Cisco 8300 シリーズ セキュアルータ ソフトウェア設定ガイド

最終更新：2026 年 4 月 13 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

はじめに

この項では、このマニュアルの目的について説明し、関連する製品とサービスの詳細情報へのリンクを示します。

目標

このガイドでは、Cisco 8300 シリーズ セキュアルータの概要と、これらのルータに含まれるさまざまな機能の設定方法について説明します。

機能およびコマンドに関する重要事項

（コンフィギュレーション ガイドで説明されている）ルータで使用可能な機能などの Cisco IOS XE ソフトウェアの詳細については、Cisco IOS XE 17S Software のドキュメントセットを参照してください。

特定の機能のサポートを確認するには、Cisco Feature Navigator を使用します。詳細については、Cisco Feature Navigator （54 ページ）を参照してください。

特定の Cisco IOS XE コマンドの参照情報については、『Cisco IOS Master Command List, All Releases』を参照してください。

関連資料

- Hardware Installation Guide for the Cisco 8300 Series Secure Routers
- Release Notes for the Cisco 8300 Series Secure Routers

コマンド

ほとんどのプラットフォームでは、Cisco IOS XE コマンドのルックアンドフィールと使用法は Cisco IOS コマンドと同じです。特定の Cisco IOS XE コマンドの参照情報については、『Cisco IOS Master Command List, All Releases』を参照してください。

機能

ルータは Cisco IOS XE ソフトウェアを実行します。このソフトウェアは複数のプラットフォームで使用されます。特定の機能のサポートを確認するには、Cisco Feature Navigator ツールを使用します。詳細については、Cisco Feature Navigator （54 ページ）を参照してください。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または **Ctrl**	^ および **Ctrl** シンボルは、Ctrl キーを表します。たとえば、**^D** または **Ctrl+D** というキーの組み合わせは、**Ctrl** キーを押しながら **D** キーを押すことを意味します。キーは大文字で表記されていますが、大文字と小文字の区別はありません。
string	ストリングは、イタリックで示される引用符を付けない一組の文字です。たとえば、SNMP コミュニティ ストリングとして public を設定する場合、ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。

コマンド構文の説明には、次の表記法を使用しています。

表記法	説明
ボールド	ユーザが入力するコマンドおよびキーワードを示します。
イタリック体	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。

表記法	説明
|	縦棒で区切られている場合、複数の任意または必須のキーワードまたは引数から、1つを選択します。
[x | y]	角カッコで囲まれ、縦棒で区切られたキーワードまたは引数は、任意の選択肢です。
{x | y}	波カッコで囲まれ、縦棒で区切られたキーワードまたは引数は、必須の選択肢です。

省略可能または必須の要素内に、さらに省略可能または必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。次に例を示します。

表記法	説明
[x {y | z}]	角カッコ内の波カッコおよび縦棒は、任意の要素内の必須の選択肢です。

例では、次の表記法を使用しています。

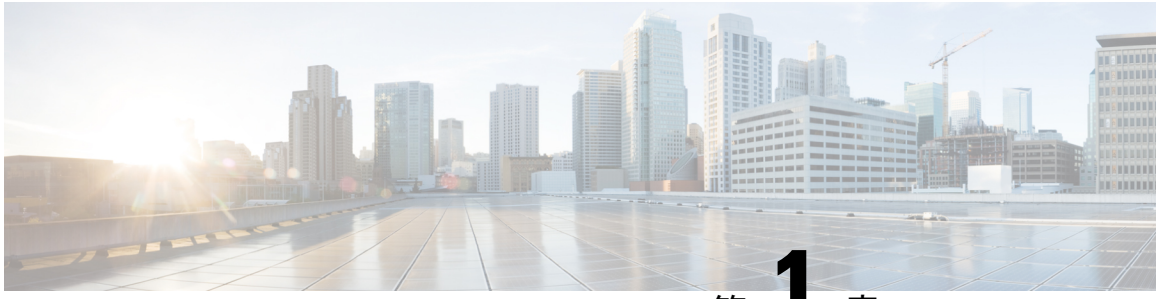
表記法	説明
`screen`	画面に表示される情報の例は、Courier フォントで表します。
`bold screen`	ユーザの入力が必要なテキストの例は、太字の Courier フォントで表します。
< >	山カッコで囲まれたテキストは、パスワードなど、画面に出力されないテキストを表します。
!	行の先頭にある感嘆符（!）は、コメント行を表します。（また、いくつかのプロセスでも、Cisco IOS XE ソフトウェアにより感嘆符が表示されることがあります）。
[ ]	角カッコは、システム プロンプトに対するデフォルトの応答です。

注意 「要注意」です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

マニュアルの入手方法およびテクニカル サポート

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services [英語] にアクセスしてください。
- サービスリクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press [英語] にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。



第 1 章

概要

この章では、Cisco 8300 シリーズセキュアルータに関する情報を含めて、自律モードとコントローラ モードについて説明します。ここで説明する内容は、次のとおりです。

Cisco 8300 シリーズ セキュアルータ

Cisco 8300 シリーズセキュアルータは、セキュアなネットワーキングの簡易化を実現します。まったく新しいセキュアネットワーキングプロセッサと、一元化されたシスコのセキュアネットワーキング プラットフォームを搭載した Cisco 8300 シリーズ セキュアルータは、堅牢なプラットフォームレベルのセキュリティ、ルーティングと SD-WAN を通じた高度なパフォーマンスエンジニアリング、およびオンプレミス、Infrastructure-as-code、またはクラウドで管理できる柔軟性により、ビジネスのシームレスな拡張と成長を可能にします。各クラスのセキュアルータは、リスクの軽減、信頼性の向上、将来への備えを実現するように設計されています。

Cisco 8300 シリーズセキュアルータは大規模なブランチロケーション向けに設計されており、プラットフォームレベルのセキュリティが組み込まれたスケーラブルで高スループットの接続を提供します。ハードウェアネイティブの保証、耐量子計算機暗号、および一元化された Infrastructure as Code を備えた Cisco 8300 シリーズにより、大規模ブランチが帯域幅を大量に消費するアプリケーションと進化する脅威の状況を確実にサポートできるようになります。

このドキュメントは、Cisco 8300 シリーズセキュアルータに固有のソフトウェア機能の概要を示します。Cisco IOS XE および Cisco IOS XE の SD-WAN 機能には、それぞれ自律モードとコントローラ実行モードでアクセスできます。自律モードはデバイスのデフォルトモードで、Cisco IOS XE 機能が含まれています。Cisco IOS XE SD-WAN 機能にアクセスするには、コントローラモードに切り替えます。既存のプラグアンドプレイ ワークフローを使用して、デバイスのモードを決定できます。

universalk9 イメージを使用して、Cisco IOS XE SD-WAN と Cisco IOS XE の両方を Cisco IOS XE プラットフォームに展開できます。C8375-E-G2 では、Cisco IOS XE 17.15.3 は SD-WAN と非 SDWAN の両方の機能と展開のシームレスなアップグレードに役立ちます。C8355-G2 は Cisco IOS XE 17.18.1a 以降でサポートされています。

Cisco CLI を使用したコントローラモードと自律モードの切り替え

コントローラモードと自律モードを切り替えるには、特権 EXEC モードで **controller-mode** コマンドを使用します。

controller-mode disable コマンドは、デバイスを自律モードに切り替えます。

```
Device# controller-mode disable
```

controller-mode enable コマンドは、デバイスをコントローラモードに切り替えます。

```
Device# controller-mode enable
```

（注） デバイスを自律モードからコントローラモードに切り替えると、スタートアップ コンフィギュレーションと NVRAM（証明書）の情報が消去されます。このアクションは **write erase** と同じです。

デバイスをコントローラモードから自律モードに切り替えると、すべての Yang ベースの設定が保持され、元のコントローラモードに切り替えた場合に再利用できます。モードをコントローラから自律に切り替える場合は、デバイスの設定が自動ブートに設定されている必要があります。

ブートストラップ コンフィギュレーション ファイルを使用したコントローラモードと自律モードの切り替え

モードを切り替えるには、**controller-mode enable** コマンドを使用して自律モードからコントローラモードに切り替え、**controller-mode disable** コマンドを使用してコントローラモードから自律モードに切り替えます。デバイスが起動すると、コンフィギュレーションファイル内の設定が適用されます。

デバイスがコントローラモードで起動すると、コンフィギュレーションファイル内の設定が適用されます。

単一の universalk9 イメージを使用して、サポートされているすべてのデバイスに Cisco IOS XE SD-WAN および Cisco IOS XE 機能を展開する方法の詳細については、『Install and Deploy Cisco IOS XE and Cisco IOS XE SD-WAN Functionality on Edge Platforms』を参照してください。

Cisco 8300 シリーズ セキュアルータのモデルは次のとおりです。

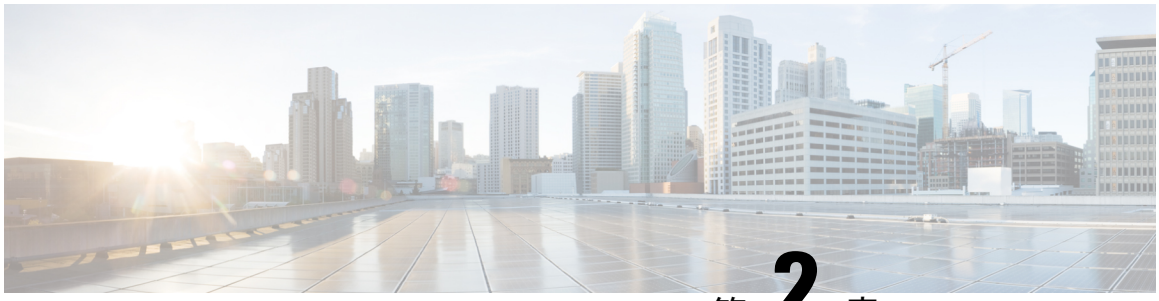
- C8375-E-G2

Cisco 8300 シリーズ セキュアルータでサポートされるモジュールと機能

次の表に、Cisco 8300 シリーズセキュアルータでサポートされているモジュールと機能を示します。

表 *1 : Cisco 8300* シリーズ セキュアルータでサポートされるモジュールと機能

機能	C8375-E-G2	C8355-G2
サービスプレーンアプリケーション（UTD、AppQoE、および TcpOpt）	対応	対応
CPU コア	16 コア	12 コア
CPU メモリ	16G または 32G	16G
バックプレーンサポート	10G	



第 2 章

プラットフォームの基本設定

ここでは、自律モードでのプラットフォームの基本設定について説明します。次の項で構成されています。

デフォルト設定

自律モードでデバイスを起動すると、デバイスはデフォルトのファイル名（デバイスの PID）を検索します。たとえば、Cisco 8300 シリーズ セキュアルータは、C8375-E-G2.cfg または C8355-G2.cfg というファイルを検索します。デバイスはこのファイルを検索した後、標準の files-router-confg または ciscortr.cfg を探します。

デバイスはブートフラッシュで C8375-E-G2.cfg または C8355-G2.cfg ファイルを検索します。ファイルがブートフラッシュで見つからない場合、デバイスは標準の router-confg と ciscortr.cfg を探します。すべてのファイルが見つからない場合、デバイスは、同じ特定の順序で、これらのファイルを保存している可能性のある挿入済みの USB をチェックします。

（注） 挿入済みの USB に PID という名前の構成ファイルがある一方で、標準ファイルの 1 つがブートフラッシュにある場合、システムは標準ファイルを検索して使用します。

show running-config コマンドを使用して、初期設定を表示します。次に、C8375-E-G2 の出力例を示します。

```
Router# show running-config
Current configuration : 6621 bytes
!
! Last configuration change at 06:24:36 UTC Fri Feb 7 2025 by admin
!
version 17.15
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
!
hostname router
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
no logging console
no aaa new-model
!
no ip domain lookup
!
!
!
!
!
!
!
!
!
login on-success log
!
!
!
!
!
!
!
!
subscriber templating
!
!
!
crypto pki trustpoint TP-self-signed-2220840378
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2220840378
 revocation-check none
 rsakeypair TP-self-signed-2220840378
 hash sha512
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
 hash sha512
!
```

```
!
crypto pki certificate chain TP-self-signed-2220840378
 certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 0D050030
  31312F30 2D060355 04030C26 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32323230 38343033 3738301E 170D3235 30313039 30393132
  31315A17 0D333530 31303930 39313231 315A3031 312F302D 06035504 030C2649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 32323038
  34303337 38308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
  0A028201 01008F2E D295CE5D 6DFDC027 4E7B4410 CD546B85 C14F0844 A4A08A47
  3621C3A8 4AF11F97 9489AD4B 00E1C57F AEAD53CE B08B684A 9018E660 8BCFABCE
  B1DCD79D 86E78BF4 DF278EF3 6C86539E 97217942 05C48B9A CBB057FB FFB2B225
  5A626C11 091376D8 A81E66B2 36ECE937 B44451F5 49D9CBB7 4D674A87 6532F4A7
  0A047D14 481A98A7 15574BE5 BFFFB4B1 F397C982 FECED50C 59605382 39B317F2
  3183C1B4 B83F62CF 3A9D6EE8 A1A34C61 86AD6B15 5474FD41 3151540D 5E387FC8
  B169558A E0DF905E F1187E78 AB59BD67 A38E97D9 79AAF825 E6D2B3A6 CF9239D6
  8B5F7E7D D4645263 F6006E12 FF69C3AF 7B769A2E F7F099AE 03A336EA 294A0423
  748E52EF 99330203 010001A3 53305130 1D060355 1D0E0416 04149FE1 4E1985FF
  AB1E7167 F6A67B35 5F3353E3 5B88301F 0603551D 23041830 1680149F E14E1985
  FFAB1E71 67F6A67B 355F3353 E35B8830 0F060355 1D130101 FF040530 030101FF
  300D0609 2A864886 F70D0101 0D050003 82010100 4F0CF81D C9E72E8B 2D5BC14A
  862DF349 42772862 46777631 3F402A07 DCD34CF7 5ED43C42 3C1839BB B68B0677
  C0C66B83 E97A0980 A54E5444 F0473525 C592D1C0 4D6C101A DA4BCDA0 D9C36EE1
CAD752AB AA37B084 A6C5F926 ED264D20 F6EF4940 F1103FAF 7122F428 0A5221F4
  DFB69177 BD7F5E67 DF662F1A F7888526 8867A938 C7F0B75B C34CDAFB 4AA2386B
  10ECE4FD 348D2028 E66E2FF1 FB6B0089 3D68FB71 E993D055 47CC0AA9 F08586E3
  319C0C26 86082E0A E4A9D4DA 99727580 6BEA0CF3 E530CD60 BBC627C5 16D8B483
  A96D47F4 B4746157 0DD2829E 7FC7E087 BE22D84B 09EDD9D7 A2D09897 247397B5
  AB6BBA3C E37BEDA0 053DE14A 748502E1 510197E4
       quit
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
       quit
!
!
diagnostic bootup level minimal
!
license udi pid C8375-E-G2 sn FDO2833M01A
```

```
memory free low-watermark processor 63953
!
spanning-tree extend system-id
!
!
username admin privilege 15 password 0 admin
!
redundancy
 mode none
!
!
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface TwoGigabitEthernet0/0/0
 no ip address
 shutdown
 negotiation auto
!
interface TwoGigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
!
interface TwoGigabitEthernet0/0/2
 no ip address
 shutdown
 negotiation auto
!
interface TwoGigabitEthernet0/0/3
 no ip address
 shutdown
 negotiation auto
!
interface TenGigabitEthernet0/0/4
 no ip address
 shutdown
!
interface TenGigabitEthernet0/0/5
 no ip address
 shutdown
!
interface TwoGigabitEthernet0/1/0
!
interface TwoGigabitEthernet0/1/1
!
interface TwoGigabitEthernet0/1/2
!
interface TwoGigabitEthernet0/1/3
!
interface TwoGigabitEthernet0/1/4
!
interface TwoGigabitEthernet0/1/5
!
interface TwoGigabitEthernet0/1/6
 switchport
!
interface TwoGigabitEthernet0/1/7
```

```
 switchport
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 ip address 10.79.58.164 255.255.255.0
 negotiation auto
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
ip tftp source-interface GigabitEthernet0
ip http server
ip http authentication local
ip http secure-server
ip route 64.104.134.61 255.255.255.255 10.79.58.1
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.79.58.1
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 64.104.134.61
ip ssh bulk-mode 131072
!
snmp-server community public RW
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 login local
 transport input telnet
line vty 5 10
 privilege level 15
 login local
 transport input telnet
line vty 11 14
 login
 transport input ssh
!
!
!
!
!
!
!
end
```

次に、C8355-G2 の出力例を示します。

```
Router# show running-config
Current configuration : 5001 bytes

 !

! Last configuration change at 09:02:29 UTC Mon Aug 18 2025

!

version 17.18

service timestamps debug datetime msec
```

```
service timestamps log datetime msec
service password-encryption
platform qfp utilization monitor load 80
platform resource data-plane-heavy
!
hostname Wilson1
!
boot-start-marker
boot-end-marker
!
!
vrf definition 4
!
address-family ipv4
exit-address-family
!
vrf definition 50
!
address-family ipv4
exit-address-family
!
vrf definition 65500
 !
address-family ipv4
exit-address-family
!
vrf definition 65528
description SIG VRF
!
address-family ipv4
exit-address-family
!
```

```
vrf definition 65529
description Speedtest VRF
!
address-family ipv4
exit-address-family
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
no logging queue-limit
no logging rate-limit
aaa new-model
!
!
aaa authentication login default local
aaa authorization console
aaa authorization exec default local
!
!
aaa session-id common
no process cpu extended history
!
!
!
!
!
!
!
```

```
!
ip dhcp pool PnPWebUI1
vrf 65500
host 192.168.1.3 255.255.255.0
client-identifier 0077.6562.7569
dns-server 192.168.1.1
!
!
!
login on-success log
!
!
!
!
!
!
fhrp version vrrp v3
ipv6 unicast-routing
ipv6 rip vrf-mode enable
!
!
subscriber templating
!
!
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
revocation-check crl
hash sha512
!
crypto pki trustpoint TP-self-signed-758392875
enrollment selfsigned
revocation-check crl
rsakeypair TP-self-signed-758392875
hash sha512
!
!
crypto pki certificate chain SLA-TrustPoint
crypto pki certificate chain TP-self-signed-758392875
!
!
!
!
!
!
!
!
!

diagnostic bootup level minimal
!
license udi pid C8355-G2 sn FDO2836M06D
license accept end user agreement
```

```
memory free low-watermark processor 63115

!

spanning-tree extend system-id

!
!

!

!

username admin privilege 15 secret 9
$9$nbNcaolXwfHkHk$FxUuHozuwCqmWCyltQ0YkluTGUubx2ijED8/Laeh72k
!

redundancy

 mode none

!

!

!

!

!

no crypto ikev2 diagnose error

!

!

vlan internal allocation policy ascending

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!
```

```
!
!
interface Loopback65528
vrf forwarding 65528
ip address 192.168.1.1 255.255.255.255
!
interface Loopback65529
vrf forwarding 65529
ip address 11.1.0.116 255.255.255.255
!
interface Tunnel1
ip unnumbered GigabitEthernet0/0/4
ipv6 unnumbered GigabitEthernet0/0/4
tunnel source GigabitEthernet0/0/4
tunnel mode sdwan
!
interface Tunnel100009
ip unnumbered TenGigabitEthernet0/0/9
tunnel source TenGigabitEthernet0/0/9
tunnel mode sdwan
!
interface FiveGigabitEthernet0/0/0
no ip address
negotiation auto
!
interface FiveGigabitEthernet0/0/1
no ip address
 negotiation auto
!
interface FiveGigabitEthernet0/0/2
no ip address
negotiation auto
```

```
!
interface FiveGigabitEthernet0/0/3
no ip address
!
interface GigabitEthernet0/0/4
ip address 10.1.12.116 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/0/5
no ip address
negotiation auto
!
interface TenGigabitEthernet0/0/6
!
interface TenGigabitEthernet0/0/7
!
interface TenGigabitEthernet0/0/8
vrf forwarding 50
ip address 8.2.1.1 255.255.255.0
no plim qos input queue 0 pause enable
!
!
interface TenGigabitEthernet0/0/9
mtu 1734
ip address 10.1.9.1 255.255.255.0
no plim qos input queue 0 pause enable
!
interface GigabitEthernet0
vrf forwarding Mgmt-intf
ip address 10.75.163.116 255.255.255.0
negotiation auto
ipv6 address autoconfig
!
```

```
 interface Vlan1
 vrf forwarding 65500
 ip address 192.168.1.1 255.255.255.0
!
router omp
!
ip forward-protocol nd
no ip forward-protocol udp
ip tftp source-interface GigabitEthernet0
ip ftp source-interface GigabitEthernet0
ip http server
ip http authentication local
ip http secure-server
!
ip nat settings central-policy
ip nat settings gatekeeper-size 1024
ip nat route vrf 65528 0.0.0.0 0.0.0.0 global
no ip nat service all-algs
ip route 0.0.0.0 0.0.0.0 10.1.9.2
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.75.163.1
ip route vrf 50 0.0.0.0 0.0.0.0 10.1.9.2
no ip ssh bulk-mode
ip scp server enable
!
no ipv6 mld ssm-map query dns
!
!
!
!
!
control-plane
!
```

```
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!

mgcp profile default
!
 !
!
!
!
!
 !
!
line con 0
exec-timeout 0 0
activation-character 13
stopbits 1
speed 115200
line aux 0
activation-character 13
line vty 0 4
privilege level 15
activation-character 13
transport input all
line vty 5 80
privilege level 15
activation-character 13
transport input none
!
no network-clock revertive
```

```
!
!
!
!
!
!
!
!
!
!
!
 !
 netconf-yang
netconf-yang feature candidate-datastore
no netconf-yang ssh server algorithm encryption aes128-cbc
no netconf-yang ssh server algorithm encryption aes256-cbc
no netconf-yang ssh server algorithm hostkey ssh-rsa
no netconf-yang ssh server algorithm kex diffie-hellman-group14-sha1
no netconf-yang ssh server algorithm mac hmac-sha1
end
```

グローバルパラメータの設定

デバイスのグローバルパラメータを設定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **hostname** *name*
3. **enable secret** *password*
4. **no ip domain-lookup**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`Router> enable`
	`Router# configure terminal`
	`Router(config)#`
		グローバル コンフィギュレーション モードを開始します（コンソール ポート使用時）。
		次のコマンドを使用して、ルータとリモート端末を接続します。
		`telnet router-name or address`
		`Login: login-id`
		`Password: *********`
		`Router> enable`

ステップ 2	**hostname** *name* 例： `Router(config)# hostname Router`	デバイスの名前を指定します。
ステップ 3	**enable secret** *password* 例： `Router(config)# enable secret cr1ny5ho`	デバイスへの不正なアクセスを防止するには、暗号化パスワードを指定します。
ステップ 4	**no ip domain-lookup** 例： `Router(config)# no ip domain-lookup`	デバイスが未知の単語（入力ミス）をIPアドレスに変換しないようにします。 グローバルパラメータコマンドの詳細については、『Cisco IOS Release Configuration Guide』マニュアルセットを参照してください。

ギガビット イーサネット インターフェイスの設定

オンボードのギガビット イーサネットインターフェイスを手動で定義するには、グローバル コンフィギュレーション モードから開始して、次の手順を実行します。

手順の概要

1. **interface TwoGigabitEthernet** *slot/bay/port*
2. **ip address** *ip-address mask*
3. **ipv6 address** *ipv6-address/prefix*
4. **no shutdown**
5. **exit**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**interface TwoGigabitEthernet** *slot/bay/port* 例： `Router(config)# interface TwoGigabitEthernet 0/0/1`	デバイスでギガビット イーサネット インターフェイスのコンフィギュレーション モードを開始します。
ステップ 2	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 192.0.2.2 255.255.255.0`	指定したギガビット イーサネット インターフェイスのIPアドレスとサブネットマスクを設定します。IPv4アドレスを設定する場合は、このステップを使用します。
ステップ 3	**ipv6 address** *ipv6-address/prefix* 例： `Router(config-if)# ipv6 address 2001.db8::ffff:1/128`	指定したギガビット イーサネット インターフェイスの IPv6 アドレスとプレフィクスを設定します。IPv6 アドレスを設定する場合は、ステップ 2 の代わりにこのステップを使用します。
ステップ 4	**no shutdown** 例： `Router(config-if)# no shutdown`	ギガビットイーサネットインターフェイスをイネーブルにし、その状態を管理上のダウンから管理上のアップに変更します。
ステップ 5	**exit** 例： `Router(config-if)# exit`	ギガビット イーサネット インターフェイスのコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ループバック インターフェイスの設定

始める前に

ループバック インターフェイスは、スタティック IP アドレスのプレースホルダーとして機能し、デフォルトのルーティング情報を提供します。

ループバック インターフェイスを設定するには、次の手順を実行します。

手順の概要

1. **interface** *type number*
2. （オプション 1）**ip address** *ip-address mask*

3. （オプション 2） **ipv6 address** *ipv6-address/prefix*
4. **exit**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**interface** *type number* 例： `Router(config)# interface Loopback 0`	ループバック インターフェイスのコンフィギュレーション モードを開始します。
ステップ 2	（オプション 1）**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.108.1.1 255.255.255.0`	ループバック インターフェイスの IP アドレスとサブネットマスクを設定します。IPv6アドレスを設定する場合は、次に説明する **ipv6 address** *ipv6-address/prefix* コマンドを使用します。
ステップ 3	（オプション 2） **ipv6 address** *ipv6-address/prefix* 例： `Router(config-if)# 2001:db8::ffff:1/128`	ループバック インターフェイスの IPv6 アドレスとプレフィクスを設定します。
ステップ 4	**exit** 例： `Router(config-if)# exit`	ループバック インターフェイスのコンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。

例

ループバック インターフェイス設定の確認

次に、静的 IP アドレスとして機能する IP アドレス 203.0.113.1/32 のギガビット イーサネットインターフェイス上に設定されるループバック インターフェイスの設定例を示します。ループバック インターフェイスは、ネゴシエートされた IP アドレスを持つ virtual-template1 に紐付けられます。

```
!
interface loopback 0
ip address 203.0.113.1 255.255.255.255 (static IP address)
ip nat outside
!
interface Virtual-Template1
ip unnumbered loopback0
no ip directed-broadcast
ip nat outside
```

show interface loopback コマンドを入力します。次の例のような出力が表示されます。

```
Router# show interface loopback 0
Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 203.0.113.1/32
  MTU 1514 bytes, BW 8000000 Kbit/sec, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

または、次の例に示すように、**ping** コマンドを使用してループバック インターフェイスを確認します。

```
Router# ping  203.0.113.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

モジュールインターフェイスの設定

サービスモジュールの設定の詳細については、『Cisco Service Module Configuration Guide』の「Service Module Management」のセクションで「Service Modules」を参照してください。

コアの動的割り当ての設定

Cisco 8300 シリーズ セキュアルータでの動的コア割り当てにより、ユーザーはさまざまなサービスや CEF/IPSec のパフォーマンスに応じて CPU コアを柔軟に活用できます。Cisco 8300 シリーズセキュアルータには、少なくとも 16 個の CPU コアが搭載されており、データプレーンからサービスプレーンにコアを柔軟に割り当てることができます。このコア割り当ては、これらのプラットフォームで使用可能なさまざまなサービスのお客様による設定に基づいています。

Cisco IOS XE リリース 17.15.3 以降は、**platform resource { service-plane-heavy | data-plane-heavy }** コマンドを使用して、サービスプレーンとデータプレーンの間でコアを調整します。

```
Router(config)# platform resource { service-plane-heavy | data-plane-heavy }
```

次に、コア割り当ての動的な変更をサポートする Cisco 8300 シリーズ セキュアルータのリストを示します。

- C8375-E-G2

C8375-E-G2 のコマンド出力を表示

次の show コマンド出力は、C8375-E-G2 のデータプレーンへの CPU コア割り当てを示しています。

（注） デフォルトでは、デバイス起動時のモードは service-plane-heavy です。

```
Router# show platform software cpu alloc

CPU alloc information:
  Control plane cpu alloc: 0
  Data plane cpu alloc: 0-15
  Service plane cpu alloc: 0
  Slow control plane cpu alloc:
  Template used: CLI-data_plane_heavy
```

（注） この例で、データプレーンコア割り当ての最大数は 15 です。

次の show コマンド出力は、C8375-E-G2 のサービスプレーンへの CPU コア割り当てを示しています。

```
Router# show platform software cpu alloc
CPU alloc information:
  Control plane cpu alloc: 0
  Data plane cpu alloc: 0,6-15
  Service plane cpu alloc: 1-5
  Slow control plane cpu alloc:
  Template used: default-service_plane_heavy
```

次の show コマンド出力は、C8375-E-G2 の PPE ステータスを示しています。

```
Router# show platform hardware qfp active datapath infrastructure sw-cio

ID      Port  Wght  Global WRKR0  WRKR1  WRKR2  WRKR3  WRKR4  WRKR5  WRKR6  WRKR12
WRKR13  WRKR14  Total
   1      rcl0     4:   6080     0      0      0      0      0      0      0       0
    0      64   6144
   1      rcl0     8:   6080     0      0      0      0      0      0      0       0
    0      64   6144
   2       ipc     1:      0     0      0      0      0      0      0      0       0
    0       0      0
   3 vxe_punti     1:    468     0      0      0      0      0      0      0       0
    0      44    512
   4      fpe0    LO:   1024     -      -      -      -      -      -      -       -
    -       -   1024
   4      fpe0    HI:   1024     -      -      -      -      -      -      -       -
    -       -   1024
   5      fpe1    LO:   1024     -      -      -      -      -      -      -       -
```

```
 -       -   1024
   5      fpe1    HI:   1024     -      -      -      -      -      -      -       -
 -       -   1024
   6      fpe2    LO:   1024     -      -      -      -      -      -      -       -
 -       -   1024
   6      fpe2    HI:   1024     -      -      -      -      -      -      -       -
 -       -   1024
   7      fpe3    LO:   1024     -      -      -      -      -      -      -       -
 -       -   1024
   7      fpe3    HI:   1024     -      -      -      -      -      -      -       -
 -       -   1024
   8      fpe4    LO:   1024     -      -      -      -      -      -      -       -
 -       -   1024
   8      fpe4    HI:   1024     -      -      -      -      -      -      -       -
 -       -   1024
   9      fpe5    LO:   1024     -      -      -      -      -      -      -       -
 -       -   1024
   9      fpe5    HI:   1024     -      -      -      -      -      -      -       -
 -       -   1024

Core Utilization over preceding 1147610.0731 seconds
-----------------------------------------------------
      ID:       0       1       2       3       4       5       6      12      13
14
    % PP:    0.73    0.18    0.19    0.19    0.19    0.19    0.19    0.00    0.00
0.00
    % RX:    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
0.47
    % TM:    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.95    0.96
0.00
  % IDLE:   99.27   99.82   99.81   99.81   99.81   99.81   99.81   99.05   99.04   99.53
```

C8355-G2 のコマンド出力を表示

次の show コマンド出力は、C8355-G2 のデータプレーンへの CPU コア割り当てを示しています。

（注） デフォルトでは、デバイス起動時のモードは service-plane-heavy です。

```
Router# show platform software cpu alloc

CPU alloc information:
Control plane cpu alloc: 0
Data plane cpu alloc: 0-11
Service plane cpu alloc: 0
Slow control plane cpu alloc:
Template used: CLI-data_plane_heavy
```

（注） この例で、データプレーンコア割り当ての最大数は 11 です。

次の show コマンド出力は、C8355-G2 の PPE ステータスを示しています。

```
Router# show platform hardware qfp active datapath infrastructure sw-cio
Credits Usage:

                                                                    ID      Port  Wght
```

```
 Global WRKR0   WRKR1   WRKR2   WRKR3   WRKR4   WRKR5   WRKR6   WRKR7   WRKR8   WRKR9   WRKR10
Total
1       rcl0     4:    4544      0       0       0       0       0       0       0       0       0
      64        0    4608
1       rcl0     8:    4544      0       0       0       0       0       0       0       0       0
      64        0    4608
2        ipc     1:       0      0       0       0       0       0       0       0       0       0
       0        0       0
3 vxe_punti      1:     271     17      23      13      18      29      31      21      22      18
       0       49     512
4     l2_mod     LO:    1024      -       -       -       -       -       -       -       -       -
       -        -    1024
4     l2_mod     HI:    1024      -       -       -       -       -       -       -       -       -
       -        -    1024
5       fpe0     LO:    1024      -       -       -       -       -       -       -       -       -
       -        -    1024
5       fpe0     HI:    1024      -       -       -       -       -       -       -       -       -
       -        -    1024
6       fpe1     LO:    1024      -       -       -       -       -       -       -       -       -
       -        -    1024
6       fpe1     HI:    1024      -       -       -       -       -       -       -       -       -
       -        -    1024
7       fpe2     LO:    1024      -       -       -       -       -       -       -       -       -
       -        -    1024
7       fpe2     HI:    1024      -       -       -       -       -       -       -       -       -
       -        -    1024
8       fpe3     LO:    1024      -       -       -       -       -       -       -       -       -
       -        -    1024
8       fpe3     HI:    1024      -       -       -       -       -       -       -       -       -
       -        -    1024
9       fpe8     LO:    1019      -       -       -       -       -       -       -       -       -
       -        -    1024
9       fpe8     HI:    1024      -       -       -       -       -       -       -       -       -
       -        -    1024
10      fpe9     LO:    1019      -       -       -       -       -       -       -       -
-       -        -    1024
10      fpe9     HI:    1024      -       -       -       -       -       -       -       -
-       -        -    1024
Core Utilization over preceding 2793.4130 seconds

-------------------------------------------------

ID:        0       1       2       3       4       5       6       7       8       9
  10
% PP:    64.19   64.51   64.10   64.61   64.08   64.13   64.20   64.57   64.42    0.00
  0.00
% RX:     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
  0.00
% TM:     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    1.89
 49.31
% IDLE:   35.81   35.49   35.90   35.39   35.92   35.87   35.80   35.43   35.58   98.11
   50.68
```

Cisco Discovery Protocol の有効化

ルータでは、Cisco Discovery Protocol（CDP）がデフォルトで有効に設定されています。

CDP の使用法の詳細については、『Cisco Discovery Protocol Configuration Guide』を参照してください。

コマンドラインアクセスの設定

デバイスへのアクセスを制御するパラメータを設定するには、次の手順を実行します。

手順

ステップ 1 **line** [| **console** | **tty** | **vty**] *line-number*

例：

```
Router(config)# line console 0
```

回線コンフィギュレーション モードを開始します。続いて、回線のタイプを指定します。

ここに示す例では、アクセス用のコンソール端末を指定します。

ステップ 2 **password** *password*

例：

```
Router(config-line)# password 5dr4Hepw3
```

コンソール端末回線に固有のパスワードを指定します。

ステップ 3 **login**

例：

```
Router(config-line)# login
```

端末セッションログイン時のパスワードチェックを有効にします。

ステップ 4 **exec-timeout** *minutes* [*seconds*]

例：

```
Router(config-line)# exec-timeout 5 30
Router(config-line)#
```

ユーザ入力が検出されるまでEXECコマンドインタープリタが待機する間隔を設定します。デフォルトは10分です。任意指定で、間隔値に秒数を追加します。

ここに示す例は、5分30秒のタイムアウトを示しています。「**0 0**」のタイムアウトを入力すると、タイムアウトが発生しません。

ステップ 5 **exit**

例：

```
Router(config-line)# exit
```

回線コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを再開します。

ステップ 6 **line** [**| console | tty | vty**] *line-number*

例：

```
Router(config)# line vty 0 4
Router(config-line)#
```

リモート コンソール アクセス用の仮想端末を指定します。

ステップ 7 **password** *password*

例：

```
Router(config-line)# password aldf2ad1
```

仮想端末回線に固有のパスワードを指定します。

ステップ 8 **login**

例：

```
Router(config-line)# login
```

仮想端末セッションログイン時のパスワードチェックを有効にします。

ステップ 9 **end**

例：

```
Router(config-line)# end
```

回線コンフィギュレーション モードを終了します。続いて、特権 EXEC モードに戻ります。

例

次の設定は、コマンドライン アクセス コマンドを示します。

default と示されているコマンドは、入力する必要はありません。これらのコマンドは、**show running-config** コマンドの使用時に、生成されたコンフィギュレーション ファイルに自動的に示されます。

```
!
line console 0
 exec-timeout 10 0
 password 4youreyesonly
 login
transport input none (default)
stopbits 1 (default)
line vty 0 4
 password secret
 login
!
```

スタティックルートの設定

スタティック ルートは、ネットワークを介した固定ルーティング パスを提供します。これらのルートは、デバイス上で手動で設定されます。ネットワーク トポロジが変更された場合には、スタティック ルートを新しいルートに更新する必要があります。スタティック ルートは、ルーティング プロトコルによって再配信される場合を除き、プライベート ルートです。

スタティック ルートを設定するには、次の手順を実行します。

手順

ステップ 1 （オプション 1） **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}

例：

```
Router(config)# ip route 192.0.2.8 255.255.0.0 10.10.10.2
```

IP パケットのスタティック ルートを指定します。（IPv6 アドレスを設定する場合は、次に説明する **ipv6 address** コマンドを使用してください）。

ステップ 2 （オプション 2） **ipv6 route** *prefix/mask* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]}

例：

```
Router(config)# ipv6 route 2001:db8:2::/64 2001:DB8:3000:1
```

IP パケットのスタティック ルートを指定します。

ステップ 3 **end**

例：

```
Router(config)# end
```

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

設定の確認

次の設定例では、宛先 IP アドレスが 192.0.2.8、サブネットマスクが 255.255.255.0 のすべての IP パケットを、IP アドレス 10.10.10.2 の他のデバイスに対して、ギガビットインターフェイス上から静的ルートで送信します。具体的には、パケットが設定済みのインターフェイスに送信されます。

default と示されているコマンドは、入力する必要はありません。このコマンドは、**running-config** コマンドの使用時に、生成されたコンフィギュレーション ファイルに自動的に示されます。

```
!
ip classless (default)
ip route 192.0.2.8 255.255.255.0 10.10.10.2
```

スタティック ルートが正しく設定されていることを確認するには、**show ip route** コマンド（または **show ipv6 route** コマンド）を入力し、文字 S で示されるスタティック ルートを見つけます。

IPv4 アドレスを使用する場合は、次のような確認用の出力が表示されます。

```
Router# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is 10.0.10.1 to network 192.0.2.6

S*    192.0.2.6/0 [254/0] via 10.0.10.1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.10.0/24 is directly connected, GigabitEthernet0/0/0
L        10.0.10.13/32 is directly connected, GigabitEthernet0/0/0
C        10.108.1.0/24 is directly connected, Loopback0
L        10.108.1.1/32 is directly connected, Loopback0
```

IPv6 アドレスを使用する場合は、次のような確認用の出力が表示されます。

```
Router# show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE -
Destination
       NDr - Redirect, 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 - LISP site, ld - LISP dyn-EID, a - Application

C   2001:DB8:3::/64 [0/0]
       via GigabitEthernet0/0/2, directly connected
S   2001:DB8:2::/64 [1/0]
       via 2001:DB8:3::1
```

ダイナミックルートの設定

ダイナミック ルーティングでは、ネットワーク トラフィックまたはトポロジに基づいて、ネットワーク プロトコルがパスを自動調整します。ダイナミックルーティングの変更は、ネットワーク上の他のデバイスにも反映されます。

デバイスは、ルーティング情報プロトコル（RIP）または Enhanced Interior Gateway Routing Protocol（EIGRP）などの IP ルーティングプロトコルを使用して、ルートを動的に学習できます。

• Routing Information Protocol の設定 （31 ページ）
• Enhanced Interior Gateway Routing Protocol の設定 （35 ページ）

Routing Information Protocol の設定

ルータの RIP を設定するには、次の手順を実行します。

手順

ステップ 1 **router rip**

例：

```
Router(config)# router rip
```

ルータ コンフィギュレーション モードを開始します。続いて、ルータの RIP を有効にします。

ステップ 2 **version** {**1** | **2**}

例：

```
Router(config-router)# version 2
```

RIP version 1 または 2 の使用を指定します。

ステップ 3 **network** *ip-address*

例：

```
Router(config-router)# network 192.0.2.8
Router(config-router)# network 10.10.7.1
```

直接接続しているネットワークの各アドレスを使用して、RIP を適用するネットワーク リストを指定します。

ステップ 4 **no auto-summary**

例：

```
Router(config-router)# no auto-summary
```

ネットワーク レベルルートへのサブネットルートの自動サマライズを無効にします。これにより、サブプレフィックス ルーティング情報がクラスフル ネットワーク境界を越えて送信されます。

ステップ 5 **end**

例：

```
Router(config-router)# end
```

ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

例

設定の確認

この設定を表示するには、特権 EXEC モードで **show running-config** コマンドを使用します。

```
!
Router# show running-config
Building configuration...

Current configuration : 6504 bytes
!
! Last configuration change at 05:04:58 UTC Mon Jul 6 2020
!
version 17.3
service config
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
platform hardware throughput crypto 1G
!
hostname Router
!
boot-start-marker
boot system bootflash:c8000be-universalk9.17.03.01prd8.SPA.bin
boot-end-marker
!
!
!
no aaa new-model
!
login on-success log

!
subscriber templating
!
!
multilink bundle-name authenticated
no device-tracking logging theft


!
crypto pki trustpoint TP-self-signed-2347094934
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2347094934
 revocation-check none
 rsakeypair TP-self-signed-2347094934
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
```

```
!
!

crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit

!
!
license feature hseck9
license udi pid C8300-1N1S-6T sn FDO2320A0CF

diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
redundancy
 mode none

!
interface GigabitEthernet0/0/0
 ip dhcp client client-id ascii FDO2320A0CF
 ip address dhcp
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
!
!
ip http server
ip http authentication local
ip http secure-server
ip http client source-interface GigabitEthernet0/0/0
ip forward-protocol nd

!
```

```
!
!
control-plane
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default

!
!
dspfarm profile 7 conference security
 shutdown

!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
 transport input ssh
!
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact
email address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http

!
!
end
```

RIP が正しく設定されていることを確認するには、**show ip route** コマンドを入力し、文字 R で示される RIP ルートを見つけます。次の例のような出力が表示されます。

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
R    192.0.2.3/8 [120/1] via 192.0.2.2, 00:00:02, Ethernet0/0/0
```

Enhanced Interior Gateway Routing Protocol の設定

拡張インテリア ゲートウェイ ルーティング プロトコル（EIGRP）を設定するには、次の手順を実行します。

手順

ステップ 1 **router eigrp** *as-number*

例：

```
Router(config)# router eigrp 109
```

ルータ コンフィギュレーション モードを開始して、ルータ上で EIGRP をイネーブルにします。自律システム（AS）番号は、他の EIGRP ルータへのルートを識別します。また、EIGRP 情報のタグ付けに使用されます。

ステップ 2 **network** *ip-address*

例：

```
Router(config)# network 192.0.2.8
Router(config)# network 10.10.12.15
```

EIGRP を適用するネットワークのリストを指定します（直接接続されているネットワークの IP アドレスを使用）。

ステップ 3 **end**

例：

```
Router(config-router)# end
```

ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

設定の確認

次に、IP ネットワーク 192.0.2.8 と 10.10.12.15 で EIGRP ルーティングプロトコルを有効にする設定例を示します。EIGRP の自律システム番号として、109 が割り当てられています。この設定を表示するには、**show running-config** コマンドを使用します。

```
Router# show running-config
.
.
.
!
router eigrp 109
 network 192.0.2.8
  network 10.10.12.15
!
.
```

.
.

IP EIGRP が正しく設定されたかどうかを確認するには、**show ip route** コマンドを入力し、文字 D で示される EIGRP ルートを探します。次のような確認用の出力が表示されます。

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
D     192.0.2.3/8 [90/409600] via 192.0.2.2, 00:00:02, Ethernet0/0
```

ポート LED の自動オフの有効化

グローバル設定 CLI コマンドを使用して、ポートの LED 制御を有効または無効にできます。デフォルトでは、この機能は無効になっています。自動オフを有効にすると、リンクステータスに関係なく、前面パネルポートおよびモジュールポートのすべてのポート LED がオフに設定されます。

- ポート LED の自動オフを有効にするには、config モードで次のコマンドを使用します。

```
Router(config)# hw-module auto-off led
```

（注） この設定は、ポートの LED のみに影響します。他のすべての LED は正常に機能します。

- ポート LED の自動オフを無効にするには、config モードで次のコマンドを使用します。

```
Router(config)# no hw-module auto-off led
```

ブルービーコン LED の有効化

ブルービーコン LED は、通常は前面パネルにあるデバイス上の視覚的なインジケータです。この LED は、複数のデバイスが設置されている環境で、ネットワーク管理者が特定のデバイスを簡単に識別できるように設計されています。

ビーコン LED は、管理者が CLI コマンドを使用して、ルータに注意が必要なことを示すために点灯できます。Cisco 8300 シリーズ セキュアルータでは、ビーコン LED は、CLI でコマンドを使用してのみ有効または無効にできます。

- ビーコン LED を点灯させるには、次のコマンドを使用します。

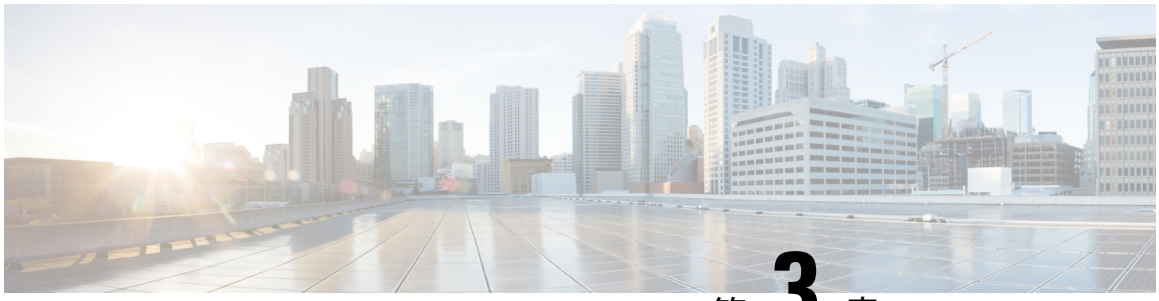
```
Router#hw-module beacon on
```

- ビーコン LED を消灯するには、次のコマンドを使用します。

```
Router#hw-module beacon off
```

- ビーコン LED のステータスを確認するには、次のコマンドを使用します。

```
Router#hw-module beacon status
```



第 3 章

Cisco IOS XE ソフトウェアの使用

この章では、Cisco IOS XE ソフトウェアを自律モードで使用する方法の基礎について説明します。この章は次のセクションで構成されています。

- Cisco IOS XE ソフトウェア （39 ページ）

Cisco IOS XE ソフトウェア

始める前に

コマンドラインインターフェイス（CLI）に直接アクセスするか、Telnet を使用する場合には、コンソール（CON）ポートを使用します。

ここでは、デバイスへの主要なアクセス方法について説明します。

手順

ステップ 1 直接接続されたコンソールを使用して CLI にアクセスする方法 （39 ページ）
ステップ 2 SSH を使用したコンソールへのアクセス （41 ページ）
ステップ 3 Telnet を使用してリモートコンソールから CLI にアクセスする方法 （41 ページ）
ステップ 4 USB シリアルコンソールポートから CLI へのアクセス （43 ページ）

直接接続されたコンソールを使用して CLI にアクセスする方法

CON ポートは、no-flow 制御と RJ-45 コネクタを備えた EIA/TIA-232 非同期シリアル接続機能です。CON ポートは、シャーシの前面パネルにあります。

ここでは、制御インターフェイスにアクセスする手順について説明します。

- コンソールポートへの接続 （40 ページ）
- コンソール インターフェイスの使用方法 （40 ページ）

コンソールポートへの接続

手順

ステップ 1 端末エミュレーション ソフトウェアを次のように設定します。

- 9,600 bps（ビット/秒）
- 8 データ ビット
- パリティなし
- フロー制御なし

ステップ 2 RJ-45/RJ-45 ケーブルと RJ-45/DB-25 DTE アダプタ、または RJ-45/DB-9 DTE アダプタ（「Terminal」のラベル付き）を使用して、CON ポートに接続します。

コンソール インターフェイスの使用方法

手順

ステップ 1 次のコマンドを入力します。

```
Router> enable
```

ステップ 2 （イネーブル パスワードが設定されていない場合は、ステップ 3 に進みます）パスワード プロンプトで、システム パスワードを入力します。

```
Password: enablepass
```

パスワードが許可されると、特権 EXEC モード プロンプトが表示されます。

```
Router#
```

これで、特権 EXEC モードの CLI へのアクセスが可能になりました。必要なコマンドを入力して、必要なタスクを実行できます。

ステップ 3 **setup** コマンドを入力する場合は、『Hardware Installation Guide for Cisco 8300 Series Secure Routers』の「Initial Configuration」の項で「Using Cisco Setup Command Facility」を参照してください。

ステップ 4 コンソール セッションを終了するには、**quit** コマンドを入力します。

```
Router# quit
```

SSH を使用したコンソールへのアクセス

Secure Shell（SSH）は、ネットワーク デバイスへのセキュアなリモート アクセス接続を提供するプロトコルです。デバイスで SSH サポートを有効にするには、次の手順を実行します。

手順

ステップ 1 ホスト名を設定します。

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

このホスト名 は、デバイスのホスト名または IP アドレスです。

ステップ 2 デバイスの DNS ドメインを設定します。

```
Router(config)# ip domain name cisco.com
```

ステップ 3 SSH で使用する SSH キーを生成します。

```
Router(config)#  crypto key generate rsa
The name for the keys will be: Router.xxx.cisco.com Choose the size of the key modulus in the range

of 360 to 4096 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a
few
minutes.
How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
Router(config)#
```

ステップ 4 デフォルトでは、vtys? transport は Telnet です。この場合、Telnet はディセーブルであり、SSH のみサポートされます。

```
Router(config)#line vty 0 4
xxx_lab(config-line)#transport input ssh
```

ステップ 5 SSH 認証用のユーザ名を作成し、ログイン認証をイネーブルにします。

```
Router(config)# username jsmith privilege 15 secret 0 p@ss3456
Router(config)#line vty 0 4
Router(config-line)# login local
```

ステップ 6 SSH を使用してデバイスへのリモート接続を確認します。

Telnet を使用してリモートコンソールから CLI にアクセスする方法

ここでは、Telnet を使用してリモートコンソールから CLI にアクセスする手順について説明します。

- Telnet を使用してデバイスコンソールに接続するための準備 （42 ページ）
- Telnet 経由でのコンソールインターフェイスへのアクセス （42 ページ）

Telnet を使用してデバイスコンソールに接続するための準備

TCP/IP ネットワークから Telnet を使用してデバイスにリモートアクセスするには、**line vty** グローバル コンフィギュレーション コマンドを使用して、仮想端末回線をサポートするようにデバイスを設定します。ユーザに対してログインとパスワードの指定を要求するように、仮想端末回線を設定します。

line vty グローバル コンフィギュレーション コマンドの詳細については、『Cisco IOS Terminal Services Command Reference』を参照してください。

回線パスワードを VTY に追加するには、**login** コマンドの設定時に **password** コマンドを使ってパスワードを指定します。

認証、認可、アカウンティング（AAA）を使用する場合は、**login authentication** コマンドを設定します。login authentication コマンドを使用してリストを設定するときに、回線上で AAA 認証に関するログインが無効化されないようにするには、**aaa authentication login** グローバル コンフィギュレーション コマンドを使用して、リストを設定する必要もあります。

AAA サービスの詳細については、『Cisco IOS XE Security Configuration Guide: Secure Connectivity』および『Cisco IOS Security Command Reference』を参照してください。**login line-configuration** コマンドの詳細については、『Cisco IOS Terminal Services Command Reference』を参照してください。

また、デバイスに Telnet 接続する前に、デバイスの有効なホスト名またはデバイスに設定された IP アドレスを取得しておく必要があります。Telnet を使用してデバイスに接続するための要件の詳細、Telnet サービスのカスタマイズ方法、および Telnet キーシーケンスの使用方法については、『Cisco IOS Configuration Fundamentals Configuration Guide』を参照してください。

Telnet 経由でのコンソールインターフェイスへのアクセス

手順

ステップ 1 端末または PC から、次のいずれかのコマンドを入力します。

- **connect host** [*port*] [*keyword*]
- **telnet host** [*port*] [*keyword*]

ここで、*host* にはデバイスのホスト名または IP アドレスを指定し、*port* には 10 進数のポート番号（デフォルトは 23）を指定します。また、*keyword* にはサポートされるキーワードを指定します。これらのコマンドの詳細については、『Cisco IOS Terminal Services Command Reference』を参照してください。

（注）
アクセスサーバーを使用する場合は、ホスト名または IP アドレスに加えて、有効なポート番号（たとえば **telnet 198.51.100.2 2004**）を指定します。

次に、**telnet** コマンドを使用して、**router** という名前のデバイスに接続する例を示します。

```
unix_host% telnet router
Trying 198.51.100.2...
```

```
Connected to 198.51.100.2.
Escape character is '^]'.
unix_host% connect
```

ステップ 2 ログイン パスワードを入力します。

```
User Access Verification
Password: mypassword
```

（注）
パスワードが設定されていない場合は、Return を押します。

ステップ 3 ユーザ EXEC モードから、**enable** コマンドを入力します。

```
Router> enable
```

ステップ 4 パスワード プロンプトで、システム パスワードを入力します。

```
Password: enablepass
```

ステップ 5 **イネーブル** パスワードが許可されると、特権 EXEC モード プロンプトが次のように表示されます。

```
Router#
```

ステップ 6 これで、特権 EXEC モードの CLI へのアクセスが可能になりました。必要なコマンドを入力して、必要なタスクを実行できます。

ステップ 7 Telnet セッションを終了するには、**exit** または **logout** コマンドを使用します。

```
Router# logout
```

USB シリアルコンソールポートから CLI へのアクセス

ルータに備わっている追加のシステム設定メカニズムであるタイプ B ミニポート USB シリアル コンソールは、タイプ B USB 対応ケーブルを使用したルータのリモート管理をサポートします。『Hardware Installation Guide for Cisco 8300 Series Secure Routers』の「Connecting to a Console Terminal or Modem」の項を参照してください。

キーボードショートカットの使用方法

コマンドには、大文字と小文字の区別はありません。また、コマンドおよびパラメータは、現在使用可能な他のコマンドまたはパラメータと区別可能な文字数まで省略できます。

次の表に、コマンドの入力および編集に使用するキーボードショートカットを示します。

表 *2:* キーボードショートカット

キー名	目的
Ctrl-B または←キー [1]	カーソルを 1 文字分だけ後ろに戻します。
Ctrl-F または→キー [1]	カーソルを 1 文字分だけ前に進めます。

キー名	目的
Ctrl+A	カーソルをコマンドラインの先頭に移動させます。
Ctrl+E	カーソルをコマンドラインの末尾に移動させます。
Esc B	カーソルを 1 ワード分だけ後ろに戻します。
Esc F	カーソルを 1 ワード分だけ前に進めます。

履歴バッファによるコマンドの呼び出し

履歴バッファには、直前に入力した 20 のコマンドが保存されます。特別な省略コマンドを使用して、再入力せずに保存されているコマンドにアクセスできます。

次の表に、ヒストリ置換コマンドの一覧を示します。

表 *3:* ヒストリ置換コマンド

コマンド	目的
Ctrl+P または↑キー [1]	履歴バッファ内のコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。キーを押すたびに、より古いコマンドが順次表示されます。
Ctrl+N または↓キー [1]	**Ctrl+P** または↑キーでコマンドを呼び出した後で、履歴バッファ内のより新しいコマンドに戻ります。
Router# show history	EXEC モードで、最後に入力したいくつかのコマンドの一覧を表示します。

[1] 矢印キーを使用できるのは、VT100 などの ANSI 互換端末に限られます。

コマンドモードの概要

Cisco IOS XE で使用できるコマンド モードは、従来の Cisco IOS で使用できるコマンド モードと同じです。これは自律モードでのみサポートされます。Cisco IOS XE ソフトウェアにアクセスするには、CLI を使用します。CLI には複数のモードがあることから、利用できるコマンドはその時点で利用しているモードにより異なります。CLI プロンプトでクエスチョン マーク（**?**）を入力すると、それぞれのコマンドモードで利用できるコマンドの一覧を取得できます。

CLI にログインしたときのモードはユーザ EXEC モードです。ユーザ EXEC モードでは、使用できるコマンドが制限されています。すべてのコマンドを使用できるようにするには、通常はパスワードを使用して、特権 EXEC モードを開始する必要があります。特権 EXEC モードから

は、すべての EXEC コマンド（ユーザ モードまたは特権モード）を実行できます。また、グローバル コンフィギュレーション モードを開始することもできます。ほとんどの EXEC コマンドは 1 回限りのコマンドです。たとえば、**show** コマンドであれば重要なステータス情報が表示され、**clear** コマンドであれば、カウンタやインターフェイスがクリアされます。EXEC コマンドはソフトウェアの再起動時に保存されません。

コンフィギュレーションモードでは、実行コンフィギュレーションを変更できます。その後、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存しておくと、変更されたコマンドはソフトウェアの再起動後も保存されます。特定のコンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードを開始する必要があります。グローバル コンフィギュレーション モードでは、インターフェイス コンフィギュレーション モード、およびプロトコル専用モードなどその他のモードを開始できます。

ROM モニタ モードは、Cisco IOS XE ソフトウェアが適切にロードしない場合に使用される別個のモードです。ソフトウェアの起動時、または起動時にコンフィギュレーション ファイルが破損している場合に、有効なソフトウェア イメージが見つからなければ、ソフトウェアは ROM モニタ モードを開始することがあります。

次の表で、Cisco IOS XE ソフトウェアのさまざまな一般的コマンドモードへのアクセス方法、またはアクセスを終了する方法について説明します。また、各モードで表示されるプロンプトの例も示します。

表 *4*: コマンドモードのアクセス方法および終了方法

コマンド モード	アクセス方法	プロンプト	終了方法
ユーザー EXEC	ログインします。	`Router>`	**logout** コマンドを使用します。
特権 EXEC	ユーザ EXEC モードから、**enable** コマンドを使用します。	`Router#`	ユーザ EXEC モードに戻るには、**disable** コマンドを使用します。
グローバル コンフィギュレーション	特権 EXEC モードで、**configure terminal** コマンドを使用します。	`Router(config)#`	グローバル コンフィギュレーション モードから特権 EXEC モードに戻るには、**exit** or **end** コマンドを使用します。
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、**interface** コマンドを使用してインターフェイスを指定します。	`Router(config-if)#`	グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。 特権 EXEC モードに戻るには、**end** コマンドを使用します。

コマンド モード	アクセス方法	プロンプト	終了方法
診断	デバイスは、次のような場合に、診断モードを開始するか、または診断モードにアクセスします。 • 場合によっては、Cisco IOS プロセスで障害が発生したときに、診断モードが開始することがあります。ただし、ほとんどの場合、デバイスはリロードされます。 • ユーザが **transport-map** コマンドを使用して設定したポリシーにより、診断モードが開始する場合があります。 • ブレーク信号（**Ctrl-C**、**Ctrl-Shift-6**、または **send break** コマンド）を入力すると、ブレーク信号を受信したデバイスが診断モードに移行するように設定されている場合があります。	`Router(diag)#`	Cisco IOS プロセスの障害によって診断モードが開始された場合は、Cisco IOS の問題を解決した後に、デバイスを再起動して診断モードを終了する必要があります。 デバイスが transport-map 設定によって診断モードを開始した場合、デバイスにアクセスするには、別のポートを使用するか、または Cisco IOS CLI に接続するよう設定された方法を使用します。

コマンド モード	アクセス方法	プロンプト	終了方法
ROM モニタ	特権 EXEC モードで、**reload** EXEC コマンドを使用します。システムの起動時、最初の 60 秒以内に **Break** キーを押します。	`rommon#>`	ROM モニタ モードを終了するには、有効なイメージを手動でブートするか、または自動ブートを設定してリセットを実行し、有効なイメージがロードされるようにします。

診断モードの概要

デバイスは、次のような場合に、診断モードを開始するか、または診断モードにアクセスします。

- IOS プロセスの障害が原因の場合があります。あるいは、IOS プロセスで障害が発生したときにシステムがリセットすることがあります。
- **transport-map** コマンドを使ってユーザ設定のアクセス ポリシーが設定されると、ユーザは診断モードに誘導されます。
- デバイスにアクセスしている間に送信ブレーク信号（**Ctrl-C** または **Ctrl-Shift-6**）が入力されると、ブレーク信号を受信したデバイスが診断モードを開始するように設定されている場合があります。

診断モードでは、ユーザ EXEC モードで使用可能なコマンドのサブセットを使用できます。このコマンドは、次のような場合に使用できます。

- IOS の状態など、デバイス上のさまざまな状態を検査する。
- コンフィギュレーションの置き換えまたはロールバック。
- IOS またはその他のプロセスの再開方法を提供する。
- デバイス全体、モジュール、または他のハードウェアコンポーネントなどのハードウェアをリブートする。
- FTP、TFTP、および SCP などのリモートアクセス方式を使用した、デバイスに対するファイル転送、またはデバイスからのファイル転送。

以前のデバイスでは、障害時に ROMMON などの制限付きアクセス方式を使用して Cisco IOS 問題を診断し、トラブルシューティングを行っていましたが、診断モードを使用すると、より広範なユーザーインターフェイスを使用してトラブルシューティングできるようになります。診断モード コマンドは、Cisco IOS プロセスが正常に動作していないときでも動作可能です。これらのコマンドは、デバイスが正常に動作している場合、デバイスの特権 EXEC モードでも使用できます。

サポートを受ける

CLI プロンプトで疑問符（**?**）を入力すると、各コマンド モードで使用できるコマンドの一覧が表示されます。またコンテキスト ヘルプ機能を使用すると、コマンドに関連するキーワードと引数のリストを取得できます。

コマンドモード、コマンド、キーワード、または引数に固有のヘルプを表示するには、次のいずれかのコマンドを使用します。

コマンド	目的
help	コマンド モードのヘルプ システムの概要を示します。
abbreviated-command-entry?	特定の文字ストリングで始まるコマンドのリストが表示されます （注） コマンドと疑問符の間にスペースは不要です。
abbreviated-command-entry<Tab>	特定のコマンド名を補完します。
?	特定のコマンド モードで使用できる全コマンドの一覧を表示します。
command ?	コマンドラインで次に入力する必要のあるキーワードまたは引数が表示されます （注） コマンドと疑問符の間にスペースを挿入してください。

コマンドオプションの検索：例

ここでは、コマンド構文の表示方法について説明します。コマンド構文には、任意または必須のキーワードおよび引数が含まれています。コマンドのキーワードおよび引数を表示するには、コンフィギュレーション プロンプトで疑問符（?）を入力するか、またはコマンドの一部を入力した後に 1 スペース空けて、疑問符（**?**）を入力します。Cisco IOS XE ソフトウェアにより、使用可能なキーワードおよび引数のリストと簡単な説明が表示されます。たとえば、グローバル コンフィギュレーション モードで **arap** コマンドのすべてのキーワードまたは引数を表示するには、**arap ?** と入力します。

コマンド ヘルプ出力の中の <cr> 記号は改行を表します。古いキーボードでは、CR キーは **Return** キーです。最近のキーボードでは、CR キーは **Enter** キーです。コマンド ヘルプの最後の <cr> 記号は、**Enter** キーを押してコマンドを完成させるオプションがあること、および <cr> 記号に先行するリスト内の引数およびキーワードはオプションであることを示します。<cr> 記号だけの場合は、使用可能な引数またはキーワードが他に存在せず、**Enter** キーを押してコマンドを完成させる必要があることを示します。

次の表に、コマンド入力支援のために疑問符（**?**）を使用する例を示します。

表 *5:* コマンドオプションの検索

コマンド	コメント
Router> **enable** Password: <password> Router#	**enable** コマンドとパスワードを入力して、特権 EXEC コマンドにアクセスします。プロンプトが「>」から「#」に変わったら（例：Router> から Router#）、特権 EXEC モードに切り替わっています。
Router# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	**configure terminal** 特権 EXEC コマンドを入力して、グローバル コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードが開始されると、プロンプトが Router(config)# に変わります。
Router(config)# **interface GigabitEthernet ?** <0-1> GigabitEthernet interface number Router(config)# **interface GigabitEthernet 0/?** <0-5> Port Adapter number Router (config)# **interface GigabitEthernet 0/0/?** <0-63> GigabitEthernet interface number Router (config)# **interface GigabitEthernet0/0/1?** . <0-5> Router(config-if)#	インターフェイス コンフィギュレーション モードを開始するには、**interface GigabitEthernet** グローバル コンフィギュレーション コマンドを使用して、設定するインターフェイスを指定します。 次にコマンド ラインに入力する必要があるコマンドを表示するには、**?** と入力します。 <cr> 記号が表示されている場合は、**Enter** キーを押してコマンドを完了できます。 インターフェイス コンフィギュレーション モードが開始されると、プロンプトが Router(config-if)# に変わります。

コマンド	コメント

`Router(config-if)# ?`
`Interface configuration commands:`
`  .`
`  .`
`  .`
`  ip  Interface Internet Protocol config commands`
`  keepalive  Enable keepalive`
`  lan-name  LAN Name command`
`  llc2  LLC2 Interface Subcommands`
`  logging  Configure logging for interface`
`  mls  mls router sub/interface commands`
`  mpoa  MPOA interface configuration commands`
`  mtu  Set the interface MTU`
`  no  Negate a command or set its defaults`
`  ntp  Configure NTP`
`  .`
`  .`
`  .`
`Router(config-if)#`
	インターフェイスに使用できるすべてのインターフェイス コンフィギュレーション コマンドのリストを表示するには、**?** を入力します。次の例では、使用可能なインターフェイス コンフィギュレーション コマンドの一部だけを示しています。

`Router(config-if)# ip ?`
`Interface IP configuration subcommands:`
`  access-group  Specify access control for packets`
`  accounting  Enable IP accounting on this interface`
`  address  Set the IP address of an interface`
`  authentication authentication subcommands`
`  cgmp  Enable/disable CGMP`
`  dvmrp  DVMRP interface commands`
`  hello-interval Configures IP-EIGRP hello interval`
`  hold-time  Configures IP-EIGRP hold time`
`  .`
`  .`
`  .`
`Router(config-if)# ip`
	インターフェイスの設定のためのコマンドを入力します。この例では、**ip** コマンドを使用します。
	次にコマンド ラインに入力する必要があるコマンドを表示するには、**?** と入力します。次の例では、使用可能なインターフェイス IP コンフィギュレーション コマンドの一部だけを示しています。

`Router(config-if)# ip address ?`
`  A.B.C.D  IP address`
`  negotiated  IP Address negotiated over PPP`
`Router(config-if)# ip address`
	インターフェイスの設定のためのコマンドを入力します。この例では、**ip address** コマンドを使用しています。
	次にコマンド ラインに入力する必要があるコマンドを表示するには、**?** と入力します。この例では、IP アドレスまたは **negotiated** キーワードを入力する必要があります。
	改行（<cr>）は表示されません。このため、コマンドを完成させるには、追加のキーワードまたは引数を入力する必要があります。

コマンド	コメント
Router(config-if)# ip address 198.51.100.5 ? A.B.C.D IP subnet mask Router(config-if)# **ip address 198.51.100.5**	使用するキーワードまたは引数を入力します。この例では、IP アドレス 198.51.100.5 を使用しています。 次にコマンド ラインに入力する必要があるコマンドを表示するには、**?** と入力します。この例では、IP サブネット マスクを入力する必要があります。 <cr> は表示されません。このため、コマンドを完成させるには、追加のキーワードまたは引数を入力する必要があります。
Router(config-if)# **ip address 198.51.100.5 255.255.255.0 ?** secondary Make this IP address a secondary address <cr> Router(config-if)# **ip address 198.51.100.5 255.255.255.0**	IP サブネット マスクを入力します。この例では、IP サブネット マスク 255.255.255.0 を使用しています。 次にコマンド ラインに入力する必要があるコマンドを表示するには、**?** と入力します。この例では、**secondary** キーワードを入力するか、Enter キーを押します。 <cr> が表示されます。Enter キーを押してコマンドを完了するか、または別のキーワードを入力します。
Router(config-if)# **ip address 198.51.100.5 255.255.255.0** Router(config-if)#	Enter キーを押してコマンドを完了します。

コマンドの no 形式および default 形式の使用方法

ほぼすべてのコンフィギュレーション コマンドに **no** 形式があります。一般には、**no** 形式を使用して機能を無効にします。無効化されている機能を再び有効にしたり、デフォルトで無効な機能を有効にするには、**no** キーワードを指定しないでコマンドを使用します。たとえば、IP ルーティングはデフォルトで有効です。IP ルーティングを無効にするには、**no ip routing** コマンドを使用します。IP ルーティングを再び有効にするには、**ip routing** コマンドを使用します。Cisco IOS ソフトウェアのコマンド リファレンスには、コンフィギュレーション コマンドの完全な構文、および **no** 形式のコマンドの機能が記載されています。

多くの CLI コマンドには **default** 形式もあります。<*command*> **default** command-name を発行すると、コマンドをデフォルト設定に戻すことができます。Cisco IOS ソフトウェア コマンド リファレンスでは、プレーン形式や **no** 形式のコマンドとは異なる機能が **default** 形式のコマンドで実行される場合の、**default** 形式の機能が説明されています。システムで使用できるデフォルト コマンドを表示するには、該当するコマンド モードで **default?** と入力します。

コンフィギュレーションの変更の保存

設定の変更をスタートアップコンフィギュレーションに保存して、ソフトウェアのリロードや停電が発生した場合に変更内容が失われないようにするには、**copy running-config startup-config** コマンドを使用します。次に例を示します。

```
Router# copy running-config startup-config
Building configuration...
```

設定の保存に数分かかることがあります。設定が保存されると、次の出力が表示されます。

```
[OK]
Router#
```

この作業により、設定が NVRAM に保存されます。

コンフィギュレーション ファイルの管理

スタートアップ コンフィギュレーション ファイルは nvram: ファイル システムに保存され、実行コンフィギュレーション ファイルは system: ファイル システムに保存されます。このコンフィギュレーション ファイルの保存設定は、他のいくつかのシスコ ルータ プラットフォームでも使用されています。

シスコ ルータの日常的なメンテナンスの一環として、スタートアップ コンフィギュレーション ファイルを NVRAM から他のいずれかのルータ ファイル システムにコピーし（さらに追加でネットワーク サーバにもコピーして）、バックアップをとっておく必要があります。スタートアップコンフィギュレーションファイルをバックアップしておくと、何らかの理由でNVRAM上のスタートアップ コンフィギュレーション ファイルが使用できなくなったときに、スタートアップ コンフィギュレーション ファイルを簡単に回復できます。

スタートアップ コンフィギュレーション ファイルのバックアップには、**copy** コマンドを使用できます。

コンフィギュレーション ファイルの管理の詳細については、『Cisco IOS XE Configuration Fundamentals Configuration Guide』の「Managing Configuration Files」の項を参照してください。

show コマンドおよび more コマンドの出力のフィルタリング

show および **more** コマンドの出力を検索してフィルタリングできます。この機能は、大量の出力を並べ替える必要がある場合や、不要な出力を除外する場合に役立ちます。

この機能を使うには、**show** または **more** コマンドに「パイプ」記号（|）を続け、**begin**、**include**、**exclude** のキーワードのいずれかを入力します。さらに検索またはフィルタリングの内容を正規表現で指定します（大文字と小文字は区別されます）。

show | {**append** | **begin** | **exclude** | **include** | **redirect** | **section** | **tee**} *regular-expression*

この出力は、コンフィギュレーション ファイル内の情報の特定の行に一致します。

例

この例では、**show interface** コマンドの修飾子（**include protocol**）を使用して、式 **protocol** が表示される出力行のみを示します。

C8375-E-G2 の出力例：

```
Router# show interface | include protocol
TwoGigabitEthernet0/0/0 is down, line protocol is down
0 unknown protocol drops
TwoGigabitEthernet0/0/1 is up, line protocol is up
0 unknown protocol drops
TwoGigabitEthernet0/0/2 is down, line protocol is down
0 unknown protocol drops
TwoGigabitEthernet0/0/3 is up, line protocol is up
0 unknown protocol drops
TenGigabitEthernet0/0/4 is up, line protocol is up
0 unknown protocol drops
TenGigabitEthernet0/0/5 is up, line protocol is up
 0 unknown protocol drops
TwoGigabitEthernet0/1/0 is administratively down, line protocol is down (disabled)
0 unknown protocol drops
TwoGigabitEthernet0/1/1 is down, line protocol is down (notconnect)
0 unknown protocol drops
TwoGigabitEthernet0/1/2 is down, line protocol is down (notconnect)
0 unknown protocol drops
TwoGigabitEthernet0/1/3 is down, line protocol is down (notconnect)
0 unknown protocol drops
TwoGigabitEthernet0/1/4 is down, line protocol is down (notconnect)
0 unknown protocol drops
TwoGigabitEthernet0/1/5 is down, line protocol is down (notconnect)
 0 unknown protocol drops
TwoGigabitEthernet0/1/6 is up, line protocol is up
0 unknown protocol drops
TwoGigabitEthernet0/1/7 is up, line protocol is up
0 unknown protocol drops
TwoGigabitEthernet0/1/7.10 is up, line protocol is up
GigabitEthernet0 is up, line protocol is up
0 unknown protocol drops
Tunnel0 is up, line protocol is up
Tunnel protocol/transport multi-GRE/IP
0 unknown protocol drops
VirtualPortGroup0 is up, line protocol is up
0 unknown protocol drops
VirtualPortGroup1 is up, line protocol is up
0 unknown protocol drops
VirtualPortGroup10 is up, line protocol is up
0 unknown protocol drops
Vlan1 is up, line protocol is down , Autostate Enabled
0 unknown protocol drops
```

