



Cisco IOS Terminal Services

October 2009

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco IOS Terminal Services

© 2009 Cisco Systems, Inc. All rights reserved.



CONTENTS

About Cisco IOS Software Documentation ix

Documentation Objectives ix

Audience ix

Documentation Conventions ix

Typographic Conventions x

Command Syntax Conventions x

Software Conventions xi

Reader Alert Conventions xi

Documentation Organization xi

Cisco IOS Documentation Set xii

Cisco IOS Documentation on Cisco.com xii

Configuration Guides, Command References, and Supplementary Resources xiii

Additional Resources and Documentation Feedback xx

Using the Command-Line Interface in Cisco IOS Software xxi

Initially Configuring a Device xxi

Using the CLI xxii

Understanding Command Modes xxii

Using the Interactive Help Feature xxv

Understanding Command Syntax xxvi

Understanding Enable and Enable Secret Passwords xxvii

Using the Command History Feature xxviii

Abbreviating Commands xxix

Using Aliases for CLI Commands xxix

Using the no and default Forms of Commands xxx

Using the debug Command xxx

Filtering Output Using Output Modifiers xxx

Understanding CLI Error Messages xxxi

Saving Changes to a Configuration xxxi

Additional Information xxxii

Terminal Services Commands TSV-1

absolute-timeout TSV-2

access-class (LAT) TSV-4

arap dedicated	TSV-6
arap enable	TSV-7
arap net-access-list	TSV-8
arap network	TSV-10
arap require-manual-password	TSV-11
arap timelimit	TSV-12
arap warningtime	TSV-13
arap zonelist	TSV-14
async default ip address	TSV-16
authentication-retries	TSV-17
autocommand	TSV-19
banner (transport map)	TSV-20
busy-message	TSV-22
clear entry	TSV-24
connect	TSV-25
connection wait	TSV-29
description (ruleset)	TSV-32
flush-at-activation	TSV-34
ip alias	TSV-36
ipx nasi-server enable	TSV-37
keymap	TSV-39
keymap-type	TSV-46
lat	TSV-48
lat access-list	TSV-50
lat enabled	TSV-52
lat group-list	TSV-53
lat host-buffers	TSV-55
lat ka-timer	TSV-56
lat node	TSV-57
lat out-group	TSV-58
lat remote-modification	TSV-60
lat retransmit-limit	TSV-61
lat server-buffers	TSV-62
lat service enabled	TSV-63
lat service-host	TSV-64

lat service ident	TSV-65
lat service password	TSV-66
lat service rating	TSV-67
lat service rotary	TSV-68
lat service-announcements	TSV-69
lat service-group	TSV-70
lat service-responder	TSV-72
lat service-timer	TSV-73
lat vc-sessions	TSV-74
lat vc-timer	TSV-75
line	TSV-76
login (EXEC)	TSV-79
login (line)	TSV-81
login-string	TSV-83
match (ruleset)	TSV-84
monitor traffic line	TSV-87
options (ruleset)	TSV-89
pad	TSV-91
resume (setting X.3 PAD parameters)	TSV-94
resume (switching sessions)	TSV-98
rlogin	TSV-100
rlogin trusted-localuser-source	TSV-102
rlogin trusted-remoteuser-source local	TSV-104
rsa keypair-name	TSV-106
rxspeed	TSV-108
secure-server	TSV-109
server (transport map)	TSV-111
service exec-callback	TSV-113
service old-slip-prompts	TSV-114
service pt-vty-logging	TSV-115
session-limit	TSV-117
session-timeout	TSV-118
set (ruleset)	TSV-120
show arap	TSV-128
show entry	TSV-130

show keymap	TSV-131
show lat advertised	TSV-133
show lat groups	TSV-135
show lat nodes	TSV-136
show lat services	TSV-138
show lat sessions	TSV-139
show lat traffic	TSV-143
show line	TSV-145
show line autodetect	TSV-150
show node	TSV-152
show platform software configuration access policy	TSV-155
show service	TSV-159
show terminal	TSV-161
show tn3270 ascii-hexval	TSV-165
show tn3270 character-map	TSV-166
show translate	TSV-167
show translate ruleset	TSV-170
show transport-map	TSV-174
show ttycap	TSV-180
show users	TSV-182
show x25 pad	TSV-184
skip (ruleset)	TSV-186
slip	TSV-189
substitute (ruleset)	TSV-191
telnet	TSV-199
telnet break-on-ip	TSV-204
telnet refuse-negotiations	TSV-206
telnet speed	TSV-208
telnet sync-on-break	TSV-209
telnet transparent	TSV-210
terminal lat out-group	TSV-211
terminal lat remote-modification	TSV-212
terminal transport preferred	TSV-213
test (ruleset)	TSV-215
test translate	TSV-222

time-out	TSV-225
tn3270	TSV-227
tn3270 8bit display	TSV-228
tn3270 8bit transparent-mode	TSV-229
tn3270 character-map	TSV-230
tn3270 datastream	TSV-234
tn3270 null-processing	TSV-235
tn3270 optimize-cursor-move	TSV-236
tn3270 reset-required	TSV-237
tn3270 status-message	TSV-238
tn3270 typeahead	TSV-239
translate lat	TSV-240
translate ruleset	TSV-247
translate lat (virtual access interfaces)	TSV-249
translate tcp	TSV-252
translate tcp (virtual access interfaces)	TSV-262
translate use telnet	TSV-265
translate x25	TSV-267
translate x25 (virtual access interfaces)	TSV-278
transport-map type console	TSV-282
transport-map type persistent	TSV-284
transport input	TSV-287
transport interface	TSV-289
transport output	TSV-292
transport preferred	TSV-294
transport type console	TSV-296
transport type persistent	TSV-298
ttycap	TSV-301
txspeed	TSV-305
where	TSV-306
x25 pvc translate ruleset	TSV-308
x25 subaddress	TSV-310
x28	TSV-312
x28 no-outgoing	TSV-318
x3	TSV-320



About Cisco IOS Software Documentation

Last Updated: October 14, 2009

This document describes the objectives, audience, conventions, and organization used in Cisco IOS software documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:

- [Documentation Objectives, page ix](#)
- [Audience, page ix](#)
- [Documentation Conventions, page ix](#)
- [Documentation Organization, page xi](#)
- [Additional Resources and Documentation Feedback, page xx](#)

Documentation Objectives

Cisco IOS documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

Audience

The Cisco IOS documentation set is intended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS commands necessary to perform particular tasks. The Cisco IOS documentation set is also intended for those users experienced with Cisco IOS software who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS release.

