "12" nr5g-sa "48" slot 0

Nota În exemplul de mai sus, banda 23 umts3g, banda 7 lte4g și banda 12 nr5g-nsa nu sunt disponibile în zonă, ceea ce înseamnă că modemul se va atașa doar la banda 48 nr5g-nsa.

Următoarele arată un exemplu de utilizare a benzii nr5g-sa 78:

Indicii de selectare a benzii de modem lte umts3g "23" lte4g "7" nr5g-nsa "78" nr5g-sa "niciun" slot 0

Nota În exemplul de mai sus, banda umts3g 23 și banda lte4g 7 nu sunt disponibile în zonă, iar benzile nr5g-sa sunt dezactivate, ceea ce înseamnă că modemul se va atașa doar la banda nr5g-nsa 78.

Limitări

nici unuleste o opțiune nevalidă pentru umts3g, lte4g și nr5g-nsa.

CAPITOL 31

Suport pentru modulul de interfață conectabil P-LTE-450

Suport pentru modulul de interfață conectabil P-LTE-450

Router-ul Cisco Catalyst IR1800 Rugged Series acceptă acum modulul de interfață conectabil (PIM) de categoria P Long-Term Evolution (PIM) de 450MHz, denumit P-LTE-450. LTE-450 PIM folosește frecvența de 450MHz pentru a aborda cazurile de utilizare LTE care vizează în primul rând utilitatea, siguranța publică și infrastructura critică întreținută de organizațiile publice din Europa și din alte țări. Modulul acceptă numai benzile 31 și 72, care sunt benzile de frecvență de operare LTE. Din cauza limitărilor hardware, P-LTE-450 este acceptat numai pe slotul 0/4.

Spre deosebire de modulele LTE obișnuite, P-LTE-450 are unele diferențe pe platforma IOS-XE. Unele dintre diferențele cheie sunt:

- IP-ul trece prin interfețe Gigabit Ethernet mai degrabă decât interfețe celulare.
- Comenzile de depanare provin din interfața de utilizator Web a hardware-ului terță parte.

Nota În documentația utilizatorului, puteți vedea modulul denumit P-LTE-450, numele produsului Cisco. Modulul este proiectat și fabricat de Intelliport, care se referă la el ca IPS-701. Ambele nume sunt prezente în documentație.

Ieșirea comenzii show afișează detaliile interfeței:

```
router#show run | sec 0/4/0 interfață
GigabitEthernet0/4/0 adresa ip dhcp

negociere auto
ipv6 dhcp client cerere furnizor ipv6
adresa autoconfig
activare ipv6
interfață GigabitEthernet0/4/0.2
încapsulare dot1Q 2
adresa ip dhcp
furnizor de solicitare client dhcp ipv6
```

autoconfig adresa ipv6

router#show ip int br
Adresa IP a interfeței OK? Metodă Stare Protocol GigabitEthernet0/0/0
10.195.236.86 DA NVRAM sus sus GigabitEthernet0/1/0 nealocat DA
dezactivat dezactivat GigabitEthernet0/1/1 nealocat DA dezactivat
dezactivat GigabitEthernet0/1/2 nealocat sus/da desetat
GigabitEthernet0/1/2 nealocat dezactivat DA1/1/2 dezactivat sus jos
Wl0/1/4 nealocat DA dezactivat

GigabitEthernet0/4/0 192.168.200.194 DA DHCP în sus
GigabitEthernet0/4/0.2 192.168.4.6 DA DHCP sus în sus
GigabitEthernet0/4/0.3 192.168.5.2 în sus/DA Async0CP în sus/ sus

Vlan1 192.168.50.1 DA NVRAM sus

Pentru mai multe informații despre cum să configurați interfața routerului pentru modulul P-LTE-450, Consultați

- Configurarea interfeței routerului pentru modulul P-LTE-450
- Ghid de configurare a modulului de interfață conectabilă celulară
- Alianță LTE 450MHz

Îmbunătățirea managementului rețelei P-LTE-450 prin obiecte MIB SNMP

În rețelele P-LTE-450, routerele pot furniza metrici de calitate esențiale prin intermediul obiectelor MIB (Simple Network Management Protocol) Management Information Base (MIB). Mai exact, routerele Cisco IR1101 și IR1800 echipate cu modulul de interfață conectabil (PIM) P-LTE-450 vă permite să vă integrați perfect cu instrumentele de management existente bazate pe SNMP pentru a raporta starea și valorile calității acestora.

Routerul identifică modulul P-LTE-450 ca o interfață Ethernet, în special Gigabit Ethernet 0/1/0, mai degrabă decât o interfață celulară. Pentru ca parametrii radio LTE450 0/1/0 să fie acceptați prin SNMP, un nou fișier MIB numit **Cisco-LTE450-MIB.my**trebuie creat. Acest fișier MIB include câmpuri specifice pentru a capta valorile calității semnalului radio.

MIB-uri SNMP acceptate

TheCISCO-LTE450-MIBSNMP este acceptatCisco P_ LTE_450 MIB.

CISCO-LTE450-MIBacceptă următoarele câmpuri MIB:

- **ciscoLte450Entry**:Punctul de intrare principal pentru MIB
- **ciscoLte450PortIndex**: Index pentru port (GigabitEthernet0/1/0)
- **ciscoLte450Rssi**: valoarea RSSI
- **ciscoLte450Rsrp**: valoarea RSRP
- **ciscoLte450Rsrq**: valoarea RSRQ
- **ciscoLte450Sinr**: valoarea SINR
- **ciscoLte450RssiMain**: valoarea RSSI pentru antena principală

- **`ciscoLte450RsrpMain`**: valoare RSRP pentru antena principală
- **`ciscoLte450RssiAux`**: valoarea RSSI pentru antena auxiliară
- **`ciscoLte450RsrpAux`**: valoare RSRP pentru antena auxiliară

Vedeți valorile de calitate a semnalului radio

Următorul exemplu afișează calitatea semnalului și calitatea semnalului antenei din configurația SNMP Cisco 4G LTE 450:

```
Router#arata radio lte450 0/1/0
Calitatea semnalului
===============
RSSI = -88 dBm
RSRP = -114 dBm
RSRQ = -12 dB
SINR = 0 dB

Calitatea semnalului antenei
=======================
RSSI principal = -87 dBm
RSRP principal = -112 dBm
RSSI auxiliar = -104 dBm
RSRP auxiliar = -143 dBm
```

CAPITOL 32

Îmbunătățiri ale timpului de pornire celulară

Îmbunătățiri ale timpului de pornire celulară

Au fost aduse numeroase îmbunătățiri în timpul de funcționare a conexiunii celulare cu versiunea IOS-XE 17.9.1. În versiunile anterioare, interfața celulară a durat aproximativ două minute și jumătate pentru a ajunge și a trece traficul după ce routerul a pornit. Timpul de funcționare a conexiunii celulare a fost îmbunătățit cu aproximativ 20% în această versiune.

Îmbunătățiri ale timpului de pornire celulară

CAPITOL 33

Suport SFP Digital Subscriber Line (DSL) pe IR1800

Suport SFP Digital Subscriber Line (DSL) pe IR1800

IR1800 acceptă acum DSL SFP în același mod ca și IR1101. Pentru detalii complete, consultați Configurarea liniei digitale de abonat (DSL)capitol din Ghidul de configurare IR1101.

Suport SFP Digital Subscriber Line (DSL) pe IR1800

CAPITOL 34

Suport pentru modulul de interfață conectabil LoRaWAN

Acest capitol conține următoarele secțiuni:

Suport pentru modulul de interfață conectabil LoRaWAN

Această versiune adaugă suport pentru modulul de interfață conectabil LoRaWAN, care a fost disponibil pentru prima dată pe IR1101.

Nota Aceasta este doar o versiune de paritate software. Modulul de interfață conectabil LoRaWAN nu poate fi comandat sau gata de implementare hardware pentru IR1800 până când produsul nu este anunțat. Vă rugăm să contactați persoana de contact Cisco pentru orice informații suplimentare.

Modulul de interfață conectabil Cisco LoRaWAN acceptă opt canale de conectivitate LoRa.

Există două module diferite P-LPWA:

- P-LPWA-900 este proiectat pentru profilul regional RF US915, AS923 și AU915, așa cum este definit de Specificații profil regional LoRa Alliance RF.
- P-LPWA-800 este proiectat pentru profilul regional RF EU868, IND865 și RU864, așa cum este definit de Specificații profil regional LoRa Alliance RF.

Modulele conectabile Cisco LoRaWAN pot fi gestionate de interfața de linie de comandă (CLI) sau de interfața de utilizator web Cisco IOS XE (WebUI).

Detalii despre instalare, configurare și informații de reglementare se găsesc înGhid de instalare și configurare a modulului de interfață conectabil Cisco LoRaWAN.

Suport pentru modulul de interfață conectabil LoRaWAN

CAPITOL 35

Suport Cisco SD-WAN

Acest capitol conține următoarele:

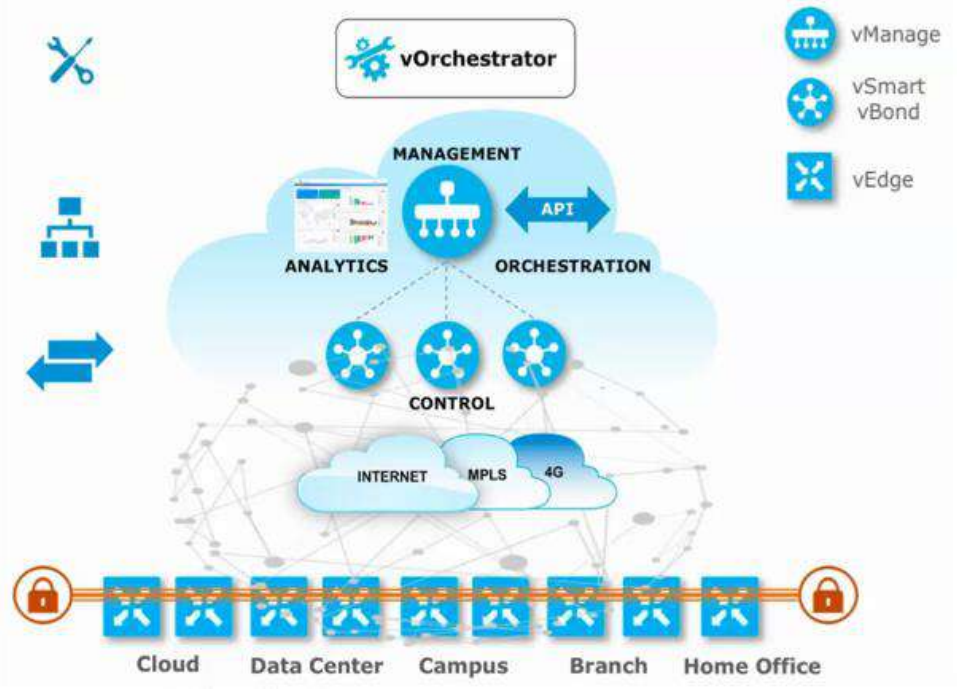
Prezentare generală Cisco SD-WAN

Cisco SD-WAN este o arhitectură bazată pe cloud care separă datele și planurile de control, gestionată prin consola Cisco vManage. Puteți stabili rapid o țesătură de suprapunere SD-WAN pentru a conecta centre de date, sucursale, campusuri și facilități de co-locație pentru a îmbunătăți viteza, securitatea și eficiența rețelei.

Cisco SDWAN adoptă o soluție bazată pe cloud, care constă din vOrchestrator, vManage, vSmart și vEdge.

- vOrchestrator este responsabil pentru lansarea tuturor VM-urilor controlerelor în cloud.
- vManage este planul de management pentru soluția generală SDWAN. Utilizează netconf/YANG pentru a vorbi cu dispozitivele vEdge.
- vSmart este planul de control pentru soluția generală SDWAN. Vorbește cu dispozitivul vEdge, acționează ca reflector de rută, reflector cheie și motor de politică.
- vEdge este planul de date al soluției generale SDWAN. Platforma IR1800 vorbește cu vSmart, vManage, ca parte a rețelei SDWAN.

Următoarea diagramă arată arhitectura de nivel înalt a SDWAN:



În timp ce Cisco SD-WAN este o arhitectură bazată pe cloud, unele dintre componente pot fi implementate la nivel local. ConsultațiCisco SD-WANpagina de destinație pentru informații suplimentare despre capacitățile SD-WAN.

Începând cu versiunea 17.3.2 a IOS XE, imaginea IOS XE poate fi configurată ca mod controler pentru a rula SD-WAN. O singură imagine universalk9 este utilizată pentru a implementa Cisco IOS XE SD-WAN și Cisco IOS XE. Această imagine universalk9 acceptă două moduri - modul autonom (pentru caracteristicile Cisco IOS XE) și modul controler (pentru caracteristicile Cisco SD-WAN).

Accesați funcționalitatea Cisco IOS XE și Cisco IOS XE SD-WAN prin modurile de execuție Autonomous și, respectiv, Controller. Modul autonom este modul implicit pentru router și include funcționalitatea Cisco IOS XE. Pentru a accesa funcționalitatea Cisco IOS XE SD-WAN, comutați la modul Controller. Puteți utiliza fluxul Plug and PlayWorkflow existent pentru a determina modul dispozitivului. VeziGhid de pornire Cisco SD-WAN pentru mai multe informații.

Nota Procesul PnP funcționează fie pe Gi0/0/0, fie pe Cellular.

Suport vManage pentru modulul WP-WIFI6-x

Această versiune va permite configurarea și monitorizarea modulului WP-WIFI6-x prin vManage din SDWAN. Acest lucru se aplică numai atunci când modulul rulează în modul EWC.

Nota

- vManage se numește acum Cisco Catalyst SD-WAN Manager.
- Cisco Catalyst SD-WAN Manager acceptă numai SD-WAN UX 1.0, care este acum înlocuit cu SD-WAN UX 2.0.
- Modul EWC este la sfârșitul vieții și nu este recomandat pentru noile implementări. Pentru mai multe informații, vezi Anunț de sfârșit de vânzare și de sfârșit de viață pentru Cisco Wireless EWC pe punctul de acces.

Pentru mai multe informații despre vManage, consultați pagina de destinație a produsului aici:https://www.cisco.com/site/us/en/products/networking/wan/vmanage/index.html

SD-WAN

SD-WAN RA este acum acceptat pe routerele IoT cu IOS XE 17.13.1. SD-WAN RA este o combinație de două caracteristici:

- IOS-XE SD-WAN
- Server de acces la distanță IOS-XE FlexVPN

Nota Toate dispozitivele IoT acceptă doar clientul SD-WAN RA.

Informații despre accesul la distanță SD-WAN pot fi găsite în următorul ghid:

Acces la distanță Cisco Catalyst SD-WAN

Documentație suplimentară

Documentația suplimentară pentru SDWAN/vManage este disponibilă la următoarele link-uri:

- Documentația utilizatorului pentru Cisco IOS XE Catalyst SD-WAN Versiunea 17
- Cisco Catalyst SD-WAN
- Informații de asistență Cisco SD-WAN
- Prezentare generală a monitorului Cisco vManage
- Gestionarea dispozitivului SD-Routing utilizând Cisco SD-WAN Manager

Documentație aferentă

Documentația Cisco SDWAN este disponibilă din următoarele surse:

https://www.cisco.com/c/en/us/support/routers/sd-wan/tsd-products-support-series-home.html

https://sdwan-docs.cisco.com/Product_Documentation/Software_Features

Toată documentația tehnică pentru Cisco SD-WAN poate fi găsită aici:

https://www.cisco.com/c/en/us/support/routers/sd-wan/tsd-products-support-series-home.html

vManage Support pentru modul EWC pe modulul de interfață Wi-Fi Cisco

Modulul de interfață Wi-Fi Cisco (WIM) este o interfață conectabilă disponibilă pentru toate modelele din seria IR1800. PID-ul este WP-WIFI6-x unde x înseamnă domeniul de reglementare.

Suportul vManage pentru modul EWC pe modulul WIM permite utilizatorului să configureze modulul în modul EWC cu profiluri WLAN, profiluri radio și detalii de management ale EWC de la router în modul SDWAN. WIM este configurat din vManage folosind șablonul de caracteristici „ISR1K/IR18 Wireless” și verificați comenzile show wireless-lan în vManage.

Cu această lansare a IOS XE, a fost adăugat suport vManage NUMAI pentru controlerul EWC.

