Basic File Transfer Services Commands

This chapter provides detailed descriptions of commands used to configure basic file transfer services on a Cisco routing device.

For configuration information and examples, refer to the "Configuring Basic File Transfer Services" chapter in the Release 12.2 *Cisco IOS Configuration Fundamentals Configuration Guide*.

async-bootp

To configure extended BOOTP requests for asynchronous interfaces as defined in RFC 1084, use the **async-bootp** global configuration command. To restore the default, use the **no** form of this command.

async-bootp *tag* [**:***hostname*] *data*

no async-bootp

Syntax Description

tag	Item being requested; expressed as filename, integer, or IP dotted decimal address. See Table 42 for possible keywords.
:*hostname*	(Optional) This entry applies only to the host specified. The **:***hostname* argument accepts both an IP address and a logical host name.
data	List of IP addresses entered in dotted decimal notation or as logical host names, a number, or a quoted string.

Table 42   tag Keyword Options

Keyword	Description
bootfile	Specifies use of a server boot file from which to download the boot program. Use the optional :*hostname* argument and the *data* argument to specify the filename.
subnet-mask *mask*	Dotted decimal address specifying the network and local subnetwork mask (as defined by RFC 950).
time-offset *offset*	Signed 32-bit integer specifying the time offset of the local subnetwork in seconds from Coordinated Universal Time (UTC).
gateway *address*	Dotted decimal address specifying the IP addresses of gateways for this subnetwork. A preferred gateway should be listed first.
time-server *address*	Dotted decimal address specifying the IP address of time servers (as defined by RFC 868).
IEN116-server *address*	Dotted decimal address specifying the IP address of name servers (as defined by IEN 116).
nbns-server *address*	Dotted decimal address specifying the IP address of Windows NT servers.
DNS-server *address*	Dotted decimal address specifying the IP address of domain name servers (as defined by RFC 1034).
log-server *address*	Dotted decimal address specifying the IP address of an MIT-LCS UDP log server.
quote-server *address*	Dotted decimal address specifying the IP address of Quote of the Day servers (as defined in RFC 865).
lpr-server *address*	Dotted decimal address specifying the IP address of Berkeley UNIX Version 4 BSD servers.
impress-server *address*	Dotted decimal address specifying the IP address of Impress network image servers.

Table 42   tag Keyword Options (continued)

Keyword	Description
rlp-server *address*	Dotted decimal address specifying the IP address of Resource Location Protocol (RLP) servers (as defined in RFC 887).
hostname *name*	The name of the client, which may or may not be domain qualified, depending upon the site.
bootfile-size *value*	A two-octet value specifying the number of 512-octet (byte) blocks in the default boot file.

Defaults

If no extended BOOTP commands are entered, the Cisco IOS software generates a gateway and subnet mask appropriate for the local network.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use the **show async-bootp** EXEC command to list the configured parameters. Use the **no async-bootp** command to clear the list.

Examples

The following example illustrates how to specify different boot files: one for a PC, and one for a Macintosh. With this configuration, a BOOTP request from the host on 172.30.1.1 results in a reply listing the boot filename as pcboot. A BOOTP request from the host named mac results in a reply listing the boot filename as macboot.

```
async-bootp bootfile :172.30.1.1 "pcboot"
async-bootp bootfile :mac "macboot"
```

The following example specifies a subnet mask of 255.255.0.0:

```
async-bootp subnet-mask 255.255.0.0
```

The following example specifies a negative time offset of the local subnetwork of 3600 seconds:

```
async-bootp time-offset –3600
```

The following example specifies the IP address of a time server:

```
async-bootp time-server 172.16.1.1
```

Related Commands

Command	Description
show async bootp	Displays the extended BOOTP request parameters that have been configured for asynchronous interfaces.

ip ftp passive

To configure the router to use only passive File Transfer Protocol (FTP) connections, use the **ip ftp passive** global configuration command. To allow all types of FTP connections, use the **no** form of this command.

ip ftp passive

no ip ftp passive

Syntax Description   This command has no arguments or keywords.

Defaults   All types of FTP connections are allowed.