Documentation Conventions

In Cisco IOS documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section contains the following topics:

- [Typographic Conventions, page x](#)
- [Command Syntax Conventions, page x](#)
- [Software Conventions, page xi](#)
- [Reader Alert Conventions, page xi](#)

Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
<i>string</i>	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to <i>public</i> , do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter as shown.
<i>italic</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
	A vertical line, called a pipe, that is enclosed within braces or square brackets indicates a choice within a set of keywords or arguments.
[x y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

Software Conventions

Cisco IOS software uses the following program code conventions:

Convention	Description
<code>Courier font</code>	Courier font is used for information that is displayed on a PC or terminal screen.
<code>Bold Courier font</code>	Bold Courier font indicates text that the user must enter.
<code>< ></code>	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
<code>!</code>	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco IOS software for certain processes.
<code>[]</code>	Square brackets enclose default responses to system prompts.

Reader Alert Conventions

Cisco IOS documentation uses the following conventions for reader alerts:



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



Timesaver

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. It also lists the configuration guides, command references, and supplementary references and resources that comprise the documentation set. It contains the following topics:

- [Cisco IOS Documentation Set, page xii](#)
- [Cisco IOS Documentation on Cisco.com, page xii](#)
- [Configuration Guides, Command References, and Supplementary Resources, page xiii](#)

Cisco IOS Documentation Set

The Cisco IOS documentation set consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and select severity 3 (moderate) defects in released Cisco IOS software. Review release notes before other documents to learn whether updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
 - Configuration guides—Compilations of documents that provide conceptual and task-oriented descriptions of Cisco IOS features.
 - Command references—Compilations of command pages in alphabetical order that provide detailed information about the commands used in the Cisco IOS features and the processes that comprise the related configuration guides. For each technology, there is a single command reference that supports all Cisco IOS releases and that is updated at each standard release.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Command pages are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

Cisco IOS Documentation on Cisco.com

The following sections describe the organization of the Cisco IOS documentation set and how to access various document types.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

Feature Guides

Cisco IOS features are documented in feature guides. Feature guides describe one feature or a group of related features that are supported on many different software releases and platforms. Your Cisco IOS software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release.

Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

Command References

Command reference books contain descriptions of Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are organized by technology. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in [Table 2 on page xix](#).

Configuration Guides, Command References, and Supplementary Resources

[Table 1](#) lists, in alphabetical order, Cisco IOS software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references contain commands for Cisco IOS software for all releases. The configuration guides and command references support many different software releases and platforms. Your Cisco IOS software release or platform may not support all these technologies.

[Table 2](#) lists documents and resources that supplement the Cisco IOS software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

For additional information about configuring and operating specific networking devices, and to access Cisco IOS documentation, go to the Product/Technologies Support area of Cisco.com at the following location:

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

Table 1 Cisco IOS Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• <i>Cisco IOS AppleTalk Configuration Guide</i> • <i>Cisco IOS AppleTalk Command Reference</i>	AppleTalk protocol.
• <i>Cisco IOS Asynchronous Transfer Mode Configuration Guide</i> • <i>Cisco IOS Asynchronous Transfer Mode Command Reference</i>	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> <i>Cisco IOS Bridging Command Reference</i> <i>Cisco IOS IBM Networking Command Reference</i>	Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM). Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.
<i>Cisco IOS Broadband Access Aggregation and DSL Configuration Guide</i> <i>Cisco IOS Broadband Access Aggregation and DSL Command Reference</i>	PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).
<i>Cisco IOS Carrier Ethernet Configuration Guide</i> <i>Cisco IOS Carrier Ethernet Command Reference</i>	Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and Operation, Administration, and Maintenance (OAM).
<i>Cisco IOS Configuration Fundamentals Configuration Guide</i> <i>Cisco IOS Configuration Fundamentals Command Reference</i>	Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.
<i>Cisco IOS DECnet Configuration Guide</i> <i>Cisco IOS DECnet Command Reference</i>	DECnet protocol.
<i>Cisco IOS Dial Technologies Configuration Guide</i> <i>Cisco IOS Dial Technologies Command Reference</i>	Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), dial-on-demand routing, dial-out, ISDN, large scale dial-out, modem and resource pooling, Multilink PPP (MLP), PPP, and virtual private dialup network (VPDN).
<i>Cisco IOS Flexible NetFlow Configuration Guide</i> <i>Cisco IOS Flexible NetFlow Command Reference</i>	Flexible NetFlow.
<i>Cisco IOS High Availability Configuration Guide</i> <i>Cisco IOS High Availability Command Reference</i>	A variety of high availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
<i>Cisco IOS Integrated Session Border Controller Command Reference</i>	A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS).