C8355-G2 の出力例：

```
Router# show interface | include protocol
FiveGigabitEthernet0/0/0 is administratively down, line protocol is down
0 unknown protocol drops
FiveGigabitEthernet0/0/1 is administratively down, line protocol is down
0 unknown protocol drops
FiveGigabitEthernet0/0/2 is administratively down, line protocol is down
0 unknown protocol drops
FiveGigabitEthernet0/0/3 is administratively down, line protocol is down
0 unknown protocol drops
GigabitEthernet0/0/4 is administratively down, line protocol is down (disabled)
0 unknown protocol drops
```

```
GigabitEthernet0/0/5 is administratively down, line protocol is down (disabled)
 0 unknown protocol drops
TenGigabitEthernet0/0/6 is administratively down, line protocol is down (disabled)
0 unknown protocol drops
TenGigabitEthernet0/0/7 is administratively down, line protocol is down (disabled)
0 unknown protocol drops
TenGigabitEthernet0/0/8 is up, line protocol is up
0 unknown protocol drops
TenGigabitEthernet0/0/9 is up, line protocol is up
0 unknown protocol drops
GigabitEthernet0 is up, line protocol is up
0 unknown protocol drops
Loopback1 is up, line protocol is up
0 unknown protocol drops
Loopback2 is up, line protocol is up
0 unknown protocol drops
Loopback3 is up, line protocol is up
0 unknown protocol drops
Tunnel3 is up, line protocol is down
 Tunnel protocol/transport IPSEC/IP
0 unknown protocol drops
Vlan1 is up, line protocol is down , Autostate Enabled
0 unknown protocol drops
Vlan10 is up, line protocol is down , Autostate Enabled
0 unknown protocol drops
```

デバイスの電源オフ

デバイスの電源スイッチをオフの位置にすることで、デバイスをいつでも安全にオフにできます。ただし、NVRAM に対する設定の最後の WRITE 処理以降に加えた実行コンフィギュレーションへの変更は失われます。

デバイスの電源をオフにする前に、スタートアップ後に必要な設定が保存されていることを確認します。copy running-config startup-config コマンドは、設定を NVRAM に保存します。デバイスの電源を入れると、保存された設定でデバイスが開始されます。

プラットフォームおよびシスコソフトウェアイメージのサポート情報の検索

Cisco IOS XE ソフトウェアは、特定のプラットフォームをサポートするソフトウェアイメージで構成されるフィーチャセットとしてパッケージ化されています。特定のプラットフォームでどのフィーチャ セットのグループを使用できるかは、リリースに含まれるシスコ ソフトウェアイメージによって異なります。特定のリリースで使用できるソフトウェアイメージのセットを確認したり、ある機能が特定の Cisco IOS XE ソフトウェアイメージで使用可能かどうかを確認したりするには、Cisco Feature Navigator を使用するか、『Release Notes for Cisco 8300 Series Secure Routers』を参照してください。

Cisco Feature Navigator

プラットフォームのサポートおよびソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator は、特定のソフトウェアリリース、フィーチャ セット、またはプラットフォームをサポートする Cisco IOS XE のソフ

トウェア イメージを判別できるツールです。Navigator ツールを使用するには、Cisco.com のアカウントは必要ありません。

Software Advisor

シスコが管理する Software Advisor ツールでは、ある機能が Cisco IOS XE リリースでサポートされているかどうかを確認したり、その機能のソフトウェアマニュアルを検索したり、デバイスに装着されているハードウェアでの Cisco IOS XE ソフトウェアの最小ソフトウェア要件を確認したりできます。このツールにアクセスするには、Cisco.com の登録ユーザである必要があります。

ソフトウェア リリース ノート

以下の事項については、『Release Notes document for Cisco 8300 Series Secure Routers』を参照してください。

- メモリに関する推奨事項
- 重大度 1 および 2 の未解決および解決済みの注意事項

リリース ノートには、最新のリリースに固有の情報が記載されています。これらの情報には、以前のリリースに記載済みの機能に関する情報が含まれていないことがあります。機能に関するこれまでのすべての情報については、Cisco Feature Navigator（https://cfnng.cisco.com/）を参照してください。

CLI セッション管理

非アクティブ タイムアウトを設定して、強制的に適用することができます。セッション ロックにより、2 人のユーザが別々に行った変更を相互に上書きできないように保護できます。使用可能なすべてのキャパシティが内部プロセスによって使用されるのを防ぐために、CLI セッション アクセス用に予備の容量が予約されています。たとえば、これによりユーザはルータにリモート アクセスすることができます。

- CLI セッション タイムアウトの変更 （56 ページ）
- CLI セッションのロック （56 ページ）

CLI セッション管理について

非アクティブ タイムアウトを設定して、強制的に適用することができます。セッション ロックにより、2 人のユーザがそれぞれ行った変更を相互に上書きできないように保護できます。使用可能なすべてのキャパシティが内部プロセスによって使用されるのを防ぐために、CLI セッション アクセス用に予備の容量が予約されています。たとえば、これによりユーザはルータにリモート アクセスできます。

CLI セッションタイムアウトの変更

手順

ステップ 1 **configure terminal**

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **line console 0**

ステップ 3 **session-timeout** *minutes*

minutes の値により、タイムアウトになるまでの CLI の待機時間が設定されます。CLI セッション タイムアウトを設定すると、CLI セッションのセキュリティが強化されます。*minutes* に値 0 を指定すると、セッション タイムアウトが無効になります。

ステップ 4 **show line console 0**

セッション タイムアウトとして設定された値を確認します（"Idle Session" の値として表示されます）。

CLI セッションのロック

始める前に

CLI セッションの一時パスワードを設定するには、EXEC モードで **lock** コマンドを使用します。**lock** コマンドを使用するには、その前に **lockable** コマンドを使用して回線を設定する必要があります。次の例では、回線が **lockable** として設定され、その後 **lock** コマンドを使用して一時パスワードが割り当てられます。

手順

ステップ 1 **Router# configure terminal**

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **lock** コマンドを使用できるようにする回線を入力します。

Router(config)# line console 0

ステップ 3 **Router(config)# lockable**

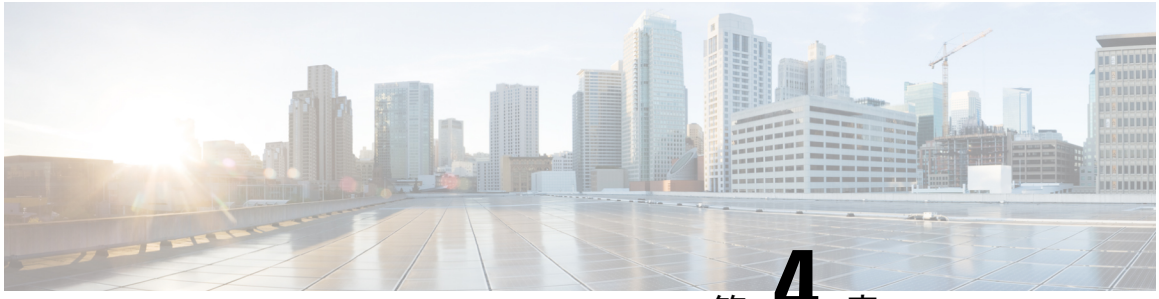
回線をロック可能にします。

ステップ 4 **Router(config)# exit**

ステップ 5 **Router# lock**

パスワードの入力が求められます。パスワードを 2 回入力する必要があります。

```
Password: <password>
Again: <password>
Locked
```



第 4 章

改ざん検出

この章では、Cisco 8300 シリーズセキュアルータでの改ざん検出に関する情報を提供します。この章で説明する内容は、次のとおりです。

改ざん検出

改ざん検出は、潜在的な改ざんイベントを特定するために Cisco 8300 シリーズ セキュアルータに実装されたセキュリティ機能です。各ルータは、シャーシカバーが安全に取り付けられた状態で製造元から出荷されます。出荷後にシャーシカバーが開かれた場合、ハードウェアは、デバイスの電源がオンになっているかオフになっているかに関係なく、すべてのシャーシカバーが開閉されたイベントを改ざん防止メモリに記録します。

起動時に、ソフトウェアは最新のイベントインデックスを読み取り、以前の既知のインデックスと比較します。不一致がある場合、ソフトウェアは起動時に Syslog メッセージを生成して、改ざんイベントを報告します。デバイスの電源が完全にオンになると、ソフトウェアは Syslog メッセージと SNMP トラップをただちに生成します。

利点

改ざん検出通知は、不正な物理アクセスやデバイスを侵害する試みを検出して、機密データとネットワークの完全性を保護します。

制限事項

改ざん検出機能は現在、SDWAN/SD ルーティングモードではサポートされていません。

改ざん検出の設定

改ざん検出はルータでデフォルトで有効になっています。シャーシカバーの開くまたは閉じるイベントが自動的に記録されます。

改ざんイベント通知は、config モードで以下のコマンドを使用して有効または無効にできます。

- 設定モードで次のコマンドを使用して、改ざん検出通知を有効にします（デフォルトで有効）。

  ```
  Router(config)#platform tamper detection
  ```

- config モードで次のコマンドを使用して、改ざん検出通知を無効化します。

  ```
  Router(config)#no platform tamper detection
  ```

改ざん検出イベントの確認

```
Router# show platform tamper-detection event [power-off | power-on] [all | lastx | new]
```

オプション	説明
電源オフ	**電源オフ** オプションは、ルータに電源ケーブルが接続されていない場合に改ざんイベントを指定します。
電源の投入	**電源オン** オプションは、ルータの電源がオンになったときの改ざんイベントを指定します。
all	[**all**]オプションでは、記録されたすべての改ざんイベントが指定されます。システムは最大 500 エントリを表示できます。 500 エントリごとにロールオーバーカウンタが 1 つ増加します。
lastx	**lastx** オプションでは、表示するイベントの数を指定します。たとえば、「lastx 10」と入力すると、直近の 10 件のイベントが表示されます。
new	**new** オプションでは、最後の既知のイベントインデックス以降の新しい改ざんイベントを指定します。

show コマンドでは、以下の詳細を含むイベントログが提供されます。

- 現在のイベントインデックス

- 現在の時刻
- ロールオーバーステータスとロールオーバー回数：
  - 改ざんイベント数が 500 以下の場合、ロールオーバー数は 0、ロールオーバーステータスは No
  - ログ数が 500 に達すると、ロールオーバー数は 1 ずつ増加します。
    - 501 ～ 1000 が 1 ～ 500 を上書きする場合、ロールオーバー数は 1、ロールオーバーステータス：Yes
    - 1001 ～ 1500 が 501 ～ 1000 を上書きする場合、ロールオーバー数は 2、ロールオーバーステータス：Yes
- イベントタイプとタイムスタンプを示すイベント

システムの電源がオフになっているときのイベントの確認

システムの電源がオフになっている場合、ルータはバッテリ電源を使用して改ざんイベントを記録します。ルータは、最後の電源オフから次の電源オンまでの最初のシャーシカバーが開いたイベントを記録します。電源オフ中にシャーシカバーが何度も開いたり閉じたりした場合、最初の開いたイベントだけが記録されます。システムの電源がオフになったときのイベントログを示します。

```
Router#show platform tamper-detection event power-off all
Current Time: 2025/04/25 19:55:03       Rollover Status: No     Rollover Count: 0
-------------------------------------------------------------------------------------------------
Tamper event index      |       Tamper event timestamp  |       Tamper events description
-------------------------------------------------------------------------------------------------

    #2                           2024/08/08 02:36:41             Chassis is opened
    #1                           2000/00/00 00:00:00             Battery not present or
used up
```

システムの電源が部分的にまたは完全にオンになっている場合のイベントの確認

システムの電源が使用できる場合、ルータはすべてのシャーシカバーの開閉イベントを記録します。次の例は、システムの電源が部分的にまたは完全にオンになっているときのイベントログを示しています。

```
Router show platform tamper-detection event power-on lastx 10
Current Time: 2025/04/25 19:54:46      Rollover Status: No     Rollover Count: 0
-------------------------------------------------------------------------------------------------
Tamper event index      |       Tamper event timestamp  |       Tamper events description
-------------------------------------------------------------------------------------------------

    #2                  025/04/24 22:10:14             Chassis is opened
    #1                   025/04/24 22:02:33             Chassis is closed
```

改ざん検出 SYSlog

ルータが起動すると、イベントログから現在のイベントインデックスが読み取られ、以前に保存されていた最後の既知のインデックスと比較されます。インデックス間に不一致がある場合、またはタイムスタンプが異なる場合、改ざん検出通知が有効になっていると、IOS は起動時に警告レベルの SYSlog メッセージを生成し、コントローラモードでコントローラに通知を送信します。

このセクションでは、SYSlog イベントの例を示します。

- 電源投入イベントの SYSlog

  改ざん検出が有効で、システムの電源がオンになっている場合、電源オンの SYSlog メッセージが起動中に表示されます。

```
Apr 25 20:15:01.064: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
was opened 0 times and closed 0 times during power up since last known event index
7 at 2025/04/24 22:11:51
```

- 電源オフイベントの SYSlog

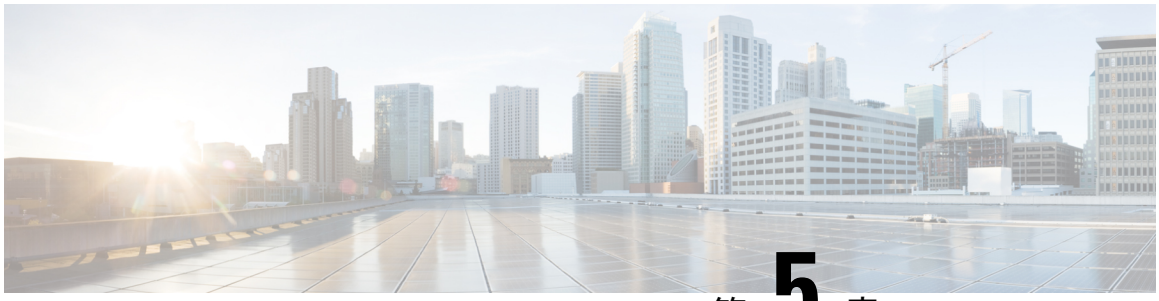
  改ざん検出が有効で、システムの電源がオフになっている場合、電源オフの SYSlog メッセージが起動中に表示されます。

```
Apr 25 20:15:01.064: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
was opened 0 times and closed 0 times during power down since last known event index
 5 at 2025/04/24 22:11:51
```

- ランタイムイベントの SYSlog

```
*Aug 29 06:56:34.560: %CMRP-4-INTRUSION_ALERT: R0/0: cmand: The system cover has
been opened !!
*Aug 29 06:56:36.130: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
 was opened 2 times and closed 0 times during power down since last known event index
 50 at 2025/06/04 08:03:06
*Aug 29 06:56:36.130: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
 was opened 20 times and closed 20 times during power up since last known event index
 1638 at 2025/06/05 07:08:12

*Aug 29 06:57:04.563: %CMRP-4-INTRUSION_ALERT: R0/0: cmand: The system cover has
been closed !!
*Aug 29 06:57:06.137: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
 was opened 2 times and closed 0 times during power down since last known event index
 50 at 2025/06/04 08:03:06
*Aug 29 06:57:06.137: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
 was opened 20 times and closed 21 times during power up since last known event index
 1638 at 2025/06/05 07:08:12
```

（注） 改ざん検出機能が無効になっている場合、SYSlog メッセージは起動時に表示されません。



第 5 章

Web ユーザーインターフェイスを使用したデバイスの管理

Web ユーザー インターフェイス（WebUI）は、組み込み GUI ベースのデバイス管理ツールです。デバイスをプロビジョニングしたり、デバイスの導入および管理性を簡素化したり、ユーザーエクスペリエンスを向上したりする機能を提供します。デフォルトのイメージが用意されているため、何かを有効化したりデバイスにライセンスをインストールしたりする必要はありません。WebUI を使用すれば、CLI の専門知識がなくても、設定を構築し、デバイスのモニタリングとトラブルシューティングを行うことができます。この章は、次のセクションで構成されています。

Web UI を使用した工場出荷時のデフォルト状態であるデバイスの設定

クイック セットアップ ウィザードを使用して、基本的なルータ設定を実行できます。ルータを設定するには、以下の手順を実行します。

（注） Web UI にアクセスする前に、デバイスで基本設定を行う必要があります。

手順

ステップ 1 シリアルケーブルの RJ-45 側をルータの RJ-45 コンソールポートに接続します。

ステップ 2 デバイスの初期設定ウィザードが表示された後、次のシステムメッセージがルータに表示されたら、「**No**」と入力してデバイスプロンプトを表示します。

Would you like to enter the initial configuration dialog? [yes/no]: no

ステップ 3 コンフィギュレーション モードで、次の設定パラメータを入力します。

```
!
ip dhcp pool WEBUIPool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1

username admin privilege 15 password 0 default
!
interface gig 0/0/1
ip address 192.168.1.1 255.255.255.0
!
```

ステップ 4 イーサネットケーブルで PC とルータを接続し、gig 0/0/1 インターフェイスに接続します。

ステップ 5 PC を DHCP クライアントとして設定し、ルータの IP アドレスを自動的に取得します。

ステップ 6 ブラウザを起動し、ブラウザのアドレス行にデバイスの IP アドレスを入力します。セキュアな接続の場合は、「https://192.168.1.1/#/dayZeroRouting」と入力します。あまりセキュアではない接続の場合は、「http://192.168.1.1/#/dayZeroRouting」と入力します。

ステップ 7 デフォルトのユーザー名（admin）とデフォルトのパスワードを入力します。

基本または詳細モードのセットアップウィザード

基本モードまたは詳細モードのセットアップを使用してルータを設定するには、次の手順を実行します。

手順

ステップ 1 [Basic Mode] または [Advanced Mode] を選択し、[Go To Account Creation Page] をクリックします。

ステップ 2 ユーザ名とパスワードを入力します。確認のためにパスワードを再入力します。

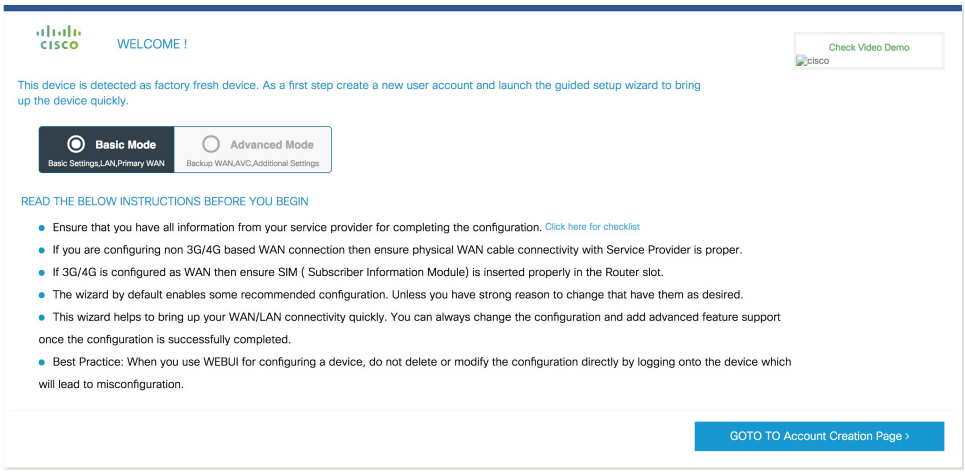
ステップ 3 [Create and Launch Wizard] をクリックします。

ステップ 4 デバイス名とドメイン名を入力します。

ステップ 5 [Time Zone] ドロップダウンリストから、適切なタイムゾーンを選択します。

ステップ 6 [Date and Time] ドロップダウンリストから、適切な日時モードを選択します。

ステップ 7 [LAN Settings] をクリックします。



LAN 設定の構成

手順

ステップ 1 [Web DHCP Pool/DHCP Pool] 名または [Create and Associate Access VLAN] オプションを選択します。

a) [Web DHCP Pool] を選択した場合は、次を指定します。

[Pool Name]：DGCP プール名を入力します。

[Network]：ネットワークアドレスおよびサブネットマスクを入力します。

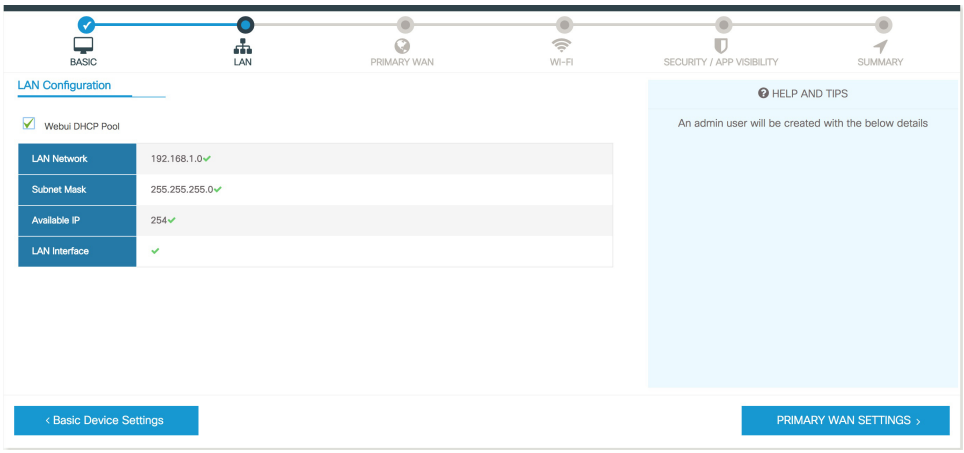
b) [Create and Associate Access VLAN] オプションを選択した場合は、次を指定します。

[Access VLAN]：アクセス VLAN の識別番号を入力します。指定できる範囲は 1 ～ 4094 です。

[Network]：VLAN の IP アドレスを入力します。

[Management Interfaces]：インターフェイスを選択し、右矢印と左矢印を使用して選択したリストボックスに移動します。ダブルクリックするかドラッグアンドドロップして、選択したリストボックスにインターフェイスを移動することもできます。

ステップ 2 [Primary WAN Settings] をクリックします。



プライマリ WAN 設定の構成

手順

ステップ 1 プライマリ WAN タイプを選択します。プライマリ WAN は、ルータがサポートする WAN のタイプに応じて、シリアル、3G/4G、イーサネット、またはブロードバンド（xDSL）を設定できます。

ステップ 2 ドロップダウン リストからインターフェイスを選択します。

ステップ 3 サービス プロバイダーから DNS サーバ情報を直接取得するには、[Get DNS Server info directly from ISP] チェックボックスをオンにします。プライマリ DNS とセカンダリ DNS は手動で入力することもできます。

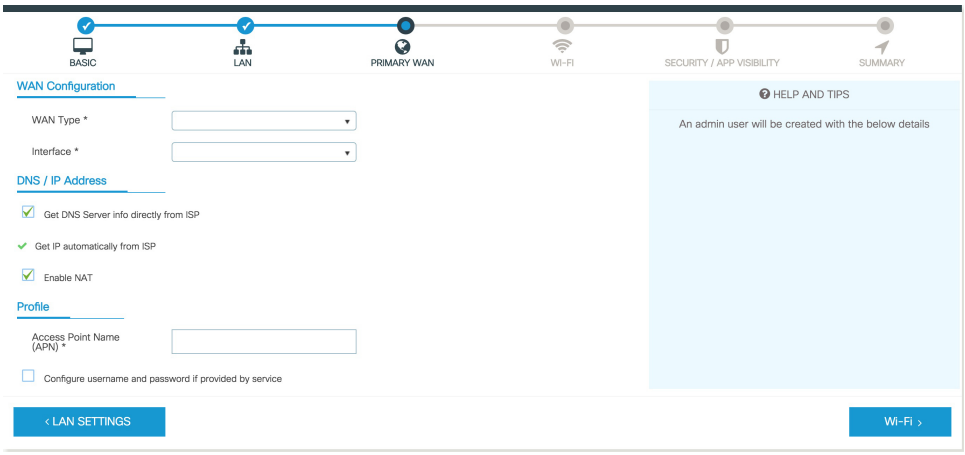
ステップ 4 [Get IP automatically from ISP] チェックボックスをオンにして、サービスプロバイダーから IP アドレス情報を直接取得します。IP アドレスおよびサブネット マスクを入力します。

ステップ 5 [Enable NAT] チェックボックスをオンにして、NAT を有効にします。NAT を有効にすることをお勧めします。

ステップ 6 [Enable PPPoE] チェックボックスをオンにして、PPPoE を有効にします。PPPoE を有効にする場合は、必要な認証モードを選択します。オプションは **PAP** と **CHAP** です。

ステップ 7 サービス プロバイダーから提供されたユーザー名とパスワードを入力します。

ステップ 8 [**Security/APP Visibility WAN Settings**] をクリックします。



セカンダリ WAN 設定の構成

詳細設定では、セカンダリ WAN 接続を設定する必要があります。

手順

ステップ 1 セカンダリ WAN タイプを選択します。ルータがサポートする WAN のタイプに応じて、シリアル、3G/4G、イーサネット、またはブロードバンド（xDSL）をセカンダリ WAN として設定できます。

ステップ 2 ドロップダウン リストからインターフェイスを選択します。

ステップ 3 サービス プロバイダーから DNS サーバ情報を直接取得するには、[Get DNS Server info directly from ISP] チェックボックスをオンにします。プライマリ DNS とセカンダリ DNS は手動で入力することもできます。

ステップ 4 [Get IP automatically from ISP] チェックボックスをオンにして、サービスプロバイダーから IP アドレス情報を直接取得します。IP アドレスおよびサブネット マスクを入力します。

ステップ 5 [Enable NAT] チェックボックスをオンにして、NAT を有効にします。NAT を有効にすることをお勧めします。

ステップ 6 [Enable PPPoE] チェックボックスをオンにして、PPPoE を有効にします。PPPoE を有効にする場合は、必要な認証モードを選択します。オプションは **PAP** と **CHAP** です。

ステップ 7 サービス プロバイダーから提供されたユーザー名とパスワードを入力します。

ステップ 8 [**Security/APP Visibility WAN Settings**] をクリックします。

セキュリティ設定の構成

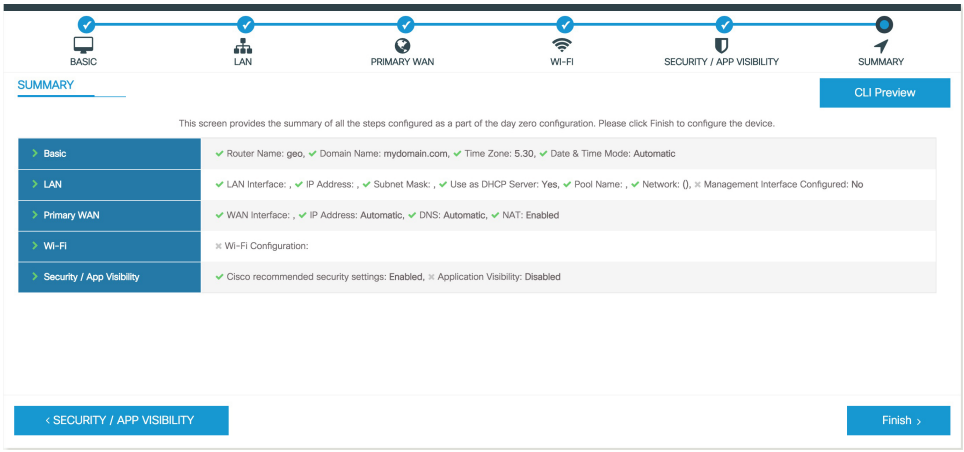
手順

ステップ 1 すべてのパスワードがプレーンテキストで表示されないようにするには、[**Enable Recommended Settings**)] チェックボックスをオンにします。パスワードは暗号化されます。

ステップ 2 [**Day 0 Config Summary**] をクリックします。

ステップ 3 設定をプレビューするには、[CLI preview] をクリックします。

ステップ 4 [Finish] をクリックして、デイゼロセットアップを完了します。



Web ユーザーインターフェイスを使用した Day One 設定

Web ユーザ インターフェイスの設定：

手順

ステップ 1 HTTP サーバを設定します。デフォルトでは、HTTP サーバの設定がデバイス上に存在する必要があります。**ip http server** コマンドと **ip http secure-server** コマンドが実行コンフィギュレーションに存在するかをチェックして、設定を確認します。

```
Device #configure terminal
Device (config)#ip http server
Device (config)#ip http secure-server
```

ステップ 2 Web UI にログインするための認証オプションを設定します。次のいずれかの認証方式を使用できます。

a) ローカルデータベースを使用して認証できます。Web UI 認証にローカル データベースを使用するには、**ip http authentication local** コマンドが実行コンフィギュレーションに含まれていることを確認します。このコマンドは、デバイスで事前に設定されています。コマンドが存在しない場合は、次の例に示すようにデバイスを設定します。

```
Device #configure terminal
Device (config)#ip http authentication local
```

（注）
Web UI の設定画面にアクセスするには、権限 15 を持つユーザが必要です。権限が 15 未満の場合は、Web UI でダッシュボードとモニタリング画面にのみアクセスできます。

ユーザアカウントを作成するには、**username** <username> **privilege** <privilege> **password 0** <passwordtext> を使用します。

```
Device #configure terminal
Device (config)# username <username> privilege <privilege> password 0 <passwordtext>
```

b) AAA オプションを使用して認証します。Web UI に AAA 認証を使用するには、デバイスで「ip http authentication aaa」を設定していることを確認します。また、必要な AAA サーバ設定がデバイスに存在することを確認します。

```
Device #configure terminal
Device (config)#ip http authentication local
```

ステップ 3 ブラウザを起動します。アドレス バーに、デバイスの IP アドレスを入力します。セキュアな接続の場合は、「https://ip-address」と入力します。

ステップ 4 デバイスに指定されたデフォルト ユーザ名（cisco）とパスワードを入力します。

ステップ 5 [Log In] をクリックします。

WebUIを使用したデバイスのプラグアンドプレイ（PnP）導入準備の監視とトラブルシューティング

表 *6:* 機能の履歴

機能名	リリース情報	説明
WebUI を使用したデバイスの PnP 導入準備の監視とトラブルシューティング	Cisco IOS XE 17.15.3	PnP 導入準備で WebUI を使用して、デイゼロデバイスの導入準備を監視およびトラブルシューティングできるようになりました。自動 PnP 導入準備が失敗した場合は、デバイスの導入準備を手動で実行できます。

ゼロタッチプロビジョニング（ZTP）またはプラグアンドプレイ（PnP）プロセスを使用して、Cisco vManage に対するデバイスの導入準備を自動的に実行できます。このセクションでは、PnP メソッドを使用してデバイスの導入準備をモニタおよびトラブルシューティングする手順について説明します。WebUI のこの機能を使用すると、PnP 導入準備プロセスをモニタおよびトラブルシューティングしたり、そのリアルタイムステータスを確認したりすることもできます。この導入準備が停止または失敗した場合は、プロセスを終了し、デバイスの導入準備を手動で行うことができます。

前提条件

- WebUI を実行しているデバイス（Web ブラウザを実行できるコンピュータ）と導入準備しているデバイスは、デバイスの L2 スイッチポート（NIM）経由で接続する必要があります。
- デバイスの DHCP クライアント ID を文字列「webui」に設定する必要があります。
- デバイスが WebUI での Cisco SD-WAN デイゼロデバイスの導入準備をサポートしている必要があります。

デバイスの PnP 導入準備のトラブルシューティング

コントローラモードでの PnP によるデバイスの導入準備をトラブルシューティングするには、次の手順を実行します。

1. WebUI でコントローラモードを開始します。
   - 自律モードからコントローラモードへの切り替え：

     通常、デバイスを初めて起動したときは、自律モードになります。URL https://192.168.1.1/webui/ に移動し、デフォルトのログイン情報（webui/cisco）を使用してログインします。デバイスが WebUI での Cisco SD-WAN デイゼロデバイスの導

入準備をサポートしている場合は、[Controller Mode] を選択してコントローラモードに切り替えることができます。続行するかどうかを確認するダイアログボックスが表示されます。**[はい（Yes）]**をクリックします。デバイスがリロードされ、コントローラモードに切り替えられます。

- コントローラモードでのデバイスの起動：

  デバイスがすでにコントローラモードになっている場合は、モードを変更する必要はありません。https://192.168.1.1 または https://192.168.1.1/webui に移動します。デバイスが WebUI での Cisco SD-WAN デイゼロデバイスの導入準備をサポートしている場合、URL は https://192.168.1.1/ciscosdwan/ にリダイレクトされ、Cisco IOS XE SD-WAN デバイスのデフォルトのログイン情報（admin/admin）を使用してログインできます。

（注） PnP 導入準備の時点でデバイスにスタートアップ コンフィギュレーションがない場合、WebUI はサポートされるデバイスにおいてデフォルトで有効になります。

2. [Welcome to Cisco SDWAN Onboarding Wizard] ページで、[Reset Default Password] をクリックします。

（注） デイゼロデバイスのデフォルトパスワードが脆弱です。したがって、安全なログインのため、WebUI でデバイスに初めてログインするときにパスワードをリセットする必要があります。デバイスが正常に導入準備されると、WebUI 設定は自動的に削除されます。Cisco vManage 上のデバイスのテンプレート設定に WebUI 設定があるまれなケースでは、デバイスの導入準備が成功した後でも削除されません。

3. デバイスのハードウェアとソフトウェアの詳細情報ページにリダイレクトされます。パスワードを入力して [Submit] をクリックします。

4. 次のページには、導入準備の進行状況が表示され、PnP Connect ポータルおよび Cisco SD-WAN コントローラのさまざまなコンポーネントのステータスが一覧表示されます。PnP IPv4 コンポーネントに障害が発生した場合、この障害は、デバイスの PnP 導入準備が失敗したことを示しています。

   導入準備プロセスのログを表示およびダウンロードするには、[SDWAN Onboarding Progress] バーの右側にある情報アイコンをクリックします。

5. 自動 PnP 導入準備が失敗した場合は、[Terminate Automated Onboarding] をクリックします。この操作により、デバイスを手動で導入準備できるようになります。

6. ダイアログボックスが表示されます。終了を続行するには、[Yes] をクリックします。終了の完了までに数分かかる場合があります。

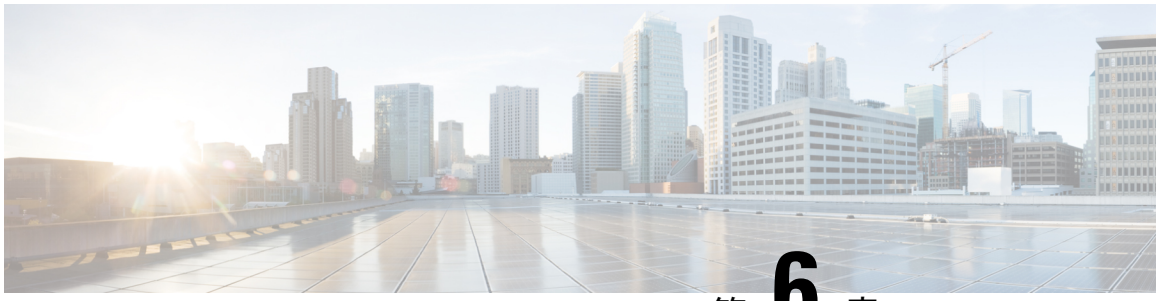
7. [Bootstrap Configuration] ページで、[Select File] をクリックし、デバイスのブートストラップファイルを選択します。このファイルは、一般的なブートストラップファイル（共通

プラットフォーム固有のファイル）と、Cisco SD-WAN Manager からダウンロード可能なフル設定ブートストラップファイルのいずれかです。このファイルには、vBond番号、UUID、WAN インターフェイス、ルート CA、設定などの詳細情報が含まれている必要があります。

8. [Upload] をクリックします。

9. ファイルが正常にアップロードされたら、[Submit] をクリックします。

10. [SDWAN Onboarding Progress] ページに、Cisco SD-WAN コントローラのステータスが再度表示されます。[Controller Connection History] テーブルを開くには、[SDWAN Control Connections] バーの右側にある情報アイコンをクリックします。このテーブルでは、導入準備対象デバイスの状態を確認できます。導入準備が完了すると、デバイスの状態が [connect] に変わります。



第 6 章

コンソールポート、Telnet、および SSH の処理、およびリセットボタン

この章の内容は、次のとおりです。

コンソールポート、Telnet、および SSH に関する注意事項と制約事項

- トランスポートマップがイーサネット管理インターフェイスに適用されるとき、トランスポート マップでの Telnet および Secure Shell（SSH）設定は、他のすべての Telnet および SSH 設定をオーバーライドします。
- イーサネット管理インターフェイスを開始するユーザの認証には、ローカルユーザ名とパスワードだけを使用できます。持続性 Telnet または持続性 SSH を使用してイーサネット管理インターフェイス経由でデバイスにアクセスするユーザーは、AAA 認証を使用できません。
- アクティブな Telnet または SSH セッションがあるイーサネット管理インターフェイスにトランスポート マップを適用すると、アクティブ セッションが切断される可能性があります。しかし、インターフェイスからトランスポートマップを削除すると、アクティブな Telnet セッションまたは SSH セッションの接続は切断されません。
- 診断バナーおよび待機バナーの設定は任意ですが、設定することを推奨します。バナーは、特に Telnet または SSH 試行ステータスをユーザに示すインジケータとして役立ちます。

コンソール ポート

デバイス上のコンソールポートは、EIA/TIA-232 非同期、フロー制御なしのシリアル接続で、RJ-45 コネクタを使用します。コンソールポートは、デバイスへのアクセスに使用され、ルートプロセッサの前面パネルに位置しています。

コンソールポートを使用したデバイスへのアクセスについては、Cisco IOS XE ソフトウェアの使用 （39 ページ）を参照してください。

コンソールポートの処理

コンソール ポートを使用してルータにアクセスする場合は、自動的に Cisco IOS Command-Line Interface （CLI）へ誘導されます。

コンソールポートを介したルータへのアクセス試行で、CLI に接続する前にブレーク信号を送った場合（**Ctrl-C** または **Ctrl-Shift-6** を押すか、Telnet プロンプトで **send break** コマンドを入力）、非 RPIOS サブパッケージにアクセス可能であれば、診断モードに誘導されます。これらの設定を変更するには、コンソール ポートに設定したトランスポート マップをコンソール インターフェイスに適用します。

コンソールポートのトランスポートマップの設定

このタスクでは、デバイス上のコンソール ポート インターフェイスにトランスポートマップを設定する方法について説明します。

手順

ステップ 1 **enable**

例：

```
Router> enable
```

特権 EXEC モードを有効にします。

パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Router# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **transport-map type console** *transport-map-name*

例：

```
Router(config)# transport-map type console consolehandler
```

コンソール接続を処理するためのトランスポート マップを作成して名前を付け、トランスポート マップ コンフィギュレーション モードを開始します。

ステップ 4 **connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]]

例：

```
Router(config-tmap)# connection wait none
```

コンソール接続を処理する方法を、このトランスポート マップで指定します。

- **allow interruptible**：コンソール接続は Cisco IOS VTY 回線が使用可能になるのを待機します。また、ユーザは Cisco IOS VTY 回線が使用可能になるのを待機しているコンソール接続に割り込むことにより、診断モードを開始できます。これがデフォルト設定です。

  （注）
  Ctrl+C キーまたは **Ctrl+Shift+6** キーを入力すると、ユーザは待機中の接続に割り込むことができます。

- **none**：コンソール接続はただちに診断モードを開始します。

ステップ 5 （任意） **banner** [**diagnostic** | **wait**] *banner-message*

例：

```
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)#
```

（オプション）診断モードを開始しているユーザ、またはコンソール トランスポート マップ設定のために Cisco IOS VTY 回線を待機しているユーザに表示されるバナー メッセージを作成します。

- **diagnostic**：コンソール トランスポート マップ設定のために診断モードに誘導されたユーザに表示されるバナー メッセージを作成します。

  （注）
  Ctrl+C キーまたは **Ctrl+Shift+6** キーを入力すると、ユーザは待機中の接続に割り込むことができます。

- **wait**：Cisco IOS VTY が使用可能になるのを待機しているユーザに表示されるバナー メッセージを作成します。

- *banner-message*：同じデリミタで開始および終了するバナー メッセージ。

ステップ 6 **exit**

例：

```
Router(config-tmap)# exit
```

トランスポート マップ コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを再開します。

ステップ 7 **transport type console** *console-line-number* **input** *transport-map-name*

例：

```
Router(config)# transport type console 0 input consolehandler
```

トランスポート マップで定義された設定をコンソール インターフェイスに適用します。

このコマンドの *transport-map-name* は、**transport-map type console** コマンドで定義された *transport-map-name* と一致する必要があります。

例

次に、コンソール ポートのアクセス ポリシーを設定し、コンソール ポート 0 に接続するためにトランスポート マップを作成する例を示します。

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS vty line
X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```

コンソールポートおよび SSH の処理設定の表示

コンソールポート、SSH、および Telnet の処理設定を表示するには、次のコマンドを使用します。

- **show transport-map**
- **show platform software configuration access policy**

トランスポート マップ設定を表示するには、**show transport-map** コマンドを使用します。

show transport-map [**all** | **name** *transport-map-name* | **type** [**console** [**ssh**]]

このコマンドは、ユーザ EXEC モードまたは特権 EXEC モードで使用可能です。

例

次に、デバイスで設定されたトランスポートマップの例（コンソールポート（consolehandler）、持続性 SSH（sshhandler）、持続性 Telnet トランスポート（telnethandler））を示します。

```
Router# show transport-map all
Transport Map:
Name: consolehandler
Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for the IOS CLI

bshell banner:

Welcome to Diagnostic Mode


Transport Map:
Name: sshhandler
Type: Persistent SSH Transport

Interface:
GigabitEthernet0/0/0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS prompt

Bshell banner:
Welcome to Diagnostic Mode



Router# show transport-map type console
Transport Map:
Name: consolehandler
Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for the IOS CLI

Bshell banner:

Welcome to Diagnostic Mode


Router# show transport-map type persistent ssh
Transport Map:
Name: sshhandler
Type: Persistent SSH Transport

Interface:
GigabitEthernet0
```

```
Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS prompt

Bshell banner:

Welcome to Diagnostic Mode


SSH:
Timeout: 120
Authentication retries: 5
RSA keypair: sshkeys



Router# show transport-map name consolehandler
Transport Map:
Name: consolehandler
Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for the IOS CLI

Bshell banner:

Welcome to Diagnostic Mode
```

着信コンソール ポート、SSH、および Telnet 接続の処理に関する現行設定を表示するには、**show platform software configuration access policy** コマンドを使用します。このコマンドの出力には、各接続タイプ（Telnet、SSH、およびコンソール）の現在の待機ポリシーと、現在設定されているバナーの情報が示されます。

show transport-map コマンドとは異なり、**show platform software configuration access policy** コマンドは診断モードで使用可能です。このため、トランスポートマップ設定情報が必要であるにもかかわらず Cisco IOS CLI にアクセスできない場合に、このコマンドを入力できます。

例

```
Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait
Shell banner:
Wait banner :

Method : ssh
Rule : wait
Shell banner:
Wait banner :

Method : console
```

```
Rule : wait with interrupt
Shell banner:
Wait banner :
```

例

この例では、SSH 用の新しいトランスポートマップが設定される前と後の両方で発行される **show platform software configuration access policy** コマンドを示します。設定時に、持続性 SSH トランスポート マップの接続ポリシーとバナーが設定され、SSH のトランスポート マップがイネーブル化されます。

```
Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS Process


Method : ssh
Rule : wait
Shell banner:
Wait banner :

Method : console
Rule : wait with interrupt
Shell banner:
Wait banner :

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
Welcome to Diag Mode
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS
X
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# transport interface gigabitethernet 1
Router(config-tmap)# exit
Router(config)# transport type persistent ssh input sshhandler
Router(config)# exit

Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS process
```

```
Method : ssh
Rule : wait with interrupt
Shell banner:
Welcome to Diag Mode

Wait banner :
Waiting for IOS


Method : console
Rule : wait with interrupt
Shell banner:
Wait banner :
```

リセットボタンの概要

リセットボタン機能は、すべての Cisco 8300 シリーズ セキュアルータにデフォルトで設定されています。リセットボタンを使用すると、設定不備が原因で応答しなくなったり、ユーザーがログイン情報を間違ってログインできなくなったりしたときに、Cisco 8300 シリーズ セキュアルータを回復できます。

リセットボタン機能について

デフォルトでは、リセットボタンの機能は有効になっています。この機能を無効にするには、**no service password-recovery strict** コマンドを使用します。

デバイスが初期化されているときに、前面パネルのリセットボタンを押すと、この機能をトリガーできます。

次の表では、サービスパスワード回復ありとサービスパスワード回復なしの条件で、さまざまな組み合わせでのリセットボタン機能の動作を示します。

表 7: Service password-recovery

リセットボタンを押す（ステータス）				動作			
番No	**ゴールデンイメージ**	**ゴールデン構成**	**スタートアップ構成**	**イメージ**	**Config**	**追加情報**	
1	あり	あり	あり	ゴールデン	ゴールデン	-	
2	あり	あり	なし	ゴールデン	ゴールデン	-	

3	あり	なし	あり	ゴールデン	PnP	スタートアップの削除
4	あり	なし	なし	ゴールデン	PnP	-
5	なし	あり	あり	標準	ゴールデン	-
6	なし	あり	なし	標準	ゴールデン	-
7	なし	なし	あり	標準	PnP	スタートアップの削除
8	なし	なし	なし	標準	PnP	-

表 *8 : No service password-recovery*

リセットボタンを押す（ステータス）				動作		
番No	**ゴールデンイメージ**	**ゴールデン構成**	**スタートアップ構成**	**イメージ**	**Config**	**追加情報**
1	あり	NVRAM内	あり	ゴールデン	PnP	消去
2	あり	ブートフラッシュ内	あり	ゴールデン	ゴールデン	消去
3	あり	NVRAM内	なし	ゴールデン	PnP	消去
4	あり	ブートフラッシュ内	なし	ゴールデン	ゴールデン	消去
5	あり	なし	あり	ゴールデン	PnP	消去
6	あり	なし	なし	ゴールデン	PnP	消去
7	なし	NVRAM内	あり	標準	PnP	消去

8	なし	ブートフラッシュ内	あり	標準	ゴールデン	消去
9	なし	NVRAM内	なし	標準	PnP	消去
10	なし	ブートフラッシュ内	なし	標準	ゴールデン	消去
11	なし	なし	あり	標準	PnP	消去
12	なし	なし	なし	標準	PnP	消去

リセットボタン機能を有効にするための前提条件

- デバイスの ROMmon バージョンが 17.18（1.5r）以上であることを確認します。
- golden.bin イメージと golden.cfg を必ず設定してください。

コントローラモードのリセットボタンに関する制約事項

- リセットボタンを使用すると、すべての SD-WAN 設定を消去したり、Cisco 8300 シリーズセキュアルータのデフォルト設定として使用可能な ciscosdwan.cfg 設定を適用したりできます。リセットボタンは、最初に golden.bin イメージを起動しようとします（使用可能な場合）。golden.bin イメージが使用できない場合、次にデフォルトのブートアップ設定を試行します。リセット機能では、golden.bin イメージは必須ではありません。
- デバイスが起動を開始している場合は、リセットボタンを押す必要があります。システムが ROMMON モードまたは IOS モードに設定されている場合、リセット機能は動作しません。

リセットボタン機能を有効にする方法

ここでは、Cisco 8100 シリーズセキュアルータでリセットボタン機能を有効にする方法について説明します。

手順の概要

1. **configure terminal**
2. **service password-recovery**
3. **no service password-recovery**
4. **exit**
5. **no service recovery-service strict**

手順の詳細

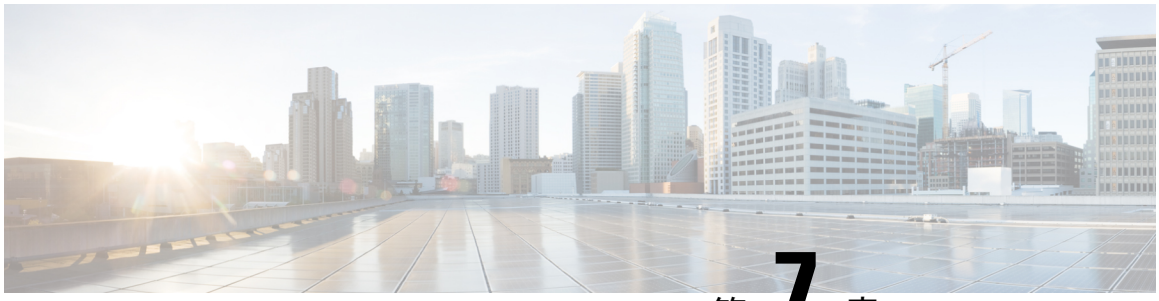
手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service password-recovery** 例： `Device(config)# service password-recovery`	デバイスでパスワード回復サービスを設定します。
ステップ 3	**no service password-recovery** 例： `Device(config)# no service password-recovery`	応答しないデバイスを回復できます。ただし、すべてのユーザー設定とキーが削除されるため、デバイスは再設定されます。 （注） IOS NVRAM の startup-config ファイルが削除されないように、リカバリメカニズムとしてデバイスに golden.bin と golden.cfg の設定があることを確認します。
ステップ 4	**exit** 例： `Device(config)# exit`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**no service recovery-service strict** 例： `Device(config)# no service recovery-service strict`**exit**	デバイスでリセットボタン機能を無効にします。 （注） Cisco IOS XE 17.18.x リリース以降では、デバイスに golden.bin や golden.cfg の設定があっても、**no service recovery-service strict** コマンドを使用するとデバイスを回復できないため、シスコへの返品許可（RMA）を通じた返品や交換が必要になります。

リセットボタン機能の有効化と無効化

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Device(config)# service password-recovery
Executing this command enables the password recovery mechanism.
Device(config)#
```

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# no service password-recovery strict

WARNING:
Executing this command will disable the password recovery mechanism.
Do not execute this command without another plan for password recovery.

Are you sure you want to continue? [yes]: yes
Device(config)#
```



第 7 章

ソフトウェアのインストール

この章の内容は、次のとおりです。

ソフトウェアのインストール

ルータにソフトウェアをインストールする際には、統合パッケージ（ブート可能イメージ）をインストールします。これはサブパッケージ（モジュール型ソフトウェアユニット）のバンドルで構成されており、各サブパッケージはそれぞれ異なる機能セットを制御します。

統合パッケージを使用して実行されるデバイスの管理と設定 （89 ページ）：この方法では、サブパッケージを個別にアップグレードでき、次に説明する方法と比較して、通常はブート時間が短くなります。モジュールのソフトウェアを個別にアップグレードする場合は、この方法を使用します。

サービスの中断が可能な、予定されている保守期間内にソフトウェアのアップグレードを実行することをお勧めします。ソフトウェアアップグレードを有効にするには、ルータをリブートする必要があります。

ROMMON イメージ

ROMMONイメージは、ルータのROMモニタ（ROMMON）ソフトウェアで使用されるソフトウェア パッケージです。このソフトウェア パッケージは、ルータの起動に通常使用される統

合パッケージとは別のものです。ROMMON の詳細については、『Hardware Installation Guide for the Cisco 8300 Series Secure Routers』を参照してください。

独立したROMMONイメージ（ソフトウェアパッケージ）がリリースされることがあります。新しいROMMONソフトウェアを使ってルータをアップグレードできます。詳細な手順については、ROMMONイメージに付属のマニュアルを参照してください。

（注） ROMMONイメージの新しいバージョンは、常にルータの統合パッケージと同時にリリースされるとは限りません。

ファイルシステム

次の表に、Cisco 8300 シリーズセキュアルータで表示可能なファイルシステムのリストを示します。

表 *9:* デバイスのファイルシステム

ファイルシステム	説明
bootflash:	ブートフラッシュ メモリのファイル システム。
flash:	上記のブートフラッシュ メモリのファイル システムのエイリアス。
harddisk:	ハードディスク ファイル システム（CLI コマンドハードディスクを使用した NVME-M2-600G または USB-M2-16G または USB-M2-32G）。
cns:	Cisco Networking Service のファイル ディレクトリ。
nvram:	デバイスの NVRAM。NVRAM 間で startup-config をコピーできます。
obfl:	オンボード障害ロギング（OBFL）ファイル用のファイル システム。
system:	実行コンフィギュレーションを含む、システム メモリ用のファイル システム。
tar:	アーカイブ ファイル システム。
tmpsys:	一時システム ファイルのファイル システム。
USB タイプ C	Universal Serial Bus（USB）フラッシュ ドライブのファイル システム。 （注） USB フラッシュ ドライブのファイル システムは、USB ドライブが usb0: または usb1: ポートに装着されている場合にのみ表示されます。

? ヘルプ オプションを使用するか、またはコマンド リファレンス ガイドの **copy** コマンドを使用します。

自動生成されるファイルディレクトリおよびファイル

ここでは、作成可能な自動生成ファイルとディレクトリについて、およびこれらのディレクトリ内のファイルを管理する方法について説明します。

表 *10 :* 自動生成されるファイル

ファイルまたはディレクトリ	説明
crashinfo ファイル	crashinfo ファイルが bootflash: ファイルシステムに保存されることがあります。 これらのファイルにはクラッシュに関する説明情報が含まれており、調整やトラブルシューティングに役立ちます。ただし、これらのファイルはデバイスの動作には使用されないため、消去してもデバイスの機能には影響がありません。
core ディレクトリ	.core ファイルのストレージ領域 このディレクトリは消去されると、ブートアップ時に自動的に再生成されます。このディレクトリ内の .core ファイルは、デバイス機能に影響を及ぼさずに消去することができますが、ディレクトリ自体は消去しないでください。
lost+found ディレクトリ	システムチェックが実行されると、ブートアップ時にこのディレクトリが作成されます。このディレクトリが表示されることは完全に正常な状態であり、デバイスに問題が発生したわけではありません。
tracelogs ディレクトリ	trace ファイルのストレージ領域 trace ファイルはトラブルシューティングに役立ちます。たとえば Cisco IOS プロセスに障害が発生した場合、ユーザやトラブルシューティング担当者は診断モードを使って trace ファイルにアクセスし、Cisco IOS 障害に関連する情報を収集できます。 ただし、trace ファイルはデバイスの動作には使用されないため、消去してもデバイスのパフォーマンスには影響がありません。

自動生成されるディレクトリに関する重要事項

自動生成されるディレクトリに関する重要な情報は次のとおりです。

- Cisco カスタマー サポートからの指示がない限り、bootflash: ディレクトリに自動生成されたファイルの削除、名前変更、移動、またはその他の変更を行わないでください。

（注） bootflash: に自動生成されたファイルを変更すると、システム パフォーマンスに予期せぬ結果をもたらす場合があります。

- crashinfo ファイル、core ファイル、trace ファイルは削除できます。

フラッシュストレージ

サブパッケージは、フラッシュなどのローカル メディア ストレージにインストールされます。フラッシュ ストレージの場合は **dir bootflash:** コマンドを使用するとファイル名がリストされます。

（注） デバイスが正常に動作するためにはフラッシュストレージが必要です。

自動ブートのコンフィギュレーション レジスタの設定

コンフィギュレーション レジスタを使用して、動作を変更できます。これには、デバイスの起動方法の制御が含まれます。次のいずれかのコマンドを使用して、ROM で起動するようにコンフィギュレーション レジスタを 0x0 に設定します。

- Cisco IOS コンフィギュレーション モードで **config-reg** 0x0 コマンドを使用します。
- ROMMON プロンプトで **confreg** 0x0 コマンドを使用します。

コンフィギュレーション レジスタの詳細については、『Use of the Configuration Register on All Cisco Routers』を参照してください。

（注） コンフィギュレーション レジスタを 0x2102 に設定すると、Cisco IOS XE ソフトウェアを自動ブートするようにデバイスが設定されます。

（注） **confreg** を 0x2102 または 0x0 に変更した後、コンソールのボーレートが 9600 に設定されます。**confreg** を設定した後にコンソールセッションを確立できない場合、または意味のない出力が表示される場合は、端末エミュレーション ソフトウェアで設定を 9600 に変更してください。

ソフトウェアのインストール方法とアップグレード方法

ソフトウェアをインストールまたはアップグレードするには、統合パッケージを使用して実行されるデバイスの管理と設定 （89 ページ） の方法を使用します。「ソフトウェアのインストール」の項も参照してください。

統合パッケージを使用して実行されるデバイスの管理と設定

次の操作でデバイスを管理し、設定できます。

copy および boot コマンドを使用した統合パッケージの管理と設定

統合パッケージをアップグレードするには、**copy** コマンドを使用してルータの **bootflash:** ディレクトリに統合パッケージをコピーします。こうして統合パッケージのコピーを作成した後、統合パッケージ ファイルを使ってブートするようルータを設定します。

この例は、TFTP を使用して **bootflash:** ファイルシステムに統合パッケージファイルをコピーする方法を示しています。さらに、**boot system** コマンドを使用して起動するようにコンフィギュレーション レジスタを設定し、**boot system** コマンドにより、**bootflash:** ファイルシステムに保存されている統合パッケージを使用して起動するようルータに指示します。その後、新しい設定は **copy running-config startup-config** コマンドにより保存され、システムがリロードされてプロセスが終了します。

```
Router# dir bootflash:
Directory of bootflash:/
23      -rw-                0   Jun 5 2025 09:50:37 +00:00  iox_alt_hdd.dsk

784897  drwx          3358720   Jun 5 2025 09:23:28 +00:00  tracelogs

392449  drwx             4096  May 21 2025 09:22:30 +00:00  .rollback_timer

11      -rw-              422  May 21 2025 09:12:33 +00:00  .iox_dir_list

915713  drwx             4096  May 21 2025 09:12:13 +00:00  SHARED-IOX

21      -rw-               30  May 21 2025 09:12:12 +00:00  throughput_monitor_params

15      -rw-           143041  May 21 2025 09:12:04 +00:00  memleak.tcl

1046531  drwx            73728  May 21 2025 09:12:00 +00:00  license_evlog

1046529  drwx             4096  May 21 2025 09:11:53 +00:00  .prst_sync

12      -rwx           261921  May 21 2025 09:11:47 +00:00  mode_event_log

59      -rw-             7762  May 21 2025 09:09:09 +00:00  packages.conf

48      -rw-             7762  May 21 2025 09:04:42 +00:00
```

```
c8kg2be-universalk9.17.15.03a.SPA.conf
1047801  -rw-         59995452  May 21 2025 09:04:39 +00:00
c8kg2be-rpboot.17.15.03a.SPA.pkg
1046537  drwx             4096  May 21 2025 09:04:38 +00:00  .images

130817  drwx             4096  May 21 2025 09:01:56 +00:00  sysboot

47      -rw-             9391  May 21 2025 08:59:39 +00:00
c8kg2be-universalk9.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.conf
1047773  -rw-         59995512  May 21 2025 08:59:38 +00:00
c8kg2be-rpboot.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg
785553  drwx             4096  May 21 2025 06:27:34 +00:00  memaudit_log
13      drwx             4096  May 19 2025 03:58:14 +00:00  core
46      -rw-       1003589796  May 14 2025 11:21:03 +00:00
c8kg2be-universalk9.BLD_V1718_THROTTLE_LATEST_20250423_010128.SSA.bin
45      -rw-              396  May 14 2025 05:39:34 +00:00  ct_persistent.txt
44      -rw-             7711   May 6 2025 08:36:06 +00:00
c8kg2be-universalk9.17.15.03.SPA.conf
1047740  -rw-         59987868   May 6 2025 08:36:03 +00:00
c8kg2be-rpboot.17.15.03.SPA.pkg
24      -rw-        953199576   May 6 2025 07:02:50 +00:00
c8kg2be-universalk9.17.15.03.SPA.bin
43      -rw-            16464   May 6 2025 05:38:49 +00:00  dizeng-crestone-confg

39      -rw-        957518956   May 5 2025 12:04:02 +00:00
c8kg2be-universalk9_npe.17.15.03a.SPA.bin
38      -rw-        953231736   May 4 2025 08:39:53 +00:00
c8kg2be-universalk9.17.15.03a.SPA.bin
1047812  -rw-        891244544   May 2 2025 19:08:25 +00:00
c8kg2be-mono-universalk9.17.15.03a.SPA.pkg
1047807  -rw-          5677056   May 2 2025 19:07:15 +00:00
c8kg2be-firmware_nim_xdsl.17.15.03a.SPA.pkg
1047809  -rw-         13889536   May 2 2025 19:07:15 +00:00
c8kg2be-firmware_sm_1t3e3.17.15.03a.SPA.pkg
1047808  -rw-         10444800   May 2 2025 19:07:15 +00:00
c8kg2be-firmware_prince.17.15.03a.SPA.pkg
1047810  -rw-         14671872   May 2 2025 19:07:15 +00:00
c8kg2be-firmware_sm_async.17.15.03a.SPA.pkg
1047804  -rw-         11956224   May 2 2025 19:07:14 +00:00
c8kg2be-firmware_ngwic_t1e1.17.15.03a.SPA.pkg
1047806  -rw-         11804672   May 2 2025 19:07:14 +00:00
c8kg2be-firmware_nim_shdsl.17.15.03a.SPA.pkg
1047805  -rw-         13254656   May 2 2025 19:07:14 +00:00
c8kg2be-firmware_nim_async.17.15.03a.SPA.pkg
1047811  -rw-           204800   May 2 2025 19:07:14 +00:00
c8kg2be-firmware_sm_nim_adpt.17.15.03a.SPA.pkg
29      -rw-        953227220  Apr 22 2025 12:40:25 +00:00
c8kg2be-universalk9.BLD_V1715_3_THROTTLE_LATEST_20250421_200058.SSA.bin
28      -rw-          5813308  Apr 22 2025 12:03:54 +00:00
SDK112312-Prod-SoC2-v17.15.3_1r-cp.pkg
26      -rw-           763701  Apr 17 2025 08:58:31 +00:00  wilson-running-cfg.txt

25      -rw-          8630272  Apr 11 2025 11:28:20 +00:00
c8kg2be-hw-programmables.C0x25033132_W0x25033132.pkg
14      -rw-         56012800   Apr 3 2025 08:56:15 +00:00
secapp-utd.17.15.03.1.0.8_SV3.1.81.0_XE17.15.aarch64.tar
75      -rw-       1002810808   Apr 1 2025 07:21:54 +00:00
c8kg2be-universalk9.BLD_POLARIS_DEV_LATEST_20250325_181737.SSA.bin
1047751  -rw-        891219968  Mar 26 2025 06:51:11 +00:00
c8kg2be-mono-universalk9.17.15.03.SPA.pkg
1047747  -rw-         10444800  Mar 26 2025 06:50:09 +00:00
c8kg2be-firmware_prince.17.15.03.SPA.pkg
1047745  -rw-         11804672  Mar 26 2025 06:50:09 +00:00
c8kg2be-firmware_nim_shdsl.17.15.03.SPA.pkg
```

```
1047750  -rw-           204800  Mar 26 2025 06:50:09 +00:00
c8kg2be-firmware_sm_nim_adpt.17.15.03.SPA.pkg
1047744  -rw-         13254656  Mar 26 2025 06:50:09 +00:00
c8kg2be-firmware_nim_async.17.15.03.SPA.pkg
1047743  -rw-         11956224  Mar 26 2025 06:50:09 +00:00
c8kg2be-firmware_ngwic_t1e1.17.15.03.SPA.pkg
1047748  -rw-         13889536  Mar 26 2025 06:50:09 +00:00
c8kg2be-firmware_sm_1t3e3.17.15.03.SPA.pkg
1047746  -rw-          5677056  Mar 26 2025 06:50:09 +00:00
c8kg2be-firmware_nim_xdsl.17.15.03.SPA.pkg
1047749  -rw-         14671872  Mar 26 2025 06:50:08 +00:00
c8kg2be-firmware_sm_async.17.15.03.SPA.pkg
74       -rw-          2510307  Mar 19 2025 07:08:14 +00:00  redirect.out

72       -rw-        953199060  Mar 12 2025 07:00:51 +00:00
c8kg2be-universalk9.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.bin


1047784  -rw-        891203584  Mar 10 2025 20:59:47 +00:00
c8kg2be-mono-universalk9.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg


1047781  -rw-         13889536  Mar 10 2025 20:58:37 +00:00
c8kg2be-firmware_sm_1t3e3.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg


1047779  -rw-          5677056  Mar 10 2025 20:58:37 +00:00
c8kg2be-firmware_nim_xdsl.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg


1047780  -rw-         10444800  Mar 10 2025 20:58:37 +00:00
c8kg2be-firmware_prince.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg


1047782  -rw-         14671872  Mar 10 2025 20:58:36 +00:00
c8kg2be-firmware_sm_async.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg


1047778  -rw-         11804672  Mar 10 2025 20:58:36 +00:00
c8kg2be-firmware_nim_shdsl.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg


1047776  -rw-         11956224  Mar 10 2025 20:58:36 +00:00
c8kg2be-firmware_ngwic_t1e1.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg


1047783  -rw-           204800  Mar 10 2025 20:58:36 +00:00
c8kg2be-firmware_sm_nim_adpt.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg
1047777  -rw-         13254656  Mar 10 2025 20:58:36 +00:00
c8kg2be-firmware_nim_async.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg


62       -rw-          5823548  Feb 25 2025 12:53:04 +00:00  C8000-NG-S2-17-15-1_17r.pkg

1046534  drwx             4096   Feb 3 2025 10:28:42 +00:00  pnp-tech

392450   drwx             4096  Jan 28 2025 07:20:24 +00:00  .dbpersist

71       -rw-           261214  Jan 28 2025 07:16:04 +00:00  ajay_backup.cfg

70       -rw-          5821500  Jan 24 2025 02:54:43 +00:00
SDK112312-Prod-SoC2-v17.15.1_14r-cp.pkg
68       -rw-          9754990  Jan 20 2025 05:17:19 +00:00  show-tech1717
```

```
69      -rw-           846347  Jan 20 2025 05:16:14 +00:00
CRFT_Admintech_C8375EG2_2025-01-20_05-16-14.tar.gz
66      -rw-             6928  Jan 13 2025 07:39:59 +00:00  ciscortr.cfg

65      -rw-             6928  Jan 13 2025 07:39:04 +00:00  C8375-E-G2.cfg

64      -rw-           301992   Jan 9 2025 09:08:37 +00:00  dual-public-ip.cfg

63      -rw-       1015740420   Jan 8 2025 07:33:57 +00:00
c8kg2be-universalk9.BLD_POLARIS_DEV_LATEST_20250106_030447.SSA.bin

      60      -rw-          4653056  Dec 25 2024 03:50:16 +00:00
c8k30be-hw-programmables.C0x2408272B.pkg
37      -rw-         969660392  Dec 11 2024 05:40:52 +00:00
c8k30be-universalk9.BLD_POLARIS_DEV_LATEST_20241209_180254_V17_17_0_27.SSA.bin

      32      -rw-         958470964   Dec 5 2024 05:25:07 +00:00
mira_rom_17.15_1.8r.s2.RelDebug.bin
50      -rw-           301239  Nov 22 2024 11:01:52 +00:00  rc_22_11_24

49      -rw-         952760408  Nov 21 2024 03:53:44 +00:00
c8k30be-universalk9.17.15.02.SPA.bin
42      -rw-          5733436   Nov 6 2024 06:19:35 +00:00
SDK112312-Prod-SoC2-v17.15.1_7d_RSA4K.pkg
41      -rw-             9044  Oct 30 2024 09:26:50 +00:00  cessna-snake.cfg

34     -rwx        39490752  Oct 23 2024 20:15:10 +00:00  mirabile_diag.14er.v0.1.6.0826

33      -rw-         14934016  Oct 23 2024 14:42:04 +00:00  mirabile_diag.zb.v1.0.0_qr3

36      drwx             4096  Oct 19 2024 11:42:32 +00:00  .geo

35      -rw-         56002560  Oct 10 2024 06:32:32 +00:00
secapp-utd.BLD_POLARIS_DEV_LATEST_20241007_181057.1.15.2_SV3.1.81.0_XEmain.aarch64.tar


1046539  -rw-         56309176  Aug 13 2024 09:04:49 +00:00
c8k30be-rpboot.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg


20      drwx             4096  Aug 13 2024 09:01:06 +00:00  guest-share

785011  drwx             4096  Aug 13 2024 09:01:04 +00:00  pnp-info

915715  drwx             4096  Aug 13 2024 09:01:04 +00:00  onep

915714  drwx             4096  Aug 13 2024 09:00:58 +00:00  virtual-instance

19      -rw-             1939  Aug 13 2024 09:00:57 +00:00  trustidrootx3_ca_062035.ca

18      -rw-             1826  Aug 13 2024 09:00:57 +00:00  trustidrootx3_ca_092025.ca

1046550  -rw-        885977088  Jul 13 2024 06:13:59 +00:00
c8k30be-mono-universalk9.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg


1046548  -rw-         14675968  Jul 13 2024 06:12:52 +00:00
c8k30be-firmware_sm_async.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg


1046544  -rw-         11804672  Jul 13 2024 06:12:52 +00:00
c8k30be-firmware_nim_shdsl.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg
```

```
1046547  -rw-         13889536  Jul 13 2024 06:12:52 +00:00
c8k30be-firmware_sm_1t3e3.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg


1046549  -rw-           204800  Jul 13 2024 06:12:52 +00:00
c8k30be-firmware_sm_nim_adpt.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg


1046545  -rw-          5677056  Jul 13 2024 06:12:52 +00:00
c8k30be-firmware_nim_xdsl.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg


1046543  -rw-         13258752  Jul 13 2024 06:12:52 +00:00
c8k30be-firmware_nim_async.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg


1046542  -rw-         11956224  Jul 13 2024 06:12:52 +00:00
c8k30be-firmware_ngwic_t1e1.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg


1046546  -rw-         10444800  Jul 13 2024 06:12:52 +00:00
c8k30be-firmware_prince.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg


27       -rw-          5788732  Feb 29 2024 18:42:07 +00:00
SDK112312-Prod-SoC2-v17.15.1_13d-cp.pkg
786101   -rw-         67728148  Feb 27 2024 17:30:28 +00:00
c8kg2be-rpboot.2024-12-12_16.42_sukhoo.SSA.pkg
31       -rw-          5784636  Feb 27 2024 17:30:19 +00:00
SDK112312-Prod-SoC2-v17.15.1_13r-cp.pkg
786100   -rw-        899686400  Feb 27 2024 17:28:58 +00:00
c8kg2be-mono-universalk9.2024-12-12_16.42_sukhoo.SSA.pkg
786095   -rw-         10444800  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_prince.2024-12-12_16.42_sukhoo.SSA.pkg
786096   -rw-            53248  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_pse_si3470a.2024-12-12_16.42_sukhoo.SSA.pkg
786097   -rw-         13889536  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_sm_1t3e3.2024-12-12_16.42_sukhoo.SSA.pkg
786099   -rw-           204800  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_sm_nim_adpt.2024-12-12_16.42_sukhoo.SSA.pkg
786098   -rw-         14675968  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_sm_async.2024-12-12_16.42_sukhoo.SSA.pkg
786091   -rw-         11956224  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_ngwic_t1e1.2024-12-12_16.42_sukhoo.SSA.pkg
786093   -rw-         11804672  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_nim_shdsl.2024-12-12_16.42_sukhoo.SSA.pkg
786094   -rw-          5677056  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_nim_xdsl.2024-12-12_16.42_sukhoo.SSA.pkg
786092   -rw-         13258752  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_nim_async.2024-12-12_16.42_sukhoo.SSA.pkg
57       -rw-             9840  Feb 27 2024 17:28:56 +00:00  prev_packages.conf

40       -rw-           301569  Feb 27 2024 17:28:49 +00:00  original-xe-config

53       -rw-           301569  Feb 27 2024 17:28:31 +00:00  241213.cfg

523273   drwx             4096  Feb 27 2024 17:28:03 +00:00  dbgd

58       -rw-              107  Feb 27 2024 17:27:55 +00:00  pki_certificates

56       -rw-              147  Feb 27 2024 17:27:20 +00:00  utm_pf_filtered_luids.json

523266   drwx             4096  Feb 27 2024 17:26:56 +00:00  vmanage-admin
```

```
523265  drwx            4096  Feb 27 2024 17:26:55 +00:00  admin_tech

130830  drwx            4096  Feb 27 2024 17:26:55 +00:00  .sdwaninternal

130831  drwx            4096  Feb 27 2024 17:26:48 +00:00  sdwan

30      drwx            4096  Feb 27 2024 17:26:04 +00:00  lost+found

                                                            20237881344 bytes total
 (1147678720 bytes free)

Router# copy tftp: bootflash:Address or name of remote host []? 203.0.113.2
Source filename []? /auto/tftp-ngio/test/c8kg2be-universalk9.17.15.03prd1.SPA.bin
Destination filename [c8kg2be-universalk9.17.15.03prd1.SPA.bin]?
Accessing
tftp://203.0.113.2//auto/tftp-ngio/test/c8kg2be-universalk9.17.15.03prd1.SPA.bin...
%Error opening
tftp://203.0.113.2//auto/tftp-ngio/test/c8kg2be-universalk9.17.15.03prd1.SPA.bin (Timed
 out)
C8300-Router#
C8300-Router#copy tftp bootflash
Address or name of remote host [203.0.113.2]? 203.0.113.2
Source filename [/auto/tftp-ngio/test/c8kg2be-universalk9.17.15.03prd1.SPA.bin]?
Destination filename [c8kg2be-universalk9.17.15.03prd1.SPA.bin]?
Accessing
tftp://203.0.113.2//auto/tftp-ngio/test/c8kg2be-universalk9.17.15.03prd1.SPA.bin...
Loading /auto/tftp-ngio/test/c8kg2be-universalk9.17.15.03prd1.SPA.bin from 203.0.113.2
(via GigabitEthernet0/0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!
[OK - 696368193 bytes]

696368193 bytes copied in 478.600 secs (1455011 bytes/sec)

Router# dir bootflash:
Directory of bootflash:/

106497  drwx            4096   Jul 8 2020 11:38:27 -07:00  tracelogs
11      -rw-       696368193   Jul 8 2020 11:34:28 -07:00
c8kg2be-universalk9.17.15.03prd1.SPA.bin
458753  drwx            4096  Jun 24 2020 17:25:47 -07:00  sysboot

7693897728 bytes total (5950341120 bytes free)
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# boot system flash bootflash:c8kg2be-universalk9.17.15.03prd1.SPA.bin
Router(config)# config-reg 0x2102
Router(config)# exit
Router# show run | include boot
boot-start-marker
boot system flash bootflash:c8kg2be-universalk9.17.15.03prd1.SPA.bin
```

```
boot-end-marker
diagnostic bootup level minimal
Router# copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router# reload
```

boot コマンドを使用して TFTP 経由で統合パッケージを起動するようにデバイスを設定：例

```
Router#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#boot system tftp://10.124.19.169/c8kg2be-universalk9.17.15.03a.SPA.bin
Router(config)#end
Router#wr
Building configuration...
[OK]
Router#show bootvar
BOOT variable = tftp://10.124.19.169/c8kg2be-universalk9.17.15.03a.SPA.bin,12;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102

Standby not ready to show bootvar

Router#reload
Proceed with reload? [confirm]

System integrity status: 0x32042000
Rom image verified correctly

System Bootstrap, Version v17.15(3.1r).s2.cp, RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.


Current image running: Boot ROM0

Last reset cause: LocalSoft
C8375-E-G2 platform with 33554432 Kbytes of main memory

........

h/w (environment):
 interface : eth0
 mac       : 48:74:10:4A:EF:1F
n/w (environment):
 ip        : 192.168.22.10
 mask      : 255.255.255.0
 gateway   : 192.168.22.1

h/w:
 interface : eth0 (Ethernet)
 status    : connected
 mac       : 48:74:10:4A:EF:1F
n/w (ip v4):
 ip        : 192.168.22.10
 mask      : 255.255.255.0
 route(s)  : 0.0.0.0 -> 192.168.22.0/255.255.255.0
           : 192.168.22.1 -> 0.0.0.0/0.0.0.0
```

```
tftp v4:
 server    : 10.124.19.169
 file      : c8kg2be-universalk9.17.15.03a.SPA.bin
 blocksize : 1460
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Performing Signature Verification of OS image...
Image validated

Jun  6 06:52:50.787: %SYS-4-ROUTER_RUNNING_BUNDLE_BOOT_MODE: R0/0: Warning: Booting with
 bundle mode will be deprecated in the near future. Migration to install mode is required.
Jun  6 06:53:13.468: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           Cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software [IOSXE], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
 17.15.3a, RELEASE SOFTWARE (fc4)
```

```
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Fri 02-May-25 11:27 by mcpre


This software version supports only Smart Licensing as the software licensing mechanism.


Please read the following carefully before proceeding. By downloading,
installing, and/or using any Cisco software product, application, feature,
license, or license key (collectively, the "Software"), you accept and
agree to the following terms. If you do not agree, do not proceed and do not
use this Software.

This Software and its use are governed by Cisco's General Terms and any
relevant supplemental terms found at
https://www.cisco.com/site/us/en/about/legal/contract-experience/index.html.
If you have a negotiated agreement with Cisco that includes this Software, the
terms of that agreement apply as well. In the event of a conflict, the order
of precedence stated in your negotiated agreement controls.

Cisco Software is licensed on a term and/or subscription-basis. The license to
the Software is valid only for the duration of the specified term, or in the
case of a subscription-based license, only so long as all required subscription
payments are current and fully paid-up. While Cisco may provide you
licensing-related alerts, it is your sole responsibility to monitor your usage.
Using Cisco Software without a valid license is not permitted and may result in
fees charged to your account. Cisco reserves the right to terminate access to,
or restrict the functionality of, any Cisco Software, or any features thereof,
that are being used without a valid license.


Jun  6 06:53:16.982: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: bootflash quota
exceeded [free space is 166800 kB] - [recommended free space is 5929066 kB] - Please
clean up files on bootflash.
cisco C8375-E-G2 (1RU) processor with 11906881K/6147K bytes of memory.
Processor board ID FDO2833M01A
Router operating mode: Autonomous
1 Virtual Ethernet interface
12 2.5 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
33554432K bytes of physical memory.
20257791K bytes of flash memory at bootflash:.

Warning: When Cisco determines that a fault or defect can be traced to
the use of third-party transceivers installed by a customer or reseller,
then, at Cisco's discretion, Cisco may withhold support under warranty or
a Cisco support program. In the course of providing support for a Cisco
networking product Cisco may require that the end user install Cisco
transceivers if Cisco determines that removing third-party parts will
assist Cisco in diagnosing the cause of a support issue.
No processes could be found for the command

 WARNING: Command has been added to the configuration using a type 0 password. However,
 recommended to migrate to strong type-6 encryption

 WARNING: ** NOTICE **  The H.323 protocol is no longer supported from IOS-XE release
17.6.1. Please consider using SIP for multimedia applications.


Press RETURN to get started!
```

