



IPCP Subnet Mask Support

This document describes the IPCP Subnet Mask Support feature in Cisco IOS Release 12.1(5)T.

This document includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 3](#)
- [Prerequisites, page 3](#)
- [Configuration Tasks, page 3](#)
- [Command Reference, page 6](#)
- [Glossary, page 8](#)

Feature Overview

IP Control Protocol (IPCP) subnet mask support allows customer premises equipment (CPE) to connect to the node route processor (NRP) and obtain IP addresses and subnet mask ranges that the CPE can use to populate the Dynamic Host Configuration Protocol (DHCP) server database.

The NRP brings up PPP sessions with the CPE and authenticates each CPE as a separate user. An extension of the normal IPCP negotiations enables the CPE to obtain an IP subnet mask associated with the returned IP address. The NRP adds a static route for the IP address with the subnet mask specified. If the subnet mask is specified by the Framed-IP-netmask attribute in the RADIUS user profile, the NRP passes the mask and IP address to the CPE during IPCP negotiation. If the Framed-IP-netmask is not specified in the RADIUS user profile, the NRP passes the subnet mask specified with the **ppp ipcp mask** command in the NRP configuration. The CPE uses the subnet mask to calculate an IP address pool from which IP addresses are assigned to PCs using the access link.

Benefits

Because the CPE can receive both the IP address and subnet mask during PPP setup negotiation, DHCP support is no longer required on the client side. If the CPE uses DHCP servers to allocate addresses for its own network, subnets can be assigned from the network access server (NAS) NRP and distributed to the remote CPE DHCP servers.

(gpamidi) ALPHA DRAFT - CISCO CONFIDENTIAL

Supported Platforms

This feature is available on all platforms that support PPP.

- Cisco 800 series
- Cisco 900 series
- Cisco 1400 series
- Cisco 1600 series
- Cisco 1700 series
- Cisco 2500 series
- Cisco 2600 series
- Cisco 3600 series
- Cisco 4000-M, 4500-M, 4700-M
- Cisco 4500 series
- Cisco 4700 series
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series (including Cisco RSP7000)
- Cisco AS5300
- Cisco AS5400
- Cisco AS5800
- Cisco MC3810
- Cisco uBR7200

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

(gpamidi) ALPHA DRAFT - CISCO CONFIDENTIAL

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

The peer CPE must support and initiate CPE subnet mask negotiation.

Configuration Tasks

See the following sections for required configuration tasks for IPCP subnet masks.

- [Configuring the Subnet Mask](#)
- [Configuring IPCP Subnet Mask Support on the CPE](#)

Configuring the Subnet Mask

Choose at least one of the methods described in the following sections to configure the subnet mask that the NRP will pass to the CPE upon request:

- [Configuring the Subnet Mask in the RADIUS User Profile](#)
- [Configuring the Subnet Mask on the NRP](#)



Note

The subnet mask in the RADIUS user profile overrides the mask configured on the NRP.

If the subnet mask is not available from either the NRP configuration or the RADIUS user profile, the NRP rejects IPCP subnet mask negotiation from the CPE.

(gpamidi) ALPHA DRAFT - CISCO CONFIDENTIAL**Configuring the Subnet Mask in the RADIUS User Profile**

To configure the subnet mask in the RADIUS user profile, use the Framed-IP-netmask RADIUS IETF attribute. For more information on setting up a RADIUS user profile, refer to the “Configuring RADIUS” section in the “Security Server Protocols” chapter of the Release 12.2 *Cisco IOS Security Configuration Guide*.

Configuring the Subnet Mask on the NRP

You can configure a subnet mask on the NRP to send to the requesting peer, in case the RADIUS user profile does not include the Framed-IP-netmask attribute. On the NRP, the subnet mask is typically configured on a virtual template. Virtual templates are used to apply properties to PPP sessions.