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS Intelligent Services Gateway Configuration Guide</i> <i>Cisco IOS Intelligent Services Gateway Command Reference</i>	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, and session state monitoring.
<i>Cisco IOS Interface and Hardware Component Configuration Guide</i> <i>Cisco IOS Interface and Hardware Component Command Reference</i>	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
<i>Cisco IOS IP Addressing Services Configuration Guide</i> <i>Cisco IOS IP Addressing Services Command Reference</i>	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
<i>Cisco IOS IP Application Services Configuration Guide</i> <i>Cisco IOS IP Application Services Command Reference</i>	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
<i>Cisco IOS IP Mobility Configuration Guide</i> <i>Cisco IOS IP Mobility Command Reference</i>	Mobile ad hoc networks (MANet) and Cisco mobile networks.
<i>Cisco IOS IP Multicast Configuration Guide</i> <i>Cisco IOS IP Multicast Command Reference</i>	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).
<i>Cisco IOS IP Routing Protocols Configuration Guide</i> <i>Cisco IOS IP Routing Protocols Command Reference</i>	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast, bidirectional forwarding detection (BFD), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), On-Demand Routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).
<i>Cisco IOS IP Routing: BFD Configuration Guide</i>	Bidirectional forwarding detection (BFD).
<i>Cisco IOS IP Routing: BGP Configuration Guide</i> <i>Cisco IOS IP Routing: BGP Command Reference</i>	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast.
<i>Cisco IOS IP Routing: EIGRP Configuration Guide</i> <i>Cisco IOS IP Routing: EIGRP Command Reference</i>	Enhanced Interior Gateway Routing Protocol (EIGRP).
<i>Cisco IOS IP Routing: ISIS Configuration Guide</i> <i>Cisco IOS IP Routing: ISIS Command Reference</i>	Intermediate System-to-Intermediate System (IS-IS).
<i>Cisco IOS IP Routing: ODR Configuration Guide</i> <i>Cisco IOS IP Routing: ODR Command Reference</i>	On-Demand Routing (ODR).

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS IP Routing: OSPF Configuration Guide</i> <i>Cisco IOS IP Routing: OSPF Command Reference</i>	Open Shortest Path First (OSPF).
<i>Cisco IOS IP Routing: Protocol-Independent Configuration Guide</i> <i>Cisco IOS IP Routing: Protocol-Independent Command Reference</i>	IP routing protocol-independent features and commands. Generic policy-based routing (PBR) features and commands are included.
<i>Cisco IOS IP Routing: RIP Configuration Guide</i> <i>Cisco IOS IP Routing: RIP Command Reference</i>	Routing Information Protocol (RIP).
<i>Cisco IOS IP SLAs Configuration Guide</i> <i>Cisco IOS IP SLAs Command Reference</i>	Cisco IOS IP Service Level Agreements (IP SLAs).
<i>Cisco IOS IP Switching Configuration Guide</i> <i>Cisco IOS IP Switching Command Reference</i>	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
<i>Cisco IOS IPv6 Configuration Guide</i> <i>Cisco IOS IPv6 Command Reference</i>	For IPv6 features, protocols, and technologies, go to the IPv6 “Start Here” document.
<i>Cisco IOS ISO CLNS Configuration Guide</i> <i>Cisco IOS ISO CLNS Command Reference</i>	ISO Connectionless Network Service (CLNS).
<i>Cisco IOS LAN Switching Configuration Guide</i> <i>Cisco IOS LAN Switching Command Reference</i>	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
<i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide</i> <i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference</i>	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
<i>Cisco IOS Mobile Wireless Home Agent Configuration Guide</i> <i>Cisco IOS Mobile Wireless Home Agent Command Reference</i>	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
<i>Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide</i> <i>Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference</i>	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
<i>Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide</i> <i>Cisco IOS Mobile Wireless Radio Access Networking Command Reference</i>	Cisco IOS radio access network products.
<i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i> <i>Cisco IOS Multiprotocol Label Switching Command Reference</i>	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS traffic engineering (TE), and MPLS Embedded Management (EM) and MIBs.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• <i>Cisco IOS Multi-Topology Routing Configuration Guide</i> • <i>Cisco IOS Multi-Topology Routing Command Reference</i>	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
• <i>Cisco IOS NetFlow Configuration Guide</i> • <i>Cisco IOS NetFlow Command Reference</i>	Network traffic data analysis, aggregation caches, and export features.
• <i>Cisco IOS Network Management Configuration Guide</i> • <i>Cisco IOS Network Management Command Reference</i>	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS software (XSM Configuration).
• <i>Cisco IOS Novell IPX Configuration Guide</i> • <i>Cisco IOS Novell IPX Command Reference</i>	Novell Internetwork Packet Exchange (IPX) protocol.
• <i>Cisco IOS Optimized Edge Routing Configuration Guide</i> • <i>Cisco IOS Optimized Edge Routing Command Reference</i>	Optimized edge routing (OER) monitoring; Performance Routing (PfR); and automatic route optimization and load distribution for multiple connections between networks.
• <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i>	Traffic queueing, traffic policing, traffic shaping, Modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), Multilink PPP (MLP) for QoS, header compression, AutoQoS, Resource Reservation Protocol (RSVP), and weighted random early detection (WRED).
• <i>Cisco IOS Security Command Reference</i>	Access control lists (ACLs); authentication, authorization, and accounting (AAA); firewalls; IP security and encryption; neighbor router authentication; network access security; network data encryption with router authentication; public key infrastructure (PKI); RADIUS; TACACS+; terminal access security; and traffic filters.
• <i>Cisco IOS Security Configuration Guide: Securing the Data Plane</i>	Access Control Lists (ACLs); Firewalls: Context-Based Access Control (CBAC) and Zone-Based Firewall; Cisco IOS Intrusion Prevention System (IPS); Flexible Packet Matching; Unicast Reverse Path Forwarding (uRPF); Threat Information Distribution Protocol (TIDP) and TMS.
• <i>Cisco IOS Security Configuration Guide: Securing the Control Plane</i>	Control Plane Policing, Neighborhood Router Authentication.
• <i>Cisco IOS Security Configuration Guide: Securing User Services</i>	AAA (includes 802.1x authentication and Network Admission Control [NAC]); Security Server Protocols (RADIUS and TACACS+); Secure Shell (SSH); Secure Access for Networking Devices (includes Autosecure and Role-Based CLI access); Lawful Intercept.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>	Internet Key Exchange (IKE) for IPsec VPNs; IPsec Data Plane features; IPsec Management features; Public Key Infrastructure (PKI); Dynamic Multipoint VPN (DMVPN); Easy VPN; Cisco Group Encrypted Transport VPN (GETVPN); SSL VPN.
• <i>Cisco IOS Service Advertisement Framework Configuration Guide</i> • <i>Cisco IOS Service Advertisement Framework Command Reference</i>	Cisco Service Advertisement Framework.
• <i>Cisco IOS Service Selection Gateway Configuration Guide</i> • <i>Cisco IOS Service Selection Gateway Command Reference</i>	Subscriber authentication, service access, and accounting.
• <i>Cisco IOS Software Activation Configuration Guide</i> • <i>Cisco IOS Software Activation Command Reference</i>	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
• <i>Cisco IOS Software Modularity Installation and Configuration Guide</i> • <i>Cisco IOS Software Modularity Command Reference</i>	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes, and patches.
• <i>Cisco IOS Terminal Services Configuration Guide</i> • <i>Cisco IOS Terminal Services Command Reference</i>	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
• <i>Cisco IOS Virtual Switch Command Reference</i>	Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP). Note For information about virtual switch configuration, see the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.
• <i>Cisco IOS Voice Configuration Library</i> • <i>Cisco IOS Voice Command Reference</i>	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
• <i>Cisco IOS VPDN Configuration Guide</i> • <i>Cisco IOS VPDN Command Reference</i>	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy; L2TP extended failover; L2TP security VPDN; multihop by Dialed Number Identification Service (DNIS); timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F); RADIUS Attribute 82 (tunnel assignment ID); shell-based authentication of VPDN users; tunnel authentication via RADIUS on tunnel terminator.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
- Cisco IOS Wide-Area Networking Configuration Guide - Cisco IOS Wide-Area Networking Command Reference	Frame Relay; Layer 2 Tunnel Protocol Version 3 (L2TPv3); L2VPN Pseudowire Redundancy; L2VPN Interworking; Layer 2 Local Switching; Link Access Procedure, Balanced (LAPB); and X.25.
- Cisco IOS Wireless LAN Configuration Guide - Cisco IOS Wireless LAN Command Reference	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