Nota

- vManage se numește acum Cisco Catalyst SD-WAN Manager.
- Cisco Catalyst SD-WAN Manager acceptă numai SD-WAN UX 1.0, care este acum înlocuit cu SD-WAN UX 2.0.
- Modul EWC este la sfârșitul vieții și nu este recomandat pentru noile implementări. Pentru mai multe informații, vezi Anunț de sfârșit de vânzare și de sfârșit de viață pentru Cisco Wireless EWC pe punctul de acces.

Documentație suplimentară

Documentația suplimentară pentru SDWAN/vManage este disponibilă la următoarele link-uri:

- Documentația utilizatorului pentru Cisco IOS XE Catalyst SD-WAN Versiunea 17
- Cisco Catalyst SD-WAN
- Informații de asistență Cisco SD-WAN
- Prezentare generală a monitorului Cisco vManage
- Gestionarea dispozitivului SD-Routing utilizând Cisco SD-WAN Manager

CAPITOL 36

Depanare

Această secțiune conține următoarele:

Depanare

Această secțiune descrie scenariile de depanare.

Înainte de a depana o problemă de software, trebuie să conectați un computer la router prin portul de consolă. Cu un computer conectat, puteți vizualiza mesajele de stare de la router și puteți introduce comenzi pentru a depana o problemă.

De asemenea, puteți accesa interfața de la distanță utilizând Telnet. Opțiunea Telnet presupune că interfața este în funcțiune.

Înțelegerea modului de diagnosticare

Routerul pornește sau accesează modul de diagnosticare în următoarele scenarii:

- Procesul sau procesele IOS eșuează, în unele scenarii. În alte scenarii, sistemul se resetează atunci când procesul sau procesele IOS eșuează.
- O politică de acces configurată de utilizator a fost configurată utilizând**transport-hartă**comandă care direcționează utilizatorul în modul de diagnosticare.
- Un semnal de pauză de trimitere (**Ctrl-C**sau**Ctrl-Shift-6**) a fost introdus în timpul accesării routerului, iar routerul a fost configurat să intre în modul de diagnosticare atunci când a fost trimis un semnal de întrerupere.

În modul de diagnosticare, un subset de comenzi care sunt disponibile în modul EXEC utilizator sunt puse la dispoziția utilizatorilor. Printre altele, aceste comenzi pot fi folosite pentru:

- Inspectați diferite stări de pe router, inclusiv starea IOS.

- Înlocuiți sau derulați înapoi configurația.
- Furnizați metode de repornire a IOS-ului sau a altor procese.
- Reporniți hardware-ul, cum ar fi întregul router, un modul sau eventual alte componente hardware.
- Transferați fișiere în sau în afara routerului utilizând metode de acces la distanță, cum ar fi FTP, TFTP și SCP.

Modul de diagnosticare oferă o interfață de utilizator mai cuprinzătoare pentru depanare decât routerele anterioare, care se bazau pe metode de acces limitat în timpul defecțiunilor, cum ar fi ROMMON, pentru a diagnostica și depana problemele Cisco IOS. Comenzile modulului de diagnosticare pot funcționa atunci când procesul Cisco IOS nu funcționează corect. Aceste comenzi sunt disponibile și în modul EXEC privilegiat pe router, atunci când routerul funcționează normal.

Înainte de a contacta Cisco sau distribuitorul dvs

Dacă nu puteți găsi sursa unei probleme, contactați distribuitorul local pentru sfaturi. Înainte de a suna, ar trebui să aveți pregătite următoarele informații:

- Tipul șasiului și numărul de serie
- Acord de întreținere sau informații despre garanție
- Tipul de software și numărul versiunii
- Data la care ați primit hardware-ul
- Scurtă descriere a problemei
- Scurtă descriere a pașilor pe care i-ați făcut pentru a izola problema

arată interfețele Comanda de depanare

Utilizați**arată interfețele**comandă pentru a afișa starea tuturor porturilor fizice și a interfețelor logice de pe router. Descrieți mesajele din ieșirea comenzii.

IR1800 acceptă următoarele interfețe:

GigabitEthernet 0/0/0

GigabitEthernet 0/1/0 până la 0/1/3

Cellular 0/4/0, 0/4/1, 0/5/0 și 0/5/1

Asincron 0/2/0 și 0/2/1

usbflash0:

msata

Contact de alarmă intrare alarmă 0

Metode de actualizare software

Sunt disponibile mai multe metode pentru actualizarea software-ului pe routerele Cisco IR1800, inclusiv:

- Copiați noua imagine software în memoria flash prin LAN sau WAN atunci când este utilizată imaginea software Cisco IOS existentă.
- Copiați noua imagine software în memoria flash prin LAN în timp ce imaginea de pornire (monitorul ROM) funcționează.
- Copiați noua imagine de software peste portul consolei în modul monitor ROM.
- Din modul monitor ROM, porniți routerul dintr-o imagine software care este încărcată pe un server TFTP. Pentru a utiliza această metodă, serverul TFTP trebuie să fie pe aceeași rețea LAN ca și routerul.

Modificați registrul de configurare

Pentru a modifica un registru de configurare, urmați acești pași:

Procedură

Pasul 1 Conectați un computer la portul CONSOLE de pe router.

Pasul 2 La promptul EXEC privilegiat (*nume_router*#),intra in**arata versiunea**comandă pentru a afișa valoarea registrului de configurare existent (afișată cu caractere aldine în partea de jos a acestui exemplu de ieșire):

Exemplu:

```
Router# arată versiunea
Software Cisco IOS XE, versiunea 17.06.01prd23
Software Cisco IOS [Bengaluru], Software ISR (ARMV8EL_LINUX_IOSD-UNIVERSALK9_IOT-M), Versiunea 17.6.1prd23,
  SOFTWARE RELEASE (fc1)
Asistență tehnică: http://www.cisco.com/techsupport Copyright (c)
1986-2021 de Cisco Systems, Inc. Compilat marți 20-iul-21 02:28 de
mcpre


Software Cisco IOS-XE, Copyright (c) 2005-2021 de către Cisco Systems, Inc. Toate drepturile
rezervate. Anumite componente ale software-ului Cisco IOS-XE sunt licențiate sub Licența publică
generală GNU („GPL”) versiunea 2.0. Codul software licențiat conform GPL Versiunea 2.0 este un
software gratuit care nu vine cu ABSOLUT NU GARANȚIE. Puteți redistribui și/sau modifica un
astfel de cod GPL în conformitate cu termenii GPL Versiunea 2.0. Pentru mai multe detalii,
consultați documentația sau fișierul „Notă de licență” care însoțește software-ul IOS-XE sau adresa
URL aplicabilă furnizată în pliantul care însoțește software-ul IOS-XE.


ROM: 3.9(REL)

Durata de funcționare a IR1833 este de 13 ore și 6 minute
Timpul de funcționare pentru acest procesor de control este de 13 ore și 9 minute.
Sistemul a revenit la ROM prin Upgrade de firmware
Fișierul imagine de sistem este „bootflash:ir1800-universalk9.17.06.01prd23.SPA.bin”
```

Ultimul motiv de reîncărcare: Comanda de reîncărcare

Acest produs conține caracteristici criptografice și este supus legilor Statelor Unite și ale țărilor locale care reglementează importul, exportul, transferul și utilizarea. Livrarea produselor criptografice Cisco nu implică o autoritate terță parte pentru a importa, exporta, distribui sau utiliza criptarea. Importatorii, exportatorii, distribuitorii și utilizatorii sunt responsabili pentru respectarea legilor din SUA și ale țărilor locale. Prin utilizarea acestui produs sunteți de acord să respectați legile și reglementările aplicabile. Dacă nu puteți respecta legile locale și americane, returnați imediat acest produs.

Un rezumat al legilor SUA care guvernează produsele criptografice Cisco poate fi găsit la: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

Dacă aveți nevoie de asistență suplimentară, vă rugăm să ne contactați trimițând un e-mail la export@cisco.com .

Informații privind licența pachetului de tehnologie:

---------- Tip de tehnologie Pachet de tehnologie Pachet de tehnologie
Următoarea repornire curentă

Nivelul curent de debit este de 50000 kbps

Stare de licență inteligentă: înregistrarea nu este aplicabilă/nu se aplică

Procesor Cisco IR1833-K9 (1RU) cu 470123K/6147K octeți de memorie. ID placă procesor FCW2447P0EB
Mod de operare al routerului: Versiune de bootloader MCU autonom: 0x22
Versiunea aplicației MCU: 0x4d 1
interfață Ethernet virtuală 6 interfețe
Gigabit Ethernet 2 interfețe seriale

1 linie terminală
4 interfețe celulare
32768K octeți de memorie de configurare nevolatilă. 3988088K octeți de memorie fizică.
7475198K octeți de Bootflash la bootflash:.

Registrul de configurare este 0x2102

Router#

Pasul 3 Înregistrați setarea registrului de configurare.

Pasul 4 Pentru a activa setarea pauzei (indicată de valoarea bitului 8 din registrul de configurare), introduceți **config-registru** *<valoare>*comandă din modul EXEC privilegiat.

- Break enabled—Bitul 8 este setat la 0.
- Pauza dezactivată (setare implicită)—Bitul 8 este setat la 1.

Configurarea registrului de configurare pentru Autoboot

Nota Modificarea registrului de configurare este doar pentru depanare avansată și ar trebui făcută numai cu îndrumări din partea asistenței Cisco.

Registrul de configurare poate fi folosit pentru a schimba comportamentul routerului. Aceasta include controlul modului în care pornește routerul. Setați registrul de configurare la 0x0 pentru a porni în ROM, utilizând una dintre următoarele comenzi:

- În modul de configurare Cisco IOS, utilizați**config-reg**Comanda 0x0.
- Din promptul ROMMON, utilizați**confreg**Comanda 0x0.

Nota Setarea registrului de configurare la 0x2102 va seta routerul să pornească automat software-ul Cisco IOS XE.

Resetați routerul

Pentru a reseta routerul, urmați acești pași:

Procedură

Pasul 1 Dacă pauză este dezactivată, opriți routerul (O), așteptați 5 secunde și porniți-l din nou (|). În 60 de secunde, apăsați tasta **Pauză**cheie. Terminalul afișează promptul monitorului ROM.

Nota
Unele tastaturi terminale au o tastă etichetată*Pauză*.Dacă tastatura nu are o tastă Break, consultați documentația livrată cu terminalul pentru instrucțiuni despre cum să trimiteți o pauză.

Pasul 2 Apăsați pauză. Terminalul afișează următorul prompt:

Exemplu:

```
rommon 2>
```

Pasul 3 Intră**confreg 0x2142**pentru a reseta registrul de configurare:

Exemplu:

```
rommon 2>confreg 0x142
```

Pasul 4 Sincronizați modificările de configurare cu**sincronizare**comanda.

Exemplu:

```
rommon 2>sincronizare
```

Pasul 5 Inițializați routerul introducând**reîncărcați**comanda:

Exemplu:

rommon 2>**reîncărcați**

Routerul își ciclează alimentarea, iar registrul de configurare este setat la 0x2142. Routerul folosește imaginea sistemului ROM de pornire, indicată de dialogul de configurare a sistemului:

Exemplu:

- - - Dialog de configurare a sistemului ---

Pasul 6 Intră**nu**ca răspuns la solicitări până când este afișat următorul mesaj:

Exemplu:

Apăsați RETURN pentru a începe!

Pasul 7 Presa**Reveni**. Apare următorul prompt:

Exemplu:

Router>

Pasul 8 Introduceți comanda de activare pentru a intra în modul de activare. Modificările de configurare pot fi făcute numai în modul de activare:

Exemplu:

Router>**permite**

Promptul se schimbă în promptul EXEC privilegiat:

Exemplu:

Router#

Pasul 9 Introduceți**arată startup-config**comandă pentru a afișa o parolă de activare în fișierul de configurare:

Exemplu:

Router#**arată startup-config**

Ce să faci în continuare

Dacă recuperați o parolă de activare, nu efectuați pașii din secțiunea Resetați parola și salvați modificările. În schimb, finalizați procesul de recuperare a parolei parcurgând pașii din secțiunea Resetați valoarea registrului de configurare.

Dacă recuperați o parolă secretă de activare, aceasta nu este afișată în**arată startup-config**ieșirea comenzii. Finalizați procesul de recuperare a parolei parcurgând pașii din secțiunea Resetați parola și salvați modificările.

Recuperarea unei parole pierdute

Pentru a recupera o parolă de activare pierdută sau o parolă secretă de activare pierdută, consultați următoarele secțiuni:

1.Modificați registrul de configurare

2.Resetați routerul

3.Resetați parola și salvați modificările (numai pentru parolele secrete pierdute)

4.Resetați valoarea registrului de configurare.

5.Dacă ați efectuat o**stergere scris**, sau ați folosit butonul de resetare, va trebui să adăugați licența.

IR1800#config termen
IR1800#licență rezervare inteligentă

Nota Orice interfață vlan va trebui să fie recreată și este posibil să fie necesar să regenerați certificatele.

Nota Recuperarea unei parole pierdute este posibilă numai atunci când sunteți conectat la router prin portul de consolă. Aceste proceduri nu pot fi efectuate printr-o sesiune Telnet.

Sfat Consultați secțiunea „Sfaturi fierbinți” de pe Cisco.com pentru informații suplimentare despre înlocuirea parolelor secrete de activare.

Resetați parola și salvați modificările

Pentru a vă reseta parola și a salva modificările, urmați acești pași:

Procedură

Pasul 1 Introduceți**configura terminalul**comandă pentru a intra în modul de configurare globală:

Exemplu:

Router#**configura terminalul**

Pasul 2 Introduceți**activați secret**comandă pentru a reseta parola secretă de activare în router:

Exemplu:

Router(config)#**activați secret** *parolă*

Pasul 3 Intră**Ieșire**pentru a ieși din modul de configurare globală:

Exemplu:

Router(config)#**Ieșire**

Pasul 4 Salvați modificările de configurare:

Exemplu:

Router#**copiați running-config startup-config**

Resetați valoarea registrului de configurare

Pentru a reseta valoarea registrului de configurare după ce ați recuperat sau reconfigurat o parolă, urmați acești pași:

Procedură

Pasul 1 Introduceți**configura terminalul**comandă pentru a intra în modul de configurare globală:

Exemplu:

Router#**configura terminalul**

Pasul 2 Introduceți**configurați registrul**comanda și valoarea originală a registrului de configurare pe care ați înregistrat-o.

Exemplu:

Router(config)#**config-reg** *valoare*

Pasul 3 Intră**Ieșire**pentru a ieși din modul de configurare:

Exemplu:

Router(config)# ieșire

Nota
Pentru a reveni la configurația utilizată înainte de a recupera parola de activare pierdută, nu salvați modificările de configurare înainte de a reporni routerul.

Pasul 4 Reporniți routerul și introduceți parola recuperată.

Configurarea unei hărți de transport porturi de consolă

Această sarcină descrie cum să configurați o hartă de transport pentru o interfață de port de consolă pe router.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**permite** **Exemplu:** Router>**permite**	Activează modul EXEC privilegiat. Introduceți parola dacă vi se solicită.

	Comanda sau Acțiune	Scop
Pasul 2	**configura terminalul** **Exemplu:** Router#**configura terminalul**	Intră în modul de configurare globală.
Pasul 3	**consolă de tip transport-hartă** *transport-hartă-nume* **Exemplu:** Router(config)#**manevrator de consolă de tip hartă de transport**	Creează și denumește o hartă de transport pentru gestionarea conexiunilor la consolă și intră în modul de configurare a hărții de transport.
Pasul 4	**conexiunea așteptați**[**permite**[**întreruptibilă**]**| nici unul**[**deconecta**]] **Exemplu:** Router(config-tmap)#**conexiune nu așteaptă niciuna**	Specifică modul în care va fi gestionată o conexiune de consolă folosind această hartă de transport. • **permite întreruptibile**—Conexiunea la consolă așteaptă ca o linie Cisco IOS VTY să devină disponibilă și, de asemenea, permite utilizatorilor să intre în modul de diagnosticare prin întreruperea unei conexiuni la consolă care așteaptă ca o linie Cisco IOS VTY să devină disponibilă. Aceasta este setarea implicită. **Nota** Utilizatorii pot întrerupe o conexiune în așteptare introducând**Ctrl-C**sau**Ctrl-Shift-6**. • **nici unul**—Conexiunea consolei intră imediat în modul de diagnosticare.
Pasul 5	(Opțional)**banner**[**diagnostic | așteaptă**] *banner-mesaj* **Exemplu:** Router(config-tmap)#**banner diagnostic X** Introduceți mesajul TEXT. Încheiați cu caracterul „X”. **- - Bun venit în modul de diagnosticare -- X** Router(config-tmap)#	(Opțional) Creează un mesaj banner care va fi văzut de utilizatorii care intră în modul de diagnosticare sau care așteaptă linia Cisco IOS VTY din cauza configurației hărții de transport a consolei. • **diagnostic**—Creează un mesaj banner văzut de utilizatori direcționați către modul de diagnosticare din cauza configurației hărții de transport din consolă. **Nota** Utilizatorii pot întrerupe o conexiune în așteptare introducând**Ctrl-C**sau**Ctrl-Shift-6**. • **așteaptă**—Creează un mesaj banner văzut de utilizatori care așteaptă ca Cisco IOS VTY să devină disponibil. • *banner-mesaj*—Mesaj banner, care începe și se termină cu același caracter delimitator.

