

## Configuring SLIP and PPP

---

This chapter describes how to configure asynchronous interfaces for telecommuting applications using Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP) encapsulation. See the *Communication Server Command Reference* for a complete description of the commands listed in this chapter.

Refer to the *Communication Server and Protocol Translator Connection Guide* for information about EXEC user commands and establishing SLIP and PPP connections.

### Cisco's Implementation of SLIP and PPP

SLIP and PPP define methods of sending Internet Protocol (IP) packets over standard RS-232 asynchronous serial lines with minimum line speeds of 1200 baud.

Using SLIP or PPP encapsulation over asynchronous lines is an inexpensive way of connecting PCs to a network. SLIP and PPP over asynchronous dial-up modems allow a home computer to be connected to a network without the cost of a leased line. Dial-up SLIP and PPP links can also be used for remote sites that need only occasional telecommuting or backup connectivity. Both public-domain and vendor-supported SLIP and PPP implementations are available for a variety of computer applications.

The communication server concentrates a large number of SLIP or PPP PC or workstation client hosts onto a network interface allowing the PCs to communicate with any host on the network. The communication server can support any combination of SLIP or PPP lines and lines dedicated to normal asynchronous devices such as terminals and modems. Refer to RFC 1055 for more information about SLIP, and RFCs 1331 and 1332 for more information about PPP.

PPP is a newer, more robust protocol than SLIP and it contains protocols that can detect or prevent misconfiguration. SLIP is an older protocol that is supported on more machines.

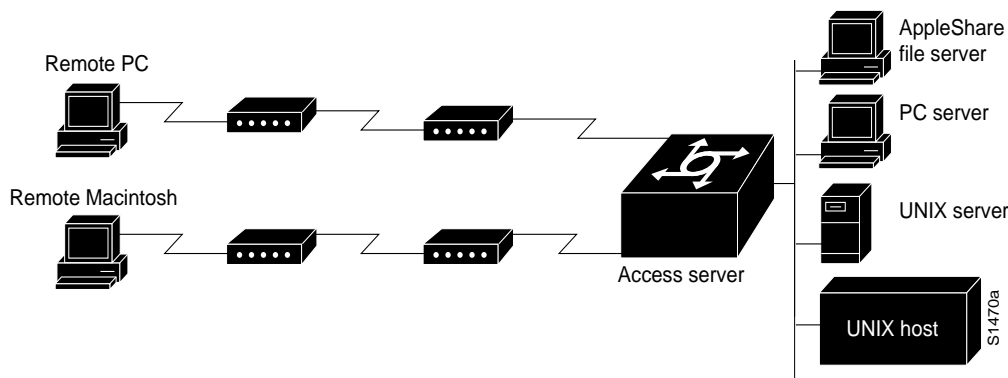
---

**Note** Most asynchronous serial links have very low bandwidth. Take care to configure your system so the links will not be overloaded. Consider using default routes and filtering routing updates to prevent them from being sent on these lines.

---

Figure 1-1 illustrates a typical asynchronous SLIP or PPP telecommuting configuration.

Figure 1-1 Sample SLIP or PPP Telecommuting Configuration



**Note** SLIP and PPP are not supported over X.25.

## Responding to BootP Requests

There is an asynchronous BootP server in your communication server. That means that SLIP and PPP clients can send BootP requests to the communication server, and the communication server will respond with information about the network. For example, the client can send a BootP request to find out what its IP address is and where the boot file is located, and the communication server can respond with the information.

BootP allows a client machine to discover its own IP address, the address of the communication server, and the name of a file to be loaded into memory and executed. There are typically two phases to using BootP: first, the client's address is determined and the bootfile is selected; then the file is transferred, typically using TFTP.

BootP compares to RARP as follows: Reverse Address Resolution Protocol (RARP) is an older protocol that allows a client to determine its IP address if it knows its hardware address. (See the "Configuring IP," and "Configuring IP Routing Protocols" chapters in this manual for more information about RARP.) However, RARP is a hardware link protocol, so it can only be implemented on hosts that have special kernel or driver modifications that allow access to these raw packets. BootP does not require kernel modifications.

