



## ルータの基本的な CLI 設定

この章は、次の項で構成されています。

- [IR1101 インターフェイスの命名 \(1 ページ\)](#)
- [基本設定 \(2 ページ\)](#)
- [グローバルパラメータの設定 \(6 ページ\)](#)
- [ギガビットイーサネット インターフェイスの設定 \(6 ページ\)](#)
- [GigabitEthernet0/0/0 でのサブインターフェイスのサポート \(8 ページ\)](#)
- [ループバック インターフェイスの設定 \(8 ページ\)](#)
- [Cisco Discovery Protocol の有効化 \(9 ページ\)](#)
- [コマンドラインアクセスの設定 \(10 ページ\)](#)
- [スタティック ルートの設定 \(11 ページ\)](#)
- [ダイナミック ルートの設定 \(13 ページ\)](#)
- [シリアル インターフェイスの設定 \(15 ページ\)](#)

### IR1101 インターフェイスの命名

サポートされているハードウェア インターフェイスとその命名規則は、次の表に記載されています。

ハードウェア インターフェイス	命名ルール
ギガビットイーサネット コンボ ポート	gigabitethernet 0/0/0
ファストイーサネット ポート	fastethernet0/0/1-0/0/4
セルラー インターフェイス	cellular 0/1/0 and cellular 0/1/1
非同期シリアル インターフェイス	async 0/2/0
USB	usbflash0:
mSATA	msata
IR1101 ベースユニットアラーム入力	alarm contact 0

さまざまな拡張モジュールのインターフェイス名は、次の章にあります。

- [IRM-1100-4A2T 拡張モジュール](#)
- [IRM-1101 拡張モジュール](#)

## 基本設定

基本設定は、初期設定ダイアログ中に作成したエントリの結果です。つまり、ルータには、WebUIを介して、またはPnPプロセスを動作させるために、IPアドレスが到達可能なインターフェイスが少なくとも1つ設定されていることを意味します。初期設定を表示するには、次の例に示すように、**show running-config** コマンドを使用します。

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

Current configuration : 8079 bytes
!
! Last configuration change at 17:33:19 GMT Tue Jun 25 2019
!
version 16.12
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname IR1101
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
clock timezone GMT 0 0
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
  no destination transport-method email
!
!
ip name-server 171.70.168.183 198.224.173.135 8.8.8.8
no ip domain lookup
ip domain name cisco.com
!
login on-success log
ipv6 unicast-routing
!
chat-script lte "" "AT!CALL" TIMEOUT 20 "OK"
chat-script hspa-R7 "" "AT!SCACT=1,1" TIMEOUT 60 "OK"
!
crypto pki trustpoint SLA-TrustPoint
  enrollment pkcs12
```