Command Modes   Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Examples   The following example configures the router to use only passive FTP connections:

```
ip ftp passive
```

Related Commands

Command	Description
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp source-interface	Specifies the source IP address for FTP connections.
ip ftp username	Configures the username for FTP connections.

ip ftp password

To specify the password to be used for File Transfer Protocol (FTP) connections, use the **ip ftp password** global configuration command. To return the password to its default, use the **no** form of this command.

ip ftp password [*type*] *password*

no ip ftp password

Syntax Description

| *type* | (Optional) Type of encryption to use on the password. A value of 0 disables encryption. A value of 7 indicates proprietary encryption. |
| *password* | Password to use for FTP connections. |

Defaults

The router forms a password *username@routername.domain*. The variable *username* is the username associated with the current session, *routername* is the configured host name, and *domain* is the domain of the router.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Examples

The following example configures the router to use the username red and the password blue for FTP connections:

```
ip ftp username red
ip ftp password blue
```

Related Commands

Command	Description
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp source-interface	Specifies the source IP address for FTP connections.
ip ftp username	Configures the username for FTP connections.

ip ftp source-interface

To specify the source IP address for File Transfer Protocol (FTP) connections, use the **ip ftp source-interface** global configuration command. To use the address of the interface where the connection is made, use the **no** form of this command.

ip ftp source-interface *interface*

no ip ftp source-interface

Syntax Description

interface	The interface type and number to use to obtain the source address for FTP connections.

Defaults

The FTP source address is the IP address of the interface the FTP packets use to leave the router.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Use this command to set the same source address for all FTP connections.

Examples

The following example configures the router to use the IP address associated with the Ethernet 0 interface as the source address on all FTP packets, regardless of which interface is actually used to send the packet:

```
ip ftp source-interface ethernet 0
```

Related Commands

Command	Description
ip ftp passive	Configures the router to use only passive FTP connections
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

ip ftp username

To configure the username for File Transfer Protocol (FTP) connections, use the **ip ftp username** global configuration command. To configure the router to attempt anonymous FTP, use the **no** form of this command.

ip ftp username *username*

no ip ftp username

Syntax Description

username	Username for FTP connections.

Defaults

The Cisco IOS software attempts an anonymous FTP.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The remote username must be associated with an account on the destination server.

Examples

In the following example, the router is configured to use the username "red" and the password "blue" for FTP connections:

```
Router(config)# ip ftp username red
Router(config)# ip ftp password blue
```

Related Commands

Command	Description
ip ftp passive	Configures the router to use only passive FTP connections.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp source-interface	Specifies the source IP address for FTP connections.

ip rarp-server

To enable the router to act as a Reverse Address Resolution Protocol (RARP) server, use the **ip rarp-server** command in interface configuration mode. To restore the interface to the default of no RARP server support, use the **no** form of this command.

> **ip rarp-server** *ip-address*

> **no ip rarp-server** *ip-address*

Syntax Description	*ip-address*	IP address that is to be provided in the source protocol address field of the RARP response packet. Normally, this is set to whatever address you configure as the primary address for the interface.

Defaults Disabled

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This feature makes diskless booting of clients possible between network subnets where the client and server are on separate subnets.

RARP server support is configurable on a per-interface basis, so that the router does not interfere with RARP traffic on subnets that need no RARP assistance.

The Cisco IOS software answers incoming RARP requests only if both of the following two conditions are met:

- The **ip rarp-server** command has been configured for the interface on which the request was received.

- A static entry is found in the IP ARP table that maps the MAC address contained in the RARP request to an IP address.

Use the **show ip arp** EXEC command to display the contents of the IP ARP cache.

Sun Microsystems, Inc. makes use of RARP and UDP-based network services to facilitate network-based booting of SunOS on it's workstations. By bridging RARP packets and using both the **ip helper-address** interface configuration command and the **ip forward-protocol** global configuration command, the Cisco IOS software should be able to perform the necessary packet switching to enable booting of Sun workstations across subnets. Unfortunately, some Sun workstations assume that the sender of the RARP response, in this case the router, is the host that the client can contact to TFTP load the bootstrap image. This causes the workstations to fail to boot.

By using the **ip rarp-server** command, the Cisco IOS software can be configured to answer these RARP requests, and the client machine should be able to reach its server by having its TFTP requests forwarded through the router that acts as the RARP server.

