



Configuring Virtual Asynchronous Traffic over ISDN

Cisco IOS software offers two solutions to send virtual asynchronous traffic over ISDN:

- Using International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Recommendation V.120, which allows for reliable transport of synchronous, asynchronous, or bit transparent data over ISDN bearer channels.
- Using ITU-T Recommendation X.75, which allows a system with an ISDN terminal adapter supporting asynchronous traffic over Link Access Procedure, Balanced (LAPB) to call into a router and establish an asynchronous PPP session. This method of asynchronous traffic transmission is also called ISDN Link Access Procedure, Balanced-Terminal Adapter (LAPB-TA).

A virtual asynchronous interface (also known as vty-async) is created on demand to support calls that enter the router through a nonphysical interface. For example, asynchronous character stream calls terminate or land on nonphysical interfaces. These types of calls include inbound Telnet, local-area transport (LAT), PPP over character-oriented protocols (such as V.120 or X.25), and LAPB-TA and packet assembler/disassembler (PAD) calls.

Virtual asynchronous interfaces are not user configurable; rather, they are dynamically created and torn down on demand. A virtual asynchronous line is used to access a virtual asynchronous interface. Refer to the section “Virtual Asynchronous Interfaces” in the chapter “Interfaces, Controllers, and Lines Used for Dial Access Overview” in this publication for more overview information about virtual asynchronous interfaces. Refer to the section “Enabling Asynchronous Functions on Virtual Terminal Lines” in the chapter “Configuring Protocol Translation and Virtual Asynchronous Devices” in this publication for additional virtual asynchronous interface configuration information.

This chapter describes how to configure virtual asynchronous traffic over ISDN lines. It includes the following main sections:

- Recommendation V.120 Overview
- V.120 Access Configuration Task List
- V.120 Configuration Example
- ISDN LAPB-TA Overview
- ISDN LAPB-TA Configuration Task List
- ISDN LAPB-TA Configuration Examples

For a complete description of the commands mentioned in this chapter, see the *Cisco IOS Dial Services Command Reference* publication. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Recommendation V.120 Overview

The V-series recommendations are ITU-T standards dealing with data communications over telephone networks. V.120 allows for reliable transport of synchronous, asynchronous, or bit transparent data over ISDN bearer channels. Cisco provides three V.120 support features for terminal adapters that do not send the low-layer compatibility fields or bearer capability V.120 information:

- Answer all incoming calls as V.120—Static configuration used when all remote users have asynchronous terminals and need to connect with a vty on the router.
- Automatically detect V.120 encapsulation—Encapsulation dynamically detected and set.
- Enable V.120 Support for Asynchronous Access over ISDN.

For terminal adapters that send the low-layer compatibility or bearer capability V.120 information, mixed V.120 and ISDN calls are supported. No special configuration is required.

V.120 Access Configuration Task List

Perform the tasks in the following sections to configure V.120 access:

- Configuring Answering of All Incoming Calls as V.120 (Required)
- Configuring Automatic Detection of Encapsulation Type (Required)
- Enabling V.120 Support for Asynchronous Access over ISDN (Required)

See the section “V.120 Configuration Example” at the end of this chapter for an example of how to configure V.120 access.

Configuring Answering of All Incoming Calls as V.120

This V.120 support feature allows users to connect using an asynchronous terminal over ISDN terminal adapters with V.120 support to a vty on the router, much like a direct asynchronous connection. Beginning with Cisco IOS Release 11.1, this feature supports incoming calls only.

When all the remote users have asynchronous terminals and call in to a router through an ISDN terminal adapter that uses V.120 encapsulation but does not send the low-layer compatibility or bearer capability V.120 information, you can configure the interface to answer all calls as V.120. Such calls are connected with an available vty on the router.

To configure an ISDN BRI or PRI interface to answer all incoming calls as V.120, use the following commands beginning in global configuration mode:

Command	Purpose
<pre>interface bri number (Cisco 4000 series) interface bri slot/port (Cisco 7200 series) or interface serial e1 controller-number:15 interface serial t1 controller-number:23</pre>	Specifies the ISDN BRI interface.
<pre>interface serial e1 controller-number:15 interface serial t1 controller-number:23</pre>	Specifies the ISDN PRI D channel.
<pre>isdn all-incoming-calls-v120</pre>	Configures the interface to answer all calls as V.120.