```

revocation-check crl
!
crypto pki trustpoint TP-self-signed-756885843
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-756885843
revocation-check none
rsakeypair TP-self-signed-756885843
!
!
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
 30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
 2310E30 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 6ADFOF0D 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
crypto pki certificate chain TP-self-signed-756885843
certificate self-signed 01
 3082032E 30820216 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
 30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 37353638 38353834 33301E17 0D313930 35333130 30303530
 385A170D 33303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
 532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3735 36383835
 38343330 82012230 0D06092A 864886F7 0D010101 05000382 010F0030 82010A02
 82010100 D2F61742 3B651909 95856431 9BC2CCB7 D4B04861 DD6E0924 4C3E6A51
 8BF2ABD9 5C3A597D 2EE0112C ECA615AA D0297F9E 071B6B5D 9B831332 021E61F4
 2352EEC9 EE70742E 46EFBAFC A03744D8 A22E4DA3 AAF919CC 0A7929A7 3BDB3B17
 C04DA5B9 028DD3EC 992493A6 EA864ED6 354CB3F4 094D3EBF 5307CAA3 192B5759
 E458712D 841A43CD 709D4D9E 72A9DE3E F935A688 59B6F278 65B59EE0 6B72469E
 7B97582A 64E511A6 D81735FF 117CE399 4C2A2973 F5FD407D BCEB62A6 FD7C6B08
 82E0749 ACE5BD44 32634790 3607ADEA 9F319343 4CA76B0D B1DE6A1C AD144548
 E38119E2 8B34F7AC 090C0450 03166B42 8C7C9EA7 5132687F E1F7BF6E B065CD4E
 889F02BB 02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F
 0603551D 23041830 16801405 77954127 36509205 7025CF4E 84B5D4A2 A3D53730
 1D060355 1D0E0416 04140577 95412736 50920570 25CF4E84 B5D4A2A3 D537300D
 06092A86 4886F70D 01010505 00038201 01004147 49C6A0A9 56F5BD4D 4892AEE0
 22955E06 AF192FA6 868D5556 959ACF05 398F3907 DFE3148B 0E2CFC12 20BEEA05
 DC23E8D7 A47DB4AE D6CB6665 BCAA7F39 24D010F0 DB8F0E70 5E7C3F73 25AB1783
 1346D540 47BB7E89 2BB1BE4D 16990318 A4612CC5 C7CC9376 7DF1A1F4 C09C0051
 4D950D99 3CC0C65B 0A98859A 3B81E324 BAB34EDF 64CA8C38 184DC796 47DDD9DD
 F71F8D5E D3B7A962 3D0FDE44 012AC034 DOE7F75A DB1BF12A CF23E2F5 6A4FDA14
 A588DCDA 8272CE33 36ABC57A BFF52980 5FFC7C34 4D4307BB AC0C0F18 AA783B9D

```

```
27C61E89 0EC1C6AA 6AB3F73B EF8450FD 782DFC63 038F6A27 456CA32B D3FEDB97
C8064523 EBB93FF5 8B98B546 44F853E9 0E04
quit
!
license udi pid IR1101-K9 sn FCW222700KS
diagnostic bootup level minimal
!
spanning-tree extend system-id
memory free low-watermark processor 50357
file prompt quiet
!
!
username cisco privilege 15 password 0 cisco
username lab password 0 lab123
!
redundancy
!
!
controller Cellular 0/1/0
 no lte firmware auto-sim
 lte modem link-recovery disable
!
controller Cellular 0/3/0
!
vlan internal allocation policy ascending
!
!
interface GigabitEthernet0/0/0
 no ip address
 shutdown
!
interface FastEthernet0/0/1
 switchport access vlan 192
 switchport mode access
!
interface FastEthernet0/0/2
 switchport access vlan 172
 switchport mode access
!
interface FastEthernet0/0/3
 switchport access vlan 172
!
interface FastEthernet0/0/4
 switchport mode access
!
interface GigabitEthernet0/0/5
!
interface Cellular0/1/0
 ip address negotiated
 load-interval 30
 dialer in-band
 dialer idle-timeout 0
 dialer watch-group 1
 ipv6 enable
 pulse-time 1
 ip virtual-reassembly
!
interface Cellular0/1/1
 no ip address
 shutdown
!
interface Cellular0/3/0
 ip address negotiated
 dialer in-band
```

```
dialer idle-timeout 0
dialer watch-group 2
ipv6 enable
pulse-time 1
ip virtual-reassembly
!
interface Cellular0/3/1
no ip address
shutdown
!
interface Vlan1
ip address 192.168.10.15 255.255.255.0
!
interface Vlan172
ip address 172.27.167.121 255.255.255.128
!
interface Vlan175
ip address 175.1.1.1 255.255.255.0
!
interface Async0/2/0
no ip address
encapsulation scada
!
ip default-gateway 172.27.167.1
ip forward-protocol nd
!
ip http server
ip http authentication local
ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.27.167.1
ip route 0.0.0.0 0.0.0.0 Cellular0/1/0
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 253
ip route 8.8.4.0 255.255.255.0 Cellular0/3/0
ip route 171.70.0.0 255.255.0.0 172.27.167.1
ip route 192.1.1.0 255.255.255.0 Cellular0/1/0
ip route 192.168.193.0 255.255.255.0 192.168.10.1
!
!
ip access-list standard 1
 10 permit any
dialer watch-list 1 ip 5.6.7.8 255.255.255.255
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
dialer watch-list 2 ip 5.6.7.8 255.255.255.255
dialer watch-list 2 delay route-check initial 60
dialer watch-list 2 delay connect 1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit
ipv6 route ::/0 Cellular0/1/0
!
!
snmp-server community public RO
snmp-server community private RW
snmp-server host 171.70.127.43 version 2c public
snmp-server host 172.27.167.220 version 2c public
snmp-server manager
!
control-plane
!
line con 0
exec-timeout 0 0
stopbits 1
speed 115200
line 0/0/0
```