In the case of RARP responses to Sun workstations attempting to diskless boot, the IP address specified in the **ip rarp-server** interface configuration command should be the IP address of the TFTP server. In addition to configuring RARP service, the Cisco IOS software must be configured to forward UDP-based Sun portmapper requests to completely support diskless booting of Sun workstations. This can be accomplished using configuration commands of the following form:

```
ip forward-protocol udp 111
interface interface name
ip helper-address target-address
```

RFC 903 documents the RARP.

Examples

The following partial example configures a router to act as a RARP server. The router is configured to use the primary address of the specified interface in its RARP responses.

```
arp 172.30.2.5 0800.2002.ff5b arpa
interface ethernet 0
ip address 172.30.3.100 255.255.255.0
ip rarp-server 172.30.3.100
```

In the following example, a router is configured to act as a RARP server, with TFTP and portmapper requests forwarded to the Sun server:

```
! Allow the router to forward broadcast portmapper requests
ip forward-protocol udp 111
! Provide the router with the IP address of the diskless sun
arp 172.30.2.5 0800.2002.ff5b arpa
interface ethernet 0
! Configure the router to act as a RARP server, using the Sun Server's IP
! address in the RARP response packet.
ip rarp-server 172.30.3.100
! Portmapper broadcasts from this interface are sent to the Sun Server.
ip helper-address 172.30.3.100
```

Related Commands

Command	Description
ip forward-protocol	Speeds up flooding of UDP datagrams using the spanning-tree algorithm.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.

ip rcmd domain-lookup

To reenable the basic DNS security check for rcp and rsh, use the **ip rcmd domain-lookup** global configuration command. To disable the basic DNS security check for rcp and rsh, use the **no** form of this command.

ip rcmd domain-lookup

no ip rcmd domain-lookup

Syntax Description   This command has no arguments or keywords.

Defaults   Enabled

Command Modes   Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines   The abbreviation RCMD (remote command) is used to indicate both rsh and rcp.

DNS lookup for RCMD is enabled by default (provided general DNS services are enabled on the system using the **ip domain-lookup** command).

The **no ip rcmd domain-lookup** command is used to disable the DNS lookup for RCMD. The **ip rcmd domain-lookup** command is used to reenable the DNS lookup for RCMD.

DNS lookup for RCMD is performed as a basic security check. This check is performed using a host authentication process. When enabled, the system records the address of the requesting client. That address is mapped to a host name using DNS. Then a DNS request is made for the IP address for that host name. The IP address received is then checked against the original requesting address. If the address does not match with any of the addresses received from DNS, the RCMD request will not be serviced.

This reverse lookup is intended to help protect against spoofing. However, please note that the process only confirms that the IP address is a valid "routable" address; it is still possible for a hacker to spoof the valid IP address of a known host.

The DNS lookup is done after the TCP handshake but before the router (which is acting as a rsh/rcp server) sends any data to the remote client.

The **no ip rcmd domain-lookup** will turn off DNS lookups for rsh and rcp only. The **no ip domain-lookup** command takes precedence over the **ip rcmd domain-lookup** command. This means that if the **no ip domain-lookup** command is in the current configuration, DNS will be bypassed for rcp and rsh even if the **ip rcmd domain-lookup** command is enabled.

Examples   In the following example, the DNS security check is disabled for RCMD (rsh/rcp):

```
Router(config)# no ip rcmd domain-lookup
```

Related Commands

Command	Description
ip domain-lookup	Enables the IP DNS-based host name-to-address translation.

ip rcmd rcp-enable

To configure the Cisco IOS software to allow remote users to copy files to and from the router using remote copy (rcp), use the **ip rcmd rcp-enable** global configuration command. To disable rcp on the device, use the **no** form of this command.

ip rcmd rcp-enable

no ip rcmd rcp-enable

Syntax Description   This command has no arguments or keywords.

Defaults   To ensure security, the router is not enabled for rcp by default.

Command Modes   Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines   To allow a remote user to execute rcp commands on the router, you must also create an entry for the remote user in the local authentication database using the **ip rcmd remote-host** command.

The **no ip rcmd rcp-enable** command does not prohibit a <u>local</u> user from using rcp to copy system images and configuration files to and from the router.

To protect against unauthorized users copying the system image or configuration files, the router is not enabled for rcp by default.