インストールコマンドを使用したソフトウェアのインストール

Cisco IOS XE 17.15.3a 以降、Cisco 8300 シリーズ セキュアルータはデフォルトでインストールモードで出荷されます。ユーザーは、一連の **install** コマンドを使用して、プラットフォームを起動し、Cisco IOS XE ソフトウェアバージョンにアップグレードできます。

機能制限

- ISSU はこの機能ではカバーされません。
- インストールモードでは、システムの再起動が必要です。

インストールコマンドを使用したソフトウェアのインストールに関する情報

Cisco IOS XE 17.15.3a リリース以降、インストールモードで出荷されるルータの場合、一連の **install** コマンドを使用して、インストールモードでプラットフォームを起動、アップグレード、およびダウングレードできます。この更新は、Cisco 8300 シリーズ セキュアルータに適用されます。

次の表に、バンドルモードとインストールモードの違いを示します。

表 *11* : バンドルモードとインストールモード

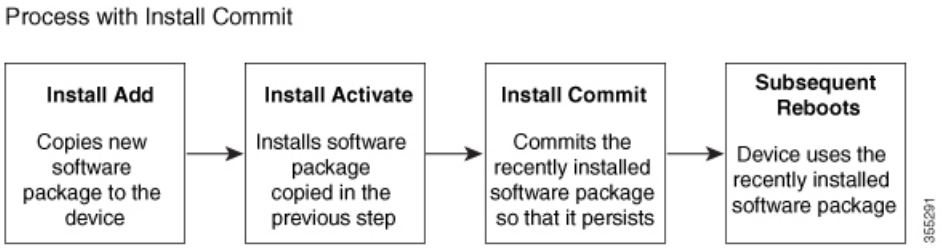
バンドルモード	インストールモード
このモードでは、ローカル（ハードディスク、フラッシュ）またはリモート（TFTP）の .bin イメージを使用して、統合されたブートプロセスが提供されます。 （注） USB および TFTP ブートからのバンドルブートはサポートされていません。	このモードでは、ブートプロセスにローカル（ブートフラッシュ）の packages.conf ファイルを使用します。
このモードでは、1 つの .bin ファイルを使用します。	このモードでは、.bin ファイルは拡張された .pkg ファイルに置き換えられます。
CLI： `#boot system file <filename>`	CLI： `#install add file bootflash: [activate commit]`

バンドルモード	インストールモード
このモードでアップグレードするには、boot system が新しいソフトウェアイメージをポイントするようにします。	このモードでアップグレードするには、**install** コマンドを使用します。
イメージの自動アップグレード：新しい Field Replaceable Unit（FRU）がモジュラ型シャーシに挿入された場合、アクティブな FRU と同じバージョンで新しい FRU を実行するには、手動による作業が必要です。	イメージの自動アップグレード：新しい FRU がモジュラ型シャーシに挿入された場合、結合する FRU は、アクティブな FRU と同期してイメージバージョンに自動アップグレードされます。
ロールバック：複数のソフトウェアメンテナンスの更新（SMU）を使用して以前のイメージにロールバックするには、複数回のリロードが必要になる場合があります。	ロールバック：1 回のリロードで、複数のパッチを含む、Cisco IOS XE ソフトウェアの以前のバージョンへのロールバックを有効にします。

インストールモードのプロセスフロー

インストールモードのプロセスフローは、プラットフォームでソフトウェアのインストールとアップグレードを実行するための次の 3 つのコマンドで構成されています。**install add**、**install activate**、**install commit**

次のフローチャートは、**install** コマンドを使用したインストールプロセスを説明しています。



install add コマンドは、ソフトウェアパッケージをローカルまたはリモートの場所からプラットフォームにコピーします。FTP、HTTP、HTTPs、または TFTP を使用できます。このコマンドは、パッケージファイルの個々のコンポーネントをサブパッケージと packages.conf ファイルに展開します。またファイルを検証して、イメージファイルがこれからインストールする先のプラットフォーム用のものであることを確認します。

install activate コマンドは、必要な検証を実行し、**install add** コマンドを使用して以前に追加されたパッケージをプロビジョニングします。また、システムのリロードをトリガーします。

install commit コマンドは、**install activate** コマンドを使用して以前にアクティブ化されたパッケージを確認し、リロード後も更新が持続されるようにします。

（注） 更新をインストールすると、以前にインストールしたソフトウェアイメージが置換されます。どんな時でも、1 つのデバイスにインストールできるのは 1 つのイメージのみです。

使用可能なインストールコマンドのリスト：

表 *12*：インストールコマンド一覧

コマンド	構文	目的
install add	**install add file** *location:filename.bin*	イメージ、パッケージ、およびSMUの内容をソフトウェアリポジトリにコピーします。ファイルの場所はローカルでもリモートでもかまいません。このコマンドは次のことを行います。 • ファイルのチェックサム、プラットフォームの互換性チェックなどを検証します。 • パッケージの個々のコンポーネントをサブパッケージと packages.conf に展開します。 • イメージをローカルインベントリにコピーし、次の手順で使用できるようにします。

コマンド	構文	目的
install activate	**install activate**	**install add** コマンドを使用して追加されたパッケージをアクティブ化します。 • **show install summary** コマンドを使用して、非アクティブなイメージを確認します。このイメージがアクティブ化されます。 • このコマンドを実行すると、システムがリロードされます。アクティベーションを続行するかどうかを確認します。確認プロンプトを自動的に無視するには、このコマンドと **prompt-level none** キーワードを使用します。

コマンド	構文	目的
(install activate) auto abort-timer	**install activate auto-abort timer** *<30-1200>*	**auto-abort timer** は自動的に開始され、デフォルト値は 120 分です。指定された時間内に **install commit** コマンドが実行されない場合、アクティベーションプロセスは中止され、システムは最後にコミットされた状態に戻ります。 • **install activate** コマンドを実行しながらタイマーの値を変更できます。 • **install commit** コマンドはタイマーを停止し、インストールプロセスを続行します。 • **install activate auto-abort timer stop** コマンドは、パッケージをコミットせずにタイマーを停止します。 • 確認プロンプトを自動的に無視するには、このコマンドと **prompt-level none** キーワードを使用します。 • このコマンドは、3 ステップインストールのバリアントでのみ有効です。
install commit	**install commit**	**install activate** コマンドを使用してアクティブ化されたパッケージをコミットし、リロード後も持続するようにします。 • **show install summary** コマンドを使用して、コミットされていないイメージを確認します。このイメージがコミットされます。

コマンド	構文	目的
install abort	**install abort**	インストールを中止し、システムを最後にコミットされた状態に戻します。 • このコマンドは、パッケージがアクティブ化された状態（コミットされていない状態）の場合にのみ適用されます。 • **install commit** コマンドを使用してイメージをすでにコミットしている場合は、**install rollback to** コマンドを使用して望みのバージョンに戻ります。
install remove	**install remove {file** <*filename*> **| inactive}**	プラットフォームリポジトリから非アクティブなパッケージを削除します。このコマンドを使用して、スペースを解放します。 • **file**：指定されたファイルを削除します。 • **inactive**：非アクティブなファイルをすべて削除します。

コマンド	構文	目的
install rollback to	**install rollback to {base | label | committed | id}**	保存されているインストールポイントか、最後にコミットされたインストールポイントに、ソフトウェアセットをロールバックします。このコマンドには次のような特長があります。 • リロードが必要です。 • パッケージがコミットされた状態の場合にのみ適用されます。 • 確認プロンプトを自動的に無視するには、このコマンドと **prompt-level none** キーワードを使用します。 （注） 以前のイメージへのインストールのロールバックを実行する場合は、以前のイメージはインストールモードでインストールされている必要があります。バンドルモードではSMUロールバックのみが可能です。
install deactivate	**install deactivate file** <*filename*>	プラットフォームリポジトリからパッケージを削除します。このコマンドは、SMUでのみサポートされています。 • 確認プロンプトを自動的に無視するには、このコマンドと **prompt-level none** キーワードを使用します。

次の show コマンドも使用できます。

表 *13 : show* コマンドの一覧

コマンド	構文	目的
show install log	**show install log**	プラットフォームがブートされた後に実行されたすべてのインストール操作の履歴と詳細を提供します。
show install package	**show install package** <*filename*>	指定された .pkg/.bin ファイルに関する詳細を提供します。
show install summary	**show install summary**	すべての FRU のイメージバージョンとそれに対応するインストール状態の概要を提供します。 • 表示される表には、この情報が適用される FRU が示されます。 • 存在するイメージとその状態に関してすべての FRU が同期している場合、1つの表のみが表示されます。 • ただし、FRU 間でイメージまたは状態の情報に違いがある場合は、スタックの残りの部分と異なる各 FRU が個別の表にリストされます。
show install active	**show install active**	すべての FRU のアクティブなパッケージに関する情報を提供します。 FRU 間で情報に違いがある場合は、スタックの残りの部分と異なる各 FRU が個別の表に示されます。

コマンド	構文	目的
show install inactive	**show install inactive**	すべての FRU に非アクティブなパッケージがあれば、そのパッケージに関する情報を提供します。 FRU 間で情報に違いがある場合は、スタックの残りの部分と異なる各 FRU が個別の表に示されます。
show install committed	**show install committed**	すべての FRU のコミットされたパッケージに関する情報を提供します。 FRU 間で情報に違いがある場合は、スタックの残りの部分と異なる各 FRU が個別の表に示されます。
show install uncommitted	**show install uncommitted**	すべての FRU について、コミットされていないパッケージがある場合はそのパッケージに関する情報を提供します。 FRU 間で情報に違いがある場合は、スタックの残りの部分と異なる各 FRU が個別の表に示されます。
show install rollback	**show install rollback {point-id | label}**	保存されているインストールポイントに関連付けられたパッケージを表示します。
show version	**show version [rp-slot] [installed [user-interface] | provisioned | running]**	ハードウェアとプラットフォームの情報とともに、現在のパッケージに関する情報を表示します。

プラットフォームをインストールモードで起動

単一のコマンド（1 ステップインストール）または複数の個別のコマンド（3 ステップインストール）を使用してソフトウェアパッケージをインストールして、アクティブ化し、コミットできます。

プラットフォームがバンドルモードで動作している場合、1 ステップインストールの手順を使用して、最初にバンドルモードからインストールモードに変換する必要があります。その後のプラットフォームでのインストールとアップグレードは、1 ステップまたは 3 ステップのバリアントのいずれかで実行できます。

1 ステップインストールまたはバンドルモードからインストールモードへの変換

（注）
- すべての CLI アクション（追加、アクティブ化など）は、使用可能なすべての FRU で実行されます。
- 保存されていない設定が検出されると、設定保存プロンプトが表示されます。
- このワークフローの 2 番目のステップの後に、リロードプロンプトが表示されます。確認プロンプトを自動的に無視するには、**prompt-level none** キーワードを使用します。
- プロンプトレベルが [None] に設定されていて、保存されていない設定がある場合、インストールは失敗します。コマンドを再発行する前に、設定を保存する必要があります。

以下で説明する 1 ステップインストールの手順を使用して、バンドルブートモードで実行されているプラットフォームをインストールモードに変換します。コマンドの実行後、プラットフォームはインストールブートモードでリブートします。

後で、1 ステップインストールの手順を使用してプラットフォームをアップグレードすることもできます。

この手順では、特権 EXEC モードで **install add file activate commit** コマンドを使用して、ソフトウェアパッケージをインストールし、プラットフォームを新しいバージョンにアップグレードします。

手順

ステップ 1 **enable**

例：

```
Device>enable
```

特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。

ステップ 2 **install add file location:** *filename* [**activate commit**]

例：

```
Device#install add file bootflash:c8kg2be-universalk9.17.15.03prd1.SPA.bin activate commit
```

ソフトウェア インストール パッケージをローカルまたはリモートの場所（FTP、HTTP、HTTPs、または TFTP 経由）からプラットフォームにコピーし、.package ファイルの個々のコンポーネントをサブパッケー

ジおよび packages.conf ファイルに展開します。プラットフォームおよびイメージバージョンの検証および互換性チェックを実行し、パッケージをアクティブ化し、そのパッケージをコミットして複数回リロードしても維持されるようにします。

このコマンドを実行すると、プラットフォームがリロードされます。

ステップ 3　exit

例：

```
Device#exit
```

特権 EXEC モードを終了し、ユーザー EXEC モードに戻ります。

3 ステップインストール

（注）
- すべての CLI アクション（追加、アクティブ化など）は、使用可能なすべての FRU で実行されます。
- 保存されていない設定が検出されると、設定保存プロンプトが表示されます。
- このワークフローの install activate ステップの後に、リロードプロンプトが表示されます。確認プロンプトを自動的に無視するには、**prompt-level none** キーワードを使用します。

3 ステップインストール手順は、プラットフォームがインストールモードになった後でのみ使用できます。このオプションにより、インストール時により多くの柔軟性と制御がもたらされます。

この手順では、個別の **install add**、**install activate**、および **install commit** コマンドを使用して、ソフトウェアパッケージをインストールし、プラットフォームを新しいバージョンにアップグレードします。

手順

ステップ 1　enable

例：

```
Device>enable
```

特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。

ステップ 2　install add file location: *filename*

例：

```
Device#install add file bootflash:c8kg2be-universalk9.17.15.03prd1.SPA.bin
```

ソフトウェア インストール パッケージをリモートの場所（FTP、HTTP、HTTPs、または TFTP 経由）からプラットフォームにコピーし、.package ファイルの個々のコンポーネントをサブパッケージおよび packages.conf ファイルに展開します。

ステップ 3 **show install summary**

例：

```
Device#show install summary
```

（オプション）すべての FRU のイメージバージョンとそれに対応するインストール状態の概要を提供します。

ステップ 4 **install activate** [**auto-abort-timer** <*time*>]

例：

```
Device# install activate auto-abort-timer 120
```

以前に追加されたパッケージをアクティブ化し、プラットフォームをリロードします。

- ソフトウェアの完全インストールを実行する場合は、パッケージ ファイル名を指定しないでください。
- 3 ステップインストールのバリアントでは、**install activate** コマンドで **auto-abort-timer** が自動的に開始されます。タイマーのデフォルトは 120 分です。タイマーの期限が切れる前に **install commit** コマンドが実行されない場合、インストールプロセスは自動的に終了します。プラットフォームがリロードされ、最後にコミットされたバージョンで起動します。

ステップ 5 **install abort**

例：

```
Device#install abort
```

（オプション）ソフトウェアインストールのアクティブ化を中止し、プラットフォームを最後にコミットされたバージョンに戻します。

- このコマンドは、イメージがアクティブ化されている状態でのみ使用できます。イメージがコミットされた状態の場合は使用できません。

ステップ 6 **install commit**

例：

```
Device#install commit
```

新しいパッケージのインストールをコミットし、リロード後も変更が持続されるようにします。

ステップ 7 **install rollback to committed**

例：

```
Device#install rollback to committed
```

（オプション）最後にコミットした状態にプラットフォームをロールバックします。

ステップ 8 **install remove** {**file** *filesystem: filename* | **inactive**}

例：

```
Device#install remove inactive
```

（オプション）ソフトウェア インストール ファイルを削除します。

- **file**：特定のファイルを削除します
- **inactive**：未使用および非アクティブ状態のインストールファイルを削除します。

ステップ 9 **show install summary**

例：

```
Device#show install summary
```

（オプション）現在のシステムの状態に関する情報を表示します。このコマンドの出力は、このコマンドよりも先に実行された **install** コマンドに応じて変化します。

ステップ 10 **exit**

例：

```
Device#exit
```

特権 EXEC モードを終了し、ユーザー EXEC モードに戻ります。

インストールモードでのアップグレード

1 ステップインストールまたは 3 ステップインストールを使用して、インストールモードでプラットフォームをアップグレードします。

インストールモードでのダウングレード

ダウングレード先のイメージがインストールモードでインストールされている場合、**install rollback** コマンドを使用して、プラットフォームを適切なイメージにポイントすることにより、プラットフォームを以前のバージョンにダウングレードします。

この **install rollback** コマンドはプラットフォームをリロードし、前のイメージで起動します。

（注） **install remove inactive** コマンドを使用して前のファイルを削除していない場合にのみ、**install rollback** コマンドは成功します。

または、**install** コマンドを使用して古いイメージをインストールすることでダウングレードすることもできます。

ソフトウェアインストールの中止

ソフトウェアパッケージのアクティブ化は次の方法で中止できます。

- 新しいイメージをアクティブ化した後にプラットフォームをリロードすると、3 ステップインストールのバリアントでは auto-abort-timer がトリガーされます。**install commit** コマンドを発行する前にタイマーが期限切れになった場合、インストールプロセスが終了します。プラットフォームはリロードし、最後にコミットしたバージョンのソフトウェアイメージで起動します。

  または、**install commit**コマンドを使用せずに、**install auto-abort-timer stop** コマンドを使用してこのタイマーを停止します。このプロセスでは、新しいイメージはコミットされていないままです。

- **install abort** コマンドを使用して、新しいソフトウェアのインストール前に実行していたバージョンにプラットフォームを戻します。このコマンドは、**install commit** コマンドを発行する前に使用します。

インストールコマンドを使用したソフトウェアインストールの設定例

以下は、1 ステップインストールまたはバンドルモードからインストールモードへの変換の例です。

```
Router# install add file bootflash:c8kg2be-universalk9.17.15.03.SPA.bin activate commit

May  6 08:35:19.308: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
add_activate_commit
bootflash:c8kg2be-universalk9.17.15.03.SPA.bininstall_add_activate_commit: START Tue May
 06 08:35:19 UTC 2025
install_add: START Tue May 06 08:35:19 UTC 2025
install_add: Adding IMG
--- Starting initial file syncing ---
Copying bootflash:c8kg2be-universalk9.17.15.03.SPA.bin from  R0 to  R0
Info: Finished copying to the selected
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
Checking status of Add on [R0]
Add: Passed on [R0]
Image added. Version: 17.15.03.0.5635

Finished Add

install_activate: START Tue May 06 08:36:08 UTC 2025
install_activate: Activating IMG
Following packages shall be activated:
/bootflash/c8kg2be-rpboot.17.15.03.SPA.pkg
/bootflash/c8kg2be-firmware_nim_xdsl.17.15.03.SPA.pkg
/bootflash/c8kg2be-mono-universalk9.17.15.03.SPA.pkg
/bootflash/c8kg2be-firmware_sm_1t3e3.17.15.03.SPA.pkg
/bootflash/c8kg2be-firmware_sm_async.17.15.03.SPA.pkg
/bootflash/c8kg2be-firmware_ngwic_t1e1.17.15.03.SPA.pkg
/bootflash/c8kg2be-firmware_nim_async.17.15.03.SPA.pkg
/bootflash/c8kg2be-firmware_sm_nim_adpt.17.15.03.SPA.pkg
/bootflash/c8kg2be-firmware_nim_shdsl.17.15.03.SPA.pkg
/bootflash/c8kg2be-firmware_prince.17.15.03.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]
May  6 08:36:08.538: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
activate NONEy
```

```
--- Starting Activate ---
Performing Activate on all members
[1] Activate package(s) on  R0

May  6 08:37:37.284: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds [1] Finished Activate on  R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
[1] Commit package(s) on  R0
[1] Finished Commit on  R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit operation

SUCCESS: install_add_activate_commit Tue May 06 08:37:59 UTC 2025

Router#
May  6 08:37:59.818: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed
install add_activate_commitMay  6 0


System integrity status: 0x32042000
Rom image verified correctly

System Bootstrap, Version v17.15(3.1r).s2.cp, RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.


Current image running: Boot ROM0

Last reset cause: LocalSoft
C8375-E-G2 platform with 33554432 Kbytes of main memory

........
boot: reading file c8kg2be-universalk9.17.15.03.SPA.bin
#################################################################################


Performing Signature Verification of OS image...
Image validated
May  6 08:40:59.347: %SYS-4-ROUTER_RUNNING_BUNDLE_BOOT_MODE: R0/0: Warning: Booting with
 bundle mode will be deprecated in the near future. Migration to install mode is required.
May  6 08:41:21.936: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           Cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706
```

```
Cisco IOS Software [IOSXE], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
 17.15.3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Tue 25-Mar-25 23:37 by mcpre


This software version supports only Smart Licensing as the software licensing mechanism.



Please read the following carefully before proceeding. By downloading,
installing, and/or using any Cisco software product, application, feature,
license, or license key (collectively, the "Software"), you accept and
agree to the following terms. If you do not agree, do not proceed and do not
use this Software.

This Software and its use are governed by Cisco's General Terms and any
relevant supplemental terms found at
https://www.cisco.com/site/us/en/about/legal/contract-experience/index.html.
If you have a negotiated agreement with Cisco that includes this Software, the
terms of that agreement apply as well. In the event of a conflict, the order
of precedence stated in your negotiated agreement controls.

Cisco Software is licensed on a term and/or subscription-basis. The license to
the Software is valid only for the duration of the specified term, or in the
case of a subscription-based license, only so long as all required subscription
payments are current and fully paid-up. While Cisco may provide you
licensing-related alerts, it is your sole responsibility to monitor your usage.
Using Cisco Software without a valid license is not permitted and may result in
fees charged to your account. Cisco reserves the right to terminate access to,
or restrict the functionality of, any Cisco Software, or any features thereof,
that are being used without a valid license.


May  6 08:41:25.397: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: bootflash quota
exceeded [free space is 3172248 kB] - [recommended free space is 5929066 kB] - Please
clean up files on bootflash.
cisco C8375-E-G2 (1RU) processor with 11906887K/6147K bytes of memory.
Processor board ID FDO2833M01A
Router operating mode: Autonomous
1 Virtual Ethernet interface
12 2.5 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
33554432K bytes of physical memory.
20257791K bytes of flash memory at bootflash:.

Warning: When Cisco determines that a fault or defect can be traced to
the use of third-party transceivers installed by a customer or reseller,
then, at Cisco's discretion, Cisco may withhold support under warranty or
a Cisco support program. In the course of providing support for a Cisco
networking product Cisco may require that the end user install Cisco
transceivers if Cisco determines that removing third-party parts will
assist Cisco in diagnosing the cause of a support issue.

WARNING: Command has been added to the configuration using a type 0 password. However,
recommended to migrate to strong type-6 encryption

WARNING: ** NOTICE **  The H.323 protocol is no longer supported from IOS-XE release
17.6.1. Please consider using SIP for multimedia applications.
```

```
Press RETURN to get started!


*May  6 08:41:23.620: %CRYPTO-5-SELF_TEST_START: Crypto algorithms release (Rel5a),
Entropy release (3.4.1)
       begin Crypto Module self-tests
*May  6 08:41:23.620: %CRYPTO-5-SELF_TEST_START: Crypto algorithms release (Rel5a),
Entropy release (3.4.1)
       begin Crypto Module Integrity Test
*May  6 08:41:23.625: %CRYPTO-5-SELF_TEST_END: Crypto Integrity self-test completed
successfully
       All tests passed.
*May  6 08:41:23.808: %CRYPTO-5-SELF_TEST_END: Crypto Algorithm self-test completed
successfully
       All tests passed.
*May  6 08:41:24.426: %ISR_THROUGHPUT-6-LEVEL: Throughput level has been set to 3000000
 kbps
*May  6 08:41:24.691: %SMART_LIC-6-AGENT_ENABLED: Smart Agent for Licensing is enabled
ESG-PM-ACL:[subsys-init] Init ESG-ACL subsystem starting

*May  6 08:41:27.684: ESG-PM-ACL:[subsys-init] Init ESG-ACL platform API reg

*May  6 08:41:27.684: ESG-PM-ACL:[subsys-init] Init ESG-ACL subsystem ended

*May  6 08:41:27.684: NGIOLite module C-NIM-8M success read extended attr from conf file


*May  6 08:41:29.186: %TLSCLIENT-5-TLSCLIENT_IOS: TLS Client is IOS based
*May  6 08:41:29.203: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
*May  6 08:41:29.252: %CRYPTO_ENGINE-5-CSDL_COMPLIANCE_ENFORCED: Cisco PSB security
compliance is being enforced
*May  6 08:41:29.267: %CUBE-3-LICENSING:  SIP trunking (CUBE) licensing is now based on
 dynamic sessions counting, static license capacity configuration through 'mode
border-element license capacity' would be ignored.
*May  6 08:41:29.268: %SIP-5-LICENSING: CUBE license reporting period has been set to
the minimum value of 8 hours.
*May  6 08:41:29.286: %VOICE_HA-7-STATUS: CUBE HA-supported platform detected.
*May  6 08:41:30.029: %CRYPTO_SL_TP_LEVELS-6-PLATFORM_BASED_LIC: Platform Based License
 Support, throughput is un-throttled
*May  6 08:41:30.061: %LINK-3-UPDOWN: Interface EOBC0, changed state to up
*May  6 08:41:30.069: %LINK-3-UPDOWN: Interface Lsmpi0, changed state to up
*May  6 08:41:30.069: %LINEPROTO-5-UPDOWN: Line protocol on Interface LI-Null0, changed
 state to up
*May  6 08:41:30.069: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-Null0, changed
 state to up
*May  6 08:41:30.069: %LINK-3-UPDOWN: Interface LIIN0, changed state to up
*May  6 08:41:30.070: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to down
*May  6 08:41:30.071: %IOSXE_RP_ALARM-6-INFO: ASSERT CRITICAL GigabitEthernet0 Physical
 Port Link Down
*May  6 08:41:30.243: %PNP-6-PNP_DISCOVERY_STARTED: PnP Discovery started
*May  6 08:40:41.171: %IOSXE-3-PLATFORM: R0/0: /usr/sbin/updatepcr8d: MPCCE: Failed to
read idprom cookie; error code: 100
*May  6 08:40:41.184: %IOSXE-3-PLATFORM: R0/0: /usr/sbin/updatepcr8d: Error logging in
to tam device, rc=0x64-TAM_LIB_ERR_MANDATORY_BUS_ENCRYPT_ENABLED
*May  6 08:40:41.184: %IOSXE-3-PLATFORM: R0/0: /usr/sbin/updatepcr8d: Error initializing
 tam device. PCR8 will not be extended.
*May  6 08:40:46.480: %IOSXE-3-PLATFORM: R0/0: /usr/sbin/updatepcr8d: MPCCE: Failed to
read idprom cookie; error code: 100
*May  6 08:40:46.493: %IOSXE-3-PLATFORM: R0/0: /usr/sbin/updatepcr8d: Error logging in
to tam device, rc=0x64-TAM_LIB_ERR_MANDATORY_BUS_ENCRYPT_ENABLED
*May  6 08:40:46.493: %IOSXE-3-PLATFORM: R0/0: /usr/sbin/updatepcr8d: Error initializing
 tam device. PCR8 will not be extended.
*May  6 08:40:59.263: %SERVICES-2-NORESOLVE_ACTIVE: C0/0: cmcc: Error resolving active
FRU: BINOS_FRU_RP
```

```
*May  6 08:40:59.346: %SYS-4-ROUTER_RUNNING_BUNDLE_BOOT_MODE: R0/0: Warning: Booting
with bundle mode will be deprecated in the near future. Migration to install mode is
required.
*May  6 08:41:21.935: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode
*May  6 08:41:25.396: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: bootflash quota
exceeded [free space is 3172248 kB] - [recommended free space is 5929066 kB] - Please
clean up files on bootflash.
*May  6 08:41:25.952: %CMRP_PFU-6-PEM_INSERTED: R0/0: cmand: Power Supply in slot 0 not
 operational.
*May  6 08:41:26.077: %CMRP_PFU-6-FANASSY_INSERTED: R0/0: cmand: Fan Assembly is inserted.
*May  6 08:41:30.313: %SYS-5-CONFIG_P: Configured programmatically by process MGMT VRF
Process from console as vty0
*May  6 08:41:30.519: %IOSXE_MGMTVRF-6-CREATE_SUCCESS_INFO: Management vrf Mgmt-intf
created with ID 1, ipv4 table-id 0x1, ipv6 table-id 0x1E000001
*May  6 08:41:30.519: %SYS-5-CONFIG_P: Configured programmatically by process MGMT VRF
Process from console as vty0
*May  6 08:41:30.688: %IOSXE_RP_ALARM-2-PEM: ASSERT CRITICAL Power Supply Module 0 Power
 Supply Failure
*May  6 08:41:30.688: %IOSXE_RP_ALARM-6-INFO: ASSERT CRITICAL POE Module 0 Power Supply
 Failure
*May  6 08:41:30.714: %ONEP_BASE-6-SS_ENABLED: ONEP: Service set Base was enabled by
Default
*May  6 08:41:31.046: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to down
*May  6 08:41:31.058: %LINEPROTO-5-UPDOWN: Line protocol on Interface EOBC0, changed
state to up
*May  6 08:41:31.066: %LINEPROTO-5-UPDOWN: Line protocol on Interface Lsmpi0, changed
state to up
*May  6 08:41:31.066: %LINEPROTO-5-UPDOWN: Line protocol on Interface LIIN0, changed
state to up
*May  6 08:41:31.066: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0,
 changed state to down
*May  6 08:41:31.262: %SMART_LIC-6-USAGE_NO_ACK: A Usage report acknowledgement has not
 been received in the last 0 days.
*May  6 08:41:31.263: %SIP-5-LICENSING: smart license report is not acknowledged.
*May  6 08:41:31.773: %SYS-7-NVRAM_INIT_WAIT_TIME: Waited 0 seconds for NVRAM to be
available
*May  6 08:41:31.944: %SYS-6-PRIVCFG_DECRYPT_SUCCESS: Successfully apply the private
config file
*May  6 08:41:32.030: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: TP-self-signed-2220840378
created succesfully
*May  6 08:41:32.031: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: SLA-TrustPoint created
succesfully
*May  6 08:41:32.034: %PKI-3-KEY_CMP_MISMATCH: Key in the certificate and stored key
does not match for Trustpoint-TP-self-signed-2220840378.
*May  6 08:41:32.041: %AAA-6-USERNAME_CONFIGURATION: user with username: admin configured
*May  6 08:41:32.041: %AAAA-4-CLI_DEPRECATED: WARNING: Command has been added to the
configuration using a type 0 password. However, recommended to migrate to strong type-6
 encryption
*May  6 08:41:32.041: %AAA-6-USER_PRIVILEGE_UPDATE: username: admin privilege updated
with priv-15
*May  6 08:41:32.259: %SYS-5-CONFIG_I: Configured from memory by console
*May  6 08:41:32.268: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/0, interfaces
disabled
*May  6 08:41:32.268: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/1, interfaces
disabled
*May  6 08:41:32.275: %SPA_OIR-6-OFFLINECARD: SPA (4M-2xSFP+) offline in subslot 0/0
*May  6 08:41:32.278: %SPA_OIR-6-OFFLINECARD: SPA (C-NIM-8M) offline in subslot 0/1
*May  6 08:41:32.306: %IOSXE_RP_ALARM-2-ESP: ASSERT CRITICAL module R0 No Working ESP
*May  6 08:41:32.309: %IOSXE_OIR-6-INSCARD: Card (fp) inserted in slot F0
*May  6 08:41:32.309: %IOSXE_OIR-6-INSCARD: Card (cc) inserted in slot 0
*May  6 08:41:32.309: %IOSXE_OIR-6-INSCARD: Card (cc) inserted in slot 1
*May  6 08:41:32.325: %CRYPTO-5-SELF_TEST_START: Crypto algorithms release (Rel5a),
Entropy release (3.4.1)
```

```
       begin Crypto Module self-tests
*May  6 08:41:32.329: %CRYPTO-5-SELF_TEST_END: Crypto Algorithm self-test completed
successfully
       All tests passed.
*May  6 08:41:32.712: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd: Server iox has been
 notified to start
*May  6 08:41:33.077: %SYS-5-RESTART: System restarted --
Cisco IOS Software [IOSXE], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
 17.15.3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Tue 25-Mar-25 23:37 by mcpre
*May  6 08:41:33.084: %SNMP-5-COLDSTART: SNMP agent on host Router is undergoing a cold
 start
*May  6 08:41:33.084: %SYS-5-CONFIG_I: Configured from console by console
*May  6 08:41:33.759: %IOSXE_OIR-6-ONLINECARD: Card (fp) online in slot F0
*May  6 08:41:34.091: %SYS-6-BOOTTIME: Time taken to reboot after reload =  215 seconds
*May  6 08:41:35.051: %LINEPROTO-5-UPDOWN: Line protocol on Interface VirtualPortGroup0,
 changed state to up
*May  6 08:41:35.063: %LINEPROTO-5-UPDOWN: Line protocol on Interface VirtualPortGroup1,
 changed state to up
*May  6 08:41:35.063: %LINEPROTO-5-UPDOWN: Line protocol on Interface VirtualPortGroup10,
 changed state to up
*May  6 08:41:38.437: %PNP-6-PNP_BEST_UDI_UPDATE: Best UDI
[PID:C8375-E-G2,VID:V01,SN:FDO2833M01A] identified via (entity-mibs)
*May  6 08:41:38.437: %PNP-6-PNP_CDP_UPDATE: Device UDI
[PID:C8375-E-G2,VID:V01,SN:FDO2833M01A] identified for CDP
*May  6 08:41:38.437: %PNP-6-PNP_DISCOVERY_STOPPED: PnP Discovery stopped (Startup Config
 Present)
*May  6 08:41:39.699: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to up
*May  6 08:41:40.707: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0,
 changed state to up
*May  6 08:41:42.333: %SYS-5-CONFIG_P: Configured programmatically by process EPM CREATE
 DEFAULT CWA URL ACL from console as console
*May  6 08:41:46.197: %IOSXE_OIR-6-ONLINECARD: Card (cc) online in slot 0
*May  6 08:41:46.230: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/0
*May  6 08:41:46.587: %IOSXE_OIR-6-ONLINECARD: Card (cc) online in slot 1
*May  6 08:41:47.126: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*May  6 08:41:47.126: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*May  6 08:41:48.779: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/1
*May  6 08:41:49.452: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*May  6 08:41:49.452: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*May  6 08:41:49.571: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: CISCO_IDEVID_SUDI created
succesfully
*May  6 08:41:49.573: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named CISCO_IDEVID_SUDI has
been generated or imported by pki-sudi
*May  6 08:41:49.609: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: CISCO_IDEVID_SUDI0 created
succesfully
*May  6 08:41:49.610: %PKI-2-NON_AUTHORITATIVE_CLOCK: PKI functions can not be initialized
 until an authoritative time source, like NTP, can be obtained.
*May  6 08:41:53.146: %IOX-3-PD_PARTITION_CREATE: R0/0: run_ioxn_caf: IOX may take upto
 3 mins to be ready. Wait for iox to be ready before installing the apps
*May  6 08:41:53.429: %IOX-3-PD_PARTITION_CREATE: R0/0: run_ioxn_caf: Successfully
allocated 4.0G in flash for hosting ApplicationsNGIOLite module C-NIM-8M success read
extended attr from conf file

*May  6 08:42:15.679: %SPA_OIR-6-ONLINECARD: SPA (C-NIM-8M) online in subslot 0/1
*May  6 08:42:16.292: %ENVIRONMENTAL-6-NOTICE: V: PEM Out, Location: P0, State: Minor_Low,
 Reading: 0 mV
*May  6 08:42:20.701: %ONEP_BASE-3-AUTHEN_ERR: [Element]: Authentication/authorization
failed. Application (utd_snort-utd): Username (*INVALID*)
*May  6 08:42:22.179: %TRANSCEIVER-6-INSERTED: C0/0: iomd: transceiver module inserted
in Te0/0/4
*May  6 08:42:22.255: %TRANSCEIVER-6-INSERTED: C0/0: iomd: transceiver module inserted
```

```
in Te0/0/5
*May  6 08:42:22.643: %LINK-3-UPDOWN: Interface TwoGigabitEthernet0/1/6, changed state
to up
*May  6 08:42:23.345: %SPA_OIR-6-ONLINECARD: SPA (4M-2xSFP+) online in subslot 0/0
*May  6 08:42:23.644: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TwoGigabitEthernet0/1/6, changed state to up
*May  6 08:42:28.999: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/4, changed state
to up
*May  6 08:42:29.011: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/5, changed state
to up
*May  6 08:42:29.975: %LINK-3-UPDOWN: Interface TwoGigabitEthernet0/0/0, changed state
to up
*May  6 08:42:30.004: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet0/0/4, changed state to up
*May  6 08:42:30.010: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet0/0/5, changed state to up
*May  6 08:42:29.901: %IM-6-IOX_INST_INFO: R0/0: ioxman: IOX SERVICE guestshell LOG:
Guestshell is up at 04/06/2025 08:42:29
*May  6 08:42:30.974: %LINK-3-UPDOWN: Interface TwoGigabitEthernet0/0/1, changed state
to up
*May  6 08:42:30.976: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TwoGigabitEthernet0/0/0, changed state to up
*May  6 08:42:31.975: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TwoGigabitEthernet0/0/1, changed state to up
*May  6 08:42:31.983: %LINK-3-UPDOWN: Interface TwoGigabitEthernet0/0/3, changed state
to up
*May  6 08:42:32.644: %LINK-3-UPDOWN: Interface TwoGigabitEthernet0/1/7, changed state
to up
*May  6 08:42:32.366: %CMRP-5-CHASSIS_MONITOR_BOOT_TIME_PRINT: R0/0: cmand: Card F0 took
 59 secs to boot
*May  6 08:42:32.367: %CMRP-5-CHASSIS_MONITOR_BOOT_TIME_PRINT: R0/0: cmand: Card 0 took
 54 secs to boot
*May  6 08:42:32.367: %CMRP-5-CHASSIS_MONITOR_BOOT_TIME_PRINT: R0/0: cmand: Card 1 took
 54 secs to boot
*May  6 08:42:32.984: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TwoGigabitEthernet0/0/3, changed state to up
*May  6 08:42:33.642: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TwoGigabitEthernet0/1/7, changed state to up
*May  6 08:42:34.003: ALL modules are online!
*May  6 08:42:34.765: %IM-6-IOX_ENABLEMENT: R0/0: ioxman: IOX is ready.
*May  6 08:42:34.766: %IM-6-START_MSG: R0/0: ioxman: app-hosting: Start succeeded: utd
is started Current is in RUNNING
May  6 08:42:36.712: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has been set.
May  6 08:42:38.080: %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement
will be required in 0 days.
May  6 08:42:38.081: ALL modules are online!
May  6 08:42:41.695: %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement
will be required in 0 days.
Router>
May  6 08:42:51.407: %ONEP_BASE-6-CONNECT: [Element]: ONEP session Application:utd_snort
 Host:utd ID:3545 User: has connected.
```

以下は、3 ステップインストールの例です。

```
Router#install add file bootflash:c8kg2be-universalk9.17.15.03a.SPA.bin
install_add: START Wed May 21 09:03:39 UTC 2025
install_add: Adding IMG
% UTD: Received appnav notification from LXC for   (src 192.0.2.5, dst 192.0.2.6)
% UTD successfully registered with Appnav (src 192.0.2.5, dst 192.0.2.6)
% UTD redirect interface set to VirtualPortGroup1 internally
--- Starting initial file syncing ---
Copying bootflash:c8kg2be-universalk9.17.15.03a.SPA.bin from  R0 to  R0
```

```
Info: Finished copying to the selected
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
Checking status of Add on [R0]
Add: Passed on [R0]
Image added. Version: 17.15.03a.0.176

Finished Add

SUCCESS: install_add /bootflash/c8kg2be-universalk9.17.15.03a.SPA.bin Wed May 21 09:04:43
 UTC 2025

Router#show install log
[0|install_op_boot]: START Wed May 21 09:02:03 Universal 2025
[0|install_op_boot(INFO, )]: Mount IMG INI state base image
[0|install_op_boot]: END SUCCESS  Wed May 21 09:02:03 Universal 2025
[0|install_op_boot(INFO, )]: cleanup_trap  remote_invocation 0 operation install_op_boot
 .. 0 .. 0
[remote|COMP_CHECK]: START Wed May 21 09:04:42 UTC 2025
[remote|COMP_CHECK]: END FAILED exit(1)  Wed May 21 09:04:43 UTC 2025

Router#
Router#install activate
install_activate: START Wed May 21 09:07:21 UTC 2025
install_activate: Activating IMG
Following packages shall be activated:
/bootflash/c8kg2be-rpboot.17.15.03a.SPA.pkg
/bootflash/c8kg2be-firmware_sm_nim_adpt.17.15.03a.SPA.pkg
/bootflash/c8kg2be-firmware_nim_async.17.15.03a.SPA.pkg
/bootflash/c8kg2be-firmware_sm_async.17.15.03a.SPA.pkg
/bootflash/c8kg2be-firmware_prince.17.15.03a.SPA.pkg
/bootflash/c8kg2be-mono-universalk9.17.15.03a.SPA.pkg
/bootflash/c8kg2be-firmware_nim_shdsl.17.15.03a.SPA.pkg
/bootflash/c8kg2be-firmware_ngwic_t1e1.17.15.03a.SPA.pkg
/bootflash/c8kg2be-firmware_sm_1t3e3.17.15.03a.SPA.pkg
/bootflash/c8kg2be-firmware_nim_xdsl.17.15.03a.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Activate ---
Performing Activate on all members
 [1] Activate package(s) on  R0

 [1] Finished Activate on  R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

SUCCESS: install_activate Wed May 21 09:09:31 UTC 2025
Router#May 21 09:

System integrity status: 0x32042000
Rom image verified correctly

System Bootstrap, Version v17.15(3.1r).s2.cp, RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.


Current image running: Boot ROM0

Last reset cause: LocalSoft
C8375-E-G2 platform with 33554432 Kbytes of main memory
```

```
........

boot: reading file packages.conf
#

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

Performing Signature Verification of OS image...
Image validated

May 21 09:11:47.581: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           Cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software [IOSXE], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
 17.15.3a, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Fri 02-May-25 11:27 by mcpre


This software version supports only Smart Licensing as the software licensing mechanism.


Please read the following carefully before proceeding. By downloading,
installing, and/or using any Cisco software product, application, feature,
license, or license key (collectively, the "Software"), you accept and
agree to the following terms. If you do not agree, do not proceed and do not
use this Software.

This Software and its use are governed by Cisco's General Terms and any
relevant supplemental terms found at
https://www.cisco.com/site/us/en/about/legal/contract-experience/index.html.
If you have a negotiated agreement with Cisco that includes this Software, the
terms of that agreement apply as well. In the event of a conflict, the order
of precedence stated in your negotiated agreement controls.

Cisco Software is licensed on a term and/or subscription-basis. The license to
the Software is valid only for the duration of the specified term, or in the
case of a subscription-based license, only so long as all required subscription
payments are current and fully paid-up. While Cisco may provide you
licensing-related alerts, it is your sole responsibility to monitor your usage.
Using Cisco Software without a valid license is not permitted and may result in
fees charged to your account. Cisco reserves the right to terminate access to,
or restrict the functionality of, any Cisco Software, or any features thereof,
that are being used without a valid license.


May 21 09:11:51.161: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: bootflash quota
```

```
exceeded [free space is 1111072 kB] - [recommended free space is 5929066 kB] - Please
clean up files on bootflash.
cisco C8375-E-G2 (1RU) processor with 11906881K/6147K bytes of memory.
Processor board ID FDO2833M01A
Router operating mode: Autonomous
1 Virtual Ethernet interface
12 2.5 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
33554432K bytes of physical memory.
20257791K bytes of flash memory at bootflash:.

Warning: When Cisco determines that a fault or defect can be traced to
the use of third-party transceivers installed by a customer or reseller,
then, at Cisco's discretion, Cisco may withhold support under warranty or
a Cisco support program. In the course of providing support for a Cisco
networking product Cisco may require that the end user install Cisco
transceivers if Cisco determines that removing third-party parts will
assist Cisco in diagnosing the cause of a support issue.
The process for the command is not responding or is otherwise unavailable

 WARNING: Command has been added to the configuration using a type 0 password. However,
 recommended to migrate to strong type-6 encryption

 WARNING: ** NOTICE **  The H.323 protocol is no longer supported from IOS-XE release
17.6.1. Please consider using SIP for multimedia applications.



Press RETURN to get started!

% UTD: Received appnav notification from LXC for   (src 192.0.2.5, dst 192.0.2.6)
% UTD successfully registered with Appnav (src 192.0.2.5, dst 192.0.2.6)
% UTD redirect interface set to VirtualPortGroup1 internally

Router>
Router>en
Router#
Router#install commit
install_commit: START Wed May 21 09:22:28 UTC 2025
--- Starting Commit ---
Performing Commit on all members
 [1] Commit packages(s) on  R0
 [1] Finished Commit packages(s) on  R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit operation

SUCCESS: install_commit Wed May 21 09:22:31 UTC 2025
```

以下は、show コマンドの出力例です。

show install log

```
Device# show install log
[0|install_op_boot]: START Thu Oct 28 22:09:29 Universal 2021
[0|install_op_boot(INFO, )]: Mount IMG INI state base image
[0|install_op_boot]: END SUCCESS  Thu Oct 28 22:09:30 Universal 2021
```

show install summary

```
Device# show install summary
[ R0 ] Installed Package(s) Information:

State (St): I - Inactive, U - Activated & Uncommitted,

C - Activated & Committed, D - Deactivated & Uncommitted

--------------------------------------------------------------------------------

Type  St   Filename/Version

--------------------------------------------------------------------------------

IMG   C    17.15.03a.0.176


--------------------------------------------------------------------------------

Auto abort timer: inactive

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

show install package *filesystem: filename*

```
Device# show install package bootflash:c8kg2be-universalk9.17.15.03a.SPA.bin
  Package: c8kg2be-universalk9.17.15.03a.SPA.bin
    Size: 953231736
    Timestamp:
  Canonical path: /bootflash/c8kg2be-universalk9.17.15.03a.SPA.bin

    Raw disk-file SHA1sum:
      d358592ccd2dd626889ef091401d06fae5458ff1
  Header size:     1084 bytes
  Package type:    30000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: rp_super
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: arm64
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: universalk9
    Build: 17.15.03a
    CardTypes:

  Package is bootable from media and tftp.
  Package contents:

  Package: c8kg2be-firmware_prince.17.15.03a.SPA.pkg
    Size: 10444800
    Timestamp:

    Raw disk-file SHA1sum:
      fa82bed30d349686d1d9700892076a3d66375698
    Header size:     4096 bytes
    Package type:    40000
    Package flags:   0
    Header version:  3

    Internal package information:
      Name: firmware_prince
```

```
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: none
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: firmware_prince
    Build: 17.15.03a
    CardTypes:

  Package is not bootable.
Package: c8kg2be-mono-universalk9.17.15.03a.SPA.pkg
  Size: 891244544
  Timestamp:

  Raw disk-file SHA1sum:
    af7ba58491731d788d9f4528d74b5bfef9dfc7f2
  Header size:     4096 bytes
  Package type:    30000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: mono
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: arm64
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: mono-universalk9
    Build: 17.15.03a
    CardTypes:

  Package is bootable from media and tftp.
  Package contents:

Package: c8kg2be-firmware_nim_xdsl.17.15.03a.SPA.pkg
  Size: 5677056
  Timestamp:

  Raw disk-file SHA1sum:
    4af7a8764651253c73c7fadebeba6f3a8f0a133d
  Header size:     4096 bytes
  Package type:    40000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: firmware_nim_xdsl
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: none
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: firmware_nim_xdsl
    Build: 17.15.03a
    CardTypes:

  Package is not bootable.
Package: c8kg2be-firmware_sm_1t3e3.17.15.03a.SPA.pkg
  Size: 13889536
  Timestamp:
```

```
  Raw disk-file SHA1sum:
    526aa41ccd8398e7691d316ca24289801e0417a8
  Header size:     4096 bytes
  Package type:    40000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: firmware_sm_1t3e3
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: none
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: firmware_sm_1t3e3
    Build: 17.15.03a
    CardTypes:

  Package is not bootable.
Package: c8kg2be-firmware_sm_async.17.15.03a.SPA.pkg
  Size: 14671872
  Timestamp:

  Raw disk-file SHA1sum:
    7c7f4c06da5b3b0e1db879e074998130db22298f
  Header size:     4096 bytes
  Package type:    40000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: firmware_sm_async
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: none
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: firmware_sm_async
    Build: 17.15.03a
    CardTypes:

  Package is not bootable.
Package: c8kg2be-firmware_nim_async.17.15.03a.SPA.pkg
  Size: 13254656
  Timestamp:

  Raw disk-file SHA1sum:
    27132c3a41c79991d1f71488ad325ad05cc7b0bb
  Header size:     4096 bytes
  Package type:    40000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: firmware_nim_async
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: none
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
```

```
    PackageName: firmware_nim_async
    Build: 17.15.03a
    CardTypes:

  Package is not bootable.
Package: c8kg2be-firmware_nim_shdsl.17.15.03a.SPA.pkg
  Size: 11804672
  Timestamp:

  Raw disk-file SHA1sum:
    51da21dffb39d2ef6b266b7ffab083b3fb339651
  Header size:     4096 bytes
  Package type:    40000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: firmware_nim_shdsl
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: none
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: firmware_nim_shdsl
    Build: 17.15.03a
    CardTypes:

  Package is not bootable.
Package: c8kg2be-firmware_ngwic_t1e1.17.15.03a.SPA.pkg
  Size: 11956224
  Timestamp:

  Raw disk-file SHA1sum:
    19376efa2ed616672c0d488b628a768e262bd8e6
  Header size:     4096 bytes
  Package type:    40000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: firmware_ngwic_t1e1
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: none
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: firmware_ngwic_t1e1
    Build: 17.15.03a
    CardTypes:

  Package is not bootable.
Package: c8kg2be-firmware_sm_nim_adpt.17.15.03a.SPA.pkg
  Size: 204800
  Timestamp:

  Raw disk-file SHA1sum:
    b3a7ddd80df900d6217bb8db36ff8bdbc6241fa3
  Header size:     4096 bytes
  Package type:    40000
  Package flags:   0
  Header version:  3
```

```
    Internal package information:
      Name: firmware_sm_nim_adpt
      BuildTime: 2025-05-02_11.57
      ReleaseDate: 2025-05-02_16.50
      BootArchitecture: none
      RouteProcessor: mirabile
      Platform: C8KG2BE
      User: mcpre
      PackageName: firmware_sm_nim_adpt
      Build: 17.15.03a
      CardTypes:

    Package is not bootable.
```

show install active

```
Device# show install active
[ R0 ] Active Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C  17.15.03a.0.158
--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

show install inactive

```
Device# show install inactive
[ R0 ] Inactive Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
No Inactive Packages
```

show install committed

```
Device# show install committed
[ R0 ] Committed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG    C   17.15.03a.0.158
--------------------------------------------------------------------------------




--------------------------------------------------------------------------------

Auto abort timer: inactive

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

show install uncommitted

```
Device# show install uncommitted
[ R0 ] Uncommitted Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
```

```
-------------------------------------------------------------------
Type  St   Filename/Version
-------------------------------------------------------------------
No Uncommitted Packages
```

インストールコマンドを使用したソフトウェアインストールのトラブルシューティング

問題 ソフトウェアインストールのトラブルシューティング

解決法 インストールの概要、ログ、およびソフトウェアバージョンを表示するには、次のshowコマンドを使用します。

- **show install summary**
- **show install log**
- **show version**
- **show version running**

問題 インストールに関するその他の問題

解決法 インストールに関する問題を解決するには、次のコマンドを使用します。

- **dir** <*install directory*>
- **more location:***packages.conf*
- **show tech-support install**：このコマンドはインストール情報に固有の情報を表示する**show**コマンドを自動的に実行します。
- **request platform software trace archive target bootflash** <*location*>：このコマンドは、最後のリロード以降にシステム上で実行されているすべてのプロセスに関連するすべてのトレースログをアーカイブし、この情報を指定された場所に保存します。

No Service Password-Recovery の設定

Cisco IOS のパスワード回復手順に従って、システムの起動時とリロード時に Break キーを使用することで、コンソールを使用してROMMONモードにアクセスできます。デバイスソフトウェアがROMMONモードからロードされている場合、設定は新しいパスワードで更新されます。パスワード回復手順により、コンソールへのアクセス権を持つ誰もがデバイスおよびデバイスのネットワークにアクセスする権限を与えられることになります。

No Service Password-Recovery 機能は、サービスパスワード回復手順を使用してデバイスおよびネットワークにアクセスできないようにすることを目的としています。

コンフィギュレーション レジスタおよびシステムブート設定

コンフィギュレーション レジスタの最小4ビット（ビット3、2、1、および0）がブートフィールドを構成します。ブートフィールドは、デバイスを手動で ROM から起動するか、フラッシュまたはネットワークから自動で起動するかを指定します。たとえば、コンフィギュレーション レジスタのブートフィールドの値が 0x2 から 0xF までの任意の値に設定されている場合、デバイスは、レジスタブートフィールドの値を使用して、ネットワークサーバーから自動起動するためのデフォルトブートファイル名を生成します。

ビット8が1に設定されると、スタートアップ コンフィギュレーションが無視されます。ビット 6 が 1 に設定されると、Break キー検出が有効になります。この機能を有効にするには、コンフィギュレーション レジスタを自動起動に設定する必要があります。他のコンフィギュレーション レジスタ設定では、機能をイネーブルにできなくなります。

（注） デフォルトでは、リロード後に確認用のプロンプトやメッセージは表示されません。

No Service Password-Recovery を有効にする方法

次の 2 つの方法で、No Service Password-Recovery を有効にできます。

- **no service password-recovery** コマンドを使用します。このオプションを有効にすると、パスワードを回復できるようになります。
- **no service password-recovery strict** コマンドを使用します。このオプションを有効にすると、デバイスの回復ができなくなります。

（注） 注意事項として、この機能を有効にする前に、有効な Cisco IOS イメージが bootflash: に存在していることを確認する必要があります。

no service password-recovery コマンドを開始する場合、シスコでは、デバイスから離れた場所にシステム コンフィギュレーション ファイルのコピーを保存することを推奨しています。

操作の開始にあたって、設定、モジュール、ソフトウェアバージョン、ROMMON バージョンの変更など、変更の重要性に関係なく、デバイスに変更を加える前に、この機能を無効にしてください。

コンフィギュレーション レジスタのブートビットを有効にして、ビット8を0に設定にすることでスタートアップ コンフィギュレーションをロードし、ビット6を0に設定することで Cisco IOS XE の Break キーを無視し、下位 4 ビット 3 ー 0 を 0x2 ー 0xF の任意の値に設定することで Cisco IOS XE イメージを自動ブートさせる必要があります。No Service Password-Recovery 機能を有効にすると、コンフィギュレーション レジスタの変更は保存されません。

（注） ビット 8 を 1 に設定すると、スタートアップ コンフィギュレーションが無視されます。ビット 6 を 1 に設定すると、Cisco IOS XE での Break キーの検出が有効になります。ビット 6 とビット 8 の両方を 0 に設定すると、No Service Password-Recovery 機能が有効になります。

次に、No Service Password-Recovery 機能を有効にする方法の例を示します。

```
Router> enable
Router# show version
Router# configure terminal
Router(config)# config-register 0x2012
Router(config)# no service password-recovery
Router(config)# exit
```

有効化された No Service Password-Recovery 機能によるデバイスの回復

no service password-recovery コマンドを使用して No Service Password-Recovery 機能を有効にした後にデバイスを回復するには、起動時に表示される「PASSWORD RECOVERY FUNCTIONALITY IS DISABLED」というメッセージを探します。「..」が表示されたら、Break キーを押します。Break キーアクションの確認を求めるプロンプトが表示されます。

- アクションを確認すると、スタートアップ コンフィギュレーションが消去され、有効化された No Service Password-Recovery 機能により、デバイスが工場出荷時のデフォルト設定で起動します。
- Break キーアクションを確認しないと、有効化された No Service Password-Recovery 機能により、デバイスが通常どおりに起動します。

（注） **no service password-recovery strict** コマンドを使用して No Service Password-Recovery 機能を有効した場合は、デバイスを回復できません。

次の例では、起動時に Break キーアクションが入力され、その後に Break キーアクションが確認されます。スタートアップ コンフィギュレーションが消去され、有効化された No Service Password-Recovery 機能により、デバイスが工場出荷時のデフォルト設定で起動します。

```
Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly


System Bootstrap, Version 17.3(1r), RELEASE SOFTWARE
Copyright (c) 1994-2020  by cisco Systems, Inc.


