



# Basic Router Configuration

This chapter contains the following sections:

- [IR8140H Interface Naming, on page 1](#)
- [Basic Configuration, on page 2](#)
- [Configuring Global Parameters, on page 8](#)
- [Configuring the Gigabit Ethernet Interface, on page 9](#)
- [Support for sub-interface on GigabitEthernet0/0/0, on page 10](#)
- [Configuring a Loopback Interface, on page 10](#)
- [Enabling Cisco Discovery Protocol, on page 11](#)
- [Configuring Command-Line Access, on page 12](#)
- [Configuring Static Routes, on page 13](#)
- [Configuring Dynamic Routes, on page 15](#)
- [Modular QoS \(MQC\), on page 16](#)

## IR8140H Interface Naming

The supported hardware interfaces and their naming conventions are in the following table:

Hardware Interface	Naming Convention
Gigabit Ethernet ports	GigabitEthernet0/0/0 GigabitEthernet0/0/1
Cellular Interface	Cellular0/2/0 Cellular0/2/1 Cellular0/3/0 Cellular0/3/1
mSATA SSD	msata
GPIO	alarm contact 1-2
WPAN	Wpan0/1/0

# Basic Configuration

The basic configuration is a result of the entries you made during the initial configuration dialog. This means the router has at least one interface set with an IP address to be reachable, either through WebUI or to allow the PnP process to work. Use the **show running-config** command to view the initial configuration, as shown in the following example:

```
IR8140H# show running-config
Building configuration...

Current configuration : 16150 bytes
!
! Last configuration change at 19:21:02 UTC Thu Nov 19 2020
!
version 17.5
service timestamps debug datetime msec
service timestamps log datetime msec
service internal
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
!
hostname IR8140H
!
boot-start-marker
boot system bootflash:/ir8100-universalk9.BLD_POLARIS_DEV_LATEST_20201108_112843.SSA.bin
boot-end-marker
!
!
!
aaa new-model
!
!
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
!
aaa session-id common
!
ip domain name cisco.com
!
login on-success log
!
subscriber templating
!
multilink bundle-name authenticated
!
chat-script lte "" "AT!CALL" TIMEOUT 20 "OK"
chat-script hspa-R7 "" "AT!SCACT=1,1" TIMEOUT 60 "OK"
!
!
crypto pki trustpoint TP-self-signed-1536777273
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-1536777273
  revocation-check none
  rsakeypair TP-self-signed-1536777273
!
crypto pki trustpoint SLA-TrustPoint
  enrollment pkcs12
  revocation-check crl
!
crypto pki trustpoint LDevID
```

```

enrollment retry count 4
enrollment retry period 2
enrollment mode ra
enrollment profile LDevID
serial-number none
fqdn none
ip-address none
password
fingerprint 7107DAB5FBDAC555893B7C047D202B5676F6C9AB
subject-name serialNumber=PID:IR8140H-P-K9 SN:FDO2420J78D,CN= IR8140H
revocation-check none
rsakeypair LDevID 2048
!
crypto pki profile enrollment LDevID
enrollment url http://172.27.127.21/certsrv/mscep/mscep.dll
!
crypto pki certificate map FlexVPN_Cert_Map 1
issuer-name co cn = sit-dc-sit-dc-ca
!
crypto pki certificate chain TP-self-signed-1536777273
certificate self-signed 01
30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 31353336 37373732 3733301E 170D3230 31313137 32323237
33325A17 0D333031 31313732 32323733 325A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 35333637
37373237 33308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
0A028201 01008D4E BBE387AB 5FE56CF9 77532A82 554176A9 3F13D193 729E1C9D
0E9AC390 D66E845E 78AFEBFE 09DD0848 15DE936F E18FB64D 85E97E52 87412474
DE16C42B 3101B84E 8C4F14C4 67EF8867 4AEE4996 6229CFBD 15556C90 F37C1C3D
4D77A046 5934F3C9 6A98DDEE E4413E33 0F260D52 2EBB88C6 C0A1D9DC 633D13BB
0DAC3ACD 6C980F61 C6521868 52EA0150 95C33DB0 26C0AB56 6CB67AD1 401CBBDD
D1994822 1337B943 019F9EDF 4FC72749 01B66A31 ACD60696 14AF9A68 3D7578F1
7BFE63CE A0D4A2F3 DA577B90 15C875EA F175CA24 B17E15A7 9C892E54 1D960D71
907D4D23 2CE67E1A 720AA7A6 9EE1EFEE 12A26353 B258FECB CBAC3FF2 95DAC73D
BBEC1F9E E1030203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603 551D2304 18301680 14A1A44D ABD867DC 26C5B2F2 3A8D9504 807FFA9C
E6301D06 03551D0E 04160414 A1A44DAB D867DC26 C5B2F23A 8D950480 7FFA9CE6
300D0609 2A864886 F70D0101 05050003 82010100 267416FA CF69B1CD 96825C67
483D698D 2B2838E5 94CDA5ED DA5E6BC0 E45739F9 676A4828 32FA2FDE C613BE3D
6B00BA4B 97F52155 966726BE B02D6E48 685190E6 2AF094BC E2A4C087 B5F2449B
4BFF2329 FD4D222D C11C3F73 727FD13C 901C51D0 3F08C6BA C6415D2F 078907E5
D8CCCB8F E28D9485 D2AA4F6D 300A7A2D 289F5E49 79637E6D 7B678332 EEEF2E80
E344AB7C F0FC70D5 694C0CC3 DB9F62E5 2A050979 E9171466 81CC91BA A99AB7C7
12CACA37 D196D178 E349C627 597CFA9C 49132F8A 17C2F471 7E9D80E5 B7D5E673
A225E086 F6E523AC 0C565E9A 3A7E1610 4275D2B7 9AFD5703 F5E1A8E0 94E53C1B
ADF8644D EF0541A8 E98A1F41 A3A6F208 920EAE57
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 2CD68E66 17222EA1 F1EFF64D
CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBAE3 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