Examples   In the following example, the rcp service is enabled on the system, the IP address assigned to the Loopback0 interface is used as the source address for outbound rcp and rsh packets, and access is granted to the user "netadmin3"on the remote host 172.16.101.101:

```
Router(config)# ip rcmd rcp-enable
Router(config)# ip rcmd source-interface Loopback0
Router(config)# ip rcmd remote-host router1 172.16.101.101 netadmin3
```

Related Commands

Command	Description
ip rcmd remote-host	Creates an entry for the remote user in a local authentication database so that remote users can execute commands on the router using rsh or rcp.

ip rcmd remote-host

To create an entry for the remote user in a local authentication database so that remote users can execute commands on the router using rsh or rcp, use the **ip rcmd remote-host** command in global configuration mode. To remove an entry for a remote user from the local authentication database, use the **no** form of this command.

> **ip rcmd remote-host** *local-username* {*ip-address* | *host-name*} *remote-username* [**enable** [*level*]]

> **no ip rcmd remote-host** *local-username* {*ip-address* | *host-name*} *remote-username* [**enable** [*level*]]

Syntax Description		
local-username	Name of the user on the local router. You can specify the router name as the username. This name needs to be communicated to the network administrator or to the user on the remote system. To be allowed to remotely execute commands on the router, the remote user must specify this value correctly.
ip-address	IP address of the remote host from which the local router will accept remotely executed commands. Either the IP address or the host name is required.
host-name	Name of the remote host from which the local router will accept remotely executed commands. Either the host name or the IP address is required.
remote-username	Name of the user on the remote host from which the router will accept remotely executed commands.
enable [*level*]	(Optional) Enables the remote user to execute privileged EXEC commands using rsh or to copy files to the router using rcp. The range is from 1 to 15. The default is 15. For information on the enable level, refer to the **privilege level** global configuration command in the Release 12.2 *Cisco IOS Security Command Reference*.

Defaults   No entries are in the local authentication database.

Command Modes   Global configuration

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines   A TCP connection to a router is established using an IP address. Using the host name is valid only when you are initiating an rcp or rsh command from a local router. The host name is converted to an IP address using DNS or host-name aliasing.

To allow a remote user to execute rcp or rsh commands on a local router, you must create an entry for the remote user in the local authentication database. You must also enable the router to act as an rsh or rcp server.

To enable the router to act as an rsh server, issue the **ip rcmd rsh-enable** command. To enable the router to act as an rcp server, issue the **ip rcmd rcp-enable** command.The router cannot act as a server for either of these protocols unless you explicitly enable the capacity.

A local authentication database, which is similar to a UNIX .rhosts file, is used to enforce security on the router through access control. Each entry that you configure in the authentication database identifies the local user, the remote host, and the remote user. To permit a remote user of rsh to execute commands in privileged EXEC mode or to permit a remote user of rcp to copy files to the router, specify the **enable** keyword and level. For information on the enable level, refer to the **privilege level** global configuration command in the Release 12.2 *Cisco IOS Security Command Reference*.

An entry that you configure in the authentication database differs from an entry in a UNIX .rhosts file in the following aspect. Because the .rhosts file on a UNIX system resides in the home directory of a local user account, an entry in a UNIX .rhosts file need not include the local username; the local username is determined from the user account. To provide equivalent support on a router, specify the local username along with the remote host and remote username in each authentication database entry that you configure.

For a remote user to be able to execute commands on the router in its capacity as a server, the local username, host address or name, and remote username sent with the remote client request must match values configured in an entry in the local authentication file.

A remote client host should be registered with DNS. The Cisco IOS software uses DNS to authenticate the remote host's name and address. Because DNS can return several valid IP addresses for a host name, the Cisco IOS software checks the address of the requesting client against all of the IP addresses for the named host returned by DNS. If the address sent by the requester is considered invalid, that is, it does not match any address listed with DNS for the host name, then the software will reject the remote-command execution request.

Note that if no DNS servers are configured for the router, then that device cannot authenticate the host in this manner. In this case, the Cisco IOS software sends a broadcast request to attempt to gain access to DNS services on another server. If DNS services are not available, you must use the **no ip domain-lookup** command to disable the attempt to gain access to a DNS server by sending a broadcast request.

If DNS services are not available and, therefore, you bypass the DNS security check, the software will accept the request to remotely execute a command *only if* all three values sent with the request match exactly the values configured for an entry in the local authentication file.