	Comanda sau Acțiune	Scop
Pasul 6	**Ieșire** **Exemplu:** Router(config-tmap)#**Ieșire**	Iese din modul de configurare a hărții de transport pentru a reintra în modul de configurare globală.
Pasul 7	**consola de tip transport** *număr-linie-consolă* **intrare** *transport-hartă-nume* **Exemplu:** Router(config)#**tip transport console 0 input consolehandler**	Aplică setările definite în harta de transport la interfața consolei. The*transport-hartă-nume*pentru că această comandă trebuie să se potrivească cu*transport-hartă-nume* definite în**consolă de tip transport-hartă**comanda.

Exemple

Următorul exemplu arată cum să creați o hartă de transport pentru a seta politicile de acces la portul de consolă și pentru a se atașa la portul de consolă 0:

Router(config)#**manevrator de consolă de tip hartă de transport**
Router(config-tmap)#**conexiune așteptați permite întreruptibil**
Router(config-tmap)#**banner diagnostic X** Introduceți mesajul TEXT. Încheiați cu caracterul „X”.
- - Bun venit în modul de diagnosticare -- X

Router(config-tmap)#**banner asteapta X**
Introduceți mesajul TEXT. Încheiați cu caracterul „X”. Se așteaptă linia vty IOS
X
Router(config-tmap)#**Ieșire**
Router(config)#**tip transport console 0 input consolehandler**

Vizualizarea configurațiilor pentru portul consolei, SSH și Telnet

Utilizați următoarele comenzi pentru a vizualiza configurațiile de gestionare a portului consolei, SSH și Telnet:

- **arata transport-harta**
- **arată politica de acces la configurația software-ului platformei**

Utilizați**arata transport-harta**comandă pentru a vizualiza configurațiile hărții de transport.

arata transport-harta[**toate | nume***transport-hartă-nume*|**tip**[**consolă**]]

Această comandă poate fi utilizată fie în modul EXEC utilizator, fie în modul EXEC privilegiat.

Exemplu

Următorul exemplu arată hărțile de transport care sunt configurate pe router: port console (manevrător de consolă):

Router#**arata transport-harta toate**
Harta transportului:
Nume: consolehandler Tip: Console Transport

Conexiune:
Opțiune de așteptare: Așteptați Permiteți banner de așteptare întreruptă:

În așteptarea bannerului IOS CLI bshell: Bun venit la
Modul de diagnosticare

Router#**afișează consola de tip hartă de transport**
Harta transportului:
Nume: consolehandler

PROIECTA DE REVIZIE - CISCO CONFIDENTIAL

Tip: Console Transport

Conexiune:
Opțiune de așteptare: Așteptați Permiteți banner de așteptare întreruptă:

În așteptarea bannerului IOS CLI Bshell: Bun venit la
Modul de diagnosticare

Router#**arată tipul hărții de transport ssh persistent** Harta
transportului:
Nume: consolehandler Tip: Console Transport

Conexiune:
Opțiune de așteptare: Așteptați Permiteți banner de așteptare întreruptă:

În așteptarea bannerului IOS CLI Bshell: Bun venit la
Modul de diagnosticare

Utilizați**arată politica de acces la configurația software-ului platformei**comandă pentru a vizualiza configurațiile curente pentru gestionarea conexiunilor portului consolei de intrare, SSH și Telnet. Ieșirea acestei comenzi oferă politica actuală de așteptare pentru fiecare tip de conexiune (Telnet, SSH și consolă), precum și informații despre bannerele configurate în prezent.

Spre deosebire de**arata transport-harta**comanda, cel**arată politica de acces la configurația software-ului platformei** comanda este disponibilă în modul de diagnosticare, astfel încât să poată fi introdusă în scenariile în care aveți nevoie de informații de configurare a hărții de transport, dar nu puteți accesa CLI Cisco IOS.

Exemplu

Următorul exemplu arată**arată politica de acces la configurația software-ului platformei**comanda.

Router#**arată politica de acces la configurația software-ului platformei**
Politicile actuale de acces

Metoda: telnet
Regula: așteptați cu întrerupere Banner Shell: Bun
venit în modul de diagnosticare

Așteptați bannerul:
Se așteaptă procesul IOS

Metoda: ssh Regulă: așteptați banner Shell: așteptați bannerul:

Metoda: consola
Regula: așteptați cu întrerupere. Banner Shell:
așteptați bannerul:

Folosind comenzile de resetare din fabrică

The**resetarea din fabrică**comenzile sunt folosite pentru a elimina toate datele specifice clientului de pe un router/comutator care a fost adăugat. Datele pot fi configurații, fișiere jurnal, variabile de boot, fișiere de bază și așa mai departe.

The**resetează toate din fabrică**comanda șterge bootflash, nvram, variabilele rommon, licențele și jurnalele.

Atenţie Utilizarea comenzii de resetare din fabrică nu trebuie făcută cu ușurință. Toate configurațiile clienților vor fi șterse și platforma se va porni ca și cum ar fi nouă din fabrică.

Nota resetarea din fabrică nu funcționează dacă IOS-XE rulează în modul controler. Vă rugăm să consultați informațiile de configurare SDWAN.

Router#**resetează toate din fabrică**
Operația de resetare din fabrică este ireversibilă pentru toate operațiunile. esti sigur? [confirma]
Intra

* 12 mai 09:55:45.831: %SYS-5-RELOAD: Reîncărcare solicitată de Exec. Motivul reîncărcării: Resetarea din fabrică.

* * * Reveniți la promptul ROMMON

Secvența de pornire după resetarea din

fabrică Pornirea imaginii:

- Bootloader-ul încearcă să pornească „golden.bin” din bootflash: partiția
- Dacă nu este prezent „golden.bin”, atunci porniți prima imagine.

Se încarcă configurația:

- IOS caută fișierul „golden.cfg” pe nvram: partitionează și îl aplică la pornire.
- Dacă nu este prezent „golden.cfg” pe nvram: atunci IOS caută fișierul „golden.cfg” pe bootflash: partiționează și îl aplică la pornire.
- Dacă nu este prezent „golden.cfg” pe bootflash: atunci configurațiile sunt șterse și este folosit dialogul de configurare software.

CAPITOL 37

Mesaje de sistem

Acest capitol conține următoarele secțiuni:

Informații despre managementul proceselor

Puteți accesa mesajele de sistem conectându-vă la consolă prin protocolul Telnet și monitorizând componentele sistemului de la distanță de la orice stație de lucru care acceptă protocolul Telnet.

Pornirea și monitorizarea software-ului este denumită managementul procesului. Infrastructura de gestionare a proceselor pentru un router este independentă de platformă, iar mesajele de eroare sunt consecvente pe platformele care rulează pe Cisco IOS XE. Nu trebuie să fiți implicat direct în managementul procesului, dar vă recomandăm să citiți mesajele de sistem care se referă la eșecurile procesului și alte probleme.

Cum să găsiți detalii despre mesajul de eroare

Pentru a afișa mai multe detalii despre gestionarea unui proces sau un mesaj de eroare syslog, introduceți mesajul de eroare în instrumentul Decodor mesaj de eroare la:https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi.

De exemplu, introduceți mesajul%PMAN-0-PROCESS_NOTIFICATIONîn instrument pentru a vizualiza o explicație a mesajului de eroare și a acțiunii recomandate care trebuie întreprinsă.

Următoarele sunt exemple de descriere și de acțiune recomandată afișate de instrumentul Error Message Decoder pentru unele dintre mesajele de eroare.

Mesaj de eroare:%PMAN-0-PROCESS_NOTIFICATION: componenta de notificare a ciclului de viață a procesului a eșuat deoarece [caractere]

Explicație	Acțiune recomandată

Componenta de notificare a ciclului de viață a procesului a eșuat, împiedicând detectarea corectă a pornirii și opririi unui proces. Această problemă este probabil rezultatul unui defect software în subpachetul software.	Notați ora mesajului și investigați jurnalele de mesaje de eroare ale nucleului pentru a afla mai multe despre problemă și pentru a vedea dacă este corectabilă. Dacă problema nu poate fi corectată sau jurnalele nu sunt utile, copiați mesajul de eroare exact așa cum apare pe consolă împreună cu rezultatul**arată suport tehnic** comanda și furnizați informațiile adunate unui reprezentant de asistență tehnică Cisco.

Mesaj de eroare:%PMAN-0-PROCFAILCRIT Un proces critic [chars] a eșuat (rc [dec])

Explicaţie	Acțiune recomandată
Un proces important pentru funcționarea routerului a eșuat.	Notați ora mesajului și investigați jurnalele de mesaje de eroare pentru a afla mai multe despre problemă. Dacă problema persistă, copiați mesajul exact așa cum apare pe consolă sau în jurnalul de sistem. Cercetați și încercați să rezolvați problema folosind instrumentele și utilitățile furnizate la:http://www.cisco.com/tac. Cu unele mesaje, aceste instrumente și utilitare vor furniza informații clarificatoare. Căutați probleme de software rezolvate folosind Instrumentul de căutare a erorilor la: http://www.cisco.com/cisco/psn/bssprt/bss. Dacă mai aveți nevoie de asistență, deschideți un caz la Centrul de asistență tehnică la: http://tools.cisco.com/ServiceRequestTool/create/sau contactați reprezentantul de asistență tehnică Cisco și furnizați reprezentantului informațiile pe care le-ați adunat. Atașați următoarele informații la cazul dvs. în format text simplu (.txt) fără arhivare: rezultatul**afișează înregistrarea**și**arată suport tehnic** comenzile și jurnalele dvs. pertinente de depanare.

Mesaj de eroare:%PMAN-3-PROCFAILOPT Un proces opțional [chars] a eșuat (rc [dec])

Explicaţie	Acțiune recomandată

Un proces care nu afectează redirecționarea traficului a eșuat.	Notați ora mesajului și investigați jurnalele de mesaje de eroare ale nucleului pentru a afla mai multe despre problemă. Deși traficul va fi în continuare redirecționat după primirea acestui mesaj, anumite funcții de pe router pot fi dezactivate din cauza acestui mesaj și eroarea ar trebui investigată. Dacă jurnalele nu sunt utile sau indică o problemă pe care nu o puteți corecta, copiați mesajul exact așa cum apare pe consolă sau în jurnalul de sistem. Cercetați și încercați să rezolvați problema folosind instrumentele și utilitățile furnizate la http://www.cisco.com/tac. Cu unele mesaje, aceste instrumente și utilitare vor furniza informații clarificatoare. Căutați probleme de software rezolvate folosind Instrumentul de căutare a erorilor la: http://www.cisco.com/cisco/psn/bssprt/bss. Dacă mai aveți nevoie de asistență, deschideți un caz la Centrul de asistență tehnică la: http://tools.cisco.com/ServiceRequestTool/create/sau contactați reprezentantul de asistență tehnică Cisco și furnizați reprezentantului informațiile pe care le-ați adunat. Atașați următoarele informații la cazul dvs. în format text simplu (.txt) fără arhivare: rezultatul**afișează înregistrarea**și**arată suport tehnic** comenzile și jurnalele dvs. pertinente de depanare.

Mesaj de eroare:%PMAN-3-PROCFAIL Procesul [chars] a eșuat (rc [dec])

Explicație	**Acțiune recomandată**
Procesul a eșuat ca urmare a unei erori.	Acest mesaj va apărea împreună cu alte mesaje legate de proces. Verificați celelalte mesaje pentru a determina motivul defecțiunilor și pentru a vedea dacă pot fi luate măsuri corective. Dacă problema persistă, copiați mesajul exact așa cum apare pe consolă sau în jurnalul de sistem. Cercetați și încercați să rezolvați problema folosind instrumentele și utilitățile furnizate la: http://www.cisco.com/tac. Cu unele mesaje, aceste instrumente și utilitare vor furniza informații clarificatoare. Căutați probleme de software rezolvate folosind Instrumentul de căutare a erorilor la: http://www.cisco.com/cisco/psn/bssprt/bss. Dacă mai aveți nevoie de asistență, deschideți un caz la Centrul de asistență tehnică la: http://tools.cisco.com/ServiceRequestTool/create/sau contactați reprezentantul de asistență tehnică Cisco și furnizați reprezentantului informațiile pe care le-ați adunat. Atașați următoarele informații la cazul dvs. în format text simplu (.txt) fără arhivare: rezultatul**afișează înregistrarea**și**arată suport tehnic** comenzile și jurnalele dvs. pertinente de depanare.

Mesaj de eroare:%PMAN-3-PROCFAIL_IGNORE [chars] ieșirile de proces și eșecurile sunt ignorate din cauza setărilor de depanare. Funcționalitatea normală a routerului va fi afectată. Este posibil ca funcțiile critice ale routerului, cum ar fi comutarea RP, reîncărcarea routerului, resetarea FRU etc., să nu funcționeze corect.

Explicație	Acțiune recomandată
Un eșec de proces este ignorat din cauza setărilor de depanare configurate de utilizator.	Dacă se dorește acest comportament și setările de depanare sunt setate în funcție de preferința unui utilizator, nu este necesară nicio acțiune. Dacă aspectul acestui mesaj este privit ca o problemă, modificați setările de depanare. Nu este de așteptat ca routerul să se comporte normal cu această setare de depanare. Funcționalități precum comutarea SSO, reîncărcările routerului, resetările FRU și așa mai departe vor fi afectate. Această setare ar trebui utilizată numai într-un scenariu de depanare. Nu este normal să rulați routerul cu această setare.

Mesaj de eroare:%PMAN-3-PROCHOLDDOWN Procesul [chars] a fost oprit (rc [dec])

Explicație	Acțiune recomandată
Procesul a fost repornit de prea multe ori cu eșecuri repetate și a fost plasat în starea de suspendare.	Acest mesaj va apărea împreună cu alte mesaje legate de proces. Verificați celelalte mesaje pentru a determina motivul defecțiunilor și pentru a vedea dacă pot fi luate măsuri corective. Dacă problema persistă, copiați mesajul exact așa cum apare pe consolă sau în jurnalul de sistem. Cercetați și încercați să rezolvați problema folosind instrumentele și utilitățile furnizate la: http://www.cisco.com/tac. Cu unele mesaje, aceste instrumente și utilitare vor furniza informații clarificatoare. Căutați probleme de software rezolvate folosind Instrumentul de căutare a erorilor la: http://www.cisco.com/cisco/psn/bssprt/bss. Dacă mai aveți nevoie de asistență, deschideți un caz la Centrul de asistență tehnică la: http://tools.cisco.com/ServiceRequestTool/create/sau contactați reprezentantul de asistență tehnică Cisco și furnizați reprezentantului informațiile pe care le-ați adunat. Atașați următoarele informații la cazul dvs. în format text simplu (.txt) fără arhivare: rezultatul**afișează înregistrarea**și**arată suport tehnic** comenzile și jurnalele dvs. pertinente de depanare.

Mesaj de eroare:%PMAN-3-RELOAD_RP_SB_NOT_READY : Reîncărcare: [caractere]

Explicație	Acțiune recomandată
Procesorul de rută este în curs de reîncărcare deoarece există instanță de așteptare pregătită.	Asigurați-vă că reîncărcarea nu se datorează unei condiții de eroare. nu este o

Mesaj de eroare:%PMAN-3-RELOAD_RP : Reîncărcare: [caractere]

Explicație	Acțiune recomandată

RP-ul este în curs de reîncărcare.	Asigurați-vă că reîncărcarea nu se datorează unei condiții de eroare. Dacă se datorează unei erori, colectați informațiile solicitate de celelalte mesaje de jurnal.