```



```

OD06092A 864886F7 OD01010B 0500305F 31133011 060A0992 268993F2 2C640119
1603636F 6D311530 13060A09 92268993 F22C6401 19160563 6973636F 31163014
060A0992 268993F2 2C640119 16067369 742D6463 31193017 06035504 03131073
69742D64 632D5349 542D4443 2D434130 20170D31 38303932 35313134 3735335A
180F3230 36383039 32353131 35373533 5A305F31 13301106 0A099226 8993F22C
64011916 03636F6D 31153013 060A0992 268993F2 2C640119 16056369 73636F31
16301406 0A099226 8993F22C 64011916 06736974 2D646331 19301706 03550403
13107369 742D6463 2D534954 2D44432D 43413082 0122300D 06092A86 4886F70D
01010105 00038201 0F003082 010A0282 010100AF 6FB5E529 DEF701CD E5ACB737
D2790873 875E9DBB 53ADAF2C 94C3D991 EC658A69 B1AB69BA C32307BE BF9D225D
4FEADF33 F396AB70 A4E49526 AE637FE4 6BA0BB32 C98528D0 94658C48 DBE550A1
ECA35F7A 4279F16C 5F3C2B11 185F95BB 9D68B2C9 82ECB523 BC3E5833 436BD1D1
AE9616BD 1E0FC85D 67EF135B 6BC68840 3103DA89 923156FC EADD0914 3DD1F75E
B166E550 A9F0FBEA 80DDE1F4 1B4D7789 3872EEA0 5B375344 03CDDFBA 72DC6F53
6C3D25A3 BF8E215F 8D55C8D1 D0C279ED 9E061673 3FC6F225 6C405AA3 E6B96310
4C2798A9 EC561A29 FF875907 B3527352 61A09CF2 D7916631 1F5215E5 6077E8C4
A5042B6E 3039B222 BCFA1133 53FA51AD 2E972D02 03010001 A351304F 300B0603
551D0F04 04030201 86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D
0E041604 1422A59D B25D909E DA074C00 39B59575 B3F8898F 53301006 092B0601
04018237 15010403 02010030 0D06092A 864886F7 OD01010B 05000382 01010039
6F03857F 8B5F0A38 E6DFA0E9 8598FE40 9231C4DF 5D747EA8 B968606B DD1593A8
2348303C 7948DD69 1FDEA891 2A249CCC 9B9C9071 D51B1AC6 EF1567EF 64E8C11A
85BDA86C AC45954E 7A86861C 1D7C622B 2211652C C8CC6359 09000B78 0E6ABF6E
06D4247B 572E91B2 1216BC9A 5D715B8D E3220C4B 4B6B1B1A 3AA4B2CB 67F7F6B5
2B3D9820 0E5A50A3 123E41F5 3C0D46E0 63E7212B 4730D9DA 4E0E8227 AEEAE386
3C1A1B3A C680B486 5F71B0B5 80C82F6C 58126809 39193ABF D145BA7D 4D695762
5DB055D4 077E779D AEA96655 576B3085 0CD9E01F 6805EF8B 494EE44B 16ACEED8
F6529B1F AA324C9F 464FA153 9DAF12C1 74872179 1DA83009 26D36774 77C52F
    Quit
!
no license feature hseck9
license udi pid IR8140H-P-K9 sn FDO2441J91D
license boot level network-advantage
memory free low-watermark processor 47507
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
redundancy
mode none

!
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
route set interface
route set access-list FlexVPN_Client_IPv4_LAN
!
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
encryption aes-cbc-256
integrity sha256
group 14
!
crypto ikev2 policy FLexVPN_IKEv2_Policy
proposal FlexVPN_IKEv2_Proposal
!
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
match certificate FlexVPN_Cert_Map
identity local dn
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint LDevID