Current image running: Boot ROM0

Last reset cause: LocalSoft
C8375-E-G2 platform with 33554432 Kbytes of main memory
```

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED

..

telnet> send brk

..

PASSWORD RECOVERY IS DISABLED.

Do you want to reset the router to the factory default
configuration and proceed [y/n] ? y

Router clearing configuration. Please wait for ROMMON prompt...

File size is 0x17938a80

Located c8kg2be-universalk9.BLD_V1718_THROTTLE_LATEST_20250423_010128.SSA.bin

...
```

次の例では、起動時に Break キーアクションが入力され、その後に Break キーアクションが確認されません。この場合、有効化された No Service Password-Recovery 機能により、デバイスが通常どおりに起動します。

```
Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly

System Bootstrap, Version v17.15(3.1r).s2.cp, RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
C8375-E-G2 platform with 33554432 Kbytes of main memory

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED

..

telnet> send brk

...

PASSWORD RECOVERY IS DISABLED.

Do you want to reset the router to the factory default
configuration and proceed [y/n] ? n

Router continuing with existing configuration...

File size is 0x17938a80

Located c8kg2be-universalk9.BLD_V1718_THROTTLE_LATEST_20250423_010128.SSA.bin


...

########################################################################## …
```

No Service Password-Recovery の設定例

次に、自動起動に設定されているコンフィギュレーション レジスタ設定を取得し、Password-Recovery機能を無効にしてから、設定がシステムのリロード後も維持されることを確認する方法の例を示します。

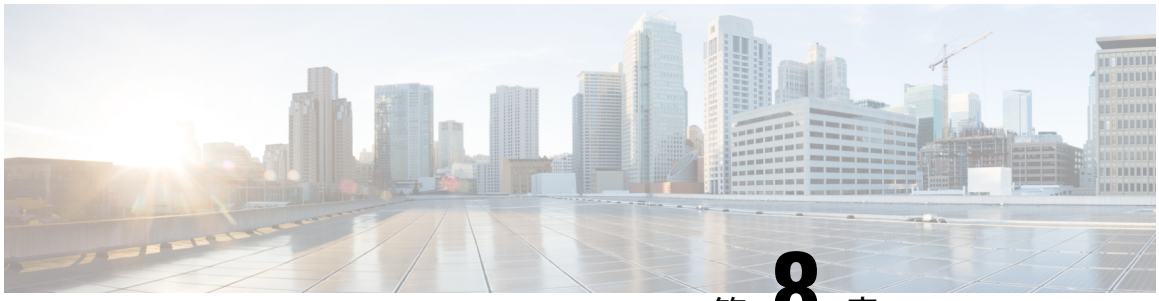
```
Router>en
Router#show version
Cisco IOS XE Software, Version 17.15.03
Cisco IOS Software [IOSXE], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
 17.15.3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Tue 25-Mar-25 23:37 by xxxx

Router(config)#no service password-recovery
WARNING:
Executing this command will disable the password recovery mechanism.
Do not execute this command without another plan for
password recovery.

Are you sure you want to continue? [yes]: yes
Router(config)#end
Router#wr
Building configuration...
[OK]
Router#reload
Proceed with reload? [confirm]
Jun  9

System integrity status: 0x32042000
Rom image verified correctly

System Bootstrap, Version v17.15(3.1r).s2.cp, RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.


Current image running: Boot ROM0

Last reset cause: LocalSoft
C8375-E-G2 platform with 33554432 Kbytes of main memory

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED

.
telnet> send brk
.....


PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to the factory default
configuration and proceed  y/n [n]: n

Router continuing with existing configuration...

boot: reading file packages.conf
############################################################

Performing Signature Verification of OS image...
Image validated

Jun  9 05:40:13.287: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode
```

```
                Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           Cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software [IOSXE], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
 17.15.3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Tue 25-Mar-25 23:37 by xxxx


This software version supports only Smart Licensing as the software licensing mechanism.


Please read the following carefully before proceeding. By downloading,
installing, and/or using any Cisco software product, application, feature,
license, or license key (collectively, the "Software"), you accept and
agree to the following terms. If you do not agree, do not proceed and do not
use this Software.

This Software and its use are governed by Cisco's General Terms and any
relevant supplemental terms found at
https://www.cisco.com/site/us/en/about/legal/contract-experience/index.html.
If you have a negotiated agreement with Cisco that includes this Software, the
terms of that agreement apply as well. In the event of a conflict, the order
of precedence stated in your negotiated agreement controls.

Cisco Software is licensed on a term and/or subscription-basis. The license to
the Software is valid only for the duration of the specified term, or in the
case of a subscription-based license, only so long as all required subscription
payments are current and fully paid-up. While Cisco may provide you
licensing-related alerts, it is your sole responsibility to monitor your usage.
Using Cisco Software without a valid license is not permitted and may result in
fees charged to your account. Cisco reserves the right to terminate access to,
or restrict the functionality of, any Cisco Software, or any features thereof,
that are being used without a valid license.


Jun  9 05:40:16.793: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: bootflash quota
exceeded [free space is 115484 kB] - [recommended free space is 5929066 kB] - Please
clean up files on bootflash.
cisco C8375-E-G2 (1RU) processor with 11906887K/6147K bytes of memory.
Processor board ID FDO2833M01A
Router operating mode: Autonomous
1 Virtual Ethernet interface
12 2.5 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
33554432K bytes of physical memory.
20257791K bytes of flash memory at bootflash:.

Warning: When Cisco determines that a fault or defect can be traced to
the use of third-party transceivers installed by a customer or reseller,
```

```
then, at Cisco's discretion, Cisco may withhold support under warranty or
a Cisco support program. In the course of providing support for a Cisco
networking product Cisco may require that the end user install Cisco
transceivers if Cisco determines that removing third-party parts will
assist Cisco in diagnosing the cause of a support issue.
No processes could be found for the command

 WARNING: Command has been added to the configuration using a type 0 password. However,
 recommended to migrate to strong type-6 encryption

 WARNING: ** NOTICE **  The H.323 protocol is no longer supported from IOS-XE release
17.6.1. Please consider using SIP for multimedia applications.



Press RETURN to get started!
```

次に、no service password-recovery strict コマンドを使用して、パスワード回復機能を無効にする例を示します。

```
Router# configure terminal

Router(config)# no service password-recovery strict

WARNING:
Executing this command will disable the password recovery mechanism.
Do not execute this command without another plan for
password recovery.

Are you sure you want to continue? [yes]: yes
Router(config)#end
Router#wr
Building configuration...
[OK]
..
```



第 8 章

インターフェイス コンフィギュレーション

この章では、インターフェイス コンフィギュレーションに関する情報について説明します。スロットはデバイスのシャーシスロット番号を示し、サブスロットはサービスモジュールが装着されているスロットを示します。

スロットおよびサブスロットの詳細については、次のマニュアルの「スロットおよびインターフェイスについて」セクションを参照してください。

- Hardware Installation Guide for Cisco 8300 Series Secure Routers

この章で説明する内容は、次のとおりです。

インターフェイスの設定

ここでは、ギガビットインターフェイスを設定する方法について説明し、ルータインターフェイスの設定例も示します。

ギガビット イーサネット インターフェイスの設定

手順

ステップ 1　enable

例：

```
Router> enable
```

特権 EXEC モードを有効にします。

パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Router# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **interface TwoGigabitEthernet** *slot/subslot/port*

例：

```
Router(config)# interface TwoGigabitEthernet 0/0/1
```

GigabitEthernet インターフェイスを設定します。

- **TwoGigabitEthernet**：インターフェイスのタイプ。
- *slot*：シャーシのスロット番号。
- */subslot*：セカンダリスロット番号。スラッシュ（/）が必要です。
- /port：ポートまたはインターフェイス番号。スラッシュ（/）が必要です。

ステップ 4 **ip address** *ip-address mask* [**secondary**] **dhcp pool**

例：

```
Router(config-if)# ip address 10.0.0.1 255.255.255.0 dhcp pool
```

GigabitEthernet に IP アドレスを割り当てます。

- **ip address** *ip-address*：インターフェイスの IP アドレス。
- *mask*：関連付けられている IP サブネットのマスク。
- **secondary**（任意）：設定されたアドレスをセカンダリ IP アドレスとして指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。
- **dhcp**：DHCP を介してネゴシエートされる IP アドレス。
- **pool**：ローカル DHCP プールから自動的に設定される IP アドレス。

ステップ 5 **negotiation auto**

例：

```
Router(config-if)# negotiation auto
```

ネゴシエーション モードを選択します。

- **auto**：リンクの自動ネゴシエーションを実行します。

ステップ 6 end

例：

```
Router(config-if)# end
```

現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。

インターフェイスの設定：例

次に、**interface TwogigabitEthernet** コマンドを使用してインターフェイスを追加し、IP アドレスを設定する例を示します。**0/0/1** はスロット/サブスロット/ポートを示します。ポートには 0 ～ 5 の番号が割り振られます。

```
Router# show running-config interface TwogigabitEthernet 0/0/1
Building configuration...
Current configuration : 108 bytes
!
interface TwoGigabitEthernet0/0/1
no ip address
shutdown
negotiation auto
mka policy priority100
end
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface TwogigabitEthernet 0/0/1
```

（注） いくつかのシスコプラットフォーム、NIM、および SM カードでは、同じインターフェイスでのマルチレート SFP の設定がサポートされています（10G ポートでの 1G SFP または 10G SFP+ など）。

ポートチャネルバンドルでは、すべてのメンバーインターフェイスの速度とデュプレックスが同じである必要があります。ポートチャネルを設定するには、メンバーインターフェイスと同じ速度のデュプレックス インターフェイスを使用することをお勧めします。

マルチレート SFP をサポートするインターフェイスの詳細については、対応するデータシートを参照してください。

すべてのインターフェイスのリストの表示：例

この例では、**show interfaces summary**、および **show platform software status control-process brief** コマンドを使用して、C8375-E-G2 のすべてのインターフェイスを表示します。

```
Router# show interfaces summary
    *: interface is up
    IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
    OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
    RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
    TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
    TRTL: throttle count

Interface                   IHQ       IQD       OHQ       OQD       RXBS      RXPS
TXBS      TXPS      TRTL
------------------------------------------------------------------------------------------------

 Tw0/0/0                      0         0         0         0         0         0
    0         0         0
 Tw0/0/1                      0         0         0         0         0         0
    0         0         0
 Tw0/0/2                      0         0         0         0         0         0
    0         0         0
*Tw0/0/3                      0         0         0         0         0         0
    0         0         0
*Tw0/0/3.10                   -         -         -         -         -         -
    -         -         -
*Te0/0/4                      0         0         0         0         0         0
    0         0         0
*Te0/0/4.10                   -         -         -         -         -         -
    -         -         -
*Te0/0/5                      0         0         0         0         0         0
    0         0         0
*Te0/0/5.10                   -         -         -         -         -         -
    -         -         -
 Tw0/1/0                      0         0         0         0         0         0
    0         0         0
 Tw0/1/1                      0         0         0         0         0         0
    0         0         0
 Tw0/1/2                      0         0         0         0         0         0
    0         0         0
 Tw0/1/3                      0         0         0         0         0         0
    0         0         0
 Tw0/1/4                      0         0         0         0         0         0
    0         0         0
 Tw0/1/5                      0         0         0         0         0         0
    0         0         0
*Tw0/1/6                      0         0         0         0         0         0
    0         0         0
*Tw0/1/7                      0         0         0         0         0         0
    0         0         0
*Tw0/1/7.10                   -         -         -         -         -         -
    -         -         -
*Service-Engine0/4/0          0         0         0         0         0         0
    0         0         0
*GigabitEthernet0             0         0         0         0      2000         3
    0         0         0
*Tunnel0                      0         0         0         3         0         0
    0         0         0
*VirtualPortGroup0            0         0         0         0         0         0
    0         0         0
*VirtualPortGroup1            0         0         0         0      4000         4
 3000         4         0
*VirtualPortGroup10           0         0         0         0         0         0
    0         0         0
 Vlan1                        0         0         0         0         0         0
    0         0         0
NOTE:No separate counters are maintained for subinterfaces
```

```
Hence Details of subinterface are not shown


Router#show platform software status control-process brief
Load Average
 Slot  Status  1-Min  5-Min 15-Min
  RP0 Healthy   0.83   0.91   0.91

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
  RP0 Healthy  7768456  2654936 (34%)  5113520 (66%)   3115212 (40%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
  RP0    0   2.70   1.70   0.00  95.59   0.00   0.00   0.00
         1   0.00   0.00   0.00 100.00   0.00   0.00   0.00
         2   0.00   0.00   0.00 100.00   0.00   0.00   0.00
         3   0.00   0.00   0.00 100.00   0.00   0.00   0.00
         4   2.40   1.40   0.00  96.19   0.00   0.00   0.00
         5   0.80   1.60   0.00  97.59   0.00   0.00   0.00
         6  12.40  12.30   0.00  75.30   0.00   0.00   0.00
         7  11.20  12.40   0.00  76.40   0.00   0.00   0.00
         8   2.80   1.80   0.00  95.40   0.00   0.00   0.00
         9   0.00   0.00   0.00 100.00   0.00   0.00   0.00
        10   0.00   0.00   0.00 100.00   0.00   0.00   0.00
        11   0.00   0.00   0.00 100.00   0.00   0.00   0.00
```

この例では、**show interfaces summary**、および **show platform software status control-process brief** コマンドを使用して、C8355-G2 のすべてのインターフェイスを表示します。

```
Router# show interfaces summary
*: interface is up

IHQ: pkts in input hold queue     IQD: pkts dropped from input queue

OHQ: pkts in output hold queue    OQD: pkts dropped from output queue

RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)

TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)

TRTL: throttle count

Interface                   IHQ       IQD       OHQ       OQD      RXBS      RXPS
TXBS      TXPS      TRTL
------------------------------------------------------------------------------------------------------------

Fi0/0/0                       0         0         0         0         0         0
   0         0         0
Fi0/0/1                       0         0         0         0         0         0
   0         0         0
Fi0/0/2                       0         0         0         0         0         0
   0         0         0
Fi0/0/3                       0         0         0         0         0         0
   0         0         0
GigabitEthernet0/0/4          0         0         0         0         0         0
   0         0         0
GigabitEthernet0/0/5          0         0         0         0         0         0
   0         0         0
Te0/0/6                       0         0         0         0         0         0
   0         0         0
Te0/0/7                       0         0         0         0         0         0
   0         0         0
* Te0/0/8                     0         0         0         0 9614824000   1353964
```

```
9614825000   1353964         0
* Te0/0/9                      0         0         0         0 9614822000   1353963
9614826000   1353963         0
* GigabitEthernet0             0         0         0         0      7000         7
  1000         2         0
* Loopback1                    0         0         0         0         0         0
     0         0         0
* Loopback2                    0         0         0         0         0         0
     0         0         0
* Loopback3                    0         0         0         0         0         0
     0         0         0
Tunnel3                      0         0         0         0         0         0
   0         0         0
Vlan1                        0         0         0         0         0         0
   0         0         0
Vlan10                       0         0         0         0         0         0
   0         0         0
```

```
Router#show platform software status control-process brief
Load Average

Slot  Status  1-Min  5-Min 15-Min

RP0 Healthy  11.15  11.17  11.10

                                                                  Memory (kB)


Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)

RP0 Healthy 16134276  3974444 (25%) 12159832 (75%)   4499476 (28%)

                                                                  CPU Utilization


Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait

RP0    0   1.79   2.69   0.00  94.80   0.49   0.19   0.00

1  99.90   0.00   0.00   0.00   0.10   0.00   0.00

2  99.80   0.00   0.00   0.00   0.10   0.10   0.00

3  99.90   0.00   0.00   0.00   0.10   0.00   0.00

4  99.90   0.00   0.00   0.00   0.10   0.00   0.00

5  99.90   0.00   0.00   0.00   0.10   0.00   0.00

6 100.00   0.00   0.00   0.00   0.00   0.00   0.00

7  99.89   0.00   0.00   0.00   0.10   0.00   0.00

8  99.90   0.00   0.00   0.00   0.10   0.00   0.00

9 100.00   0.00   0.00   0.00   0.00   0.00   0.00

10  14.00  58.50   0.00  23.90   3.60   0.00   0.00

11  99.90   0.00   0.00   0.00   0.10   0.00   0.00
```

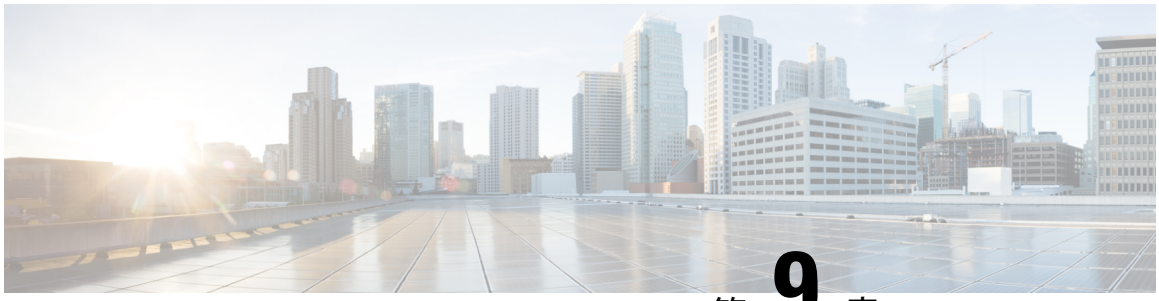
インターフェイスに関する情報の表示：例

この例では、C8375-E-G2 で **show ip interface brief** コマンドを使用して、インターフェイスの IP 情報とステータスの要約（仮想インターフェイスバンドル情報を含む）を表示する方法を示します。

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Tw0/0/0                192.168.10.1    YES NVRAM  down                  down
Tw0/0/1                unassigned      YES NVRAM  administratively down down
Tw0/0/2                192.168.11.1    YES NVRAM  down                  down
Tw0/0/3                unassigned      YES NVRAM  up                    up
Tw0/0/3.10             192.168.3.1     YES NVRAM  up                    up
Te0/0/4                unassigned      YES NVRAM  up                    up
Te0/0/4.10             192.168.4.1     YES NVRAM  up                    up
Te0/0/5                unassigned      YES NVRAM  up                    up
Te0/0/5.10             192.168.4.2     YES NVRAM  up                    up
Tw0/1/0                unassigned      YES unset  administratively down down
Tw0/1/1                unassigned      YES unset  down                  down
Tw0/1/2                unassigned      YES unset  down                  down
Tw0/1/3                unassigned      YES unset  down                  down
Tw0/1/4                unassigned      YES unset  down                  down
Tw0/1/5                unassigned      YES unset  down                  down
Tw0/1/6                192.168.22.200  YES NVRAM  up                    up
Tw0/1/7                unassigned      YES NVRAM  up                    up
Tw0/1/7.10             192.168.3.2     YES NVRAM  up                    up
Service-Engine0/4/0    unassigned      YES unset  up                    up
GigabitEthernet0       10.79.58.164    YES NVRAM  up                    up
Tunnel0                192.0.2.5       YES unset  up                    up
VirtualPortGroup0      192.0.2.1       YES NVRAM  up                    up
VirtualPortGroup1      192.0.2.5       YES NVRAM  up                    up
VirtualPortGroup10     10.88.88.1      YES NVRAM  up                    up
Vlan1                  unassigned      YES unset  up                    down
```

この例では、C8355-G2 で **show ip interface brief** コマンドを使用して、インターフェイスの IP 情報とステータスの要約（仮想インターフェイスバンドル情報を含む）を表示する方法を示します。

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Fi0/0/0                unassigned      YES NVRAM  administratively down down
Fi0/0/1                unassigned      YES NVRAM  administratively down down
Fi0/0/2                unassigned      YES NVRAM  administratively down down
Fi0/0/3                unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0/4   unassigned      YES unset  administratively down down
GigabitEthernet0/0/5   unassigned      YES unset  administratively down down
Te0/0/6                unassigned      YES unset  administratively down down
Te0/0/7                unassigned      YES unset  administratively down down
Te0/0/8                8.1.1.1         YES NVRAM  up                    up
Te0/0/9                9.1.1.1         YES NVRAM  up                    up
GigabitEthernet0       10.75.163.116   YES NVRAM  up                    up
Loopback1              192.168.100.1   YES NVRAM  up                    up
Loopback2              192.168.101.1   YES NVRAM  up                    up
Loopback3              192.168.102.1   YES NVRAM  up                    up
Tunnel3                unassigned      YES TFTP   up                    down
Vlan1                  unassigned      YES unset  up                    down
Vlan10                 7.1.1.1         YES NVRAM  up                    down
```



第 9 章

Security-Enhanced Linux のサポート

この章では SELinux の機能について説明します。具体的な内容は次のとおりです。

概要

Security-Enhanced Linux（SELinux）は、Linux カーネル セキュリティ モジュールとシステム ユーティリティで構成されるソリューションで、強力で柔軟な Mandatory Access Control（MAC）アーキテクチャを Cisco IOS-XE プラットフォームに組み込みます。

SELinux には機密性と整合性の要件に基づいて情報を分離するための拡張メカニズムが備わっています。これにより、アプリケーションのセキュリティメカニズムの改ざんやバイパスの脅威に対処し、悪意のあるアプリケーションや欠陥のあるアプリケーションによって引き起こされる可能性のある障害を封じ込めることができます。

SELinux の前提条件

この機能に関する固有の要件はありません。

SELinux の制限事項

この機能に関する特定の制限はありません。

SELinux に関する情報

SELinux はユーザープログラムやシステムサービスを、割り当てられた機能を実行するために必要になる最小限の権限に制限する強制アクセス制御ポリシーを適用します。これにより、（バッファのオーバーフローや設定ミスなどによって）侵害された場合、害を生じさせるこれらのプログラムやデーモンの能力が削減または排除されます。これは、Cisco IOS-XE プラットフォームで MAC を適用することによる最小権限の原則の実用的な実装です。この制限メカニズムは、従来の Linux アクセス制御メカニズムとは独立して機能します。SELinux は、アプリケーションプロセスからリソースオブジェクトへのアクセスを制御するポリシーを定義する機能を提供します。これにより、プロセス動作の明確な定義と制限を明確にできます。

SELinux は、システムで有効になっている場合、**Permissive モード**または **Enforcing モード**のいずれかで動作します。

- Permissive モードでは、SELinux はポリシーを適用せず、リソースアクセスポリシーの違反によって発生した拒否のシステムログのみを生成します。操作は拒否されず、リソースアクセスポリシー違反についてのみログに記録されます。
- Enforcing モードでは、SELinux ポリシーが有効になり、適用されます。アクセスポリシールールに基づいてリソースアクセスを拒否し、システムログを生成します。

サポートされている Cisco IOS XE プラットフォームでは、SELinux はデフォルトで Enforcing モードで有効になっています。Enforcing モードでは、必要な許可ポリシーを持たないシステムリソースアクセスは違反として扱われ、操作は拒否されます。拒否が発生すると、違反操作は失敗し、システムログが生成されます。Enforcing モードでは、ソリューションはアクセス違反防止モードで機能します。

SELinux の設定

Enforcing モードで SELinux 機能を有効化または操作するために必要な追加の要件や設定手順はありません。

SELinux の機能の一部として、次のコマンドが導入されています。

```
platform security selinux {enforcing | permissive}
show platform software selinux
```

SELinux の設定（EXEC モード）

set platform software selinux コマンドを使用して、EXEC モードで SELinux を設定します。

次に、EXEC モードでの SELinux 設定の例を示します。

```
Device# set platform software selinux ?

default  Set SELinux mode to default
enforcing  Set SELinux mode to enforcing
permissive  Set SELinux mode to permissive
```

SELinux の設定（CONFIG モード）

platform security selinux コマンドを使用して、コンフィギュレーション モードで SELinux を設定します。

次の例は、CONFIG モードでの SELinux 設定を示しています。

```
Device(config)# platform security selinux

enforcing  Set SELinux policy to Enforcing mode
permissive  Set SELinux policy to Permissive mode

Device(config)# platform security selinux permissive

Device(config)#
*Oct 20 21:52:45.155: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode downgraded to permissive!

Device(config)#
```

SELinux の例

次に、モードを Enforcing から Permissive に変更した場合の出力例を示します。

```
"*Oct 20 21:44:03.609: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode downgraded to permissive!"
```

次に、モードを Permissive から Enforcing に変更した場合の出力例を示します。

```
"*Oct 20 21:44:34.160: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode upgraded to enforcing!"
```

（注） SELinux モードが変更されると、この変更はシステム セキュリティ イベントと見なされ、システムログメッセージが生成されます。

Syslog メッセージリファレンス

機能重大度ニーモニック	%SELINUX-1-VIOLATION
重大度の意味	アラートレベルログ
メッセージ	該当なし
メッセージの説明	リソースのアクセスポリシーが存在しないプロセスによって、リソースアクセスが実行されました。操作にフラグが設定され、リソースアクセスが拒否されました。プロセスリソースアクセスが拒否されたという情報を含むシステムログが生成されました。
コンポーネント	SELINUX

機能重大度ニーモニック	%SELINUX-1-VIOLATION
推奨処置	次の関連情報を添付ファイルとしてCisco TACにご連絡ください。 • コンソールまたはシステムに出力されるとおりのメッセージ • **show tech-support** コマンドの出力（テキストファイル） • ボックスからの Btrace ファイルのアーカイブ（次のコマンドを使用）： **request platform software trace archive target <URL>** • **show platform software selinux** コマンドの出力

次に、syslog メッセージの例を示します。

例 1：

```
*Nov 14 00:09:04.943: %SELINUX-1-VIOLATION: R0/0: audispd: type=AVC
msg=audit(1699927057.934:129): avc: denied { getattr } for pid=5899 comm="ls"
path="/root/test" dev="rootfs" ino=25839
scontext=system_u:system_r:polaris_iosd_t:s0
tcontext=system_u:object_r:admin_home_t:s0 tclass=file permissive=0
```

例 2：

```
*Nov 14 00:09:04.947: %SELINUX-1-VIOLATION: R0/0: audispd: t type=AVC
msg=audit(1699927198.486:130): avc: denied { write } for pid=6012 comm="echo"
path="/root/test" dev="rootfs" ino=25839
scontext=system_u:system_r:polaris_iosd_t:s0
tcontext=system_u:object_r:admin_home_t:s0 tclass=file permissive= 0
```

SELinux の有効化の確認

show platform software selinux コマンドを使用して、SELinux 設定モードを表示します。

```
Device# show platform software selinux
========================================
IOS-XE SELINUX STATUS
========================================
SElinux Status :    Enabled
Current Mode :      Enforcing
Config file Mode :  Enforcing
```

SELinux のトラブルシューティング

デバイスまたはネットワークで SELinux 違反のインスタンスがある場合は、次の詳細を Cisco TAC に連絡してください。

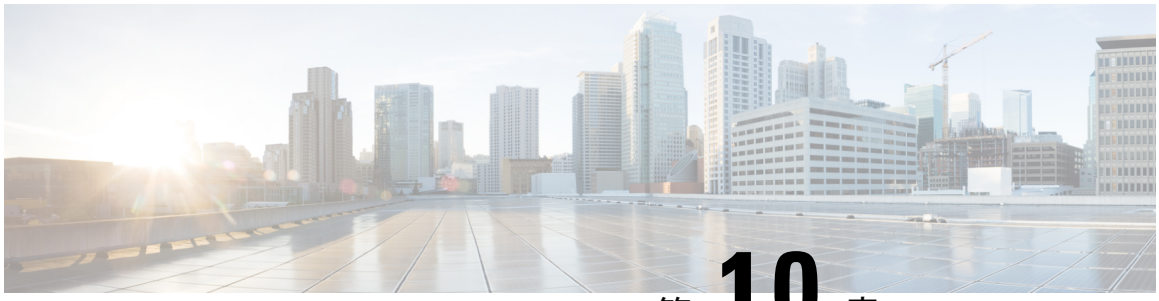
- コンソールまたはシステムログに出力されるとおりのメッセージ。次に例を示します。

```
device#request platform software trace archive target
    flash:selinux_btrace_logs
```

- **show tech-support** コマンドの出力（テキストファイル）
- ボックスからの Btrace ファイルのアーカイブ（次のコマンドを使用）：

  request platform software trace archive target <URL>

- **show platform software selinux** コマンドの出力



第 10 章

Cisco Thousand Eyes エンタープライズ エージェント アプリケーションのホスティング

この章では Cisco Thousand Eyes エンタープライズ エージェント アプリケーションのホスティングについて説明します。この章で説明する内容は、次のとおりです。

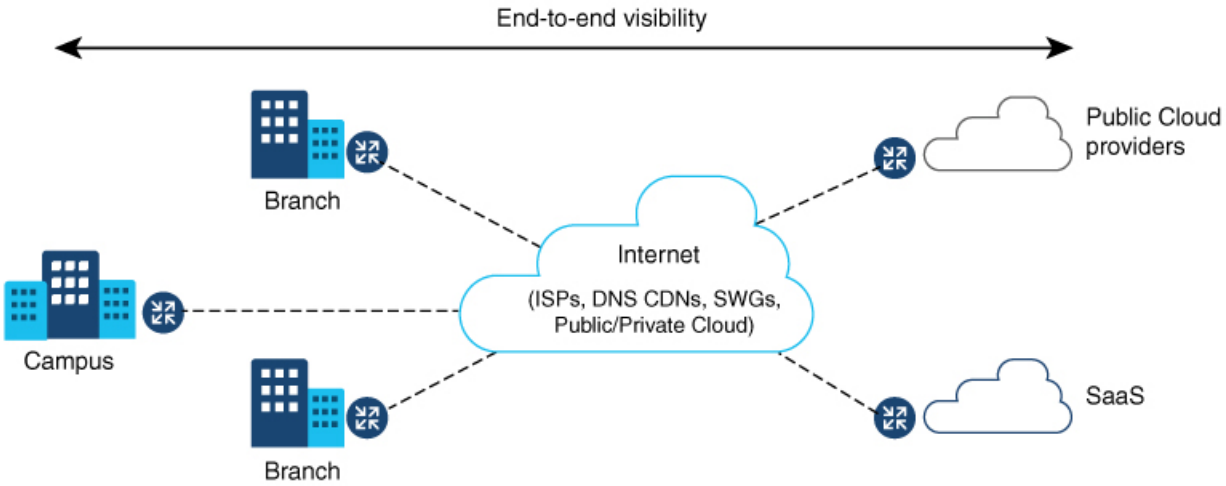
Cisco ThousandEyes エンタープライズ エージェント アプリケーションのホスティング

Cisco ThousandEyes は、ネットワーク インテリジェンス プラットフォームであり、エージェントを使用してさまざまなテストを実行し、ネットワークとアプリケーションのパフォーマンスをモニタできます。このアプリケーションを使用して、ビジネスに影響を及ぼすネットワークおよびサービス全体のエンドツーエンドパスを表示できます。Cisco ThousandEyes アプリケーションは、内部、外部、およびインターネットネットワークのネットワーク トラフィック パスをリアルタイムでアクティブにモニターし、ネットワークパフォーマンスの分析を支援します。また、Cisco ThousandEyes アプリケーションはルーティングとデバイスデータで強化されたアプリケーション可用性に関する分析情報を提供し、デジタルエクスペリエンスの多次元的な表示を可能にします。

Cisco IOS XE リリース 17.15.3a 以降、アプリケーション ホスティング機能を使用して、Cisco ThousandEyes Enterprise Agent をコンテナアプリケーションとして Cisco 8300 シリーズ セキュアルータに展開できます。このエージェント アプリケーションは、Cisco IOx docker-type オプ

ションを使用して docker イメージとして実行されます。コントローラモードで Cisco ThousandEyes を設定する方法の詳細については、『Cisco SD-WAN Systems and Interfaces Configuration Guide』を参照してください。

図 *1 : ThousandEyes* アプリケーションによるネットワークの表示



Cisco ThousandEyes Enterprise エージェント アプリケーションの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *14 : Cisco ThousandEyes Enterprise* エージェント アプリケーションの機能情報

機能名	リリース	機能情報
Cisco ThousandEyes Enterprise Agent アプリケーションのホスティング	Cisco IOS XE 17.15.3a	Cisco ThousandEyes Enterprise Agent アプリケーションには、デバイスからドメインネームサーバー（DNS）情報を継承する機能が導入されています。この機能強化により、vManage ThousandEyes 機能テンプレートの DNS フィールドはオプションのパラメータになりました。

機能名	リリース	機能情報
Cisco ThousandEyes Enterprise Agent アプリケーションのホスティング	Cisco IOS XE 17.15.3a	アプリケーション ホスティング機能をコンテナとして使用して、ルーティング プラットフォームで実行される ThousandEyes エージェント アプリケーションを統合することで、インターネット、クラウドプロバイダー、およびエンタープライズ ネットワークに関する詳細な分析情報を用いてアプリケーション エクスペリエンスを可視化できます。

サポートされるプラットフォームとシステム要件

次の表に、サポートされるプラットフォームとシステム要件を示します。

表 *15*：サポートされるプラットフォームとシステム要件

プラットフォーム	ブートフラッシュ	FRU ストレージ	DRAM
Cisco 8300 シリーズ セキュアルータ			
C8375-E-G2	16 GB	32 GB M.2 USB（デフォルト）	16 GB
C8355-G2	16 GB	32 GB M.2 USB（デフォルト）	16 GB

（注） Cisco ThousandEyes Enterprise Agent を実行するための最小 DRAM およびストレージの要件は 8 GB です。デバイスに十分なメモリまたはストレージがない場合は、DRAM をアップグレードするか、または M.2 USB などの外部ストレージを追加することをお勧めします。使用可能なリソースが他のアプリケーションを実行するのに十分でない場合、Cisco IOx はエラーメッセージを生成します。

Cisco ThousandEyes アプリケーションのインストールと実行のワークフロー

デバイスに Cisco ThousandEyes イメージをインストールして実行するには、次の手順を実行します。

手順

ステップ 1 Cisco ThousandEyes ポータルで新しいアカウントを作成します。

ステップ 2 ソフトウェアのダウンロードページから Cisco ThousandEyes アプリケーションパッケージをダウンロードし、エージェントバージョン 4.0.2 を使用していることを確認します。

ステップ 3 デバイスでイメージをコピーします。

ステップ 4 イメージをインストールして起動します。

ステップ 5 エージェントをコントローラに接続します。

（注）
Cisco IOS XE 17.15.3a ソフトウェアとともに Cisco ThousandEyes アプリケーションをサポートするプラットフォームを注文した場合、Cisco ThousandEyes アプリケーションパッケージはデバイスのブートフラッシュで使用できます。

Cisco ThousandEyes アプリケーションをホストするワークフロー

アプリケーションをインストールして起動するには、次の手順を実行します。

始める前に

Cisco ThousandEyes ポータルで新しいアカウントを作成し、トークンを生成します。Cisco ThousandEyes エージェント アプリケーションは、このトークンを使用して、正しい Cisco ThousandEyes アカウントを認証し、チェックインします。トークンが無効であるというメッセージが表示された場合に、その問題のトラブルシューティングを行うには、Cisco ThousandEyes アプリケーションのトラブルシューティング （155 ページ）を参照してください。

（注） 正しいトークンとドメインネームサーバー（DNS）情報を設定すると、デバイスが自動的に検出されます。

手順

ステップ 1 デバイスで Cisco IOx アプリケーション環境を有効にします。

- 非 SD-WAN（自立モード）イメージには次のコマンドを使用します。

```
config terminal
 iox
end
write
```

• SD-WAN（コントローラモード）イメージには次のコマンドを使用します。

```
config-transaction
iox
commit
```

ステップ 2 IOx コマンドが受け入れられる場合は、数秒間待機してから、**show iox** コマンドを使用して IOx プロセスが動作しているかどうかを確認します。出力に、show IOxman プロセスが実行中であると表示される必要があります。

```
Device #show iox

IOx Infrastructure Summary:
---------------------------
IOx service (CAF) 192.0.2.8     : Running
IOx service (HA)               : Not Supported
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Not Supported
Libvirtd 1.3.4                 : Running
```

ステップ 3 ThousandEyes アプリケーション LXC tarball がデバイスの *bootflash:* で使用可能であることを確認します。

ステップ 4 仮想ポート グループ インターフェイスを作成して、Cisco ThousandEyes アプリケーションへのトラフィックパスを有効にします。

```
interface VirtualPortGroup 0
          ip address 192.0.2.22 255.255.255.0
        exit
```

ステップ 5 生成されたトークンを使用して、アプリケーション ホスティング アプリケーションを設定します。

```
app-hosting appid te
          app-vnic gateway1 virtualportgroup 0 guest-interface 0
          guest-ipaddress 192.0.2.22 netmask 255.255.255.0
          app-default-gateway 192.0.2.22 guest-interface 0
          app-resource docker
             prepend-pkg-opts □ Required to get the default run-time options from package.yaml
             run-opts 1 "--hostname thousandeyes"
             run-opts 2 "-e TEAGENT_ACCOUNT_TOKEN=<ThousandEyes token>"
      run-opts 3 "-e TEAGENT_PROXY_TYPE=STATIC -e TEAGENT_PROXY_LOCATION=proxy.something.other:80"

          name-server0 192.0.2.10 □ ISP's DNS server
        end

app-hosting appid te
 app-resource docker
  prepend-pkg-opts
  run-opts 2 "--hostname
```

（注）
プロキシ設定は、Cisco ThousandEyes エージェントがプロキシなしでインターネットにアクセスできない場合にのみ使用できます。また、ホスト名はオプションです。インストール時にホスト名を指定しない場合、デバイスのホスト名が Cisco ThousandEyes エージェントのホスト名として使用されます。デバイスのホスト名が Cisco ThousandEyes ポータルに表示されます。DNS ネームサーバー情報はオプションです。Cisco ThousandEyes エージェントがプライベート IP アドレスを使用する場合は、NAT 経由でデバイスへの接続を確立します。

ステップ 6 **install** コマンドを使用してアプリケーションがデバイスにインストールされたときに、アプリケーションを自動的に実行するように **start** コマンドを設定します。

```
app-hosting appid te
         start
```

ステップ 7 ThousandEyes アプリケーションをインストールします。

```
app-hosting install appid <appid> package [bootflash: | harddisk: | https:]
```

次のオプションから ThousandEyes アプリケーションをインストールする場所を選択します。

```
Device# app-hosting install appid te package ?
           bootflash:  Package path □ ISR4K case if image is locally available in bootflash:
           harddisk:   Package path □ Cat8K case if image is locally available in M.2 USB
           https:      Package path □ Download over the internet if image is not locally present in
 router. URL to ThousandEyes site hosting agent image to be provided here
```

ステップ 8 アプリケーションが動作しているかどうかを確認します。

```
Device#show app-hosting list
 App id                                   State
---------------------------------------------------------
  te                                       RUNNING
```

（注）
これらの手順のいずれかに失敗した場合は、**show logging** コマンドを使用して IOx エラーメッセージを確認します。ディスク容量が不足しているというエラーメッセージが表示される場合は、ストレージメディア（ブートフラッシュまたはハードディスク）をクリーンアップして空き容量を増やします。**show app-hosting resource** コマンドを使用して、CPU とディスクメモリを確認します。

デバイスへのイメージのダウンロードとコピー

イメージをダウンロードしてブートフラッシュにコピーするには、次の手順を実行します。

手順

ステップ 1 Cisco ThousandEyes イメージが bootflash:/<directory name> に事前にコピーされているかどうかを確認します。

ステップ 2 デバイスのディレクトリにイメージがない場合は、次の手順を実行します。

a) デバイスがインターネットに直接アクセスできる場合は、**application install command.** コマンドで https:. オプションを使用します。このオプションにより、Cisco ThousandEyes ソフトウェアのダウンロードページから bootflash:/apps にイメージがダウンロードされ、アプリケーションがインストールされます。

```
Device# app-hosting install appid <appid string> package [bootflash: | flash | http | https://
  | ftp | ] URL to image location hosted on ThousandEyes portal
```

```
Device# app-hosting install appid te1000 package
https://downloads.thousandeyes.com/enterprise-agent/thousandeyes-enterprise-agent-4.0.2.cisco.tar

Installing package
'https://downloads.thousandeyes.com/enterprise-agent/thousandeyes-enterprise-agent-4.0.2.cisco.tar'
 for 'te1000'.

Use 'show app-hosting list' for progress.
*Jun 29 23:43:29.244: %IOSXE-6-PLATFORM: R0/0: IOx:  App verification successful
*Jun 29 23:45:00.449: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Install succeeded: te1000
installed successfully Current state is DEPLOYED
*Jun 29 23:45:01.801: %IOSXE-6-PLATFORM: R0/0: IOx:  App verification successful
*Jun 29 23:45:51.054: %IM-6-START_MSG: R0/0: ioxman: app-hosting: Start succeeded: te1000 started
 successfully Current state is RUNNING

Device#show app-hosting detail appid te1000  ( Details of Application)
App id                 : te1000
Owner                  : iox
State                  : RUNNING
Application
  Type                 : docker
  Name                 : ThousandEyes Enterprise Agent
  Version              : 4.0
  Author               : ThousandEyes <support@thousandeyes.com>
  Path                 : bootflash:thousandeyes-enterprise-agent-4.0-22.cisco.tar
Resource reservation
  Memory               : 500 MB
  Disk                 : 1 MB
  CPU                  : 1500 units
  CPU-percent          : 70 %
```

b) デバイスにプロキシサーバーがある場合は、イメージを bootflash:/apps に手動でコピーします。

c) ソフトウェアのダウンロードページから Cisco ThousandEyes アプリケーションパッケージをダウンロードし、エージェントバージョン 4.0.2 を使用していることを確認します。

d) bootflash: にアプリケーション ディレクトリを作成し、イメージをコピーします。

```
Device# mkdir bootflash:apps
Create directory filename [apps]?
Created dir bootflash:/apps
```

e) Cisco ThousandEyes イメージを *bootflash:apps* ディレクトリにコピーします。

f) **verify** コマンドを使用してイメージを検証します。

```
verify /md5 bootflash:apps/<file name>
```

Cisco ThousandEyes エージェントとコントローラの接続

始める前に

エージェントをコントローラに接続する前に、インターネットに接続していることを確認します。

手順

Cisco ThousandEyes アプリケーションが稼働状態になると、エージェント（ThousandEyes エージェント）プロセスがクラウド環境で実行されているコントローラに接続します。

（注）
接続に関連する問題がある場合、関連するエラーメッセージがアプリケーション固有のログ（*/var/logs*）に記録されます。

エージェントのパラメータの変更

エージェントのパラメータを変更するには、次のアクションを実行します。

手順

ステップ 1 **app-hosting stop appid appid** コマンドを使用して、アプリケーションを停止します。
ステップ 2 **app-hosting deactivate appid appid** コマンドを使用して、アプリケーションを非アクティブ化します。
ステップ 3 アプリケーション ホスティングの設定に必要な変更を加えます。
ステップ 4 **app-hosting activate appid appid** コマンドを使用して、アプリケーションをアクティブ化します。
ステップ 5 **app-hosting start appid appid**コマンドを使用して、アプリケーションを起動します。

アプリケーションのアンインストール

アプリケーションをアンインストールするには、次の手順を実行します。

手順

ステップ 1 **app-hosting stop appid te** コマンドを使用して、アプリケーションを停止します。
ステップ 2 **show app-hosting list** コマンドを使用して、アプリケーションがアクティブ状態であるかどうかを確認します。
ステップ 3 **app-hosting deactivate appid te** コマンドを使用して、アプリケーションを非アクティブ化します。
ステップ 4 アプリケーションがアクティブ状態でないことを確認します。**show app-hosting list** コマンドを使用して、アプリケーションのステータスを確認します。

ステップ 5 **app-hosting install appid te** コマンドを使用して、アプリケーションをアンインストールします。

ステップ 6 アンインストールプロセスが完了したら、**show app-hosting list** コマンドを使用して、アプリケーションが正常にアンインストールされたかどうかを確認します。

Cisco ThousandEyes アプリケーションのトラブルシューティング

Cisco ThousandEyes アプリケーションをトラブルシューティングするには、次の手順を実行します。

1. **app-hosting connect appid appid session /bin/bash** コマンドを使用して、Cisco ThousandEyes エージェント アプリケーションに接続します。
2. アプリケーション */etc/te-agent.cfg* に適用されている設定を確認します。
3. */var/log/agent/te-agent.log* のログを表示します。これらのログを使用して、設定のトラブルシューティングを行うことができます。

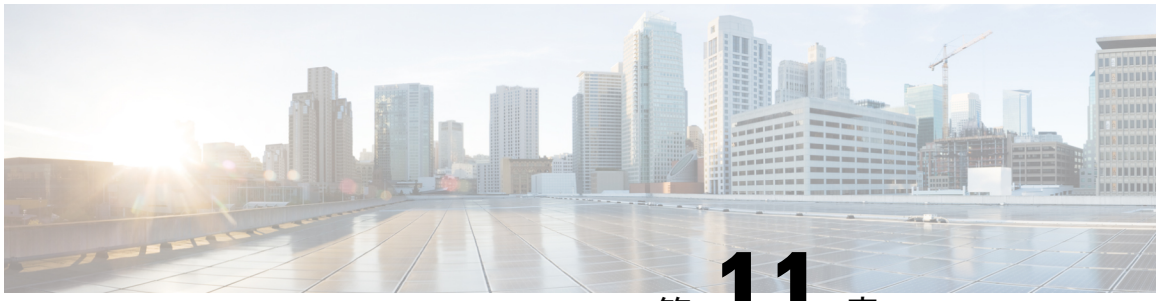
ThousandEyes アプリケーションのステータスの確認

Cisco ThousandEyes アプリケーションが実行状態の場合、ThousandEyes ポータルに登録されます。エージェントが実行状態になってから数分以内にアプリケーションが表示されない場合は、**app-hosting connect appid thousandeyes_enterprise_agent session** コマンドを使用して確認します。

```
Device#app-hosting connect appid thousandeyes_enterprise_agent session
Device# cat /var/log/agent/te-agent.log
2021-02-04 08:59:29.642 DEBUG [e4736a40] [te.agent.AptPackageInterface] {} Initialized
APT package interface
2021-02-04 08:59:29.642 INFO  [e4736a40] [te.agent.main] {} Agent version 1.103.0 starting.
  Max core size is 0 and max open files is 1024
2021-02-04 08:59:29.642 DEBUG [e4736a40] [te.agent.db] {} Vacuuming database
2021-02-04 08:59:29.643 INFO  [e4736a40] [te.agent.db] {} Found version 0, expected
version 50
2021-02-04 08:59:29.672 INFO  [e4708700] [te.probe.ServerTaskExecutor] {} ProbeTaskExecutor
 started with 2 threads.
2021-02-04 08:59:29.673 INFO  [e2f05700] [te.probe.ProbeTaskExecutor.bandwidth] {}
ProbeTaskExecutor started with 1 threads.
2021-02-04 08:59:29.673 INFO  [e2704700] [te.probe.ProbeTaskExecutor.realtime] {}
ProbeTaskExecutor started with 1 threads.
2021-02-04 08:59:29.673 INFO  [e1f03700] [te.probe.ProbeTaskExecutor.throughput] {}
ProbeTaskExecutor started with 1 threads.
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.agent.DnssecTaskProceessor] {} Agent is not
 running bind
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.snmp.RequestDispatcher] {} Initialised
SNMP++ session
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.snmp.RequestDispatcher] {} Initialised
SNMP++ session
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.snmp.RequestDispatcher] {} Initialised
SNMP++ session
2021-02-04 08:59:29.674 INFO  [e4736a40] [te.agent.main] {} Agent starting up
```

```
2021-02-04 08:59:29.675 INFO  [e4736a40] [te.agent.main] {} No agent id found, attempting
 to obtain one
2021-02-04 08:59:29.675 INFO  [e4736a40] [te.agent.ClusterMasterAdapter] {} Attempting
to get agent id from sc1.thousandeyes.com
2021-02-04 08:59:29.679 ERROR [e4736a40] [te.agent.main] {} Error calling create_agent:
 Curl error - Couldn't resolve host name
2021-02-04 08:59:29.680 INFO  [e4736a40] [te.agent.main] {} Sleeping for 30 seconds
Note :
```

（注） DNS サーバーの接続を確認します。Cisco ThousandEyes エージェントがプライベート IP アドレスに割り当てられている場合は、NAT 設定を確認します。



第 11 章

プロセス ヘルス モニタリング

この章では、デバイスの各種コンポーネントの正常性を管理および監視する方法について説明します。この章の内容は、次のとおりです。

コントロールプレーンのリソースの監視

ここでは、Cisco IOS プロセスとコントロール プレーン全体の観点から見たメモリおよび CPU の監視について説明します。

定期的な監視による問題の回避

プロセスを正しく動作させるには、プロセスのステータス/正常性を監視して通知する機能が必要です。プロセスに障害が発生すると、Syslog エラーメッセージが表示され、プロセスの再起動またはデバイスのリブートが実行されます。プロセスがスタックしているかクラッシュしたことをモニターが検出すると、syslog エラーメッセージが表示されます。プロセスが再起動可能な場合は再起動され、それ以外の場合はデバイスが再起動されます。

システム リソースの監視によって、起こり得る問題を発生前に検出できるため、システムの停止を回避できます。次に、定期的な監視のメリットを示します。

- 数年にわたって稼働しているラインカードのメモリ不足が原因で、大規模な停止が発生する可能性があります。メモリの使用状況を監視することで、ラインカードのメモリの問題を特定でき、停止を防止できます。

- 定期的な監視によって、正常なシステム負荷の基準が確立されます。ハードウェアやソフトウェアをアップグレードした時に、この情報を比較の根拠として使用し、アップグレードがリソースの使用率に影響を与えたかどうかを確認できます。

Cisco IOS プロセスのリソース

アクティブ プロセスの CPU 使用率統計情報を表示し、これらのプロセスで使用されているメモリの容量を確認するには、**show memory** コマンドと **show process cpu** コマンドを使用できます。これらのコマンドは、Cisco IOS プロセスのみのメモリと CPU の使用状況を示します。プラットフォーム全体のリソースに関する情報は含まれません。たとえば、8 GB RAM を搭載し、1 つの Cisco IOS プロセスを実行しているシステムで **show memory** コマンドを実行すると、次のメモリ使用状況が表示されます。

```
Router# show memory
Tracekey : 1#cb0b8989b15e46da15c7630297789582

                                                                                Head
   Total(b)     Used(b)     Free(b)   Lowest(b)  Largest(b)

Processor  FFFF59A6B048   20578847040   289787696   20289059344   655646464   19922943908
reserve P  FFFF59A6B0A0      102404          92      102312      102312      102312
lsmpi_io  FFFF434FA1A8     6295128     6294304         824         824         412
Dynamic heap limit(MB) 19000     Use(MB) 0
```

show process cpu コマンドは、Cisco IOS CPU の平均使用率を次のように表示します。

```
Router# show process cpu
CPU utilization for five seconds: 1%/0%; one minute: 1%; five minutes: 1%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           1          14         71  0.00%  0.00%  0.00%   0 Chunk Manager
   2         127         872        145  0.00%  0.00%  0.00%   0 Load Meter
   3           0           1          0  0.00%  0.00%  0.00%   0 Policy bind Proc
   4           0           1          0  0.00%  0.00%  0.00%   0 Retransmission o
   5           0           1          0  0.00%  0.00%  0.00%   0 IPC ISSU Dispatc
   6          11          13        846  0.00%  0.00%  0.00%   0 RF Slave Main Th
   7           0           1          0  0.00%  0.00%  0.00%   0 EDDRI_MAIN
   8           0           1          0  0.00%  0.00%  0.00%   0 RO Notify Timers
   9        1092         597       1829  0.00%  0.01%  0.00%   0 Check heaps
  10           8          73        109  0.00%  0.00%  0.00%   0 Pool Manager
  11           0           1          0  0.00%  0.00%  0.00%   0 DiscardQ Backgro
  12           0           2          0  0.00%  0.00%  0.00%   0 Timers
  13           0          32          0  0.00%  0.00%  0.00%   0 WATCH_AFS
  14           0           1          0  0.00%  0.00%  0.00%   0 MEMLEAK PROCESS
  15        1227       40758         30  0.00%  0.02%  0.00%   0 ARP Input
  16          41        4568          8  0.00%  0.00%  0.00%   0 ARP Background
  17           0           2          0  0.00%  0.00%  0.00%   0 ATM Idle Timer
  18           0           1          0  0.00%  0.00%  0.00%   0 ATM ASYNC PROC
  19           0           1          0  0.00%  0.00%  0.00%   0 CEF MIB API
  20           0           1          0  0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
  21           0           1          0  0.00%  0.00%  0.00%   0 Policy Manager
  22           0           2          0  0.00%  0.00%  0.00%   0 DDR Timers
  23          60          23       2608  0.00%  0.00%  0.00%   0 Entity MIB API
  24          43          45        955  0.00%  0.00%  0.00%   0 PrstVbl
  25           0           2          0  0.00%  0.00%  0.00%   0 Serial Backgroun
  26           0           1          0  0.00%  0.00%  0.00%   0 RMI RM Notify Wa
  27           0           2          0  0.00%  0.00%  0.00%   0 ATM AutoVC Perio
  28           0           2          0  0.00%  0.00%  0.00%   0 ATM VC Auto Crea
  29          30        2181         13  0.00%  0.00%  0.00%   0 IOSXE heartbeat
```

```
 30           1           9         111  0.00%  0.00%  0.00%   0 Btrace time base
 31           5         182          27  0.00%  0.00%  0.00%   0 DB Lock Manager
 32          16        4356           3  0.00%  0.00%  0.00%   0 GraphIt
 33           0           1           0  0.00%  0.00%  0.00%   0 DB Notification
 34           0           1           0  0.00%  0.00%  0.00%   0 IPC Apps Task
 35           0           1           0  0.00%  0.00%  0.00%   0 ifIndex Receive
 36           4         873           4  0.00%  0.00%  0.00%   0 IPC Event Notifi
 37          49        4259          11  0.00%  0.00%  0.00%   0 IPC Mcast Pendin
 38           0           1           0  0.00%  0.00%  0.00%   0 Platform appsess
 39           2          73          27  0.00%  0.00%  0.00%   0 IPC Dynamic Cach
 40           5         873           5  0.00%  0.00%  0.00%   0 IPC Service NonC
 41           0           1           0  0.00%  0.00%  0.00%   0 IPC Zone Manager
 42          38        4259           8  0.00%  0.00%  0.00%   0 IPC Periodic Tim
 43          18        4259           4  0.00%  0.00%  0.00%   0 IPC Deferred Por
 44           0           1           0  0.00%  0.00%  0.00%   0 IPC Process leve
 45           0           1           0  0.00%  0.00%  0.00%   0 IPC Seat Manager
 46           3         250          12  0.00%  0.00%  0.00%   0 IPC Check Queue
 47           0           1           0  0.00%  0.00%  0.00%   0 IPC Seat RX Cont
 48           0           1           0  0.00%  0.00%  0.00%   0 IPC Seat TX Cont
 49          22         437          50  0.00%  0.00%  0.00%   0 IPC Keep Alive M
 50          25         873          28  0.00%  0.00%  0.00%   0 IPC Loadometer
 51           0           1           0  0.00%  0.00%  0.00%   0 IPC Session Deta
 52           0           1           0  0.00%  0.00%  0.00%   0 SENSOR-MGR event
 53           2         437           4  0.00%  0.00%  0.00%   0 Compute SRP rate
```

コントロール プレーン全体のリソース

各コントロール プロセッサのコントロール プレーンのメモリおよび CPU の使用状況により、コントロール プレーン全体のリソースを管理できます。**show platform resources** コマンドを使用すると、IOS XE プラットフォームの全体的なシステムの正常性とリソース使用率をモニタできます。また、コントロールプレーンのメモリと CPU の使用状況についての情報を表示するには、**show platform software status control-processor brief** コマンド（サマリービュー）または **show platform software status control-processor** コマンド（詳細ビュー）を使用できます。

すべてのコントロール プロセッサのステータスとして [Healthy] が表示されるのが正常です。他に表示されうるステータスの値は、[Warning] と [Critical] です。[Warning] は、デバイスが動作中であるものの、動作レベルの確認が必要であることを示しています。[Critical] は、デバイスで障害が発生する可能性が高いことを示しています。

[Warning] または [Critical] ステータスが表示されたら、次の対処方法に従ってください。

- 設定内の要素の数を減らすか、動的なサービスの容量を制限して、システムに対する静的および動的な負荷を減らします。
- ルータと隣接機器の数を減らしたり、ACL などのルールの数を制限したり、VLAN の数を減らしたりなどの対処を行います。

ここでは、**show platform software status control-processor** コマンドの出力のフィールドについて説明します。

Load Average

[Load Average] は、CPU リソースのプロセス キューまたはプロセス コンテンションを示します。たとえば、シングルコアプロセッサで瞬間的な負荷が 7 の場合は、7 つのプロセスが実行可能な状態になっていて、そのうちの 1 つが現在実行中という意味です。デュアルコアプロ

セッサで負荷が 7 となっている場合、7 つのプロセスが実行可能な状態になっていて、そのうちの 2 つが現在実行中であることを示します。

Memory Utilization

[Memory Utilization] は次のフィールドで示されます。

- Total：ラインカードの合計メモリ
- Used：使用済みメモリ
- Free：使用可能なメモリ
- Committed：プロセスに割り当てられている仮想メモリ

CPU Utilization

[CPU Utilization] は CPU が使用されている時間の割合を表すもので、次のフィールドで示されます。

- CPU：割り当て済みプロセッサ
- User：Linux カーネル以外のプロセス
- System：Linux カーネルのプロセス
- Nice：プライオリティの低いプロセス
- Idle：CPU が非アクティブだった時間の割合
- IRQ：割り込み
- SIRQ：システムの割り込み
- IOwait：CPU が入出力を待っていた時間の割合

例：**show platform software status control-processor** コマンド

次に **show platform software status control-processor** コマンドのいくつかの使用例を示します。

```
Router# show platform software status control-processor
RP0: online, statistics updated 3 seconds ago
RP0: online, statistics updated 5 seconds ago
Load Average: healthy
  1-Min: 1.35, status: healthy, under 9.30
  5-Min: 1.06, status: healthy, under 9.30
  15-Min: 1.02, status: healthy, under 9.30
Memory (kb): healthy
  Total: 7768456
  Used: 2572568 (33%), status: healthy
  Free: 5195888 (67%)
  Committed: 3112968 (40%), under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  3.00, System:  2.40, Nice:  0.00, Idle: 94.60
```

```
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  0.00, System:  0.00, Nice:  0.00, Idle:100.00
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  0.00, System:  0.00, Nice:  0.00, Idle:100.00
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  0.00, System:  0.00, Nice:  0.00, Idle:100.00
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU4: CPU Utilization (percentage of time spent)
  User:  7.30, System:  1.70, Nice:  0.00, Idle: 91.00
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU5: CPU Utilization (percentage of time spent)
  User:  3.30, System:  1.50, Nice:  0.00, Idle: 95.20
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU6: CPU Utilization (percentage of time spent)
  User: 17.91, System: 11.81, Nice:  0.00, Idle: 70.27
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU7: CPU Utilization (percentage of time spent)
  User: 11.91, System: 13.31, Nice:  0.00, Idle: 74.77
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU8: CPU Utilization (percentage of time spent)
  User:  2.70, System:  2.00, Nice:  0.00, Idle: 95.30
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU9: CPU Utilization (percentage of time spent)
  User:  0.00, System:  0.00, Nice:  0.00, Idle:100.00
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU10: CPU Utilization (percentage of time spent)
  User:  0.00, System:  0.00, Nice:  0.00, Idle:100.00
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU11: CPU Utilization (percentage of time spent)
  User:  0.00, System:  0.00, Nice:  0.00, Idle:100.00
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
```

```
Router# show platform software status control-processor brief
Load Average
 Slot  Status  1-Min  5-Min 15-Min
  RP0 Healthy   1.14   1.07   1.02

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
  RP0 Healthy  7768456  2573416 (33%)  5195040 (67%)   3115096 (40%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
  RP0    0   2.80   1.80   0.00  95.39   0.00   0.00   0.00
         1   0.00   0.00   0.00 100.00   0.00   0.00   0.00
         2   0.00   0.00   0.00 100.00   0.00   0.00   0.00
         3   0.00   0.00   0.00 100.00   0.00   0.00   0.00
         4   6.80   1.80   0.00  91.39   0.00   0.00   0.00
         5   3.20   1.60   0.00  95.19   0.00   0.00   0.00
         6  16.30  12.60   0.00  71.10   0.00   0.00   0.00
         7  12.40  13.70   0.00  73.90   0.00   0.00   0.00
         8   2.40   2.40   0.00  95.19   0.00   0.00   0.00
         9   0.00   0.00   0.00 100.00   0.00   0.00   0.00
        10   0.00   0.00   0.00 100.00   0.00   0.00   0.00
        11   0.00   0.00   0.00 100.00   0.00   0.00   0.00
```

アラームを使用したハードウェアの監視

デバイスの設計とハードウェアの監視

問題が検出されるとルータからアラーム通知が送信されます。これにより、ネットワークをリモートで監視できます。**show** コマンドを使用してデバイスを定期的にポーリングする必要はありませんが、必要に応じてオンサイト モニタリングを実行できます。

ブートフラッシュディスクの監視

ブートフラッシュディスクには、2つのコアダンプを保存できる十分な空き領域が必要です。この条件が監視されて、ブートフラッシュディスクが2つのコアダンプを保存するには小さすぎる場合には、次の例に示すような SYSlog アラームが生成されます。

```
Aug 22 13:40:41.038 R0/0: %FLASH_CHECK-3-DISK_QUOTA: Flash disk quota exceeded
[free space is 7084440 kB] - Please clean up files on bootflash.
```

ブートフラッシュディスクのサイズは、少なくともデバイスに搭載されている物理メモリと同じサイズでなければなりません。この条件を満たしていない場合、次の例に示すようなSYSlogアラームが生成されます。

```
%IOSXEBOOT-2-FLASH_SIZE_CHECK: (rp/0): Flash capacity (8 GB) is insufficient for fault
analysis based on
installed memory of RP (16 GB)
%IOSXEBOOT-2-FLASH_SIZE_CHECK: (rp/0): Please increase the size of installed flash to
at least 16 GB (same as
physical memory size)
```

ハードウェアアラームの監視方法

オンサイトのネットワーク管理者が可聴アラームまたは可視アラームに対応する

可聴アラームと可視アラームについて

電源モジュールの DB-25 アラーム コネクタを使用することにより、外部デバイスを電源モジュールに接続できます。外部デバイスは視覚アラーム用 DC 電球または聴覚アラーム用ベルです。

デバイスの前面プレートにあるCRIT、MIN、またはMAJのいずれかのLEDがアラームによって点灯する場合、可視アラームまたは可聴アラームが有線接続されていると、アラームによって電源DB-25コネクタのアラームリレーも作動し、ベルが鳴るか、または電球が点滅します。

可聴アラームの解除

可聴アラームを解除するには、次のいずれかの操作を実行します。

- 前面プレートの **Audible Cut Off** ボタンを押す
- **clear facility-alarm** コマンドを入力する

可視アラームの解除

視覚アラームを解除するには、アラーム条件を解決する必要があります。**clear facility-alarm** コマンドを入力しても、前面プレートのアラームLEDの解除やDC電球の消灯はできません。たとえば、アクティブなモジュールをグレースフルに非アクティブ化せずに取り外したためにクリティカル アラーム LED が点灯した場合、このアラームを解決する唯一の方法はモジュールを再度取り付けることです。

コンソールまたは syslog でのアラームメッセージの確認

ネットワーク管理者は、システム コンソールまたはシステム メッセージ ログ（syslog）に送信されるアラーム メッセージを確認することにより、アラーム メッセージを監視できます。

logging alarm コマンドの有効化

アラーム メッセージをコンソールや syslog などのロギング デバイスに送信するには、**logging alarm** コマンドを有効にする必要があります。このコマンドはデフォルトでは無効になっています。

ログに記録されるアラームの重大度レベルを指定できます。指定したしきい値以上のアラームが発生するたびに、アラーム メッセージが生成されます。たとえば、次のコマンドではクリティカル アラーム メッセージだけがロギング デバイスに送信されます。

```
Router(config)# logging alarm critical
```

アラームの重大度を指定しない場合、すべての重大度のレベルのアラーム メッセージがロギング デバイスに送信されます。

アラームメッセージの例

正しい非アクティブ化の実行前にモジュールが取り外された場合にコンソールに送信されるアラーム メッセージの例を、次に示します。モジュールを再び装着すると、アラームは消去されます。

モジュールが削除されました

```
*Aug 22 13:27:33.774: %C-SM-X-16G4M2X: Module removed from subslot 1/1, interfaces
disabled
*Aug 22 13:27:33.775: %SPA_OIR-6-OFFLINECARD: Module (SPA-4XT-SERIAL) offline in subslot
 1/1
```

モジュールが再び装着された場合

```
*Aug 22 13:32:29.447: %CC-SM-X-16G4M2X: Module inserted in subslot 1/1
*Aug 22 13:32:34.916: %SPA_OIR-6-ONLINECARD: Module (SPA-4XT-SERIAL) online in subslot
1/1
*Aug 22 13:32:35.523: %LINK-3-UPDOWN: SIP1/1: Interface EOBC1/1, changed state to up
```

アラーム

アラームを表示するには、**show facility-alarm status** コマンドを使用します。電源のクリティカルアラームの例を次に示します。

```
Router# show facility-alarm status
System Totals  Critical: 1  Major: 0  Minor: 0

Source                    Time                  Severity      Description [Index]
------                    ------                --------      -------------------

Power Supply Bay 1        Jul 08 2020 11:51:34  CRITICAL      Power Supply/FAN Module
 Missing [0]

POE Bay 0                 Jul 08 2020 11:51:34  INFO          Power Over Ethernet
Module Missing [0]

POE Bay 1                 Jul 08 2020 11:51:34  INFO          Power Over Ethernet
Module Missing [0]

xcvr container 0/0/4      Jul 08 2020 11:51:47  INFO          Transceiver Missing -
Link Down [1]

TenGigabitEthernet0/1/0   Jul 08 2020 11:52:24  INFO          Physical Port
Administrative State Down [2]

GigabitEthernet1/0/0      Jul 08 2020 11:56:35  INFO          Physical Port
Administrative State Down [2]

GigabitEthernet1/0/1      Jul 08 2020 11:56:35  INFO          Physical Port
Administrative State Down [2]

GigabitEthernet1/0/2      Jul 08 2020 11:56:35  INFO          Physical Port
Administrative State Down [2]
```

```
GigabitEthernet1/0/3       Jul 08 2020 11:56:35   INFO          Physical Port
Administrative State Down [2]

GigabitEthernet1/0/4       Jul 08 2020 11:56:35   INFO          Physical Port
Administrative State Down [2]

GigabitEthernet1/0/5       Jul 08 2020 11:56:35   INFO          Physical Port
Administrative State Down [2]

GigabitEthernet1/0/6       Jul 08 2020 11:56:35   INFO          Physical Port
Administrative State Down [2]

GigabitEthernet1/0/7       Jul 08 2020 11:56:35   INFO          Physical Port
Administrative State Down [2]

TwoGigabitEthernet1/0/17   Jul 08 2020 11:56:35   INFO          Physical Port
Administrative State Down [2]

TwoGigabitEthernet1/0/18   Jul 08 2020 11:56:35   INFO          Physical Port
Administrative State Down [2]

TwoGigabitEthernet1/0/19   Jul 08 2020 11:56:35   INFO          Physical Port
Administrative State Down [2]
```

クリティカルアラームを表示するには、次の例に示すように **show facility-alarm status critical** コマンドを使用します。

```
Router# show facility-alarm status critical
System Totals  Critical: 1  Major: 0  Minor: 0

Source                     Time                   Severity      Description [Index]
------                     ------                 --------      -------------------

Power Supply Bay 1         Jul 08 2020 11:51:34   CRITICAL      Power Supply/FAN Module
 Missing [0]
```

デバイスの主要ハードウェアコンポーネントの動作状態を表示するには、**show platform diag** コマンドを使用します。

```
Router# show platform diag
Slot: 0, C8375-E-G2
Running state               : ok
Internal state              : online
Internal operational state  : ok
Physical insert detect time : 00:00:23 (2d01h ago)
Software declared up time   : 00:01:07 (2d01h ago)
CPLD version                : 25033132
Firmware version            : v17.15(3.1r).s2.cp
Sub-slot: 0/0, 4M-2xSFP+
Operational status          : ok
Internal state              : inserted
Physical insert detect time : 00:01:17 (2d01h ago)
Logical insert detect time  : 00:01:17 (2d01h ago)
Sub-slot: 0/1, C-NIM-8M
Operational status          : ok
Internal state              : inserted
Physical insert detect time : 00:01:17 (2d01h ago)
Logical insert detect time  : 00:01:17 (2d01h ago)
Slot: 1, C8375-E-G2
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:00:23 (2d01h ago)
```

```
  Software declared up time   : 00:01:13 (2d01h ago)
  CPLD version                : 25033132

  Firmware version            : v17.15(3.1r).s2.cp

                                                                Slot: R0, C8375-E-G2


  Running state               : ok, active

  Internal state              : online

  Internal operational state  : ok

  Physical insert detect time : 00:00:23 (2d01h ago)

  Software declared up time   : 00:00:23 (2d01h ago)

  CPLD version                : 25033132

  Firmware version            : v17.15(3.1r).s2.cp

                                                                Slot: F0, C8375-E-G2
  Running state               : ok, active
  Internal state              : online

  Internal operational state  : ok
  Physical insert detect time : 00:00:23 (2d01h ago)
  Software declared up time   : 00:01:00 (2d01h ago)

  Hardware ready signal time  : 00:00:58 (2d01h ago)
  Packet ready signal time    : 00:01:13 (2d01h ago)

  CPLD version                : 25033132
  Firmware version            : v17.15(3.1r).s2.cp

Slot: P0, PWR-CC1-760WAC
  State                       : fail, badinput
  Physical insert detect time : 00:00:01 (2d01h ago)
Slot: P1, PWR-CC1-400WAC
  State                       : ok
  Physical insert detect time : 00:00:01 (2d01h ago)
  Slot: P2, C8300-FAN-1R
  State                       : ok
  Physical insert detect time : 00:00:02 (2d01h ago)
  Slot: POE0, PWR-CC1-760WAC
  State                       : fail, badinput

  Physical insert detect time : 00:00:01 (2d01h ago)
  Slot: POE1, Unknown
  State                       : empty
  Physical insert detect time : 00:00:00 (never ago)
```

アラーム メッセージの確認と分析

アラームメッセージの確認を容易にするために、コンソールまたはsyslogに送信されたアラームメッセージを分析するスクリプトを作成できます。スクリプトは、アラーム、セキュリティの警告、インターフェイスのステータスなどのイベントに関するレポートを表示できます。

syslog メッセージも、CISCO-SYSLOG-MIB に定義されている履歴表を使用して、簡易ネットワーク管理プロトコル（SNMP）経由でアクセスできます。

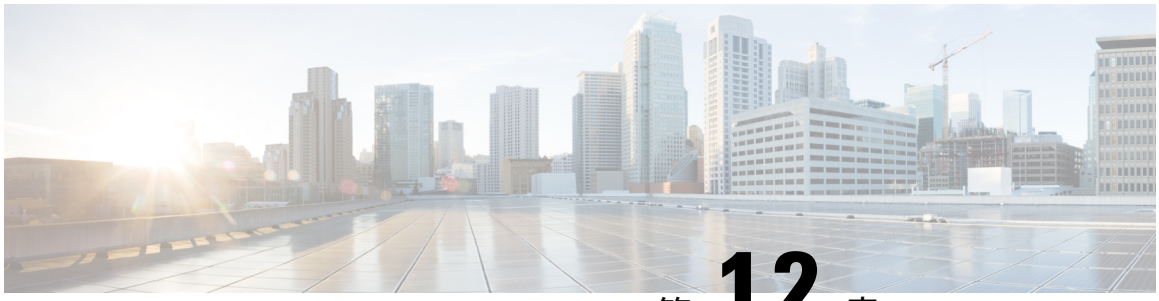
SNMP を介して報告されるアラーム

アプリケーション層プロトコルであるSNMPは、ネットワーク内のデバイスを監視および管理するための、標準化されたフレームワークと共通の言語を提供します。アラームを監視するすべての方法の中で、SNMPは、企業とサービスプロバイダーのセットアップで複数のデバイスを監視するための最適な方法です。

SNMPは、サービスに影響を及ぼす可能性のある障害、アラーム、状況を通知します。これにより、ネットワーク管理者は、ログの確認、デバイスのポーリング、ログレポートの確認を行う代わりに、ネットワーク管理システム（NMS）経由でデバイス情報を入手できます。

SNMP を使用してアラーム通知を取得するには、次の MIB を使用します。

- ENTITY-MIB, RFC 4133（CISCO-ENTITY-ALARM-MIB およびCISCO-ENTITY-SENSOR-MIB の稼働に必要）
- CISCO-ENTITY-ALARM-MIB
- CISCO-ENTITY-SENSOR-MIB（トランシーバ環境アラーム情報用。この情報は CISCO-ENTITY-ALARM-MIB では提供されません）



第 12 章

システム メッセージ

システム メッセージは、ログ ファイルに保存されるか、またはルータで実行中のソフトウェアから他のデバイスに転送されます。これらのメッセージは syslog メッセージとも呼ばれます。システム メッセージは、監視およびトラブルシューティングのためのロギング情報を提供します。

この章の内容は、次のとおりです。

プロセス管理

Telnet プロトコルを使ってコンソールにログインし、Telnet プロトコルをサポートする任意のワークステーションからシステム コンポーネントを監視することで、システム メッセージを確認できます。

ソフトウェアの開始と監視は、プロセス管理と呼ばれます。ルータのプロセス管理インフラストラクチャはプラットフォームに依存しないため、Cisco IOS XE が稼働するプラットフォーム全体でエラー メッセージが一貫しています。ユーザがプロセス管理に直接関与する必要はありませんが、プロセス障害などの問題を示すシステム メッセージを確認することをお勧めします。

エラーメッセージの詳細の検索方法

プロセス管理または Syslog エラーメッセージの詳細については、『System Error Messages Guide For Access and Edge Routers Guide』を参照してください。

エラーメッセージに表示される説明と推奨処置の例を以下に示します。

エラー メッセージ：`%PMAN-0-PROCESS_NOTIFICATION : The process lifecycle notification component failed because [chars]`

説明	推奨処置

プロセス ライフサイクル通知コンポーネントで障害が発生し、これが原因でプロセスの開始と停止を適切に検出できません。この問題は、ソフトウェア サブパッケージでのソフトウェアの不具合が原因で発生する可能性があります。	メッセージの時刻を書きとめ、カーネルエラーメッセージログを調べて問題の詳細を理解し、エラーが修正可能かどうかを確認してください。問題を解決できない場合、またはログが有用ではない場合は、コンソールに出力されたエラー メッセージ全体と、**show tech-support** コマンドの出力をそのままコピーし、収集した情報をシスコのテクニカル サポートに提出してください。

エラー メッセージ：`%PMAN-0-PROCFAILCRIT A critical process [chars] has failed (rc [dec])`

説明	推奨処置
ルータが機能するために必要な、重要なプロセスが失敗しました。	メッセージの時刻を書きとめ、エラーメッセージ ログを調査して、問題の詳細について理解してください。問題が解消されない場合は、コンソールまたはシステム ログに出力されたメッセージをそのままコピーします。http://www.cisco.com/tac で提供されているツールやユーティリティを使用して問題を調べ、解決してください。ツールやユーティリティのメッセージによって明確な情報が得られます。解決済みのソフトウェアの問題を検索するには、Bug Search Tool（http://www.cisco.com/cisco/psn/bssprt/bss）を使用します。さらに支援が必要な場合は、http://tools.cisco.com/ServiceRequestTool/create/ にアクセスして Technical Assistance Center でケースをオープンするか、シスコのテクニカルサポート担当者に問い合わせて、収集した情報を提出してください。**show logging** コマンドおよび **show tech-support** コマンドの出力結果および関連するトラブルシューティング ログを、提出する情報に、プレーンテキスト（.txt）形式で圧縮せずに添付してください。

エラー メッセージ：`%PMAN-3-PROCFAILOPT An optional process [chars] has failed (rc [dec])`

説明	推奨処置

トラフィックの転送に影響しないプロセスで、障害が発生しました。	メッセージの時刻を書きとめ、カーネルエラーメッセージ ログを調査して、問題の詳細について理解してください。このメッセージの受信後もトラフィックは引き続き転送されますが、このメッセージが原因でルータの一部の機能が無効になる可能性があるため、エラーを調査する必要があります。ログが有用ではないか、そこに示されている問題を解決できない場合は、コンソールまたはシステム ログに出力されたメッセージをそのままコピーします。http://www.cisco.com/tac で提供されているツールやユーティリティを使用して問題を調べ、解決してください。ツールやユーティリティのメッセージによって明確な情報が得られます。解決済みのソフトウェアの問題を検索するには、Bug Search Tool（http://www.cisco.com/cisco/psn/bssprt/bss）を使用します。さらに支援が必要な場合は、http://tools.cisco.com/ServiceRequestTool/create/ にアクセスして Technical Assistance Center でケースをオープンするか、シスコのテクニカルサポート担当者に問い合わせて、収集した情報を提出してください。**show logging** コマンドおよび **show tech-support** コマンドの出力結果および関連するトラブルシューティング ログを、提出する情報に、プレーンテキスト（.txt）形式で圧縮せずに添付してください。

エラー メッセージ：`%PMAN-3-PROCFAIL The process [chars] has failed (rc [dec])`

説明	推奨処置

エラーが発生したためにプロセスが失敗しました。	このメッセージは、プロセスに関連する他のメッセージとともに表示されます。他のメッセージを調べて失敗の理由を判別し、修正処置を実行できるかどうかを確認します。問題が解消されない場合は、コンソールまたはシステム ログに出力されたメッセージをそのままコピーします。http://www.cisco.com/tac で提供されているツールやユーティリティを使用して問題を調べ、解決してください。ツールやユーティリティのメッセージによって明確な情報が得られます。解決済みのソフトウェアの問題を検索するには、Bug Search Tool（http://www.cisco.com/cisco/psn/bssprt/bss）を使用します。さらに支援が必要な場合は、http://tools.cisco.com/ServiceRequestTool/create/ にアクセスして Technical Assistance Center でケースをオープンするか、シスコのテクニカルサポート担当者に問い合わせて、収集した情報を提出してください。**show logging** コマンドおよび **show tech-support** コマンドの出力結果および関連するトラブルシューティング ログを、提出する情報に、プレーンテキスト（.txt）形式で圧縮せずに添付してください。

エラー メッセージ：`%PMAN-3-PROCFAIL_IGNORE [chars] process exits and failures are being ignored due to debug settings. Normal router functionality will be affected. Critical router functions like RP switchover, router reload, FRU resets, etc. may not function properly.`

説明	推奨処置
ユーザにより設定されたデバッグ設定のため、プロセス障害は無視されます。	この動作が意図されたものであり、ユーザの設定に基づいてデバッグ設定が行われている場合、対処は不要です。このメッセージが表示されることが問題であると判断される場合は、デバッグ設定を変更します。このデバッグ設定では通常、ルータは正常に動作しません。SSO スイッチオーバー、ルータのリロード、FRU リセットなどの機能が影響を受けます。この設定は、デバッグを実行する場合にだけ使用してください。通常は、この設定でルータを動作させることはありません。

エラー メッセージ：`%PMAN-3-PROCHOLDDOWN The process [chars] has been helddown (rc [dec])`

説明	推奨処置

繰り返し発生する障害に伴って行われたプロセス再起動の回数が多すぎるため、ホールドダウン状態になりました。	このメッセージは、プロセスに関連する他のメッセージとともに表示されます。他のメッセージを調べて失敗の理由を判別し、修正処置を実行できるかどうかを確認します。問題が解消されない場合は、コンソールまたはシステム ログに出力されたメッセージをそのままコピーします。http://www.cisco.com/tac で提供されているツールやユーティリティを使用して問題を調べ、解決してください。ツールやユーティリティのメッセージによって明確な情報が得られます。解決済みのソフトウェアの問題を検索するには、Bug Search Tool（http://www.cisco.com/cisco/psn/bssprt/bss）を使用します。さらに支援が必要な場合は、http://tools.cisco.com/ServiceRequestTool/create/ にアクセスして Technical Assistance Center でケースをオープンするか、シスコのテクニカルサポート担当者に問い合わせて、収集した情報を提出してください。**show logging** コマンドおよび **show tech-support** コマンドの出力結果および関連するトラブルシューティング ログを、提出する情報に、プレーンテキスト（.txt）形式で圧縮せずに添付してください。

エラー メッセージ：`%PMAN-3-RELOAD_RP_SB_NOT_READY : Reloading: [chars]`

説明	推奨処置
準備のできたスタンバイ インスタンスがないため、ルート プロセッサがリロードされています。	リロードが、エラー状態に起因するものではないことを確認してください。

エラー メッセージ：`%PMAN-3-RELOAD_RP : Reloading: [chars]`

説明	推奨処置
RP がリロードされています。	リロードが、エラー状態に起因するものではないことを確認してください。エラー状態に起因している場合は、他のログ メッセージで要求されている情報を収集します。

エラー メッセージ：`%PMAN-3-RELOAD_SYSTEM : Reloading: [chars]`

説明	推奨処置

システムがリロードされています。	リロードが、エラー状態に起因するものではないことを確認してください。エラー状態に起因している場合は、他のログ メッセージで要求されている情報を収集します。

エラー メッセージ：`%PMAN-3-PROC_BAD_EXECUTABLE : Bad executable or permission problem with process [chars]`

説明	推奨処置
プロセスで使用される実行可能ファイルに問題があるか、またはアクセス許可に関する問題があります。	示されている実行可能ファイルを正しい実行可能ファイルに置き換えます。

エラー メッセージ：`%PMAN-3-PROC_BAD_COMMAND:Non-existent executable or bad library used for process <process name>`

説明	推奨処置
プロセスで使用される実行可能ファイルが存在していないか、または依存ライブラリに問題があります。	示されている実行可能ファイルが存在しており、依存ライブラリに問題がないことを確認します。

エラー メッセージ：`%PMAN-3-PROC_EMPTY_EXEC_FILE : Empty executable used for process [chars]`

説明	推奨処置
プロセスで使用される実行可能ファイルが空です。	示されている実行可能ファイルのサイズがゼロではないことを確認します。

エラー メッセージ：`%PMAN-5-EXITACTION : Process manager is exiting: [chars]`

説明	推奨処置
プロセス マネージャを終了します。	プロセス マネージャの終了が、エラー状態に起因するものではないことを確認します。エラー状態に起因している場合は、他のログメッセージで要求されている情報を収集します。

エラー メッセージ：`%PMAN-6-PROCSHUT : The process [chars] has shutdown`

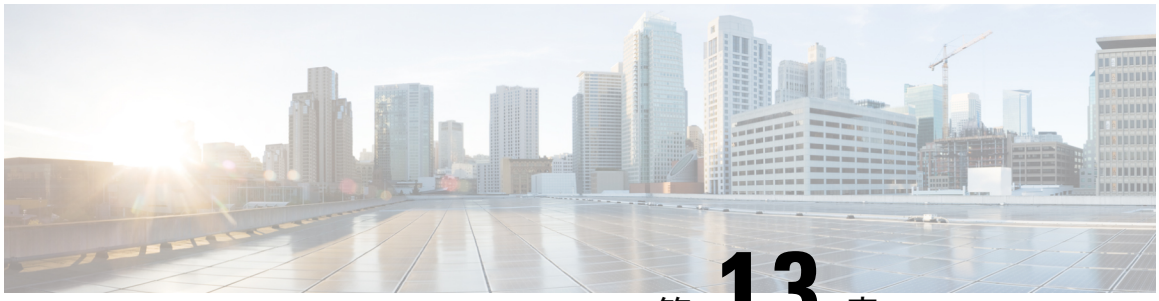
説明	推奨処置
プロセスのグレースフル シャットダウンが完了しました。	ユーザによる操作は必要ありません。このメッセージは、通知目的で示されます。