Examples

The following example allows the remote user named netadmin3 on a remote host with the IP address 172.16.101.101 to execute commands on router1 using the rsh or rcp protocol. User netadmin3 is allowed to execute commands in privileged EXEC mode.

```
ip rcmd remote-host router1 172.16.101.101 netadmin3 enable
```

Related Commands

Command	Description
ip rcmd rcp-enable	Configures the Cisco IOS software to allow remote users to copy files to and from the router.

Command	Description
ip rcmd rsh-enable	Configures the router to allow remote users to execute commands on it using the rsh protocol.
ip domain-lookup	Enables the IP DNS-based host name-to-address translation.

ip rcmd remote-username

To configure the remote username to be used when requesting a remote copy using rcp, use the **ip rcmd remote-username** global configuration command. To remove from the configuration the remote username, use the **no** form of this command.

ip rcmd remote-username *username*

no ip rcmd remote-username *username*

Syntax Description

username	Name of the remote user on the server. This name is used for rcp copy requests. All files and images to be copied are searched for or written relative to the directory of the remote user's account, if the server has a directory structure, for example, as do UNIX systems.

Defaults

If you do not issue this command, the Cisco IOS software sends the remote username associated with the current tty process, if that name is valid, for rcp copy commands. For example, if the user is connected to the router through Telnet and the user was authenticated through the **username** command, then the software sends that username as the remote username.

> **Note** The remote username must be associated with an account on the destination server.

If the username for the current tty process is not valid, the Cisco IOS software sends the host name as the remote username. For rcp boot commands, the Cisco IOS software sends the access server host name by default.

> **Note** For Cisco, tty lines are commonly used for access services. The concept of tty originated with UNIX. For UNIX systems, each physical device is represented in the file system. Terminals are called tty devices (tty stands for teletype, the original UNIX terminal).

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The rcp protocol requires that a client send the remote username on an rcp request to the server. Use this command to specify the remote username to be sent to the server for an rcp copy request. If the server has a directory structure, as do UNIX systems, all files and images to be copied are searched for or written relative to the directory of the remote user's account.

Note Cisco IOS Release 10.3 added the **ip** keyword to **rcmd** commands. If you are upgrading from Release 10.2 to Release 10.3 or a later release, this keyword is automatically added to any **rcmd** commands you have in your Release 10.2 configuration files.

Examples The following example configures the remote username to netadmin1:

```
ip rcmd remote-username netadmin1
```

Related Commands

Command	Description
boot network rcp	Changes the default name of the network configuration file from which to load configuration commands.
boot system rcp	Specifies the system image that the router loads at startup.
bridge acquire	Forwards any frames for stations that the system has learned about dynamically.
copy	Copies any file from a source to a destination.

ip rcmd rsh-enable

To configure the router to allow remote users to execute commands on it using rsh, use the
ip rcmd rsh-enable global configuration command. To disable a router that is enabled for rsh, use the
no form of this command.

> **ip rcmd rsh-enable**

> **no ip rcmd rsh-enable**

Syntax Description   This command has no arguments or keywords.

Defaults   To ensure security, the router is not enabled for rsh by default.

Command Modes   Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines   Remote Shell (rsh), used as a client process, gives users the ability to remotely get router info (such as status)
without the need to connect into the router and then disconnect. This is valuable when looking at many
statistics on many different routers.

Use this command to enable the router to receive rsh requests from remote users. In addition to issuing
this command, you must create an entry for the remote user in the local authentication database to allow
a remote user to execute rsh commands on the router.

The **no ip rcmd rsh-enable** command does not prohibit a local user of the router from executing a
command on other routers and UNIX hosts on the network using rsh. The no form of this command only
disables remote access to rsh on the router.

Examples   The following example enables a router as an rsh server:

```
ip rcmd rsh-enable
```

Related Commands

Command	Description
ip rcmd remote-host	Creates an entry for the remote user in a local authentication database so that remote users can execute commands on the router using rsh or rcp.

ip rcmd source-interface

To force rcp or rsh to use the IP address of a specified interface for all outgoing rcp/rsh communication packets, use the **ip rcmd source-interface** command in global configuration mode. To disable a previously configured **ip rcmd source-interface** command, use the **no** form of this command.

> **ip rcmd source-interface** *interface-id*

> **no ip rcmd source-interface** *interface-id*

Syntax Description	*interface-id*	The name and number used to identify the interface. For example, "Loopback2."