```

```

dpd 120 3 periodic
aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
!
crypto ikev2 dpd 60 10 periodic
crypto ikev2 client flexvpn FlexVPN_Client_2
  peer 1 103.0.0.254
  client connect Tunnel2
!
crypto ikev2 client flexvpn FlexVPN_Client_1
  peer 1 102.0.0.254
  client connect Tunnel1
!
!
controller Cellular 0/2/0
!
controller Cellular 0/3/0
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes 256 esp-sha256-hmac
mode tunnel
!
crypto ipsec profile FlexVPN_IPsec_Profile
  set transform-set FlexVPN_IPsec_Transform_Set
  set pfs group14
  set ikev2-profile FlexVPN_IKEv2_Profile
!
interface Loopback1
  ip address 12.12.12.12 255.255.255.255
!
interface Tunnel1
  ip unnumbered Loopback1
  tunnel source Cellular0/2/0
  tunnel destination dynamic
  tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel2
  ip unnumbered Loopback1
  tunnel source Cellular0/3/0
  tunnel destination dynamic
  tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface VirtualPortGroup1
  ip address 192.168.11.1 255.255.255.0
  no mop enabled
  no mop sysid
!
interface GigabitEthernet0/0/0
  ip address 172.27.127.74 255.255.255.128
  negotiation auto
!
interface GigabitEthernet0/0/1
  no ip address
  shutdown
  negotiation auto
!
interface Cellular0/2/0
  ip address negotiated
  ip access-group 1 out
  ip tcp adjust-mss 1460
  load-interval 30
  dialer in-band
  dialer idle-timeout 0
  dialer-group 1
  ipv6 enable
  pulse-time 1

```

```
    ip virtual-reassembly
!
interface Cellular0/2/1
  no ip address
!
interface Cellular0/3/0
  ip address negotiated
  ip access-group 1 out
  ip tcp adjust-mss 1460
  load-interval 30
  dialer in-band
  dialer idle-timeout 0
  dialer-group 2
  ipv6 enable
  pulse-time 1
  ip virtual-reassembly
!
interface Cellular0/3/1
  no ip address
!
interface WPAN0/1/0
  no ip address
  arp timeout 0
  no mop enabled
  no mop sysid
!
no ip http server
ip http auth-retry 3 time-window 1
ip http authentication local
ip http secure-server
ip forward-protocol nd
ip route 102.0.0.0 255.255.255.0 Cellular0/2/0 192.168.5.1
ip route 103.0.0.0 255.255.255.0 Cellular0/3/0 192.168.4.1
ip route 192.168.4.0 255.255.255.0 Cellular0/3/0
ip route 192.168.5.0 255.255.255.0 Cellular0/2/0
!
ip access-list standard FlexVPN_Client_IPv4_LAN
  10 permit 192.168.11.0 0.0.0.255
  20 permit 12.12.12.12
!
!
ip access-list standard 1
  10 permit any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit
!
snmp-server enable traps wpan
!
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
  stopbits 1
line vty 0 4
  transport input ssh
line vty 5 14
  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
app-hosting appid iperf
app-vnic gateway0 virtualportgroup 1 guest-interface 0
  guest-ipaddress 192.168.11.2 netmask 255.255.255.0
app-default-gateway 192.168.11.1 guest-interface 0
end