To configure a subnet mask on the NRP, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface virtual-template <i>number</i>	Creates or specifies the virtual template interface, and enters interface configuration mode.
Step 2	Router(config-if)# ppp ipcp mask <i>subnet-mask</i>	Assigns the subnet mask to pass to a requesting peer (CPE). ¹

1. The subnet mask configured with the **ppp ipcp mask** command is passed to the requesting CPE only if the RADIUS user profile does not contain a subnet mask in the form of the Framed-IP-netmask attribute. If a subnet mask is not available from either the NRP configuration or the RADIUS user profile, the request is rejected.

Configuring IPCP Subnet Mask Support on the CPE

Some CPE is hard-coded to request the subnet mask from the peer. If, however, the CPE uses Cisco IOS software, you must configure the CPE to support and initiate PPP subnet mask negotiation.

**Note**

Make sure you check and follow the documentation for your CPE software release. The following sections provide typical configuration guidelines for enabling CPE to support subnet mask negotiation.

To configure the CPE to support and initiate IPCP subnet mask negotiation, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface <i>type number</i>	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
Step 2	Router(config-if)# ppp ipcp mask request	Requests or rejects IPCP subnet mask negotiations, or specifies a secondary subnet mask if the RADIUS user profile does not contain one.

Verifying the Subnet Mask Configuration

See the following sections for verifying the subnet mask configuration:

(gpamidi) ALPHA DRAFT - CISCO CONFIDENTIAL

- [Verifying the Subnet Mask in the RADIUS User Profile](#)
- [Verifying the Subnet Mask on the NRP](#)
- [Verifying IPCP Subnet Mask Support on the CPE](#)

Verifying the Subnet Mask in the RADIUS User Profile

To verify the RADIUS user profile, refer to the user documentation for your RADIUS server.

You can also examine a RADIUS accounting packet and verify that the Framed-IP-netmask attribute is included in the packet, as shown in the following example:

```
Wed Jun 16 13:57:31 1999
NAS-IP-Address = 10.168.100.192

NAS-Port = 268566560
NAS-Port-Type = Virtual
User-Name = "cisco"
Acct-Status-Type = Start
Service-Type = Framed

Acct-Session-Id = "1/0/0/2.32_00000009"
Framed-Protocol = PPP
Framed-IP-Address = 10.16.7.254
!
Framed-IP-netmask = 255.255.255.248
Acct-Delay-Time = 0
```

Verifying the Subnet Mask on the NRP

To verify that you successfully configured the subnet mask on the NRP, use the **more system:running-config EXEC** command to display the current running configuration. Check that the **ppp ipcp mask subnet-mask** interface configuration command is applied to the appropriate virtual template.

Verifying IPCP Subnet Mask Support on the CPE

To verify that your CPE is hard-coded to request the subnet mask from the peer, refer to the user documentation for your CPE.

To verify that you successfully configured IPCP subnet mask support, use the **more system:running-config EXEC** command to display the current running configuration. Check that the **ppp ipcp mask request** interface configuration command is applied to the appropriate interface.

Troubleshooting Tips

To troubleshoot IPCP subnet mask support on the NRP, use the following **debug** commands:

- **debug aaa authentication**—displays the methods and results of authentication being used
- **debug aaa authorization**—displays the methods and results of authorization being used
- **debug ppp negotiations**—displays the details of PPP and IPCP subnet negotiations

(gpamidi) ALPHA DRAFT - CISCO CONFIDENTIAL

Configuration Examples

This section provides the following configuration examples:

- [Configuring the Subnet Mask in the RADIUS User Profile Example](#)
- [Configuring the Subnet Mask on the NRP Example](#)
- [Configuring IPCP Subnet Mask Support on the CPE Example](#)

Configuring the Subnet Mask in the RADIUS User Profile Example

In the following example, the RADIUS user profile contains the netmask 255.255.255.248:

```
CPE1 Password = "cisco"
    Service-Type = Framed,
    Framed-Protocol = PPP,
    Framed-IP-Address=10.0.0.1
!
    Framed-IP-netmask=255.255.255.248
    Framed-MTU = 1500
```