Defaults

The address of the interface closest to the destination is used as the source interface for rcp/rsh communications.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

If this command is not used, or if the interface specified in this command is not available (not up), the Cisco IOS software uses the address of the interface closest to the destination as the source address.

Use this command to force the system to tag all outgoing rcp/rsh packets with the IP address associated with the specified interface. This address is used as the source address as long as the interface is in the up state.

This command is especially useful in cases where the router has many interfaces, and you want to ensure that all rcp and/or rsh packets from this router have the same source IP address. A consistent address is preferred so that the other end of the connection (the rcp/rsh server or client) can maintain a single session. The other benefit of a consistent address is that an access list can be configured on the remote device.

The specified interface must have an IP address associated with it. If the specified interface does not have an IP address or is in a down state, then rcp/rsh reverts to the default. To avoid this, add an IP address to the subinterface or bring the interface to the up state.

Examples

In the following example, the Loopback0 interface is assigned an IP address of 220.144.159.200, and the **ip rcmd source-interface** command is used to specify that the source IP address for all rcp/rsh packets will be the IP address assigned to the Loopback0 interface:

```
interface Loopback0
  description Loopback interface
  ip address 220.144.159.200 255.255.255.255
```

Cisco IOS Configuration Fundamentals Command Reference ■

```
  no ip directed-broadcast
!
. . .
clock timezone GMT 0
ip subnet-zero
no ip source-route
no ip finger
ip rcmd source-interface Loopback0
ip telnet source-interface Loopback0
ip tftp source-interface Loopback0
ip ftp source-interface Loopback0
ip ftp username cisco
ip ftp password shhhhsecret
no ip bootp server
ip domain-name net.galaxy
ip name-server 220.144.159.1
ip name-server 220.144.159.2
ip name-server 219.10.2.1
!
. . .
```

Related Commands	Command	Description
	ip rcmd remote-host	Creates an entry for the remote user in a local authentication database so that remote users can execute commands on the router using rsh or rcp.

mop device-code

To identify the type of device sending Maintenance Operation Protocol (MOP) System Identification (sysid) messages and request program messages, use the **mop device-code** global configuration command. To set the identity to the default value, use the **no** form of this command.

> **mop device-code** {**cisco** | **ds200**}

> **no mop device-code** {**cisco** | **ds200**}

Syntax Description		
cisco	Denotes a Cisco device code.
ds200	Denotes a DECserver 200 device code.

Defaults   Cisco device code

Command Modes   Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines The sysid messages and request program messages use the identity information indicated by this command.

Examples   The following example identifies a DECserver 200 device as sending MOP sysid and request program messages:

```
mop device-code ds200
```

Related Commands

Command	Description
mop sysid	Enables an interface to send out periodic MOP system identification messages.

mop retransmit-timer

To configure the length of time that the Cisco IOS software waits before resending boot requests to a Maintenance Operation Protocol (MOP) server, use the **mop retransmit-timer** global configuration command. To reinstate the default value, use the **no** form of this command.

mop retransmit-timer *seconds*

no mop retransmit-timer

Syntax Description	*seconds*	Sets the length of time (in seconds) that the software waits before resending a message. The value is a number from 1 to 20.

Defaults 4 seconds

Command Modes Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines By default, when the software sends a request that requires a response from a MOP boot server and the server does not respond, the message is re-sent after 4 seconds. If the MOP boot server and router are separated by a slow serial link, it might take longer than 4 seconds for the software to receive a response to its message. Therefore, you might want to configure the software to wait longer than 4 seconds before resending the message if you are using such a link.

Examples In the following example, if the MOP boot server does not respond within 10 seconds after the router sends a message, the server will resend the message:

```
mop retransmit-timer 10
```

Related Commands

Command	Description
mop device-code	Identifies the type of device sending MOP sysid messages and requests program messages.
mop enabled	Enables an interface to support the MOP.

mop retries

To configure the number of times the Cisco IOS software will resend boot requests to a Maintenance Operation Protocol (MOP) server, use the **mop retries** global configuration command. To reinstate the default value, use the **no** form of this command.

mop retries *count*

no mop retries

Syntax Description

count	Indicates the number of times the software will resend a MOP boot request. The value is a number from 3 to 24.