```

## Configuring Global Parameters

To configure global parameters for your router, follow these steps.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>Router&gt; enable Router# configure terminal Router(config)#</pre>	Enters global configuration mode when using the console port.  Use the following to connect to the router with a remote terminal: <pre>telnet router-name or address Login: login-id Password: ***** Router&gt; enable</pre>
<b>Step 2</b>	<b>hostname <i>name</i></b> <b>Example:</b> <pre>Router(config)# hostname Router</pre>	Specifies the name for the router.
<b>Step 3</b>	<b>enable password <i>password</i> or enable secret password <i>password</i></b> <b>Example:</b> <pre>Router(config)# enable password crlny5ho</pre>	Specifies a password to prevent unauthorized access to the router.  <b>Note</b> In this form of the command, password is not encrypted. To encrypt the password use enable secret password as noted in the previously mentioned Device Hardening Guide.



# Configuring the Gigabit Ethernet Interface

The router features two Gigabit Ethernet (GE) ports that can be used to enable WAN connectivity to a primary substation or a control center:

- One GigE Copper port (RJ45) on the midplane board. It supports standard 3-speed (10/100/1000) Ethernet features including auto-MDIX.
- One SFP socket. It supports standard 1000Base-X or 100Base-FX Ethernet over single-mode or multi-mode fiber.

To configure the Gigabit Ethernet interface, follow these steps:

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>	
<b>Step 2</b>	<b>ipv6 unicast-routing</b> <b>Example:</b> Router#configure terminal Router(config)# <b>ipv6 unicast-routing</b>	Enables forwarding of IPv6 unicast data packets.
<b>Step 3</b>	<b>interface GigabitEthernet slot/bay/port</b> <b>Example:</b> Router(config)# <b>interface GigabitEthernet 0/0/0</b>	Enters the configuration mode for an interface on the router.
<b>Step 4</b>	<b>ip address ip-address mask</b> <b>Example:</b> Router(config-if)# <b>ip address 192.168.12.2 255.255.255.0</b>	Sets the IP address and subnet mask for the specified interface. Use this Step if you are configuring an IPv4 address.
<b>Step 5</b>	<b>ipv6 address ipv6-address/prefix</b> <b>Example:</b> Router(config-if)# <b>ipv6 address 2001.db8::ffff:1/128</b>	Sets the IPv6 address and prefix for the specified interface. Use this step instead of Step 2, if you are configuring an IPv6 address. IPv6 unicast-routing needs to be set-up as well, see further information in the <b>IPv6 Addressing and Basic Connectivity Configuration Guide</b> located here: <a href="https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/x6-16-10/ip6b-xe-16-10-book/read-me-first.html">https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/x6-16-10/ip6b-xe-16-10-book/read-me-first.html</a>
<b>Step 6</b>	<b>no shutdown</b> <b>Example:</b> Router(config-if)# <b>no shutdown</b>	Enables the interface and changes its state from administratively down to administratively up.

	Command or Action	Purpose
<b>Step 7</b>	<b>exit</b>  <b>Example:</b>  Router(config-if) # <b>exit</b>	Exits the configuration mode of interface and returns to the global configuration mode.

## Support for sub-interface on GigabitEthernet0/0/0

Cisco IOS XE supports sub-interfaces and dot1q configuration on the g0/0/0 interface. For example:

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

## Configuring a Loopback Interface

### Before you begin

The loopback interface acts as a placeholder for the static IP address and provides default routing information.

To configure a loopback interface, follow these steps.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>	
<b>Step 2</b>	<b>interface</b> <i>type number</i>  <b>Example:</b>  Router(config)# <b>interface</b> Loopback 0	Enters configuration mode on the loopback interface.
<b>Step 3</b>	(Option 1) <b>ip address</b> <i>ip-address mask</i>  <b>Example:</b>  Router(config-if) # <b>ip address</b> 10.108.1.1 255.255.255.0	Sets the IP address and subnet mask on the loopback interface. (If you are configuring an IPv6 address, use the <b>ipv6 address</b> <i>ipv6-address/prefix</i> command described below.
<b>Step 4</b>	(Option 2) <b>ipv6 address</b> <i>ipv6-address/prefix</i>  <b>Example:</b>  Router(config-if) # <b>ipv6 address</b> 2001:db8::ffff:1/128	Sets the IPv6 address and prefix on the loopback interface.