BootP supports the extended BootP requests specified in RFC 1084 and works for both SLIP and PPP encapsulation.

## Asynchronous Network Connections and Routing

Line configuration commands configure a connection to a terminal or a modem. Interface configuration (**async**) commands described in this chapter configure a line as an asynchronous network interface over which networking functions are performed.

Your communication server also supports IP routing connections for communication that requires connecting one network to another.

If asynchronous dynamic routing is enabled, you can enable routing at the user level by using the **routing** keyword with the **slip** or **ppp** EXEC command.

---

**Note** See the “Configuring IP” chapter in this publication for additional information about how to configure TCP/IP for terminal connections and routing.

---

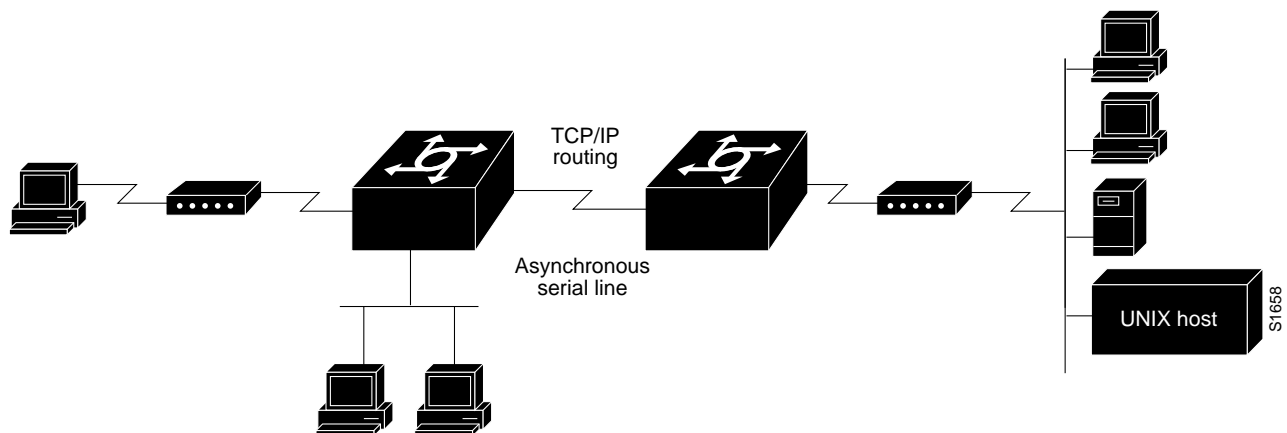
Asynchronous interfaces offer both dedicated and dynamic address assignment, configurable hold queues and IP packet sizes, extended BootP requests, and permit and deny conditions for controlling access to lines. Figure 1-2 shows a sample asynchronous routing configuration.

---

**Note** Disable software flow control on SLIP and PPP lines.

---

Figure 1-2 Sample Asynchronous Routing Configuration



## Asynchronous Interfaces and Broadcasts

Communication servers recognize a variety of Internet broadcast addresses. When a communication server receives an Internet packet from an asynchronous client, it rebroadcasts the packet onto the network without changing the Internet header. The communication server does not alter the packet's broadcast address to match the form of broadcast address it prefers.

The communication server receives a copy of asynchronous client broadcasts, and responds to BootP requests with the current IP address assigned to the asynchronous interface on which the request was received. This facility allows the asynchronous client software to automatically determine its own Internet address.