Mesaj de eroare:%PMAN-3-RELOAD_SYSTEM : Reîncărcare: [caractere]

Explicație	Acțiune recomandată
Sistemul este în curs de reîncărcare.	Asigurați-vă că reîncărcarea nu se datorează unei condiții de eroare. Dacă se datorează unei erori, colectați informațiile solicitate de celelalte mesaje de jurnal.

Mesaj de eroare:%PMAN-3-PROC_BAD_EXECUTABLE: executabil greșit sau problemă cu permisiunea procesului [caractere]

Explicație	Acțiune recomandată
Fișierul executabil folosit pentru proces este prost sau are o problemă de permisiune.	Asigurați-vă că executabilul numit este înlocuit cu executabilul corect.

Mesaj de eroare:%PMAN-3-PROC_BAD_COMMAND:Bibliotecă executabilă inexistentă sau proastă folosită pentru procesul <numele procesului>

Explicație	Acțiune recomandată
Fișierul executabil folosit pentru proces lipsește sau o bibliotecă dependentă este proastă.	Asigurați-vă că executabilul numit este prezent și că bibliotecile dependente sunt bune.

Mesaj de eroare:%PMAN-3-PROC_EMPTY_EXEC_FILE : executabil gol folosit pentru proces [caractere]

Explicație	Acțiune recomandată
Fișierul executabil folosit pentru proces este gol.	Asigurați-vă că executabilul numit are dimensiunea diferită de zero.

Mesaj de eroare:%PMAN-5-EXITACTION : Managerul de proces iese: [caractere]

Explicație	Acțiune recomandată
Managerul de proces iese.	Asigurați-vă că managerul de proces nu iese din cauza unei condiții de eroare. Dacă se datorează unei erori, colectați informațiile solicitate de celelalte mesaje de jurnal.

Mesaj de eroare:%PMAN-6-PROCSHUT: Procesul [chars] s-a oprit

Explicație	Acțiune recomandată
Procesul s-a oprit cu grație.	Nu este necesară nicio acțiune a utilizatorului. Acest mesaj este furnizat doar în scop informativ.

Mesaj de eroare:%PMAN-6-PROCSTART: Procesul [chars] a început

Explicație	Acțiune recomandată

Procesul a început și funcționează corect.	Nu este necesară nicio acțiune a utilizatorului. Acest mesaj este furnizat doar în scop informativ.

Mesaj de eroare:%PMAN-6-PROCSTATELESS: Procesul [chars] repornește fără stat

Explicaţie	**Acțiune recomandată**
Procesul a solicitat o repornire fără stat.	Nu este necesară nicio acțiune a utilizatorului. Acest mesaj este furnizat doar în scop informativ.

CAPITOL 38

Monitorizarea Mediului

Acest capitol conține următoarele secțiuni:

Funcții de monitorizare și raportare de mediu

Funcțiile de monitorizare și raportare vă permit să mențineți funcționarea normală a sistemului prin identificarea și rezolvarea condițiilor adverse înainte de pierderea funcționării.

Funcții de monitorizare a mediului

Routerul oferă un sistem robust de monitorizare a mediului cu mai mulți senzori care monitorizează temperaturile sistemului. Următoarele sunt câteva dintre funcțiile cheie ale sistemului de monitorizare a mediului:

- Monitorizarea temperaturii CPU-urilor și a plăcii de bază
- Înregistrarea evenimentelor anormale și generarea de notificări
- Monitorizarea capcanelor SNMP (Simple Network Management Protocol).
- Generarea și colectarea datelor Onboard Failure Logging (OBFL).
- Trimiterea notificărilor de eveniment de apel acasă
- Înregistrarea mesajelor de eroare ale sistemului
- Afișarea setărilor și stării actuale

Funcțiile de monitorizare a mediului utilizează senzori pentru a monitoriza temperatura aerului de răcire pe măsură ce acesta se deplasează prin șasiu.

Se așteaptă ca routerul să îndeplinească următoarele condiții de funcționare de mediu

- Temperatura de nefuncționare: -40°F până la 158°F (-40°C până la 70°C)
- Umiditate nefuncțională: 5 până la 95% umiditate relativă (fără condensare)
- Temperatura de funcționare:
  - 40° până la 140°F (-40° până la 60°C) într-un dulap NEMA etanș, fără flux de aer
  - 40° până la 158°F (-40° până la 70°C) într-un dulap ventilat cu 40 lfm de aer
  - 40° până la 167°F (-40° până la 75°C) într-o incintă cu aer forțat cu 200 lfm de aer
- Umiditate de funcționare: 10% până la 95% umiditate relativă (fără condensare)
- Altitudine de operare: -500 până la 5.000 de picioare. Reduceți temperatura maximă de funcționare cu 1,5°C la 1000 de picioare.

Următorul tabel afișează nivelurile condițiilor de stare utilizate de sistemul de monitorizare a mediului.

Tabelul 26: Niveluri ale condițiilor de stare utilizate de sistemul de monitorizare a mediului

Nivel de stare	Descriere
Normal	Toți parametrii monitorizați se încadrează în toleranța normală.
Avertizare	Sistemul a depășit un prag specificat. Sistemul continuă să funcționeze, dar se recomandă acțiunea operatorului pentru a readuce sistemul la o stare normală.
Critic	Există o temperatură sau o stare de tensiune în afara toleranței. Deși sistemul continuă să funcționeze, se apropie de oprire. Este necesară acțiunea imediată a operatorului.

Sistemul de monitorizare a mediului trimite mesaje de sistem către consolă, de exemplu, când sunt îndeplinite condițiile descrise aici:

Temperatura și tensiunea depășesc pragurile Max/Min

Următorul exemplu prezintă mesajele de avertizare care indică pragurile maxime și minime ale temperaturii sau tensiunii:

```
Avertismente:
- - - - - - - -
Pentru toți senzorii de temperatură (numele care începe cu „Temp:”) de mai sus, pragul
critic de avertizare este 100C (100C și mai mare)
pragul de avertizare este 80C (interval de la 80C la 99C) pragul de avertizare
scăzut este 1C (interval de la -inf la 1C).

Pentru toți senzorii de tensiune (numele care încep cu „V:”),
pragul ridicat de avertizare începe la acea tensiune +10%. (tensiune + 10% este avertizare) pragul scăzut de
avertizare începe la tensiunea -10%. (tensiune - 10% este avertizare)
```

Funcții de raportare de mediu

Puteți prelua și afișa rapoarte privind starea mediului utilizând următoarele comenzi:

- **arată diag toate eeprom**
- **mediu de spectacol**
- **arată mediul tot**
- **arata inventarul**
- **platforma de spectacol**
- **arata platforma diag**
- **arată starea software-ului platformei de control-procesor**
- **afișează detaliul eeprom-ului slotul diag R0**
- **arata versiunea**
- **arata putere**

Aceste comenzi arată valorile curente ale parametrilor precum temperatura și tensiunea.

Sistemul de monitorizare a mediului actualizează valorile acestor parametri la fiecare 60 de secunde. Exemple scurte ale acestor comenzi sunt prezentate mai jos:

arată diag toate eeprom

Router#**arată diag toate eeprom**
Date EEPROM MIDPLANE:

Identificator de produs (PID) : IR1800-K9
Identificator de versiune (VID) : V00
Număr de serie PCB: FOC21482ZQF Număr de
serie PCB: FOC214822CK Număr de serie PCB:
FOC21482SY7 Top Assy. Număr piese:
68-6479-01 Top Assy. Revizia: 13

Revizie hardware: 0.2 ID de
material:
Cod CLEI: NEASIGNAT
Modulul de alimentare/ventilator P0 Datele EEPROM nu sunt inițializate

Modulul de alimentare/ventilator P1 Datele EEPROM nu sunt inițializate

Date EEPROM slot R0:

Identificator de produs (PID) : IR1800-K9
Identificator de versiune (VID) : V00
Număr de serie PCB: FOC21482ZQF Număr de
serie PCB: FOC214822CK Număr de serie PCB:
FOC21482SY7 Top Assy. Număr piese:
68-6479-01 Top Assy. Revizia: 13

Revizie hardware : 0.2 Cod
CLEI : NEASIGNAT

Date EEPROM slot F0:

Identificator de produs (PID) : IR1800-K9
Identificator de versiune (VID) : V00
Număr de serie PCB: FOC21482ZQF Număr de serie PCB: FOC214822CK Număr de serie PCB: FOC21482SY7 Top Assy. Număr piese: 68-6479-01 Top Assy. Revizia: 13

Revizie hardware: 0.2 Cod CLEI: UNASSIGNED Slot 0 Date EEPROM:

Identificator de produs (PID) : IR1800-K9
Identificator de versiune (VID) : V00
Număr de serie PCB: FOC21482ZQF Număr de serie PCB: FOC214822CK Număr de serie PCB: FOC21482SY7 Top Assy. Număr piese: 68-6479-01 Top Assy. Revizia: 13

Revizie hardware : 0.2 Cod
CLEI : NEASIGNAT
Date EEPROM SPA pentru subslot 0/0:

Identificator de produs (PID) : IR1800-ES-5
Identificator de versiune (VID) : V01
Număr de serie PCB:
Top Assy. Număr piese: 68-2236-01 Top Assy.
Revizie: A0
Revizie hardware : 2.2 Cod
CLEI : CNUIAHSAAA
Datele SPA EEPROM pentru subslot 0/1 nu sunt disponibile

Datele SPA EEPROM pentru subslot 0/2 nu sunt disponibile

Datele EEPROM SPA pentru subslot 0/3 nu sunt disponibile

Datele SPA EEPROM pentru subslot 0/4 nu sunt disponibile

Datele EEPROM SPA pentru subslot 0/5 nu sunt disponibile

Router#

arata mediul:

Router#**mediu de spectacol** Număr de alarme critice: 0 Număr de alarme majore: 0 Număr de alarme minore: 0

Pragul de citire a stării curente a senzorului slot (minor, major, critic, oprire)
- R0 Temp. ,90 ,na)(Celsius)

Router#

arată mediul pe toate:

Router#**arată mediul tot** Lista senzorilor:
Monitorizarea mediului Citirea stării locației
senzorului
Temp: LM75BXXX R0 Normal 48 Celsius

arata inventarul:

Router#**arata inventarul**
+ +
+ + + + INFORMAȚII: Utilizați „afișați licența UDI" pentru a obține numărul de serie pentru licențiere.
+ +

NAME: „Șasiu", DESCR: „Router Cisco Catalyst IR1833 Rugged Series" PID: IR1833-K9 , VID: V00 , SN: FCW2447P0EB

NAME: „Modul sursă de alimentare 0", DESCR: „Sursă de alimentare CC Cisco IR1800" PID: PWR-12V , VID: , SN:

NAME: „GE-POE Module", DESCR: „POE Module for On Board GE for Cisco IR183X" PID: IR1800-I-POE , VID: V00 , SN: FOC24382K4W

NAME: „modul 0", DESCR: „Controler NIM Cisco IR-1833-K9 încorporat" PID: IR1833-K9 , VID: , SN:

NAME: „NIM subslot 0/3", DESCR: „Cisco Wide Pluggable Form Factor WIFI6 AP Module" PID: WP-WIFI6-B , VID: V00 , SN: FOC24490FEP

NAME: „NIM subslot 0/4", DESCR: „P-LTEA-LA Module" PID: P-LTEA-LA , VID: V01 , SN: FOC22287JMC

NAME: „Modem pe Cellular0/4/0", DESCR: „Sierra Wireless EM7430" PID: EM7430 , VID: 1.0 , SN: 355813070165276

NAME: „NIM subslot 0/5", DESCR: „P-LTEA-LA Module" PID: P-LTEA-LA , VID: V01 , SN: FOC22287JLZ

NAME: „Modem pe Cellular0/5/0", DESCR: „Sierra Wireless EM7430" PID: EM7430 , VID: 1.0 , SN: 355813070165524

NAME: „NIM subslot 0/0", DESCR: „Modul Gigabitethernet pe panoul frontal 1 port" PID: IR1833-1x1GE, VID: V01, SN:

NAME: „NIM subslot 0/1", DESCR: „IR1833-ES-4" PID: IR1833-ES-4 , VID: V01 , SN:

NAME: „modul R0", DESCR: „Plăcă de bază Cisco IR1833-K9" PID: IR1833-K9 , VID: V00 , SN: FOC24384177

NAME: „modulul F0", DESCR: „Procesor de redirecționare Cisco IR1833-K9" PID: IR1833-K9 , VID: , SN:

platforma de prezentare:

Router#**platforma de spectacol**
Tip șasiu: IR1833-K9

Starea tipului slotului Ora de inserare (acum)
- 0 IR1833-K9 ok
00:04:03
0/0 IR1833-1x1GE ok 00:01:22 0/1 IR1833-
ES-4 ok 00:01:22 0/3 WP-WIFI6-B ok
00:01:22 0/4 P-LTEA-LA ok 00:01:21 0/5 ok:-0
RLTEA IR1833-K9 ok, activ 00:04:03 F0
IR1833-K9 ok, activ 00:04:03 P0 PWR-12V ok
00:02:00

GE-POE IR1800-I-POE ok 00:02:00

arată diagrama platformei:

Router#**arata platforma diag** Tip
șasiu: IR1833-K9

Slot: 0, IR1833-K9
Stare de funcționare: ok Stare internă:
online Stare de funcționare internă: ok

Timp de detectare a inserției fizice: 00:01:09 (acum 00:04:38) Timp de
funcționare declarat software: 00:03:19 (acum 00:02:28) Versiunea CPLD:

Versiunea de firmware: 3.9(REL)

Sub-slot: 0/0, IR1833-1x1GE Stare
operațională: ok Stare internă:
introdus
Ora de detectare a inserției fizice: 00:03:51 (acum 00:01:57) Ora de
detectare a inserției logice: 00:03:51 (acum 00:01:57)

Sub-slot: 0/1, IR1833-ES-4 Stare
operațională: ok Stare internă:
introdus
Ora de detectare a inserției fizice: 00:03:51 (acum 00:01:57) Ora de
detectare a inserției logice: 00:03:51 (acum 00:01:57)

Sub-slot: 0/3, WP-WIFI6 Stare
operațională: ok Stare internă:
introdus
Ora de detectare a inserției fizice: 00:03:51 (acum 00:01:57) Ora de
detectare a inserției logice: 00:03:51 (acum 00:01:57)

Sub-slot: 0/4, P-LTEA-LA Stare
operațională: ok Stare internă:
introdus
Ora de detectare a inserției fizice: 00:03:51 (acum 00:01:56) Ora de
detectare a inserției logice: 00:03:51 (acum 00:01:56)

Sub-slot: 0/5, P-LTEA-LA Stare
operațională: ok Stare internă:
introdus

Ora de detectare a inserției fizice: 00:03:51 (acum 00:01:56) Ora de detectare a inserției logice: 00:03:51 (acum 00:01:56)

Slot: R0, IR1833-K9
Stare de funcționare: ok, activ Stare
internă: online Stare de funcționare
internă: ok
Timp de detectare a inserției fizice: 00:01:09 (acum 00:04:38) Timp de funcționare declarat software: 00:01:09 (acum 00:04:38) Versiunea CPLD: 00000000
Versiunea de firmware: 3.9(REL)

Slot: F0, IR1833-K9
Stare de funcționare: ok, activ Stare
internă: online Stare de funcționare
internă: ok
Timp de detectare a inserției fizice: 00:01:09 (acum 00:04:38) Timp de activare a software-ului: 00:03:30 (acum 00:02:17) Ora semnalului hardware pregătit: 00:00:00 (niciodată în urmă) Timpul semnalului de pachet gata: 00:03:36 (00:02:17 în urmă, versiunea 00:02:00 CP:001)

Versiunea de firmware: 3.9(REL)

Slot: P0, PWR-12V
Stare: ok
Ora detectării inserției fizice: 00:03:13 (acum 00:02:35)

Slot: GE-POE, IR1800-I-POE Stare:
ok
Ora detectării inserției fizice: 00:03:13 (acum 00:02:35)

arată starea software-ului platformei-procesor de control:

Router#**arată starea software-ului platformei de control-procesor** RP0:
online, statistici actualizate acum 9 secunde Încărcare medie: sănătos

1-Min: 0,32, stare: sănătos, sub 5,00 5-Min: 0,33, stare:
sănătos, sub 5,00 15-Min: 0,35, stare: sănătos, sub 5,00
Memorie (kb): sănătos

Total: 3959840
Folosit: 2894588 (73%), stare: sănătos Gratuit:
1065252 (27%)
Angajate: 2435656 (62%), sub 90% Statistici per-
core
CPU0: Utilizare CPU (procent de timp petrecut) Utilizator: 0,50,
Sistem: 0,91, Nice: 0,00, Inactiv: 98,07 IRQ: 0,40, SIRQ: 0,10, IOwait:
0,00
CPU1: Utilizare CPU (procent de timp petrecut) Utilizator: 0,81,
Sistem: 0,30, Nice: 0,00, Inactiv: 98,48 IRQ: 0,20, SIRQ: 0,20, IOwait:
0,00
CPU2: Utilizare CPU (procent de timp petrecut) Utilizator: 0,81,
Sistem: 2,65, Nice: 0,00, Inactiv: 95,41 IRQ: 1,12, SIRQ: 0,00, IOwait:
0,00
CPU3: Utilizare CPU (procent de timp petrecut) Utilizator: 7,66,
Sistem: 17,05, Nice: 0,00, Inactiv: 70,58 IRQ: 4,59, SIRQ: 0,10, IOwait:
0,00
Router#

Afișați detaliul eeprom al slotului diag RO:

Router#**afișează detaliul eeprom-ului slotul diag R0** Slot R0 Date EEPROM: Versiune EEPROM: 4 Tip compatibil: 0xFF Tip controler: 3457 Revizuire hardware: 0.2 Număr piesă PCB: 73-18820-03 Revizia plăcii: 02

Număr abatere: 0 Versiune
Fab: 02
Număr de serie PCB: FOC22106KKH Top Assy.
Număr piese: 68-6479-03 Top Assy. Revizia: 04

Număr de serie al șasiului: FCW2213TH07
Număr abatere: 0
Istoric test RMA: 00 Număr
RMA: 0-0-0-0 Istoric RMA: 00

Identificator de produs (PID) : IR1800-K9
Identificator de versiune (VID) : V00
Cod CLEI: NEASIGNAT
Date de testare de fabricație : 00 00 00 00 00 00 00 00 Date de diagnosticare pe teren : 00 00 00 00 00 00 00 00 Adresa MAC a șasiului : 682c.7b4d.7880
Dimensiunea blocului de adrese MAC: 128
ID de material:
Alias de activ:
Număr piesă PCB: 73-18821-03 Revizia plăcii: 03
Număr abatere: 0 Versiune
Fab: 02
Număr de serie PCB: FOC22106KHD
Număr piesă PCB: 73-19117-02 Revizia plăcii: 02
Număr abatere: 0 Versiune
Fab: 01
Număr de serie PCB: FOC22106KJ9 ID material:
Router#

arata versiunea:

Router#**arata versiunea**
Software Cisco IOS XE, versiunea 17.06.01prd23
Software Cisco IOS [Bengaluru], Software ISR (ARMV8EL_LINUX_IOSD-UNIVERSALK9_IOT-M), Versiunea 17.6.1prd23, SOFTWARE RELEASE (fc1)
Asistență tehnică: http://www.cisco.com/techsupport Copyright (c) 1986-2021 de Cisco Systems, Inc. Compilat marți 20-iul-21 02:28 de mcpre

Software Cisco IOS-XE, Copyright (c) 2005-2021 de către Cisco Systems, Inc. Toate drepturile rezervate. Anumite componente ale software-ului Cisco IOS-XE sunt licențiate sub Licența publică generală GNU („GPL”) versiunea 2.0. Codul software licențiat conform GPL Versiunea 2.0 este un software gratuit care nu vine cu ABSOLUT NU GARANȚIE. Puteți redistribui și/sau modifica un astfel de cod GPL în conformitate cu termenii GPL Versiunea 2.0. Pentru mai multe detalii, consultați documentația sau fișierul „Notă de licență” care însoțește software-ul IOS-XE sau adresa URL aplicabilă furnizată în pliantul care însoțește software-ul IOS-XE.

ROM: 3.9(REL)

Durata de funcționare a IR1833 este de 13 ore și 6 minute
Timpul de funcționare pentru acest procesor de control este de 13 ore și 9 minute.
Sistemul a revenit la ROM prin Upgrade de firmware
Fișierul imagine de sistem este „bootflash:ir1800-universalk9.17.06.01prd23.SPA.bin” Ultimul motiv de reîncărcare: Comanda de reîncărcare

Acest produs conține caracteristici criptografice și este supus legilor Statelor Unite și ale țărilor locale care reglementează importul, exportul, transferul și utilizarea. Livrarea produselor criptografice Cisco nu implică o autoritate terță parte pentru a importa, exporta, distribui sau utiliza criptarea. Importatorii, exportatorii, distribuitorii și utilizatorii sunt responsabili pentru respectarea legilor din SUA și ale țărilor locale. Prin utilizarea acestui produs sunteți de acord să respectați legile și reglementările aplicabile. Dacă nu puteți respecta legile locale și americane, returnați imediat acest produs.

Un rezumat al legilor SUA care guvernează produsele criptografice Cisco poate fi găsit la: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

Dacă aveți nevoie de asistență suplimentară, vă rugăm să ne contactați trimițând un e-mail la export@cisco.com .

Informații privind licența pachetului de tehnologie:
---------- Tip de tehnologie Pachet de tehnologie Pachet de tehnologie
Următoarea repornire curentă

Nivelul curent de debit este de 50000 kbps
Stare de licență inteligentă: Înregistrare Nu se aplică/Nu se aplică Procesor cisco IR1833-K9 (1RU) cu 470123K/6147K octeți de memorie. ID placă procesor FCW2447P0EB

Mod de operare al routerului: Versiune de
bootloader MCU autonom: 0x22
Versiunea aplicației MCU: 0x4d 1
interfață Ethernet virtuală 6 interfețe
Gigabit Ethernet 2 interfețe seriale

1 linie terminală
4 interfețe celulare
32768K octeți de memorie de configurare nevolatilă. 3988088K octeți de memorie fizică.
7475198K octeți de Bootflash la bootflash:. Registrul de configurare este 0x2102

arată puterea:

Router#**arata putere**
PSU principal:
Putere totală consumată: 8,16 wați Router#

Sondaj SNMP pentru OID de temperatură

A fost adăugat suport pentru SNMP MIB pentru a putea returna valori de la senzorii de temperatură. Ieșirea ar trebui să arate similar cu**mediu de spectacol**CLI.

Ieșirea a**mediu de spectacol**pe un IR1101:

```
IR1101#mediu de spectacol

Număr de alarme critice: Număr de    0
alarme majore: Număr de alarme       0
minore:                              0

 Slot          Senzor              Starea actuală      Lectură
Prag (minor, major, critic, oprire)
 ------------------------------------------------------------------------
---------------------------------------- R0
               Temp: TS1           Normal              42      Celsius
 R0            Temp: TS2           Normal              37      Celsius
```

(75 ,80 ,90 ,na)(Celsius) (75 ,80 ,90 ,na)(Celsius)

Ieșirea dintr-un snmpwalk ar arăta similar cu acesta:

```
[root@sg-centos-hv ~]#snmpwalk -v 2c -c public 33.33.33.204 1.3.6.1.4.1.9.9.13.1.3.1 SNMPv2-
SMI::întreprinderi.9.9.13.1.3.1.2.1 = STRING: „Senzor 1” SNMPv2-SMI::întreprinderi.9.9.13.1.3.1.3.1 = Gauge32: 48
SNMPv2-SMI::1.9întreprinderi.13.1..9.13.1..3. ÎNTREG: 93 SNMPv2-SMI::întreprinderi.9.9.13.1.3.1.5.1 = ÎNTREG: 0
SNMPv2-SMI::întreprinderi.9.9.13.1.3.1.6.1 = ÎNTREG: 1 SNMPv2-SMI:::1.9.13.1.9. INTREG: 0
```

Oidul ciscoEnvMonTemperatureStatusEntry este 1.3.6.1.4.1.9.9.13.1.3.1:

- ciscoEnvMonTemperatureStatusIndex (.1)
- ciscoEnvMonTemperatureStatusDescr (.2)
- ciscoEnvMonTemperatureStatusValue (.3)
- ciscoEnvMonTemperatureThreshold (.4)
- ciscoEnvMonTemperatureLastShutdown (.5)
- ciscoEnvMonTemperatureStatus (.6)

Referințe suplimentare

Următoarele secțiuni oferă referințe legate de caracteristica de gestionare a eficienței energetice.

MIB-uri

MIB-uri	Link-uri MIB
CISCO-ENTITATE-FRU-CONTROL-MIB	Pentru a localiza și descărca MIB-uri pentru anumite platforme, versiuni Cisco IOS și seturi de caracteristici, utilizați Cisco MIB Locator la: http://www.cisco.com/go/mibs.

Asistență tehnică

Descriere	Legătură
Site-ul web de asistență Cisco oferă resurse online extinse, inclusiv documentație și instrumente pentru depanarea și rezolvarea problemelor tehnice cu produsele și tehnologiile Cisco. Pentru a primi informații tehnice și de securitate despre produsele dvs., vă puteți abona la diferite servicii, cum ar fi Instrumentul de alertă de produs (accesat din Field Notices), Buletinul informativ al Serviciilor tehnice Cisco și Feed-uri Really Simple Syndication (RSS). Accesul la majoritatea instrumentelor de pe site-ul web de asistență Cisco necesită un ID de utilizator și o parolă Cisco.com.	http://www.cisco.com/cisco/web/support/index.html

Asistență tehnică

CAPITOL 39

Monitorizarea sănătății proceselor

Acest capitol descrie cum să gestionați și să monitorizați starea diferitelor componente ale routerului dumneavoastră. Acesta conține următoarele secțiuni:

Monitorizarea resurselor planului de control

Următoarele secțiuni explică detaliile monitorizării memoriei și CPU din perspectiva procesului Cisco IOS și a planului de control general:

Evitarea problemelor prin monitorizare regulată

Procesele ar trebui să asigure monitorizarea și notificarea stării/sănătății lor pentru a asigura funcționarea corectă. Când un proces eșuează, este afișat un mesaj de eroare syslog și fie procesul este repornit, fie routerul este repornit. Un mesaj de eroare syslog este afișat atunci când un monitor detectează că un proces este blocat sau s-a blocat. Dacă procesul poate fi repornit, este repornit; altfel, routerul este repornit.

Monitorizarea resurselor sistemului vă permite să detectați potențialele probleme înainte ca acestea să apară, evitând astfel întreruperile. De asemenea, stabilește o linie de bază pentru o încărcare normală a sistemului. Puteți utiliza aceste informații ca bază pentru comparație, atunci când faceți upgrade hardware sau software pentru a vedea dacă upgrade-ul a afectat utilizarea resurselor.