Configuring Automatic Detection of Encapsulation Type

If an ISDN call does not identify the call type in the lower-layer compatibility fields and is using an encapsulation that is different from the one configured on the interface, the interface can change its encapsulation type dynamically.

This feature enables interoperability with ISDN terminal adapters that use V.120 encapsulation but do not signal V.120 in the call setup message. An ISDN interface that by default answers a call as synchronous serial with PPP encapsulation can change its encapsulation and answer such calls.

Automatic detection is attempted for the first 10 seconds after the link is established or the first 5 packets exchanged over the link, whichever is first.

To enable automatic detection of V.120 encapsulation, use the following command in interface configuration mode:

Command	Purpose
<code>autodetect encapsulation v120</code>	Enables automatic detection of encapsulation type on the specified interface.

You can specify one or more encapsulations to detect. Cisco IOS software currently supports automatic detection of PPP and V.120 encapsulations.

Enabling V.120 Support for Asynchronous Access over ISDN

You can optionally configure a router to support asynchronous access over ISDN by globally enabling PPP on vty lines. Asynchronous access is then supported over ISDN from the ISDN terminal to the vty session on the router.

To enable asynchronous protocol features on vty lines, use the following command in global configuration mode:

Command	Purpose
<code>vty-async</code>	Configures all vty lines to support asynchronous protocol features.

This task enables PPP on vty lines on a global basis on the router. If you prefer instead to configure PPP on a per-vty basis, use the **translate** command, which is described in the *Cisco IOS Dial Services Command Reference* publication.

V.120 Configuration Example

The following example configures BRI 0 to call and receive calls from two sites, to use PPP encapsulation on outgoing calls, and to use Challenge Handshake Authentication Protocol (CHAP) authentication on incoming calls. This example also enables BRI 0 to configure itself dynamically to answer calls that use V.120 but that do not signal V.120 in the call setup message.

```
interface bri 0
  encapsulation ppp
  autodetect encapsulation v120
  no keepalive
  dialer map ip 131.108.36.10 name EB1 234
  dialer map ip 131.108.36.9 name EB2 456
  dialer-group 1
  ppp authentication chap
```

ISDN LAPB-TA Overview

To carry asynchronous traffic over ISDN, your system must be able to convert that traffic and forward it over synchronous connections. This process can be implemented by the V.120 protocol, which carries asynchronous traffic over ISDN. However, several countries in Europe (Germany, Switzerland, and some Eastern European countries) use LAPB as the protocol to forward their asynchronous traffic over synchronous connections. Your system, therefore, must be able to recognize and accept calls from these asynchronous/synchronous conversion devices. LAPB-TA performs that function. (LAPB is sometimes referred to as “X.75,” because LAPB is the link layer specified in the ITU-T X.75 recommendation for carrying asynchronous traffic over ISDN.)

LAPB-TA allows devices that use LAPB instead of the V.120 protocol to communicate with routers on the Cisco 3600 and 5300 series.

LAPB supports both local CHAP authentication and external RADIUS authorization on the authentication, authorization, and accounting (AAA) server.

Before configuring ISDN LAPB-TA in your network, observe these restrictions:

- LAPB-TA does not currently support the ability to set a maximum frame size per user.
- Outbound LAPB-TA calls are not supported.
- PPP over LAPB-TA (and V.120) connections impose a greater overhead on the router than synchronous PPP over ISDN. The number of simultaneous sessions can be limited by dedicating a pool of virtual terminals to these protocols and limiting the number of virtual terminals in the pool.
- Multilink PPP compression is not supported.

ISDN LAPB-TA Configuration Task List

ISDN LAPB-TA is supported on the Cisco 3600 series and Cisco 5300 series routers that meet the following additional requirements:

- A virtual terminal must be configured for incoming LAPB-TA. If no appropriately configured virtual terminals are available, the incoming call will be cleared.
- ISDN, LAPB, and PPP must be running to configure LAPB-TA.
- The Cisco IOS software must include the **vtty-async** global configuration command, which must be configured before you can run asynchronous PPP traffic over a LAPB-TA connection.

If an interface is already configured for V.120, only the following two additional configuration commands are required on the interface because V.120 and LAPB-TA sessions are configured in a similar way:

- Use the **autodetect encapsulation** command to enable autodetection of LAPB-TA connections.
- Use the **transport input** command to list LAPB-TA as an acceptable transport on a specific router.