```

line 0/2/0
line vty 0 4
  exec-timeout 0 0
  password cisco
  login
  transport input none
!
!
end

IR1101#

```

## グローバルパラメータの設定

ルータ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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 :  Router> <b>enable</b> Router# <b>configure terminal</b> 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、ルータとリモートターミナルを接続します。  <pre>telnet router-name or address Login: login-id Password: ***** Router&gt; enable</pre>
ステップ 2	<b>hostname name</b> 例 :  Router(config)# <b>hostname Router</b>	ルータ名を指定します。
ステップ 3	<b>enable password password</b> 例 :  Router(config)# <b>enable password crlny5ho</b>	ルータへの不正なアクセスを防止するには、パスワードを指定します。  (注) この形式のコマンドでは、パスワードは暗号化されません。パスワードを暗号化するには、前述のデバイス強化ガイドに記載されているように、イネーブルシークレットパスワードを使用します。

## ギガビットイーサネットインターフェイスの設定

IR1101 上のギガビットイーサネットインターフェイス (GI0/0/0) のデフォルト設定は、レイヤ 3 (L3) です。そのインターフェイスを、レイヤ 2 (L2) インターフェイスとして設定すること

が可能です。IR1101 のギガビットイーサネットインターフェイスはコンボポートであり、これは RJ45+SFP コネクタであることを意味します。

IRM-1100-SPMI 拡張モジュールには SFP ポートも搭載されています。IRM-1100-SPMI のギガビットイーサネットインターフェイス (GIO/0/5) は、レイヤ 2 (L2) のみです。つまり、このポートを任意の VLAN (switchport acc vlan #) に割り当てて SVI インターフェイスを使用できます。このポート直下に IP アドレスを割り当てることはできません。

正しいコネクタを選択する必要があります。次の場所にある『Cisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide』[英語]を参照してください。

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

	コマンドまたはアクション	目的
ステップ 1	<b>interface GigabitEthernet slot/bay/port</b> 例：  Router(config)# <b>interface GigabitEthernet 0/0/0</b>	ルータ上で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	<b>ip address ip-address mask</b> 例：  Router(config-if)# <b>ip address 192.168.12.2 255.255.255.0</b>	指定した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	<b>ipv6 address ipv6-address/prefix</b> 例：  Router(config-if)# <b>ipv6 address 2001.db8::ffff:1/128</b>	指定した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。IPv6 ユニキャストルーティングも設定する必要があります。詳細については、 <a href="https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-16-10/ip6b-xe-16-10-book/read-me-first.html">https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-16-10/ip6b-xe-16-10-book/read-me-first.html</a> にある『IPv6 Addressing and Basic Connectivity Configuration Guide』を参照してください。
ステップ 4	<b>ipv6 unicast-routing</b> 例：  Router (config)# <b>ipv6 unicast-routing</b>	IPv6 ユニキャストデータパケットの転送を有効にします。
ステップ 5	<b>no shutdown</b> 例：  Router(config-if)# <b>no shutdown</b>	インターフェイスを無効にします。状態が管理ダウンから管理アップに変化します。

	コマンドまたはアクション	目的
ステップ 6	<b>exit</b> 例：  Router(config-if)# <b>exit</b>	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、グローバルコンフィギュレーションモードに戻ります。

## GigabitEthernet0/0/0 でのサブインターフェイスのサポート

Cisco IOS-XE リリース 16.11.1 以降では、g0/0/0 インターフェイスのサブインターフェイスと dot1q 設定がサポートされています。次に例を示します。