Table 2 lists documents and resources that supplement the Cisco IOS software configuration guides and command references.

Table 2 Cisco IOS Supplementary Documents and Resources

Document Title or Resource	Description
Cisco IOS Master Command List, All Releases	Alphabetical list of all the commands documented in all Cisco IOS releases.
Cisco IOS New, Modified, Removed, and Replaced Commands	List of all the new, modified, removed, and replaced commands for a Cisco IOS release.
Cisco IOS Software System Messages	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system, may be informational only, or may help diagnose problems with communications lines, internal hardware, or system software.
Cisco IOS Debug Command Reference	Alphabetical list of debug commands including brief descriptions of use, command syntax, and usage guidelines.
Release Notes and Caveats	Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator .
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/

Additional Resources and Documentation Feedback

What's New in Cisco Product Documentation is released monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2008–2009 Cisco Systems, Inc. All rights reserved.



Using the Command-Line Interface in Cisco IOS Software

Last Updated: October 14, 2009

This document provides basic information about the command-line interface (CLI) in Cisco IOS software and how you can use some of the CLI features. This document contains the following sections:

- [Initially Configuring a Device, page xxi](#)
- [Using the CLI, page xxii](#)
- [Saving Changes to a Configuration, page xxxi](#)
- [Additional Information, page xxxii](#)

For more information about using the CLI, see the “[Using the Cisco IOS Command-Line Interface](#)” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the “[About Cisco IOS Software Documentation](#)” document.

Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product/Technologies Support area of Cisco.com at <http://www.cisco.com/go/techdocs>.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

Changing the Default Settings for a Console or AUX Port

There are only two changes that you can make to a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

**Note**

The AUX port on the Route Processor (RP) installed in a Cisco ASR 1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

Using the CLI

This section describes the following topics:

- [Understanding Command Modes, page xxii](#)
- [Using the Interactive Help Feature, page xxv](#)
- [Understanding Command Syntax, page xxvi](#)
- [Understanding Enable and Enable Secret Passwords, page xxvii](#)
- [Using the Command History Feature, page xxviii](#)
- [Abbreviating Commands, page xxix](#)
- [Using Aliases for CLI Commands, page xxix](#)
- [Using the no and default Forms of Commands, page xxx](#)
- [Using the debug Command, page xxx](#)
- [Filtering Output Using Output Modifiers, page xxx](#)
- [Understanding CLI Error Messages, page xxxi](#)

Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

[Table 3](#) lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 3 *CLI Command Modes*

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	Router>	Issue the logout or exit command.	• Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the enable command.	Router#	Issue the disable command or the exit command to return to user EXEC mode.	• Issue show and debug commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, issue the configure terminal command.	Router(config)#	Issue the exit command or the end command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the interface command.	Router(config-if)#	Issue the exit command to return to global configuration mode or the end command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the line vty or line console command.	Router(config-line)#	Issue the exit command to return to global configuration mode or the end command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 3 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the reload command. Press the Break key during the first 60 seconds while the system is booting.	rommon # > The # symbol represents the line number and increments at each prompt.	Issue the continue command.	- Run as the default operating mode when a valid image cannot be loaded. - Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. - Perform password recovery when a Ctrl-Break sequence is issued within 60 seconds of a power-on or reload event.
Diagnostic (available only on Cisco ASR 1000 series routers)	The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload. - A user-configured access policy was configured using the transport-map command, which directed the user into diagnostic mode. - The router was accessed using an RP auxiliary port. - A break signal (Ctrl-C, Ctrl-Shift-6, or the send break command) was entered, and the router was configured to enter diagnostic mode when the break signal was received.	Router(diag) #	If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or use a method that is configured to connect to the Cisco IOS CLI. If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.	- Inspect various states on the router, including the Cisco IOS state. - Replace or roll back the configuration. - Provide methods of restarting the Cisco IOS software or other processes. - Reboot hardware (such as the entire router, an RP, an ESP, a SIP, a SPA) or other hardware components. - Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias                set and display aliases command
boot                 boot up an external process
confreg              configuration register utility
cont                 continue executing a downloaded image
context              display the context of a loaded image
cookie               display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```



Note

A keyboard alternative to the **end** command is Ctrl-Z.