## Telecommuting Configuration Task List

To configure your communication server to support telecommuting, you must perform the first task in the following list on your asynchronous interfaces. Perform the rest of the tasks to customize the asynchronous interface for your particular network environment and to monitor asynchronous connections:

- Configure asynchronous interfaces
- Optimize available bandwidth
- Specify the maximum transmission unit (MTU) size of Internet packets
- Modify the IP output queue size
- Specify IP access lists
- Configure support for extended BootP requests
- Monitor and maintain asynchronous interfaces

The steps to perform these tasks are described in the following sections. See the “Asynchronous Interface Configuration Examples” section at the end of this chapter for examples of asynchronous configuration files. Tasks are performed in global configuration mode unless otherwise specified.

## Configure Asynchronous Interfaces

To configure your communication server to support telecommuting, configure basic functionality on your asynchronous interfaces, and then customize the interfaces for your environment. Basic configuration tasks include the following:

- Step 1** Specify an asynchronous interface
- Step 2** Configure SLIP or PPP encapsulation
- Step 3** Specify dedicated or interactive mode
- Step 4** Configure the asynchronous addressing method
- Step 5** Assign IP addresses for local devices
- Step 6** Enable asynchronous routing
- Step 7** Make SLIP and PPP connections at the EXEC level if you have configured interactive mode. See the *Communication Server and Protocol Translator Connection Guide* for more information about making SLIP and PPP connections.

---

**Note** In Release 9.1, SLIP was configured and monitored using **slip** line, EXEC, and debug commands. In this release, SLIP and PPP asynchronous interfaces are configured using **async** commands in interface command mode. See the release note for a table listing old and new commands.

---

## Specify an Asynchronous Interface

Perform the following task in global configuration mode to specify an asynchronous interface.

Task	Command
Specify an asynchronous interface.	<b>interface async unit</b>

## Configuring SLIP or PPP Encapsulation

SLIP and PPP are methods of encapsulating datagrams and other network-layer protocol information over point-to-point links. Perform the following task in interface configuration mode to configure the default encapsulation on an asynchronous interface.

Task	Command
Configure PPP or SLIP encapsulation on an asynchronous line.	<b>encapsulation {ppp   slip}</b>

In order to use SLIP or PPP, the communication server must be configured with an IP routing protocol or with the **ip host-routing** command. This configuration is done automatically if you are using old-style **slip address** commands. However, you must configure it manually if you configure SLIP or PPP via the **interface async** command.

## Specify Dedicated or Interactive Mode

You can configure one or more asynchronous interfaces on your communication server to be in dedicated network interface mode. In dedicated mode, an interface is automatically configured for SLIP or PPP connections. There is no user prompt or EXEC level, and no end-user commands are required to initiate telecommuting connections. If you want a line to be used only for SLIP or PPP connections, configure the line for dedicated mode.

In interactive mode, a line can be used to make any type of connection, depending on the EXEC command entered by the user. For example, depending on its configuration, the line could be used for Telnet or XRemote connections, or SLIP or PPP encapsulation. The user is prompted for an EXEC command before a connection is initiated.

## Configure Dedicated Network Mode

You can configure an asynchronous interface to be in dedicated network mode. When the interface is configured for dedicated mode, the end user cannot change the encapsulation method, address, or other parameters.

Perform the following task in interface configuration mode to configure an interface for dedicated network mode.

Task	Command
Place the line into dedicated asynchronous network mode.	<b>async mode dedicated</b>

See the “Managing the System” chapter for more information about automatic dialing using DTR.

## Return a Line to Interactive Mode

After a line has been placed in dedicated mode, perform the following task to return it to interactive mode.

Task	Command
Return the line to interactive mode.	<b>async mode interactive</b>

By default, no asynchronous mode is configured. In this state, the line is not available for inbound networking because the SLIP and PPP connections are disabled.

## Configure the Interface Addressing Method for Remote Device

You can control whether addressing is dynamic (the user specifies the address at the EXEC level when making the connection), or whether default addressing is used (the address is forced by the system). If you specify dynamic addressing, the communication server must be in interactive mode and the user will enter the address at the EXEC level.