	Command or Action	Purpose
<b>Step 5</b>	<b>exit</b> <b>Example:</b> Router(config-if)# <b>exit</b>	Exits configuration mode for the loopback interface and returns to global configuration mode.

## Example

### Verifying Loopback Interface Configuration

Enter the **show interface loopback** command. You should see an output similar to the following example:

```
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
```

Alternatively, use the **ping** command to verify the loopback interface, as shown in the following example:

```
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
```

# Enabling Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is enabled by default on the router. It may be disabled if needed for security purposes.

For more information on using CDP, see [Cisco Discovery Protocol Configuration Guide, Cisco IOS XE Release 3S](#).

# Configuring Command-Line Access

To configure parameters to control access to the router, follow these steps.



**Note** Transport input must be set as explained in the previous Telnet and SSH sections of the guide.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>line</b> [ <b>aux</b>   <b>console</b>   <b>tty</b>   <b>vty</b> ] <i>line-number</i> <b>Example:</b> Router(config)# <b>line console 0</b>	Enters line configuration mode, and specifies the type of line.  The example provided here specifies a console terminal for access.
<b>Step 2</b>	<b>password</b> <i>password</i> <b>Example:</b> Router(config-line)# <b>password 5dr4Hepw3</b>	Specifies a unique password for the console terminal line.
<b>Step 3</b>	<b>login</b> <b>Example:</b> Router(config-line)# <b>login</b>	Enables password checking at terminal session login.
<b>Step 4</b>	<b>exec-timeout</b> <i>minutes</i> [ <i>seconds</i> ] <b>Example:</b> Router(config-line)# <b>exec-timeout 5 30</b> Router(config-line)#	Sets the interval during which the EXEC command interpreter waits until user input is detected. The default is 10 minutes. Optionally, adds seconds to the interval value.  The example provided here shows a timeout of 5 minutes and 30 seconds. Entering a timeout of <b>0 0</b> specifies never to time out.
<b>Step 5</b>	<b>exit</b> <b>Example:</b> Router(config-line)# <b>exit</b>	Exits line configuration mode to re-enter global configuration mode.
<b>Step 6</b>	<b>line</b> [ <b>aux</b>   <b>console</b>   <b>tty</b>   <b>vty</b> ] <i>line-number</i> <b>Example:</b> Router(config)# <b>line vty 0 4</b> Router(config-line)#	Specifies a virtual terminal for remote console access.
<b>Step 7</b>	<b>password</b> <i>password</i> <b>Example:</b>	Specifies a unique password for the virtual terminal line.

	Command or Action	Purpose
	Router(config-line) # <b>password aldf2ad1</b>	
<b>Step 8</b>	<b>login</b> <b>Example:</b> Router(config-line) # <b>login</b>	Enables password checking at the virtual terminal session login.
<b>Step 9</b>	<b>end</b> <b>Example:</b> Router(config-line) # <b>end</b>	Exits line configuration mode, and returns to privileged EXEC mode.

### Example

The following configuration shows the command-line access commands. Note that transport input none is the default, but if SSH is enabled this must be set to ssh.

You do not have to input the commands marked **default**. These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

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

## Configuring Static Routes

Static routes provide fixed routing paths through the network. They are manually configured on the router. If the network topology changes, the static route must be updated with a new route. Static routes are private routes unless they are redistributed by a routing protocol.

To configure static routes, follow these steps.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	(Option 1) <b>ip route</b> <i>prefix mask {ip-address</i>   <i>interface-type interface-number</i> [ <i>ip-address</i> ]} <b>Example:</b>	Specifies a static route for the IP packets. (If you are configuring an IPv6 address, use the <b>ipv6 route</b> command described below.)