Perform the following required task to configure LAPB-TA: Configuring ISDN LAPB-TA (required).

Procedures for verifying the configuration are found in the section “Verifying ISDN LAPB-TA” later in this chapter. The section “ISDN LAPB-TA Configuration Examples” at the end of this chapter provides configuration examples.

Configuring ISDN LAPB-TA

To configure ISDN LAPB-TA, use the following commands beginning in global configuration command mode:

	Command	Purpose
Step 1	<code>Router(config)# vty-async</code>	Creates a virtual asynchronous interface.
Step 2	<code>Router(config)# vty-async virtual-template 1</code>	Applies virtual template to the virtual asynchronous interface.
Step 3	<code>Router(config)# interface virtual-template 1</code>	Creates a virtual interface template, and enters interface configuration mode.
Step 4	<code>Router(config-if)# ip unnumbered Ethernet0</code>	Assigns an IP address to the virtual interface template.
Step 5	<code>Router(config-if)# encapsulation ppp</code>	Enables encapsulation on the virtual interface template.
Step 6	<code>Router(config-if)# no peer default ip address</code>	Disables an IP address from a pool to the device connecting to the virtual access interface
Step 7	<code>Router(config-if)# ppp authentication chap</code>	Enables the CHAP protocol for PPP authentication.
Step 8	<code>Router(config-if)# exit</code>	Exits to global configuration mode.
Step 9	<code>Router(config)# username user1 password home</code>	Specifies CHAP password to be used to authenticate calls from caller “user1.”
Step 10	<code>Router(config)# interface Serial10:236</code>	Enters interface configuration mode for a D-channel serial interface. ¹
Step 11	<code>Router(config-if)# encapsulation ppp</code>	Configures PPP encapsulation as the default.

	Command	Purpose
Step 12	Router(config-if)# dialer-group 1	Specifies the dialer group belonging to the interface.
Step 13	Router(config-if)# ppp authentication chap	Enables the CHAP protocol for PPP authentication.
Step 14	Router(config-if)# autodetect encapsulation lapb-ta	Enables autodetect encapsulation for LAPB-TA protocols.
Step 15	Router(config)# line vty 0 32	Configures a range of 32 vty lines starting with vty0.
Step 16	Router(config-line)# transport input telnet lapb-ta	Defines which protocol to use to connect to a specific line of the access server.

1. The D channel is the signalling channel.

Verifying ISDN LAPB-TA

Enter the **show running configuration** command to verify that LAPB-TA is configured. The following output shows LAPB-TA enabled for interface serial0:23:

```
Router# show running configuration

Building configuration...

Current configuration:
!
version 12.0
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname Router
...(output omitted)

interface Serial0:23
description ENG PBX BRI num.:81063
no ip address
no ip directed-broadcast
encapsulation ppp
no ip route-cache
dialer pool-member 1
autodetect encapsulation ppp lapb-ta
isdn switch-type primary-5ess
no peer default ip address
no fair-queue
no cdp enable
ppp authentication chap
...(output omitted)
!
end
```

ISDN LAPB-TA Configuration Examples

The following example configures a virtual template LAPB-TA connection capable of running PPP. It assumes you have already configured usernames and passwords for PPP authentication.

```
vty-async
vty-async virtual-template 1
interface virtual-template 1
 ip unnumbered Ethernet0
 encapsulation ppp
 no peer default ip address
 ppp authentication chap
 exit
interface Serial0:23
 autodetect encapsulation lapb-ta
```

The following example treats the LAPB-TA and V.120 calls identically, by immediately starting a PPP session without asking for username and password, and relying on PPP authentication to identify the caller:

```
vty-async
vty-async virtual-template 1
interface Loopback0
 ip address 10.2.2.1 255.255.255.0
 exit
interface BRI3/0
 encapsulation ppp
 autodetect encapsulation ppp lapb-ta v120
 exit
interface Virtual-Template1
 ip unnumbered Loopback0
 ppp authentication chap
 exit
ip local pool default 10.2.2.64 10.2.2.127
line vty 0 2
 password <removed>
 login
 transport input telnet
 exit
line vty 3 4
 no login
 transport input lapb-ta v120
 autocommand ppp neg
 exit
end
```