It is common to configure an asynchronous interface to have a default address and to allow dynamic addressing. With this configuration, the choice between the default address or a dynamic addressing is made by the user when they enter the **slip** or **ppp** EXEC command. If the user enters an address, it is used, and if the user enters the **default** keyword, the default address is used.

This section describes the following tasks:

- Assign a default asynchronous address
- Allow an asynchronous address to be assigned dynamically

### Assign a Default Asynchronous Address

Perform the following task in interface configuration mode to assign a permanent default asynchronous address:

Task	Command
Assign a default IP address to an asynchronous interface.	<b>async default ip address</b> <i>address</i>

Use the **no** version of this command to disable the default address. If the server has been configured to authenticate asynchronous connections, you are prompted for a password after entering the SLIP or PPP EXEC command before the line is placed into asynchronous mode.

The assigned default address is implemented when the user enters the **slip default** or **ppp default** EXEC command. The transaction is validated by the TACACS server (when enabled) and the line is put into network mode using the address that is in the configuration file.

Configuring a default address useful when the user is not required to know the IP address to gain access to a system; for example, users of a server that is available to many students on a campus. Instead of requiring each user to know an IP address, they need only enter the **slip default** or **ppp default** EXEC command and let the server select the address to use. See the *Communication Server and Protocol Translator Connection Guide* for more information about the **slip** and **ppp** EXEC commands.

### Allow an Asynchronous Address To Be Assigned Dynamically

When a line is configured for dynamic assignment of asynchronous addresses, the user enters the **slip** or **ppp** EXEC command and is prompted for an address or logical host name. The address is validated by the Terminal Access Controller Access System (TACACS), when enabled, and the line is assigned the given address and put into asynchronous mode. Assigning asynchronous addresses dynamically is also useful when you want to assign set addresses to users. For example, an application on a personal computer that automatically dials in using SLIP and polls for electronic mail messages can be set up to dial in periodically and enter the required IP address and password.

Perform the following task in interface configuration mode:

Task	Command
Allow the IP address to be assigned when the protocol is initiated.	<b>async dynamic address</b>

The dynamic addressing features of the internetwork allow packets to get to their destination and back regardless of the communication server or network they are sent from. For example, if a host such as a laptop computer moves from place to place it can keep the same address no matter where it is dialing in from.

Logical host names are first converted to uppercase and then sent to the TACACS server for authentication.

## Assign IP Addresses for Local Devices

The local address is set using the **ip address** or **ip unnumbered** command.

IP addresses identify locations to which IP datagrams can be sent. You must assign each router interface an IP address. See the *Internetworking Technology Overview* publication for detailed information on IP addresses.

To assign an IP address to a network interface on the communication server, enter an IP address and a subnet mask:

Task	Command
Set an IP address for an interface.	<b>ip address</b> <i>address mask</i> [ <b>secondary</b> ]

A subnet mask identifies the subnet field of a network address. Subnets are described in the *Internetworking Technology Overview* manual.

## Conserve Network Addresses

When asynchronous routing is enabled, you might find it necessary to conserve network addresses by configuring the asynchronous interfaces as *unnumbered*. An unnumbered interface does not have an address. Network resources are therefore conserved because fewer network numbers are used and routing tables are smaller.

Perform the following task in interface configuration mode to configure an unnumbered interface.

Task	Command
Configure the asynchronous interface to be unnumbered.	<b>ip unnumbered</b> <i>interface-name</i>

Whenever the unnumbered interface generates a packet (for example, a routing update), it uses the address of the specified interface as the source address of the IP packet. It also uses the address of the specified interface to determine which routing processes are sending updates over the unnumbered interface.

You can use the IP unnumbered feature on the communication server whether or not the system on the other end of the asynchronous link supports this feature. The IP unnumbered feature is transparent to the other end of the link because each system bases its routing activities on information in the routing updates it receives and on its own interface address on the link.

## Enable Asynchronous Routing

To route IP packets, perform the following task in interface configuration mode to enable routing protocols IGRP, RIP, and OSPF, on an interface.