	Command or Action	Purpose
	Router(config)# <b>ip route</b> 192.10.2.3 255.255.0.0 10.10.10.2	
<b>Step 2</b>	(Option 2) <b>ipv6 route</b> <i>prefix/mask</i> { <i>ipv6-address</i>   <i>interface-type</i> <i>interface-number</i> [ <i>ipv6-address</i> ]}  <b>Example:</b>  Router(config)# <b>ipv6 route</b> 2001:db8:2::/64 2001:db8:3::0	Specifies a static route for the IP packets. See additional information for IPv6 here: <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>
<b>Step 3</b>	<b>end</b>  <b>Example:</b>  Router(config)# <b>end</b>	Exits global configuration mode and enters privileged EXEC mode.

In the following configuration example, the static route sends out all IP packets with a destination IP address of 192.168.1.0 and a subnet mask of 255.255.255.0 on the Gigabit Ethernet interface to another device with an IP address of 10.10.10.2. Specifically, the packets are sent to the configured PVC.

You do not have to enter the command marked **default**. This command appears automatically in the configuration file generated when you use the **running-config** command.

```
!
ip classless (default)
ip route 2001:db8:2::/64 2001:db8:3::0
```

### Verifying Configuration

To verify that you have configured static routing correctly, enter the **show ip route** command (or **show ipv6 route** command) and look for static routes marked with the letter S.

When you use an IPv4 address, you should see verification output similar to the following:

```
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, GigabitEthernet0
```

When you use an IPv6 address, you should see verification output similar to the following:

```
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

```

## Configuring Dynamic Routes

In dynamic routing, the network protocol adjusts the path automatically, based on network traffic or topology. Changes in dynamic routes are shared with other routers in the network.

All of the Cisco IOS-XE configuration guides can be found here: <https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-amsterdam-17-3-1/model.html>

## Configuring Routing Information Protocol

To configure the RIP on a router, follow these steps.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>router rip</b>  <b>Example:</b>  Router(config)# <b>router rip</b>	Enters router configuration mode, and enables RIP on the router.
<b>Step 2</b>	<b>version {1   2}</b>  <b>Example:</b>  Router(config-router)# <b>version 2</b>	Specifies use of RIP version 1 or 2.
<b>Step 3</b>	<b>network ip-address</b>  <b>Example:</b>  Router(config-router)# <b>network 192.168.1.1</b> Router(config-router)# <b>network 10.10.7.1</b>	Specifies a list of networks on which RIP is to be applied, using the address of the network of each directly connected network.
<b>Step 4</b>	<b>no auto-summary</b>  <b>Example:</b>	Disables automatic summarization of subnet routes into network-level routes. This allows subprefix routing information to pass across classful network boundaries.

	Command or Action	Purpose
	Router(config-router)# <b>no auto-summary</b>	
<b>Step 5</b>	<b>end</b>  <b>Example:</b>  Router(config-router)# <b>end</b>	Exits router configuration mode, and enters privileged EXEC mode.

### Example

#### Verifying Configuration

To verify that you have configured RIP correctly, enter the **show ip route** command and look for RIP routes marked with the letter R. You should see an output similar to the one shown in the following example:

```
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
```

## Configuring Enhanced Interior Gateway Routing Protocol

The Enhanced Interior Gateway Routing Protocol (EIGRP) is an enhanced version of the Interior Gateway Routing Protocol (IGRP) developed by Cisco. The convergence properties and the operating efficiency of EIGRP have improved substantially over IGRP, and IGRP is now obsolete.

The convergence technology of EIGRP is based on an algorithm called the Diffusing Update Algorithm (DUAL). The algorithm guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize. Devices that are not affected by topology changes are not involved in recomputations.

Details on configuring Enhanced Interior Gateway Routing Protocol (EIGRP), are found in the following guide: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_eigrp/configuration/xr-16-10/ire-xr-16-10-book/ire-enhanced-igrp.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xr-16-10/ire-xr-16-10-book/ire-enhanced-igrp.html)

## Modular QoS (MQC)

This section provides an overview of Modular QoS CLI (MQC), which is how all QoS features are configured on the IoT Integrated Services Router. MQC is a standardized approach to enabling QoS on Cisco routing and switching platforms.



Follow the procedures that are in the QoS Modular QoS Command-Line Interface Configuration Guide, Cisco IOS XE 17 guide.