Configuring the Subnet Mask on the NRP Example

In the following example, the PPP sessions in permanent virtual circuit (PVC) 1/43 are configured to support IPCP subnet negotiation. If the RADIUS user profile does not contain the Framed-IP-netmask attribute, the NRP returns 255.255.255.224 to the requesting CPE.

```
!
interface ATM0/0/0.30 multipoint
  pvc 1/43
    encapsulation aal5cisco ppp Virtual-Template 2
  !
!
interface Virtual-Template2
  ip unnumbered FastEthernet0/0/0
  no peer default ip address
  ppp authentication pap chap
  ppp ipcp mask 255.255.255.224
!
```

Configuring IPCP Subnet Mask Support on the CPE Example

In the following example, the CPE is configured to initiate IPCP subnet mask negotiation:

```
!
interface Dialer 0
  ppp ipcp mask request
!
```

Command Reference

This section documents the new **ppp ipcp mask** command that configures the IPCP Subnet Mask Support feature. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

(gpamidi) ALPHA DRAFT - CISCO CONFIDENTIAL

ppp ipcp mask

To request or reject IP Control Protocol (IPCP) subnet mask negotiation, or to specify a secondary subnet mask to use in case the RADIUS user profile does not contain one, use the **ppp ipcp mask** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

```
ppp ipcp mask {subnet-mask | reject | request}
```

```
no ppp ipcp mask [subnet-mask | reject | request]
```

Syntax Description

<i>subnet-mask</i>	Specifies the 32-bit subnet mask sent to requesting peer when the RADIUS user profile does not include the Framed-IP-netmask attribute.
reject	Rejects IPCP subnet mask negotiations.
request	Requests the subnet mask from the peer.

Defaults

Responds to IPCP subnet mask requests, but does not initiate IPCP subnet mask negotiations.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)DC	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

Typically, the customer premises equipment (CPE) is configured or hard-coded to request the subnet mask information from the node route processor (NRP).

If the subnet mask is not available from either the NRP configuration or the RADIUS user profile, the NRP rejects the CPE request as if the **ppp ipcp mask reject** command was configured on the NRP.

Examples

In the following example, the PPP sessions in permanent virtual circuit (PVC) 1/43 are configured to support IPCP subnet negotiation. If the RADIUS user profile does not contain the Framed-IP-netmask attribute, the NRP returns 255.255.255.224 to the requesting CPE.

```
!
interface ATM 0/0/0.30 multipoint
  pvc 1/43
    encapsulation aal5cisco ppp Virtual-Template 2
  !
!
interface Virtual-Template 2
  ip unnumbered FastEthernet 0/0/0
  no peer default ip address
  ppp authentication pap chap
  !
  ppp ipcp mask 255.255.255.224
!
```

(gpamidi) ALPHA DRAFT - CISCO CONFIDENTIAL

Glossary

address mask—Bit combination used to describe which portion of an address refers to the network or subnet and which part refers to the host.

CPE—customer premises equipment. Terminating equipment such as terminals, telephones, and modems supplied by the telephone company, installed at customer sites, and connected to the telephone company network.

DHCP—Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when no longer needed.

IETF—Internet Engineering Task Force. Task force consisting of over 80 working groups responsible for developing Internet standards. The IETF operates under the auspices of ISOC. See also ISOC.

ISOC—Internet Society. International nonprofit organization, founded in 1992, that coordinates the evolution and use of the Internet. In addition, ISOC delegates authority to other groups related to the Internet, such as the IAB. ISOC is headquartered in Reston, Virginia (United States).

IPCP—IP Control Protocol. Protocol that establishes and configures IP over PPP.

PVC—permanent virtual circuit (or connection). Virtual circuit that is permanently established.

RADIUS—Remote Authentication Dial-In User Service. Database for authenticating dial-in connections and for tracking connection time.

subnet mask—32-bit address mask used in IP to indicate the bits of an IP address that are being used for the subnet address.