Task	Command
Configure an asynchronous interface for routing.	<b>async dynamic routing</b>

When the user makes a connection, they must specify **/routing** on the SLIP or PPP command line.

## Optimize Available Bandwidth

Asynchronous lines have relatively low bandwidth and can easily be overloaded, resulting in slow traffic across these lines.

To optimize available bandwidth, perform any of the following tasks:

- Configure header compression
- Force header compression at the EXEC level

## Configure Header Compression

One way to optimize available bandwidth is by using TCP header compression. Van Jacobson TCP header compression (defined by RFC 1144) can increase bandwidth availability between two and five times when compared to lines not using header compression. Theoretically, it can improve bandwidth availability by a ratio of seven to one.

Perform the following task in interface configuration mode to configure header compression:

Task	Command
Configure Van Jacobson TCP header compression on the asynchronous link.	<b>ip tcp header-compression [on   off   passive]</b>

## Force Header Compression at the EXEC Level

On SLIP interfaces, you can force header compression at the EXEC prompt on a line on which header compression has been set to passive. This allows more efficient use of the available bandwidth and does not require entering privileged configuration mode.

Perform the following task to implement header compression:

Task	Command
Allow status of header compression to be assigned at the user level.	<b>ip tcp header compression passive</b>

For PPP interfaces, the **passive** option functions the same as the **on** option.

See the *Communication Server and Protocol Translator Connection Guide* for information about the **slip** and **ppp** EXEC commands. You cannot force header compression if header compression on the asynchronous interface is off.



## Specify the MTU Size of Internet Packets

The maximum transmission unit (MTU) refers to the size of an IP packet. You might want to change to a smaller MTU size for any of the following reasons:

- The SLIP or PPP application at the other end only supports packets up to a certain size.
- You want to assure a shorter delay by using smaller packets.
- The host Telnet echoing takes longer than 0.2 seconds.

For example, at 9600 baud a 1500 byte packet takes about 1.5 seconds to transmit. This delay would indicate that you want an MTU size of about 200 ( $1.5 \text{ seconds} / 0.2 \text{ seconds} = 7.5$  and  $1500 \text{ byte packet} / 7.5 = 200 \text{ byte packet}$ ).

Perform the following task in interface configuration mode to specify maximum IP packet size:

Task	Command
Specify the size of the largest Internet packet that the asynchronous line can support.	<b>ip mtu bytes</b>

The MTU size can be negotiated by TCP, regardless of the asynchronous interface settings. In other words, TCP running on the device to which the communication server is connected can negotiate for a different MTU size than is configured on the communication server. The communication server performs IP fragmentation of packets larger than the specified MTU. Do not change the MTU size unless the SLIP or PPP implementation running on the host at the other end of the asynchronous line supports reassembly of IP fragments. Because each fragment occupies a spot in the output queue, it might also be necessary to increase the size of the SLIP or PPP hold queue, if your MTU size is such that you might have a high amount of fragments of packets in the output queue.

## Modify the IP Output Queue Size

The IP output queue stores packets received from the network that are waiting to be sent to the asynchronous client. You can limit the size of the IP output queue to enhance performance by performing the following task in interface configuration mode:

Task	Command
Change the size of the IP output hold queue.	<b>hold-queue packets</b>

## Specify IP Access Lists

Access lists allow the system administrator to control the hosts that a PC can access through a communication server. Separate access lists can be defined for asynchronous and for other connections.

The tasks described in this section are as follows:

- Define access control on packets from the IP host
- Define access control on packets to the IP host

See the “Configuring IP” chapter for information about defining IP access lists.

You can define an access list for packets from the IP host by performing the following task in interface configuration mode.

Task	Command
Configure an access list for packets <i>from</i> the IP host.	<b>ip access-group <i>access-list-number</i> in</b>

You can define an access list for packets to the IP host by performing the following task in interface configuration mode.