エラー メッセージ： `%PMAN-6-PROCSTART : The process [chars] has started`

説明	推奨処置
プロセスが正常に起動され、正常に稼働しています。	ユーザによる操作は必要ありません。このメッセージは、通知目的で示されます。

エラー メッセージ：`%PMAN-6-PROCSTATELESS : The process [chars] is restarting stateless`

説明	推奨処置
プロセスがステートレス再起動を要求しました。	ユーザによる操作は必要ありません。このメッセージは、通知目的で示されます。



第 13 章

トレース管理

この章の内容は、次のとおりです。

トレース管理

トレースは、内部イベントをログする機能です。トレース メッセージを含むトレース ファイルが自動的に作成され、ルータの hard disk: ファイル システムの tracelogs ディレクトリに保存されます（ブートフラッシュにトレース ファイルが保存されます）。

トレースファイルのデータは、次の処理を行う場合に役立ちます。

- トラブルシューティング：ルータの問題を特定して解決するのに役立ちます。システムで他の問題が同時に発生している場合でも、診断モードでトレースファイルにアクセスできます。
- デバッグ：システム アクションと操作の詳細を取得するのに役立ちます。

トレースの機能

トレースは、ルータの内部イベントの内容を記録します。モジュールに関するすべてのトレース出力を含むトレース ファイルが定期的に作成および更新され、tracelog ディレクトリに保存されます。トレースファイルは、システムパフォーマンスに影響を及ぼすことなく、このディレクトリから消去して、ファイルシステムのスペースを回復することができます。ファイル転送機能（FTP、TFTP など）を使用してこれらのファイルを他の宛先にコピーできます。また、プレーン テキスト エディタで開くことができます。

（注） ルータでトレースをディセーブルにすることはできません。

トレース情報を表示し、トレースレベルを設定するには、次のコマンドを使用します。

- **show logging process module**：特定のモジュールに関する最新のトレース情報を表示します。このコマンドは特権EXECモードおよび診断モードで使用可能です。診断モードでこのコマンドを使用すると、Cisco IOS XE の障害発生時にトレース ログ情報を収集できます。
- **set platform software trace**：出力に保存されるメッセージのタイプを決定するトレースレベルを設定します。トレース レベルの詳細については、トレースレベル（181 ページ）を参照してください。

UDF オフセットを使用したパケットトレーサの設定

オフセットを使用してパケットトレース UDF を設定するには、次の手順を実行します。

手順

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **udf** *udf name* **header** {**inner** | **outer**} {**13**|**14**} **offset** *offset-in-bytes* **length** *length-in-bytes*

例：

```
Router(config)# udf TEST_UDF_NAME_1 header  inner l3 64 1

Router(config)# udf TEST_UDF_NAME_2 header  inner l4 77 2

Router(config)# udf TEST_UDF_NAME_3 header outer l3 65 1
Router(config)# udf TEST_UDF_NAME_4 header outer l4 67 1
```

個々の UDF 定義を設定します。UDF の名前、オフセット元のネットワーキングヘッダー、抽出するデータの長さを指定できます。

inner キーワードまたは **outer** キーワードは、カプセル化されていないレイヤ 3 またはレイヤ 4 のヘッダーからのオフセットの開始を指定するか、またはカプセル化されたパケットがある場合は内部 L3/L4 からのオフセットの開始を指定します。

length キーワードはオフセットからの長さをバイト単位で指定します。有効な範囲は 1 ～ 2 です。

ステップ 4 **udf** *udf name* {**header | packet-start**} *offset-base offset length*

例：

```
Router(config)# udf TEST_UDF_NAME_5 packet-start 120 1
```

- header：オフセットの基本設定を指定します。
- packet-start：packet-start からのオフセットベースを指定します。packet-start は、パケットトレースがインバウンドパケット用かアウトバウンドパケット用かによって異なります。パケットトレースがインバウンドパケット用である場合、パケット開始はレイヤ 2 になります。アウトバウンドの場合は、packet-start はレイヤ 3 になります。
- offset：オフセットベースからオフセットさせるバイト数を指定します。オフセットベース（レイヤ 3/レイヤ 4 ヘッダー）からの先頭バイトに一致させるには、オフセットを 0 に設定します。
- length：オフセットからのバイト数を指定します。1 バイトまたは 2 バイトだけがサポートされます。追加のバイト数に一致させるには、複数の UDF の定義が必要です。

ステップ 5 **ip access-list extended** {*acl-name* |*acl-num*}

例：

```
Router(config)# ip access-list extended acl2
```

拡張 ACL コンフィギュレーション モードを有効にします。CLI は拡張 ACL コンフィギュレーション モードを開始します。このモードでは、後続のすべてのコマンドが現在の拡張アクセスリストに適用されます。拡張 ACL は、IP パケットの送信元アドレスおよび宛先アドレスを ACL に設定されているアドレスと比較して、トラフィックを制御します。

ステップ 6 **ip access-list extended { deny | permit } udf udf-name value mask**

例：

```
Router(config-acl)# permit ip any any udf TEST_UDF_NAME_5 0xD3 0xFF
```

現在のアクセス制御エントリ（ACE）と併せて、UDF で一致するように ACL を設定します。ACL で定義されているバイトは 0xD3 です。マスクは、許可および拒否するトラフィックを指定するように、IP ACL で IP アドレスとともに使用します。

ステップ 7 **debug platform condition [ipv4 | ipv6] [interface** *interface*] **[access-list** *access-list -name* **|** *ipv4-address* **/** *subnet-mask* **|** *ipv6-address* **/** *subnet-mask*] **[ingress | egress |both]**

例：

```
Router# debug platform condition interface gi0/0/0 ipv4 access-list acl2 both
```

パケットをトレースするための一致基準を指定します。プロトコル、IP アドレスおよびサブネットマスク、アクセス制御リスト（ACL）、インターフェイス、方向によるフィルタリング機能を提供します。

ステップ 8 **debug platform condition start**

例：

```
Router# debug platform condition start
```

指定した位置基準を有効にしてパケットトレースを開始します。

ステップ 9 **debug platform packet-trace packet** *pkt-num* **[fia-trace | summary-only] [circular] [data-size** *data-size***]**

例：

```
Router# debug platform packet-trace packet 1024 fia-trace data-size 2048
```

指定した数のパケットのサマリーデータを収集します。デフォルトでは機能パスデータをキャプチャし、必要に応じて FIA トレースを実行します。

pkt-num：所定の時間に維持されるパケットの最大数を指定します。

fia-trace：サマリーデータ、機能固有のデータなど、詳細なレベルのデータキャプチャを実行します。また、パケット処理中にアクセスされた各機能エントリも表示します。

summary-only：詳細情報を最小限にしたサマリーデータのキャプチャを有効にします。

circular：最近トレースされたパケットのデータを保存します。

data-size：各パケットの機能データと FIA トレースデータを保存するデータバッファのサイズをバイト単位で指定します。パケットで非常に重いパケット処理が実行された場合、ユーザーは必要に応じてデータバッファのサイズを増やすことができます。デフォルト値は 2048 です。

ステップ 10 **debug platform packet-trace {punt | inject|copy | drop |packet | statistics}**

例：

```
Router# debug platform packet-trace punt
```

データからコントロールプレーンへパントされたパケットのトレースを有効にします。

ステップ 11 **debug platform condition stop**

例：

```
Router# debug platform condition start
```

条件を非アクティブにして、パケットのトレースを停止します。

ステップ 12 **exit**

例：

```
Router# exit
```

特権 EXEC モードを終了します。

トレースレベル

トレースレベルは、トレースバッファまたはトレースファイルに保存する必要のあるモジュール情報の量を決定します。

次の表に、使用可能なすべてのトレースレベルと、各トレースレベルで表示されるメッセージのタイプについて説明します。

表 *16*：トレースレベルとその内容

トレースレベル	レベル番号	説明
緊急	0	システムが使用不能になる問題のメッセージです。
アラート	1	ただちに対応する必要のある動作についてのメッセージです。
重要	2	クリティカルな状態についてのメッセージです。これは、ルータ上のすべてのモジュールに関するデフォルト設定です。
エラー	3	システムエラーについてのメッセージです。
警告	4	システム警告についてのメッセージです。
通知	5	重大な問題に関するメッセージです。ただし、ルータは通常どおり動作しています。
情報	6	単に情報を提供するだけのメッセージです。
デバッグ	7	デバッグレベルの出力を提供するメッセージです。
詳細	8	生成可能なすべてのトレースメッセージが送信されます。

トレースレベル	レベル番号	説明
ノイズ	—	モジュールについて生成可能なすべてのトレース メッセージが記録されます。 ノイズレベルは常に最上位のトレースレベルに相当します。トレース機能の今後の拡張によって、Verbose レベルよりも高いトレース レベルが導入される場合でも、Noise レベルは新規に導入されるトレース レベルと同等になります。

トレース レベルが設定されている場合、設定されているトレース レベル自体と、それより低いすべてのトレース レベルの両方のメッセージが収集されます。

たとえば、トレース レベルを 3（エラー）に設定すると、トレース ファイルにはレベル 0（緊急）、1（アラート）、2（重要）、および 3（エラー）のメッセージが出力されます。

トレース レベルを 4（警告）に設定すると、レベル 0（緊急）、1（アラート）、2（重要）、3（エラー）、および 4（警告）のメッセージが出力されます。

ルータのすべてのモジュールのデフォルト トレース レベルは 5（通知）です。

トレース レベルは、コンフィギュレーション モードでは設定されません。このため、ルータのリロード後にトレース レベル設定がデフォルト値に戻ります。

注意 モジュールのトレース レベルをデバッグ レベル以上に設定すると、パフォーマンスに悪影響を及ぼす可能性があります。

注意 多数のモジュールで高いトレース レベルを設定すると、パフォーマンスが大幅に低下する可能性があります。特定の状況で高いトレース レベルが必要な場合は、複数のモジュールで高いレベルを設定する代わりに、常に 1 つのモジュールのトレース レベルを高く設定することをお勧めします。

トレースレベルの表示

デフォルトでは、ルータ上のすべてのモジュールが 5（通知）に設定されます。ユーザが変更しないかぎり、この設定はそのまま維持されます。

ルータのモジュールのトレースレベルを表示するには、特権 EXEC モードまたは診断モードで **show logging process** コマンドを入力します。

次の例では、**show logging process** コマンドを使用して、アクティブな RP 上のフォワーディング マネージャ プロセスのトレースレベルを表示します。

```
Router# showlogging process forwarding-manager rp active
Module Name                      Trace Level
-----------------------------------------------
acl                              Notice
binos                            Notice
binos/brand                      Notice
bipc                             Notice
bsignal                          Notice
btrace                           Notice
cce                              Notice
cdllib                           Notice
cef                              Notice
chasfs                           Notice
chasutil                         Notice
erspan                           Notice
ess                              Notice
ether-channel                    Notice
evlib                            Notice
evutil                           Notice
file_alloc                       Notice
fman_rp                          Notice
fpm                              Notice
fw                               Notice
icmp                             Notice
interfaces                       Notice
iosd                             Notice
ipc                              Notice
ipclog                           Notice
iphc                             Notice
IPsec                            Notice
mgmte-acl                        Notice
mlp                              Notice
mqipc                            Notice
nat                              Notice
nbar                             Notice
netflow                          Notice
om                               Notice
peer                             Notice
qos                              Notice
route-map                        Notice
sbc                              Notice
services                         Notice
sw_wdog                          Notice
tdl_acl_config_type              Notice
tdl_acl_db_type                  Notice
tdl_cdlcore_message              Notice
tdl_cef_config_common_type       Notice
tdl_cef_config_type              Notice
tdl_dpidb_config_type            Notice
tdl_fman_rp_comm_type            Notice
tdl_fman_rp_message              Notice
tdl_fw_config_type               Notice
tdl_hapi_tdl_type                Notice
tdl_icmp_type                    Notice
tdl_ip_options_type              Notice
tdl_ipc_ack_type                 Notice
tdl_IPsec_db_type                Notice
tdl_mcp_comm_type                Notice
tdl_mlp_config_type              Notice
tdl_mlp_db_type                  Notice
tdl_om_type                      Notice
```

```
tdl_ui_message                  Notice
tdl_ui_type                     Notice
tdl_urpf_config_type            Notice
tdllib                          Notice
trans_avl                       Notice
uihandler                       Notice
uipeer                          Notice
uistatus                        Notice
urpf                            Notice
vista                           Notice
wccp                            Notice
```

トレースレベルの設定

ルータに含まれる1つのモジュールのトレースレベル、またはルータにおける特定プロセスに含まれるすべてのモジュールのトレースレベルを設定するには、特権EXECモードまたは診断モードで **set platform software trace** コマンドを入力します。

次の例では、スロット 0 の ESP プロセッサの Forwarding Manager で ACL モジュールに関するトレースレベルを `info` に設定します。

```
set platform software trace forwarding-manager F0 acl info
```

トレースバッファの内容の表示

トレースバッファ内またはファイル内のトレースメッセージを表示するには、特権EXECモードまたは診断モードで **show logging process** コマンドを入力します。次の例では、**show logging process command** コマンドを使用して、Route Processor スロット 0 での Host Manager プロセスのトレースメッセージを表示します。

```
Router# show logging process host-manager R0
08/23 12:09:14.408 [uipeer]: (info): Looking for a ui_req msg
08/23 12:09:14.408 [uipeer]: (info): Start of request handling for con 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Accepted connection for 14 as 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Received new connection 0x100a61c8 on descriptor
14
08/23 12:09:14.398 [uipeer]: (info): Accepting command connection on listen fd 7
08/23 11:53:57.440 [uipeer]: (info): Going to send a status update to the shell manager
 in slot 0
08/23 11:53:47.417 [uipeer]: (info): Going to send a status update to the shell manager
 in slot 0
```

例：パケットトレースの使用

次に、パケットトレースを使用して Cisco ASR 1006 ルータの NAT 設定でパケットドロップのトラブルシューティングを行うシナリオの例を示します。この例には、パケットトレース機能によって提供される詳細レベルを効果的に利用して問題に関する情報を収集し、問題を切り分けて、解決策を見つける方法が示されています。

このシナリオでは、問題があることはわかりますが、どこからトラブルシューティングを開始すればよいかはわかりません。したがって、多数の着信パケットのパケットトレースのサマリーにアクセスすることを検討する必要があります。

```
Router# debug platform condition ingress
Router# debug platform packet-trace packet 2048 summary-only
Router# debug platform condition start
Router# debug platform condition stop
Router# show platform packet-trace summary
Pkt   Input             Output            State  Reason
0     Gi0/0/0           Gi0/0/0           DROP   402 (NoStatsUpdate)
1     internal0/0/rp:0  internal0/0/rp:0  PUNT   21  (RP<->QFP keepalive)
2     internal0/0/recycle:0  Gi0/0/0      FWD
```

この出力には、ギガビット イーサネット インターフェイス 0/0/0 の NAT 設定が原因でパケットがドロップされていることが示されています。これによって、問題は特定のインターフェイスで発生していることがわかります。この情報を使用して、トレースするパケットを制限し、データキャプチャのパケット数を減らし、検査レベルを上げることができます。

```
Router# debug platform packet-trace packet 256
Router# debug platform packet-trace punt
Router# debug platform condition interface Gi0/0/0
Router# debug platform condition start
Router# debug platform condition stop
Router# show platform packet-trace summary
Router# show platform packet-trace 15
Packet: 15          CBUG ID: 238
Summary
  Input     : GigabitEthernet0/0/0
  Output    : internal0/0/rp:1
  State     : PUNT 55  (For-us control)
  Timestamp
    Start   : 1166288346725 ns (06/06/2016 09:09:42.202734 UTC)
    Stop    : 1166288383210 ns (06/06/2016 09:09:42.202770 UTC)
Path Trace
  Feature: IPV4
    Input       : GigabitEthernet0/0/0
    Output      : <unknown>
    Source      : 10.64.68.3
    Destination : 224.0.0.102
    Protocol    : 17 (UDP)
      SrcPort   : 1985
      DstPort   : 1985
IOSd Path Flow: Packet: 15    CBUG ID: 238
  Feature: INFRA
    Pkt Direction: IN
    Packet Rcvd From CPP
  Feature: IP
    Pkt Direction: IN
    Source      : 10.64.68.122
    Destination : 10.64.68.255
  Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.64.68.122
    Destination : 10.64.68.255
    Interface   : GigabitEthernet0/0/0
  Feature: UDP
    Pkt Direction: IN
    src         : 10.64.68.122(1053)
```

```
    dst         : 10.64.68.255(1947)
    length      : 48

Router#show platform packet-trace packet 10
Packet: 10          CBUG ID: 10
Summary
  Input     : GigabitEthernet0/0/0
  Output    : internal0/0/rp:0
  State     : PUNT 55  (For-us control)
  Timestamp
    Start   : 274777907351 ns (01/10/2020 10:56:47.918494 UTC)
    Stop    : 274777922664 ns (01/10/2020 10:56:47.918509 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet0/0/0
    Output      : <unknown>
    Source      : 10.78.106.2
    Destination : 224.0.0.102
    Protocol    : 17 (UDP)
      SrcPort   : 1985
      DstPort   : 1985

IOSd Path Flow: Packet: 10    CBUG ID: 10
  Feature: INFRA
    Pkt Direction: IN
Packet Rcvd From DATAPLANE
 Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.78.106.2
    Destination : 224.0.0.102
    Interface   : GigabitEthernet0/0/0

  Feature: UDP
    Pkt Direction: IN DROP
    Pkt : DROPPED
    UDP: Discarding silently
    src        : 881 10.78.106.2(1985)
    dst         : 224.0.0.102(1985)
    length      : 60

Router#show platform packet-trace packet  12
Packet: 12          CBUG ID: 767
Summary
  Input     : GigabitEthernet3
  Output    : internal0/0/rp:0
  State     : PUNT 11  (For-us data)
  Timestamp
    Start   : 16120990774814 ns (01/20/2020 12:38:02.816435 UTC)
    Stop    : 16120990801840 ns (01/20/2020 12:38:02.816462 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet3
    Output      : <unknown>
    Source      : 12.1.1.1
    Destination : 12.1.1.2
    Protocol    : 6 (TCP)
      SrcPort   : 46593
      DstPort   : 23
IOSd Path Flow: Packet: 12    CBUG ID: 767
  Feature: INFRA
    Pkt Direction: IN
    Packet Rcvd From DATAPLANE
```

```
  Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 12.1.1.1
    Destination : 12.1.1.2
    Interface   : GigabitEthernet3

  Feature: IP
    Pkt Direction: IN
    FORWARDEDTo transport layer
    Source        : 12.1.1.1
    Destination   : 12.1.1.2
    Interface     : GigabitEthernet3

  Feature: TCP
    Pkt Direction: IN
    tcp0: I NoTCB 12.1.1.1:46593 12.1.1.2:23 seq 1925377975 OPTS 4 SYN  WIN 4128
```

```
Router# show platform packet-trace summary
Pkt   Input                     Output                    State  Reason
0     INJ.2                     Gi1                       FWD
1     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
2     INJ.2                     Gi1                       FWD
3     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
4     INJ.2                     Gi1                       FWD
5     INJ.2                     Gi1                       FWD
6     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
7     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
8     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
9     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
10    INJ.2                     Gi1                       FWD
11    INJ.2                     Gi1                       FWD
12    INJ.2                     Gi1                       FWD
13    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
14    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
15    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
16    INJ.2                     Gi1                       FWD
```

次に、パケットトレースデータの統計を表示する例を示します。

```
Router#show platform packet-trace statistics
Packets Summary
  Matched  3
  Traced   3
Packets Received
  Ingress  0
  Inject   0
Packets Processed
  Forward  0
  Punt     3
    Count       Code  Cause
    3           56    RP injected for-us control
  Drop     0
  Consume  0

          PKT_DIR_IN
             Dropped       Consumed       Forwarded
INFRA            0              0              0
TCP              0              0              0
UDP              0              0              0
IP               0              0              0
IPV6             0              0              0
ARP              0              0              0

         PKT_DIR_OUT
```

```
             Dropped       Consumed       Forwarded
INFRA            0              0              0
TCP              0              0              0
UDP              0              0              0
IP               0              0              0
IPV6             0              0              0
ARP              0              0              0
```

次に、コントロールプレーンからフォワーディングプロセッサに挿入およびパントされるパケットを表示する例を示します。

```
Router#debug platform condition ipv4 10.118.74.53/32 both
 Router#Router#debug platform condition start
Router#debug platform packet-trace packet 200
Packet count rounded up from 200 to 256

Router#show platform packet-tracer packet 0
show plat pack pa 0
Packet: 0           CBUG ID: 674
Summary
  Input     : GigabitEthernet1
  Output    : internal0/0/rp:0
  State     : PUNT 11  (For-us data)
  Timestamp
    Start   : 17756544435656 ns (06/29/2020 18:19:17.326313 UTC)
    Stop    : 17756544469451 ns (06/29/2020 18:19:17.326346 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet1
    Output      : <unknown>
    Source      : 10.118.74.53
    Destination : 198.51.100.38
    Protocol    : 17 (UDP)
      SrcPort   : 2640
      DstPort   : 500

IOSd Path Flow: Packet: 0    CBUG ID: 674
  Feature: INFRA
  Pkt Direction: IN
    Packet Rcvd From DATAPLANE

  Feature: IP
  Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.118.74.53
    Destination : 198.51.100.38
    Interface   : GigabitEthernet1

  Feature: IP
  Pkt Direction: IN
  FORWARDED To transport layer
    Source        : 10.118.74.53
    Destination   : 198.51.100.38
    Interface     : GigabitEthernet1

  Feature: UDP
  Pkt Direction: IN
  DROPPED
 UDP: Checksum error: dropping
 Source      : 10.118.74.53(2640)
 Destination : 198.51.100.38(500)

Router#show platform packet-tracer packet 2
Packet: 2           CBUG ID: 2
```

```
IOSd Path Flow:
  Feature: TCP
  Pkt Direction: OUTtcp0: O SYNRCVD 198.51.100.38:22 198.51.100.55:52774 seq 3052140910
 OPTS 4 ACK 2346709419 SYN  WIN 4128

  Feature: TCP
  Pkt Direction: OUT
  FORWARDED
 TCP: Connection is in SYNRCVD state
 ACK         : 2346709419
 SEQ         : 3052140910
 Source      : 198.51.100.38(22)
 Destination : 198.51.100.55(52774)


  Feature: IP
  Pkt Direction: OUTRoute out the generated packet.srcaddr: 198.51.100.38, dstaddr:
198.51.100.55

  Feature: IP
  Pkt Direction: OUTInject and forward successful srcaddr: 198.51.100.38, dstaddr:
198.51.100.55

  Feature: TCP
  Pkt Direction: OUTtcp0: O SYNRCVD 198.51.100.38:22 198.51.100.55:52774 seq 3052140910
 OPTS 4 ACK 2346709419 SYN  WIN 4128
Summary
  Input     : INJ.2
  Output    : GigabitEthernet1
  State     : FWD
  Timestamp
    Start   : 490928006866 ns (06/29/2020 13:31:30.807879 UTC)
    Stop    : 490928038567 ns (06/29/2020 13:31:30.807911 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : internal0/0/rp:0
    Output      : <unknown>
    Source      : 172.18.124.38
    Destination : 172.18.124.55
    Protocol    : 6 (TCP)
      SrcPort   : 22
      DstPort   : 52774
  Feature: IPSec
    Result    : IPSEC_RESULT_DENY
    Action    : SEND_CLEAR
    SA Handle : 0
    Peer Addr : 55.124.18.172
    Local Addr: 38.124.18.172


Router#
```

第 14 章

環境モニタリングおよび PoE 管理

Cisco 8300 シリーズ セキュアルータには、ルータの環境を定期的に監視するハードウェアおよびソフトウェア機能があります。この章では、ルータの環境モニタリング機能について説明します。この機能により、重大なイベントを監視し、さまざまなルータコンポーネントのステータスに関する統計レポートを生成できます。この章の内容は、次のとおりです。

環境モニタ

ルータには、システム温度を監視する複数のセンサーを備えた強力な環境モニタ システムがあります。重大なイベントが発生すると、マイクロプロセッサは HOST CPU への割り込みを生成し、定期的なステータスおよび統計情報レポートを生成します。環境モニタシステムの主要な機能の一部を以下に示します。

- CPU、マザーボード、ミッドプレーンの温度の監視
- ファン回転速度の監視
- 異常なイベントの記録と通知の生成
- 簡易ネットワーク管理プロトコル（SNMP）トラップの監視
- オンボード障害ロギング（OBFL）データの生成と収集
- Call Home イベント通知の送信
- システム エラー メッセージの記録
- 現在の設定およびステータスの表示

環境モニタおよびリポート機能

モニタおよびリポート機能により、環境状態が悪化する前に状態を特定し、解決することができるので、システムの正常な稼働を維持できます。

環境モニタ機能

環境モニタ機能では、センサーを使用して、シャーシ内部を流れる冷却空気の温度を監視します。

ローカル電源モジュールで監視できるものは、次のとおりです。

- 入出力電流
- 出力電圧
- 入出力電力
- 温度
- ファン回転速度

デバイスは、次の環境動作条件を満たしている必要があります。

- 動作温度（公称）：0°C ～ 40°C（32°F ～ 104°F）
- 動作湿度（公称）：10% ～ 85% RH（結露しないこと）
- 動作湿度（短期）：10% ～ 85% RH（結露しないこと）
- 動作高度：海抜高度 0 m ～ 3000 m （0 ～ 10,000 フィート）
- AC 入力範囲：85 ～ 264 VAC

また、各電源はそれぞれの内部温度と電圧を監視します。電源モジュールの状態は、許容範囲内（ノーマル）または許容範囲外（クリティカル）のどちらかです。内部電源の温度または電圧がクリティカル レベルに達すると、電源はシステム プロセッサと相互作用することなくシャットダウンします。

次の表に、環境モニタリング システムで使用されるステータス状態のレベルを示します。

表 *17*：環境モニタリング システムで使用されるステータス状態のレベル

ステータス レベル	説明
標準	監視対象のすべてのパラメータが通常の許容範囲内にあります。

ステータス レベル	説明
警告	システムが特定のしきい値を超えています。システムは稼働し続けますが、オペレータが操作してシステムをノーマル ステートに戻すことを推奨します。
重大	温度または電圧条件が許容値を超えています。システムは引き続き動作しますが、やがてシャットダウンします。ただちにオペレータが操作する必要があります。

たとえば以下に示す状態が発生した場合、環境モニタリング システムからコンソールにメッセージが送信されます。

ファン障害

システム電源がオンである場合、すべてのファンが作動するはずです。1 つのファンに障害が発生してもシステムは引き続き稼働しますが、次のメッセージが表示されます。

```
%IOSXE_PEM-3-FANFAIL: The fan in slot 2/0 is encountering a failure condition
```

センサーが許容範囲外

センサーが許容範囲外になると、次のメッセージが表示されます。

```
%ENVIRONMENTAL-1-ALERT: V: 1.0v PCH, Location: R0, State: Warning, Reading: 1102 mV

%ENVIRONMENTAL-1-ALERT: V: PEM Out, Location: P1, State: Warning, Reading: 0 mV

%ENVIRONMENTAL-1-ALERT: Temp: Temp 3, Location R0, State : Warning, Reading : 90C
```

ファン トレイ（スロット P2）の取り外し

ファントレイ（スロット P2）が取り外されると、次のメッセージが表示されます。

```
%IOSXE_PEM-6-REMPEM_FM: PEM/FM slot P2 removed
```

ファン トレイ（スロット P2）の再挿入

ファントレイ（スロット P2）が再び挿入されると、次のメッセージが表示されます。

```
%IOSXE_PEM-6-INSPEM_FM: PEM/FM slot P2 inserted
```

ファン トレイ（スロット 2）が正常稼働している

ファントレイ（スロット 2）が正常に稼働している場合は、次のメッセージが表示されます。

```
%IOSXE_PEM-6-PEMOK: The PEM in slot P2 is functioning properly
```

スロット 2（ファン トレイ）のファン 0 が動作していない

ファントレイ（スロット 2）のファン 0 が正常に動作していない場合は、次のメッセージが表示されます。

```
%IOSXE_PEM-3-FANFAIL: The fan in slot 2/0 is encountering a failure condition
```

スロット 2（ファン トレイ）のファン 0 が正常に動作しいる

ファントレイ（スロット 2）のファン 0 が正常に動作している場合は、次のメッセージが表示されます。

```
%IOSXE_PEM-6-FANOK: The fan in slot 2/0 is functioning properly
```

スロット 1 の主電源モジュールがオフになっている

スロット 1 の主電源モジュールがオフになると、次のメッセージが表示されます。

```
%IOSXE_PEM-3-PEMFAIL: The PEM in slot 1 is switched off or encountering a
failure condition.
```

スロット 1 に主電源モジュールが装着された

スロット 1 に主電源モジュールが装着されると、次のメッセージが表示されます。

```
%IOSXE_PEM-6-INSPEM_FM: PEM/FM slot P1 inserted
%IOSXE_PEM-6-PEMOK: The PEM in slot 1 is functioning properly
```

温度および電圧が最大または最小しきい値を超えている

温度または電圧の最大しきい値と最小しきい値を示す警告メッセージを次の例に示します。

```
Warnings :
--------
For all the temperature sensors (name starting with “Temp:”) above,
the critical warning threshold is 100C (100C and higher)
the warning threshold is 80C (range from 80C to 99C)
the low warning threshold is 1C (range from -inf to 1C).

For all voltage sensors (names starting with "V:"),
the high warning threshold starts at that voltage +10%. (voltage + 10% is warning)
the low warning threshold starts at the voltage -10%. (voltage - 10% is warning)
```

環境レポート機能

次のコマンドを使用して、環境ステータスレポートを取得および表示できます。

- **debug environment**
- **debug platform software cman env monitor polling**
- **debug ilpower**
- **debug power** [**inline** | **main**]
- **show diag all eeprom**
- **show diag slot R0 eeprom detail**
- **show environment**
- **show environment all**
- **show inventory**
- **show platform all**

- **show platform diag**
- **show platform software status control-processor**
- **show version**
- **show power**
- **show power inline**

これらのコマンドは、温度や電圧などのパラメータの現在値を表示します。

環境モニタリング システムにより、これらのパラメータの値が 60 秒ごとに更新されます。これらのコマンドの簡単な例を次に示します。

debug environment：例

```
Router# debug environment location P0
Environmental sensor Temp: Temp 1 P0 debugging is on
Environmental sensor Temp: Temp 2 P0 debugging is on
Environmental sensor Temp: Temp 3 P0 debugging is on
Environmental sensor V: PEM Out P0 debugging is on
Environmental sensor I: PEM In P0 debugging is on
Environmental sensor I: PEM Out P0 debugging is on
Environmental sensor W: In pwr P0 debugging is on
Environmental sensor W: Out pwr P0 debugging is on
Environmental sensor RPM: fan0 P0 debugging is on

*Jul  8 21:49:23.292 PDT:     Sensor: Temp: Temp 1 P0, In queue 1
*Jul  8 21:49:23.292 PDT:     State=Normal  Reading=35
*Jul  8 21:49:23.292 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.292 PDT:     Sensor: Temp: Temp 1 P0  State=Normal Reading=35
*Jul  8 21:49:23.292 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.292 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.292 PDT:     Sensor: Temp: Temp 2 P0, In queue 1
*Jul  8 21:49:23.292 PDT:     State=Normal  Reading=40
*Jul  8 21:49:23.292 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.292 PDT:     Sensor: Temp: Temp 2 P0  State=Normal Reading=40
*Jul  8 21:49:23.292 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.292 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.292 PDT:     Sensor: Temp: Temp 3 P0, In queue 1
*Jul  8 21:49:23.292 PDT:     State=Normal  Reading=44
*Jul  8 21:49:23.292 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.292 PDT:     Sensor: Temp: Temp 3 P0  State=Normal Reading=44
*Jul  8 21:49:23.292 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.292 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.292 PDT:     Sensor: V: PEM In P0, In queue 1
*Jul  8 21:49:23.292 PDT:     State=Normal  Reading=118501
*Jul  8 21:49:23.292 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.293 PDT:     Sensor: V: PEM In P0  State=Normal Reading=118501
*Jul  8 21:49:23.293 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.293 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.293 PDT:     Sensor: V: PEM Out P0, In queue 1
*Jul  8 21:49:23.293 PDT:     State=Normal  Reading=12000
*Jul  8 21:49:23.293 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.293 PDT:     Sensor: V: PEM Out P0  State=Normal Reading=12000
*Jul  8 21:49:23.293 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.293 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.293 PDT:     Sensor: I: PEM In P0, In queue 1
*Jul  8 21:49:23.293 PDT:     State=Normal  Reading=820
*Jul  8 21:49:23.293 PDT:     Rotation count=0  Poll period=20000
```

```
*Jul  8 21:49:23.293 PDT:     Sensor: I: PEM In P0  State=Normal Reading=828
*Jul  8 21:49:23.293 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.293 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.293 PDT:     Sensor: I: PEM Out P0, In queue 1
*Jul  8 21:49:23.293 PDT:     State=Normal  Reading=7200
*Jul  8 21:49:23.293 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.293 PDT:     Sensor: I: PEM Out P0  State=Normal Reading=7100
*Jul  8 21:49:23.293 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.293 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.293 PDT:     Sensor: P: In pwr P0, In queue 1
*Jul  8 21:49:23.293 PDT:     State=Normal  Reading=97
*Jul  8 21:49:23.293 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.293 PDT:     Sensor: P: In pwr P0  State=Normal Reading=98
*Jul  8 21:49:23.293 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.293 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.293 PDT:     Sensor: P: Out pwr P0, In queue 1
*Jul  8 21:49:23.293 PDT:     State=Normal  Reading=87
*Jul  8 21:49:23.293 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.293 PDT:     Sensor: P: Out pwr P0  State=Normal Reading=89
*Jul  8 21:49:23.293 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.293 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.293 PDT:     Sensor: RPM: fan0 P0, In queue 1
*Jul  8 21:49:23.293 PDT:     State=Normal  Reading=5824
*Jul  8 21:49:23.293 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.293 PDT:     Sensor: RPM: fan0 P0  State=Normal Reading=5824
*Jul  8 21:49:23.293 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.293 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:43.296 PDT:     Sensor: Temp: Temp 1 P0, In queue 1
*Jul  8 21:49:43.296 PDT:     State=Normal  Reading=35
*Jul  8 21:49:43.296 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:43.296 PDT:     Sensor: Temp: Temp 1 P0  State=Normal Reading=35
*Jul  8 21:49:43.296 PDT:     Inserting into queue 1 on spoke 209.
*Jul  8 21:49:43.296 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:43.296 PDT:     Sensor: Temp: Temp 2 P0, In queue 1
*Jul  8 21:49:43.296 PDT:     State=Normal  Reading=40
*Jul  8 21:49:43.296 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:43.296 PDT:     Sensor: Temp: Temp 2 P0  State=Normal Reading=40
*Jul  8 21:49:43.296 PDT:     Inserting into queue 1 on spoke 209.
*Jul  8 21:49:43.296 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:43.296 PDT:     Sensor: Temp: Temp 3 P0, In queue 1
*Jul  8 21:49:43.296 PDT:     State=Normal  Reading=44
*Jul  8 21:49:43.296 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:53:43.329 PDT:     State=Normal  Reading=5824
*Jul  8 21:53:43.329 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:53:43.329 PDT:     Sensor: RPM: fan0 P0  State=Normal Reading=5824
*Jul  8 21:53:43.329 PDT:     Inserting into queue 1 on spoke 149.
*Jul  8 21:53:43.329 PDT:     Rotation count=20 Displacement=0
```

debug platform software cman env monitor polling：例

```
Router# debug platform software cman env monitor polling
platform software cman env monitor polling debugging is on
Router#
*Jul  8 21:56:23.351 PDT: Sensor: Temp: Temp 1 P0, In queue 1
*Jul  8 21:56:23.351 PDT: State=Normal  Reading=35
*Jul  8 21:56:23.351 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.351 PDT: IOS-RP-ENVMON: sensor READ callback Temp: Temp 1, P0, 35
*Jul  8 21:56:23.351 PDT: Sensor: Temp: Temp 1 P0  State=Normal Reading=35
*Jul  8 21:56:23.351 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.351 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.351 PDT: Sensor: Temp: Temp 2 P0, In queue 1
*Jul  8 21:56:23.351 PDT: State=Normal  Reading=40
```

```
*Jul  8 21:56:23.351 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.351 PDT: IOS-RP-ENVMON: sensor READ callback Temp: Temp 2, P0, 40
*Jul  8 21:56:23.351 PDT: Sensor: Temp: Temp 2 P0  State=Normal Reading=40
*Jul  8 21:56:23.351 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.351 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.351 PDT: Sensor: Temp: Temp 3 P0, In queue 1
*Jul  8 21:56:23.351 PDT: State=Normal  Reading=44
*Jul  8 21:56:23.351 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.351 PDT: IOS-RP-ENVMON: sensor READ callback Temp: Temp 3, P0, 44
*Jul  8 21:56:23.351 PDT: Sensor: Temp: Temp 3 P0  State=Normal Reading=44
*Jul  8 21:56:23.351 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.351 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.351 PDT: Sensor: V: PEM In P0, In queue 1
*Jul  8 21:56:23.351 PDT: State=Normal  Reading=118501
*Jul  8 21:56:23.351 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.351 PDT: IOS-RP-ENVMON: sensor READ callback V: PEM In, P0, 118501
*Jul  8 21:56:23.351 PDT: Sensor: V: PEM In P0  State=Normal Reading=118501
*Jul  8 21:56:23.351 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.351 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.351 PDT: Sensor: V: PEM Out P0, In queue 1
*Jul  8 21:56:23.351 PDT: State=Normal  Reading=12100
*Jul  8 21:56:23.351 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.351 PDT: IOS-RP-ENVMON: sensor READ callback V: PEM Out, P0, 12000
*Jul  8 21:56:23.351 PDT: Sensor: V: PEM Out P0  State=Normal Reading=12000
*Jul  8 21:56:23.351 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.351 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.351 PDT: Sensor: I: PEM In P0, In queue 1
*Jul  8 21:56:23.351 PDT: State=Normal  Reading=820
*Jul  8 21:56:23.351 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.351 PDT: IOS-RP-ENVMON: sensor READ callback I: PEM In, P0, 828
*Jul  8 21:56:23.351 PDT: Sensor: I: PEM In P0  State=Normal Reading=828
*Jul  8 21:56:23.351 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.351 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.351 PDT: Sensor: I: PEM Out P0, In queue 1
*Jul  8 21:56:23.351 PDT: State=Normal  Reading=7200
*Jul  8 21:56:23.351 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.351 PDT: IOS-RP-ENVMON: sensor READ callback I: PEM Out, P0, 7100
*Jul  8 21:56:23.352 PDT: Sensor: I: PEM Out P0  State=Normal Reading=7100
*Jul  8 21:56:23.352 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.352 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.352 PDT: Sensor: P: In pwr P0, In queue 1
*Jul  8 21:56:23.352 PDT: State=Normal  Reading=97
*Jul  8 21:56:23.352 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback P: In pwr, P0, 98
*Jul  8 21:56:23.352 PDT: Sensor: P: In pwr P0  State=Normal Reading=98
*Jul  8 21:56:23.352 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.352 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.352 PDT: Sensor: P: Out pwr P0, In queue 1
*Jul  8 21:56:23.352 PDT: State=Normal  Reading=88
*Jul  8 21:56:23.352 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback P: Out pwr, P0, 88
*Jul  8 21:56:23.352 PDT: Sensor: P: Out pwr P0  State=Normal Reading=88
*Jul  8 21:56:23.352 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.352 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.352 PDT: Sensor: RPM: fan0 P0, In queue 1
*Jul  8 21:56:23.352 PDT: State=Normal  Reading=5888
*Jul  8 21:56:23.352 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback RPM: fan0, P0, 5888
*Jul  8 21:56:23.352 PDT: Sensor: RPM: fan0 P0  State=Normal Reading=5888
*Jul  8 21:56:23.352 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.352 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback RPM: fan0, P2, 12600
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback RPM: fan1, P2, 12840
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback RPM: fan2, P2, 12900
```

```
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback P: pwr, P2, 8
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback Temp: Inlet 1, R0, 29
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback Temp: Inlet 2, R0, 30
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback Temp: Outlet 1, R0, 35
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback Temp: Outlet 2, R0, 36
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback Temp: CP-CPU, R0, 42
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 12v, R0, 12127
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 5v, R0, 5022
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 3.3v, R0, 3308
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 3.0v, R0, 3023
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 2.5v, R0, 2490
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 1.8v, R0, 1798
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 1.2v, R0, 1203
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 1.2v_CPU, R0, 1201
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 1.05v_CPU, R0, 1052
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 1.05v, R0, 1062
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 1.0v, R0, 1002
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 0.6v, R0, 593
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback P: pwr, R0, 86
*Jul  8 21:56:25.352 PDT: IOS-RP-ENVMON: sensor READ callback P: pwr: Pwr, 0/1, 5
*Jul  8 21:56:32.354 PDT: IOS-RP-ENVMON: sensor READ callback P: pwr: Pwr, 1/0, 27
```

debug ilpower：例

```
Router# debug ilpower ?
  cdp          ILPOWER CDP messages
  controller   ILPOWER controller
  event        ILPOWER event
  ha           ILPOWER High-Availability
  port         ILPOWER port management
  powerman     ILPOWER powerman
  registries   ILPOWER registries
  scp          ILPOWER SCP messages
  upoe         ILPOWER upoe
```

debug power [inline|main]：例

この例では、1 台の 1000 W 電源と 1 台の 450 W 電源があります。インラインパワーおよび主電源の出力を示します。

```
Router# debug power ?
  inline  ILPM inline power related
  main    Main power related
  <cr>    <cr>
Router# debug power
POWER all debug debugging is on

Router# show debugging | include POWER
POWER:
POWER main debugging is on
POWER inline debugging is on
Router#
..

*Jul  8 21:56:23.351: %ENVIRONMENTAL-6-NOTICE: V: PEM Out, Location: P1, State: Warning,
 Reading: 0 mV
*Jul  8 21:56:23.351: %IOSXE_PEM-6-PEMOK: The PEM in slot P1 is functioning properly
*Jul  8 21:56:23.351: %PLATFORM_POWER-6-MODEMATCH: Main power is in Boost mode
*Jul  8 21:56:23.351: Power M: Received Msg for 12V/Main, total power 1450, Run same as
 cfg Yes
```

```
*Jul  8 21:56:23.351: Power M: Received Msg for POE/ILPM, total power 500, Run same as
cfg No
*Jul  8 21:56:23.351: Power I: Updating pool power is 500 watts
*Jul  8 21:56:23.351: Power I: Intimating modules of total power 500 watts
*Jul  8 21:56:23.351: Power M: Received Msg for 12V/Main, total power 1450, Run same as
 cfg Yes
*Jul  8 21:56:23.351: Power M: Received Msg for POE/ILPM, total power 500, Run same as
cfg No
*Jul  8 21:56:23.351: Power I: Updating pool power is 500 watts
*Jul  8 21:56:23.351: Power I: Intimating modules of total power 500 watts
Router#
```

show diag all eeprom：C8375-E-G2 の例

```
Router# show diag all eeprom
MIDPLANE EEPROM data:

        Product Identifier (PID) : C8375-E-G2
        Version Identifier (VID) : V01
        PCB Serial Number        : FDO28310870
        Top Assy. Part Number    : 68-7625-01
        Hardware Revision        : 1.0
        CLEI Code                : CMM8K00ARA
Power/Fan Module P0 EEPROM data:

        Product Identifier (PID) : PWR-CC1-760WAC
        Version Identifier (VID) : V01
        PCB Serial Number        : LIT2748A9MU
        CLEI Code                : CMUPAKBCAA
Power/Fan Module P1 EEPROM data:

        Product Identifier (PID) : PWR-CC1-400WAC
        Version Identifier (VID) : V01
        PCB Serial Number        : LIT2650C53E
        CLEI Code                : CMUPAG4CAA
External PoE Module POE0 EEPROM data:

        Product Identifier (PID) : PWR-CC1-760WAC
        Version Identifier (VID) : V01
        PCB Serial Number        : LIT2748A9MU
        CLEI Code                : CMUPAKBCAA
External PoE Module POE1 EEPROM data is not initialized

Slot R0 EEPROM data:

        Product Identifier (PID) : C8375-E-G2
        Version Identifier (VID) : V01
        PCB Serial Number        : FDO28310870
        Top Assy. Part Number    : 68-7625-01
        Hardware Revision        : 1.0
        CLEI Code                : CMM8K00ARA
Slot F0 EEPROM data:

        Product Identifier (PID) : C8375-E-G2
        Version Identifier (VID) : V01
        PCB Serial Number        : FDO28310870
        Top Assy. Part Number    : 68-7625-01
Hardware Revision        : 1.0
        CLEI Code                : CMM8K00ARA
Slot 0 EEPROM data:

        Product Identifier (PID) : C8375-E-G2
```

```
        Version Identifier (VID) : V01
        PCB Serial Number        : FDO28310870
        Top Assy. Part Number    : 68-7625-01
        Hardware Revision        : 1.0
        CLEI Code                : CMM8K00ARA
Slot 1 EEPROM data:

        Product Identifier (PID) : C8375-E-G2
        Version Identifier (VID) : V01
        PCB Serial Number        : FDO28310870
        Top Assy. Part Number    : 68-7625-01
        Hardware Revision        : 1.0
        CLEI Code                : CMM8K00ARA
SPA EEPROM data for subslot 0/0:

        Product Identifier (PID) : 4M-2xSFP+
        Version Identifier (VID) : V01
        PCB Serial Number        :
        Top Assy. Part Number    : 68-2236-01
        Top Assy. Revision       : A0
        Hardware Revision        : 2.2
        CLEI Code                : CNUIAHSAAA
SPA EEPROM data for subslot 0/1:

        Product Identifier (PID) : C-NIM-8M
        Version Identifier (VID) : V01
        PCB Serial Number        : FDO26500YDL
        Hardware Revision        : 1.0
        CLEI Code                : CMUIAYSCAA
SPA EEPROM data for subslot 0/2 is not available

SPA EEPROM data for subslot 0/3 is not available

SPA EEPROM data for subslot 0/4 is not available

SPA EEPROM data for subslot 0/5 is not available

SPA EEPROM data for subslot 0/6 is not available

SPA EEPROM data for subslot 1/0 is not available

SPA EEPROM data for subslot 1/1 is not available

SPA EEPROM data for subslot 1/2 is not available

SPA EEPROM data for subslot 1/3 is not available

SPA EEPROM data for subslot 1/4 is not available

SPA EEPROM data for subslot 1/5 is not available

SPA EEPROM data for subslot 1/6 is not available
```

show diag all eeprom：C8355-G2 の例

```
Router# show diag all eeprom
MIDPLANE EEPROM data:

                                                                    Product
Identifier (PID) : C8355-G2

Version Identifier (VID) : V01
```

```
PCB Serial Number        : FDO28330C27

Top Assy. Part Number    : 68-7722-01

Hardware Revision        : 1.0

CLEI Code                : CMM8J00ARA

Power/Fan Module P0 EEPROM data is not initialized

Power/Fan Module P1 EEPROM data:

Product Identifier (PID) : PWR-CC1-230WAC

Version Identifier (VID) : V02

PCB Serial Number        :

CLEI Code                : IPUPAMFAAB

Slot R0 EEPROM data:
Product Identifier (PID) : C8355-G2

Version Identifier (VID) : V01

PCB Serial Number        : FDO28330C27

Top Assy. Part Number    : 68-7722-01

Hardware Revision        : 1.0

CLEI Code                : CMM8J00ARA

Slot F0 EEPROM data:

Product Identifier (PID) : C8355-G2

 Version Identifier (VID) : V01

PCB Serial Number        : FDO28330C27
Top Assy. Part Number    : 68-7722-01

Hardware Revision        : 1.0

CLEI Code                : CMM8J00ARA

Slot 0 EEPROM data:
Product Identifier (PID) : C8355-G2

Version Identifier (VID) : V01

PCB Serial Number        : FDO28330C27

Top Assy. Part Number    : 68-7722-01

Hardware Revision        : 1.0

CLEI Code                : CMM8J00ARA

SPA EEPROM data for subslot 0/0:

Product Identifier (PID) : 4M-2x1G-4xSFP+
```

```
Version Identifier (VID) : V01

PCB Serial Number        :

Top Assy. Part Number    : 68-2236-01

Top Assy. Revision       : A0

Hardware Revision        : 2.2

CLEI Code                : CNUIAHSAAA

SPA EEPROM data for subslot 0/1 is not available

SPA EEPROM data for subslot 0/2 is not available

SPA EEPROM data for subslot 0/3 is not available
SPA EEPROM data for subslot 0/4 is not available

SPA EEPROM data for subslot 0/5 is not available

SPA EEPROM data for subslot 0/6 is not available
```

show environment：C8375-E-G2 の例

この例で、スロット POE0 および POE1 の出力に注目してください。

```
Router# show environment
 Number of Critical alarms:  0
Number of Major alarms:     0
Number of Minor alarms:     2

 Slot        Sensor          Current State   Reading
Threshold(Minor,Major,Critical,Shutdown)
 ----------  --------------  --------------- ------------
-------------------------------------
 R0          Temp: Inlet 1   Normal          23    Celsius      (40 ,na ,42 ,na )(Celsius)

 R0          Temp: Inlet 2   Normal          26    Celsius      (90 ,na ,100,na )(Celsius)

 R0          Temp: Outlet 1  Normal          24    Celsius      (70 ,na ,75 ,na )(Celsius)

 R0          Temp: Outlet 2  Normal          26    Celsius      (70 ,na ,75 ,na )(Celsius)

 R0          Temp: CPU       Normal          34    Celsius      (na ,na ,na ,na )(Celsius)

 R0          Temp: Working   Normal          23    Celsius      (na ,na ,na ,na )(Celsius)

 R0           V: 12V          Normal           12044 mV           na
 R0           V: 5V           Normal           5010  mV           na
 R0           V: 3.3V_STBY    Normal           3314  mV           na
 R0           V: 3.3V         Normal           3315  mV           na
 R0           V: 3.3V_USB     Normal           3315  mV           na
 R0           V: 2.5V         Normal           2502  mV           na
 R0           V: 1.8V         Normal           1799  mV           na
 R0           V: 1.2V_CPU     Normal           1197  mV           na
 R0           V: 1.2V         Normal           1208  mV           na
 R0           V: 1.1V         Normal           1100  mV           na
 R0           V: 1.0V         Normal           1001  mV           na
 R0           V: 0.8V_SW      Normal           790   mV           na
 R0           V: 0.85V_DDR    Normal           850   mV           na
 R0           V: 0.8V_SYS     Normal           848   mV           na
```

```
 R0          V: 0.8V_CORE    Normal          800   mV          na
 R0          V: 0.75V        Normal          750   mV          na
 R0          P: Power        Normal          41    Watts       na
 P0         Temp: Temp 1    Normal         0     Celsius     (na ,na ,na ,na )(Celsius)

 P0         Temp: Temp 2    Normal         0     Celsius     (na ,na ,na ,na )(Celsius)

 P0         Temp: Temp 3    Normal         0     Celsius     (na ,na ,na ,na )(Celsius)

 P0          V: PEM In       Normal          0     mV          na
 P0          V: PEM Out      Minor_Low       0     mV          na
 P0          I: PEM In       Normal          0     mA          na
 P0          I: PEM Out      Normal          0     mA          na
 P0          P: In power     Normal          0     Watts       na
 P0          P: Out power    Normal          0     Watts       na
 P0          RPM: fan0       Minor_Low       0     RPM         na
 P1         Temp: Temp 1    Normal         28    Celsius     (na ,na ,na ,na )(Celsius)

 P1         Temp: Temp 2    Normal         31    Celsius     (na ,na ,na ,na )(Celsius)
P1         Temp: Temp 3    Normal         30    Celsius     (na ,na ,na ,na )(Celsius)

 P1          V: PEM In       Normal          226503mV          na
 P1          V: PEM Out      Normal          12000 mV          na
 P1          I: PEM In       Normal          265   mA          na
 P1          I: PEM Out      Normal          3600  mA          na
 P1          P: In power     Normal          54    Watts       na
 P1          P: Out power    Normal          42    Watts       na
 P1          RPM: fan0       Normal          6080  RPM         na
 P2          P: Power        Normal          3     Watts       na
 P2          RPM: fan0       Normal          9480  RPM         na
 P2          RPM: fan1       Normal          9540  RPM         na
 P2          RPM: fan2       Normal          9360  RPM         na
 0/1         P: pwr: Pwr     Normal          11    Watts       na
```

show environment：C8355-G2 の例

この例で、スロット POE0 および POE1 の出力に注目してください。

```
Router# show environment
 Number of Critical alarms:  0

Number of Major alarms:     0

Number of Minor alarms:     0

Slot        Sensor          Current State   Reading
Threshold(Minor,Major,Critical,Shutdown)
----------  --------------  --------------- ------------
-------------------------------------
R0          Temp: Inlet 1   Normal          30     Celsius     (na ,na ,na ,na )(Celsius)

R0          Temp: Inlet 2   Normal          35     Celsius     (na ,na ,na ,na )(Celsius)

R0          Temp: Outlet 1  Normal          42     Celsius     (na ,na ,na ,na )(Celsius)

R0          Temp: Outlet 2  Normal          40     Celsius     (na ,na ,na ,na )(Celsius)

R0          Temp: CPU       Normal          46     Celsius     (na ,na ,95 ,na )(Celsius)

R0          Temp: Working   Normal          30     Celsius     (na ,na ,na ,na )(Celsius)

R0          V: 12V          Normal          12242  mV          na
```

```
R0          V: 5V           Normal          5012    mV          na

R0          V: 3.3V_STBY    Normal          3299    mV          na

R0          V: 3.3V         Normal          3300    mV          na

R0          V: 3.3V_USB     Normal          3302    mV          na

R0          V: 2.5V         Normal          2504    mV          na

R0          V: 1.8V         Normal          1802    mV          na

R0          V: 1.2V_CPU     Normal          1202    mV          na

R0          V: 1.2V         Normal          1205    mV          na

R0          V: 1.1V         Normal          1104    mV          na

R0          V: 1.0V         Normal          998     mV          na

R0          V: 0.8V_SW      Normal          796     mV          na

R0          V: 0.8V_SYS     Normal          851     mV          na

R0          V: 0.8V_CORE    Normal          748     mV          na

R0          V: 0.8V_PHY     Normal          800     mV          na

R0          V: 0.75V        Normal          754     mV          na
R0          P: Power        Normal          33      Watts       na

R0          P: module       Normal          0       Watts       na
```

show environment all：C8375-E-G2 の例

```
Router# show environment all
Sensor List:  Environmental Monitoring
 Sensor           Location          State             Reading
 Temp: Temp 1     P0                Normal            36 Celsius
 Temp: Temp 2     P0                Normal            38 Celsius
 Temp: Temp 3     P0                Normal            38 Celsius
 V: PEM In        P0                Normal            206502 mV
 V: PEM Out       P0                Normal            12000 mV
 I: PEM In        P0                Normal            281 mA
 I: PEM Out       P0                Normal            3500 mA
 P: In pwr        P0                Normal            53 Watts
 P: Out pwr       P0                Normal            43 Watts
 RPM: fan0        P0                Normal            3712 RPM
 RPM: fan0        P2                Normal            7260 RPM
 RPM: fan1        P2                Normal            7260 RPM
 RPM: fan2        P2                Normal            7200 RPM
 P: pwr           P2                Normal            3 Watts
 Temp: Inlet 1    R0                Normal            19 Celsius
 Temp: Inlet 2    R0                Normal            21 Celsius
 Temp: Outlet 1   R0                Normal            25 Celsius
 Temp: Outlet 2   R0                Normal            23 Celsius
 Temp: CP-CPU     R0                Normal            29 Celsius
 V: 12v           R0                Normal            11984 mV
 V: 5v            R0                Normal            5018 mV
 V: 3.3v          R0                Normal            3311 mV
```

```
 V: 3.0v          R0                Normal            2992 mV
 V: 2.5v          R0                Normal            2488 mV
 V: 1.8v          R0                Normal            1785 mV
 V: 1.2v          R0                Normal            1201 mV
 V: 1.2v_CPU      R0                Normal            1200 mV
 V: 1.05v_CPU     R0                Normal            1051 mV
 V: 1.05v         R0                Normal            1058 mV
 V: 1.0v          R0                Normal            1001 mV
 V: 0.6v          R0                Normal            595 mV
 P: pwr           R0                Normal            45 Watts
```

show environment all：C8355-G2 の例

```
Router# show environment all
Sensor List:  Environmental Monitoring
Sensor                   Location        State           Reading

Temp: Inlet 1            R0              Normal          30 Celsius

Temp: Inlet 2            R0              Normal          35 Celsius

Temp: Outlet 1           R0              Normal          41 Celsius

Temp: Outlet 2           R0              Normal          40 Celsius

Temp: CPU                R0              Normal          45 Celsius

Temp: Working            R0              Normal          30 Celsius

V: 12V                   R0              Normal          12250 mV

V: 5V                    R0              Normal          5016 mV

V: 3.3V_STBY             R0              Normal          3297 mV

V: 3.3V                  R0              Normal          3302 mV

V: 3.3V_USB              R0              Normal          3306 mV

V: 2.5V                  R0              Normal          2505 mV

V: 1.8V                  R0              Normal          1802 mV

V: 1.2V_CPU              R0              Normal          1201 mV

V: 1.2V                  R0              Normal          1206 mV

V: 1.1V                  R0              Normal          1104 mV

V: 1.0V                  R0              Normal          999 mV

V: 0.8V_SW               R0              Normal          797 mV

V: 0.8V_SYS              R0              Normal          850 mV

V: 0.8V_CORE             R0              Normal          748 mV

V: 0.8V_PHY              R0              Normal          800 mV

V: 0.75V                 R0              Normal          752 mV

P: Power                 R0              Normal          33 Watts
```

```
P: module               R0              Normal          0 Watts
```

show inventory：C8375-E-G2 の例

```
Router# show inventory
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

NAME: "Chassis", DESCR: "Cisco C8375-E-G2 Chassis"
PID: C8375-E-G2         , VID: V01  , SN: FDO2833M01A

NAME: "Power Supply Module 0", DESCR: "760W AC Power Supply for Cisco C8375"
PID: PWR-CC1-760WAC     , VID: V01  , SN: LIT2748A9MU

NAME: "Power Supply Module 1", DESCR: "400W AC power supply for Cisco C8300 1RU"
PID: PWR-CC1-400WAC     , VID: V01  , SN: LIT2650C53E

NAME: "Fan Tray", DESCR: "Cisco C8300 1RU Fan Assembly"
PID: C8300-FAN-1R       , VID: V02  , SN: LIT2214364L

NAME: "POE Module 0", DESCR: "760W AC Power Supply for Cisco C8375"
PID: PWR-CC1-760WAC     , VID: V01  , SN: LIT2748A9MU

NAME: "module 0", DESCR: "Cisco C8375-E-G2 Built-In NIM controller"
PID: C8375-E-G2         , VID:      , SN:

NAME: "NIM subslot 0/1", DESCR: "C-NIM-8M"
PID: C-NIM-8M           , VID: V01  , SN: FDO26500YDL

NAME: "NIM subslot 0/0", DESCR: "4M-2xSFP+"
PID: 4M-2xSFP+          , VID: V01  , SN:
NAME: "subslot 0/0 transceiver 4", DESCR: "10G AOC5M"
PID: SFP-10G-AOC5M        , VID: V01  , SN: DPZ2618A261-B

NAME: "subslot 0/0 transceiver 5", DESCR: "10G AOC5M"
PID: SFP-10G-AOC5M        , VID: V01  , SN: DPZ2618A261-A
```

```
NAME: "module 1", DESCR: "Cisco C8375-E-G2 Built-In SM controller"

PID: C8375-E-G2        , VID:      , SN:


NAME: "module R0", DESCR: "Cisco C8375-E-G2 Route Processor"

PID: C8375-E-G2        , VID: V01  , SN: FDO28310870


NAME: "module F0", DESCR: "Cisco C8375-E-G2 Forwarding Processor"

PID: C8375-E-G2        , VID:      , SN:
```

show inventory：C8355-G2 の例

```
Router# show inventory

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

INFO: Please use "show license UDI" to get serial number for licensing.

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
NAME: "Chassis", DESCR: "Cisco C8355-G2 Chassis"

PID: C8355-G2          , VID: V01  , SN: FDO2836M06D

NAME: "Power Supply Module 1", DESCR: "230W AC PS w/ POE Module for Cisco C823X/C835X"

PID: PWR-CC1-230WAC    , VID: V02  , SN:

NAME: "POE Module 1", DESCR: "230W AC PS w/ POE Module for Cisco C823X/C835X"

PID: PWR-CC1-230WAC    , VID: V02  , SN:

NAME: "module 0", DESCR: "Cisco C8355-G2 Built-In SM controller"

PID: C8355-G2          , VID:      , SN:

NAME: "NIM subslot 0/0", DESCR: "4M-2x1G-4xSFP+"

PID: 4M-2x1G-4xSFP+    , VID: V01  , SN:

NAME: "subslot 0/0 transceiver 8", DESCR: "SFP+ 10GBASE-SR"

PID: SFP-10G-SR-S        , VID: V01  , SN: OPM26181F0B

NAME: "subslot 0/0 transceiver 9", DESCR: "SFP+ 10GBASE-SR"

PID: SFP-10G-SR-S        , VID: V01  , SN: OPM26200JQA

NAME: "module R0", DESCR: "Cisco C8355-G2 Route Processor"

PID: C8355-G2          , VID: V01  , SN: FDO28330C27
NAME: "harddisk", DESCR: "M.2 USB"

PID: eMMC  HS-SD/MMC   , VID:      , SN:

NAME: "module F0", DESCR: "Cisco C8355-G2 Forwarding Processor"
```

```
PID: C8355-G2          , VID:      , SN:
```

show platform：C8375-E-G2 の例

```
Router# show platform
 Chassis type: C8375-E-G2

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         C8375-E-G2          ok                    3d17h
0/0       4M-2xSFP+           ok                    3d17h
0/1       C-NIM-8M            ok                    3d17h
1         C8375-E-G2          ok                    3d17h
R0        C8375-E-G2          ok, active            3d17h
F0        C8375-E-G2          ok, active            3d17h
P0        PWR-CC1-760WAC      fail, badinput        3d17h
P1        PWR-CC1-400WAC      ok                    3d17h
P2        C8300-FAN-1R        ok                    3d17h
POE0      PWR-CC1-760WAC      fail, badinput        3d17h


Slot      CPLD Version        Firmware Version
--------- ------------------- ----------------------------------------
0         25033132            v17.15(1.17r).s2.cp
1         25033132            v17.15(1.17r).s2.cp
R0        25033132            v17.15(1.17r).s2.cp
F0        25033132            v17.15(1.17r).s2.cp
```

show platform：C8355-G2 の例

```
Router# show platform
 Chassis type: C8355-G2
Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         C8355-G2            ok                     06:21:27
0/0      4M-2x1G-4xSFP+      ok                    06:20:36
```

```
R0        C8355-G2            ok, active            06:21:27
F0        C8355-G2            ok, active            06:21:27
P0        Unknown             empty                 never
P1        PWR-CC1-230WAC      ok                    06:20:52
POE1      PWR-CC1-230WAC      ok                    06:20:52
Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
0         25071533            v17.15(3.3r).s2.cp
R0        25071533            v17.15(3.3r).s2.cp
F0        25071533            v17.15(3.3r).s2.cp
```

show platform diag：C8375-E-G2 の例

```
Router# show platform diag
Chassis type: C8375-E-G2

Slot: 0, C8375-E-G2
Running state               : ok
Internal state              : online
Internal operational state  : ok
Physical insert detect time : 00:00:24 (3d17h ago)
Software declared up time   : 00:01:16 (3d17h ago)
CPLD version                : 25033132
Firmware version            : v17.15(1.17r).s2.cp

Sub-slot: 0/0, 4M-2xSFP+
Operational status          : ok
Internal state              : inserted
Physical insert detect time : 00:01:24 (3d17h ago)
Logical insert detect time  : 00:01:24 (3d17h ago)

Sub-slot: 0/1, C-NIM-8M
Operational status          : ok
Internal state              : inserted
Physical insert detect time : 00:01:26 (3d17h ago)
```

```
Logical insert detect time  : 00:01:26 (3d17h ago)

Sub-slot: 0/4, VDSP-CC

Operational status          : ok

Internal state              : inserted

Physical insert detect time : 00:01:27 (3d17h ago)

Logical insert detect time  : 00:01:27 (3d17h ago)
Slot: 1, C8375-E-G2

Running state               : ok

Internal state              : online

Internal operational state  : ok

Physical insert detect time : 00:00:24 (3d17h ago)

Software declared up time   : 00:01:17 (3d17h ago)

CPLD version                : 25033132

Firmware version            : v17.15(1.17r).s2.cp

Slot: R0, C8375-E-G2

Running state               : ok, active

Internal state              : online

Internal operational state  : ok

Physical insert detect time : 00:00:24 (3d17h ago)

Software declared up time   : 00:00:24 (3d17h ago)

CPLD version                : 25033132

Firmware version            : v17.15(1.17r).s2.cp

Slot: F0, C8375-E-G2

Running state               : ok, active

Internal state              : online

Internal operational state  : ok

Physical insert detect time : 00:00:24 (3d17h ago)

Software declared up time   : 00:01:04 (3d17h ago)

Hardware ready signal time  : 00:01:02 (3d17h ago)

Packet ready signal time    : 00:01:17 (3d17h ago)

CPLD version                : 25033132
```

```
Firmware version            : v17.15(1.17r).s2.cp
Slot: P0, PWR-CC1-760WAC

State                       : fail, badinput

Physical insert detect time : 00:00:02 (3d17h ago)


Slot: P1, PWR-CC1-400WAC

State                       : ok

Physical insert detect time : 00:00:02 (3d17h ago)


Slot: P2, C8300-FAN-1R

State                       : ok

Physical insert detect time : 00:00:02 (3d17h ago)


Slot: POE0, PWR-CC1-760WAC

State                       : fail, badinput

Physical insert detect time : 00:00:02 (3d17h ago)


Slot: POE1, Unknown

State                       : empty

Physical insert detect time : 00:00:00 (never ago)
```

show platform diag：C8355-G2 の例

```
Router# show platform diag
Chassis type: C8355-G2

Slot: 0, C8355-G2

Running state               : ok

Internal state              : online

Internal operational state  : ok

Physical insert detect time : 00:00:22 (06:14:37 ago)

Software declared up time   : 00:01:09 (06:13:50 ago)

CPLD version                : 25071533

Firmware version            : v17.15(3.3r).s2.cp

Sub-slot: 0/0, 4M-2x1G-4xSFP+

Operational status          : ok

Internal state              : inserted
```

```
Physical insert detect time : 00:01:13 (06:13:46 ago)

Logical insert detect time  : 00:01:13 (06:13:46 ago)

Slot: R0, C8355-G2

Running state               : ok, active

Internal state              : online

Internal operational state  : ok

Physical insert detect time : 00:00:22 (06:14:37 ago)

Software declared up time   : 00:00:22 (06:14:37 ago)

CPLD version                : 25071533

Firmware version            : v17.15(3.3r).s2.cp

Slot: F0, C8355-G2

Running state               : ok, active

Internal state              : online
 Internal operational state  : ok

Physical insert detect time : 00:00:22 (06:14:37 ago)

Software declared up time   : 00:01:04 (06:13:55 ago)

Hardware ready signal time  : 00:01:02 (06:13:57 ago)

Packet ready signal time    : 00:01:16 (06:13:43 ago)

CPLD version                : 25071533

Firmware version            : v17.15(3.3r).s2.cp

Slot: P0, Unknown

State                       : empty

Physical insert detect time : 00:00:00 (never ago)

Slot: P1, PWR-CC1-230WAC

State                       : ok

Physical insert detect time : 00:00:03 (06:14:02 ago)

Slot: POE1, PWR-CC1-230WAC

State                       : ok

Physical insert detect time : 00:00:03 (06:14:02 ago)
```

show platform software status control-processor：C8375-E-G2 の例

```
Router# show platform software status control-processor
RP0: online, statistics updated 10 seconds ago
Load Average: healthy
  1-Min: 0.53, status: healthy, under 5.00
  5-Min: 0.90, status: healthy, under 5.00
  15-Min: 0.87, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3884836
  Used: 1976928 (51%), status: healthy
  Free: 1907908 (49%)
  Committed: 3165956 (81%), under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  2.10, System:  2.20, Nice:  0.00, Idle: 95.69
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  2.80, System:  2.60, Nice:  0.00, Idle: 94.50
  IRQ:  0.00, SIRQ:  0.10, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  1.90, System:  2.10, Nice:  0.00, Idle: 96.00
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User: 10.12, System:  0.60, Nice:  0.00, Idle: 89.27
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
```

show platform software status control-processor：C8355-G2 の例

```
Router# show platform software status control-processor
RP0: online, statistics updated 4 seconds ago

Load Average: healthy

1-Min: 11.00, status: healthy, under 18.00

5-Min: 11.03, status: healthy, under 18.00

15-Min: 11.12, status: healthy, under 18.00

Memory (kb): healthy

Total: 16134276

Used: 4006772 (25%), status: healthy

Free: 12127504 (75%)

Committed: 4515476 (28%), under 90%

Per-core Statistics

CPU0: CPU Utilization (percentage of time spent)

User:  1.89, System:  3.19, Nice:  0.00, Idle: 94.20

IRQ:  0.49, SIRQ:  0.19, IOwait:  0.00

CPU1: CPU Utilization (percentage of time spent)

User: 99.90, System:  0.00, Nice:  0.00, Idle:  0.00
```

```
IRQ:  0.10, SIRQ:  0.00, IOwait:  0.00

CPU2: CPU Utilization (percentage of time spent)

User: 99.90, System:  0.00, Nice:  0.00, Idle:  0.00

IRQ:  0.10, SIRQ:  0.00, IOwait:  0.00

CPU3: CPU Utilization (percentage of time spent)

 User: 99.90, System:  0.00, Nice:  0.00, Idle:  0.00

IRQ:  0.10, SIRQ:  0.00, IOwait:  0.00

CPU4: CPU Utilization (percentage of time spent)

User: 99.90, System:  0.00, Nice:  0.00, Idle:  0.00

IRQ:  0.10, SIRQ:  0.00, IOwait:  0.00

CPU5: CPU Utilization (percentage of time spent)

User: 99.80, System:  0.00, Nice:  0.00, Idle:  0.00

IRQ:  0.09, SIRQ:  0.09, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)

User: 99.90, System:  0.00, Nice:  0.00, Idle:  0.00

IRQ:  0.10, SIRQ:  0.00, IOwait:  0.00

CPU4: CPU Utilization (percentage of time spent)

User: 99.90, System:  0.00, Nice:  0.00, Idle:  0.00

IRQ:  0.10, SIRQ:  0.00, IOwait:  0.00

CPU5: CPU Utilization (percentage of time spent)

User: 99.80, System:  0.00, Nice:  0.00, Idle:  0.00

IRQ:  0.09, SIRQ:  0.09, IOwait:  0.00

CPU6: CPU Utilization (percentage of time spent)

User: 99.80, System:  0.00, Nice:  0.00, Idle:  0.00

IRQ:  0.09, SIRQ:  0.09, IOwait:  0.00

CPU7: CPU Utilization (percentage of time spent)

User: 99.90, System:  0.00, Nice:  0.00, Idle:  0.00

IRQ:  0.10, SIRQ:  0.00, IOwait:  0.00

CPU8: CPU Utilization (percentage of time spent)

User: 99.90, System:  0.00, Nice:  0.00, Idle:  0.00

IRQ:  0.10, SIRQ:  0.00, IOwait:  0.00

CPU9: CPU Utilization (percentage of time spent)
```

```
User: 99.90, System:  0.00, Nice:  0.00, Idle:  0.00
IRQ:  0.10, SIRQ:  0.00, IOwait:  0.00
CPU10: CPU Utilization (percentage of time spent)
 User: 14.81, System: 60.06, Nice:  0.00, Idle: 21.62
IRQ:  3.50, SIRQ:  0.00, IOwait:  0.00
CPU11: CPU Utilization (percentage of time spent)
User: 99.90, System:  0.00, Nice:  0.00, Idle:  0.00
IRQ:  0.10, SIRQ:  0.00, IOwait:  0.00
```

show diag slot R0 eeprom detail：C8375-E-G2 の例

```
Router# show diag slot R0 eeprom detail

       Slot R0 EEPROM data:

                                                                    EEPROM
 version           : 4
Compatible Type          : 0xFF
FRU Specific Info        : 0100
PCB Serial Number        : FDO28310870
Controller Type          : 4487
Hardware Revision        : 1.0
PCB Part Number          : 73-20702-08
Board Revision           : 03
Top Assy. Part Number    : 68-7625-01
Deviation Number         : 0
Fab Version              : 08
Product Identifier (PID) : C8375-E-G2
Version Identifier (VID) : V01
CLEI Code                : CMM8K00ARA
Chassis Serial Number    : FDO2833M01A
Chassis MAC Address      : 481b.a465.9470
MAC Address block size   : 144
Manufacturing Test Data  : 00 00 00 00 00 00 00 00
Asset ID                 :
```

show diag slot R0 eeprom detail：C8355-G2 の例

```
Router# show diag slot R0 eeprom detail
Slot R0 EEPROM data:
EEPROM version           : 4
Compatible Type          : 0xFF

FRU Specific Info        : 0100

PCB Serial Number        : FDO28330C27

Controller Type          : 4486

Hardware Revision        : 1.0

PCB Part Number          : 73-20990-07

Board Revision           : 05

Top Assy. Part Number    : 68-7722-01

Deviation Number         : 0

Fab Version              : 07

Product Identifier (PID) : C8355-G2

Version Identifier (VID) : V01

CLEI Code                : CMM8J00ARA

Chassis Serial Number    : FDO2836M06D

Chassis MAC Address      : 4874.104a.e9e0

MAC Address block size   : 96

Manufacturing Test Data  : 00 00 00 00 00 00 00 00

Asset ID                 :
```

show version：C8375-E-G2 の例

```
Router# show version
Cisco IOS XE Software, Version BLD_V1718_THROTTLE_LATEST_20250513_033132_V17_18_0_38
Cisco IOS Software [IOSXE], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M),
Experimental Version 17.18.20250513:042531
[BLD_V1718_THROTTLE_LATEST_20250513_033132:/nobackup/mcpre/s2c-build-ws 101]
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Mon 12-May-25 21:26 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2025 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
```

```
ROM: v17.15(1.19d).s2.cp.RSA2K
Crestone-1 uptime is 4 minutes
Uptime for this control processor is 5 minutes
System returned to ROM by Reload Command
System image file is "bootflash:c8kg2be-universalk9.17.18.01.0.700_V17_18_0_38.SSA.bin"
Last reload reason: Reload Command



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.


Technology Package License Information:

------------------------------------------------------------------
Technology     Type         Technology-package Technology-package
                            Current            Next Reboot
------------------------------------------------------------------
Smart License  Subscription advantage          advantage

The current crypto throughput level is 10000 kbps (Aggregate)


Smart Licensing Status: Smart Licensing Using Policy

cisco C8375-E-G2 (1RU) processor with 3703488K/6147K bytes of memory.
Processor board ID FDO2721M02R
Router operating mode: Autonomous
1 Virtual Ethernet interface
4 Gigabit Ethernet interfaces
4 2.5 Gigabit Ethernet interfaces
8 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
20257791K bytes of flash memory at bootflash:.

Configuration register is 0x3922
```

show version：C8355-G2 の例

```
Router# show version

Cisco IOS XE Software, Version 17.18.01eft30
```

```
Cisco IOS Software [IOSXE], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
 17.18.1eft30, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2025 by Cisco Systems, Inc.

Compiled Fri 25-Jul-25 21:47 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2025 by cisco Systems, Inc.

All rights reserved.  Certain components of Cisco IOS-XE software are

licensed under the GNU General Public License ("GPL") Version 2.0.  The

software code licensed under GPL Version 2.0 is free software that comes

with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such

GPL code under the terms of GPL Version 2.0.  For more details, see the

documentation or "License Notice" file accompanying the IOS-XE software,

or the applicable URL provided on the flyer accompanying the IOS-XE

software.


ROM: v17.15(3.3r).s2.cp

Wilson1 uptime is 5 hours, 53 minutes

Uptime for this control processor is 5 hours, 54 minutes

System returned to ROM by PowerOn

System image file is "bootflash:c8kg2be-universalk9.17.18.01eft30.SPA.bin"

Last reload reason: PowerOn


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and

use. Delivery of Cisco cryptographic products does not imply

third-party authority to import, export, distribute or use encryption.

Importers, exporters, distributors and users are responsible for

compliance with U.S. and local country laws. By using this product you

agree to comply with applicable laws and regulations. If you are unable

to comply with U.S. and local laws, return this product immediately.


A summary of U.S. laws governing Cisco cryptographic products may be found at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html


If you require further assistance please contact us by sending email to
```

```
export@cisco.com.
Technology Package License Information:


------------------------------------------------------------------

Technology     Type         Technology-package Technology-package

Current            Next Reboot

------------------------------------------------------------------

Smart License  Subscription advantage          advantage


The current crypto throughput level is unthrottled
cisco C8355-G2 (1RU) processor with 7799156K/6147K bytes of memory.

Processor board ID FDO2836M06D

Router operating mode: Autonomous

2 Virtual Ethernet interfaces

2 Gigabit Ethernet interfaces

4 Ten Gigabit Ethernet interfaces

4 Five Gigabit Ethernet interfaces

32768K bytes of non-volatile configuration memory.

16777216K bytes of physical memory.

18250751K bytes of flash memory at bootflash:.

29933568K bytes of M.2 USB at harddisk:.


Configuration register is 0x2102
```