Using the Interactive Help Feature

The CLI includes an interactive Help feature. [Table 4](#) describes the purpose of the CLI interactive Help commands.

Table 4 CLI Interactive Help Commands

Command	Purpose
help	Provides a brief description of the Help feature in any command mode.
?	Lists all commands available for a particular command mode.
<i>partial command?</i>	Provides a list of commands that begin with the character string (no space between the command and the question mark).
<i>partial command</i> <Tab>	Completes a partial command name (no space between the command and <Tab>).
<i>command ?</i>	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
<i>command keyword ?</i>	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the help commands:

help

```
Router> help
```

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)

?

```
Router# ?
```

```
Exec commands:
```

access-enable	Create a temporary access-List entry
access-profile	Apply user-profile to interface
access-template	Create a temporary access-List entry
alps	ALPS exec commands
archive	manage archive files

```
<snip>
```

partial command?

```
Router(config)# zo?
```

```
zone zone-pair
```

partial command<Tab>

```
Router(config)# we<Tab> webvpn
```

command ?

```
Router(config-if)# pppoe ?
```

enable	Enable pppoe
max-sessions	Maximum PPPoE sessions

command keyword ?

```
Router(config-if)# pppoe enable ?
```

group	attach a BBA group
-------	--------------------

```
<cr>
```

Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. [Table 5](#) describes these conventions.

Table 5 *CLI Syntax Conventions*

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```
Router(config)# ethernet cfm domain ?
WORD domain name
Router(config)# ethernet cfm domain dname ?
level
Router(config)# ethernet cfm domain dname level ?
<0-7> maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
<cr>

Router(config)# snmp-server file-transfer access-group 10 ?
protocol protocol options
<cr>

Router(config)# logging host ?
Hostname or A.B.C.D IP address of the syslog server
ipv6 Configure IPv6 syslog server
```

Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable password**
- **enable secret password**

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a numeral. Spaces are also valid password characters; for example, “two words” is a valid password. Leading spaces are ignored, but trailing spaces are recognized.

**Note**

Both password commands have numeric keywords that are single integer values. If you choose a numeral for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable password** or **no enable secret password**.

For more information about password recovery procedures for Cisco products, see http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml.

Using the Command History Feature

The command history feature saves, in a command history buffer, the commands that you enter during a session. The default number of saved commands is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the Up Arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.
- Press Ctrl-N or the Down Arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the Up Arrow key. Repeat the key sequence to recall successively more recent commands.

**Note**

The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

The command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrrp** as a keyword in addition to **version**. (Command and keyword examples are from Cisco IOS Release 12.4(13)T.)

Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 6 shows the default command aliases.

Table 6 *Default Command Aliases*

Command Alias	Original Command
h	help
lo	logout
p	ping
s	show
u or un	undebug
w	where

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias mode command-alias original-command**. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_a1.html.

Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values.

The **no** form is documented in the command pages of command references. The **default** form is generally documented in the command pages only when the **default** form performs a different function than the plain and **no** forms of the command. To see what **default** commands are available on your system, enter **default ?** in the appropriate command mode.

Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebg all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html.



Caution

Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

The following three output modifiers are available:

- **begin** *regular-expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular-expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular-expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (**|**), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression “protocol.”

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

Understanding CLI Error Messages

You may encounter some error messages while using the CLI. [Table 7](#) shows the common CLI error messages.

Table 7 Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: “show con”	You did not enter enough characters for the command to be recognized.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at “^” marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

For more system error messages, see the following document:

- [Cisco IOS Release 12.4T System Message Guide](#)

Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved.

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Additional Information

- “Using the Cisco IOS Command-Line Interface” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*
http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html
- Cisco Product/Technology Support
<http://www.cisco.com/go/techdocs>
- Support area on Cisco.com (also search for documentation by task or product)
<http://www.cisco.com/en/US/support/index.html>
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com user ID and password)
<http://www.cisco.com/kobayashi/sw-center/>
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software
<http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>
- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)
<http://tools.cisco.com/Support/CLILookup>
- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands
<https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2008–2009 Cisco Systems, Inc. All rights reserved.



Terminal Services Commands



absolute-timeout

To set the interval for closing the connection, use the **absolute-timeout** command in line configuration mode. To restore the default, use the **no** form of this command.

absolute-timeout *minutes*

no absolute-timeout

Syntax Description	<i>minutes</i> Number of minutes after which the user session will be terminated.
---------------------------	---

Defaults	No timeout interval is automatically set.
-----------------	---

Command Modes	Line configuration
----------------------	--------------------

Command History	Release	Modification
	11.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	Use the absolute-timeout command line configuration command to configure the EXEC to terminate when the configured number of minutes occurs on the virtual terminal (vty) line. The absolute-timeout command terminates the connection after the specified time period has elapsed, regardless of whether the connection is being used at the time of termination. You can specify an absolute-timeout value for each port. The user is given 20 seconds notice before the session is terminated. You can use this command along with the logout-warning command to notify users of an impending logout.
-------------------------	--

Cisco IOS software also provides the **session-timeout** and **exec-timeout** line configuration commands for releasing lines when they have been idle for too long.

You can set the **absolute-timeout** command and an AppleTalk Remote Access Protocol (ARAP) timeout for the same line; however, this command supersedes any timeouts set in ARAP. Additionally, ARAP users will receive no notice of any impending termination if you use this command.

Examples	The following example sets an interval of 60 minutes on line 5:
-----------------	---