Task	Command
Configure an access list for packets being sent <i>to</i> the IP host.	<b>ip access-group <i>access-list-number</i> out</b>

## Configure Support for Extended BootP Requests

Perform the following task in global configuration mode to configure your communication server support to respond to BootP requests from client machines:

Task	Command
Specify the communication server network information that will be sent in response to response to BootP requests.	<b>async-bootp tag [<i>:hostname</i>] <i>data...</i></b>

## Monitor and Maintain Asynchronous Interfaces

This section describes the following monitoring and maintenance tasks:

- Monitor and maintain asynchronous activity
- Debug asynchronous interfaces
- Debug PPP

You can monitor and maintain asynchronous activity in the following ways in privileged EXEC mode:

Task	Command
Return a line to its idle state.	<b>clear line <i>line-number</i></b>
Display parameters that have been set for extended BootP requests.	<b>show async bootp</b>
Display statistics for asynchronous activity.	<b>show async status</b>
Display the status of asynchronous line connections.	<b>show line [<i>line-number</i>]</b>

Perform the following task in privileged EXEC mode to debug asynchronous interfaces:

Task	Command
Displays errors, changes in interface state, and log input and output.	<b>debug async { <b>framing</b>   <b>state</b>   <b>packets</b> }</b>

Perform the following task in privileged EXEC mode to debug PPP links:

Task	Command
Enable debugging of PPP protocol negotiation process.	<b>debug ppp negotiation</b>
Display PPP protocol errors.	<b>debug ppp error</b>
Display PPP packets sent and received.	<b>debug ppp packet</b>
Display errors encountered during remote or local system authentication. <sup>1</sup>	<b>debug ppp chap</b>

1. See the “Configuring Dial-on-Demand Routing” chapter in this publication or more information about the Challenge Handshake Authentication Protocol (CHAP).

## Asynchronous Interface Configuration Examples

This section contains asynchronous configuration examples. Each configuration is designed to illustrate different communication requirements.

- Configuring a Dedicated Asynchronous Interface
- Restricting Access on an Asynchronous Interface
- Configuring Asynchronous Routing and Dynamic Addressing
- Configuring TCP Header Compression
- Conserving Network Addresses Using the IP Unnumbered Feature
- Configuring Routing on a Dedicated Dial-In Router
- Configuring an Asynchronous Interface as the Only Network Interface
- Configuring IGRP Routing Protocol
- Configuring an Interface

### Example of Configuring a Dedicated Asynchronous Interface

The following example assigns an IP address to an asynchronous interface and places the line in dedicated network mode. Setting the stop bit to 1 is a performance enhancement.

```

!
line 20
location Department PC Lab
stopbits 1
speed 19200
!
interface async 20
async default ip address 182.32.7.51
async mode dedicated
!

```

---

**Note** The interface number is the same as the absolute line number, in decimal format. The 500-CS defaults to decimal numbers. To display line numbers in decimal rather than octal format on the ASM-CS, use the **service decimal-tty** command. See the “System Management Commands” chapter in the *Communication Server Command Reference* for a description of the **service decimal-tty** command.

---

### Example of Restricting Access on an Asynchronous Interface

The following example assumes that users are restricted to certain servers designated as asynchronous servers, but that normal terminal users can access anything on the local network.

```
! access list for normal connections
access-list 1 permit 131.108.0.0 0.0.255.255
!
access-list 2 permit 131.108.42.55
access-list 2 permit 131.108.111.1
access-list 2 permit 131.108.55.99
!
interface async 6
async dynamic address
ip access-group 1 out
ip access-group 2 in
```

### Example of Configuring Asynchronous Routing and Dynamic Addressing

The following example shows a simple configuration that allows routing and dynamic addressing. With this configuration, if the user specifies **/routing** in the EXEC **slip** or **ppp** command, routing protocols will be sent and received.

```
interface async 6
async dynamic routing
async dynamic address
```