電源モードの設定

デバイスおよび接続している Power over Ethernet（PoE）モジュールの両方の電源を設定できます。

- 外部 PoE サービスモジュールの電源モードの設定 （220 ページ）
- 電源モードの設定例 （220 ページ）
- 使用可能な PoE 電力 （221 ページ）

電源モードの詳細については、「電源オプションの概要」のセクションを参照してください。

- Hardware Installation Guide for Cisco 8300 Series Secure Routers

外部 PoE サービスモジュールの電源モードの設定

power inline redundant コマンドを使用して、外部 PoE サービスモジュールの電源を次のように設定します。

- **power inline redundant**：外部 PoE サービスモジュール電源を redundant モードに設定します。
- **no power inline redundant**：外部 PoE サービスモジュール電源を boost モードに設定します。

（注） 外部 PoE サービス モジュールの電源のデフォルト モードは redundant （冗長）モードです。

show power コマンドは、boost と redundant のどちらのモードが設定されているか、およびそのモードがシステムで現在実行中かどうかを示します。

電源モードの設定例

例：主電源装置および PoE モジュールの設定モード：Redundant

この例では、**show power** コマンドにより、主電源とインラインパワーの両方に設定されたモードとして Redundant が表示されます。システムには、400 W と 360 W の電源が 1 つずつあります。

```
Router# show powerMain PSU :
    Router#show power
Main PSU :
    Power Operating Mode : Normal
    Configured Mode : Redundant
    Current runtime state same : Yes
    Total power available : 400 Watts
POE Module :
    Configured Mode : Redundant
    Current runtime state same : Yes
    Total power available : 360 Watts

Router#
```

例：PoE 電源の設定モード：Boost

この例では、**power inline redundant** コマンドの **no** 形式を使用して、インラインパワーを Boost モードに設定しようとしています。インラインパワーのモードは、Boost モードには変更**されません**。Boost モードに変更するには、Redundant モードで使用可能な総電力として 1000 W が必要となるためです。インラインパワーのモードは Redundant です。これは、PoE モジュールの次の値によって示されます。

- `Configured Mode : Boost`

```
   • Current runtime state same : No

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no power inline redundant
Router(config)#
*Jan 31 03:42:40.947: %PLATFORM_POWER-6-MODEMISMATCH: Inline power not in Boost mode
Router(config)#
Router(config)# exit
Router#
*Jan 31 03:36:13.111: %SYS-5-CONFIG_I: Configured from console by console
Router# show power
    Main PSU :
    Power Operating Mode : Normal
    Configured Mode : Redundant
    Current runtime state same : Yes
    Total power available : 400 Watts
POE Module :
    Configured Mode : Boost
    Current runtime state same : Yes
    Total power available : 720 Watts
Router#
```

使用可能な PoE 電力

外部 PoE モジュールで PoE 機能を使用可能にするには、電源から供給される総電力が 760 W 以上である必要があります。

（注） 外部 PoE モジュールで PoE 機能が動作することを確認するには **show platform** コマンドおよび **show power** コマンドを使用して、ルータの PoE 電力の可用性を検証します。

外部 PoE サービスモジュール用に十分な PoE 電力があることを判別するには、**show platform** コマンドと **show power** コマンドを使用し、主電源および PoE インバータのワット値に基づいて、使用可能な PoE 電力量を計算します。

P0 および P1 主電源の値を使用して、総電力量（主電源用）を求めます。次に、PoE1 および PoE2 の電源インバータの値を使用して、PoE 総電力量を計算します。

実際の設定に類似していると思われる操作モードの例を、次の表に示します。

接続している PoE サービス モジュールで PoE 機能が動作するためには、表の最終列の「PoE 総電力」の値が 760 W 以上である必要があります。

（注） 外部PoEモジュールを挿入する前に、ルータに電源インバーターを追加します。このようにしないと、PoE総電力量が十分であったとしても、外部PoEモジュールによりPoE電力が使用されず、PoE 機能が適切に機能させるためにモジュールをリブートする必要が生じます。

主電源で電力モードとして Boost または Redundant を設定すると、PoE 総電力量の値に影響が生じることがあります。

次の表に、総電力量をワット単位で示します。主電源のワット数は、「主電源P0」および「主電源 P1」列に示されます。PoE インバーターのワット数は、「PoE0」および「PoE1」列に示されます。

表 *18 : C8375-E-G2* の動作モード

モードの例	主電源 P0	主電源 P1	設定モード	総電力量（主電源）	PoE0	PoE1	設定モード	PoE 総電力量
1	400	なし	Redundant	400	なし	なし	Redundant または Boost	0（なし）
2	なし	400	冗長	400	なし	なし	Redundant または Boost	0（なし）
3	400	なし	Redundant	400	360	なし	Redundant または Boost	360
4	なし	400	冗長	400	なし	360	Redundant または Boost	360
5	400	400	冗長	400	なし	なし	Redundant または Boost	0（なし）
6 （注） P0 に 760WAC を装着した場合のみ	400	なし	Redundant	400	360	なし	Redundant または Boost	360
7 （注） P1 に 760WAC を装着した場合のみ	なし	400	冗長	400	なし	360	Redundant または Boost	360
8	400	400	冗長	400	360	360	冗長	360

モードの例	主電源 P0	主電源 P1	設定モード	総電力量（主電源）	PoE0	PoE1	設定モード	PoE 総電力量
9	400	400	冗長	400	360	360	BOOST	720
10	500	なし	Redundant	500	なし	なし	Redundant または Boost	0（なし）
11	なし	500	冗長	500	なし	なし	Redundant または Boost	0（なし）
12	500	500	冗長	500	なし	なし	Redundant または Boost	0（なし）

（注） 上記の表では、360 W 以上の PoE 総電力量が使用可能になるには、（主電源の）「総電力量」が 760 W 以上である必要があります。

PoE 総電力量が 720 W（モードの例 6 を参照）の場合、760 W の主電源（`Boost` モード）が 2 台と、PoE インバータ（`Boost` モード）が 2 台必要です。

表 *19 : C8355-G2* の動作モード

モードの例	主電源 P0	主電源 P1	設定モード	総電力量（主電源）	PoE0	PoE1	設定モード	PoE 総電力量
1	110	なし	Redundant	110	なし	なし	Redundant または Boost	0（なし）
2	なし	110	冗長	110	なし	なし	Redundant または Boost	0（なし）
3 （注） P0 に 230WAC を装着した場合のみ	110	なし	Redundant	110	なし	なし	Redundant または Boost	0（なし）

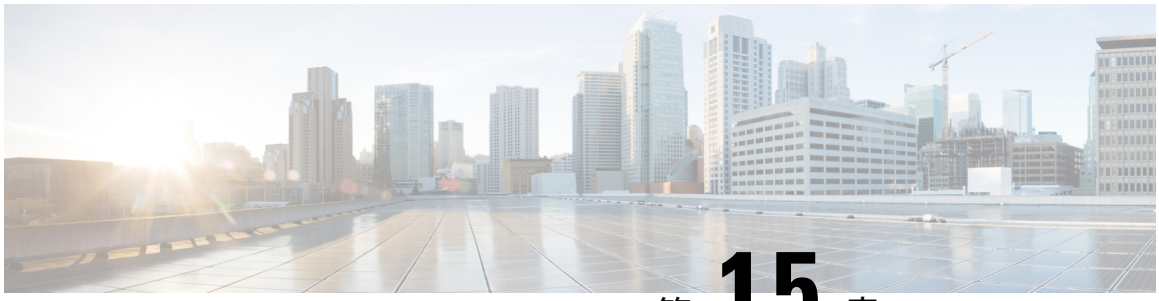
モードの例	主電源 P0	主電源 P1	設定モード	総電力量（主電源）	PoE0	PoE1	設定モード	PoE 総電力量
4	なし	110	冗長	110	なし	120	Redundant または Boost	120
5	110	110	冗長	110	なし	なし	Redundant または Boost	0（なし）
6 （注） P0 および P1 に 230WAC を装着した場合	110	110	冗長	110	なし	120	Redundant または Boost	120
7 （注） P0 に 110WAC を、P1 に 230WAC を装着した場合	110	110	冗長	110	なし	120	Redundant または Boost	120
8	110	110	冗長	110	なし	なし	Redundant	0（なし）

（注） C8355-G2 の場合、電源コンセント 1 のみが PoE をサポートします。したがって、すべてのシナリオで PoE0 は常に「なし」です。

⚠

注意 電源と電源インバータを取り外す際には（特に `Boost` モードで動作している場合は）注意が必要です。総消費電力が、1 台の電源だけで供給可能な電力を超えている場合、この状態で電源を取り外すとハードウェアが損傷する可能性があります。その結果、システムが不安定になったり使用できない状態になることがあります。

同様に、サービス モジュールに PoE 電力を供給する PoE インバーターが 1 台だけの場合、この状態でPoEインバーターを取り外すと、ハードウェアが損傷し、システムが不安定または使用不能になることがあります。



第 15 章

ハイ アベイラビリティの設定

Cisco ハイ アベイラビリティ（HA）テクノロジーにより、ネットワークのどの部分でも発生し得る中断から迅速にリカバリでき、ネットワーク全体の保護が実現します。ネットワークのハードウェアとソフトウェアは、Cisco ハイ アベイラビリティ テクノロジーと連携して、中断から迅速にリカバリすることに加えて、ユーザとネットワーク アプリケーションに対して障害の透過性を提供します。

ここでは、デバイスで Cisco ハイアベイラビリティ機能を設定する方法について説明します。

Cisco ハイアベイラビリティ

ルータ独自のハードウェアおよびソフトウェア アーキテクチャは、あらゆるネットワーク イベントの発生時にルータのアップタイムを最大化するように設計されているため、すべてのネットワーク シナリオで最大アップタイムと復元力が実現します。

ここでは、Cisco 8300 シリーズ セキュアルータで使用される Cisco ハイアベイラビリティのいくつかの側面について説明します。

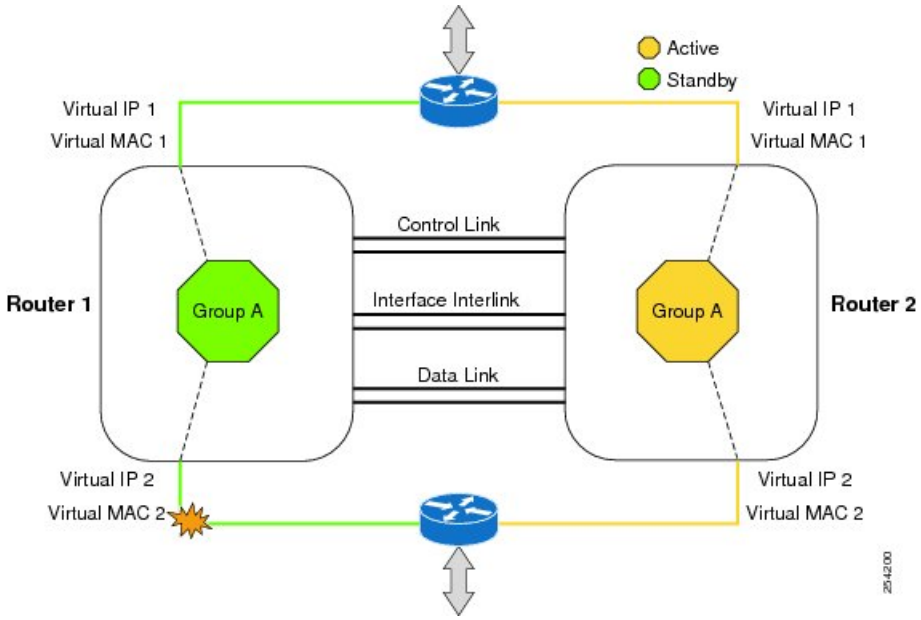
シャーシ間ハイ アベイラビリティ

シャーシ間ハイ アベイラビリティ（HA）機能は、ボックスツーボックス冗長性機能とも呼ばれます。シャーシ間高可用性を使用すると、相互にバックアップとして動作するデバイスのペアを設定できます。いくつかのフェールオーバー条件に基づいてアクティブデバイスを決定す

るよう、この機能を設定できます。フェールオーバーが発生すると、中断なくスタンバイデバイスが引き継ぎ、コールシグナリングの処理と、メディア転送タスクの実行を開始します。

冗長インターフェイスのグループは、冗長グループと呼ばれます。次の図は、アクティブ/スタンバイ デバイスのシナリオを示しています。また、1つの発信インターフェイスを持つデバイスのペアについて、冗長グループを設定する方法を示します。

図 *2:* 冗長グループの設定



設定可能なコントロールリンクおよびデータ同期リンクによってデバイスが結合されます。コントロール リンクは、デバイスのステータスを通信するために使用されます。データ同期リンクを使ってステートフル情報を転送し、コールとメディア フローに関してステートフル データベースを同期します。冗長インターフェイスの各ペアは同じ一意のID番号（RIIとも呼びます）で設定されます。デバイスでのシャーシ間HA設定の詳細については、シャーシ間ハイアベイラビリティの設定 （229 ページ） を参照してください。

双方向フォワーディング検出

双方向フォワーディング検出（BFD）は、すべてのメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルのために短時間での転送パス障害検出を提供するよう設計された検出プロトコルです。BFDは、転送パス障害を高速で検出するだけでなく、ネットワーク管理者のために一貫した障害検出方式を提供します。ネットワーク管理者はBFD を使用することで、さまざまなルーティング プロトコルのHELLOメカニズムにより、変動速度ではなく一定速度で転送パス障害を検出できるため、ネットワーク プロファイリングおよびプランニングが容易になります。また、再収束時間の整合性が保たれ、予測可能になります。

BFD の詳細については、『IP Routing: BFD Configuration Guide』の「Bidirectional Forwarding Detection」を参照してください。

双方向フォワーディング検出オフロード

双方向フォワーディング検出オフロード機能は、障害検出にかかる時間を短縮するために、BDF セッション管理をフォワーディング エンジンにオフロードできるようにします。BFD オフロードにより、ルーティング テーブル再計算のために迅速な障害検出パケット（メッセージ）をルーティング プロトコルに送信することで、全体的なネットワーク コンバージェンス時間が短縮されます。BFD オフロードの設定 （230 ページ）を参照してください。

Cisco ハイアベイラビリティの設定

シャーシ間ハイアベイラビリティの設定

前提条件

- アクティブデバイスとスタンバイ デバイスは、同じバージョンの Cisco IOS XE ソフトウェアを実行する必要があります。
- アクティブ デバイスとスタンバイは、制御パス用の L2 接続を介して接続する必要があります。
- タイムスタンプとコール タイマーが一致するように、両方のデバイスでネットワーク タイム プロトコル（NTP）を設定するか、クロックを同じに設定する必要があります。
- データの正確な同期のために、アクティブデバイスとスタンバイデバイスの両方で Virtual Route Forwarding（VRF）を同じ順序で定義する必要があります。
- 遅延時間は、タイム アウトを防止するため、すべての制御リンクおよびデータ リンクで最小にする必要があります。
- Gigabit EtherChannel などの物理的に冗長なリンクを、制御パスおよびデータ パスに使用する必要があります。

制約事項

- ボックスツーボックス アプリケーションのフェールオーバー時間は、非ボックスツーボックス アプリケーションではより高くなります。
- LAN および MESH シナリオはサポートされません。

- VRF はサポートされておらず、ZBFW 高可用性データおよび制御インターフェイスでは設定できません。
- Front Panel Gigabit Ethernet（FPGE）インターフェイスでサポートされる仮想 MAC の最大数は、プラットフォームによって異なります。FPGE インターフェイスについては、『Hardware Installation Guide for Cisco 8300 Series Secure Router』を参照してください。
- スタンバイデバイスに複製された設定は、スタートアップ コンフィギュレーションに適用されず、実行コンフィギュレーションに適用されます。アクティブデバイスから同期された変更を適用するには、スタンバイデバイスで **write memory** コマンドを実行する必要があります。

シャーシ間ハイアベイラビリティの設定方法

ルータでのシャーシ間高可用性の設定の詳細については、『IP Addressing: NAT Configuration Guide, Cisco IOS XE Release 3S』を参照してください。

双方向フォワーディングの設定

使用中のデバイスでの BFD の設定については、『IP Routing BFD Configuration Guide』を参照してください。

BFD コマンドについては、『Cisco IOS IP Routing: Protocol-Independent Command Reference』を参照してください。

BFD オフロードの設定

制約事項

- BFD バージョン 1 のみサポートされます。
- これを設定すると、オフロードされる BFD セッションだけがサポートされ、RP の BFD セッションはサポートされません。
- BFD の非同期モードまたはエコーなしモードだけがサポートされます。
- 511 非同期 BFD セッションがサポートされます。
- BFD ハードウェア オフロードは、エコーなしモードの IPv4 セションでのみサポートされます。
- BFD オフロードは、ポート チャネル インターフェイスでのみサポートされます。
- BFD オフロードは、イーサネット インターフェース用にのみサポートされます。
- BFD オフロードは、IPv6 BFD セッションではサポートされません。
- BFD オフロードは、TE/FRR を使用する BFD セッションではサポートされません。

BFD オフロードの設定方法

BFDオフロード機能はデフォルトでイネーブルに設定されています。ルートプロセッサでBFDハードウェア オフロードを設定できます。詳細については、『Configuring BFD』と『IP Routing BFD Configuration Guide』を参照してください。

シャーシ間ハイ アベイラビリティの検証

シャーシ間ハイアベイラビリティを検証するには、次の **show** コマンドを使用します。

（注） シャーシ間ハイ アベイラビリティの設定に関する前提条件とマニュアルへのリンクが、シャーシ間ハイアベイラビリティの設定 （229 ページ）にリストされています。

- **show redundancy application group [group-id | all]**
- **show redundancy application transport {client | group [group-id]}**
- **show redundancy application control-interface group [group-id]**
- **show redundancy application faults group [group-id]**
- **show redundancy application protocol {protocol-id | group [group-id]}**
- **show redundancy application if-mgr group [group-id]**
- **show redundancy application data-interface group [group-id]**

次の例は、デバイスで設定された冗長アプリケーショングループを示します。

```
Router# show redundancy application group
Group ID    Group Name                     State
--------    ----------                     -----
1           Generic-Redundancy-1           STANDBY
2           Generic-Redundancy2            ACTIVE
```

次の例は、冗長アプリケーショングループ 1 の詳細を示します。

```
Router# show redundancy application group 1
Group ID:1
Group Name:Generic-Redundancy-1

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
RF state: STANDBY HOT
Peer RF state: ACTIVE
```

次の例は、冗長アプリケーショングループ 2 の詳細を示します。

```
Router# show redundancy application group 2
Group ID:2
```

```
Group Name:Generic-Redundancy2

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-two
RF state: ACTIVE
Peer RF state: STANDBY HOT
```

次の例は、冗長アプリケーション トランスポート クライアントの詳細を示します。

```
Router# show redundancy application transport client
Client          Conn#  Priority   Interface   L3        L4
( 0)RF            0      1         CTRL       IPV4      SCTP

( 1)MCP_HA        1      1         DATA       IPV4      UDP_REL

( 4)AR            0      1         ASYM       IPV4      UDP

( 5)CF            0      1         DATA       IPV4      SCTP
```

次の例は、冗長アプリケーション トランスポート グループの設定の詳細を示します。

```
Router# show redundancy application transport group
Transport Information for RG (1)
Client = RF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
0    0       192.0.2.8       59000    192.0.2.4       59000    CTRL    IPV4    SCTP
Client = MCP_HA
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
1    1       10.10.2.10      53000    10.10.6.9       53000    DATA    IPV4    UDP_REL
Client = AR
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
2    0       192.0.2.3       0       192.0.2.3        0        NONE_IN NONE_L3 NONE_L4
Client = CF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
3    0       10.10.2.10      59001    10.10.6.9       59001    DATA    IPV4    SCTP
Transport Information for RG (2)
Client = RF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
8    0       192.0.2.8       59004    192.0.2.2       59004    CTRL    IPV4    SCTP
Client = MCP_HA
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
9    1       10.10.2.10      53002    10.10.6.9       53002    DATA    IPV4    UDP_REL
Client = AR
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
10   0       192.0.2.3       0        192.0.2.3       0        NONE_IN NONE_L3 NONE_L4
Client = CF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
11   0       10.10.2.10      59005    10.10.6.9       59005    DATA    IPV4    SCTP
```

次の例は、冗長アプリケーション トランスポート グループ 1 の設定の詳細を示します。

```
Router# show redundancy application transport group 1
Transport Information for RG (1)
Client = RF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
0    0       192.0.2.8       59000    192.0.2.4       59000    CTRL    IPV4    SCTP
Client = MCP_HA
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
```

```
1    1       10.10.2.10      53000    10.10.2.10      53000    DATA    IPV4    UDP_REL
Client = AR
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
2    0       192.0.2.3       0        192.0.2.3       0        NONE_IN NONE_L3 NONE_L4
Client = CF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
3    0       10.10.2.10      59001    10.10.2.10      59001    DATA    IPV4    SCTP
```

次の例は、冗長アプリケーション トランスポート グループ 2 の設定の詳細を示します。

```
Router# show redundancy application transport group 2
Transport Information for RG (2)
Client = RF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
8    0       192.0.2.8       59004    192.0.2.4       59004    CTRL    IPV4    SCTP
Client = MCP_HA
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
9    1       10.10.2.10      53002    10.10.2.10      53002    DATA    IPV4    UDP_REL
Client = AR
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
10   0       192.0.2.3       0        192.0.2.3       0        NONE_IN NONE_L3 NONE_L4
Client = CF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
11   0       10.10.2.10      59005    10.10.2.10      59005    DATA    IPV4    SCTP
```

次の例は、冗長アプリケーション制御インターフェイスグループの設定の詳細を示します。

```
Router# show redundancy application control-interface group
The control interface for rg[1] is TwoGigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
Peer: 192.0.2.4 Active RGs: 1 Standby RGs: 2 BFD handle: 0

The control interface for rg[2] is TwoGigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
Peer: 192.0.2.4 Active RGs: 1 Standby RGs: 2 BFD handle: 0
```

次の例は、冗長アプリケーション制御インターフェイスグループ 1 の設定の詳細を示します。

```
Router# show redundancy application control-interface group 1
The control interface for rg[1] is TwoGigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
Peer: 192.0.2.4 Active RGs: 1 Standby RGs: 2 BFD handle: 0
```

次の例は、冗長アプリケーション制御インターフェイスグループ 2 の設定の詳細を示します。

```
Router# show redundancy application control-interface group 2
The control interface for rg[2] is TwoGigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
Peer: 192.0.2.4 Active RGs: 1 Standby RGs: 2 BFD handle: 0
```

次の例は、冗長アプリケーション フォールト グループの設定の詳細を示します。

```
Router# show redundancy application faults group
Faults states Group 1 info:
Runtime priority: [50]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
```

```
Total # of down/up state changes due to faults: 2
Faults states Group 2 info:
Runtime priority: [135]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
```

次の例は、冗長アプリケーション フォールト グループ 1 に固有の設定の詳細を示します。

```
Router# show redundancy application faults group 1
Faults states Group 1 info:
Runtime priority: [50]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
```

次の例は、冗長アプリケーション フォールト グループ 2 に固有の設定の詳細を示します。

```
Router# show redundancy application faults group 2
Faults states Group 2 info:
Runtime priority: [135]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
```

次の例は、冗長アプリケーション プロトコル グループの設定の詳細を示します。

```
Router# show redundancy application protocol group
RG Protocol RG 1
------------------
Role: Standby
Negotiation: Enabled
Priority: 50
Protocol state: Standby-hot
Ctrl Intf(s) state: Up
Active Peer: address 192.0.4.2, priority 150, intf Gi0/0/0
Standby Peer: Local
Log counters:
role change to active: 0
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
Ctx State: Standby
Protocol ID: 1
Media type: Default
Control Interface: TwoGigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 117, Bytes 7254, HA Seq 0, Seq Number 117, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 115, Bytes 3910, HA Seq 0, Seq Number 1453975, Pkt Loss 0



RG Protocol RG 2
```

```
------------------
Role: Active
Negotiation: Enabled
Priority: 135
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 192.0.4.2, priority 130, intf Gi0/0/0
Log counters:
role change to active: 1
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 2
--------------------------
Ctx State: Active
Protocol ID: 2
Media type: Default
Control Interface: TwoGigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 118, Bytes 7316, HA Seq 0, Seq Number 118, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 1
Standby Peer: Present. Hold Timer: 10000
Pkts 102, Bytes 3468, HA Seq 0, Seq Number 1453977, Pkt Loss 0
```

次の例は、冗長アプリケーション プロトコル グループ 1 の設定の詳細を示します。

```
Router# show redundancy application protocol group 1
RG Protocol RG 1
------------------
Role: Standby
Negotiation: Enabled
Priority: 50
Protocol state: Standby-hot
Ctrl Intf(s) state: Up
Active Peer: address 192.0.4.2, priority 150, intf Gi0/0/0
Standby Peer: Local
Log counters:
role change to active: 0
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
Ctx State: Standby
Protocol ID: 1
Media type: Default
Control Interface: TwoGigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 120, Bytes 7440, HA Seq 0, Seq Number 120, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
```

```
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 118, Bytes 4012, HA Seq 0, Seq Number 1453978, Pkt Loss 0
```

次の例は、冗長アプリケーション プロトコル グループ 2 の設定の詳細を示します。

```
Router# show redundancy application protocol group 2
RG Protocol RG 2
------------------
Role: Active
Negotiation: Enabled
Priority: 135
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 192.0.4.2, priority 130, intf Gi0/0/0
Log counters:
role change to active: 1
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 2
--------------------------
Ctx State: Active
Protocol ID: 2
Media type: Default
Control Interface: TwoGigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 123, Bytes 7626, HA Seq 0, Seq Number 123, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 1
Standby Peer: Present. Hold Timer: 10000
Pkts 107, Bytes 3638, HA Seq 0, Seq Number 1453982, Pkt Loss 0
```

次の例は、冗長アプリケーションプロトコル 1 の設定の詳細を示します。

```
Router# show redundancy application protocol 1
Protocol id: 1, name: rg-protocol-1
BFD: ENABLE
Hello timer in msecs: 3000
Hold timer in msecs: 10000
OVLD-1#show redundancy application protocol 2
Protocol id: 2, name: rg-protocol-2
BFD: ENABLE
Hello timer in msecs: 3000
Hold timer in msecs: 10000
```

次の例は、冗長アプリケーション インターフェイス マネージャ グループの設定の詳細を示します。

```
Router# show redundancy application if-mgr group
 RG ID: 1
 ==========

 interface      TwoGigabitEthernet0/0/3.152
 ---------------------------------------
 VMAC           0007.b421.4e21
```

```
VIP             203.0.113.1
Shut            shut
Decrement       10

interface       TwoGigabitEthernet0/0/2.152
----------------------------------------
VMAC            0007.b421.5209
VIP             203.0.113.4
Shut            shut
Decrement       10


RG ID: 2
==========

interface       TwoGigabitEthernet0/0/3.166
----------------------------------------
VMAC            0007.b422.14d6
VIP             203.0.113.6
Shut            no shut
Decrement       10

interface       TwoGigabitEthernet0/0/2.166
----------------------------------------
VMAC            0007.b422.0d06
VIP             203.0.113.9
Shut            no shut
Decrement       10
```

次の例は、冗長アプリケーション インターフェイス マネージャ グループ 1 およびグループ 2 の設定の詳細を示します。

```
Router# show redundancy application if-mgr group 1

RG ID: 1
==========

interface       TwoGigabitEthernet0/0/3.152
----------------------------------------
VMAC            0007.b421.4e21
VIP             203.0.113.3
Shut            shut
Decrement       10

interface       TwoGigabitEthernet0/0/2.152
----------------------------------------
VMAC            0007.b421.5209
VIP             203.0.113.2
Shut            shut
Decrement       10

Router# show redundancy application if-mgr group 2
RG ID: 2
==========

interface     TwoGigabitEthernet0/0/3.166
----------------------------------------
VMAC            0007.b422.14d6
VIP             203.0.113.5
Shut            no shut
Decrement       10

interface       TwoGigabitEthernet0/0/2.166
----------------------------------------
```

```
VMAC            0007.b422.0d06
VIP             203.0.113.7
Shut            no shut
Decrement       10
```

次の例は、冗長アプリケーションデータインターフェイス グループの設定の詳細を示します。

```
Router# show redundancy application data-interface group
The data interface for rg[1] is TwoGigabitEthernet0/0/1
The data interface for rg[2] is TwoGigabitEthernet0/0/1
```

次の例は、冗長アプリケーション データ インターフェイス グループ 1 およびグループ 2 に固有の設定の詳細を示します。

```
Router# show redundancy application data-interface group 1
The data interface for rg[1] is TwoGigabitEthernet0/0/1

Router # show redundancy application data-interface group 2
The data interface for rg[2] is TwoGigabitEthernet0/0/1
```

BFD オフロードの検証

デバイスの BFD オフロード機能を検証および監視するには、次のコマンドを使用します。

（注） BFDオフロードの設定については、双方向フォワーディングの設定（230ページ）に説明があります。

- **show bfd neighbors [details]**
- **debug bfd [packet | event]**
- **debug bfd event**

show bfd neighbors コマンドは、BFD 隣接関係データベースを表示します。

```
Router# show bfd neighbor

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
192.0.2.1                             362/1277       Up        Up        Gi0/0/1.2
192.0.2.5                             445/1278       Up        Up        Gi0/0/1.3
192.0.2.3                            1093/961        Up        Up        Gi0/0/1.4
192.0.2.2                            1244/946        Up        Up        Gi0/0/1.5
192.0.2.6                            1094/937        Up        Up        Gi0/0/1.6
192.0.2.7                            1097/1260       Up        Up        Gi0/0/1.7
192.0.2.4                            1098/929        Up        Up        Gi0/0/1.8
192.0.2.9                            1111/928        Up        Up        Gi0/0/1.9
192.0.2.8                            1100/1254       Up        Up        Gi0/0/1.10
```

debug bfd neighbor detail コマンドは、BFD パケットに関連するデバッグ情報を表示します。

```
Router# show bfd neighbor detail

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
192.0.2.1                             362/1277       Up        Up        Gi0/0/1.2
Session state is UP and not using echo function.
Session Host: Hardware
```

```
OurAddr: 192.0.2.2
Handle: 33
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 50(0)
Rx Count: 3465, Rx Interval (ms) min/max/avg: 42/51/46
Tx Count: 3466, Tx Interval (ms) min/max/avg: 39/52/46
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: CEF EIGRP
Uptime: 00:02:50
Last packet: Version: 1                  - Diagnostic: 0
             State bit: Up               - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             C bit: 1
             Multiplier: 3               - Length: 24
             My Discr.: 1277             - Your Discr.: 362
             Min tx interval: 50000      - Min rx interval: 50000
             Min Echo interval: 0
```

show bfd summary コマンドは、BFD の概要情報を表示します。

```
Router# show bfd summary

                    Session          Up          Down

Total                   400         400             0
```

show bfd drops コマンドは、BFD でドロップされたパケットの数を表示します。

```
Router# show bfd drops
BFD Drop Statistics
                       IPV4     IPV6    IPV4-M    IPV6-M    MPLS_PW   MPLS_TP_LSP
Invalid TTL               0        0         0         0          0         0
BFD Not Configured        0        0         0         0          0         0
No BFD Adjacency         33        0         0         0          0         0
Invalid Header Bits       0        0         0         0          0         0
Invalid Discriminator     1        0         0         0          0         0
Session AdminDown        94        0         0         0          0         0
Authen invalid BFD ver    0        0         0         0          0         0
Authen invalid len        0        0         0         0          0         0
Authen invalid seq        0        0         0         0          0         0
Authen failed             0        0         0         0          0         0
```

debug bfd packet コマンドは、BFD 制御パケットに関するデバッグ情報を表示します。

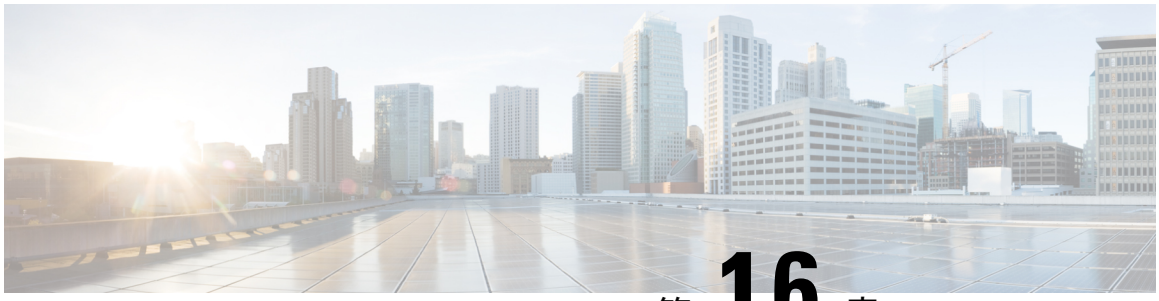
```
Router# debug bfd packet
*Nov 12 23:08:27.982: BFD-DEBUG Packet: Rx IP:192.0.2.1 ld/rd:1941/0 diag:0(No Diagnostic)
 Down C cnt:4 ttl:254 (0)
*Nov 12 23:08:27.982: BFD-DEBUG Packet: Tx IP:192.0.2.1 ld/rd:983/1941 diag:3(Neighbor
Signaled Session Down) Init  C cnt:44 (0)
*Nov 12 23:08:28.007: BFD-DEBUG Packet: Rx IP:192.0.2.1 ld/rd:1941/983 diag:0(No
Diagnostic) Up PC cnt:4 ttl:254 (0)
*Nov 12 23:08:28.007: BFD-DEBUG Packet: Tx IP:192.0.2.1 ld/rd:983/1941 diag:0(No
Diagnostic) Up F C cnt:0 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Rx IP:192.0.2.1 ld/rd:1941/983 diag:0(No
Diagnostic) Up FC cnt:0 ttl:254 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Tx IP:192.0.2.1 ld/rd:983/1941 diag:0(No
Diagnostic) Up  C cnt:0 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Rx IP:192.0.2.3 ld/rd:1907/0 diag:0(No Diagnostic)
 Down C cnt:3 ttl:254 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Tx IP:192.0.2.3 ld/rd:993/1907 diag:3(Neighbor
Signaled Session Down) Init  C cnt:43 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Rx IP:192.0.2.1 ld/rd:1941/983 diag:0(No
Diagnostic) Up C cnt:0 ttl:254 (0)
```

```
*Nov 12 23:08:28.626: BFD-DEBUG Packet: Rx IP:192.0.2.3 ld/rd:1907/993 diag:0(No
Diagnostic) Up PC cnt:3 ttl:254 (0)
*Nov 12 23:08:28.626: BFD-DEBUG Packet: Tx IP:192.0.2.3 ld/rd:993/1907 diag:0(No
Diagnostic) Up F C cnt:0 (0)
*Nov 12 23:08:28.645: BFD-DEBUG Packet: Rx IP:192.0.2.3 ld/rd:1907/993 diag:0(No
Diagnostic) Up C cnt:0 ttl:254 (0)
*Nov 12 23:08:28.700: BFD-DEBUG Packet: Rx IP:192.0.2.3 ld/rd:1907/993 diag:0(No
Diagnostic) Up FC cnt:0 ttl:254 (0)
*Nov 12 23:08:28.700: BFD-DEBUG Packet: Tx IP:192.0.2.3 ld/rd:993/1907 diag:0(No
Diagnostic) Up  C cnt:0 (0)
*Nov 12 23:08:28.993: BFD-DEBUG Packet: Rx IP:192.0.2.3 ld/rd:1907/993 diag:0(No
Diagnostic) Up C cnt:0 ttl:254 (0)
```

debug bfd event コマンドは、BFD 状態遷移に関するデバッグ情報を表示します。

```
Router# deb bfd event

*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.6, ld:1401,
handle:77, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.6, ld:1401, handle:77,
 event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.10, ld:1400,
handle:39, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.10, ld:1400,
handle:39, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.8, ld:1399,
handle:25, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.8, ld:1399, handle:25,
 event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.5, ld:1403,
handle:173, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.6, ld:1403,
handle:173, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.4, ld:1402,
handle:95, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.4, ld:1402, handle:95,
 event:DOWN adminDown, (0)
*Nov 12 23:11:30.639: BFD-HW-API: Handle 1404: Timers: Tx timer 1000000 Detect timer 0
*Nov 12 23:11:30.639: BFD-HW-API: Handle 1404: Flags: Poll 0 Final 0
*Nov 12 23:11:30.639: BFD-HW-API: Handle 1404: Buffer: 0x23480318 0x0000057C 0x00000000
 0x000F4240 0x000F4240 0x00000000 size 24
*Nov 12 23:11:30.641: BFD-HW-API: Handle 1405: Timers: Tx timer 1000000 Detect timer 0
*Nov 12 23:11:30.641: BFD-HW-API: Handle 1405: Flags: Poll 0 Final 0
*Nov 12 23:11:30.641: BFD-HW-API: Handle 1405: Buffer: 0x23480318 0x0000057D 0x00000000
 0x000F4240 0x000F4240 0x00000000 size 24
*Nov 12 23:11:30.649: BFD-DEBUG Packet: Rx IP:192.0.2.6 ld/rd:1601/1404
diag:7(Administratively Down) AdminDown C cnt:0 ttl:254 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: V1 FSM ld:1404 handle:207 event:RX ADMINDOWN
state:UP (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: resetting timestamps ld:1404 handle:207 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.1, ld:1404,
handle:207, event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Packet: Tx IP:192.0.2.1 ld/rd:1404/0 diag:3(Neighbor
Signaled Session Down) Down C cnt:0 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Packet: Rx IP:192.0.2.1 ld/rd:1620/1405
diag:7(Administratively Down) AdminDown C cnt:0 ttl:254 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: V1 FSM ld:1405 handle:209 event:RX ADMINDOWN
state:UP (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: resetting timestamps ld:1405 handle:209 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.1, ld:1405,
handle:209, event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Packet: Tx IP:192.0.2.7 ld/rd:1405/0 diag:3(Neighbor
Signaled Session Down) Down C cnt:0 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.7, ld:1404,
handle:207, event:DOWN adminDown, (0)
```

```
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.7, ld:1404,
handle:207, event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.7, ld:1405,
handle:209, event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.7, ld:1405,
handle:209, event:DOWN adminDown, (0)
*Nov 12 23:11:31.035: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 192.0.2.8
```



第 16 章

セキュアストレージの設定

セキュア ストレージ機能では、重要な設定情報を暗号化して保護できます。VPN、IPSec とその他の非対称キーペア、事前共有秘密、タイプ 6 のパスワード暗号化キーおよび特定のクレデンシャルを暗号化します。インスタンス固有の暗号キーは、危険にさらされることを防ぐためにハードウェアのトラスト アンカーに保管されます。

デフォルトでは、この機能はハードウェアのトラストアンカーを備えたプラットフォームで有効です。この機能は、ハードウェアのトラストアンカーがないプラットフォームではサポートされません。

セキュアストレージの有効化

始める前に

デフォルトでは、この機能はプラットフォームで有効です。この手順は、無効になっているプラットフォームで使用します。

手順

ステップ 1 Config terminal

例：

```
router#config terminal
```

コンフィギュレーション モードを開始します。

ステップ 2 service private-config-encryption

例：

```
router(config)# service private-config-encryption
```

プラットフォームでセキュリティ ストレージ機能を有効にします。

ステップ 3 do write memory

例：

```
router(config)# do write memory
```

private-config ファイルを暗号化し、暗号化フォーマットで保存します。

例

次に、セキュアストレージを有効にする例を示します。

```
router#config terminal
router(config)# service private-config-encryption
router(config)# do write memory
```

セキュアストレージの無効化

始める前に

プラットフォームでセキュア ストレージ機能を無効にするには、次のタスクを実行します。

手順

ステップ 1 Config terminal

例：

```
router#config terminal
```

コンフィギュレーション モードを開始します。

ステップ 2 no service private-config-encryption

例：

```
router(config)# no service private-config-encryption
```

プラットフォームでセキュリティ ストレージ機能を無効にします。

ステップ 3 do write memory

例：

```
router(config)# do write memory
```

private-config ファイルを復号し、プレーン フォーマットで保存します。

例

次に、セキュアストレージをディセーブルにする例を示します。

```
router#config terminal
router(config)# no service private-config-encryption
router(config)# do write memory
```

暗号化のステータスの確認

暗号化のステータスを確認するには、**show parser encrypt file status** コマンドを使用します。次のコマンド出力は、機能は利用できるが、ファイルが暗号化されていないことを示します。ファイルは「プレーン テキスト」形式です。

```
router#show parser encrypt file status
Feature: Enabled
File Format: Plain Text
Encryption Version: Ver1
```

次のコマンド出力は、機能は有効で、ファイルが暗号化されていることを示します。ファイルは「暗号テキスト」形式です。

```
router#show parser encrypt file status
Feature: Enabled
File Format: Cipher Text
Encryption Version: Ver1
```

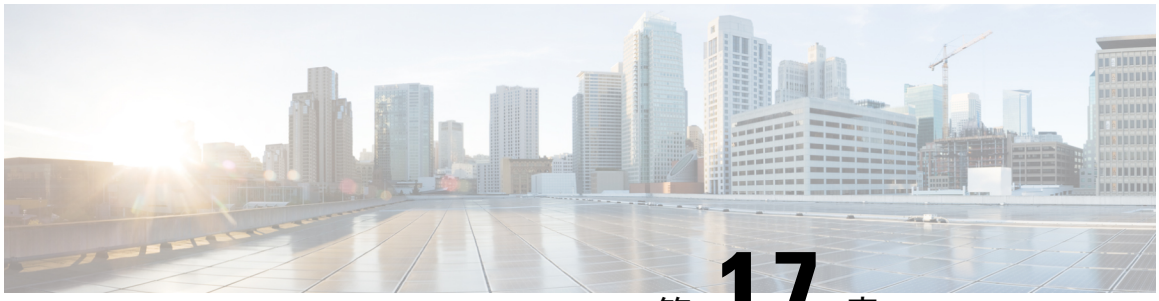
プラットフォーム ID の確認

標準の PEF 形式で SUDI 証明書を表示するには、show platform sudi certificate コマンドを使用します。コマンド出力から、プラットフォーム ID を簡単に確認できます。

コマンド出力にある最初の証明書は Cisco Root CA 2048 で、2 番目はシスコの下位 CA（ACT2 SUDI CA）です。3 番目は SUDI 証明書です。

```
router#show platform sudi certificate sign nonce 123
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmaHBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUl4F1pyXOWWqCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6keO1aO6g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
```

```
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBVrBW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA0m5l3THIxA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYVt/zEbslZq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPclM4iYKHumMQMqmgmg+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXlXtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIhvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcCl0lJu0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdIlplR1nH7KNDl5618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
 MIIDhzCCAm+gAwIBAgIEAJT3DDANBgkqhkiG9w0BAQsFADAnMQ4wDAYDVQQKEwVD
aXNjbzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMB4XDTE1MTExNDA5MzMzN1oXDTI1
MTExNDA5MzMzN1owczEsMCoGA1UEBRMjUElEOldTLUMzNjUwLTEyWDQ4VVEgU046
RkRPMTk0NkJHMDUxDjAMBgNVBAoTBUNpc2NvMRgwFgYDVQQLEw9BQ1QtMiBMaXRl
IFNVREkxGTAXBgNVBAMTEFdTLUMzNjUwLTEyWDQ4VVEwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC6SARWyImWrRV/x7XQogAE+02WmzKki+4arMVBvl9o
GgvJfkoJDdaHOROSUkEE3qXtd8N3lfKy3TZ+jtHD85m2aGz6+IRx/e/lLsQzi6dl
WIB+N94pgecFBONPR9wJriox1IGD3B43b0hMLkmro4R5Zrs8XFkDo9k1tBU7F2O7
GEzb/WkO5NLexznef2Niglx9fCDL0HC27BbsR5+03p8jhG0+mvrp8M9du1HKiGin
ZIV4XgTMp1/k/TVaIepEGZuWM3hxdUZjkNGG1c1m+oB8vLX3UlSL76sDBBoiaprD
rjXBgBIozyFW8tTjh50jMDG84hKD5s31ifOe4KpqEcnVAgMBAAGjbzBtMA4GA1Ud
DwEB/wQEAwIF4DAMBgNVHRMBAf8EAjAAME0GA1UdEQRGMESgQgYJKwYBBAEJFQID
oDUTM0NoaXBJRD1VWUpOTlZJMENBUkhVM1Z1SUVSbFl5QXlPQ0F4TXpvek5Ub3lN
U0EwS0NnPTANBgkqhkiG9w0BAQsFAAOCAQEADjtM8vdlf+p1WKSKX1C1qQ4aEnD5
p8T5e4iTer7Y1fbCrHIEEm3mnip+568j299z0H8V7PDp1ljuLHyMFTC+945F9RfA
eAuVWVb5A9dnGL8MssBJe2lVSnZwrWkT1EIdxLYrTiPAQHtll6CN77S4u/f71oYE
tzPE5AGfyGw7ro1MEPVGffaQmYUDAwKFNBH1uI7c2S1qlwk4WWZ6xxci+lhaQnIG
pWzapaiAYL1XrcBz4KwFc1ZZpQT6hHw24jzYaYimvCo+/kSKuA9xNdtSu18ycox0
zKnXQ17s6aChMMt7Y8Nh4iz9BDejoOF6/b3sM0wRi+2/4j+6/GhcMRs0Og==
-----END CERTIFICTAE
Signature version: 1
Signature:
405C70D802B73947EDBF8D0D2C8180F10D4B3EF9694514219C579D2ED52F7D583E0F40813FC4E9F549B2EB1C21725F7C
B1C79F98271E47E780E703E67472380FB52D4963E1D1FB9787B38E28B8E696570A180B7A2F131B1F174EA79F5DB4765DF67386126D8
9E07EDF6C26E0A81272EA1437D03F2692937082756AE1F1BFAFBFACD6BE9CF9C84C961FACE9FA0FE64D85AE4FA086969D0702C536ABD
B8FBFDC47C14C17D02FEBF4F7F5B24D2932FA876F56B4C07816270A0B4195C53D975C85AEAE3A74F2DBF293F52423ECB7B853967080A
9C57DA3E4B08B2B2CA623B2CBAF7080A0AEB09B2E5B756970A3A27E0F1D17C8A243
```



第 17 章

Call Home の設定

Call Home 機能は、クリティカルなシステム イベントを E メールおよび Web 上で通知します。ポケットベル サービス、通常の電子メール、または XML ベースの自動解析アプリケーションとの適切な互換性のために、さまざまなメッセージの形式が使用できます。この機能の一般的な使用方法としては、ネットワーク サポート技術者の直接ページング、ネットワーク オペレーション センターへの E メール通知、サポート Web サイトへの XML 送信、シスコのテクニカル サポート（TAC）で事例を直接生成するための Cisco Smart Call Home サービスの使用などがあります。

この章の内容は、次のとおりです。

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。

プラットフォームのサポート、および Cisco IOS、Catalyst OS ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするために、シスコのアカウントは必要ありません。

Call Home の前提条件

Call Home を設定するための前提条件を次に示します。

- 受信者が受け取ったメッセージの送信元を判別できるように、連絡先の電子メールアドレス（Smart Call Home のフル登録では必須、Call Mode が匿名モードでイネーブルになっている場合は任意）、電話番号（任意）、住所情報（任意）を設定する必要があります。
- 少なくとも 1 つの宛先プロファイル（定義済みまたはユーザ定義）を設定する必要があります。使用する宛先プロファイルは、受信エンティティがポケットベル、電子メールアドレス、または Cisco Smart Call Home などの自動サービスのいずれであるかによって異なります。

  宛先プロファイルが E メール メッセージ送信を使用している場合、シンプル メール転送プロトコル（SMTP）サーバを指定する必要があります。
- ルータは E メール サーバまたは宛先 HTTP サーバに IP 接続されている必要があります。
- Cisco Smart Call Home を使用する場合は、完全な Cisco Smart Call Home サービスを提供するために、デバイスを対象とした有効なサービス契約が必要です。

Call Home の概要

Call Home 機能を使用すると、設定、環境条件、インベントリ、syslog、スナップショット、およびクラッシュ イベントについての情報を含むアラート メッセージを送信できます。これらのアラート メッセージは、電子メール ベースまたは Web ベースのメッセージとして提供されます。複数のメッセージ フォーマットから選択できるので、ポケットベル サービス、標準的な電子メール、または XML ベースの自動解析アプリケーションとの互換性が得られます。この機能では、複数の受信者（Call Home 宛先プロファイルという）にアラートを送信できます。宛先プロファイルごとに、メッセージ形式とコンテンツのカテゴリを設定できます。Cisco TAC（callhome@cisco.com）にアラートを送信するための事前定義された宛先プロファイルが用意されています。また、独自の宛先プロファイルを定義することもできます。

柔軟なメッセージの配信オプションとフォーマット オプションにより、個別のサポート要件を簡単に統合できます。

ここでは、次の内容について説明します。

- Call Home を使用するメリット
- Smart Call Home サービスの取得

Call Home のメリット

Call Home 機能には次のようなメリットがあります。

- 次のような複数のメッセージ形式オプション：

  ショート テキスト：ポケットベルまたは印刷形式のレポートに最適。

  プレーン テキスト：人間が読むのに適した形式に完全整形されたメッセージ情報。

  XML：XML および Adaptive Markup Language（AML）Document Type Definitions（DTD）を使用するマシンが判読可能な形式です。XML 形式では、シスコ TAC と通信できます。

- 複数のメッセージ宛先への同時配信が可能。
- 複数のメッセージ カテゴリ（設定、環境条件、インベントリ、syslog、スナップショット、クラッシュ イベントなど）。
- シビラティ（重大度）とパターンマッチによるメッセージのフィルタリング
- 定期的なメッセージ送信のスケジューリング

Smart Call Home サービスの取得

シスコと直接サービス契約を結んでいる場合は、Smart Call Home サービスに登録できます。Smart Call Home は、Smart Call Home メッセージを分析し、背景説明と推奨措置を提供します。既知の問題、特にオンライン診断障害については、TAC に Automatic Service Request が作成されます。

Smart Call Home には、次の機能があります。

- 継続的なデバイス ヘルス モニタリングとリアルタイムの診断アラート。
- Smart Call Home メッセージの分析。必要に応じて、自動サービス要求（詳細な診断情報が含まれる）が作成され、該当する TAC チームにルーティングされるため、問題解決を高速化できます。
- セキュアなメッセージ転送が、ご使用のデバイスから直接、または HTTP プロキシ サーバやダウンロード可能な転送ゲートウェイ（TG）を経由して行われます。TG 集約ポイントは、複数のデバイスをサポートする場合またはセキュリティ要件によって、デバイスをインターネットに直接接続できない場合に使用できます。
- すべての Smart Call Home デバイスの Smart Call Home メッセージと推奨事項、インベントリ情報、および設定情報に Web アクセスすることにより、関連するフィールド通知、セキュリティ勧告、およびサポート終了日情報にアクセスできます。

Smart Call Home で次の項目を登録する必要があります。

- ルータの SMARTnet 契約番号
- 電子メール アドレス
- Cisco.com のユーザ名

Smart Call Home の詳細については、https://supportforums.cisco.com/community/4816/smart-call-home を参照してください。

Anonymous Reporting

Smart Call Home は、多くのシスコ サービス契約に含まれるサービス機能で、顧客が問題をより迅速に解決できるように支援することを目的としています。また、クラッシュ メッセージから取得した情報は、シスコが現場の機器や発生している問題を理解しやすくします。Smart Call Home を使用しない場合でも、Anonymous Reporting をイネーブルにすると、シスコはデバイスから最小限のエラーおよびヘルス情報をセキュアに受信できます。Anonymous Reporting をイネーブルにした場合、顧客が誰であるかは匿名のままで、識別情報は送信されません。

（注） Anonymous Reporting をイネーブルにすると、シスコまたはシスコに代わって業務を行うベンダーに指定データを転送することに同意することになります（米国以外の国を含む）。シスコでは、すべてのお客様のプライバシーを保護しています。シスコでの個人情報の取り扱いについては、シスコのプライバシー ステートメント（http://www.cisco.com/web/siteassets/legal/privacy.html）参照してください。

Call Home が匿名で設定されていると、クラッシュ、インベントリ、およびテスト メッセージだけがシスコに送信されます。顧客の識別情報は送信されません。

これらのメッセージの送信内容の詳細については、アラートグループの起動イベントとコマンド （290 ページ）を参照してください。

Call Home の設定方法

以下の項では、1 つのコマンドを使用して Call Home を設定する方法について説明します。

- Smart Call Home の設定（単一コマンド） （251 ページ）
- Smart Call Home の設定と有効化 （252 ページ）

以下の項では、詳細な設定およびオプションの設定について説明します。

- Call Home のイネーブル化とディセーブル化 （252 ページ）
- 連絡先情報の設定 （253 ページ）
- 宛先プロファイルの設定 （254 ページ）
- アラートグループへの登録 （259 ページ）
- 一般的な電子メールオプションの設定 （264 ページ）
- Call Home メッセージ送信のレート制限の指定 （266 ページ）
- HTTP プロキシサーバーの指定 （267 ページ）
- Call Home メッセージの IOS コマンドを実行するための AAA 認証の有効化 （267 ページ）
- syslog スロットリングの設定 （268 ページ）

• Call Home データプライバシーの設定 （269 ページ）
• Call Home 通信の手動送信 （270 ページ）

Smart Call Home の設定（単一コマンド）

1 つのコマンドですべての Call Home の基本設定をイネーブルにするには、次の手順を実行します。

手順

ステップ 1 **configure terminal**

例：

```
Router# configure terminal
```

コンフィギュレーション モードに入ります。

ステップ 2 **call-home reporting** {**anonymous** | **contact-email-addr** *email-address*} [**http-proxy** {*ipv4-address* | *ipv6-address* | *name*} **port** *port-number*]

例：

```
Router(config)# call-home reporting contact-email-addr email@company.com
```

1 つのコマンドを使用して Call Home の基本設定をイネーブルにします。

- **anonymous**：Call-Home TAC プロファイルがクラッシュメッセージ、インベントリメッセージ、およびテストメッセージのみを送信し、これらのメッセージを匿名で送信するようにします。
- **contact-email-addr**：Smart Call Home サービスのフル レポート機能をイネーブルにし、フル インベントリ メッセージを Call Home TAC プロファイルから Smart Call Home サーバに送信してフル登録プロセスを開始します。
- **http-proxy** {*ipv4-address* | *ipv6-address* | *name*}：IPv4 または IPv6 アドレス、あるいはサーバー名を設定します。最大長は 64 文字です。
- **port** *port-number*：ポート番号。

  有効値の範囲は 1 ～ 65535 です。

（注）
HTTP プロキシ オプションでは、バッファリングするための独自のプロキシ サーバおよびデバイスからのセキュア接続を利用できます。

（注）
call-home reporting コマンドを使用して匿名またはフル登録モードで Call Home を正常にイネーブルにした後、インベントリ メッセージが送信されます。Call Home がフル登録モードでイネーブルになっている場合、フル登録モードのフル インベントリ メッセージが送信されます。Call Home が匿名モードでイネーブ

ルになっている場合、匿名のインベントリ メッセージが送信されます。これらのメッセージの送信内容の詳細については、アラートグループの起動イベントとコマンド （290 ページ）を参照してください。

Smart Call Home の設定と有効化

Cisco Smart Call Home サービスのアプリケーションおよび設定に関する情報については、https://supportforums.cisco.com/community/4816/smart-call-home にある『Smart Call Home User Guide』の「Getting Started」の項を参照してください。このマニュアルには、デバイスから直接、または転送ゲートウェイ（TG）集約ポイントを介して Smart Call Home メッセージを送信するための設定例が含まれています。

（注） HTTPS には追加的なペイロード暗号化が含まれているため、セキュリティ上の理由から、HTTPS 転送オプションを使用することをお勧めします。インターネットへの接続に集約ポイントまたはプロキシが必要な場合は、Cisco.com からダウンロード可能な転送ゲートウェイ ソフトウェアを使用できます。

Call Home のイネーブル化とディセーブル化

Call Home 機能をイネーブルまたはディセーブルにするには、次の手順に従います。

手順

ステップ 1 **configure terminal**

例：

```
Router# configure terminal
```

コンフィギュレーション モードに入ります。

ステップ 2 **service call-home**

例：

```
Router(config)# service call-home
```

Call Home 機能をイネーブルにします。

ステップ 3 **no service call-home**

例：

```
Router(config)# no service call-home
```

Call Home 機能をディセーブルにします。

連絡先情報の設定

各ルータには、連絡先電子メール アドレスが含まれる必要があります（ただしCall Homeが匿名モードでイネーブルに設定されている場合を除く）。任意で、電話番号、住所、契約 ID、カスタマー ID、サイト ID を割り当てることができます。

連絡先情報を割り当てるには、次の手順を実行します。

手順

ステップ 1 **configure terminal**

例：

```
Router# configure terminal
```

コンフィギュレーション モードに入ります。

ステップ 2 **call-home**

例：

```
Router(config)# call-home
```

Call Home 設定サブモードに入ります。

ステップ 3 **contact-email-addr** *email-address*

例：

```
Router(cfg-call-home)# contact-email-addr username@example.com
```

自分の電子メール アドレスを指定します。E メール アドレス フォーマットにはスペースなしで最大 200 文字まで入力できます。

ステップ 4 **phone-number** *+phone-number*

例：

```
Router(cfg-call-home)# phone-number +1-800-555-4567
```

（任意）自分の電話番号を割り当てます。

（注）
番号は必ずプラス（+）記号で始まり、ダッシュ（-）と数字だけが含まれるようにしてください。17 文字まで入力できます。スペースを含める場合は、エントリを引用符（“”）で囲む必要があります。

ステップ 5 **street-address** *street-address*

例：

```
Router(cfg-call-home)# street-address “1234 Picaboo Street, Any city, Any state, 12345“
```

（任意）RMA機器の配送先である自分の住所を割り当てます。最大200文字まで入力できます。スペースを含める場合は、エントリを引用符（“”）で囲む必要があります。

ステップ 6 **customer-id** *text*

例：

```
Router(cfg-call-home)# customer-id Customer1234
```

（任意）カスタマー ID を指定します。最大 64 文字まで入力できます。スペースを含める場合は、エントリを引用符（“”）で囲む必要があります。

ステップ 7 **site-id** *text*

例：

```
Router(cfg-call-home)# site-id Site1ManhattanNY
```

（任意）カスタマーサイトIDを指定します。最大200文字まで入力できます。スペースを含める場合は、エントリを引用符（“”）で囲む必要があります。

ステップ 8 **contract-id** *text*

例：

```
Router(cfg-call-home)# contract-id Company1234
```

（任意）ルータの契約 ID を指定します。最大 64 文字まで入力できます。スペースを含める場合は、エントリを引用符（“”）で囲む必要があります。

例

次に、連絡先情報を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# call-home
Router(cfg-call-home)# contact-email-addr username@example.com
Router(cfg-call-home)# phone-number +1-800-555-4567
Router(cfg-call-home)# street-address “1234 Picaboo Street, Any city, Any state, 12345”
Router(cfg-call-home)# customer-id Customer1234
Router(cfg-call-home)# site-id Site1ManhattanNY
Router(cfg-call-home)# contract-id Company1234
Router(cfg-call-home)# exit
```

宛先プロファイルの設定

宛先プロファイルには、アラート通知に必要な配信情報が入っています。少なくとも1つの宛先プロファイルが必要です。1 つまたは複数のタイプの複数の宛先プロファイルを設定できます。

新しい宛先プロファイルを作成して定義することも、定義済みの宛先プロファイルをコピーして使用することもできます。新しい宛先プロファイルを定義する場合は、プロファイル名を割り当てる必要があります。

（注） Cisco Smart Call Home サービスを使用する場合、宛先プロファイルは XML メッセージ フォーマットでなければなりません。

次の属性を宛先プロファイルに設定できます。

- プロファイル名：ユーザ定義の宛先プロファイルを一意に識別する文字列。プロファイル名は 31 文字までで大文字と小文字は区別されません。

（注） プロファイル名として **all** は使用できません。

- 転送方法：アラートを送信するための転送メカニズム（電子メールまたは HTTP（HTTPS を含む））。
  - ユーザ定義の宛先プロファイルの場合、E メールがデフォルトで、どちらかまたは両方の転送メカニズムをイネーブルにできます。両方の方法をディセーブルにすると、E メールがイネーブルになります。
  - あらかじめ定義された Cisco TAC プロファイルの場合、いずれかの転送メカニズムをイネーブルにできますが、同時にはイネーブルにできません。
- 宛先アドレス：アラートを送信する転送方法に関連した実際のアドレス。
- メッセージ形式：アラートの送信に使用するメッセージ形式。ユーザ定義宛先プロファイルの形式オプションは、ロング テキスト、ショート テキスト、または XML です。デフォルトは XML です。定義済みのシスコ TAC プロファイルの場合、XML しか使用できません。
- メッセージ サイズ：宛先メッセージの最大サイズ。有効範囲は 50 ～ 3,145,728 バイトです。デフォルト値は 3,145,728 バイトです。

  Anonymous Reporting：顧客 ID を匿名のままにするよう選択できます。これにより、識別情報が送信されません。
- 関心のあるアラート グループへの登録：各自の関心事項を示すアラート グループに登録することができます。

ここでは、次の内容について説明します。

- 新しい宛先プロファイルの作成 （255 ページ）
- 宛先プロファイルのコピー （257 ページ）
- プロファイルの匿名モードの設定 （258 ページ）

新しい宛先プロファイルの作成

新しい宛先プロファイルを作成し、設定するには、次の手順に従います。

手順

ステップ 1 **configure terminal**

例：

```
Router# configure terminal
```

コンフィギュレーション モードに入ります。

ステップ 2 **call-home**

例：

```
Router(config)# call-home
```

Call Home 設定サブモードに入ります。

ステップ 3 **profile** *name*

例：

```
Router(config-call-home)# profile profile1
```

指定された宛先プロファイルに対する Call Home 宛先プロファイル設定サブモードに入ります。指定された宛先プロファイルが存在しない場合、作成されます。

ステップ 4 [**no**] **destination transport-method** {**email** | **http**}

例：

```
Router(cfg-call-home-profile)# destination transport-method email
```

（任意）メッセージ転送方法をイネーブルにします。**no** オプションを選択すると、方法がディセーブルになります。

ステップ 5 **destination address** {**email** *email-address* | **http** *url*}

例：

```
Router(cfg-call-home-profile)# destination address email myaddress@example.com
```

Call Home メッセージを送信する宛先 E メール アドレスまたは URL を設定します。

（注）
宛先 URL を入力する場合は、サーバがセキュア サーバであるかどうかに応じて **http://** または **https://** を指定します。

ステップ 6 **destination preferred-msg-format** {**long-text** | **short-text** | **xml**}

例：

```
Router(cfg-call-home-profile)# destination preferred-msg-format xml
```

（任意）使用するメッセージ形式を設定します。デフォルトは XML です。

ステップ 7 **destination message-size-limit** *bytes*

例：

```
Router(cfg-call-home-profile)# destination message-size-limit 3145728
```

（任意）宛先プロファイルの宛先メッセージの最大サイズを設定します。

ステップ 8 **active**

例：

```
Router(cfg-call-home-profile)# active
```

宛先プロファイルをイネーブルにします。デフォルトでは、プロファイルは作成時にイネーブルになります。

ステップ 9 **end**

例：

```
Router(cfg-call-home-profile)# end
```

特権 EXEC モードに戻ります。

ステップ 10 **show call-home profile** {*name* | **all**}

例：

```
Router# show call-home profile profile1
```

指定されたプロファイル、または設定済みのすべてのプロファイルに関する宛先プロファイル設定を表示します。

宛先プロファイルのコピー

既存のプロファイルをコピーして新しい宛先プロファイルを作成するには、次の手順に従います。

手順

ステップ 1 **configure terminal**

例：

```
Router# configure terminal
```

コンフィギュレーション モードに入ります。

ステップ 2 **call-home**

例：

```
Router(config)# call-home
```

Call Home 設定サブモードに入ります。

ステップ 3 **copy profile** *source-profile target-profile*

例：

```
Router(cfg-call-home)# copy profile profile1 profile2
```

既存の宛先プロファイルと同じ設定で新しい宛先プロファイルを作成します。

プロファイルの匿名モードの設定

匿名プロファイルを設定するには、次の手順に従います。

手順

ステップ 1 **configure terminal**

例：

```
Router# configure terminal
```

コンフィギュレーション モードに入ります。

ステップ 2 **call-home**

例：

```
Router(config)# call-home
```

Call Home 設定サブモードに入ります。

ステップ 3 **profile** *name*

例：

```
Router(cfg-call-home) profile Profile-1
```

プロファイル コンフィギュレーション モードをイネーブルにします。

ステップ 4 **anonymous-reporting-only**

例：

```
Router(cfg-call-home-profile)# anonymous-reporting-only
```

プロファイルを匿名モードに設定します。

（注）
デフォルトで、Call Home は、プロファイルに登録されているすべてのイベント タイプに関する完全なレポートを送信します。**anonymous-reporting-only** が設定されている場合は、クラッシュ、インベントリ、およびテストメッセージだけが送信されます。

アラートグループへの登録

アラート グループは、すべてのルータでサポートされている Call Home アラートをあらかじめ定義したサブセットです。Call Home アラートはタイプごとに別のアラート グループにグループ化されます。次のアラートグループが使用可能です。

- Crash
- 設定
- Environment
- Inventory
- Snapshot
- Syslog

ここでは、次の内容について説明します。

- 定期通知 （262 ページ）
- メッセージシビラティ（重大度）しきい値 （262 ページ）
- スナップショット コマンド リストの設定 （263 ページ）

各アラート グループの起動イベントをアラートグループの起動イベントとコマンド（290 ページ）に示します。アラート グループ メッセージの内容をメッセージの内容 （297 ページ）に示します。

宛先プロファイルごとに受信するアラート グループを 1 つまたは複数選択できます。

（注） Call Home アラートは、その Call Home アラートが含まれているアラート グループに登録されている宛先プロファイルにしか送信されません。さらに、アラート グループをイネーブルにする必要があります。

宛先プロファイルを 1 つまたは複数のアラートグループに登録する場合、次の手順に従います。

手順

ステップ 1 **configure terminal**

例：

```
Router# configure terminal
```

コンフィギュレーション モードに入ります。

ステップ 2 **call-home**

例：

```
Router(config)# call-home
```

Call Home 設定サブモードに入ります。

ステップ 3 **alert-group** {**all** | **configuration** | **environment** | **inventory** | **syslog** | **crash** | **snapshot**}

例：

```
Router(cfg-call-home)# alert-group all
```

指定されたアラート グループをイネーブルにします。すべてのアラート グループをイネーブル（有効）にするには、**all** キーワードを使用します。デフォルトでは、すべてのアラート グループがイネーブルになります。

ステップ 4 **profile** *name*

例：

```
Router(cfg-call-home)# profile profile1
```

指定された宛先プロファイルに対する Call Home 宛先プロファイル設定サブモードに入ります。

ステップ 5 **subscribe-to-alert-group all**

例：

```
Router(cfg-call-home-profile)# subscribe-to-alert-group all
```

最も低いシビラティ（重大度）を使用しているすべての使用可能なアラート グループに登録します。

ステップ 6 からステップ 11 で説明しているように、特定のタイプごとに個別にアラート グループに登録することもできます。

（注）
このコマンドは、syslog のデバッグのデフォルトのシビラティ（重大度）に登録されます。これにより、大量の syslog メッセージが生成されます。可能な場合は、適切なシビラティ（重大度）およびパターンを使用してアラート グループに個別に登録してください。

ステップ 6 **subscribe-to-alert-group configuration** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}]

例：

```
Router(cfg-call-home-profile)# subscribe-to-alert-group configuration
periodic daily 12:00
```

この宛先プロファイルを Configuration アラート グループに登録します。定期通知 （262 ページ）で説明しているように、定期的な通知用に Configuration アラート グループを設定できます。

ステップ 7 **subscribe-to-alert-group environment** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}]

例：