```
Router(config)#interface g0/0/0 ?
<1-4294967295> GigabitEthernet interface number
Router(config-subif)#encapsulation ?
dot1q                IEEE 802.1Q Virtual LAN
```

## 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

	コマンドまたはアクション	目的
ステップ 1	<b>interface type number</b> 例：  Router(config)# <b>interface Loopback 0</b>	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) <b>ip address ip-address mask</b> 例：  Router(config-if)# <b>ip address 10.108.1.1 255.255.255.0</b>	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 <b>ipv6 address ipv6-address/prefix</b> コマンドを使用します。
ステップ 3	(オプション 2) <b>ipv6 address ipv6-address/prefix</b> 例：  Router(config-if)# <b>ipv6 address 2001:db8::ffff:1/128</b>	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。

	コマンドまたはアクション	目的
ステップ 4	<b>exit</b> 例 : Router(config-if)# <b>exit</b>	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

**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 192.0.2.0/16
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  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 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
    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 192.0.2.0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.0, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

## 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。セキュリティ上の理由から、必要に応じて無効にすることができます。

CDP の使用法の詳細については、『[Cisco Discovery Protocol Configuration Guide, Cisco IOS XE Release 3S](#)』を参照してください。

# コマンドラインアクセスの設定

ルータ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。



(注) トランスポート入力は、このガイドの Telnet と SSH のセクションで先に説明されているとおりに設定する必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>line</b> [aux   console   tty   vty] <i>line-number</i> 例 : Router(config)# <b>line console 0</b>	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	<b>password</b> <i>password</i> 例 : Router(config-line)# <b>password 5dr4Hepw3</b>	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	<b>login</b> 例 : Router(config-line)# <b>login</b>	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	<b>exec-timeout</b> <i>minutes</i> [ <i>seconds</i> ] 例 : Router(config-line)# <b>exec-timeout 5 30</b> Router(config-line)#	ユーザ入力が検出されるまで EXEC コマンドインタ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。「00」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	<b>exit</b> 例 : Router(config-line)# <b>exit</b>	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	<b>line</b> [aux   console   tty   vty] <i>line-number</i> 例 :	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。

	コマンドまたはアクション	目的
	Router(config)# <b>line vty 0 4</b> Router(config-line)#	
ステップ 7	<b>password password</b>  例：  Router(config-line)# <b>password aldf2ad1</b>	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	<b>login</b>  例：  Router(config-line)# <b>login</b>	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	<b>end</b>  例：  Router(config-line)# <b>end</b>	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。デフォルトは **transport input none** ですが、SSH が有効になっている場合は SSH に設定する必要がある点に注意してください。

**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。これらは、ルータ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

	コマンドまたはアクション	目的
ステップ 1	(オプション 1) <b>ip route</b> <i>prefix mask {ip-address   interface-type interface-number [ip-address]}</i> 例 : <pre>Router(config)# ip route 192.10.2.3 255.255.0.0 10.10.10.2</pre>	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 <b>ipv6 address</b> コマンドを使用してください)。
ステップ 2	(オプション 2) <b>ipv6 route</b> <i>prefix/mask {ipv6-address   interface-type interface-number [ipv6-address]}</i> 例 : <pre>Router(config)# ipv6 route 2001:db8:2::/64 2001:db8:3::0</pre>	IP パケットのスタティック ルートを指定します。IPv6 の詳細については、次を参照してください。 <a href="https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xr-16-10/ipv6b-xe-16-10-book/read-me-first.html">https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xr-16-10/ipv6b-xe-16-10-book/read-me-first.html</a>
ステップ 3	<b>end</b> 例 : <pre>Router(config)# end</pre>	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。

次の設定例は、宛先 IP アドレスが 192.168.1.0、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 の他の装置に対して、ギガビット インターフェイス上からスタティック ルートで送信します。具体的には、パケットが設定済みの PVC 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 2001:db8:2::/64 2001:db8:3::0
```

### 設定の確認

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: 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
S*     0.0.0.0/0 is directly connected, FastEthernet0
    