Defaults

8 times

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

In the following example, the software will attempt to resend a message to an unresponsive host 11 times before declaring a failure:

```
mop retries 11
```

Related Commands

Command	Description
mop device-code	Identifies the type of device sending MOP sysid messages and requests program messages.
mop enabled	Enables an interface to support the MOP server.
mop retransmit-timer	Configures the length of time that the Cisco IOS software waits before resending boot requests to a MOP server.

rsh

To execute a command remotely on a remote rsh host, use the **rsh** privileged EXEC command.

rsh {*ip-address* | *host*} [**/user** *username*] *remote-command*

Syntax Description

ip-address	IP address of the remote host on which to execute the **rsh** command. Either the IP address or the host name is required.
host	Name of the remote host on which to execute the command. Either the host name or the IP address is required.
/user *username*	(Optional) Remote username.
remote-command	Command to be executed remotely.

Defaults   If you do not specify the **/user** *username* keyword and argument, the Cisco IOS software sends a default remote username. As the default value of the remote username, the software sends the username associated with the current tty process, if that name is valid. For example, if the user is connected to the router through Telnet and the user was authenticated through the **username** command, then the software sends that username as the remote username. If the tty username is invalid, the software uses the host name as the both the remote and local usernames.

> **Note**   For Cisco, tty lines are commonly used for access services. The concept of tty originated with UNIX. For UNIX systems, each physical device is represented in the file system. Terminals are sometimes called tty devices (tty stands for teletype, the original UNIX terminal).

Command Modes   Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines   Use the **rsh** command to execute commands remotely. The host on which you remotely execute the command must support the rsh protocol, and the .rhosts files on the rsh host must include an entry that permits you to remotely execute commands on that host.

For security reasons, the software does not default to a remote login if no command is specified, as does UNIX. Instead, the router provides Telnet and connect services that you can use rather than rsh.

Examples   The following command specifies that the user named sharon attempts to remotely execute the UNIX **ls** command with the *-a* argument on the remote host named mysys.cisco.com. The command output resulting from the remote execution follows the command example:

```
Router1# rsh mysys.cisco.com /user sharon ls -a
.
```

```
             ..
             .alias
             .cshrc
             .emacs
             .exrc
             .history
             .login
             .mailrc
             .newsrc
             .oldnewsrc
             .rhosts
             .twmrc
             .xsession
             jazz
```

show async bootp

To display the extended BOOTP request parameters that have been configured for asynchronous interfaces, use the **show async bootp** privileged EXEC command.

> **show async bootp**

Syntax Description   This command has no arguments or keywords.

Command Modes   Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples   The following is sample output from the **show async bootp** command:

```
Router# show async bootp

The following extended data will be sent in BOOTP responses:

bootfile (for address 192.168.1.1) "pcboot"
bootfile (for address 172.16.1.111) "dirtboot"
subnet-mask 255.255.0.0
time-offset -3600
time-server 192.168.1.1
```

Table 43 describes the significant fields shown in the display.

Table 43   show async bootp Field Descriptions

Field	Description
bootfile... "pcboot"	Boot file for address 192.168.1.1 is named pcboot.
subnet-mask 255.255.0.0	Subnet mask.
time-offset -3600	Local time is one hour (3600 seconds) earlier than UTC time.
time-server 192.168.1.1	Address of the time server for the network.

Related Commands

Command	Description
async-bootp	Configures extended BOOTP requests for asynchronous interfaces as defined in RFC 1084.

tftp-server

To configure a router or a Flash memory device on the router as a TFTP server, use one of the following **tftp-server** global configuration commands. This command replaces the **tftp-server system** command. To remove a previously defined filename, use the **no tftp-server** command with the appropriate filename.

> **tftp-server flash** [*partition-number***:**]*filename1* [**alias** *filename2*] [*access-list-number*]

> **tftp-server rom alias** *filename1* [*access-list-number*]

> **no tftp-server** {**flash** [*partition-number***:**]*filename1* | **rom alias** *filename2*}