```
Router(cfg-call-home-profile)# subscribe-to-alert-group environment severity major
```

この宛先プロファイルをEnvironmentアラートグループに登録します。メッセージシビラティ（重大度）しきい値（262ページ）で説明しているように、シビラティ（重大度）に応じてメッセージをフィルタリングするためにEnvironmentアラートグループを設定できます。

ステップ8 **subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}]

例：

```
Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic monthly 1 12:00
```

この宛先プロファイルをInventoryアラートグループに登録します。定期通知（262ページ）で説明しているように、定期的な通知用にInventoryアラートグループを設定できます。

ステップ9 **subscribe-to-alert-group syslog** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}]

例：

```
Router(cfg-call-home-profile)# subscribe-to-alert-group environment severity major
```

この宛先プロファイルをSyslogアラートグループに登録します。メッセージシビラティ（重大度）しきい値（262ページ）で説明しているように、シビラティ（重大度）に応じてメッセージをフィルタリングするようSyslogアラートグループを設定できます。

各syslogメッセージ内で照合するテキストパターンを指定できます。パターンを設定すると、指定されたパターンが含まれ、シビラティ（重大度）しきい値に一致する場合にだけSyslogアラートグループメッセージが送信されます。パターンにスペースが含まれる場合は、引用符（“”）でスペースを囲む必要があります。宛先プロファイルごとにパターンを5つまで指定できます。

ステップ10 **subscribe-to-alert-group crash**

例：

```
Router(cfg-call-home-profile)# [no | default]
subscribe-to-alert-group crash
```

ユーザプロファイルのCrashアラートグループに登録します。デフォルトでTACプロファイルはCrashアラートグループに登録され、登録を解除できません。

ステップ11 **subscribe-to-alert-group snapshot periodic** {**daily** *hh:mm* | **hourly** *mm* | **interval** *mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}

例：

```
Router(cfg-call-home-profile)# subscribe-to-alert-group snapshot periodic daily 12:00
```

この宛先プロファイルをSnapshotアラートグループに登録します。定期通知（262ページ）で説明しているように、定期的な通知用にSnapshotアラートグループを設定できます。

デフォルトでは、Snapshotアラートグループに実行するコマンドはありません。コマンドをアラートグループの中に追加できます（スナップショットコマンドリストの設定（263ページ）を参照）。こうすることで、Snapshotアラートグループに追加されたコマンドの出力がスナップショットメッセージに組み込まれます。

ステップ12 **exit**

例：

```
Router(cfg-call-home-profile)# exit
```

Call Home 宛先プロファイル設定サブモードを終了します。

定期通知

Configuration、Inventory、または Snapshot アラート グループに宛先プロファイルを登録するとき、アラート グループ メッセージを非同期的に受信するか、または指定の時間に定期的に受信するかを選択できます。送信期間は、次のいずれかのオプションに設定できます。

- 日次：24 時間表記の時間:分形式（*hh:mm*）で送信する時刻を指定します（例：14:30）。
- 週次：*day hh:mm* の形式で曜日と時刻を指定します。day は曜日を省略せずスペルアウトします（例：Monday）。
- 月次：*date hh:mm* の形式で 1 ～ 31 の日と時刻を指定します。
- 間隔：定期的なメッセージが送信される間隔を 1 ～ 60 分で指定します。
- 毎時：定期的なメッセージが送信される時刻（分）を 0 ～ 59 分で指定します。

（注） 毎時および間隔による定期通知は、Snapshot アラート グループでのみ使用可能です。

メッセージシビラティ（重大度）しきい値

宛先プロファイルを Environment、または Syslog アラート グループに登録するとき、メッセージシビラティ（重大度）に基づいてアラート グループ メッセージを送信するためのしきい値を設定できます。宛先プロファイルに指定したしきい値より低い値のメッセージは、宛先に送信されません。

シビラティ（重大度）しきい値の設定に使用されるキーワードを、次の表に示します。シビラティ（重大度）しきい値の範囲は、catastrophic（レベル 9、最高緊急度）から debugging（レベル 0、最低緊急度）です。Syslog または Environment アラート グループのシビラティ（重大度）しきい値が設定されていない場合、デフォルトは debugging （レベル 0）です。Configuration アラート グループおよび Inventory アラート グループではシビラティ（重大度）は設定できません。シビラティ（重大度）は常に normal に固定されます。

（注） Call Home のシビラティ（重大度）は、システム メッセージ ロギングのシビラティ（重大度）とは異なります。

表 *20 :* シビラティ（重大度）と *syslog* レベルのマッピング

レベル	キーワード	Syslog レベル	説明
9	catastrophic	—	ネットワーク全体に壊滅的な障害が発生しています。

レベル	キーワード	Syslog レベル	説明
8	disaster	—	ネットワークに重大な影響が及びます。
7	fatal	緊急（0）	システムが使用不可能な状態。
6	critical	アラート（1）	クリティカルな状態、ただちに注意が必要。
5	major	重要（2）	重大な状態。
4	minor	エラー（3）	軽微な状態。
3	warning	警告（4）	警告状態。
2	notification	通知（5）	基本的な通知および情報メッセージです。他と関係しない、重要性の低い障害です。
1	normal	情報（6）	標準状態に戻ることを示す標準イベントです。
0	debugging	デバッグ（7）	デバッグ メッセージ。

スナップショット コマンド リストの設定

スナップショット コマンド リストを設定するには、次の手順を実行します。

手順

ステップ 1 **configure terminal**

例：

```
Router# configure terminal
```

コンフィギュレーション モードに入ります。

ステップ 2 **call-home**

例：

```
Router(config)# call-home
```

Call Home 設定サブモードに入ります。

ステップ 3 [**no** | **default**] **alert-group-config snapshot**

例：

```
Router(cfg-call-home)# alert-group-config snapshot
```

スナップショット コンフィギュレーション モードを開始します。

no または **default** コマンドは、すべてのスナップショット コマンドを削除します。

ステップ 4 [**no** | **default**] **add-command** *command string*

例：

```
Router(cfg-call-home-snapshot)# add-command "show version"
```

Snapshot アラート グループにコマンドを追加します。**no** または **default** コマンドは、対応するコマンドを削除します。

- *command string*：IOS コマンド。最大長は 128 文字です。

ステップ 5 **exit**

例：

```
Router(cfg-call-home-snapshot)# exit
```

終了し、設定を保存します。

一般的な電子メールオプションの設定

E メール メッセージ転送を使用するには、少なくとも 1 つの Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）E メール サーバ アドレスを設定する必要があります。発信元と返信先 E メール アドレスを設定し、バックアップ E メール サーバを 4 つまで指定できます。

一般的な電子メールオプションの設定時には、次の点に注意してください。

- バックアップ E メール サーバは、異なるプライオリティ番号を使用して、**mail-server** コマンドを繰り返すと定義できます。
- **mail-server priority** number パラメータは 1 ～ 100 に設定可能です。プライオリティが最も高い（プライオリティ番号が最も低い）サーバを最初に試します。

一般的な電子メールオプションを設定するには、次の手順に従います。

手順

ステップ 1 **configure terminal**

例：

```
Router# configure terminal
```

コンフィギュレーション モードに入ります。

ステップ 2 **call-home**

例：

```
Router(config)# call-home
```

Call Home 設定サブモードに入ります。

ステップ 3 **mail-server** [{*ipv4-address* | *ipv6-address*} | *name*] **priority** *number*

例：

```
Router(cfg-call-home)# mail-server stmp.example.com priority 1
```

E メール サーバ アドレスを割り当て、設定済みの E メール サーバ内の相対的なプライオリティを割り当てます。

次のいずれかの方法で指定します。

- 電子メール サーバの IP アドレス
- 電子メール サーバの完全修飾ドメイン名（FQDN）（64 文字まで）。

1（最高のプライオリティ）から 100（最低のプライオリティ）のプライオリティ番号を割り当てます。

ステップ 4 **sender from** *email-address*

例：

```
Router(cfg-call-home)# sender from username@example.com
```

（任意）Call Home 電子メール メッセージの [from] フィールドに表示される電子メール アドレスを割り当てます。アドレスが指定されていない場合は、連絡用の E メール アドレスが使用されます。

ステップ 5 **sender reply-to** *email-address*

例：

```
Router(cfg-call-home)# sender reply-to username@example.com
```

（任意）Call Home 電子メール メッセージの [reply-to] フィールドに表示される電子メール アドレスを割り当てます。

ステップ 6 **source-interface** *interface-name*

例：

```
Router(cfg-call-home)# source-interface loopback1
```

Call-Home メッセージを送信するための発信元インターフェイス名を割り当てます。

- *interface-name*：発信元インターフェイス名。最大長は 64 文字です。

（注）
HTTP メッセージの場合、発信元インターフェイス名を設定するには、グローバル コンフィギュレーション モードで **ip http client source-interface** *interface-name* コマンドを使用します。これにより、デバイスのすべての HTTP クライアントが同じ発信元インターフェイスを使用できるようになります。

ステップ 7 **vrf** *vrf-name*

例：

```
Router(cfg-call-home)# vrf vpn1
```

（任意）Call-Home 電子メール メッセージを送信するため VRF インスタンスを指定します。VRF を指定しないと、グローバル ルーティング テーブルが使用されます。

（注）

HTTP メッセージでは、発信元インターフェイスが VRF に関連付けられている場合、グローバル コンフィギュレーション モードで **ip http client source-interface** *interface-name* コマンドを使用して、デバイスのすべての HTTP クライアントで使われる VRF インスタンスを指定します。

例

次に、プライマリ電子メールサーバーおよびセカンダリ電子メールサーバーなど、一般的な電子メールパラメータの設定例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# call-home
Router(cfg-call-home)# mail-server smtp.example.com priority 1
Router(cfg-call-home)# mail-server 192.0.2.1 priority 2
Router(cfg-call-home)# sender from username@example.com
Router(cfg-call-home)# sender reply-to username@example.com
Router(cfg-call-home)# source-interface loopback1
Router(cfg-call-home)# vrf vpn1
Router(cfg-call-home)# exit
Router(config)#
```

Call Home メッセージ送信のレート制限の指定

Call Home メッセージ送信のレート制限を指定するには、次の手順を実行します。

手順

ステップ 1 **configure terminal**

例：

```
Router# configure terminal
```

コンフィギュレーション モードに入ります。

ステップ 2 **call-home**

例：

```
Router(config)# call-home
```

Call Home 設定サブモードに入ります。

ステップ 3 **rate-limit** *number*

例：

```
Router(cfg-call-home)# rate-limit 40
```

1 分間に送信するメッセージ数の制限を指定します。

• *number*：範囲は 1 ～ 60 です。デフォルトは 20 です。

HTTP プロキシサーバーの指定

宛先に Call Home HTTP（S）メッセージを送信するために HTTP プロキシサーバーを指定するには、次の手順を実行します。

手順

ステップ 1 **configure terminal**

例：

```
Router# configure terminal
```

コンフィギュレーション モードに入ります。

ステップ 2 **call-home**

例：

```
Router(config)# call-home
```

Call Home 設定サブモードに入ります。

ステップ 3 **http-proxy** {*ipv4-address* | *ipv6-address* | *name*} **port** *port-number*

例：

```
Router(cfg-call-home)# http-proxy 192.0.2.1 port 1
```

HTTP 要求のプロキシ サーバを指定します。

Call Home メッセージの IOS コマンドを実行するための AAA 認証の有効化

宛先に Call Home HTTP（S）メッセージを送信するために HTTP プロキシサーバーを指定するには、次の手順を実行します。

手順

ステップ 1 **configure terminal**

例：

```
Router# configure terminal
```

コンフィギュレーション モードに入ります。

ステップ 2 call-home

例：

```
Router(config)# call-home
```

Call Home 設定サブモードに入ります。

ステップ 3 aaa-authorization

例：

```
Router(cfg-call-home)# aaa-authorization
```

AAA 認証をイネーブルにします。

（注）
デフォルトでは、AAA 認証は Call Home でディセーブルです。

ステップ 4 aaa-authorization [**username** *username*]

例：

```
Router(cfg-call-home)# aaa-authorization username user
```

許可のためのユーザ名を指定します。

- **username** ユーザー名：デフォルトのユーザー名は callhome です。最大長は 64 文字です。

syslog スロットリングの設定

宛先に Call Home HTTP（S）メッセージを送信するために HTTP プロキシサーバーを指定するには、次の手順を実行します。

手順

ステップ 1 configure terminal

例：

```
Router# configure terminal
```

コンフィギュレーション モードに入ります。

ステップ 2 call-home

例：

```
Router(config)# call-home
```

Call Home 設定サブモードに入ります。

ステップ 3 [**no**] **syslog-throttling**

例：

```
Router(cfg-call-home)# syslog-throttling
```

Call Home syslog メッセージのスロットリングをイネーブルまたはディセーブルにし、Call Home syslog メッセージが繰り返し送信されないようにします。

（注）
デフォルトでは、syslog メッセージ スロットリングはイネーブルです。

Call Home データ プライバシーの設定

data-privacy コマンドは、顧客のプライバシーを保護するために、IP アドレスなどのデータのスクラビング処理を行います。data-privacy コマンドをイネーブルにすると、大量のデータのスクラビング処理を行ったときに CPU 使用率に影響を及ぼすことがあります。現在、**show running-config all** および **show startup-config data** コマンド出力の中の設定メッセージを除いて、**show** コマンドの出力はスクラビング処理されません。

手順

ステップ 1 **configure terminal**

例：

```
Router# configure terminal
```

コンフィギュレーション モードに入ります。

ステップ 2 **call-home**

例：

```
Router(config)# call-home
```

Call Home 設定サブモードに入ります。

ステップ 3 **data-privacy** {**level** {**normal** | **high**} | **hostname**}

例：

```
Router(cfg-call-home)# data-privacy level high
```

ユーザのプライバシーを保護するために、実行コンフィギュレーション ファイルのデータをスクラビング処理します。デフォルトの data-privacy レベルは normal です。

（注）
data-privacy コマンドをイネーブルにすると、大量のデータのスクラビング処理を行ったときに CPU 使用率に影響を及ぼすことがあります。

- **normal**：すべての標準レベル コマンドをスクラビング処理します。

- **high**：標準レベル コマンドに加えて、IP ドメイン名と IP アドレスのコマンドのスクラビング処理を行います。
- **hostname**：高レベル コマンドに加えて hostname コマンドのスクラビング処理を行います。

（注）
一部のプラットフォームでは、設定メッセージのホスト名をスクラビング処理すると、Smart Call Home 処理が失敗することがあります。

Call Home 通信の手動送信

数種類の Call Home 通信を手動で送信できます。Call Home 通信を送信するには、この項の作業を実行します。ここでは、次の内容について説明します。

Call Home テストメッセージの手動送信

call-home test コマンドを使用して、ユーザー定義の Call Home テストメッセージを送信できます。

Call Home テストメッセージを手動で送信するには、次の手順に従います。

手順

call-home test [*“test-message”*] **profile** *name*

例：

```
Router# call-home test profile profile1
```

指定された宛先プロファイルにテストメッセージを送信します。ユーザ定義のテストメッセージのテキストは任意指定ですが、スペースが含まれる場合には、引用符（“”）で囲む必要があります。ユーザ定義のメッセージが設定されていない場合、デフォルト メッセージが送信されます。

Call Home アラートグループメッセージの手動送信

call-home send コマンドを使用して、特定のアラートグループメッセージを手動で送信できます。

Call Home アラートグループメッセージを手動で送信する場合は、次の注意事項に従ってください。

- 手動で送信できるのは、Crash、Snapshot、Configuration、および Inventory アラート グループだけです。
- Crash、Snapshot、Configuration、または Inventory アラート グループ メッセージを手動でトリガーする場合、宛先プロファイル名を指定すると、プロファイルのアクティブ ステータス、加入ステータス、またはシビラティ（重大度）設定に関係なく、宛先プロファイルにメッセージが送信されます。
- Crash、Snapshot、Configuration、または Inventory アラート グループ メッセージを手動でトリガーするとき、宛先プロファイル名を指定しないと、normal または指定されたアラート グループへの定期的な登録に指定されたアクティブなプロファイルすべてにメッセージが送信されます。

Call Home アラートグループメッセージを手動でトリガーするには、次の手順に従います。

手順

ステップ 1 **call-home send alert-group snapshot** [**profile** *name*]

例：

```
Router# call-home send alert-group snapshot profile profile1
```

1 つの宛先プロファイル（指定されている場合）または登録されているすべての宛先プロファイルに Snapshot アラート グループ メッセージを送信します。

ステップ 2 **call-home send alert-group crash** [**profile** *name*]

例：

```
Router# call-home send alert-group crash profile profile1
```

1 つの宛先プロファイル（指定されている場合）または登録されているすべての宛先プロファイルに Crash アラート グループ メッセージを送信します。

ステップ 3 **call-home send alert-group configuration** [**profile** *name*]

例：

```
Router# call-home send alert-group configuration profile profile1
```

宛先プロファイルの 1 つ（指定されている場合）または登録されているすべての宛先プロファイルに Configuration アラート グループ メッセージを送信します。

ステップ 4 **call-home send alert-group inventory** [**profile** *name*]

例：

```
Router# call-home send alert-group inventory profile profile1
```

宛先プロファイルの 1 つ（指定されている場合）または登録されているすべての宛先プロファイルに Inventory アラート グループ メッセージを送信します。

Call Home 分析およびレポート要求の送信

call-home request コマンドを使用すると、システムに関する情報を Cisco に送信して、システム固有の便利な分析/およびレポート情報を受け取ることができます。セキュリティの警告、既知のバグ、ベスト プラクティス、コマンド リファレンスなど、さまざまなレポートを要求できます。

Call Home 分析およびレポート要求を手動で送信する場合、次の注意事項に従ってください。

- **profile** *name* を指定すると、要求はプロファイルに送信されます。プロファイルが指定されていない場合、要求は Cisco TAC プロファイルに送信されます。Call Home 要求の受信者プロファイルをイネーブルにする必要はありません。要求メッセージを Cisco TAC に転送し、Smart Call Home サービスから返信を受信できるように、Transport Gateway が設定された電子メール アドレスをプロファイルに指定します。
- **ccoid** *user-id* は、Smart Call Home ユーザの登録済み ID です。*user-id* を指定すると、応答は登録ユーザの E メール アドレスに送信されます。*user-id* を指定しなければ、応答はデバイスの連絡先電子メール アドレスに送信されます。
- 要求するレポートのタイプを指定するキーワードに基づいて、次の情報が返されます。
  - **config-sanity**：現在の実行コンフィギュレーションに関連するベスト プラクティス情報。
  - **bugs-list**：実行バージョンおよび現在適用されている機能に関する既知のバグ。
  - **command-reference**：実行コンフィギュレーションのすべてのコマンドに対する参照リンク。
  - **product-advisory**：ネットワーク内のデバイスに影響する可能性のある Product Security Incident Response Team（PSIRT）通知、サポート終了（EOL）または販売終了（EOS）通知、あるいは Field Notice（FN）。

Cisco Output Interpreter ツールから分析およびレポート情報の要求を送信するには、次の手順に従います。

手順

ステップ 1 **call-home request output-analysis** *“show-command”* [**profile** *name*] [**ccoid** *user-id*]

例：

```
Router# call-home request output-analysis “show diag” profile TG
```

指定した show コマンドの出力を分析用に送信します。show コマンドは、引用符（""）で囲む必要があります。

ステップ 2 **call-home request** {**config-sanity** | **bugs-list** | **command-reference** | **product-advisory**} [**profile** *name*] [**ccoid** *user-id*]

例：

```
Router# call-home request config-sanity profile TG
```

分析のために、**show running-config all**、**show version** または **show module** コマンドなどの所定のコマンドセットの出力を送信します。また、**call home request product-advisory** サブコマンドには、すべてのインベントリ アラート グループ コマンドが含まれます。**request** の後に指定されたキーワードにより、必要なレポートのタイプが指定されます。

例

次に、ユーザー指定の **show** コマンドの分析要求の例を示します。

```
Router# call-home request output-analysis "show diag" profile TG
```

1 つのコマンドまたはコマンドリストのコマンド出力メッセージの手動送信

call-home send コマンドを使用して、1 つの IOS コマンドまたは IOS コマンドのリストを実行し、コマンド出力を HTTP または電子メールプロトコルを介して送信できます。

コマンド出力を送信する場合は、次の注意事項に従ってください。

- IOS コマンドまたは IOS コマンドリストとして、すべてのモジュール用のコマンドを含めて、任意の実行コマンドを指定できます。コマンドは、引用符（“”）で囲む必要があります。
- 「email」キーワードを使って電子メール オプションを選択し、電子メール アドレスを指定すると、コマンド出力はそのアドレスに送信されます。電子メール オプションも HTTP オプションも指定しない場合、出力は指定のサービス要求番号と共にロング テキスト形式で Sisco TAC （attach@cisco.com）に送信されます。
- 「email」キーワードも「http」キーワードも指定しない場合、ロング テキスト形式と XML メッセージ形式の両方でサービス要求番号が必要とされ、電子メールの件名行にサービス要求番号が示されます。
- HTTP オプションを指定している場合、CiscoTac-1 プロファイルの宛先 HTTP または HTTPS URL が宛先として使用されます。Smart Call Home から電子メール アドレスにメッセージを転送するよう、宛先の電子メールアドレスを指定できます。ユーザは、宛先の電子メール アドレスまたは SR 番号のいずれかを指定する必要があります（両方を指定することもできます）。

コマンドを実行し、コマンド出力を送信するには、次の手順を実行します。

手順

call-home send {*cli command* | *cli list*} [**email** *email* **msg-format** {**long-text** | **xml**} | **http** {**destination-email-address** *email*}] [**tac-service-request** *SR#*]

例：

```
Router# call-home send "show version;show running-config;show inventory" email support@example.com
 msg-format xml
```

CLI または CLI リストを実行し、電子メールまたは HTTP 経由で出力を送信します。

- {*cli command* | *cli list*}：1 つの IOS コマンドまたは（「,」で区切った）IOS コマンドリストを指定します。すべてのモジュールに対するコマンドを含む、あらゆる run コマンドを指定できます。これらのコマンドは引用符（“”）で囲む必要があります。
- **email** *email* **msg-format {long-text | xml}**：この **email** オプションが選択されている場合、指定の電子メールアドレスに向けてロングテキスト形式または XML 形式でコマンド出力が送信され、サービス要求番号がその件名に含められます。電子メール アドレス、サービス要求番号、またはその両方を指定する必要があります。電子メール アドレスが指定されない場合は、サービス リクエスト番号が必要です（デフォルトでは、ロング テキスト形式の場合は attach@cisco.com、XML 形式の場合は callhome@cisco.com）。
- **http** {**destination-email-address** *email*}：この **http** オプションが選択されている場合、コマンド出力は XML 形式で Smart Call Home バックエンドサーバー（TAC プロファイルで指定された URL）に送信されます。

  destination-email-address *email* を指定して、バックエンドサーバーから電子メールアドレスにメッセージを転送できるようにすることが可能です。電子メール アドレス、サービス要求番号、またはその両方を指定する必要があります。
- **tac-service-request** *SR#*：サービス要求番号を指定します。電子メール アドレスが指定されない場合は、サービス リクエスト番号が必要です。

例

以下に、コマンドの出力をユーザー指定の電子メールアドレスに送信する例を示します。

```
Router# call-home send "show diag" email support@example.com
```

以下に、SR 番号が指定され、ロングテキスト形式で attach@cisco.com に送信されるコマンド出力の例を示します。

```
Router# call-home send "show version; show run" tac-service-request 123456
```

以下に、XML メッセージ形式で callhome@cisco.com に送信されるコマンド出力の例を示します。

```
Router# call-home send "show version; show run" email callhome@cisco.com msg-format xml
```

以下に、SR 番号が指定され、XML メッセージ形式で Cisco TAC バックエンドサーバーへ送信されるコマンド出力の例を示します。

```
Router# call-home send "show version; show run" http tac-service-request 123456
```

以下に、Cisco TAC バックエンドサーバーに HTTP プロトコルを使用して送信され、ユーザーが指定した電子メールアドレスに転送されるコマンド出力の例を示します。

```
Router# call-home send "show version; show run" http destination-email-address
user@company.com
```

診断シグニチャの設定

診断シグニチャ機能は、デジタル署名されたシグニチャをデバイスにダウンロードします。診断シグニチャ（DS）ファイルは、診断イベントの情報を含んでいるフォーマット済みファイルです。これにより、シスコ ソフトウェアをアップグレードすることなくトラブルシューティングを実行できます。DS の目的は、お客様のネットワークで発生している既知の問題を解決するために使用可能なトラブルシューティング情報を検出/収集できる、柔軟性の高いインテリジェンスを提供することです。

診断シグニチャについて

診断シグニチャ

Call Home システムの診断シグニチャ（DS）に備わっている柔軟なフレームワークにより、新しいイベントおよび対応する CLI を定義できます。これらの CLI を使用すると、シスコ ソフトウェアをアップグレードせずにこれらのイベントを分析できます。

診断シグニチャにより、標準の Call Home 機能でサポートされていないイベント タイプとトリガー タイプを追加的に定義できます。診断シグニチャのサブシステムは、ファイルをデバイスにダウンロードして処理し、診断シグニチャイベントのコールバックを処理します。

診断シグニチャ機能は、ファイルの形式のデジタル署名シグニチャをデバイスにダウンロードします。DS ファイルは、診断イベントの情報を照合し、これらのイベントのトラブルシューティング手段を提供する、フォーマット済みファイルです。

DS ファイルには、イベントの説明を指定する XML データと、必要なアクションを実行する CLI コマンドまたはスクリプトが含まれています。これらのファイルは、整合性、信頼性、セキュリティを証明するために、シスコまたはサード パーティによりデジタル署名されています。

DS ファイルの構造は、次のいずれかです。

- イベント タイプを指定する、メタデータに基づく単純な署名。また、イベントの照合やアクションの実行（たとえば CLI を使用した情報の収集）に使用できるその他の情報もこれに含まれます。さらに、この署名は、特定のバグに対する回避策としてデバイスの設定を変更することもできます。
- 組み込みイベント マネージャ（EEM）Tool Command Language（Tcl）スクリプトに基づく署名。これはイベント レジスタ行で新しいイベントを指定し、Tcl スクリプトで追加のアクションを指定します。
- 上記の両方の形式の組み合わせ。

DS ファイルには次の基本情報が含まれています。

- **ID（一意の番号）**：DS の検索に使用できる DS ファイルを表す一意のキー。
- **名前（ShortDescription）**：選択用リストで使用できる、DS ファイルに関する一意の記述。
- **説明**：署名に関する詳細な記述。
- **リビジョン**：バージョン番号。DS の内容が更新されると大きくなります。
- **イベントおよびアクション**：検出対象のイベントと、イベントの発生後に実行すべきアクションを定義します。

診断シグニチャの前提条件

デバイスに診断シグニチャ（DS）をダウンロードして設定する前に、次の条件を満たしていることを確認します。

- デバイスに 1 つ以上の DS を割り当てる必要があります。デバイスへの DS の割り当ての詳細については、診断シグネチャのダウンロード （277 ページ）を参照してください。
- DS ファイルをダウンロードするためには HTTP/Secure HTTP（HTTPS）トランスポートが必要です。宛先 HTTPS サーバの認証をイネーブルにするには、認証局（CA）証明書をインストールする必要があります。

（注） トラストプール機能を設定する場合は、CA 証明書は不要です。

診断シグネチャのダウンロード

診断シグニチャ（DS）ファイルをダウンロードするには、セキュアHTTP（HTTPS）プロトコルが必要です。デバイスにファイルをダウンロードする方式として電子メール転送方式をすでに設定している場合、DS をダウンロードして使用するには、割り当て済みプロファイル転送方式を HTTPS に変更する必要があります。

Cisco ソフトウェアは既知の証明機関（CA）からの証明書プールをプロビジョニング、保存、および管理する方式を作成するためにPKIトラストプール管理機能を使用します。デバイスではこの機能がデフォルトでイネーブルに設定されています。トラストプール機能により、CA 証明書が自動的にインストールされます。CA 証明書は、宛先 HTTPS サーバの認証に必要です。

DS ファイルをダウンロードするためのDS更新要求には、標準ダウンロードと強制ダウンロードの 2 種類があります。標準ダウンロードは、最近更新された DS ファイルを要求します。標準ダウンロード要求をトリガーするには、定期的な設定を使用するか、またはオンデマンドで CLI を開始します。標準ダウンロード更新は、要求された DS バージョンがデバイス上の DS バージョンと異なる場合にのみ実行されます。定期的なダウンロードは、DS Web ポータルからデバイスにすでに割り当てられた DS が存在する場合にのみ開始されます。割り当てが行われた後、同じデバイスからの定期インベントリ メッセージへの応答の中に、定期的なDSのダウンロードおよび更新を開始するようデバイスに通知するフィールドが含まれます。DS 更新要求メッセージには、DS のステータスとリビジョン番号が含まれます。これにより、最新リビジョン番号の DS だけがダウンロードされます。

強制ダウンロードでは、特定の 1 つの DS または一連の DS がダウンロードされます。強制ダウンロード更新要求をトリガーする唯一の方法は、オンデマンドでCLIを開始することです。強制ダウンロード更新要求では、デバイス上の現在の DS ファイルのバージョンに関係なく、最新バージョンの DS ファイルがダウンロードされます。

DS ファイルにはデジタル署名が付いています。ダウンロードされるすべての DS ファイルに対して署名の検証が実行され、ファイルが信頼できるソースからのものであることが確認されます。

診断シグニチャのワークフロー

Cisco ソフトウェアでは診断シグニチャ（DS）機能がデフォルトでイネーブルに設定されています。診断シグニチャを使用する際のワークフローを次に示します。

- ダウンロードする DS を見つけて、それらをデバイスに割り当てます。このステップは、標準の定期ダウンロードでは必須ですが、強制ダウンロードでは必要ではありません。
- デバイスは、標準の定期ダウンロードまたはオンデマンドの強制ダウンロードで、割り当てられているすべての DS または特定の 1 つの DS をダウンロードします。

- デバイスはすべての DS のデジタル署名を検証します。検証に合格すると、デバイスはブートフラッシュやハードディスクなどの固定型ディスクに DS ファイルを保存します。これにより、デバイスのリロード後に DS ファイルを読み取ることができます。ルータでは、DS ファイルが bootflash:/call home ディレクトリに保存されます。
- デバイスは DS の最新リビジョンを取得してデバイス内の古いリビジョンを置き換えるために、標準の定期 DS ダウンロード要求を送信し続けます。
- デバイスはイベントを監視し、イベントが発生すると、DS ファイルに定義されているアクションを実行します。

診断シグニチャのイベントとアクション

イベントセクションとアクションセクションは、診断シグニチャで使用される主な領域です。イベントセクションでは、イベント検出に使用されるすべてのイベントの属性を定義します。アクションセクションでは、イベント発生後に実行する必要があるすべてのアクション（たとえば show コマンド出力を収集して解析のために Smart Call Home に送信）がリストされます。

診断シグニチャのイベント検出

診断シグニチャ（DS）のイベント検出の方法として、単一イベント検出と複数イベント検出の 2 つが定義されています。

単一イベント検出

単一イベント検出では、DS 内で 1 つのイベント ディテクタだけが定義されます。イベントの指定形式は、次の 2 種類のいずれかです。

- DS イベント指定タイプ：サポートされているイベント タイプは、syslog、定期、設定、即時活性挿抜（OIR）、および Call Home です。「即時」とは、このタイプの DS はイベントを検出せず、ダウンロードされると直ちにそのアクションが実行されることを示しています。Call-Home タイプは、既存のアラート グループに関して定義されている現在の CLI コマンドを変更します。
- 組み込みイベント マネージャ（EEM）指定タイプ：Cisco ソフトウェアを変更することなく、すべての新しい EEM イベント ディテクタをサポートします。

  EEM を使用したイベント検出以外では、Tool Command Language（Tcl）スクリプトを使ってイベント検出タイプが指定されると、DS がトリガーされます。

複数イベント検出

複数イベント検出では、複数のイベントディテクタ、対応する複数の追跡対象オブジェクト状態、およびイベント発生期間を定義します。複数イベント検出の指定形式には、追跡対象イベントディテクタに関する複合イベント相関を含めることができます。たとえば、3 つのイベントディテクタ（syslog、OIR、IPSLA）が、DS ファイルの作成時に定義されます。これらのイベント ディテクタに関して指定される相関は、syslog イベントおよび OIR イベントが同時にトリガーされるか、または IPSLA が単独でトリガーされる場合に、DS がアクションを実行することを示します。

診断シグニチャのアクション

診断シグニチャ（DS）ファイルは、イベントの発生時に開始すべきさまざまなアクションで構成されます。アクションタイプは、特定のイベントに対応して開始されるアクションの種類を示します。

変数は、ファイルをカスタマイズするために使用される DS 内の要素です。

DS アクションは、次の 4 つのタイプに分類されます。

- call-home
- command
- emailto
- script

DS アクション タイプ call-home および emailto はイベント データを収集し、Call-Home サーバまたは定義済み電子メール アドレスにメッセージを送信します。このメッセージでは、メッセージ タイプとして「diagnostic-signature」、メッセージ サブタイプとして DS ID が使用されます。

DS アクションタイプに関して定義されているコマンドは、デバイスの設定の変更、show コマンド出力の収集、またはデバイスでの任意の EXEC コマンドの実行を行う CLI コマンドを開始します。DS アクション タイプ script は、Tcl スクリプトを実行します。

診断シグニチャの変数

変数は診断シグニチャ（DS）内で参照され、DS ファイルをカスタマイズするために使用されます。DS 変数を他の変数と区別するために、すべての DS 変数名にはプレフィックス ds_ が付いています。サポートされる DS 変数の型は次のとおりです。

- システム変数：設定を変更することなく、デバイスにより自動的に割り当てられる変数。診断シグニチャ機能では、ds_hostname および ds_signature_id の 2 つのシステム変数がサポートされています。
- 環境変数：call-home diagnostic-signature コンフィギュレーション モードで **environment** *variable-name variable-value* コマンドを使って手動で割り当てられる値。すべての DS 環境変数の名前と値を表示するには、**show call-home diagnostic-signature** コマンドを使用します。未解決の環境変数が DS ファイルに含まれている場合、変数が解決されるまで、この DS は保留状態のままになります。
- プロンプト変数：特権 EXEC モードで **call-home diagnostic-signature install** *ds-id* コマンドを使って手動で割り当てられる値。この値を設定しない場合、DS のステータスは保留中になります。
- 正規表現変数：事前定義された CLI コマンド出力との、正規表現を使用したパターンマッチによって割り当てられる値。この値は DS の実行中に割り当てられます。
- syslog イベント変数：DS ファイルでの syslog イベント検出中に割り当てられる値。この変数は、syslog イベント検出に関してのみ有効です。

診断シグニチャの設定方法

診断シグニチャ用の Call Home サービスの設定

診断シグニチャ（DS）に関連する通知の送信先である連絡先の電子メール アドレスや、DS ファイルのダウンロード元である HTTP/secure HTTP（HTTPS） URL などの属性を設定するために、Call Home サービス機能を設定します。

また、新しいユーザ プロファイルを作成し、正しい属性を設定し、そのプロファイルを DS プロファイルとして割り当てることもできます。定期的なダウンロードの場合、フルインベントリ メッセージの直後に要求が送信されます。インベントリの定期設定を変更すると、DS の定期ダウンロードも再スケジュールされます。

（注） デフォルトでは、事前定義された Cisco TAC-1 プロファイルが DS プロファイルとしてイネーブルに設定されます。これを使用することをお勧めします。これを使用する場合、必要となる設定は、宛先転送方式の設定を **http** に変更することだけです。

手順

ステップ 1 **configure terminal**

例：

```
Router# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **service call-home**

例：

```
Router(config)# service call-home
```

デバイスで Call Home サービスをイネーブルにします。

ステップ 3 **call-home**

例：

```
Router(config)# call-home
```

Call Home を設定するために、Call-Home コンフィギュレーション モードを開始します。

ステップ 4 **contact-email-addr** *email-address*

例：

```
Router(cfg-call-home)# contact-email-addr userid@example.com
```

（任意）Call Home の顧客連絡先に使用する電子メール アドレスを割り当てます。

ステップ 5 **mail-server** {*ipv4-addr* | *name*} **priority** *number*

例：

```
Router(cfg-call-home)# mail-server 10.1.1.1 priority 4
```

（任意）Call Home の Simple Mail Transfer Protocol（SMTP）の電子メール サーバ アドレスを設定します。このコマンドは、いずれかの DS で定義されているアクションに電子メール送信が含まれる場合にのみ使用されます。

ステップ 6 **profile** *profile-name*

例：

```
Router(cfg-call-home)# profile user1
```

Call Home の宛先プロファイルを設定し、Call Home プロファイル コンフィギュレーション モードを開始します。

ステップ 7 **destination transport-method** {**email** | **http**}

例：

```
Router(cfg-call-home-profile)# destination transport-method http
```

Call Home の宛先プロファイルの転送方式を指定します。

（注）
診断シグニチャを設定するには、**http** オプションを使用する必要があります。

ステップ 8 **destination address** {**email** *address* | **http** *url*}

例：

```
Router(cfg-call-home-profile)# destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

Call Home メッセージ送信先のアドレス タイプとロケーションを設定します。

（注）
診断シグニチャを設定するには、**http** オプションを使用する必要があります。

ステップ 9 **subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm*}]

例：

```
Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30
```

Call Home の Inventory アラート グループに関するメッセージを送信するよう、宛先プロファイルを設定します。

- このコマンドは、DS ファイルの定期的ダウンロード用にのみ使用されます。

ステップ 10 **exit**

例：

```
Router(cfg-call-home-profile)# exit
```

Call Home プロファイル コンフィギュレーション モードを終了して、Call Home コンフィギュレーション モードに戻ります。

次のタスク

前述の手順で設定したプロファイルを DS プロファイルとして設定し、その他の DS パラメータを設定します。

診断シグニチャの設定

始める前に

Call Home 機能を設定して、Call Home プロファイルの属性を設定します。デフォルトの Cisco TAC-1 プロファイルを使用するか、新しく作成したユーザ プロファイルを使用できます。

手順

ステップ 1 **call-home**

例：

```
Router(config)# call-home
```

Call Home を設定するために、Call-Home コンフィギュレーション モードを開始します。

ステップ 2 **diagnostic-signature**

例：

```
Router(cfg-call-home)# diagnostic-signature
```

Call Home 診断シグニチャ モードを開始します。

ステップ 3 **profile** *ds-profile-name*

例：

```
Router(cfg-call-home-diag-sign)# profile user1
```

デバイス上で診断シグニチャ（DS）が使用する宛先プロファイルを指定します。

ステップ 4 **environment** *ds_env-var-name ds-env-var-value*

例：

```
Router(cfg-call-home-diag-sign)# environment ds_env1 envarval
```

デバイスの DS の環境変数値を設定します。

ステップ 5 **end**

例：

```
Router(cfg-call-home-diag-sign)# end
```

Call-Home 診断シグニチャ モードを終了して、特権 EXEC モードに戻ります。

ステップ 6 **call-home diagnostic-signature** [{**deinstall** | **download**} {*ds-id* | **all**} | **install** *ds-id*]

例：

```
Router# call-home diagnostic-signature download 6030
```

デバイスで診断シグニチャ ファイルをダウンロード、インストール、またはアンインストールします。

ステップ 7 **show call-home diagnostic-signature** [*ds-id* {**actions** | **events** | **prerequisite** | **prompt** | **variables** | **failure** | **statistics** | **download**}]

例：

```
Router# show call-home diagnostic-signature actions
```

Call-Home 診断シグニチャ情報を表示します。

診断シグニチャの設定例

次に、診断シグニチャ（DS）ファイルの定期的なダウンロード要求をイネーブルにする例を示します。この設定では、毎日午後 2:30 にサービス Call-Home サーバに向けてダウンロード要求が送信され、DS ファイルのチェックをします。転送方法は HTTP に設定されます。

```
Router> enable
Router# configure terminal
Router(config)# service call-home
Router(config)# call-home
Router(cfg-call-home)# contact-email-addr userid@example.com
Router(cfg-call-home)# mail-server 10.1.1.1 priority 4
Router(cfg-call-home)# profile user-1
Router(cfg-call-home-profile)# destination transport-method http
Router(cfg-call-home-profile)# destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30
Router(cfg-call-home-profile)# exit
Router(cfg-call-home)# diagnostic-signature
Router(cfg-call-home-diag-sign)# profile user1
Router(cfg-call-home-diag-sign)# environment ds_env1 envarval
Router(cfg-call-home-diag-sign)# end
```

次に、前述の構成での **show call-home diagnostic-signature** コマンドの出力例を示します。

```
outer# show call-home diagnostic-signature

Current diagnostic-signature settings:
Diagnostic-signature: enabled
Profile: user1 (status: ACTIVE)
Environment variable:
ds_env1: abc
Downloaded DSes:
DS ID    DS Name                          Revision Status     Last Update (GMT+00:00)
-------- -------------------------------- -------- ---------- -------------------
6015     CronInterval                     1.0      registered 2013-01-16 04:49:52
```

```
6030     ActCH                          1.0      registered 2013-01-16 06:10:22
6032     MultiEvents                    1.0      registered 2013-01-16 06:10:37
6033     PureTCL                        1.0      registered 2013-01-16 06:11:48
```

Call Home コンフィギュレーション情報の表示

show call-home コマンドをさまざまな形式で使用して、Call Home 設定情報を表示できます。

手順

ステップ 1 **show call-home**

例：

```
Router# show call-home
```

Call Home 設定の概要を表示します。

ステップ 2 **show call-home detail**

例：

```
Router# show call-home detail
```

Call Home 設定の詳細を表示します。

ステップ 3 **show call-home alert-group**

例：

```
Router# show call-home alert-group
```

使用可能なアラート グループとそれらのステータスを表示します。

ステップ 4 **show call-home mail-server status**

例：

```
Router# show call-home mail-server status
```

設定済みのE メール サーバのアベイラビリティをチェックして表示します。

ステップ 5 **show call-home profile** {**all** | *name*}

例：

```
Router# show call-home profile all
```

指定された宛先プロファイルの設定を表示します。**all**キーワードを使用してすべての宛先プロファイルの設定を表示します。

ステップ 6 **show call-home statistics** [**detail** | **profile** *profile_name*]

例：

```
Router# show call-home statistics
```

Call Home イベントの統計情報を表示します。

例

Call Home 情報の要約

Call Home 情報の詳細

使用可能な Call Home アラートグループ

電子メールサーバーのステータス情報

すべての宛先プロファイルの情報

ユーザー定義宛先プロファイルの情報

Call Home の統計情報

次に、**show call-home** コマンドの異なるオプションを使用した場合の出力例を示します。

```
Router# show call-home
Current call home settings:
    call home feature : enable
    call home message's from address: router@example.com
    call home message's reply-to address: support@example.com

    vrf for call-home messages: Not yet set up

    contact person's email address: technical@example.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Picaboo Street, Any city, Any state, 12345
    customer ID: ExampleCorp
    contract ID: X123456789
    site ID: SantaClara

    source ip address: Not yet set up
    source interface: GigabitEthernet0/0
    Mail-server[1]: Address: 192.0.2.1 Priority: 1
    Mail-server[2]: Address: 209.165.202.254 Priority: 2
    http proxy: 192.0.2.2:80

    aaa-authorization: disable
    aaa-authorization username: callhome (default)
    data-privacy: normal
    syslog throttling: enable

    Rate-limit: 20 message(s) per minute

    Snapshot command[0]: show version
    Snapshot command[1]: show clock
```

```
Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- --------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info

Profiles:
    Profile Name: campus-noc
    Profile Name: CiscoTAC-1
Router#
```

```
Router# show call-home detail
Current call home settings:
    call home feature : enable
    call home message's from address: router@example.com
    call home message's reply-to address: support@example.com

    vrf for call-home messages: Not yet set up

    contact person's email address: technical@example.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Picaboo Street, Any city, Any state, 12345
    customer ID: ExampleCorp
    contract ID: X123456789
    site ID: SantaClara

    source ip address: Not yet set up
    source interface: GigabitEthernet0/0
    Mail-server[1]: Address: 192.0.2.1 Priority: 1
    Mail-server[2]: Address: 209.165.202.254 Priority: 2
    http proxy: 192.0.2.2:80

    aaa-authorization: disable
    aaa-authorization username: callhome (default)
    data-privacy: normal
    syslog throttling: enable

    Rate-limit: 20 message(s) per minute

    Snapshot command[0]: show version
    Snapshot command[1]: show clock

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- --------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info

Profiles:

Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
```

```
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     normal
    environment               debug
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug

Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    Profile mode: Full Reporting
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 14 day of the month at 11:12

    Periodic inventory info message is scheduled every 14 day of the month at 10:57

    Alert-group               Severity
    ------------------------  ------------
    crash                     normal
    environment               minor

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug
Router#

Router# show call-home alert-group
Available alert groups:
    Keyword                   State   Description
    ------------------------ ------- --------------------------------
    configuration             Enable  configuration info
    crash                     Enable  crash and traceback info
    environment               Enable  environmental info
    inventory                 Enable  inventory info
    snapshot                  Enable  snapshot info
    syslog                    Enable  syslog info
Router#

Router# show call-home mail-server status
Please wait. Checking for mail server status ...

    Mail-server[1]: Address: 192.0.2.1 Priority: 1 [Not Available]
    Mail-server[2]: Address: 209.165.202.254 Priority: 2 [Available]
Router#

Router# show call-home profile all

Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up
```

```
    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     normal
    environment               debug
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug

Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    Profile mode: Full Reporting
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 14 day of the month at 11:12

    Periodic inventory info message is scheduled every 14 day of the month at 10:57

    Alert-group               Severity
    ------------------------  ------------
    crash                     normal
    environment               minor

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug
Router#
```

```
Router# show call-home profile campus-noc
Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     normal
    environment               debug
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug

Router#
```

```
Router# show call-home statistics
Message Types    Total               Email               HTTP
-------------   -------------------- -------------------- ------------------
Total Success   3                    3                    0
    Config      3                    3                    0
    Crash       0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    Snapshot    0                    0                    0
```

```
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0

Total In-Queue  0                   0                   0
    Config      0                   0                   0
    Crash       0                   0                   0
    Environment 0                   0                   0
    Inventory   0                   0                   0
    Snapshot    0                   0                   0
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0

Total Failed    0                   0                   0
    Config      0                   0                   0
    Crash       0                   0                   0
    Environment 0                   0                   0
    Inventory   0                   0                   0
    Snapshot    0                   0                   0
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0

Total Ratelimit
      -dropped  0                   0                   0
    Config      0                   0                   0
    Crash       0                   0                   0
    Environment 0                   0                   0
    Inventory   0                   0                   0
    Snapshot    0                   0                   0
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0

Last call-home message sent time: 2011-09-26 23:26:50 GMT-08:00
Router#
```

Call Home のデフォルト設定

次の表に、Call Home のデフォルト設定を示します。

表 *21 : Call Home* のデフォルト設定

パラメータ	デフォルト
Call Home 機能のステータス	ディセーブル
ユーザ定義プロファイルのステータス	Active
定義済みのシスコ TAC プロファイルのステータス	Inactive

パラメータ	デフォルト
転送方法	電子メール
メッセージのフォーマット タイプ	XML
ロングテキスト、ショートテキスト、または XML 形式で送信されるメッセージの宛先メッセージのサイズ	3,145,728
アラート グループのステータス	イネーブル
Call Home メッセージのシビラティ（重大度）しきい値	Debug
1 分間に送信するメッセージのレート制限	20
AAA Authorization	ディセーブル
Call Home の syslog メッセージ スロットリング	イネーブル
データ プライバシー レベル	標準

アラートグループの起動イベントとコマンド

Call Home 起動イベントはアラート グループに分類され、各アラート グループには、イベント発生時に実行されるコマンドが割り当てられます。転送されるメッセージにはコマンド出力が含まれます。次の表では、各アラート グループに含まれる起動イベントを示します。アラート グループの各イベントのシビラティ（重大度）と、実行されるコマンドも示します。

表 *22 : Call Home* アラート グループ、イベント、および動作

アラート グループ	Call Home 起動イベント	Syslog イベント	シビラティ（重大度）	説明および実行されるコマンド
Crash	SYSTEM_CRASH	–	–	ソフトウェア クラッシュに関連するイベント。 The following commands are executed: **show version** **show logging** **show region** **show inventory** **show stack** **crashinfo file**（このコマンドは crashinfo ファイルの内容を表示します）
–	TRACEBACK	–	–	ソフトウェアのトレース バック イベントを検出します。 The following commands are executed: **show version** **show logging** **show region** **show stack**

アラート グループ	Call Home 起動イベント	Syslog イベント	シビラティ（重大度）	説明および実行されるコマンド
設定	–	–	–	設定または設定変更イベントに関するユーザ生成された要求。 The following commands are executed: **show platform** **show inventory** **show running-config all** **show startup-config** **show version**
環境	–	–	–	電源、ファン、温度アラームなどの環境センシング要素に関連するイベント。 The following commands are executed: **show environment** **show inventory** **show platform** **show logging**
–	–	SHUT	0	環境モニタがシャットダウンを開始しました。
–	–	ENVCRIT	2	温度または電圧測定値がクリティカルなしきい値を超えました。
–	–	BLOWER	3	必要な数のファントレイがない。

アラート グループ	Call Home 起動イベント	Syslog イベント	シビラティ（重大度）	説明および実行されるコマンド
–	–	ENVWARN	4	温度または電圧測定値が警告しきい値を超えました。
–	–	RPSFAIL	4	電源に故障したチャネルがあります。
–	ENVM	PSCHANGE	6	電源名の変更
–	–	PSLEV	6	電源状態の変更
–	–	PSOK	6	電源が正常に動作しているようです。

アラート グループ	Call Home 起動イベント	Syslog イベント	シビラティ（重大度）	説明および実行されるコマンド
Inventory	–	–	–	

アラート グループ	Call Home 起動イベント	Syslog イベント	シビラティ（重大度）	説明および実行されるコマンド
				Inventory ステータスは、ユニットがコールド ブートされた場合や、FRU が挿入または取り外された場合に指定される。これは、重大ではないイベントと見なされ、情報はステータスと資格設定に使用される 匿名モードで送信されるすべてのインベントリ メッセージとフル登録モードで送信されるデルタ インベントリ メッセージに対して実行されるコマンド： **show diag all eeprom detail** **show version** **show inventory oid** **show platform** フル登録モードで送信されるフル インベントリ メッセージに対して実行されるコマンド： **show platform** **show diag all eeprom detail** **show version** **show inventory oid** **show bootflash: all** **show**

アラート グループ	Call Home 起動イベント	Syslog イベント	シビラティ（重大度）	説明および実行されるコマンド
				data-corruption **show interfaces** **show file systems** **show memory statistics** **show process memory** **show process cpu** **show process cpu history** **show license udi** **show license detail** **show buffers**
–	HARDWARE_ REMOVAL	REMCARD	6	カードがスロット %d から取り外され、インターフェイスがディセーブルになった。
–	HARDWARE_ INSERTION	INSCARD	6	カードがスロット %d に挿入されました。管理上インターフェイスはシャットダウンします。
Syslog	–	–	–	syslog にログ記録されるイベント The following commands are executed: **show inventory** **show logging**
–	SYSLOG	LOG_EMERG	0	システムが使用不可能な状態。
–	SYSLOG	LOG_ALERT	1	即時対処が必要。
–	SYSLOG	LOG_CRIT	2	深刻な状況です。

アラート グループ	Call Home 起動イベント	Syslog イベント	シビラティ（重大度）	説明および実行されるコマンド
–	SYSLOG	LOG_ERR	3	エラー状態です。
–	SYSLOG	LOG_WARNING	4	警告状態。
–	SYSLOG	LOG_NOTICE	5	正常だが重大な状態。
–	SYSLOG	LOG_INFO	6	通知
–	SYSLOG	LOG_DEBUG	7	デバッグレベル メッセージ。
Test	–	TEST	–	ユーザが作成したテスト メッセージ The following commands are executed: **show platform** **show inventory** **show version**

メッセージの内容

ここでは、アラート グループ メッセージの内容の形式を示すいくつかの表を示します。

次の表に、ショートテキストメッセージの内容フィールドを示します。

表 *23 :* ショートテキストメッセージの形式

データ項目	説明
デバイス ID	設定されたデバイス名
日時スタンプ	起動イベントのタイム スタンプ
エラー判別メッセージ	起動イベントの簡単な説明（英語）
アラームの緊急度	システム メッセージに適用されるようなエラー レベル

次の表に、すべてのロングテキストメッセージと XML メッセージに共通する内容フィールドを示します。特定のアラート グループ メッセージに固有のフィールドは、共通フィールドの間に挿入されます。挿入ポイントは表に示しています。

表 *24 :* ロングテキストメッセージと *XML* メッセージすべてに共通のフィールド

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
Time stamp	ISO 時刻表記（*YYYY-MM-DD HH:MM:SS GMT+HH:MM*）によるイベントの日付とタイムスタンプ。	CallHome/EventTime
メッセージ名	メッセージの名前。具体的なイベント名のリストはアラートグループの起動イベントとコマンド（290 ページ）に示されています。	ショート テキスト メッセージの場合のみ
メッセージ タイプ	「Call Home」を指定。	CallHome/Event/Type
Message subtype	特定のメッセージ タイプ：full、delta、test	CallHome/Event/SubType
メッセージ グループ	「reactive」を指定。デフォルトは「reactive」であるため、任意。	Long-text メッセージ専用
シビラティ（重大度）	メッセージのシビラティ（重大度）（メッセージシビラティ（重大度）しきい値（262 ページ）を参照）。	Body/Block/Severity
送信元 ID	ワークフロー エンジンから経路指定する製品タイプ。一般に製品ファミリ名です。	Long-text メッセージ専用

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
デバイス ID	メッセージを生成するエンドデバイスの Unique Device Identifier（UDI）。メッセージがファブリック スイッチに固有でない場合、このフィールドは空白。形式は、*type@Sid@serial*。 • *type* は、バックプレーン IDPROM からの製品の型番。 • @ は区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：CISCO3845@C@12345678	CallHome/CustomerData/ContractData/DeviceId
カスタマー ID	サポート サービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド	CallHome/CustomerData/ContractData/CustomerId
連絡先 ID	サポート サービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド	CallHome/CustomerData/ContractData/CustomerId
サイト ID	シスコが提供したサイト ID または別のサポート サービスにとって意味のあるその他のデータに使用されるオプションのユーザ設定可能なフィールド	CallHome/CustomerData/ContractData/CustomerId

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
Server ID	メッセージがファブリック スイッチから生成されている場合、これはスイッチの固有のデバイス ID（UDI）。 • *type* は、バックプレーン IDPROM からの製品の型番。 • @ は区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：CISCO3845@C@12345678	ロング テキスト メッセージの場合のみ。
メッセージの説明	エラーを説明する短い文章。	CallHome/MessageDescription
デバイス名	イベントが発生するノード。これは、デバイスのホスト名です。	CallHome/CustomerData/SystemInfo/NameName
担当者名	イベント発生中のノードに関する問題の問い合わせ先の担当者名。	CallHome/CustomerData/SystemInfo/Contact
連絡先 E メール	このユニットの連絡先である人物の電子メール アドレス。	CallHome/CustomerData/SystemInfo/ContactEmail
連絡先電話番号	このユニットの連絡先である人物の電話番号	CallHome/CustomerData/SystemInfo/ContactPhoneNumber
住所	このユニットに関連した RMA 部品の送付先住所を格納しているオプションのフィールド。	CallHome/CustomerData/SystemInfo/StreetAddress
モデル名	ルータのモデル名。これは製品ファミリ名の一部である固有モデルです。	CallHome/Device/Cisco_Chassis/Model
シリアル番号	ユニットのシャーシのシリアル番号	CallHome/Device/Cisco_Chassis/SerialNumber

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
シャーシの部品番号	シャーシの最上アセンブリ番号	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name=“PartNumber”
System object ID	システムを一意に識別するシステム オブジェクト ID。	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name=“sysObjectID”
システム記述	管理対象デバイスのシステム説明。	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name=“sysDescr”

次の表に、特定のアラートグループメッセージに固有の挿入フィールドを示します。

（注） このアラートグループに対して複数のコマンドが実行されると、次のフィールドが繰り返される場合があります。

表 *25*：特定のアラートグループメッセージに固有の挿入フィールド

コマンド出力名	実行されたコマンドの正確な名前。	/aml/Attachments/Attachment/Name
添付タイプ	アタッチメントのタイプ。通常は “inline”。	/aml/Attachments/Attachment@type
MIME タイプ	通常は、"text"、"plain"、または符号化タイプのいずれか。	/aml/Attachments/Attachment/Data@encoding
コマンド出力テキスト	自動的に実行されたコマンドの出力（アラートグループの起動イベントとコマンド（290 ページ） を参照）。	/mml/attachments/attachment/atdata

次の表に、対処的メッセージ（TAC ケースを必要とするシステム障害）と予防的メッセージ（システムパフォーマンスの低下を引き起こす可能性のある問題）に挿入される内容フィールドを示します。

表 *26*：対処的または予防的イベントメッセージに挿入されるフィールド

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
シャーシのハードウェア バージョン	シャーシのハードウェア バージョン	CallHome/Device/Cisco_Chassis/HardwareVersion

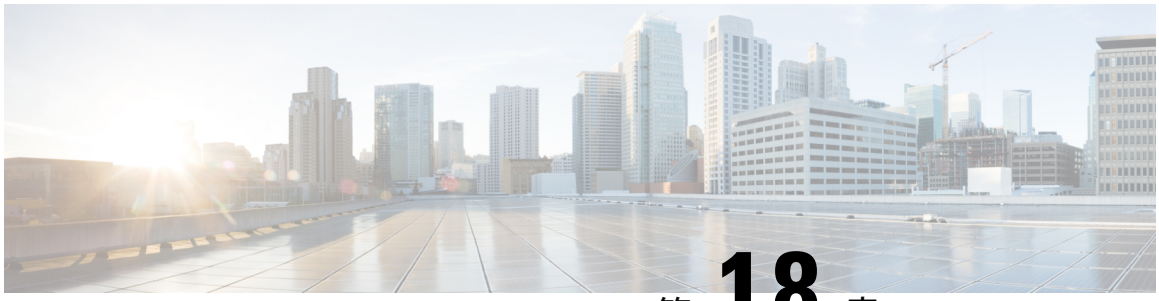
データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
スーパーバイザ モジュールのソフトウェア バージョン	最上位ソフトウェア バージョン	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name=“SoftwareVersion”
影響のある FRU の名前	イベント メッセージを生成している問題の FRU の名前	CallHome/Device/Cisco_Chassis/Cisco_Card/Model
影響のある FRU のシリアル番号	問題を起こした FRU のシリアル番号	CallHome/Device/Cisco_Chassis/Cisco_Card/SerialNumber
影響のある FRU の製品番号	問題を起こした FRU の部品番号	CallHome/Device/Cisco_Chassis/Cisco_Card/PartNumber
FRU スロット	イベント メッセージを生成している FRU のスロット番号	CallHome/Device/Cisco_Chassis/Cisco_Card/LocationWithinContainer
FRU ハードウェア バージョン	問題を起こした FRU のハードウェア バージョン	CallHome/Device/Cisco_Chassis/Cisco_Card/HardwareVersion
FRU ソフトウェア バージョン	問題を起こした FRU で動作するソフトウェア バージョン	CallHome/Device/Cisco_Chassis/Cisco_Card/SoftwareIdentity/VersionString

次の表に、インベントリメッセージに挿入される内容フィールドを示します。

表 *27*：コンポーネント イベント メッセージの挿入フィールド

データ項目（プレーン テキストおよび XML）	説明（プレーンテキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
シャーシのハードウェア バージョン	シャーシのハードウェア バージョン	CallHome/Device/Cisco_Chassis/HardwareVersion
スーパーバイザ モジュールのソフトウェア バージョン	最上位ソフトウェアバージョン	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name=“SoftwareVersion”
FRU name	イベントメッセージを生成している問題の FRU の名前	CallHome/Device/Cisco_Chassis/Cisco_Card/Model
FRU s/n	FRU のシリアル番号	CallHome/Device/Cisco_Chassis/Cisco_Card/SerialNumber
FRU 製品番号	FRU の製品番号	CallHome/Device/Cisco_Chassis/Cisco_Card/PartNumber
FRU スロット	FRU のスロット番号	CallHome/Device/Cisco_Chassis/Cisco_Card/LocationWithinContainer
FRU ハードウェア バージョン	FRUのハードウェア バージョン	CallHome/Device/Cisco_Chassis/CiscoCard/HardwareVersion

データ項目（プレーン テキストおよび XML）	説明（プレーンテキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
FRU ソフトウェア バージョン	FRU 上で動作しているソフトウェア バージョン	CallHome/Device/Cisco_Chassis/Cisco_Card/SoftwareIdentity/VersionString



第 18 章

Cisco 拡張サービス モジュールおよびネットワーク インターフェイス モジュールの管理

ルータは Cisco 拡張サービス モジュールおよび Cisco ネットワーク インターフェイス モジュール（NIM）をサポートしています。これらのモジュールは、アダプタ（キャリア カード）を使用して、ルータのさまざまなスロットに装着されます。詳細については、次のマニュアルを参照してください。

- Hardware Installation Guide for Cisco 8300 Series Secure Routers

この章の内容は、次のとおりです。

Cisco サービスモジュールおよびネットワーク インターフェイス モジュールに関する情報

ルータは、アーキテクチャに組み込まれているモジュール管理機能を使用して、サポートされている Cisco サービスモジュール（SM）、ネットワーク インターフェイス モジュール（NIM）および PIM（着脱可能インターフェイスモジュール）を設定、管理、制御します。この新しい一元化されたモジュール管理機能により、システムのすべてのモジュールを、そのタイプや用途とは無関係に共通の方法で制御および監視できます。ルータでサポートされるすべての Cisco 拡張サービス モジュールとネットワーク インターフェイス モジュールは、標準 IP プロトコル

を使用してホスト ルータと通信します。Cisco IOS ソフトウェアは、モジュール間の切り替えに異種データ パス統合を使用します。

- サポートされるモジュール （306 ページ）
- ネットワーク インターフェイス モジュールと拡張サービスモジュール （306 ページ）

サポートされるモジュール

Cisco 8300 シリーズ セキュアルータでサポートされるインターフェイスおよびモジュールについては、『Hardware Installation Guide for Cisco 8300 Series Secure Routers』を参照してください。

ネットワーク インターフェイス モジュールと拡張サービスモジュール

サポートされているネットワーク インターフェイス モジュールとサービスモジュールの詳細については、Cisco 8300 シリーズ セキュアルータのデータシートを参照してください。

プラットフォームでの SM および NIM の導入

- モジュールファームウェアのダウンロード （306 ページ）
- SM と NIM のインストール （307 ページ）
- コンソール接続または Telnet 経由でのモジュールへのアクセス （307 ページ）
- ホットスワップ（OIR） （307 ページ）

モジュールファームウェアのダウンロード

サービスモジュールを使用できるようにするには、ルータにモジュール ファームウェアをロードする必要があります。

ファームウェアをダウンロードするために、モジュールは内部 eth0 インターフェイスを介して RP に接続します。最初に、モジュールは BOOTP を介して自身の IP アドレスを取得します。また、BOOTP はイメージのダウンロードに使われる TFTP サーバのアドレスも提供します。イメージがロードされ、モジュールが起動された後、モジュールは DHCP を介して実行中のイメージの IP アドレスを提供します。

SM と NIM のインストール

詳細については、『Hardware Installation Guide for Cisco 8300 Series Secure Routers』の「Installing and Removing NIMs and SMs」を参照してください。

コンソール接続または Telnet 経由でのモジュールへのアクセス

モジュールにアクセスするには、その前にルータ コンソールまたは Telnet 経由でホスト ルータに接続する必要があります。ルータに接続したら、モジュールに接続されているギガビット イーサネット インターフェイスで IP アドレスを設定する必要があります。ルータ上で特権 EXEC モードで **hw-module session** コマンドを使用して、モジュールへのセッションを開始します。

モジュールへの接続を確立するには、Telnet またはセキュアシェル（SSH）を使用してルータ コンソールに接続し、ルータ上で特権 EXEC モードで **hw-module session** *slot/subslot* コマンドを使用して、スイッチへのセッションを開始します。

次の設定例を使用して、接続を確立します。

- 次に、**hw-module session** コマンドを使用してルータからセッションを開始する例を示します。

```
Router# hw-module session slot/card
Router# hw-module session 0/1 endpoint 0

Establishing session connect to subslot 0/1
```

- 次に、キーボードで **Ctrl-A** を押した後に **Ctrl-Q** を押して、ルータからセッションを終了する例を示します。

```
type ^a^q
picocom v1.4

port is        : /dev/ttyDASH2
flowcontrol    : none
baudrate is    : 9600
parity is      : none
databits are   : 8
escape is      : C-a
noinit is      : no
noreset is     : no
nolock is      : yes
send_cmd is    : ascii_xfr -s -v -l10
receive_cmd is : rz -vv
```

ホットスワップ（OIR）

ルータは Cisco 拡張サービス モジュールおよび Cisco ネットワーク インターフェイス モジュールの活性挿抜（OIR）をサポートしています。OIR 機能を使用して、次の作業を実行できます。

（注） ルータはモジュールの OIR をサポートしますが、モジュールのホットリムーブとホットインサーションはサポートしていません。挿入するか取り外す前に、これらのモジュールでトラフィックを停止してください。

モジュールの活性挿抜の準備

ルータでは、装着されている別のモジュールの取り外しに関係なく、モジュールの活性挿抜（OIR）がサポートされています。つまり、アクティブなモジュールをルータに装着したままで、別のモジュールをいずれかのサブスロットから取り外すことができます。モジュールを直ちに交換する予定がない場合は、サブスロットにブランク フィラー プレートを必ず取り付けてください。

モジュールの非アクティブ化

モジュールは、ルータから取り外す前に非アクティブ化する必要があります。正常に非アクティブにするには、EXEC モードで **hw-module subslot** *slot/subslot* **stop** コマンドを実行します。

（注） モジュールの OIR を準備しているときには、モジュールを非アクティブ化する前に各インターフェイスを個別にシャット ダウンする必要はありません。EXEC モードで **hw-module subslot** *slot/subslot* **stop** コマンドを実行すると、インターフェイスのトラフィックが自動的に停止し、OIR に備えてモジュールと共にこれらのインターフェイスが非アクティブ化されます。同様に、OIR の後にモジュールのインターフェイスを個別に再起動する必要はありません。

次の例では、**show facility-alarm status** コマンドを使用して、モジュールがシステムから取り外された時点でクリティカルアラームが生成されるかどうかを確認します。

```
Router# show facility-alarm status
System Totals  Critical: 18  Major: 0  Minor: 0

Source                    Time                  Severity      Description [Index]
------                    ------                --------      -------------------

Power Supply Bay 1        Sep 28 2020 10:02:34  CRITICAL      Power Supply/FAN Module
 Missing [0]
POE Bay 0                 Sep 28 2020 10:02:34  INFO          Power Over Ethernet
Module Missing [0]
POE Bay 1                 Sep 28 2020 10:02:34  INFO          Power Over Ethernet
```

```
Module Missing [0]
GigabitEthernet0/0/2       Sep 28 2020 10:02:46   INFO          Physical Port
Administrative State Down [2]
GigabitEthernet0/0/3       Sep 28 2020 10:02:46   INFO          Physical Port
Administrative State Down [2
xcvr container 0/0/4       Sep 28 2020 10:02:46   INFO          Transceiver Missing -
Link Down [1]
TenGigabitEthernet0/0/5    Sep 28 2020 10:02:54   CRITICAL      Physical Port Link Down
 [1]
TenGigabitEthernet0/1/0    Sep 28 2020 10:03:26   INFO          Physical Port
Administrative State Down [2]
GigabitEthernet1/0/0       Sep 28 2020 10:07:35   CRITICAL      Physical Port Link Down
 [1]
GigabitEthernet1/0/1       Sep 28 2020 10:07:35   CRITICAL      Physical Port Link Down
 [1]
GigabitEthernet1/0/2       Sep 28 2020 10:07:35   CRITICAL      Physical Port Link Down
 [1]
GigabitEthernet1/0/3       Sep 28 2020 10:07:35   CRITICAL      Physical Port Link Down
 [1]
GigabitEthernet1/0/4       Sep 28 2020 10:07:35   CRITICAL      Physical Port Link Down
 [1]
GigabitEthernet1/0/5       Sep 28 2020 10:07:35   CRITICAL      Physical Port Link Down
 [1]
TwoGigabitEthernet1/0/16   Sep 28 2020 10:07:35   INFO          Physical Port
Administrative State Down [2]
TwoGigabitEthernet1/0/17   Sep 28 2020 10:07:35   INFO          Physical Port
Administrative State Down [2]
TwoGigabitEthernet1/0/18   Sep 28 2020 10:07:35   INFO          Physical Port
Administrative State Down [2]
TwoGigabitEthernet1/0/19   Sep 28 2020 10:07:35   INFO          Physical Port
Administrative State Down [2]
xcvr container 1/0/20      Sep 28 2020 10:04:00   INFO          Transceiver Missing -
Link Down [1]
xcvr container 1/0/21      Sep 28 2020 10:04:00   INFO          Transceiver Missing -
Link Down [1]1]
```

（注） 正しい非アクティブ化の後にモジュールを取り外した場合でも、クリティカルアラーム（Active Card Removed OIR Alarm）が生成されます。

異なるコマンドモードでのモジュールおよびインターフェイスの非アクティブ化

次のいずれかのモードで **hw-module subslot** コマンドを使用して、モジュールとそのインターフェイスを非アクティブにできます。

1. **hw-module subslot** *slot/subslot* **shutdown unpowered**

   グローバル コンフィギュレーション モードで **hw-module subslot** *slot/subslot* **shutdown unpowered** コマンドを実行してモジュールとそのインターフェイスを非アクティブにする場合は、ルータを何度リブートしてもモジュールがブートしないように設定を変更することができます。リモート場所に設置されているモジュールをシャットダウンする必要がある場合、ルータのリブート時にモジュールが自動的にブートしないようにするには、このコマンドが役立ちます。

   ```
   Router(config)# hw-module subslot 0/2 shutdown unpowered
   ```

ルータの指定のスロットおよびサブスロットに装着されているモジュールを非アクティブにします。ここで、

- *slot*：モジュールが装着されているシャーシスロット番号を指定します。
- *subslot*：モジュールが装着されているシャーシのサブスロット番号を指定します。
- **shutdown**：指定したモジュールをシャットダウンします。
- **unpowered**：実行コンフィギュレーションからモジュールのすべてのインターフェイスを削除し、モジュールの電源をオフにします。

2. **hw-module subslot** *slot/subslot* [**reload** | **stop** | **start**]

EXEC モードで **hw-module subslot** *slot/subslot* **stop** コマンドを使用すると、モジュールが正常にシャットダウンされます。**hw-module subslot** *slot/subslot* **start** コマンドを実行すると、モジュールがリブートされます。

```
Router# hw-module subslot 0/2 stop
```

指定のスロットおよびサブスロットに装着されたモジュールを非アクティブにします。ここで、

- *slot*：モジュールが装着されているシャーシスロット番号を指定します。
- *subslot*：モジュールが装着されているシャーシのサブスロット番号を指定します。
- **reload**：指定したモジュールを停止してから再起動します。
- **stop**：モジュールからすべてのインターフェイスを削除し、モジュールの電源をオフにします。
- **start**：指定のスロットに物理的に装着されたモジュールの場合と同様に、モジュールの電源をオンにします。モジュール ファームウェアがリブートし、モジュール初期化シーケンス全体が IOMd および Input/Output Module daemon（IOSd）プロセスで実行されます。

モジュールの再アクティブ化

hw-module subslot *slot/subslot* **stop** コマンドを使用してモジュールを非アクティブにした後に、OIR を実行せずにモジュールを再アクティブ化するには、次のいずれかのコマンドを（特権 EXEC モードで）使用します。

- **hw-module subslot** *slot/subslot* **start**
- **hw-module subslot** *slot/subslot* **reload**

モジュールの非アクティブ化およびアクティブ化の確認

モジュールを非アクティブにすると、対応するインターフェイスも非アクティブになります。そのため、これらのインターフェイスは **show interface** コマンドの出力に表示されなくなります。

1. モジュールが非アクティブになったかどうかを確認するには、特権 EXEC コンフィギュレーション モードで **show hw-module subslot all oir** コマンドを入力します。

   確認するモジュールに対応した [Operational Status] フィールドを調べます。次の例では、ルータのサブスロット 1 に装着されているモジュールが管理上、ダウン状態になっています。

```
Router# show hw-module subslot all oir

  Module                   Model              Operational Status
----------------------- -------------------- ------------------------

subslot 0/0             4M-2xSFP+            ok

subslot 0/1             C-NIM-8M             ok
subslot 0/4             VDSP-CC              ok
```