Resurse de proces Cisco IOS

Puteți vizualiza statisticile de utilizare a CPU pentru procesele active și puteți vedea cantitatea de memorie utilizată în aceste procese folosind**arata memoria**comanda și**arata procesorul procesorului**comanda. Aceste comenzi oferă o reprezentare a memoriei și a utilizării CPU din perspectiva doar a procesului Cisco IOS; nu includ informații pentru resurse de pe întreaga platformă. Când**arata memoria**comanda este utilizată într-un sistem cu 4 GB RAM care rulează un singur proces Cisco IOS, este afișată următoarea utilizare a memoriei:

```
Router#arata memoria
Cheie de urmărire: 1#b93c0f1c0d5d16ddc3ab8e54342a8dd5

                     Cap          Total(b)     Folosit(b)   gratuit (b)  Cel mai mic(b) Cel mai mare(b)
Procesor 7F5F358048          1997625144    290200588    1707424556    487419128 1509949348
```

```
rezerva P      7F5F3580A0      102404          92      102312      102312      102312
lsmpi_io       7F5D9901A8     6295128       6294304         824         824         412
Limită dinamică heap (MB) 1440          Utilizați (MB) 0

                Memoria procesorului

Adresa          octeți          Prev        Următorul       Ref     PrevF       UrmătorulF      ce
    Alloc PC
7F5F358048 0000102408 00000000 7F5F3710A8 001           ---------------* Init*
:555F22A000+5E5691C
7F5F3710A8 0000000056 7F5F358048 7F5F371138 001         ---------------* Init*
:555F22A000+5E56938
7F5F371138 0000008224 7F5F3710A8 7F5F3731B0 001         ---------------* Init*
:555F22A000+5E56958
7F5F3731B0 0000000296 7F5F371138 7F5F373330 001         ---------------* Init*
:555F22A000+86B9178
7F5F373330 0000000568 7F5F3731B0 7F5F3735C0 001         ---------------* Init*
:555F22A000+86BEE5C
7F5F3735C0 0000032776 7F5F373330 7F5F37B620 001         ---------------Porțiune gestionată Q
:555F22A000+86AAC38
7F5F37B620 0000000056 7F5F3735C0 7F5F37B6B0 001         ---------------* Init*
:555F22A000+5EA29DC
7F5F37B6B0 0000032776 7F5F37B620 7F5F383710 001         ---------------Pereche de coadă - Q
:555F22A000+86D3A28
7F5F383710 0000012808 7F5F37B6B0 7F5F386970 001         ---------------* Init*
:555F22A000+11EFF930
7F5F386970 0000032776 7F5F383710 7F5F38E9D0 001         ---------------Lista Elemente
:555F22A000+86798AC
7F5F38E9D0 0000032776 7F5F386970 7F5F396A30 001         ---------------Lista antete
:555F22A000+86798EC
7F5F396A30 0000032776 7F5F38E9D0 7F5F39EA90 001         ---------------Procesul IOSXE S
:555F22A000+984FEE0
7F5F39EA90 0000032776 7F5F396A30 7F5F3A6AF0 001         ---------------IOSXE Queue Pro
:555F22A000+984FF24
7F5F3A6AF0 0000065544 7F5F39EA90 7F5F3B6B50 001         ---------------Bal. coadă IOSXE
:555F22A000+984FF68
7F5F3B6B50 0000000328 7F5F3A6AF0 7F5F3B6CF0 001         ---------------* Init*
:555F22A000+11EF88AC
7F5F3B6CF0 0000000328 7F5F3B6B50 7F5F3B6E90 001         ---------------* Init*
:555F22A000+11EF88AC
7F5F3B6E90 0000000192 7F5F3B6CF0 7F5F3B6FA8 001         ---------------SDB String
:555F22A000+8629F60
7F5F3B6FA8 0000036872 7F5F3B6E90 7F5F3C0008 001         ---------------* Init*
:555F22A000+98482F4
7F5F3C0008 0000010008 7F5F3B6FA8 7F5F3C2778 001         ---------------Platforma VM Pag
:555F22A000+986FC68
7F5F3C2778 0000002008 7F5F3C0008 7F5F3C2FA8 001         ---------------* Init*
iosd_crb_crankshaft_unix:7F83050000+6D850 7F5F3C2FA8
0000277573C 7F5F3F4008 001 :555F22A000+98482F4          ---------------Întrerupe stiva

7F5F3F4008 0000000328 7F5F3C2FA8 7F5F3F41A8 001         ---------------* Init*
:555F22A000+11EF88AC
7F5F3F41A8 0000002008 7F5F3F4008 7F5F3F49D8 001         ---------------Mesaj observator
:555F22A000+86DE21C
7F5F3F49D8 0000000360 7F5F3F41A8 7F5F3F4B98 001         ---------------Procesează evenimente
:555F22A000+86D94A4
7F5F3F4B98 0000000328 7F5F3F49D8 7F5F3F4D38 001         ---------------* Init*
:555F22A000+11EF88AC
7F5F3F4D38 0000000184 7F5F3F4B98 7F5F3F4E48 001         ---------------* Init*
:555F22A000+86C945C
7F5F3F4E48 0000000264 7F5F3F4D38 7F5F3F4FA8 001         ---------------* Init*
:555F22A000+86C945C
7F5F3F4FA8 0000036872 7F5F3F4E48 7F5F3FE008 001         ---------------* Init*
:555F22A000+98482F4
```

```
7F5F3FE008 0000000328 7F5F3F4FA8 7F5F3FE1A8 001                 ---------------- * Init*
:555F22A000+11EF88AC
7F5F3FE1A8 0000001504 7F5F3FE008 7F5F3FE7E0 001                 ---------------- Reg Function Se
:555F22A000+868AE50
7F5F3FE7E0 0000001504 7F5F3FE1A8 7F5F3FEE18 001                 ---------------- Reg Function Se
:555F22A000+868AEE0
7F5F3FEE18 0000000064 7F5F3FE7E0 7F5F3FEEB0 001                 ---------------- Legătura parserului
:555F22A000+5D98838
7F5F3FEEB0 0000000160 7F5F3FEE18 7F5F3FEFA8 001                 ---------------- * Init*
:555F22A000+530A17C
7F5F3FEFA8 0000036872 7F5F3FEEB0 7F5F408008 001                 ---------------- * Init*
:555F22A000+98482F4
7F5F408008 0000000328 7F5F3FEFA8 7F5F4081A8 001                 ---------------- * Init*
:555F22A000+11EF88AC
7F5F4081A8 0000000760 7F5F408008 7F5F4084F8 001                 ---------------- * Init*
:555F22A000+868BC18
7F5F4084F8 0000000576 7F5F4081A8 7F5F408790 001                 ---------------- * Init*
:555F22A000+868BC18
7F5F408790 0000000400 7F5F4084F8 7F5F408978 001                 ---------------- * Init*
:555F22A000+868BC18
7F5F408978 0000000488 7F5F408790 7F5F408BB8 001                 ---------------- * Init*
:555F22A000+868BC18
7F5F408BB8 0000000920 7F5F408978 7F5F408FA8 001                 ---------------- * Init*
:555F22A000+868BC18
7F5F408FA8 0000200712 7F5F408BB8 7F5F43A008 001                 ---------------- Întrerupe stiva
:555F22A000+98482F4
7F5F43A008 0000000968 7F5F408FA8 7F5F43A428 001                 ---------------- * Init*
iosd_crb_crankshaft_unix:7F83050000+378C0 7F5F43A428
0000007005F43A428 7F5F43A598 001 :555F22A000+A3CE294            ---------------- * Init*

7F5F43A598 0000000896 7F5F43A428 7F5F43A970 001                 ---------------- Mesaj urmărit
:555F22A000+86DE1E8
7F5F43A970 0000001320 7F5F43A598 7F5F43AEF0 001                 ----------------- Proces
:555F22A000+86E50BC
7F5F43AEF0 0000000096 7F5F43A970 7F5F43AFA8 001                 ---------------- * Init*
:555F22A000+868BC18
7F5F43AFA8 0000036872 7F5F43AEF0 7F5F444008 001                 ---------------- * Init*
:555F22A000+98482F4
7F5F444008 0000003008 7F5F43AFA8 7F5F444C20 001                 ----------------- Am urmărit Semapho
:555F22A000+86DE180
7F5F444C20 0000000360 7F5F444008 7F5F444DE0 001                 ---------------- Procesează evenimente
:555F22A000+86D94A4
7F5F444DE0 0000000368 7F5F444C20 7F5F444FA8 001                 ---------------- * Init*
:555F22A000+11EF88AC
7F5F444FA8 0000200712 7F5F444DE0 7F5F476008 001                 ---------------- Întrerupe stiva
:555F22A000+98482F4
7F5F476008 0000002336 7F5F444FA8 7F5F476980 001                 ----------------- Process Array
:555F22A000+86E4F94
7F5F476980 0000000184 7F5F476008 7F5F476A90 001                 ---------------- * Init*
:555F22A000+86C945C
7F5F476A90 0000000184 7F5F476980 7F5F476BA0 001                 ---------------- * Init*
:555F22A000+86C945C
7F5F476BA0 0000000184 7F5F476A90 7F5F476CB0 001                 ---------------- * Init*
:555F22A000+86C945C
7F5F476CB0 0000000184 7F5F476BA0 7F5F476DC0 001                 ---------------- * Init*
:555F22A000+86C945C
7F5F476DC0 0000000184 7F5F476CB0 7F5F476ED0 001                 ---------------- * Init*
:555F22A000+86C945C
7F5F476ED0 0000000128 7F5F476DC0 7F5F476FA8 001                 ---------------- * Init*
:555F22A000+868BC18
7F5F476FA8 0000036872 7F5F476ED0 7F5F480008 001                 ---------------- * Init*
:555F22A000+98482F4
7F5F480008 0000001320 7F5F476FA8 7F5F480588 001                 ----------------- Proces
:555F22A000+86E50BC
```

```
7F5F480588 0000000184 7F5F480008 7F5F480698 001 ---------- * Init*
:555F22A000+86C945C
7F5F480698 0000000184 7F5F480588 7F5F4807A8 001 ---------- * Init*
:555F22A000+86C945C
7F5F4807A8 0000000184 7F5F480698 7F5F4808B8 001 ---------- * Init*
:555F22A000+86C945C
7F5F4808B8 0000000184 7F5F4807A8 7F5F4809C8 001 ---------- * Init*
:555F22A000+86C945C
7F5F4809C8 0000000184 7F5F4808B8 7F5F480AD8 001 ---------- * Init*
:555F22A000+86C945C
7F5F480AD8 0000000184 7F5F4809C8 7F5F480BE8 001 ---------- * Init*
:555F22A000+86C945C
7F5F480BE8 0000000184 7F5F480AD8 7F5F480CF8 001 ---------- * Init*
:555F22A000+86C945C
7F5F480CF8 0000000096 7F5F480BE8 7F5F480DB0 001 ---------- * Init*
:555F22A000+86C940C
7F5F480DB0 0000000096 7F5F480CF8 7F5F480E68 001 ---------- Init
:555F22A000+862A110
7F5F480E68 0000000232 7F5F480DB0 7F5F480FA8 001 ---------- * Init*
:555F22A000+60E2660
7F5F480FA8 0000200712 7F5F480E68 7F5F4B2008 001 ---------- Întrerupe stiva
:555F22A000+98482F4
7F5F4B2008 0000003008 7F5F480FA8 7F5F4B2C20 001 ---------- Reg Function Li
:555F22A000+868AE80
7F5F4B2C20 0000000064 7F5F4B2008 7F5F4B2CB8 001 ---------- Legătura parserului
:555F22A000+5D98838
7F5F4B2CB8 0000000064 7F5F4B2C20 7F5F4B2D50 001 ---------- Legătura parserului
:555F22A000+5D98A78
7F5F4B2D50 0000000080 7F5F4B2CB8 7F5F4B2DF8 001 ---------- Init
:555F22A000+5E87AC0
7F5F4B2DF8 0000000200 7F5F4B2D50 7F5F4B2F18 001 ---------- Init
:555F22A000+5E87AC0
7F5F4B2F18 0000000056 7F5F4B2DF8 7F5F4B2FA8 001 ---------- Init
:555F22A000+54DD60C
7F5F4B2FA8 0000036872 7F5F4B2F18 7F5F4BC008 001 ---------- * Init*
:555F22A000+98482F4
7F5F4BC008 0000001504 7F5F4B2FA8 7F5F4BC640 001 ---------- Reg Function Ca
:555F22A000+868AF10
7F5F4BC640 0000000224 7F5F4BC008 7F5F4BC778 001 ---------- * Init*
:555F22A000+868BC18
7F5F4BC778 0000000224 7F5F4BC640 7F5F4BC8B0 001 ---------- * Init*
:555F22A000+868BC18
7F5F4BC8B0 0000000328 7F5F4BC778 7F5F4BCA50 001 ---------- * Init*
:555F22A000+868BC18
7F5F4BCA50 0000000328 7F5F4BC8B0 7F5F4BCBF0 001 ---------- * Init*
:555F22A000+868BC18
7F5F4BCBF0 0000000328 7F5F4BCA50 7F5F4BCD90 001 ---------- * Init*
:555F22A000+868BC18
7F5F4BCD90 0000000216 7F5F4BCBF0 7F5F4BCEC0 001 ---------- Init
:555F22A000+5E87AC0
7F5F4BCEC0 0000000144 7F5F4BCD90 7F5F4BCFA8 001 ---------- Init
:555F22A000+530F7A4
7F5F4BCFA8 0000200712 7F5F4BCEC0 7F5F4EE008 001 ---------- Întrerupe stiva
:555F22A000+98482F4
7F5F4EE008 0000006888 7F5F4BCFA8 7F5F4EFB48 001 ---------- Date TTY
:555F22A000+85C9E44
7F5F4EFB48 0000004104 7F5F4EE008 7F5F4F0BA8 001 ---------- Buf de intrare TTY
:555F22A000+85CBD60
7F5F4F0BA8 0000004104 7F5F4EFB48 7F5F4F1C08 001 ---------- Buf de ieșire TTY
:555F22A000+85CBDB0
7F5F4F1C08 0000024584 7F5F4F0BA8 7F5F4F7C68 001 ---------- proc_hist_lmt_v
:555F22A000+BA3B718
7F5F4F7C68 0000008200 7F5F4F1C08 7F5F4F9CC8 001 ---------- proc_hist_lmt_v
:555F22A000+BA3B74C
```

```
7F5F4F9CC8 0000008200 7F5F4F7C68 7F5F4FBD28 001 ---------- proc_hist_lmt_v
:555F22A000+BA3B784
7F5F4FBD28 0000005008 7F5F4F9CC8 7F5F4FD110 001 ---------- mesaje
:555F22A000+86DE040
7F5F4FD110 0000005008 7F5F4FBD28 7F5F4FE4F8 001 ---------- Mesaj urmărit
:555F22A000+86DE078
7F5F4FE4F8 0000020008 7F5F4FD110 7F5F503378 001 ---------- Coada de urmărire
:555F22A000+86DE0AC
7F5F503378 0000065544 7F5F4FE4F8 7F5F5133D8 001 ---------- Coada I urmărită
:555F22A000+86DE0E4
7F5F5133D8 0000020008 7F5F503378 7F5F518258 001 ---------- Vizionat boolean
:555F22A000+86DE118
7F5F518258 0000020008 7F5F5133D8 7F5F51D0D8 001 ---------- Am urmărit Bitfiel
:555F22A000+86DE14C
7F5F51D0D8 0000010008 7F5F518258 7F5F51F848 001 ---------- Informații observator
:555F22A000+86DE1B4
7F5F51F848 0000010008 7F5F51D0D8 7F5F521FB8 001 ---------- Blocare citire/scriere
:555F22A000+86DE250
7F5F521FB8 0000001232 7F5F51F848 7F5F5224E0 001 ---------- * Init*
:555F22A000+868BC18
7F5F5224E0 0000000064 7F5F521FB8 7F5F522578 001 ---------- Init
:555F22A000+8D8F3A0
7F5F522578 0000002008 7F5F5224E0 7F5F522DA8 001 ---------- Mesaj injectat CB
:555F22A000+ACBBF08
7F5F522DA8 0000000064 7F5F522578 7F5F522E40 001 ---------- SDB String
:555F22A000+8629F60
7F5F522E40 0000000056 7F5F522DA8 7F5F522ED0 001 ---------- * Init*
:555F22A000+5EA29DC
7F5F522ED0 0000000128 7F5F522E40 7F5F522FA8 001 ---------- XOS_MEM_XDT
:555F22A000+894FE1C
7F5F522FA8 0000028104 7F5F522ED0 7F5F529DC8 001 ---------- Stiva de procese
:555F22A000+98482F4
7F5F529DC8 0000000096 7F5F522FA8 7F5F529E80 001 ---------- Init
:555F22A000+862A110
7F5F529E80 0000000208 7F5F529DC8 7F5F529FA8 001 ---------- * Init*
:555F22A000+86C8D58
7F5F529FA8 0000016104 7F5F529E80 7F5F52DEE8 001 ---------- Stiva de procese
:555F22A000+98482F4
7F5F52DEE8 0000032776 7F5F529FA8 7F5F535F48 001 ---------- Lista Elemente
:555F22A000+8679DCC
7F5F535F48 0000032776 7F5F52DEE8 7F5F53DFA8 001 ---------- Lista Elemente
:555F22A000+8679DCC
7F5F53DFA8 0000032776 7F5F535F48 7F5F546008 001 ---------- Lista Elemente
:555F22A000+8679DCC
7F5F546008 0000032776 7F5F53DFA8 7F5F54E068 001 ---------- Lista Elemente
:555F22A000+8679DCC
7F5F54E068 0000032776 7F5F546008 7F5F5560C8 001 ---------- Lista Elemente
:555F22A000+8679DCC
7F5F5560C8 0000032776 7F5F54E068 7F5F55E128 001 ---------- Lista Elemente
:555F22A000+8679DCC
7F5F55E128 0000032776 7F5F5560C8 7F5F566188 001 ---------- Lista Elemente
:555F22A000+8679DCC
7F5F566188 0000032776 7F5F55E128 7F5F56E1E8 001 ---------- Lista Elemente
:555F22A000+8679DCC
7F5F56E1E8 0000005008 7F5F566188 7F5F56F5D0 001 ---------- Funcția Reg 12
:555F22A000+868AE1C
7F5F56F5D0 0000020008 7F5F56E1E8 7F5F574450 001 ---------- Subsys Malloc I
:555F22A000+86875C8
7F5F574450 0000001176 7F5F56F5D0 7F5F574940 001 ---------- Variabila SPA ms
:555F22A000+B9B3700
7F5F574940 0000000920 7F5F574450 7F5F574D30 001 ---------- SAMsgThread
:555F22A000+54E49DC
7F5F574D30 0000000064 7F5F574940 7F5F574DC8 001 ---------- Legătura parserului
:555F22A000+5D98A78
```

```
7F5F574DC8 0000000064 7F5F574D30 7F5F574E60 001          ---------------- Legătura parserului
:555F22A000+5D98838
7F5F574E60 0000000064 7F5F574DC8 7F5F574EF8 001          ---------------- Legătura parserului
:555F22A000+5D98A78
7F5F574EF8 0000000088 7F5F574E60 7F5F574FA8 001          ---------------- Init
:555F22A000+54DD60C
7F5F574FA8 0000000968 7F5F574EF8 7F5F5753C8 001          ---------------- Crypto CA
:555F22A000+8DC26C0
7F5F5753C8 0000000216 7F5F574FA8 7F5F5754F8 001          ---------------- Crypto CA
:555F22A000+8DC2588
7F5F5754F8 0000002648 7F5F5753C8 7F5F575FA8 000          7F609C3C28 7F69C82D38 (coalesced)
:555F22A000+52BC2B8
7F5F575FA8 0000028104 7F5F5754F8 7F5F57CDC8 001          ---------------- Stiva de procese
:555F22A000+98482F4
7F5F57CDC8 0000013112 7F5F575FA8 7F5F580158 001          ---------------- SAMsgThread
:555F22A000+5360944
7F5F580158 0000004728 7F5F57CDC8 7F5F581428 001          ---------------- * Pachet de date*
:555F22A000+AF448CC
7F5F581428 0000000968 7F5F580158 7F5F581848 001          ---------------- Exec
:555F22A000+5D9C004
7F5F581848 0000000600 7F5F581428 7F5F581AF8 001          ---------------- Eter OAM subbl
:555F22A000+962A100
7F5F581AF8 0000000056 7F5F581848 7F5F581B88 000          7F69F8B620 7F6A906D40 (fragment)
:555F22A000+962A100
7F5F581B88 0000005008 7F5F581AF8 7F5F582F70 001          ---------------- Reg Function iL
:555F22A000+868AEB0
7F5F582F70 0000065544 7F5F581B88 7F5F592FD0 001          ---------------- Apel de registru S
:555F22A000+8690EFC
7F5F592FD0 0000002584 7F5F582F70 7F5F593A40 001          ---------------- * Init*
:555F22A000+868BC18
7F5F593A40 0000002080 7F5F592FD0 7F5F5942B8 001          ---------------- * Init*
:555F22A000+ACB41D8
7F5F5942B8 0000002600 7F5F593A40 7F5F594D38 001          ---------------- * Init*
:555F22A000+ACB41D8
7F5F594D38 0000020008 7F5F5942B8 7F5F599BB8 001          ---------------- Peer uid cb chu
:555F22A000+ACBBE98
```