```
line 5
 absolute-timeout 60
```

Related Commands

Command	Description
exec-timeout	Sets the interval that the EXEC command interpreter waits until user input is detected.
logout-warning	Sets and displays a warning for users about an impending forced timeout.
session-timeout	Sets the interval for closing the connection on a console or terminal line.

access-class (LAT)

To define restrictions on incoming and outgoing connections, use the **access-class** command in line configuration mode. To remove the access list number, use the **no** form of this command.

access-class *access-list-number* { **in** [**vrf-also**] | **out** }

no access-class *access-list-number* { **in** | **out** }

Syntax Description

<i>access-list-number</i>	Specifies an integer from 1 to 199 that defines the access list.
in	Controls which nodes can make local-area transport (LAT) connections into the server.
vrf-also	(Optional) Accepts incoming connections from interfaces that belong to a VRF.
out	Defines the access checks made on outgoing connections. (A user who types a node name at the system prompt to initiate a LAT connection is making an outgoing connection.)

Defaults

Disabled

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2	The vrf-also keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command defines access list numbers that will then be used with the **lat access-list** command to specify the access conditions.

The value supplied for the *access-list-number* argument is used for all protocols supported by the Cisco IOS software. If you are already using an IP access list, you must define LAT and possibly X.25 access lists permitting connections to all devices, to emulate the behavior of previous software versions.

When both IP and LAT connections are allowed from a terminal line and an IP access list is applied to that line with the **access-class** line configuration command, you must also create a LAT access list with the same number if you want to allow any LAT connections from that terminal. You can specify only one incoming and one outgoing access list number for each terminal line. When checking LAT access lists, if the specified list does not exist, the system denies all LAT connections.

If you do not specify the **vrf-also** keyword, incoming Telnet connections from interfaces that are part of a VRF are rejected.

Examples

The following example configures an incoming access class on vty line 4:

```
line vty 4
access-class 4 in
```

Related Commands

Command	Description
lat access-list	Specifies access conditions to nodes on the LAT network.

arap dedicated

To configure a line to be used only as an AppleTalk Remote Access (ARA) connection, use the **arap dedicated** command in line configuration mode. To return the line to interactive mode, use the **no** form of this command.

arap dedicated

no arap dedicated

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures line 3 to be used only for ARA connections:

```
line 3
  arap dedicated
```

arap enable

To enable AppleTalk Remote Access (ARA) for a line, use the **arap enable** command in line configuration mode. To disable ARA, use the **no** form of this command.

arap enable

no arap enable

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	Disabled
-----------------	----------

Command Modes	Line configuration
----------------------	--------------------

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples	The following example enables ARA on line 3:
-----------------	--

```
line 3
 arap enable
```

Related Commands	Command	Description
	appletalk routing	Enables AppleTalk routing.
	autoselect	Configures a line to start an ARA, PPP, or SLIP session.

arap net-access-list

To control Apple Macintosh access to networks, use the **arap net-access-list** command in line configuration mode. To return to the default setting, use the **no** form of this command.

arap net-access-list *net-access-list-number*

no arap net-access-list *net-access-list-number*

Syntax Description	<i>net-access-list-number</i> One of the <i>list</i> values configured using the AppleTalk access-list cable-range , access-list includes , access-list network , access-list other-access , or access-list within commands.
---------------------------	---

Defaults	Disabled. The Macintosh has access to all networks.
-----------------	---

Command Modes	Line configuration
----------------------	--------------------

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	You can use the arap net-access-list command to apply access lists defined by the access-list cable-range , access-list includes , access-list network , access-list other-access , or access-list within commands.
	You cannot use the arap net-access-list command to apply access lists defined by the access-list zone or access-list additional-zones commands.

Examples	In the following example, ARA is enabled on line 3 and the Macintosh will have access to the AppleTalk access list numbered 650:
	<pre> line 3 arap enable arap net-access-list 650 </pre>

Related Commands

Command	Description
access-list cable-range	Defines an AppleTalk access list for a cable range (for extended networks only).
access-list includes	Defines an AppleTalk access list that overlaps any part of a range of network numbers or cable ranges (for both extended and nonextended networks).
access-list network	Defines an AppleTalk access list for a single network number (that is, for a nonextended network).
access-list other-access	Defines the default action to take for subsequent access checks that apply to networks or cable ranges.
access-list within	Defines an AppleTalk access list for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range.
arap zonelist	Controls which zones the Apple Macintosh client sees.

arap network

To create a new network or zone and cause it to be advertised, use the **arap network** command in global configuration mode. To prevent a new network or zone from being advertised, use the **no** form of this command.

arap network [*network-number*] [*zone-name*]

no arap network

Syntax Description

<i>network-number</i>	(Optional) AppleTalk network number. The network number must be unique on your AppleTalk network. This network is where all AppleTalk Remote Access (ARAP) users appear when they dial in to the network.
<i>zone-name</i>	(Optional) AppleTalk zone name.

Defaults

A new network or zone is not created.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This is a required command. ARAP does not run without it in Cisco IOS Release 10.2 and later.

Examples

The following example creates a new zone named test zone:

```
arap network 400 test zone
```

arap require-manual-password

To require users to enter their password manually at the time they log in, use the **arap require-manual-password** command in line configuration mode. To disable the manual password-entry requirement, use the **no** form of this command.

arap require-manual-password

no arap require-manual-password

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Line configuration

Command History	Release	Modification
	11.1	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines This command only works for AppleTalk Remote Access Protocol (ARAP) 2.0 connections.

Examples The following example forces users to enter their passwords manually at the time they log in, rather than use a saved password:

```
arap require-manual-password
```

Related Commands	Command	Description
	enable password	Sets a local password to control access to various privilege levels.
	login (line)	Enables password checking at login and defines the method (local or TACACS+).
	peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.

arap timelimit

To set the maximum length of an AppleTalk Remote Access (ARA) session for a line, use the **arap timelimit** command in line configuration mode. To return to the default of unlimited session length, use the **no** form of this command.

arap timelimit [*minutes*]

no arap timelimit

Syntax Description	<i>minutes</i> (Optional) Maximum length of time, in minutes, for a session.	
Defaults	Unlimited session length	
Command Modes	Line configuration	
Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Usage Guidelines	After the specified length of time, the session will be terminated.	
Examples	The following example specifies a maximum length of 20 minutes for ARA sessions:	
	<pre>line 3 arap enable arap timelimit 20</pre>	
Related Commands	Command	Description
	arap warningtime	Sets when a disconnect warning message is displayed.

arap warningtime

To set when a disconnect warning message is displayed, use the **arap warningtime** command in line configuration mode. To disable this function, use the **no** form of this command.

arap warningtime [*minutes*]

no arap warningtime

Syntax Description	<i>minutes</i>	(Optional) Amount of time, in minutes, before the configured session time limit. At the configured amount of time before a session is to be disconnected, the router sends a message to the Apple Macintosh client, which causes a warning message to appear on the user screen.
---------------------------	----------------	--

Defaults	Disabled
-----------------	----------

Command Modes	Line configuration
----------------------	--------------------

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	This command can only be used if a session time limit has been configured on the line.
-------------------------	--

Examples	The following example shows a line configured for 20-minute AppleTalk Remote Access (ARA) sessions, with a warning 17 minutes after the session is started:
-----------------	---

```
line 3
  arap enable
  arap dedicated
  arap timelimit 20
  arap warningtime 3
```

Related Commands	Command	Description
	arap timelimit	Sets the maximum length of an ARA session for a line.

arap zonelist

To control which zones the Apple Macintosh client sees, use the **arap zonelist** command in line configuration mode. To disable the default setting, use the **no** form of this command.

arap zonelist *zone-access-list-number*

no arap zonelist *zone-access-list-number*

Syntax Description	<i>zone-access-list-number</i> One of the <i>list</i> values configured using the AppleTalk access-list zone or access-list additional-zones command.
---------------------------	---

Defaults	Disabled. The Macintosh will see all defined zones.
-----------------	---

Command Modes	Line configuration
----------------------	--------------------

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	You can use the arap zonelist command to apply access lists defined by the access-list zone and access-list additional-zones commands.
	You cannot use the arap zonelist command to apply access lists defined by the access-list network command.
	Hiding a zone from users is not the same as preventing them from sending and receiving packets from the networks that make up that zone. For true security, an arap net-access-list command must be issued to prevent traffic to and from those networks.

Examples	The following example enables AppleTalk Remote Access (ARA) on line 3; the Macintosh will see only zones permitted by access list 650.
	<pre> line 3 arap enable arap zonelist 650 </pre>

Related Commands	Command	Description
	access-list additional-zones	Defines the default action to take for access checks that apply to zones.

Command	Description
access-list zone	Defines an AppleTalk access list that applies to a zone.
arap net-access-list	Controls Apple Macintosh access to networks.

async default ip address

The **async default ip address** command is replaced by the **peer default ip address** command. See the **peer default ip address** command for more information.

authentication-retries

To specify the number of authentication retries before dropping the connection for a persistent Secure Shell (SSH) connection attempt, use the **authentication-retries** transport map configuration mode command. To restore the default setting of three retries, use the **no** form of the command.

authentication-retries *number-of-retries*

no authentication-retries

Syntax Description	<i>number-of-retries</i> Specifies the number of retries before the connection attempt is dropped.
---------------------------	--

Command Default	The default <i>number-of-retries</i> is 3.
------------------------	--

Command Modes	Transport map configuration (config-tmap)
----------------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines	This command configures the number of authentication retries for users using SSH to connect to a Management Ethernet interface with an applied transport map.
-------------------------	---

Examples	In the following example, a transport map is configured that will apply the following settings to any users attempting to access the Management Ethernet port via SSH: • Users using SSH wait for the IOS process to become active, but enter diagnostic mode if the attempt to access IOS is interrupted. • The RSA keypair name is “sshkeys”. • The connection allows one authentication retry. • The banner “--Welcome to Diagnostic Mode--” appears if diagnostic mode is entered as a result of SSH handling through this transport map. • The banner “--Waiting for IOS Process--” appears if the connection is waiting for the IOS process to become active.
-----------------	---

The transport map is then applied to the interface when the **transport type persistent ssh input** command is entered to enable persistent SSH.

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# rsa keypair-name sshkeys
```

```

Router(config-tmap)# authentication-retries 1
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for IOS Process--
X
Router(config-tmap)# time-out 30
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit

Router(config)# transport type persistent ssh input sshhandler

```

Related Commands

Command	Description
banner (transport map)	Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of the transport map configuration.
connection wait	Specifies how an incoming connection will be handled.
rsa keypair-name	Names the RSA keypair to be used for persistent SSH connections.
time-out	Specifies the SSH timeout interval in seconds.
transport interface	Applies the transport map settings to the interface.
transport type persistent	Applies an already-configured persistent transport map to an interface.
transport-map type persistent	Creates and names a persistent transport map and enters transport map configuration mode.

autocommand

To configure the system to automatically execute a specific EXEC command when it connects to a port, use the **autocommand** command in line configuration mode. To disable the automatic execution, use the **no** form of this command.

autocommand [**no-suppress-linenum**] *command-text*

no autocommand

Syntax Description

no-suppress-linenum	Displays the service line number for which the EXEC commands are automatically executed.
<i>command-text</i>	Any appropriate EXEC command, including the host name and any switches that must be used with the EXEC command.

Defaults

No commands are configured to automatically execute.