2. モジュールがアクティブ化されて適切に動作していることを確認するには、**show hw-module subslot all oir** コマンドを入力して、次の例のように [Operational Status] フィールドに「ok」と表示されるかどうかを調べます。

```
Router# show hw-module subslot all oir

 Module                   Model              Operational Status
----------------------- -------------------- ------------------------

subslot 0/0             4M-2xSFP+            ok

subslot 0/1             C-NIM-8M             ok
subslot 0/4             VDSP-CC              ok
```

モジュールおよびインターフェイスの管理

ルータはさまざまなモジュールをサポートしています。サポートされるモジュールの一覧については、サポートされるモジュール（306 ページ）を参照してください。モジュール管理プロセスでは、モジュールのリソースを利用できるよう、モジュールを起動する操作が行われます。このプロセスは、モジュールの検出、認証、クライアントによる設定、ステータス の報告、リカバリなどのタスクから成ります。

ルータでサポートされる Small Form-Factor Pluggable（SFP）モジュールの一覧については、『Hardware Installation Guide for Cisco 8300 Series Secure Routers』の「Installing and Upgrading Internal Modules and FRUs」の項を参照してください。

ここでは、モジュールとインターフェイスの管理に関する追加情報を示します。

モジュールインターフェイスの管理

モジュールの稼動後に、そのモジュール インターフェイスを制御および監視できます。インターフェイス管理には、**shut** または **no shut** コマンドを使用したクライアントの設定や、インターフェイスの状態およびインターフェイス レベルの統計情報のレポートが含まれます。

設定例

ここでは、モジュールを非アクティブおよびアクティブにする例を示します。

モジュール設定の非アクティブ化：例

モジュールを非アクティブにして、そのモジュールのOIRを実行できます。次に、モジュール（およびそのインターフェイス）を非アクティブにしてモジュールの電源を切断する例を示します。この例では、モジュールはルータのサブスロット0に装着されています。

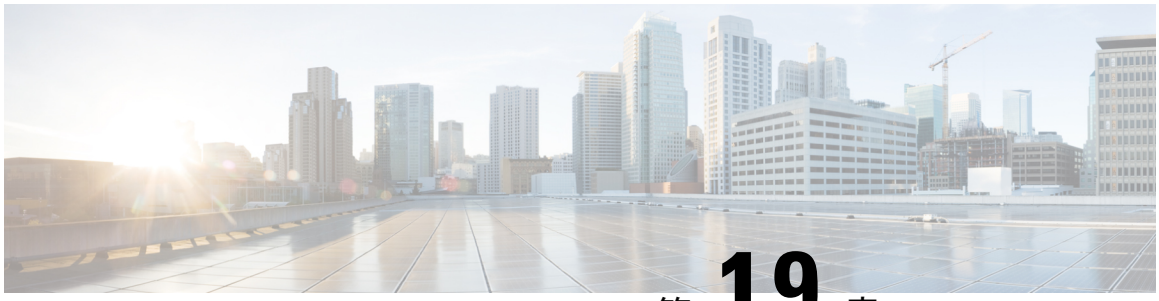
```
Router(config)# hw-module subslot 1/0 shutdown unpowered
```

モジュール設定のアクティブ化：例

以前にモジュールを非アクティブにした場合は、そのモジュールをアクティブ化できます。OIR実行中にモジュールとそのインターフェイスを非アクティブにしなかった場合は、ルータを再アクティブ化するとモジュールが自動的に再アクティブ化されます。

次に、モジュールをアクティブにする例を示します。この例では、ルータのスロット1にあるサブスロット0にモジュールが装着されています。

```
Router(config)# no hw-module subslot 1/0 shutdown unpowered
```



第 19 章

セルラー IPv6 アドレス

この章では、IPv6 アドレスの概要と、Cisco 8300 シリーズ セキュアルータでセルラー IPv6 アドレスを設定する方法について説明します。

この章は、次の項で構成されています。

セルラー IPv6 アドレス

IPv6 アドレスは、x:x:x:x:x:x:x:x のようにコロン（:）で区切られた一連の 16 ビットの 16 進フィールドで表されます。次に、IPv6 アドレスの例を 2 つ示します。

- 2001:CDBA:0000:0000:0000:0000:3257:9652
- 2001:CDBA::3257:9652（ゼロは省略可能）

IPv6 アドレスには通常、連続する 16 進数のゼロのフィールドが含まれています。IPv6 アドレスの先頭、中間、または末尾にある連続した 16 進数のゼロのフィールドを圧縮するために、2 つのコロン（::）が使用されることがあります（このコロンは連続した 16 進数のゼロのフィールドを表します）。次の表に、圧縮された IPv6 アドレスの形式を示します。

IPv6 アドレス プレフィックスは、ipv6-prefix/prefix-length の形式で、アドレス空間全体のビット連続ブロックを表すために使用できます。ipv6-prefix は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。プレフィックス長は、アドレスの高次の連続ビットのうち、何個がプレフィックス（アドレスのネットワーク部分）を構成しているかを指定する 10 進数値です。たとえば、2001:cdba::3257:9652 /64 は有効な IPv6 プレフィックスです。

IPv6 ユニキャスト ルーティング

IPv6 ユニキャスト アドレスは、単一ノード上の単一インターフェイスの識別子です。ユニキャスト アドレスに送信されたパケットは、そのアドレスが示すインターフェイスに配信されます。

Cisco 8300 シリーズ セキュアルータは、次のアドレス タイプをサポートしています。

リンクロックアドレス

リンクローカル アドレスは、リンクローカル プレフィックス FE80::/10（1111 1110 10）と変更された EUI-64 形式のインターフェイス識別子を使用するすべてのインターフェイスを自動的に設定できる IPv6 ユニキャスト アドレスです。IPv6 アドレスが有効になっている場合、リンクローカル アドレスはセルラーイ ンターフェイスで自動的に設定されます。

データ コールが確立されると、セルラー インターフェイスのリンクローカル アドレスは、ホストによって生成されたリンクローカル アドレス（リンクローカル プレフィックス FF80::/10 (1111 1110 10) と USB ハードウェア アドレスから自動生成されたインターフェイス識別子で構成）で更新されます。

グローバルアドレス

グローバル IPv6 ユニキャスト アドレスは、グローバル ルーティング プレフィックス、サブネット ID、およびインターフェイス ID で定義されます。ルーティング プレフィックスは PGW から取得されます。インターフェイス識別子は、修正された EUI-64 形式のインターフェイス識別子を使用して、USB ハードウェア アドレスから自動的に生成されます。ルータのリロード後に、USB ハードウェア アドレスが変更されます。

セルラー IPv6 アドレスの設定

セルラー IPv6 アドレスを設定するには、次の手順を実行します。

手順

ステップ 1 **configure terminal**

例：

```
Router# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **ipv6 unicast-routing**

例：

```
Router(config)# ipv6 unicast-routing
```

IPv6 ユニキャスト データ パケットの転送をイネーブルにします。

ステップ 3 **interface Cellular** {**type** | **number**}

例：

```
Router(config)# interface cellular 0/1/0
```

セルラー インターフェイスを指定します。

ステップ 4 ip address negotiated

例：

```
Router(config-if)# ip address negotiated
```

このインターフェイスの IP アドレスが動的に取得されるように設定します。

ステップ 5 load-interval***seonds***

例：

```
Router(config-if)# load-interval 30
```

（任意）負荷統計情報の計算に使用されるデータを取る時間の長さを指定します。

ステップ 6 dialer in-band

例：

```
Router(config-if)# dialer in-band
```

DDR をイネーブルにし、インバンド ダイヤリングを使用するよう、指定したシリアル インターフェイスを設定します。

ステップ 7 dialer idle-timeout ***seonds***

例：

```
Router(config-if)# dialer idle-timeout 0
```

ダイヤラのアイドル タイムアウト期間を指定します。

ステップ 8 dialer-group**group-number**

例：

```
Router(config-if)# dialer-group 1
```

指定したインターフェイスが属するダイヤラ アクセス グループの番号を指定します。

ステップ 9 no peer default ip address

例：

```
Router(config-if)# no peer default ip address
```

設定からデフォルトアドレスを削除します。

ステップ 10 ipv6 address autoconfig or ipv6 enable

例：

```
Router(config-if)# ipv6 address autoconfig
```

または

```
Router(config-if)# ipv6 enable
```

インターフェイスに対してステートレス自動設定を使用した IPv6 アドレスの自動設定をイネーブルにし、インターフェイスにおける IPv6 処理をイネーブルにします。

ステップ 11 **dialer-listdialer-groupprotocolprotocol-name** {**permit** |deny|**list** |*access-list-number* | *access-group* }

例：

```
Router(config)# dialer-list 1 protocol ipv6 permit
```

プロトコルによって、またはプロトコルと以前に定義したアクセス リストの組み合わせによって、ダイヤルするためのダイヤルオンデマンド ルーティング（DDR）ダイヤラ リストを定義します。

ステップ 12 **ipv6 route** *ipv6-prefix/prefix-length 128*

例：

```
Router(config)#ipv6 route 2001:1234:1234::3/128 Cellular0/1/0
```

ステップ 13 **End**

例：

```
Router(config-if)#end
```

グローバル コンフィギュレーション モードに戻ります。

例

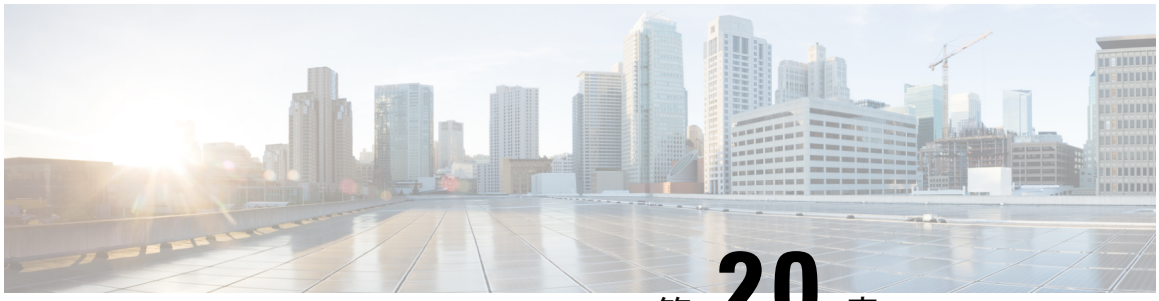
次の例は、NIM-LTEA-EA および NIM-LTEA-LA モジュールのセルラー IPv6 の設定を示しています。

```
Router(config)# interface Cellular0/1/0
ip address negotiated
load-interval 30
dialer in-band
dialer idle-timeout 0
lte dialer-group 1
no peer default ip address
ipv6 address autoconfig
!
interface Cellular0/1/1
ip address negotiated
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer-group 1
no peer default ip address
ipv6 address autoconfig
```

次の例は、P-LTEAP18-GL、P-LTEA-XX、P-LTE-XX モジュールのセルラー IPv6 の設定を示しています。

```
Router(config)# interface Cellular0/2/0
ip address negotiated
load-interval 30
dialer in-band
dialer idle-timeout 0
lte dialer-group 1
no peer default ip address
ipv6 enable
!
interface Cellular0/2/1
```

```
ip address negotiated
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer-group 1
no peer default ip address
ipv6 enable
```



第 20 章

無線対応ルーティング

無線対応ルーティング（RAR）は、無線がルーティングプロトコルOSPFv3と情報を交換し、1ホップルーティングネイバーのアピアランス、ディスアピアランス、およびリンク状態について信号で伝えるメカニズムです。

大規模なモバイルネットワークでは、ルーティングネイバーへの接続が距離と無線障害により中断されることがよくあります。該当する信号がルーティングプロトコルに到達しない場合、プロトコルタイマーを使用してネイバーのステータスが更新されます。ルーティングプロトコルには期間の長いタイマーがありますが、モバイルネットワークでは推奨されません。

無線対応ルーティングの利点

無線対応ルーティング機能には次のようなメリットがあります。

- 変更を即座に認識することで、ネットワーク コンバージェンスを高速化します。
- 障害の発生している、または減衰している無線リンクのルーティングを有効にします。
- ラインオブサイトパスと非ラインオブサイトパス間のルーティングを容易にします。
- 高速コンバージェンスと最適なルート選択が可能になるため、音声やビデオなど遅延の影響を受けやすいトラフィックが中断されません。
- 無線リソースと帯域幅の効率的な使用が可能になります。
- ルータで輻輳制御を実行することにより、無線リンクへの影響を軽減します。

- 無線電力の節減に基づくルート選択が可能になります。
- ルーティング機能と無線機能の分離を有効にします。
- RFC 5578、R2CP、および DLEP に準拠した無線へのシンプルなイーサネット接続を実現します。

制約事項と制限

無線対応ルーティング機能には次の制約事項と制限があります。

- DLEP および R2CP プロトコルは、Cisco 8300 シリーズ セキュアルータではサポートされていません。
- マルチキャストトラフィックは、集約モードではサポートされていません。
- 高可用性（HA）はサポートされていません。

ライセンス要件

この機能は、AppX ライセンスで使用できます。

システムコンポーネント

無線対応ルーティング（RAR）機能は、PPPoE、仮想マルチポイント インターフェイス（VMI）、QoS、ルーティング プロトコル インターフェイス、RAR プロトコルなどのさまざまなコンポーネントで構成される MANET（モバイル アドホック ネットワーク）インフラストラクチャを使用して導入されます。

Point-to-Point Protocol over Ethernet（PPPoE）

PPPoE は、クライアントとサーバーの間の明確に定義された通信メカニズムです。RAR の導入では、無線が PPPoE クライアントの役割を果たし、ルータが PPPoE サーバーの役割を果たします。その結果、明確に定義された予測可能な通信メカニズムを提供しながら、無線とルータを疎結合することが可能になります。

PPPoEはセッションまたは接続指向プロトコルであるため、外部無線からIOSルータへのポイントツーポイント無線周波数（RF）リンクを拡張します。

PPPoE 拡張

PPPoE 拡張は、ルータが無線と通信するときに使用されます。PPPoE の Cisco IOS 導入では、個々のセッションは仮想アクセスインターフェイス（無線ネイバーへの接続）で表され、これらの PPPoE 拡張を使用して QoS を適用できます。

RFC5578 は、信頼ベースのフロー制御とセッションベースのリアルタイム リンク メトリック をサポートするための PPPoE の拡張を実現します。この拡張は、可変帯域幅および制限付き バッファリング機能（無線リンクなど）を使用した接続に非常に役立ちます。

仮想マルチポイント インターフェイス（VMI）

PPPoE拡張によってルータと無線間で通信するためのセットアップの大部分が実現しますが、VMIは、上位レイヤ（ルーティングプロトコルなど）が消費するイベントを管理および変換する必要に対処します。また、VMI はバイパスモードで動作します。

バイパスモードでは、無線ネイバーを表すすべての仮想アクセスインターフェイス（VAI）がルーティングプロトコル OSPFv3 および EIGRP に明示されるため、ルーティングプロトコルは、ユニキャストとマルチキャスト両方のルーティング プロトコル トラフィックに関してそれぞれの VAI と直接通信します。

集約モードでは、VMI がルーティングプロトコル（OSPF）に明示されるため、ルーティングプロトコルは VMI を活用して効率を最適化できます。ネットワークネイバーが、VMI でのブロードキャストおよびマルチキャスト機能を備えたポイントツーマルチポイント リンク上のネットワークの集合と見なされる場合、VMIは、PPPoEから作成された複数の仮想アクセスインターフェイスの集約に役立ちます。VMIは、単一のマルチアクセスレイヤ2ブロードキャスト対応インターフェイスを提供します。VMI レイヤは、ユニキャスト ルーティング プロトコル トラフィックを適切な P2P リンク（仮想アクセスインターフェイス）にリダイレクトし、フローする必要があるすべてのマルチキャスト/ブロードキャストトラフィックを複製します。ルーティングプロトコルは単一のインターフェイスと通信するため、ネットワークの完全性に影響を与えることなく、トポロジデータベースのサイズが縮小されます。

PPPoE 拡張セッションでの QoS プロビジョニング

次の例では、PPPoE 拡張セッションでの QoS プロビジョニングについて説明します。

```
policy-map rar_policer
 class class-default
  police 10000 2000 1000 conform-action transmit  exceed-action drop  violate-action
drop
policy-map rar_shaper
 class class-default
  shape average percent 1

interface Virtual-Template2
 ip address 192.0.2.7 255.255.255.0
 no peer default ip address
 no keepalive
 service-policy input rar_policer
end
```

例：バイパスモードでの RAR 機能の設定

次に、バイパスモードにおける RAR のエンドツーエンド設定の例を示します。

（注） RAR を設定する前に、まず **subscriber authorization enable** コマンドを設定して RAR セッションを起動する必要があります。認証され有効になっていないと、ポイントツーポイントプロトコルはこれを RAR セッションとして認識せず、PPPoE Active Discovery Initiate（PADI）の提示の際に *manet_radio* をタグ付けしない場合があります。デフォルトでは、設定にバイパスモードが表示されません。モードがバイパスとして設定されている場合にのみ表示されます。

RAR のサービスの設定

```
policy-map type service rar-lab
 pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

ブロードバンドの設定

```
bba-group pppoe VMI2
 virtual-template 2
service profile rar-lab
!
interface GigabitEthernet0/0/0
 description Connected to Client1
  negotiation auto
  pppoe enable group VMI2
!
```

RAR のサービスの設定

```
policy-map type service rar-lab
 pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

バイパスモードの設定

- 仮想テンプレートで明示的に設定された IP アドレス

```
interface Virtual-Template2
ip address 192.0.2.7 255.255.255.0
no ip redirects
peer default ip address pool PPPoEpool2
ipv6 enable
ospfv3 1 network manet
ospfv3 1 ipv4 area 0
ospfv3 1 ipv6 area 0
no keepalive
service-policy input rar_policer Or/And
service-policy output rar_shaper
```

- 仮想テンプレートで設定された番号なしの VMI

```
interface Virtual-Template2
ip unnumbered vmi2
```

```
    no ip redirects
    peer default ip address pool PPPoEpool2
    ipv6 enable
    ospfv3 1 network manet
    ospfv3 1 ipv4 area 0
    ospfv3 1 ipv6 area 0
    no keepalive
    service-policy input rar_policer Or/And
    service-policy output rar_shaper
```

バイパスモードでの仮想マルチポイント インターフェイスの設定

```
interface vmi2 //configure the virtual multi interface
ip address 192.0.2.5 255.255.255.0
physical-interface GigabitEthernet0/0/0
mode bypass

interface vmi3//configure the virtual multi interface
 ip address 192.0.2.6 255.255.255.0
 physical-interface GigabitEthernet0/0/1
mode bypass
```

OSPF ルーティングの設定

```
router ospfv3 1
 router-id 192.0.2.1
!
 address-family ipv4 unicast
  redistribute connected metric 1 metric-type 1
  log-adjacency-changes
 exit-address-family
 !
 address-family ipv6 unicast
  redistribute connected metric-type 1
  log-adjacency-changes
 exit-address-family
!
ip local pool PPPoEpool2 192.0.2.8 192.0.2.4
```

例：集約モードでの RAR 機能の設定

次に、集約モードにおける RAR のエンドツーエンド設定の例を示します。

（注） RAR を設定する前に、まず **subscriber authorization enable** コマンドを設定して RAR セッションを起動する必要があります。許可を有効にしないと、ポイントツーポイント プロトコルはこれを RAR セッションとして認識せず、PADI で *manet_radio* がタグ付けされない場合があります。

RAR のサービスの設定

```
policy-map type service rar-lab
 pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

ブロードバンドの設定

```
bba-group pppoe VMI2
 virtual-template 2
service profile rar-lab

!
interface GigabitEthernet0/0/0
 description Connected to Client1
  negotiation auto
  pppoe enable group VMI2

!
```

RAR のサービスの設定

```
policy-map type service rar-lab
 pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

集約モードでの設定

```
interface Virtual-Template2
ip unnumbered vmi2
no ip redirects
no peer default ip address
ipv6 enable
no keepalive
service-policy input rar_policer Or/And
service-policy output rar_shaper
```

集約モードでの仮想マルチポイント インターフェイスの設定

```
interface vmi2 //configure the virtual multi interface
ip address 192.0.2.8 255.255.255.0
physical-interface GigabitEthernet0/0/0
mode aggregate

interface vmi3//configure the virtual multi interface
 ip address 192.0.2.4 255.255.255.0
 no ip redirects
 no ip split-horizon eigrp 1
 physical-interface GigabitEthernet0/0/1
mode aggregate
```

OSPF ルーティングの設定

```
router ospfv3 1
 router-id 192.0.2.1
!
 address-family ipv4 unicast
  redistribute connected metric 1 metric-type 1
  log-adjacency-changes
```

```
 exit-address-family
 !
 address-family ipv6 unicast
  redistribute connected metric-type 1
  log-adjacency-changes
 exit-address-family
!
ip local pool PPPoEpool2 192.0.2.4 192.0.2.8
ip local pool PPPoEpool3 192.0.2.6 192.0.2.2
```

RAR セッションの詳細の確認

RAR セッションの詳細を取得するには、次の show コマンドを使用します。

```
Router#show pppoe session packets all
Total PPPoE sessions 2

session id: 9
local MAC address: 006b.f10e.a5e0, remote MAC address: 0050.56bc.424a
virtual access interface: Vi2.1, outgoing interface: Gi0/0/0
    1646 packets sent, 2439363 received
    176216 bytes sent, 117250290 received

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 32928     PADG Timer index: 0
 PADG last rcvd Seq Num: 17313
 PADG last nonzero Seq Num: 17306
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 33308  rcvd: 17313
 PADC xmit: 17313  rcvd: 19709
 In-band credit pkt xmit: 7 rcvd: 2434422
 Last credit packet snapshot
  PADG xmit: seq_num = 32928, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 32928, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17313, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 17313, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 0


session id: 10
local MAC address: 006b.f10e.a5e1, remote MAC address: 0050.56bc.7dcb
virtual access interface: Vi2.2, outgoing interface: Gi0/0/1
    1389302 packets sent, 1852 received
    77869522 bytes sent, 142156 received

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 18787     PADG Timer index: 0
 PADG last rcvd Seq Num: 18784
 PADG last nonzero Seq Num: 18768
```

```
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 18787  rcvd: 18784
 PADC xmit: 18784  rcvd: 18787
 In-band credit pkt xmit: 1387764 rcvd: 956
 Last credit packet snapshot
  PADG xmit: seq_num = 18787, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 18787, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 18784, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 18784, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 0, bcn = 64222
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 1


Router#show pppoe session packets
Total PPPoE sessions 2

SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
9       2439391         1651            117252098       176714
10      1858            1389306         142580          77869914


Router#show vmi counters
Interface vmi2: - Last Clear Time =

Input Counts:
  Process Enqueue      =          0 (VMI)
  Fastswitch           =          0
  VMI Punt Drop:
       Queue Full      =          0

Output Counts:
  Transmit:
       VMI Process DQ  =       4280
       Fastswitch VA   =          0
       Fastswitch VMI  =          0
  Drops:
       Total           =          0
       QOS Error       =          0
       VMI State Error =          0
       Mcast NBR Error =          0
       Ucast NBR Error =          0
Interface vmi3: - Last Clear Time =

Input Counts:
  Process Enqueue      =          0 (VMI)
  Fastswitch           =          0
  VMI Punt Drop:
       Queue Full      =          0

Output Counts:
  Transmit:
       VMI Process DQ  =       2956
       Fastswitch VA   =          0
       Fastswitch VMI  =          0
  Drops:
       Total           =          0
       QOS Error       =          0
       VMI State Error =          0
       Mcast NBR Error =          0
       Ucast NBR Error =          0
Interface vmi4: - Last Clear Time =
```

```
Input Counts:
  Process Enqueue      =          0 (VMI)
  Fastswitch           =          0
  VMI Punt Drop:
       Queue Full      =          0

Output Counts:
  Transmit:
       VMI Process DQ  =          0
       Fastswitch VA   =          0
       Fastswitch VMI  =          0
  Drops:
       Total           =          0
       QOS Error       =          0
       VMI State Error =          0
       Mcast NBR Error =          0
       Ucast NBR Error =          0
Router#


Router#show vmi neighbor details
1 vmi2 Neighbors
      1 vmi3 Neighbors
      0 vmi4 Neighbors
      2 Total Neighbors

vmi2   IPV6 Address=FE80::21E:E6FF:FE43:F500
       IPV6 Global Addr=::
       IPV4 Address=192.0.2.6, Uptime=05:15:01
       Output pkts=89, Input pkts=0
       No Session Metrics have been received for this neighbor.
       Transport PPPoE, Session ID=9
       INTERFACE STATS:
          VMI Interface=vmi2,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          V-Access intf=Virtual-Access2.1,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          Physical intf=GigabitEthernet0/0/0,
             Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 33038     PADG Timer index: 0
 PADG last rcvd Seq Num: 17423
 PADG last nonzero Seq Num: 17420
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 33418  rcvd: 17423
 PADC xmit: 17423  rcvd: 19819
 In-band credit pkt xmit: 7 rcvd: 2434446
 Last credit packet snapshot
  PADG xmit: seq_num = 33038, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 33038, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17423, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 17423, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 0
```

```
vmi3   IPV6 Address=FE80::21E:7AFF:FE68:6100
       IPV6 Global Addr=::
       IPV4 Address=192.0.2.10, Uptime=05:14:55
       Output pkts=6, Input pkts=0
       METRIC DATA: Total rcvd=1, Avg arrival rate (ms)=0
          CURRENT: MDR=128000 bps, CDR=128000 bps
                   Lat=0 ms, Res=100, RLQ=100, load=0
          MDR      Max=128000 bps, Min=128000 bps, Avg=128000 bps
          CDR      Max=128000 bps, Min=128000 bps, Avg=128000 bps
          Latency  Max=0, Min=0, Avg=0 (ms)
          Resource Max=100%, Min=100%, Avg=100%
          RLQ      Max=100, Min=100, Avg=100
          Load     Max=0%, Min=0%, Avg=0%
       Transport PPPoE, Session ID=10
       INTERFACE STATS:
          VMI Interface=vmi3,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          V-Access intf=Virtual-Access2.2,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          Physical intf=GigabitEthernet0/0/1,
             Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 18896     PADG Timer index: 0
 PADG last rcvd Seq Num: 18894
 PADG last nonzero Seq Num: 18884
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 18896  rcvd: 18894
 PADC xmit: 18894  rcvd: 18896
 In-band credit pkt xmit: 1387764 rcvd: 961
 Last credit packet snapshot
  PADG xmit: seq_num = 18896, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 18896, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 18894, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 18894, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 0, bcn = 64222
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 1


Router#show vmi neighbor details vmi 2
              1 vmi2 Neighbors

vmi2   IPV6 Address=FE80::21E:E6FF:FE43:F500
       IPV6 Global Addr=::
       IPV4 Address=192.0.2.4, Uptime=05:16:03
       Output pkts=89, Input pkts=0
       No Session Metrics have been received for this neighbor.
       Transport PPPoE, Session ID=9
       INTERFACE STATS:
          VMI Interface=vmi2,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          V-Access intf=Virtual-Access2.1,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          Physical intf=GigabitEthernet0/0/0,
             Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
```

```
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 33100     PADG Timer index: 0
 PADG last rcvd Seq Num: 17485
 PADG last nonzero Seq Num: 17449
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 33480  rcvd: 17485
 PADC xmit: 17485  rcvd: 19881
 In-band credit pkt xmit: 7 rcvd: 2434460
 Last credit packet snapshot
  PADG xmit: seq_num = 33100, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 33100, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17485, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 17485, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 0


Router#show platform hardware qfp active feature ess session
Current number sessions: 2
Current number TC flow: 0
Feature Type: A=Accounting D=Policing(DRL) F=FFR M=DSCP Marking L=L4redirect P=Portbundle
 T=TC

   Session    Type      Segment1      SegType1      Segment2      SegType2 Feature Other
-------------------------------------------------------------------------------------

        21     PPP 0x0000001500001022    PPPOE 0x0000001500002023    LTERM -------
        24     PPP 0x0000001800003026    PPPOE 0x0000001800004027    LTERM -------


Router#show platform software subscriber pppoe_fctl evsi 21
PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 33215     PADG Timer index: 0
 PADG last rcvd Seq Num: 17600
 PADG last nonzero Seq Num: 17554
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 33595  rcvd: 17600
 PADC xmit: 17600  rcvd: 19996
 In-band credit pkt xmit: 7 rcvd: 2434485
 Last credit packet snapshot
  PADG xmit: seq_num = 33215, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 33215, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17600, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 17600, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534

BQS buffer statistics
 Current packets in BQS buffer: 0
 Total en-queue packets: 0 de-queue packets: 0
 Total dropped packets: 0

Internal flags: 0x0
```

```
Router#show platform hardware qfp active feature ess session id 21
Session ID: 21

  EVSI type: PPP
  SIP Segment ID: 0x1500001022
  SIP Segment type: PPPOE
  FSP Segment ID: 0x1500002023
  FSP Segment type: LTERM
  QFP if handle: 16
  QFP interface name: EVSI21
  SIP TX Seq num: 0
  SIP RX Seq num: 0
  FSP TX Seq num: 0
  FSP RX Seq num: 0
  Condition Debug: 0x00000000
    session
```

```
Router#show ospfv3 neighbor

          OSPFv3 1 address-family ipv4 (router-id 192.0.2.3)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
192.0.2.1           0   FULL/  -        00:01:32    19              Virtual-Access2.1

          OSPFv3 1 address-family ipv6 (router-id 192.0.2.3)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
192.0.2.1           0   FULL/  -        00:01:52    19              Virtual-Access2.1
Router#
```

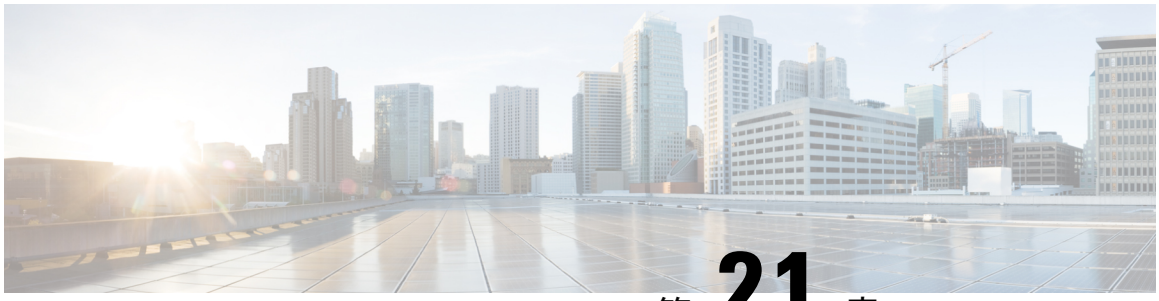
```
Router#sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      192.0.2.8/8 is variably subnetted, 3 subnets, 2 masks
C        192.0.2.5/24 is directly connected, Virtual-Access2.1
O        192.0.2.6/32 [110/1] via 192.0.2.22, 00:00:03, Virtual-Access2.1
L        192.0.2.7/32 is directly connected, Virtual-Access2.1
      192.0.2.12/32 is subnetted, 1 subnets
C        192.0.2.20 is directly connected, Virtual-Access2.1
```

無線対応ルーティングのトラブルシューティング

RAR をトラブルシューティングするには、次の debug コマンドを使用します。

- **debug pppoe errors**

- **debug pppoe events**
- **debug ppp error**
- **debug vmi error**
- **debug vmi neighbor**
- **debug vmi packet**
- **debug vmi pppoe**
- **debug vmi registries**
- **debug vmi multicast**
- **debug vtemplate cloning**
- **debug vtemplate event**
- **debug vtemplate error**
- **debug plat hard qfp ac feature subscriber datapath pppoe detail**



第 21 章

ソフトウェア メディア ターミネーション ポイントのサポート

ソフトウェア メディア ターミネーション ポイント（MTP）のサポート機能は、2 つの接続間のメディアストリームをブリッジして、Cisco Unified Communications Manager（CUCM）が SIP または H.323 エンドポイントを介してルーティングされたコールを Skinny Client Control Protocol（SCCP）コマンドでリレーできるようにします。これらのコマンドにより、CUCM はコールシグナリング用の MTP を確立できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/に進みます。Cisco.com のアカウントは必要ありません。

ソフトウェア メディア ターミネーション ポイントのサポートに関する情報

この機能は、ソフトウェア MTP サポートを Cisco Unified Border Element（Enterprise）に拡張します。ソフトウェア MTP は、Cisco UCM の大規模展開に不可欠なコンポーネントです。この機能により、新しい機能が有効になり、Cisco UBE が SIP トランキングに移行する大規模な展開でエンタープライズエッジのシスコ セッション ボーダー コントローラとして機能できるようになります。

ソフトウェア メディア ターミネーション ポイントの前提条件

- ソフトウェア MTP が適切に機能するには、着信コールレッグと発信コールレッグの両方に同じ方法でコーデックとパケット化を設定する必要があります。

ソフトウェア メディア ターミネーション ポイントの制約事項

- RSVP エージェントはソフトウェア MTP ではサポートされていません。
- 再パケット化のためのソフトウェア MTP はサポートされていません。
- コールしきい値は、スタンドアロンのソフトウェア MTP ではサポートされていません。
- コールごとのデバッグはサポートされていません。
- 同じ宛先 IP とポートを持つ複数の同時同期ソース（SSRC）はサポートされていません。

SRTP-DTMF インターワーキング

Cisco IOS XE 17.10.1a 以降、Secure Real-time Transport Protocol（SRTP）デュアルトーン多重周波数（DTMF）インターワーキングは、パススルーモードのソフトウェア MTP でサポートされています。SMTP は非セキュアコールの DTMF インターワーキングをサポートします。また、この機能はさらにセキュアコールの SRTP DTMF インターワーキングをサポートします。

この機能の CUCM サポートは、今後のリリースで実装される予定です。

SRTP-DTMF インターワーキングの制約事項

- SRTP-DTMF インターワーキング機能は、コーデックパススルー形式のみをサポートします。
- SRTP-DTMF インターワーキング機能は、同じ宛先 IP とポートを持つ複数の同時同期ソース（SSRC）をサポートしていません。

- SRTP-DTMF インターワーキングをサポートするコールは、非セキュア DTMF インターワーキングでサポートされるコールと比較すると、パフォーマンスにわずかな影響を与える可能性があります。

サポートされる SRTP-DTMF インターワーキングのプラットフォーム

Cisco IOS XE 17.10.1a 以降、次のプラットフォームは SMTP との SRTP DTMF インターワーキングをサポートしています。

- Cisco 4461 サービス統合型ルータ（ISR）
- Cisco Catalyst 8200 Edge シリーズ プラットフォーム
- Cisco Catalyst 8300 Edge シリーズ プラットフォーム
- Cisco 8300 シリーズ セキュアルータ
- Cisco Catalyst 8000V Edge ソフトウェア

ソフトウェア メディア ターミネーション ポイントのサポートの設定

ソフトウェア メディア ターミネーション ポイントのサポート機能を有効にして設定するには、次のタスクを実行します。

手順

ステップ 1 **enable**

例：

```
Router> enable
```

特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。

ステップ 2 **configure terminal**

例：

```
Router# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **sccp local** *interface-type interface-number* [**port** *port-number*]

例：

```
Router(config)# sccp local gigabitethernet0/0/0
```

Cisco UCM に登録するために SCCP アプリケーション（トランスコーディングと会議）が使用する、ローカルインターフェイスを選択します。

- *interface type*：インターフェイスアドレスまたは仮想インターフェイスアドレス（イーサネットなど）を指定できます。
- *interface number*：Cisco UCM に登録するために SCCP アプリケーションが使用するインターフェイス番号。
- （任意）**port** *port-number*：選択したインターフェイスで使用するポート番号。範囲は 1025 ～ 65535 です。デフォルトでは 2000 です。

ステップ 4 **sccp ccm** {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* [**port** *port-number*] **version** *version-number*

例：

```
Router(config)# sccp ccm 10.1.1.1 identifier 1 version 7.0+
```

使用可能なサーバーのリストに Cisco UCM サーバーを追加し、次のパラメーターを設定します。

- *ipv4-address*：Cisco UCM サーバーの IP バージョン 4 アドレス。
- *ipv6-address*：Cisco UCM サーバーの IP バージョン 6 アドレス。
- *dns*：DNS 名。
- **identifier**：Cisco UCM サーバーを識別する番号を指定します。有効値の範囲は 1 ～ 65535 です。
- **port** *port-number*（任意）：TCP ポート番号を指定します。範囲は 1025 ～ 65535 です。デフォルトでは 2000 です。
- **version** *version-number*：Cisco UCM のバージョン。有効なバージョンは、3.0、3.1、3.2、3.3、4.0、4.1、5.0.1、6.0、および 7.0+ です。デフォルト値はありません。

ステップ 5 **sccp**

例：

```
Router(config)# sccp
```

Skinny Client Control Protocol （SCCP）とそれに関連するアプリケーション（トランスコーディングと会議）を有効にします。

ステップ 6 **sccp ccm group** *group-number*

例：

```
Router(config)# sccp ccm group 10
```

Cisco UCM グループを作成して、SCCP Cisco UCM コンフィギュレーション モードを開始します。

- *group-number*：Cisco UCM グループを識別します。範囲は 1 ～ 50 です。

ステップ 7 **associate ccm** *identifier-number* **priority** *number*

例：

```
Router(config-sccp-ccm)# associate ccm 10 priority 3
```

Cisco UCM を Cisco UCM グループに関連付けて、グループ内の優先順位を設定します。

- *identifier-number*：Cisco UCM を識別します。有効値の範囲は 1 ～ 65535 です。デフォルト値はありません。
- **priority** *number*：Cisco UCM グループ内の Cisco UCM の優先順位。範囲は 1 ～ 4 です。デフォルト値はありません。最も高い優先順位は 1 です。

ステップ 8 **associate profile** *profile-identifier* **register** *device-name*

例：

```
Router(config-sccp-ccm)# associate profile 1 register MTP0011
```

DSP ファームプロファイルを Cisco UCM グループに関連付けます。

- *profile-identifier*：DSP ファームプロファイルを識別します。有効値の範囲は 1 ～ 65535 です。デフォルト値はありません。
- **register** *device-name*：Cisco UCM 内のデバイス名。デバイス名は最大 15 文字まで入力できます。

ステップ 9 **dspfarm profile** *profile-identifier* {**conference** | **mtp** | **transcode**} [**security**]

例：

```
Router(config-sccp-ccm)# dspfarm profile 1 mtp
```

DSP ファーム プロファイル コンフィギュレーション モードを開始し、DSP ファームサービス用のプロファイルを定義します。

- *profile-identifier*：プロファイルを一意に識別する番号。有効値の範囲は 1 ～ 65535 です。デフォルトはありません。
- **conference**：会議用のプロファイルを有効にします。
- **mtp**：MTP 用のプロファイルを有効にします。
- **transcode**：トランスコーディング用のプロファイルを有効にします。
- **security**（任意）：セキュア DSP ファームサービス用のプロファイルを有効にします。設定例の詳細については、#unique_285 unique_285_Connect_42_GUID-5FB6A48E-204C-45AA-AE63-413B075A7871（338 ページ）の項を参照してください。

ステップ 10 **trustpoint** *trustpoint-label*

例：

```
Router(config-dspfarm-profile)# trustpoint dspfarm
```

（任意）トラストポイントを DSP ファーム プロファイルに関連付けます。

ステップ 11 **codec** *codec*

例：

```
Router(config-dspfarm-profile)# codec g711ulaw
```

DSP ファーム プロファイルでサポートされるコーデックを指定します。

- codec-type：優先されるコーデックを指定します。サポートされるコーデックのリストを表示するには、? を入力します。

  サポートされるコーデックごとに、この手順を繰り返します。

ステップ 12 **maximum sessions** {**hardware** | **software**} *number*

例：

```
Router(config-dspfarm-profile)# maximum sessions software 10
```

このプロファイルでサポートされる最大セッション数を指定します。

- **hardware**：MTP ハードウェアリソースがサポートできるセッションの数。
- **software**：MTP ソフトウェアリソースがサポートできるセッションの数。
- *number*：プロファイルでサポートされるセッションの数。範囲は 0 ～ x です。デフォルトは 0 です。x の値は、リソースプロバイダーで使用可能なリソースの数に応じて、実行時に決定されます。

ステップ 13 **associate application sccp**

例：

```
Router(config-dspfarm-profile)# associate application sccp
```

SCCP を DSP ファーム プロファイルに関連付けます。

ステップ 14 **no shutdown**

例：

```
Router(config-dspfarm-profile)# no shutdown
```

インターフェイスのステータスを UP 状態に変更します。

例：ソフトウェア メディア ターミネーション ポイントのサポート

次に、ソフトウェア メディア ターミネーション ポイントのサポート機能の設定例を示します。

```
sccp local GigabitEthernet0/0/1
sccp ccm 10.13.40.148 identifier 1 version 6.0
sccp
!
sccp ccm group 1
 bind interface GigabitEthernet0/0/1
```

```
 associate ccm 1 priority 1
 associate profile 6 register RR_RLS6
!
 dspfarm profile 6 mtp
 codec g711ulaw
 maximum sessions software 100
 associate application SCCP
!
!
gateway
media-inactivity-criteria all
timer receive-rtp 400
```

次に、セキュアな dspfarm プロファイルを使用した SRTP-DTMF インターワーキング機能の設定例を示します。

```
sccp local GigabitEthernet0/0/0
sccp ccm 172.18.151.125 identifier 1 version 7.0
sccp
!
sccp ccm group 1
 bind interface GigabitEthernet0/0/0
 associate ccm 1 priority 1
 associate profile 1 register Router
!
dspfarm profile 1 mtp security
 trustpoint IOSCA
 codec g711ulaw
 codec pass-through
 tls-version v1.2
 maximum sessions software 5000
 associate application SCCP
```

（注） dspfarm プロファイルがコーデックパススルーでプロビジョニングされていて、TLS およびセキュリティ関連の設定がない場合、SR-TP トラフィックは SMTP リソースを通過できます。SRTP-DTMF インターワーキングのサポートを必要とするトラフィックフローの場合は、SMTP dspfarm プロファイルには **security** キーワードと TLS およびコーデックパススルー設定を含める必要があります。この dspfarm リソースプロファイルは、SRTP-DTMF インターワーキングサポートに関係なく、SRTP トラフィックを通過させることもできます。

ソフトウェア メディア ターミネーション ポイントの設定の確認

この機能を確認し、トラブルシューティングを行うには、次の **show** コマンドを使用します。

- SCCP に関する情報を確認するには、**show sccp** コマンドを使用します。

```
Router# show sccp

SCCP Admin State: UP
Gateway IP Address: 10.13.40.157, Port Number: 2000
IP Precedence: 5
```

```
User Masked Codec list: None
Call Manager: 10.13.40.148, Port Number: 2000
                Priority: N/A, Version: 6.0, Identifier: 1
                Trustpoint: N/A
```

- DSPfarm プロファイルに関する情報を確認するには、**show dspfarm profile** コマンドを使用します。

```
Router# show dspfarm profile 6

Dspfarm Profile Configuration
 Profile ID = 6, Service = MTP, Resource ID = 1
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : NONE   Status : NONE
 Number of Resource Configured : 100
 Number of Resource Available : 100
 Hardware Configured Resources : 0
 Hardware Available Resources : 0
 Software Resources : 100
 Codec Configuration
 Codec : g711ulaw, Maximum Packetization Period : 30
```

- セキュア DSPfarm プロファイルのステータスに関する情報を確認するには、**show dspfarm profile** コマンドを使用して、セキュアサービスモードが設定されていることを確認します。

```
Router# show dspfarm profile 2
Dspfarm Profile Configuration
 Profile ID = 2, Service = MTP, Resource ID = 2
 Profile Service Mode : secure
 Trustpoint : IOSCA
 TLS Version  : v1.2
 TLS Cipher   : AES128-SHA
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : NONE   Status : NONE
 Total Number of Resources Configured : 8000
 Total Number of Resources Available : 8000
 Total Number of Resources Out of Service : 0
 Total Number of Resources Active : 0
 Hardware Configured Resources : 0
 Hardware Resources Out of Service: 0
 Software Configured Resources : 8000
 Number of Hardware Resources Active : 0
 Number of Software Resources Active : 0
 Codec Configuration: num_of_codecs:2
 Codec : pass-through, Maximum Packetization Period : 0
 Codec : g711ulaw, Maximum Packetization Period : 30
```

- SCCP 接続の統計を表示するには、**show sccp connections** コマンドを使用します。

```
Router# show sccp connections

sess_id   conn_id    stype  mode       codec    ripaddr        rport   sport
```

```
16808048  16789079    mtp   sendrecv   g711u    10.13.40.20    17510   7242
16808048  16789078    mtp   sendrecv   g711u    10.13.40.157   6900    18050
```

SMTP セキュア DTMF の場合、**show sccp connections** コマンドはコーデックタイプ（pass-th）、S タイプ（s-mtp）、および DTMF メソッド（rfc2833_pthru）に関する情報を表示します。

```
Router# show sccp connections

sess_id   conn_id   stype   mode      codec    sport  rport   ripaddr conn_id_tx
dtmf_method
16791234  16777308  s-mtp   sendrecv  pass_th  8006   24610   172.18.153.37
rfc2833_pthru
16791234  16777306  s-mtp   sendrecv  pass_th  8004   17576   172.18.154.2
rfc2833_report

Total number of active session(s) 1, and connection(s) 2
```

- RTP 接続に関する情報を表示するには、**show rtpspi call** コマンドを使用します。

```
Router# show rtpspi call
RTP Service Provider info:
No. CallId  dstCallId   Mode      LocalRTP  RmtRTP  LocalIP     RemoteIP    SRTP
1    22      19         Snd-Rcv   7242      17510   0x90D080F   0x90D0814    0
2    19      22         Snd-Rcv   18050     6900    0x90D080F   0x90D080F    0
```

SRTP DTMF インターワーキングがアクティブになっている場合、SRTP フィールドにはゼロ以外の値が表示されます。

```
Router# show rtpspi call
RTP Service Provider info:
No. CallId  dstCallId   Mode      LocalRTP  RmtRTP  LocalIP     RemoteIP    SRTP
1   13      14          Snd-Rcv   8024      18270   0xA7A5355   0xAC129A02   1
2   14      13          Snd-Rcv   8026      24768   0xA7A5355   0xAC129925   1
```

- VoIP RTP 接続に関する情報を表示するには、 **show voip rtp connections** コマンドを使用します。

```
Router# show voip rtp connections
VoIP RTP Port Usage Information
Max Ports Available: 30000, Ports Reserved: 100, Ports in Use: 102
Port range not configured, Min: 5500, Max: 65499
VoIP RTP active connections :
No. CallId    dstCallId  LocalRTP  RmtRTP    LocalIP         RemoteIP
1     114       117        19822    24556   10.13.40.157     10.13.40.157
2     115       116        24556    19822   10.13.40.157     10.13.40.157
3     116       115        19176    52625   10.13.40.157     10.13.40.20
4     117       114        16526    52624   10.13.40.157     10.13.40.20
```

- 具体的には、次のような **show** コマンドを使用できます。
  - **show sccp connection callid**
  - **show sccp connection connid**
  - **show sccp connection sessionid**
  - **show rtpspi call callid**
  - **show rtpspi stat callid**
  - **show voip rtp connection callid**

- **show voip rtp connection type**
- **show platform hardware qfp active feature sbc global**

- 特定の問題を切り分けるには、**debug sccp** コマンドを使用します。
  - **debug sccp** [**all** | **config** | **errors** | **events** | **keepalive** | **messages** | **packets** | **parser** | **tls**]

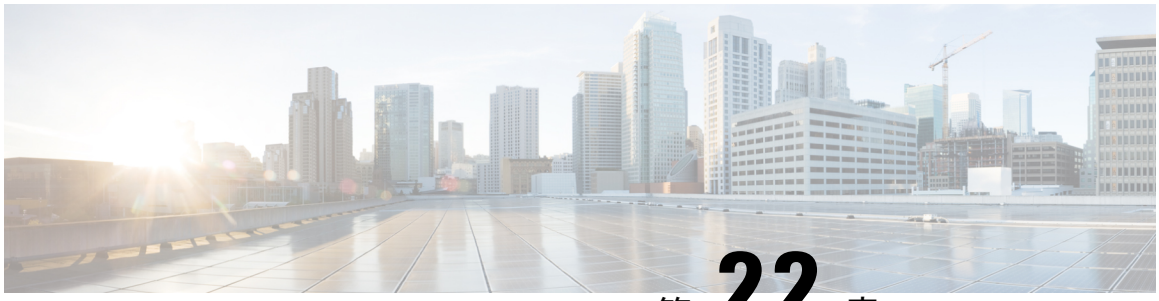
ソフトウェア メディア ターミネーション ポイントのサポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェアリリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *28* : ソフトウェア メディア ターミネーション ポイントのサポートに関する機能情報

機能名	リリース	機能情報
ソフトウェア メディア ターミネーション ポイントのサポート	Cisco IOS XE リリース 2.6 S	ソフトウェア メディア ターミネーション ポイント（MTP）は、Cisco Unified Communications Manager（Cisco UCM）が Skinny Client Control Protocol（SCCP）コマンドを介して音声ゲートウェイと対話する機能を提供します。これらのコマンドにより、Cisco UCM はコールシグナリング用の MTP を確立できます。
Secure Real-time Transport Protocol（SRTP）デュアルトーン多重周波数（DTMF）インターワーキングのサポート	Cisco IOS XE Dublin 17.10.1a	Secure Real-time Transport Protocol（SRTP）デュアルトーン多重周波数（DTMF）機能は、パススルーモードのみでの Secure Software MTP と CUCM との間の DTMF インターワーキングをサポートします。



第 22 章

イーサネット OAM を使用した Dying Gasp

Dying Gasp は、最後の通知であり、電源が切れそうになったときにデバイスによって送信される信号です。デバイスはピアデバイスにアラート信号を送信し、ピアデバイスは電源関連の問題を特定して対処します。

イーサネットの運用、管理、保守（OAM）は、イーサネットネットワークを監視および管理する一連のプロトコルです。イーサネット OAM が有効になっているインターフェイスの場合、デバイスはイーサネット OAM プロトコルを使用して Dying Gasp メッセージを送信します。ローカルデバイスに電源障害があることをリモートピアデバイスに通知する、イーサネット OAM Dying Gasp パケットの生成をサポートしています。

このタイプの状況はベンダー固有です。状況に関するイーサネット運用、管理、保守（OAM）通知がただちに送信される場合があります。

Dying Gasp サポートの前提条件

- イーサネット OAM は、L3 インターフェイスでデフォルトで有効になっています。

  Dying Gasp 機能は、以下のコマンドを使用して無効化できます。

  ```
  Router(config-if)#ethernet oam mode passive
  ```

  次の CLI コマンドを使用して再度有効にできます。

  ```
  Router (config-if)#ethernet oam mode active
  ```

- イーサネット OAM は、電力損失がある場合にのみ送信されます。

Dying Gasp サポートの制約事項

- Power Failure Dying Gasp 機能は、C8355-G2 ルータでのみサポートされています。

イーサネット OAM を使用した Dying Gasp

- C8355-G2 ルータの Power Failure Dying Gasp は、イーサネット OAM パケットの送信のみをサポートしています。

イーサネット OAM を使用した Dying Gasp

IEEE 802.3ah で定義されている OAM 機能の 1 つにリモート障害表示があります。これは、品質の低下が原因で発生するイーサネット接続の障害の検出に役立ちます。イーサネットの運用、管理、保守（OAM）プロトコルは、障害状態を示すためにOAMプロトコルデータユニット（PDU）の特定のフラグを送信します。この機能はベンダー固有であり、C8355-G2 ルータでサポートされています。状態に関する通知は、デバイスの電源が切れそうになっていることを示すために、即座に継続的に送信される可能性があります。

OAMPDU の設定

C8355-G2 ルータの Dying Gasp 機能を使用すると、OAMPDU フレームで **Code** フィールド値を設定できます。設定できる値は次のとおりです。

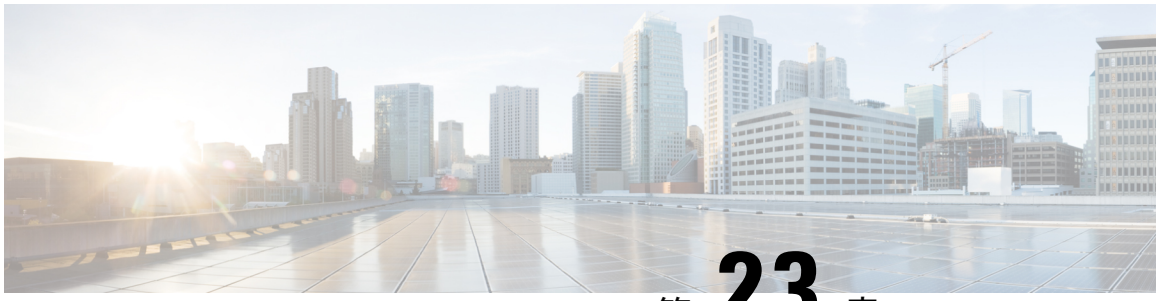
- **Information**：OAM パッケージがローカルまたはリモートの情報データを転送していることを示します。0x00 は情報 OAMPDU を表します。
- **Organization specific**：これがベンダー専用であることを示します。各ベンダーは、このコードを使用して、カスタマイズされたデータを伝送できます。0xFE は、組織固有の OAMPDU を表しており、OAMPDU のデフォルトタイプ設定です。

情報 OAMPDU の設定

```
Router# enable
 Router# configure terminal
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ethernet oam dying-gasp type information
Router(config-if)# exit
Router(config)# exit
Router#show ethernet oam status interface GigabitEthernet0/0/0
GigabitEthernet0/0/0
General
-------
  Admin state:           enabled
  Mode:                  passive
  Type:                  information
  PDU max rate:          10 packets per second
  PDU min rate:          1 packet per 1000 ms
… …
```

組織固有の OAMPDU の設定

```
Router# enable
 Router# configure terminal
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ethernet oam dying-gasp type organization
Router (config-if)# exit
Router(config)# exit
Router# show ethernet oam status interface GigabitEthernet0/0/0
GigabitEthernet0/0/0
General
-------
  Admin state:           enabled
  Mode:                  passive
  Type:                  organization
  PDU max rate:          10 packets per second
  PDU min rate:          1 packet per 1000 ms
```



第 23 章

仮想 DSP

仮想 DSP

仮想 DSP リソースは、次のようなソフトウェアベースの DSP ソリューションです。

- トランスコーディング、会議、およびハードウェア メディア ターミネーション ポイント サービスなどの音声処理機能を提供
- 専用 DSP チップではなく、ルータの CPU リソースを使用して動作
- ハードウェアに依存しない音声サービスの展開が可能

利点

- 仮想 DSP では、物理 DSP ハードウェアモジュールの必要がなくなり、物理 DSP スロットのないルータに展開できます。
- 仮想 DSP キャパシティは、CPU の可用性とコール量に基づいて調整できます。

機能制限

- 17.18.2 では、vDSP は自律モードでのみサポートされています。
- マルチアプリケーションのサポートはありません。vDSP は、UTD、TE、または同じボックス上の他の vDSP などの別のコンテナアプリケーションと共存できません。

サポートされる vDSP プロファイル

次の表に、Cisco 8200 シリーズ セキュアルータおよび Cisco 8300 シリーズ セキュアルータでサポートされる vDSP プロファイルに関する詳細を示します。

表 *29*：サポートされる *vDSP* プロファイル

vDSP プロファイル	C8231-G2 C8235-G2	C8231-E-G2 C8235-E-G2	C8355-G2	C8375-E-G2
vDSP-32	あり	あり	あり	あり
vDSP-64	あり	あり	あり	あり
vDSP-256	あり	あり	あり	あり
vDSP-512			あり	あり
vDSP-1024			あり	あり
vDSP-2048			あり	あり

ルータでサポートされている vDSP プロファイルを表示するには、**show voice dsp capabilities** コマンドを使用します。

次の例は、C8375-E-G2 の vDSP 機能を示しています。

```
Device#show voice dsp capabilities
Supported vDSP profiles are:
vDSP-32     (Max credits 3360)
vDSP-64     (Max credits 6720)
vDSP-256    (Max credits 26880)
vDSP-512    (Max credits 53760)
vDSP-1024   (Max credits 107520)
vDSP-2048   (Max credits 215040)

Current active vDSP profile is vDSP-2048

Credit Information:

Transcode Credit:
LC (G711) Credits: 105
MC (G722/G729a) Credits: 240
HC (iLBC/G729) Credits: 420
VHC (iSAC/Opus) Credits: 420
```

```
Universal Transcode Credit:
LC (G711) Credits: 105
MC (G722/G729a) Credits: 336
HC (iLBC/G729) Credits: 672
VHC (iSAC/Opus) Credits: 840

Conference 8-party credits:
LC (G711) Credits: 420
MC (G722) Credits: 672
HC (G729/G729a) Credits: 1120
VHC (iLBC) Credits: 1120
```

各機能の最大クレジットは、トランスコーディングや会議など、サポートされている IP-IP サービスの処理能力です。

vDSP コンテナのダウンロード

vDSP コンテナソフトウェアは、Cisco Software Centralでホストされています。

（注） 各 IOS XE バージョンには、最適なパフォーマンスを確保するために対応する推奨 vDSP バージョンがあります。vDSP パッケージ名には、vDSP バージョンと、互換性のある IOS XE バージョンの両方を指定します。

vDSP ファイル名が `vDSP package name: vDSP_2.1.0_17.18.2.aarch64.tar` の場合

vDSP バージョン	2.1.0 メジャーバージョン：2 マイナーバージョン：1 正式リリース 0
IOS-XE バージョン	17.18.2

IOS XE バージョンに一致する vDSP パッケージをダウンロードし、ルータのブートフラッシュにインストールします。tftp、scp、ftp、http などのサポートされている方法を使用して、vDSP イメージをルータのフラッシュにコピーします。

```
copy tftp://IPaddress/vDSP.tar flash:
```

Cisco IOx の有効化

次のコマンドを使用して IOx サービスを有効にします。

```
Device#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#iox
```

VirtualPortGroup の設定

このタスクでは、VirtualPortGroup を設定する手順の概要を説明します。

手順

ステップ 1 VirtualPortGroup インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。<number> の有効範囲は 0 ～ 31 です。

例：

```
Device(config)#interface VirtualPortGroup0
 Device(config)#description vDSP
 Device(config)#ip address 192.168.253.250 255.255.255.252
```

（注）
ここで設定する `ip address` は、ローカルネットワーク内でのみ使用されるプライベート IP アドレスであり、パブリックインターネット上や、ローカルデバイスまたはネットワークセグメントの外部から到達可能またはルーティング可能にすることを目的としていません。

ステップ 2 VPG 0 に IP アドレスが指定されていることを確認し、ステータスが稼働中であることを確認します。

例：

```
Device#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
Tw0/0/0                172.19.155.52   YES NVRAM  up                    up
Tw0/0/1                3.3.3.52        YES NVRAM  up                    up
Tw0/0/2                4.4.4.52        YES NVRAM  up                    up
Tw0/0/3                2.2.2.52        YES NVRAM  up                    up
Te0/0/4                192.168.10.52   YES NVRAM  down                  down
Te0/0/5                unassigned      YES NVRAM  administratively down down
GigabitEthernet0       unassigned      YES NVRAM  up                    up
VirtualPortGroup0      192.168.253.250 YES NVRAM  up                    up
```

vDSP アプリケーションの設定

このタスクは、デバイス上で vDSP アプリケーションを設定する手順を示します。

手順

ステップ 1 このコマンドを使用して、グローバル コンフィギュレーション モードを開始し、コンフィギュレーション コマンドを 1 行に 1 つずつ入力します。コンフィギュレーション コマンドの入力が終了したら、Ctrl+Z を押します。

例：

```
Device# configure terminal
```

ステップ 2 このコマンドを使用してアプリケーションを設定し、アプリケーション コンフィギュレーション モードを開始します。

例：

```
Device(config)# app-hosting appid vdsp
```

`appid` 名は、ユーザーが任意の文字列を使用して定義できます。ただし、vdsp が推奨されます。

ステップ 3 app-vnic コマンドを使用して、アプリケーション インターフェイスとアプリケーションのゲートウェイを設定します。

例：

```
Device(config-app-hosting)# app-vnic gateway0 virtualportgroup 0 guest-interface 0
```

virtualportgroup の値は、以前に設定した値と一致する必要があります。また、guest-interface の値は 0 にすることもできます。

ステップ 4 guest-ipaddress コマンドを使用して、アプリケーション イーサネット インターフェイスの IP アドレスを設定します。

例：

```
Device(config-app-hosting-gateway0)# guest-ipaddress 192.168.253.249 netmask 255.255.255.255
```

ステップ 5 app-default-gateway コマンドを使用して、アプリケーションのデフォルトゲートウェイを設定します。

例：

```
Device(config-app-hosting-gateway0)# app-default-gateway 192.168.253.250 guest-interface 0
```

app-default-gateway IP は、VPG IP と同じである必要があります。また、guest-interface の値は virtualportgroup の値と一致する必要があります。

ステップ 6 デバイスのプロファイルサイズを割り当てます。このプロファイルサイズによって、デバイス上のアプリケーション ホスティングに割り当てられるリソース数が決まります。**show voice dsp capabilities** コマンドを使用して、サポートされる vDSP プロファイルを表示するか、「サポートされる vDSP プロファイル」を参照してください。

ステップ 7 このコマンドを入力してグローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例：

```
Device# end
```

vDSP コンテナのインストール

このタスクでは、vDSP コンテナをインストールするために実行する手順の概要を説明します。

手順

ステップ 1 vDSP コンテナアプリケーションをインストールします。

例：

```
app-hosting install appid vdsp package flash: vDSP_2.1.0_17.18.02eftr1.aarch64.tar
```

（注）
app-hosting 設定で定義された `appid` を使用します。

ステップ 2 vDSP アプリケーションを手動でアクティブ化して起動します。

例：

```
app-hosting activate appid vdsp
app-hosting start appid vdsp
```

`app-hosting appid vdsp` で `start` が設定されている場合、vdsp アプリケーションが自動的にアクティブ化されて起動します。

ステップ 3 すべての DSP グループを確認します。

例：

```
Device#show voice dsp group

DSP groups on vdsp
DSP recommended version: 2.1.0

dsp 1:
  State: UP, firmware version: 2.1.0
  Max voice channel: 256
  Max credits: 26880.  Transcoding channels allocated: 0
  Group: FLEX_GROUP_VOICE, complexity: FLEX
    Shared credits: 26880, reserved credits: 0
    Voice channels allocated: 0
    Credits used (rounded-up): 0
```

ステップ 4 dspfarm プロファイルを設定して、トランスコーディング リソースまたは会議リソースを予約し、通話を開始します。dspfarm プロファイルの設定方法の詳細については、「Configuring Conferencing and Transcoding for Voice Gateway Routers」を参照してください。

vDSP のアンインストール

vDSP 設定をアンインストールするには、次のコマンドを使用します。

```
app-hosting stop appid vdsp
app-hosting deactivate appid vdsp
app-hosting uninstall appid vdsp
```

vDSP のアップグレードまたはダウングレード

vDSP バージョンをアップグレードまたはダウングレードするには、vDSP をアンインストールし、IOS イメージを変更してから、一致する vDSP を再度インストールすることを推奨します。

`app-hosting upgrade appid vdsp package bootflash:new-vDSP-image.tar` コマンドは、vDSP を自動で停止、非アクティブ化、アップグレード、アクティブ化、および再起動します。

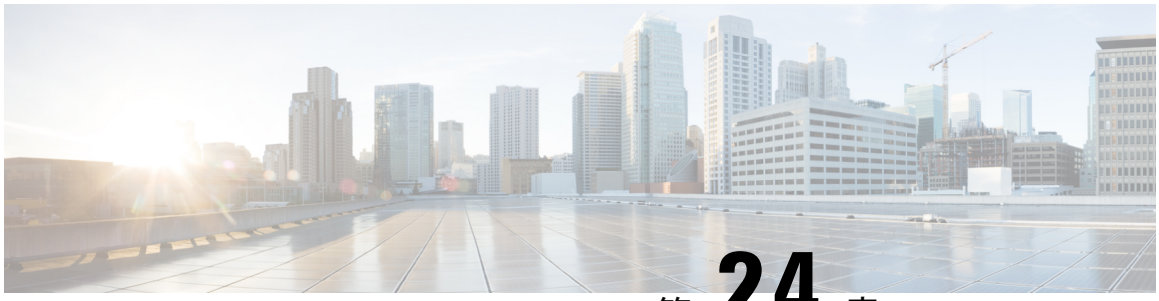
vDSP を手動でアップグレードするには、次のコマンドを使用します。

```
app-hosting stop appid vdsp
app-hosting deactivate appid vdsp
app-hosting upgrade appid vdsp package bootflash:new-vDSP-image.tar
app-hosting activate appid vdsp
app-hosting start appid vdsp
```

検証コマンド

リストされているコマンドを使用して、vDSP のインストールまたは設定を確認します。

コマンド	説明
show app-hosting list	デバイスでホストされているアプリケーションに関する情報を表示します。アプリケーション ID と、RUNNING や ACTIVATED などの現在の状態が一覧表示されます。
show app-hosting detail appid vdsp	デバイスでホストされている、アプリケーション ID が「vdsp」であるアプリケーションに関する詳細情報を表示します。
show app-hosting utilization appid vdsp	デバイスでホストされている、アプリケーション ID が「vdsp」であるアプリケーションのリソース使用率情報を表示します。
show voice dsp group	デバイス上の音声リソースに関連する DSP グループについての情報を表示します。
show voice dsp capabilities	デバイス上の特定の DSP の機能を表示します。



第 24 章

トラブルシューティング

トラブルシューティング

システムレポートを使用したトラブルシューティング

システムレポート

システムレポートまたはcrashinfoファイルには、シスコのテクニカルサポート担当者が、Cisco IOSイメージのクラッシュを引き起こした問題をデバッグするときに使用する情報が保存されています。重大なクラッシュに関する情報の迅速かつ確実な収集とバンドルが、特定のクラッシュ事案によって情報が識別されるような方法で行われることが必要です。システムレポートが生成され、harddisk:またはflash:ファイルシステムの「/core」ディレクトリに保存されます。リロード時はレポートは生成されません。

システムクラッシュの場合、次の詳細情報が収集されます。

1. □□□□□□□□ core
2. IOSd □□□□□□□□□□□□□□□□□□□□ IOSd □□□□□□□□□□ IOS crashinfo □□□□
3. □□□□□□□
4. □□□□□□□□□□□□
5. □□□□□□□□□
6. □□□□□□□□ /proc □□

このレポートは、ルータがROMMON/ブートローダーに対してダウン状態になる前に生成されます。この情報は、個別のファイルに格納されてから、アーカイブされてtar.gzバンドルに圧縮されます。このバンドルにより、クラッシュスナップショットを1ヵ所で取得できるようになります。ファイルは、分析のためにボックスから移動することもできます。

デバイスのホスト名、システムレポートを生成したモジュールの ID、およびその作成タイムスタンプがファイル名に組み込まれます。

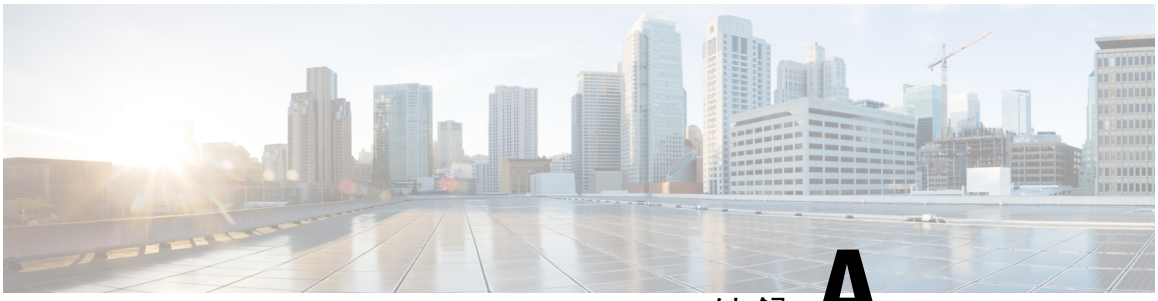
```
<hostname>_<moduleID>-system-report_<timestamp>.tar.gz
```

システムレポートの例

ファイル名が `Router1_RP_0-system-report_20210204-163559-UTC` のサンプルレポートを参照してください。

ここでは、ホスト名が Router1 のデバイスで、RP0 モジュールの予期しないリロードが発生し、2021 年 2 月 4 日午後 4 時 39 分 59 秒（UTC）にシステムレポートが生成されました。

```
├── bootflash/
│   └── pd_info/
│       ├── dmesg_output-20210204-163538-UTC.log
│       ├── filesystems-20210204-163538-UTC.log
│       ├── memaudit-20210204-163538-UTC.log
│       ├── proc_cpuinfo-20210204-163538-UTC.log
│       ├── proc_diskstats-20210204-163538-UTC.log
│       ├── proc_interrupts-20210204-163538-UTC.log
│       ├── proc_oom_stats-20210204-163538-UTC.log
│       ├── proc_softirqs-20210204-163538-UTC.log
│       ├── system_report_trigger.log
│       └── top_output-20210204-163538-UTC.log
├── harddisk/
│   ├── core/
│   │   └── Router1_RP_0_hman_17716_20210212-123836-UTC.core.gz
│   └── tracelogs/
├── tmp/
│   ├── fp/
│   │   └── trace/
│   ├── maroon_stats/
│   ├── rp/
│   │   └── trace/
│   └── Router1_RP_0-bootuplog-20210204-163559-UTC.log
└── var/
    └── log/
        └── audit/
            └── audit.log
```



付録 A

サポートされていないコマンド

Cisco 8300 シリーズ セキュアルータには、**logging** または **platform** キーワードを指定する一連のコマンドがあり、これらを入力しても出力が生成されないか、またはお客様にとって不要な出力が表示されます。お客様にとって不要なこのようなコマンドは、サポート対象外のコマンドと見なされます。サポート対象外のコマンドに関するシスコ製品マニュアルは今後公開されない予定です。

Cisco 8300 シリーズ セキュアルータのサポート対象外のコマンドのリストを以下に示します。

- backplaneswitchport
- clear logging onboard slot f0 dram
- clear logging onboard slot f0 voltage
- clear logging onboard slot f0 temperature
- show logging onboard slot f0 dram
- show logging onboard slot f0 serdes
- show logging onboard slot f0 status
- show logging onboard slot f0 temperature
- show logging onboard slot f0 uptime
- show logging onboard slot f0 uptime latest
- show logging onboard slot f0 voltage
- show logging onboard slot 0 dram
- show logging onboard slot 0 serdes
- show logging onboard slot 0 status
- show logging onboard slot 0 temperature
- show logging onboard slot 0 uptime
- show logging onboard slot 0 uptime latest
- show logging onboard slot 0 voltage

サポートされていないコマンド

- show platform software adjacency r0 special
- show platform software adjacency rp active special
- show platform hardware backplaneswitch-manager RP active summary
- show platform hardware backplaneswitch-manager RP active subslot GEO statistics
- show platform software backplaneswitch-manager RP [active [detail]]
- show platform hardware backplaneswitch-manager [R0 [status] | RP]
- show platform hardware backplaneswitch-manager RPactive CP statistics
- platform hardware backplaneswitch-manager rp active subslot GEO statistics
- show platform software ethernet rp active l2cp
- show platform software ethernet rp active l2cp interface GigabitEthernet0
- show platform software ethernet rp active loopback
- show platform software ethernet rp active vfi
- show platform software ethernet r0 vfi
- show platform software ethernet r0 vfi id 0
- show platform software ethernet r0 vfi name GigabitEthernet0
- show platform software ethernet r0 l2cp
- show platform software ethernet r0 l2cp interface GigabitEthernet0
- show platform software ethernet r0 bridge-domain statistics
- show platform software flow r0 exporter name GigabitEthernet0
- show platform software flow r0 exporter statistics
- show platform software flow r0 global
- show platform software flow r0 flow-def
- show platform software flow r0 interface
- show platform software flow r0 ios
- show platform software flow r0 monitor
- show platform software flow r0 sampler
- show platform hardware qfp active classification feature-manager label GigabitEthernet 0 0
- show platform software interface f0 del-track
- show platform software interface fp active del-track
- show platform software rg r0 services
- show platform software rg r0 services rg-id 0
- show platform software rg r0 services rg-id 0 verbose

- show platform software rg r0 services verbose
- show platform software rg r0 statistics
- show platform software rg rp active services
- show platform software rg rp active services rg-id 0
- show platform software rg rp active services rg-id 0 verbose
- show platform software rg rp active statistics
- show platform hardware slot 0 dram statistics
- show platform hardware slot f0 dram statistics
- show platform hardware slot 0 eobc interface primary rmon
- show platform hardware slot 0 eobc interface primary status
- show platform hardware slot 0 eobc interface standby rmon
- show platform hardware slot 0 eobc interface standby status
- show platform hardware slot f0 eobc interface primary rmon
- show platform hardware slot f0 eobc interface primary status
- show platform hardware slot f0 eobc interface standby rmon
- show platform hardware slot f0 eobc interface standby status
- show platform hardware slot f0 sensor consumer
- show platform hardware slot f0 sensor producer

サポートされていないコマンド

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。