The**arata procesorul procesorului**comanda afișează media de utilizare a procesorului Cisco IOS:

```
Router#arata procesorul procesorului
Utilizarea procesorului timp de cinci secunde: 0%/0%; un minut: 0%; cinci minute: 0% PID Runtime
(ms)                   Invocat      uSecs     5 sec     1 min   Proces TTY de 5 minute
  1           8           31        258 0,00% 0,00% 0,00%        0 Chink Manager
  2           8        10141          0 0,00% 0,00% 0,00% 0 0,00%  0 Contor de sarcină
  3           0            1          0,00% 0,00% 0 0,00% 0,00%    0 PKI Trustpool
  4           0            1          0,00% 0 0,00% 0,00% 0,00%    0 Retransmisie o
  5           0            1          2153 0,00% 0,00% 0,00%       0 IPC ISSU Dispatc 0 RF
  6          28           13                                       Slave Main Th 0
  7           0            1          0 0,00% 0,00% 0,00% 0 0,00%  EDDRI_MAIN
  8           0            1          0,00% 0,00% 5182 0,00%       0 RO Notificare cronometre
  9       40648         7844       0,06% 0,05%                     0 Verificați grămezi
 10          16          845         18 0,00% 0,00% 0,00% 0 0,00%  0 Manager de bazin
 11           0            1          0,00% 0,00% 0 0,00% 0,00%    0 DiscardQ Backgro
 12           0            2          0,00% 0 0,00% 0,00% 0,00% 0  0 Temporizatoare
 13           0          176          0,00% 0,00% 0,00% 0,00%      0 WATCH_AFS
 14           0            1          0,00% 0,00% 0,00% 0,00%      0 PROCES MEMLEAK
 15           0            1          0,00% 0 0,00% 0,00% 0,00% 0  0 Intrare ARP
 16           4        52892          0,00% 0,00% 0,00% 0 0,00%    0 Fundal ARP
 17           0            2          0,00% 0,00% 0 0,00% 0,00%    0 ATM Idle Timer 0
 18           0            1          0,00%                        ATM ASYNC PROC 0
 19           0            1                                       CEF MIB API
```

20	0	1	0 0,00% 0,00% 0,00% 0 0,00%	0 AAA_SERVER_DEADT
21	0	1	0,00% 0,00% 0 0,00% 0,00%	0 Manager de politici
22	0	2	0,00% 1600 0,00% 0,00%	0 cronometre DDR
23	16	10	0,00% 4444 0,00% 0,00% 0,00%	0 Entity MIB API 0
24	120	27	0,00%	PrstVbl
25	0	2	0 0,00% 0,00% 0,00% 0 0,00%	0 Fundal serial
26	0	1	0,00% 0,00% 0 0,00% 0,00%	0 RMI RM Notify Wa 0
27	0	2	0,00% 0 0,00% 0,00% 0,00% 0	ATM AutoVC Perio 0 ATM
28	0	2	0,00% 0,00% 0,00% 0,00%	VC Auto Crea 0 IOSXE
29	4	25354	0,00% 0,00% 0,00% 0,00%	heartbeat
30	0	86	0,00% 0 0,00% 0,00% 0,00% 0	0 Btrace baza de timp 0
31	0	10	0,00% 0,00% 0,00% 0 0,00%	DB Lock Manager 0
32	4	50697	0,00% 0,00% 0 0,00% 0,00%	GraphIt
33	0	1	0,00% 0 0,00% 0,00% 0,00%	0 DB Notificare
34	0	1	0,00% 0,00% 0,00% 0,00%	0 Sarcină aplicații IPC
35	0	1	0,00% 0,00% 0 0,00% 0,00%	0 ifIndex Primire
36	0	10142	0,00% 0 0,00% 0,00% 0,00% 0	0 IPC Event Notifi 0 IPC
37	0	49518	0,00% 0,00% 0,00% 0 0,00%	Mcast Pendin 0 Platform
38	0	1	0,00% 0,00% 0,00% 0,00%	appsess
39	0	846	0,00% 0,00% 0,00% 0,00%	0 IPC Dynamic Cach 0
40	0	10142	0,00% 0,00% 0,00% 0 0,00%	IPC Service NonC 0 IPC
41	0	1	0,00% 0,00% 0 0,00% 0,00%	Zone Manager 0 IPC
42	8	49518	0,00% 0 0,00% 0,00% 0,00%	Periodic Tim 0 IPC
43	0	49518		Defered Por 0 IPC
44	0	1		Process level 0 IPC Seat
45	0	1		Manager

arata procesul procesor platforma sortate

Utilizarea procesorului timp de cinci secunde: 9%, un minut: 10%, cinci minute: 10% Core 0:
Utilizarea procesorului timp de cinci secunde: 3%, un minut: 4%, cinci minute: 4%
Nucleul 1: Utilizarea procesorului timp de cinci secunde: 4%, un minut: 4%, cinci minute: 4%
Nucleul 2: Utilizarea procesorului timp de cinci secunde: 2%, un minut: 2%, cinci minute: 2%
Core 3: Utilizarea procesorului timp de cinci secunde: 38%, un minut: 38%, cinci minute: 38%

Pid	PPid	5Sec	1Min	5Min	Stare	Nume mărime	
18700							
	18679	44%	44%	44%	S	235192	qfp-ucode-avent
5226	5216	2%	3%	3%	S	697124	linux_iosd-imag
24238	24231	1%	1%	1%	S	8288	ngiolit
18412	18398	1%	1%	1%	S	135696	fman_fp_image
30574	2	0%	0%	0%	S	0	kworker/0:3
24231	16366	0%	0%	0%	S	2460	pman
24025	23998	0%	0%	0%	S	3392	nginx
24024	23998	0%	0%	0%	S	4300	nginx
23998	23990	0%	0%	0%	S	7944	nginx
23990	4251	0%	0%	0%	S	2460	pman
23605	23599	0%	0%	0%	S	7988	ngiolit
23599	16366	0%	0%	0%	S	2464	pman
23330	23309	0%	0%	0%	S	39600	iomd
23309	16366	0%	0%	0%	S	2460	pman
21981	15002	0%	0%	0%	S	416	dormi
21935	21906	0%	0%	0%	S	38680	iomd
21906	16366	0%	0%	0%	S	2460	pman
21830	13884	0%	0%	0%	S	416	dormi
21694	2	0%	0%	0%	S	0	kworker/0:0
21042	2	0%	0%	0%	S	0	kworker/u8:4
21041	2	0%	0%	0%	S	0	kworker/u8:3
21040	2	0%	0%	0%	S	0	kworker/u8:0
20737	2	0%	0%	0%	S	0	kworker/1:3
20731	2	0%	0%	0%	S	0	SarIosdMond
20574	20548	0%	0%	0%	S	12004	btman
20548	16921	0%	0%	0%	S	2432	pman
20180	20146	0%	0%	0%	S	17428	cman_fp
20146	16921	0%	0%	0%	S	2432	pman
20135	20105	0%	0%	0%	S	12228	btman

20105	16366	0%	0%	0%	S	2432	pman
20093	2	0%	0%	0%	S	0	kworker/0:1
19819	19796	0%	0%	0%	S	107992	cpp_cp_svr
19796	16921	0%	0%	0%	S	2436	pman
19549	19528	0%	0%	0%	S	18948	cmcc
19541	19512	0%	0%	0%	S	35124	cpp_driver
19528	16366	0%	0%	0%	S	2432	pman
19512	16921	0%	0%	0%	S	2432	pman
19280	19243	0%	0%	0%	S	38708	cpp_ha_top_leve
19243	16921	0%	0%	0%	S	2436	pman
18966	18959	0%	0%	0%	S	49916	cpp_sp_svr
18959	16921	0%	0%	0%	S	2436	pman
18877	18862	0%	0%	0%	S	5780	pttcd
18862	4251	0%	0%	0%	S	2432	pman
18856	2	0%	0%	0%	S	0	kworker/1:1
18711	18691	0%	0%	0%	S	10352	hman
18691	16366	0%	0%	0%	S	2432	pman
18679	16921	0%	0%	0%	S	2436	pman
18517	18495	0%	0%	0%	S	60720	pudd
18495	4251	0%	0%	0%	S	2432	pman
18398	16921	0%	0%	0%	S	2432	pman
18211	2	0%	0%	0%	S	0	kworker/0:2
18140	18120	0%	0%	0%	S	10352	hman
18120	16921	0%	0%	0%	S	2436	pman
17448	16921	0%	0%	0%	S	428	inotifywait
17253	2	0%	0%	0%	S	0	kworker/1:0
17204	1	0%	0%	0%	S	2064	rotee
16921	1	0%	0%	0%	S	5512	pvp.sh
16744	16366	0%	0%	0%	S	428	inotifywait
16582	1	0%	0%	0%	S	2060	rotee
16366	1	0%	0%	0%	S	5512	pvp.sh
15627	2	0%	0%	0%	S	0	bioset
15626	2	0%	0%	0%	S	0	dmcrypt_write
15625	2	0%	0%	0%	S	0	kcryptd
15624	2	0%	0%	0%	S	0	kcryptd_io
15623	2	0%	0%	0%	S	0	bioset
15621	2	0%	0%	0%	S	0	kdmflush
15618	2	0%	0%	0%	S	0	bucla1
15563	2	0%	0%	0%	S	0	ext4-rsv-conver
15562	2	0%	0%	0%	S	0	jbd2/mmcblk0p1-
15023	2	0%	0%	0%	S	0	kworker/u8:1
15002	14992	0%	0%	0%	S	1440	sort_files_by_i
14992	4251	0%	0%	0%	S	2416	pman
13884	13874	0%	0%	0%	S	2816	flash_check.sh

Resurse generale ale planului de control

Memoria planului de control și utilizarea CPU pe fiecare procesor de control vă permit să păstrați o filă asupra resurselor globale ale planului de control. Puteți folosi**afișează starea software-ului platformei control-procesor scurt**comanda (vizualizare rezumat) sau**arată starea software-ului platformei control-procesor comanda**(vizualizare detaliată) pentru a vizualiza memoria planului de control și informațiile despre utilizarea CPU.

Toate procesoarele de control ar trebui să arate starea, Sănătos. Alte valori posibile de stare sunt Avertisment și Critic. Avertismentul indică faptul că routerul este operațional, dar că nivelul de operare ar trebui revizuit. Critic implică faptul că routerul se apropie de eșec.

Dacă vedeți o stare de Avertizare sau Critică, luați următoarele acțiuni:

- Reducerea sarcinilor statice și dinamice ale sistemului prin reducerea numărului de elemente din configurație sau prin limitarea capacității pentru servicii dinamice.

- Reduceți numărul de rute și adiacențele, limitați numărul de ACL-uri și alte reguli, reduceți numărul de VLAN-uri și așa mai departe.

Următoarele secțiuni descriu câmpurile din**arată starea software-ului platformei de control-procesor**ieșirea comenzii.

Încărcare medie

Media de încărcare reprezintă coada de procese sau disputa de proces pentru resursele CPU. De exemplu, pe un procesor cu un singur nucleu, o încărcare instantanee de 7 ar însemna că șapte procese sunt gata de rulare, dintre care unul rulează în prezent. Pe un procesor dual-core, o încărcare de 7 ar însemna că șapte procese sunt gata de rulare, dintre care două rulează în prezent.

Utilizarea memoriei

Utilizarea memoriei este reprezentată de următoarele câmpuri:

- Total—Memorie totală de sistem
- Utilizat—Memorie consumată
- Liberă—Memorie disponibilă
- Committed—Memorie virtuală dedicată proceselor

Utilizarea CPU

Utilizarea CPU este o indicație a procentului de timp în care CPU este ocupat și este reprezentată de următoarele câmpuri:

- CPU—Procesor alocat
- Utilizator—procese ale nucleului non-Linux
- Sistem — Procesul nucleului Linux
- Nice—Procese cu prioritate redusă
- Idle—Procentul de timp în care CPU a fost inactiv
- IRQ—Întreruperi
- SIRQ—System Interrupts
- IOwait—Procentul de timp în care CPU a așteptat I/O

Exemplu: arată starea software-ului platformei control-procesor Command

Următoarele sunt câteva exemple de utilizare a**arată starea software-ului platformei de control-procesor** comanda:

Router#**arată starea software-ului platformei de control-procesor** RP0:
online, statistici actualizate acum 10 secunde Încărcare medie: sănătos

1-Min: 1,28, stare: sănătos, sub 5,00 5-Min: 0,74, stare:
sănătos, sub 5,00 15-Min: 0,78, stare: sănătos, sub 5,00

```
Memorie (kb): sănătoasă
   Total: 8154204
   Folosit: 2282364 (28%), stare: sănătos Gratuit:
   5871840 (72%)
   Angajate: 2025108 (25%), sub 90% Statistici per-
   core
CPU0: Utilizarea CPU (procentul de timp petrecut)
   Utilizator:  2.46, Sistem: 5.53, Nice: 0.82, SIRQ:    0,00, inactiv: 90,87
   IRQ:    0.20, IOwait:                          0,10
CPU1: Utilizarea CPU (procentul de timp petrecut)
   Utilizator:  2.24, Sistem: 5.91, Nice: 0.71, SIRQ:    0,00, inactiv: 90,91
   IRQ:    0.20, IOwait:                          0,00
CPU2: Utilizarea CPU (procentul de timp petrecut)
   Utilizator:  0.50, Sistem: 1.82, Nice: 0.50, SIRQ:    0,00, inactiv: 97,16
   IRQ:    0.00, IOwait:                          0,00
CPU3: Utilizarea CPU (procentul de timp petrecut)
   Utilizator: 13.03, Sistem: 12.88, Nice: IRQ:         0,00, inactiv: 62,51
   11.55, SIRQ: 0.00, IOwait:                         0,00

Router#afișează starea software-ului platformei control-procesor scurt
Încărcare medie
Stare slot 1-min 5-min 15-min
   RP0 Sănătos 0,99 0,72 0,77

Memorie (kB)
Stare slot              Total          Folosit (buc)          Gratuit (Pct) Angajat (Pct) 5873192
   RP0 Sănătos          8154204        2281012 (28%)          (72%) 2032232 (25%)

Utilizarea CPU
Slot     CPU    Sistemul utilizatorului   Frumos    Inactiv    IRQ    SIRQ IOașteaptă
   RP0     0     1,02 1,84 0,00                    96,30 0,61 0,10 0,10
           1     0,72 1,85 0,00                    96,60 0,61 0,20 0,00
           2     0,50 1,62 0,00                    97,25 0,60 0,00 0,00
           3 11,78 14,28 0,00                      62,44 11,34 0,14 0,00

Boot Flash Disk Monitoring

* 24 august 07:48:31.088 GMT: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: Cota de disc flash a fost depășită

[spațiul liber este de 83820 kB] - Vă rugăm să curățați fișierele de pe flash1.
```

Monitorizarea hardware-ului folosind alarme

Această secțiune conține următoarele:

Design de router și hardware de monitorizare

Routerul trimite notificări de alarmă atunci când sunt detectate probleme, permițându-vă să monitorizați rețeaua de la distanță. Nu trebuie să utilizați**spectacol**comenzi pentru sondarea dispozitivelor în mod obișnuit; cu toate acestea, puteți efectua monitorizare la fața locului dacă doriți.

Monitorizarea discului BootFlash

Discul bootflash trebuie să aibă suficient spațiu liber pentru a stoca două core-dump. Această condiție este monitorizată și, dacă discul bootflash este prea mic pentru a stoca două dump-uri de bază, este generată o alarmă syslog, așa cum se arată în exemplul următor:

6 octombrie 14:10:56.292: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: a fost depășită cota de disc flash

[spațiul liber este de 1429020 kB] - Vă rugăm să curățați fișierele de pe bootflash.

Abordări pentru monitorizarea alarmelor hardware

Această secțiune conține următoarele:

Vizualizarea consolei sau Syslog pentru mesaje de alarmă

Administratorul de rețea poate monitoriza mesajele de alarmă examinând mesajele de alarmă trimise către consola de sistem sau către un jurnal de mesaje de sistem (syslog).

Activarea alarmei de înregistrare

The**alarmă de înregistrare**comanda trebuie să fie activată pentru ca sistemul să trimită mesaje de alarmă către un dispozitiv de înregistrare, cum ar fi consola sau un syslog. Această comandă nu este activată implicit.