Cisco 1600 Series and Cisco 3600 Series Routers

> **tftp-server flash** [*device***:**][*partition-number***:**]*filename*

> **no tftp-server flash** [*device***:**][*partition-number***:**]*filename*

Cisco 7000 Family Routers

> **tftp-server flash** *device***:***filename*

> **no tftp-server flash** *device***:***filename*

Syntax Description		
flash	Specifies TFTP service of a file in Flash memory.	
rom	Specifies TFTP service of a file in ROM.	
filename1	Name of a file in Flash or in ROM that the TFTP server uses in answering TFTP Read Requests.	
alias	Specifies an alternate name for the file that the TFTP server uses in answering TFTP Read Requests.	
filename2	Alternate name of the file that the TFTP server uses in answering TFTP Read Requests. A client of the TFTP server can use this alternate name in its Read Requests.	
access-list-number	(Optional) Basic IP access list number. Valid values are from 0 to 99.	
*partition-number***:**	(Optional) Specifies TFTP service of a file in the specified partition of Flash memory. If the partition number is not specified, the file in the first partition is used.	
	For the Cisco 1600 series and Cisco 3600 series routers, you must enter a colon after the partition number if a filename follows it.	

*device***:**	(Optional) Specifies TFTP service of a file on a Flash memory device in the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers. The colon is required. Valid devices are as follows:
	• **flash**—Internal Flash memory on the Cisco 1600 series and Cisco 3600 series routers. This is the only valid device for the Cisco 1600 series routers.
	• **bootflash**—Internal Flash memory in the Cisco 7000 family routers.
	• **slot0**—First PCMCIA slot on the Cisco 3600 series and Cisco 7000 family routers.
	• **slot1**—Second PCMCIA slot on the Cisco 3600 series and Cisco 7000 family.
	• **slavebootflash**—Internal Flash memory on the slave RSP card of a Cisco 7507 or Cisco 7513 router configured for HSA.
	• **slaveslot0**—First PCMCIA slot of the slave RSP card on a Cisco 7507 or Cisco 7513 router configured for HSA.
	• **slaveslot1**—Second PCMCIA slot of the slave RSP card on a Cisco 7507 or Cisco 7513 router configured for HSA.
filename	Name of the file on a Flash memory device that the TFTP server uses in answering a TFTP Read Request. Use this argument only with the Cisco 1600 series, Cisco 3600 series, Cisco 7000 series, or Cisco 7500 series routers.

Defaults Disabled

Command Modes Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines You can specify multiple filenames by repeating the **tftp-server** command. The system sends a copy of the system image contained in ROM or one of the system images contained in Flash memory to any client that issues a TFTP Read Request with this filename.

If the specified *filename1* or *filename2* argument exists in Flash memory, a copy of the Flash image is sent. On systems that contain a complete image in ROM, the system sends the ROM image if the specified *filename1* or *filename2* argument is not found in Flash memory.

Images that run from ROM cannot be loaded over the network. Therefore, it does not make sense to use TFTP to offer the ROMs on these images.

On the Cisco 7000 family routers, the system sends a copy of the file contained on one of the Flash memory devices to any client that issues a TFTP Read Request with its filename.

Examples In the following example, the system uses TFTP to send a copy of the version-10.3 file located in Flash memory in response to a TFTP Read Request for that file. The requesting host is checked against access list 22.

```
tftp-server flash version-10.3 22
```

In the following example, the system uses TFTP to send a copy of the ROM image gs3-k.101 in response to a TFTP Read Request for the gs3-k.101 file:

```
tftp-server rom alias gs3-k.101
```

In the following example, the system uses TFTP to send a copy of the version-11.0 file in response to a TFTP Read Request for that file. The file is located on the Flash memory card inserted in slot 0.

```
tftp-server flash slot0:version-11.0
```

The following example enables a Cisco 3600 series router to operate as a TFTP server. The source file c3640-i-mz is in the second partition of internal Flash memory.

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
router(config)# tftp-server flash flash:2:dirt/gate/c3640-i-mz
```

In the following example, the source file is in the second partition of the Flash memory PC card in slot 0 on a Cisco 3600 series:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
router(config)# tftp-server flash slot0:2:dirt/gate/c3640-j-mz
```

The following example enables a Cisco 1600 series router to operate as a TFTP server. The source file c1600-i-mz is in the second partition of Flash memory:

```
router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
router(config)# tftp-server flash flash:2:dirt/gate/c1600-i-mz
```

Related Commands

Command	Description
access-list	Creates an extended access list.

tftp-server system

The tftp-**server system** command has been replaced by the **tftp-server** command. See the description of the **tftp-server** command in this chapter for more information.