### Example of Configuring TCP Header Compression

The following example configures asynchronous interface 7 with a default IP address, allowing header compression if it is specified in the **slip** or **ppp** connection command entered by the user, or if the connecting system sends compressed packets.

```
interface async 7
ip address 150.136.79.1
async default ip address 150.136.79.2
ip tcp header-compression passive
```

### Example of Conserving Network Addresses Using the IP Unnumbered Feature

The following example shows how to configure your communication server for routing using unnumbered interfaces. The source (local) address is shared between ethernet 0 and async 6 (128.66.1.1). The default remote address is 128.66.1.2.

```
interface ethernet 0
ip address 128.66.1.1 255.255.255.0
!
interface async 6
ip unnumbered ether 0
async dynamic routing
! default address is on the local subnet
async dynamic address
async default ip address 128.66.1.2
ip tcp header-compression passive
```

The following example shows how the IP unnumbered configuration works. Although the user assigned an address, the system response shows the interface as unnumbered, and the address typed by the user will be used only in response to BootP requests.

```
cs> slip /compressed 1.1.1.1
Password:
Entering async mode.
Interface IP address is unnumbered, MTU is 1500 bytes.
Header compression is On.
```

## Example of Configuring Routing on a Dedicated Dial-In Router

In the following example, the communication server is set up as a dedicated dial-in router. Interfaces are configured as IP unnumbered to conserve network resources, primarily IP addresses.

```
ip routing
interface ether 0
ip address 1.0.1.1 255.255.255.0
!
interface async 1
ip unnumbered ether 0
async dynamic routing
! The addresses assigned with SLIP or PPP EXEC commands are not used except
! to reply to BootP requests.
! Normally, the routers dialing in will have their own address
! and not use BootP at all.
async default ip address 1.0.2.1
interface async 2
async default ip address 1.0.5.1
ip tcp header-compression passive
async mode dedicated
!
! run RIP on the asynchronous lines, because few implementations of SLIP
! understand IGRP. Run IGRP on the ethernet (and in the local network).
!
router igrp 109
network 1.0.0.0
! send routes from the asynchronous lines on the production network.
redistribute RIP
! don't send IGRP updates on the async interfaces
passive-interface async 1
!
router RIP
network 1.0.0.0
redistribute igrp
passive-interface ethernet 0
! consider filtering everything except a default route from the routing
! updates sent on the (slow) asynchronous lines
distribute-list 1 out
ip unnumbered async 2
async dynamic routing
```

## Example of Configuring an Asynchronous Interface as the Only Network Interface

In the following example, one of the asynchronous lines is used as the only network interface. The communication server is used primarily as a terminal server, but is at a remote location and dials into the central site for its only network connection.

```
ip default-gateway 1.0.0.2
interface ethernet 0
shutdown
interface async 1
async dynamic routing
ip tcp header-compression on
async default ip address 1.0.5.1
async mode dedicated
ip address 1.0.0.1 255.255.255.0
!
```

## Example of Configuring the IGRP Routing Protocol

In the following example, only the IGRP TCP/IP routing protocol is running; it is assumed that the systems that are dialing in to use routing will either support IGRP or have some other method (for example, a static default route) of determining that the communication server is the best place to send most of its packets.

```
router igrp 109
network 1.0.0.0
interface ether 0
ip address 1.0.0.1 255.255.255.0
!
interface async 1
async default ip address 1.0.0.101
async dynamic routing
ip tcp header-compression passive
ip unnumbered ethernet 0

line 1
modem ri-is-cd
```

## Example of Configuring an Interface

The following configuration shows interface and line configuration. The interface is configured with access lists, passive header compression and a default address. The line is configured for TACACS authentication.

```
interface async 1
ip access-group 1 in
ip access-group 1 out
ip tcp header-compression passive
async default ip address 128.148.176.201

line 1
login tacacs
location 457-5xxx
exec-timeout 20 0
password XXXXXXXX
session-timeout 20
stopbits 1
```