Puteți specifica nivelul de severitate al alarmelor care urmează să fie înregistrate. Toate alarmele la sau peste pragul specificat generează mesaje de alarmă. De exemplu, următoarea comandă trimite numai mesaje de alarmă critice către dispozitivele de înregistrare:

Router(config)#**alarmă de înregistrare critică**

Dacă nu este specificată severitatea alarmei, mesajele de alarmă pentru toate nivelurile de severitate sunt trimise la dispozitivele de înregistrare.

Sistemul de management al rețelei alertează un administrator de rețea atunci când o alarmă este raportată prin SNMP

SNMP este un protocol de nivel de aplicație care oferă un cadru standardizat și un limbaj comun utilizat pentru monitorizarea și gestionarea dispozitivelor într-o rețea.

SNMP oferă notificări despre defecțiuni, alarme și condiții care ar putea afecta serviciile. Permite unui administrator de rețea să acceseze informațiile despre router printr-un sistem de management al rețelei (NMS) în loc să examineze jurnalele, să interogheze dispozitivele sau să revizuiască rapoartele de jurnal.

Pentru a utiliza SNMP pentru a primi notificări de alarmă, utilizați următoarele MIB-uri:

- ENTITY-MIB, RFC4133 (necesar pentru ca CISCO-ENTITY-ALARM-MIB, ENTITY-STATE-MIB și CISCO-ENTITY-SENSOR-MIB să funcționeze)
- CISCO-ENTITATE-ALARMA-MIB
- ENTITATE-STAT-MIB
- CISCO-ENTITY-SENSOR-MIB (pentru informații despre alarmele de mediu ale transceiver, care nu sunt furnizate prin CISCO-ENTITY-ALARM-MIB)

Sistemul de management al rețelei alertează un administrator de rețea atunci când o alarmă este raportată prin SNMP

CAPITOL 40

Monitorizare WAN

Acest capitol conține următoarele subiecte:

Informații despre WANMon

WANMon este o soluție flexibilă pentru a răspunde cerințelor de recuperare a conexiunii WAN pentru următoarele produse și interfețe:

- Rețele fizice: 4G LTE și Ethernet (port WAN)
- Legături virtuale: tuneluri IPSec non-criptate bazate pe hartă (fie moștenire, fie FlexVPN); adică orice tunel IPSec pe care îl configurați ca interfață.

Permiteți WANMon să vă monitorizeze legăturile WAN și să inițieze acțiuni de recuperare a legăturii la primirea declanșatoarelor de eșec a legăturii.

Acțiuni de recuperare încorporate

Următoarele sunt cele trei niveluri ale proceselor de recuperare încorporate specifice tipului de legătură:

Legătură **Tip**	**Acțiuni de recuperare**		
	Nivelul 0 (imediat)	**Nivelul 1 (activ)**	**Nivelul 2 (Ultima soluție)**
4G LTE	Ștergeți interfața, apoi închideți/nu închideți	Reîncărcarea modulului	Reîncărcarea sistemului
Ethernet	Ștergeți interfața, apoi închideți/nu închideți	Nicio acțiune luate	Reîncărcarea sistemului

Legătură Tip	Acțiuni de recuperare		
	Nivelul 0 (imediat)	**Nivelul 1 (activ)**	**Nivelul 2 (Ultima soluție)**
Tunel	Închide/nu-închide	Nicio acțiune luate	Reîncărcarea sistemului

Fiecare nivel are două praguri bazate pe timp pe baza cărora sunt întreprinse acțiunile de recuperare încorporate. Următoarele sunt setările implicite pentru fiecare nivel:

- *prag*este timpul de așteptare în minute după primirea unui declanșator de eroare a conexiunii pentru a iniția acțiunea de recuperare, așa cum se stabilește la nivelul specificat.
- *mintime*este frecvența de a efectua acțiunea de recuperare dacă legătura rămâne întreruptă.

Valorile încorporate sunt:

Nivel	prag	mintime	Descriere
Nivel 0	10 min	10 min	Declanșează acțiuni de nivel 0 la 10 minute după ce linkul a încetat. Repetați nu mai mult de fiecare 10 minute.
Nivel 1	60 min	60 min	Declanșează acțiuni de nivel 1 la 10 minute după ce linkul a încetat. Repetați nu mai mult de fiecare 60 de minute.
Nivel 2	480 min	60 min	Declanșează acțiuni de nivel 2 la 480 de minute după ce linkul a încetat. Repetați nu mai mult de fiecare 60 de minute.

Nota Dacă valorile de prag sunt specificate ca 0, nu se iau măsuri de recuperare pentru acel nivel. Puteți utiliza acest lucru pentru a evita reîncărcarea sistemului (acțiunea de recuperare de nivel 2 încorporată) la primirea unui declanșator de eroare a legăturii unde alte legături WAN pot fi operaționale.

Cerințe preliminare

Asigurați-vă că modulul WANMon este disponibil. Modulul WANMon este inclus în imaginea IOS-XE ca *tm_wanmon.tcl*dosarul politicii.

Orientări și limitări

• WANMon efectuează automat verificarea adresei IP (fără configurație de utilizator) așa cum este necesar pentru interfețele celulare.

• Pentru toate celelalte interfețe, WANMon nu efectuează niciodată verificarea adresei IP.

• WANMon declanșează indirect acțiuni specificate de utilizator prin generarea unui eveniment de aplicație care conectează monitorul applet-urilor de resetare.

• Dacă rețeaua dvs. este activă, asigurați-vă că înțelegeți impactul potențial al oricărei comenzi.

Configurarea WANMon

Puteți activa WANMon pe router și puteți atribui suport WAMMon unor interfețe specifice. Opțional, puteți suprascrie acțiunile de recuperare încorporate, puteți defini legături personalizate de recuperare și puteți defini o politică de mediu pentru managerul de evenimente pentru a seta valoarea obiectului de urmărire și a dezactiva verificarea adresei IP. WANMon este dezactivat implicit.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**politica managerului de evenimente** *tm_wanmon.tcl* **bypass de autorizare**	Activează modulul de recuperare a legăturii WANMon. Utilizare**bypass de autorizare**pentru a evita autorizarea pentru CLI invocate de această politică.
Pasul 2	**mediu manager de evenimente wanmon_if_list** *<instanță>*{*numele interfeței*{**ipsla** *<instanță>*}}	Configurați WANMon pentru interfețele din WAN și indică faptul că aceasta este o comandă de configurare a interfeței. **Nota** Orice variabilă de mediu cu prefixul wanmon_if_list constituie o configurație de interfață. Sunt permise mai multe interfețe prin specificarea unei instanțe. Asigurați-vă că specificați numele complet al interfeței (de exemplu, cellular0/4/0 sau cellular0/5/0). Puteți seta declanșatorul IP SLA icmp-echo, dacă doriți. Mai multe declanșatoare IP SLA sunt permise prin specificarea unei instanțe. **Nota** WANMon se uită numai la starea ID-ului SLA. Chiar dacă*icmp-eco*este cel mai frecvent, dacă este necesar orice alt tip de sondă SLA (de exemplu,*udp-eco*) poate fi folosit în schimb.
Pasul 3	**mediu manager de evenimente wanmon_if_listx** { *numele interfeței*{**recuperare***Nivel 0*{*Nivelul 1*} *Nivelul 2*}}	(Opțional) Depășește pragurile încorporate.
Pasul 4	**subsistem publish-event 798 tip 2000 arg1** *<numele interfeței>***arg2***<nivel >*	(Opțional) Configurați acțiuni personalizate de recuperare folosind aplicații de resetare a linkurilor. <*interfata*>este numele complet al interfeței (de exemplu, cellular0/4/0 sau cellular0/5/0).

	Comanda sau Acțiune	Scop
		<*nivel*>este 0, 1 sau 2 pentru a se potrivi cu acțiunea de recuperare a legăturii dorită.
Pasul 5	**{ciot***<track-stub-id >***}**	(Opțional) Permite unei politici de mediu manager de evenimente să seteze valoarea obiectului de urmărire. WANMon poate seta o valoare track-stub-object pentru a reflecta starea legăturii, astfel încât un applet extern să poată urmări obiectul stub.
Pasul 6	**mediu manager de evenimente wanmon_if_listx** { *<numele interfeței >*{**checkip***<exemplu >*}}	(Opțional) Dezactivează verificarea adresei IP.

Ce să faci în continuare

EXEMPLE

politica managerului de evenimente tm_wanmon.tcl bypass de autorizare

Următoarele exemple sunt comenzi Event Manager pentru a configura interfețele celulare și Ethernet:

mediu manager de evenimente wanmon_if_list1 {cellular0/4/0 {ipsla 1}} mediu manager de evenimente wanmon_if_list2 {GigabitEthernet0/0/0 {ipsla 2}}

Acest exemplu setează praguri personalizate de recuperare:

mediu manager de evenimente wanmon_if_list {cellular0/4/0 {recuperare 20 {90 75} 600}

Unde:

- Pragul de nivel 0 este setat la 20 de minute după declanșarea eșecului conexiunii. Acțiunile de recuperare de nivel 0 sunt efectuate pentru interfața celulară. Se repetă la nesfârșit, nu mai mult de 10 minute (implicit).
- Pragul de nivel 1 este setat la 90 de minute. Acțiunile de recuperare de nivel 1 sunt efectuate pentru interfața celulară. Nu se repetă mai des decât la fiecare 75 de minute.
- Pragul de nivel 2 este setat la 600 de minute (10 ore).

Următoarele setează valoarea track-stub-object la 21:

conf t
track 21 stub-object
mediu manager de evenimente wanmon_if_list {cellular0/4/0 {ipsla 1} {stub 21}

Se verifică configurația WANMon

Utilizați următorii pași pentru a vă verifica configurația WANMon.

Procedură

	Comanda sau Acțiune	Scop
Pasul 1	**Afișează politica managerului de evenimente înregistrată**	Afișează politica de monitorizare WAN.
Pasul 2	**arată mediul managerului de evenimente**	Afișează variabilele de mediu ale interfeței setate în timpul configurării interfeței.

Ce să faci în continuare

EXEMPLU

Afișează politica managerului de evenimente înregistrată 1 sistem de script multiplu Off joi 16 ianuarie 18:44:29 2014 tm_wanmon.tcl

arată mediul managerului de evenimente
1 wanmon_if_list {cell0/4/0 {ipsla 1}}

Exemple de configurare

Sunt oferite următoarele exemple:

Exemplu de configurare a interfeței celulare WANMon

```
pista 1 ip sla 1 ip sla 1

  icmp-echo 172.27.166.250
  timeout 6000
  frecventa 300
ip sla program 1 life forever start-time acum
mediu manager de evenimente wanmon_if_list {cellular0/4/0 {ipsla 1}} politica
managerului de evenimente tm_wanmon.tcl ocolire autorizare
```

Exemplu de monitorizare a legăturii WAN multiple

```
track 1 ip sla 1 track 21
stub-object
ip sla 1
  icmp-echo 172.27.166.250
  timeout 6000
  frecventa 300
ip sla program 1 life forever start-time acum track 2 ip sla 2

track 22 stub-object
ip sla 2
  icmp-echo 10.27.16.25
  timeout 6000
  frecventa 300
ip sla program 2 life forever start-time acum
mediu manager de evenimente wanmon_if_list1 {cellular0/4/0 {ipsla 1} {stub 21}} politica managerului de
evenimente tm_wanmon.tcl ocolire autorizare
```

CAPITOL 41

Modele de date Yang

Acest capitol conține următoarele:

Suport pentru modelele de date YANG (Call-home)

Modelele YANG acceptate pentru funcția de apelare la domiciliu sunt similare cu versiunile anterioare ale Cisco-IOS-XE și același lucru este acceptat și pe lansarea IOS-XE pe IR1800. Următoarele referințe sunt disponibile pentru modelele YANG anterioare:

https://github.com/YangModels/yang/tree/master/vendor/cisco/xePentru informații suplimentare despre call-home pentru IOS-XE, consultați următoarele:

Ghid de configurare pentru activarea software-ului, Cisco IOS XE Release 3S

Suport pentru modelul de date Yang pentru transportul de prize brute

Versiunea 17.2.1 adaugă suport pentru modele de date Yang suplimentare. Aceste modele suplimentare includ Raw Socket Transport.

Modelele de date Yang pot fi găsite aici:

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1721

Există două module de caracteristici disponibile pentru socketul brut care aparțin modelului principal Cisco-IOS-XE nativ. Sunt:

- Cisco-IOS-XE-rawsocket.yang
- Cisco-IOS-XE-rawsocket-oper.yang

Modulul Cisco-IOS-XE-rawsocket-oper.yang conține o colecție de definiții YANG pentru comenzile Raw Socket Transport Configuration.

Modulul are următoarele comenzi CLI corespunzătoare:

 # încapsulare raw-tcp
 # încapsulare raw-udp

 # raw-socket packet-length <lungime>
 # raw-socket packet-timer <timer>
 # raw-socket special-char <valoare>
 # server tcp raw-socket <port> <ip>
 # raw-socket tcp idle-timeout <valoare>
 # raw-socket tcp client <dest-ip> <dest-port>
 # raw-socket tcp idle-timeout <timeout>
 # raw-socket tcp tcp-session <valoare>
 # raw-socket tcp dscp <valoare>
 # raw-socket udp connection <dest-ip> <dest-port> <local_port>

Modulul Cisco-IOS-XE-rawsocket-oper.yang conține o colecție de definiții YANG pentru datele operaționale Raw Socket Transport.

Modulul are următoarele comenzi CLI corespunzătoare:

 # arată statisticile brute udp
 # arată statisticile brute tcp
 # arată sesiunea tcp brută
 # arată sesiunea brută udp
 # arată sesiunea TCP brută locală
 # afișează sesiunea udp brută locală

Următoarea este o listă a modulelor dependente:

- Cisco-IOS-XE-nativ
- Caracteristici Cisco-IOS-XE
- ietf-inet-tipuri
- Interfețe Cisco-IOS-XE
- Cisco-IOS-XE-ip
- Cisco-IOS-XE-vlan
- ietf-yang-types @ (orice revizuire)
- cisco-semver

Suport pentru modelul de date Yang pentru Scada

Versiunea Cisco IOS XE 17.1.1 introduce suport pentru modelul Cisco IOS XE YANG pentru sistemul Scada. Lansările anterioare au oferit deja modele Yang în alte domenii.

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/17111.

CAPITOL 42

Operațiuni de rețea gRPC

Actualizarea interfeței de operațiuni de rețea gRPC

gNOI este interfața gRPPCNetworkOperations. gNOI definește un set de microservicii bazate pe gRPC pentru executarea comenzilor și procedurilor operaționale pe dispozitivele de rețea, cum ar fi Instalarea, Activarea și Verificarea sistemului de operare.

Prin intermediul gNOI os.proto va fi posibilă efectuarea sarcinilor legate de sistemul de operare, cum ar fi activarea sistemului de operare, instalarea, prezentarea generală detaliată, comenzile interne ale sistemului de operare și, în final, să scoată un rezumat al operațiunilor sistemului de operare.

În plus, gNOI os.proto poate fi folosit și pentru a afișa starea detaliată a gnmib, a verifica statisticile operaționale gnmib și, de asemenea, pentru a ieși modificatori.

Actualizare GNMI Broker (GNMIB).

Brokerul GNMI (GNMIB) a fost extins pentru a suporta serviciul reset.proto gRPC Network Operations Interface (gNOI). Acest serviciu oferă funcționalitate pentru restabilirea dispozitivului la valorile implicite din fabrică prin gRPC.

Când serviciul este executat, acesta se comportă în mod similar cu comanda „resetare din fabrică a tuturor” și, ulterior, declanșează o reîncărcare. În plus, serviciul va menține imaginea pornită curentă. Pașii suplimentari de mai jos vor fi luați pentru a respecta serviciul reset.proto:

- Setați variabila rommon BOOT la imaginea pornită curentă și mențineți-o prin reîncărcare după resetarea din fabrică
- Activați pornirea automată pentru a afișa dispozitivul pe imaginea pornită curentă după resetarea din fabrică.

Actualizare GNMI Broker (GNMIB).

****

TRADUCĂTOR

Subsemnata, **ALBU MARIA CAMELIA,** interpret şi traducător autorizat pentru limba engleză în temeiul autorizaţiei nr. 8963/2003, certific exactitatea traducerii documentului din limba engleză în limba română, care a fost văzut de mine, că textul prezentat a fost tradus complet, fără omisiuni, şi că, prin traducere, înscrisului nu i-au fost denaturate conţinutul şi sensul.

TRADUCĂTOR

ALBU MARIA CAMELIA