```

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ルータにも反映されます。

すべての Cisco IOS-XE コンフィギュレーション ガイドを次から入手できます：

<https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/series.html#Configuration>

## 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

	コマンドまたはアクション	目的
ステップ 1	<b>router rip</b>  例：  Router(config)# <b>router rip</b>	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。

	コマンドまたはアクション	目的
ステップ 2	<b>version</b> {1   2} 例： Router(config-router)# <b>version 2</b>	RIP version 1 または 2 の使用を指定します。
ステップ 3	<b>network</b> <i>ip-address</i> 例： Router(config-router)# <b>network 192.168.1.1</b> Router(config-router)# <b>network 10.10.7.1</b>	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	<b>no auto-summary</b> 例： Router(config-router)# <b>no auto-summary</b>	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	<b>end</b> 例： Router(config-router)# <b>end</b>	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

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       3.0.0.0/8 [120/1] via 2.2.2.1, 00:00:02, Ethernet0/0/0
```

## Enhanced Interior Gateway Routing Protocol の設定

Enhanced Interior Gateway Routing Protocol (EIGRP) は、シスコによって開発された Interior Gateway Routing Protocol (IGRP) の拡張バージョンです。EIGRP のコンバージェンス プロパティおよび作業効率は、IGRP よりも大幅に改善され、IGRP は使用されなくなりました。

EIGRP のコンバージェンス テクノロジーは、Diffusing Update Algorithm (DUAL) と呼ばれるアルゴリズムに基づいています。このアルゴリズムは、ルート計算中のどの時点でもループが発生しないようにし、トポロジ変更に関与するすべてのデバイスを同期できるようにします。トポロジ変更の影響を受けないデバイスは、再計算に含まれません。

Enhanced Interior Gateway Routing Protocol (eigrp) の設定の詳細については、次のガイドを参照してください。 <https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/ip-routing/b-ip-routing.html>

## シリアルインターフェイスの設定

このセクションでは、シリアルインターフェイス管理の設定について説明します。

IR1101 は、SCADA、raw ソケット、またはリバース Telnet に使用される非同期シリアルインターフェイス プロトコルをサポートしています。単一のシリアルインターフェイスと専用の非同期 0/2/0 を装備しています。シリアルインターフェイスは DTE のみです。



(注) 非同期シリアル ケーブルの説明については、次の場所にある IR1101 HW 設置ガイドを参照してください。 <https://www.cisco.com/c/en/us/td/docs/routers/access/1101/hardware/installation/guide/1101hwinst.html>

## 非同期インターフェイスの指定

非同期シリアル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで次のいずれかのコマンドを使用します。

コマンドまたはアクション	目的
Router (config) # interface async 0/2/0	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。

## 非同期シリアル カプセル化の指定

非同期シリアル インターフェイスは、次のシリアル カプセル化方式をサポートします。

- Raw-TCP
- Raw-UDP
- SCADA
- カプセル化リレー

コマンドまたはアクション	目的
Router(config-if)# encapsulation {raw-tcp   raw-udp   scada}	非同期シリアル カプセル化を設定します。

カプセル化の方式は、Cisco IOS ソフトウェアで設定するプロトコルまたはアプリケーションのタイプに応じて設定されます。

その他のカプセル化方式は、プロトコルまたはアプリケーションについて説明するそれぞれの文書および章で定義されています。

## シリアルポートの設定

シリアルポートを設定するには、次の手順を実行します。

```
IR1101#sh run int async 0/2/0
Building configuration...
Current configuration : 62 bytes
!
interface Async0/2/0
no ip address
encapsulation raw-tcp
end
IR1101#show line
  Tty Line Typ   Tx/Rx    A Modem  Roty AccO AccI  Uses  Noise Overruns  Int
*   0    0 CTY       - -      - - -    0     0    0/0    -
  0/2/0 50 TTY      9600/9600 - -      - - -    0     0    0/0    -
      74   74 VTY       - -      - - -    3     0    0/0    -
      75   75 VTY       - -      - - -    0     0    0/0    -
      76   76 VTY       - -      - - -    0     0    0/0    -
      77   77 VTY       - -      - - -    0     0    0/0    -
      78   78 VTY       - -      - - -    0     0    0/0    -
```

回線が非同期モードではない、または、ハードウェア サポートがない：

1-49、51-73、79-726

## 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。