Command Modes

Line configuration (config-line)

Command History

Release	Modification
10.0	This command was introduced.
12.0T	The no-suppress-linenum keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The line number message enables users to track the port that is currently connected. The line numbers for these messages are provided by the **service linenum** command. The **autocommand** command generally suppresses the line number message. However, when **autocommand** is used with the **no-suppress-linenum** keyword, the line number messages are not suppressed.

Examples

The following example shows how to force an automatic connection to host21:

```
Router(config)# line vty 4
Router(config-line)# autocommand no-suppress-linenum connect host21
Router(config-line)#
```

Related Commands

Command	Description
service linenum	Configures Cisco IOS software to display line number information after the EXEC or incoming banner.

banner (transport map)

To create a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of a transport map configuration configured on a console port or for users using Telnet or Secure Shell (SSH), use the **banner** command in transport map configuration mode. To restore the default setting of no diagnostic or no wait banner, use the **no** form of the command.

banner [**diagnostic** | **wait**] *banner-message*

no banner [**diagnostic** | **wait**]

Syntax Description

diagnostic	Creates a banner message seen by users directed into diagnostic mode as a result of the transport map handling of the connection.
wait	Creates a banner message seen by users waiting for the IOS mode to become active as a result of the transport map handling of the connection.
<i>banner-message</i>	The banner message, which begins and ends with the same delimiting character.

Command Default

There are no banners configured for transport maps by default.

Command Modes

Transport map configuration (config-tmap)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

Configuring the diagnostic and wait banners is optional but recommended. The banners are especially useful as indicators to users of the status of their Telnet, SSH, or console port connection attempts.

When defining the *banner-message*, it is advisable to press **Enter** before entering the final delimiting character. Pressing **Enter** moves the cursor down a line and ensures the prompt on the router does not appear on the same line as the banner when the banner posts during a Telnet or SSH session.

The currently applied banner messages can be checked using the **show platform software configuration access policy** command.

Examples

In the following example, a transport map that will make all Telnet connections wait for the IOS process to become active before connecting to the router, while also allowing the user to interrupt the process and enter diagnostic mode, is configured and applied to the Management Ethernet interface (interface gigabitethernet 0).

A diagnostic and a wait banner are also configured.

The transport map is then applied to the interface when the **transport type persistent telnet input** command is entered to enable persistent Telnet.

```

Router(config)# transport-map type persistent telnet telnethandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for IOS Process--
X

Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler

```

In the following example, a transport map to set console port access policies is created and attached to console port 0. The transport map configuration includes both a diagnostic and a wait banner.

```

Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
Welcome to diagnostic mode
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS prompt
X
Router(config-tmap)# exit

Router(config)# transport type console 0 input consolehandler

```

Related Commands

Command	Description
authentication-retries	Specifies the number of SSH authentication retries before dropping the connection when a persistent SSH transport map is applied to the receiving interface.
connection wait	Specifies how an incoming connection will be handled.
rsa keypair-name	Names the RSA keypair to be used for persistent SSH connections.
show platform software configuration access policy	Displays the access policy and banner settings for console, Telnet, and SSH connections.
time-out	Specifies the SSH timeout interval in seconds.
transport interface	Applies the transport map settings to the interface.
transport type persistent	Applies an already-configured persistent transport map to an interface.
transport-map type persistent	Creates and names a persistent transport map and enters transport map configuration mode.

busy-message

To create a “host failed” message that displays when a connection fails, use the **busy-message** command in global configuration mode. To disable the “host failed” message from displaying on the specified host, use the **no** form of this command.

busy-message *host-name d message d*

no busy-message *host-name*

Syntax Description

<i>host-name</i>	Name of the host that cannot be reached.
<i>d</i>	Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the message.
<i>message</i>	Message text.

Defaults

No message is displayed.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies only to Telnet connections.

Follow the **busy-message** command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Defining a “host failed” message for a host prevents all Cisco IOS software-initiated user messages, including the initial message that indicates the connection is “Trying...” The **busy-message** command can be used in the **autocommand** command to suppress these messages.

Examples

The following example sets a message that will be displayed on the terminal whenever an attempt to connect to the host named router1 fails. The pound sign (#) is used as a delimiting character.

```
busy-message router1 #
Cannot connect to host. Contact the computer center.
#
```

Related Commands

Command	Description
autocommand	Automatically execute a command when a user connects to a particular line.

clear entry

To delete an entry from the list of queued host-initiated connections, use the **clear entry** command in EXEC mode.

clear entry *number*

Syntax Description

<i>number</i>	An entry number obtained from the show entry EXEC command.
---------------	---

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example deletes pending entry number 3 from the queue:

```
Router# clear entry 3
```

Related Commands

Command	Description
show entry	Displays the list of queued host-initiated connections to a router.

connect

To log in to a host that supports Telnet, rlogin, or local-area transport (LAT), use the **connect** command in EXEC mode.

connect *host* [*port*] [*keyword*]

Syntax Description

<i>host</i>	A host name or an IP address.
<i>port</i>	(Optional) A decimal TCP port number; the default is the Telnet router port (decimal 23) on the host.
<i>keyword</i>	(Optional) One of the keywords listed in Table 8 .

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced in a release prior to Cisco IOS Release 10.0.
12.0(21)ST	The /ipv4 and /ipv6 keywords were added.
12.1	The /quiet keyword was added.
12.2(2)T	Support for the /ipv4 and /ipv6 keywords was integrated into Cisco IOS Release 12.2(2)T.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

[Table 8](#) lists the optional **connect** command keywords.

Table 8 *connect* Keyword Options

Option	Description
/debug	Enables Telnet debugging mode.
/encrypt kerberos	Enables an encrypted Telnet session. This keyword is available only if you have the Kerberized Telnet subsystem. If you authenticate using Kerberos Credentials, the use of this keyword initiates an encryption negotiation with the remote server. If the encryption negotiation fails, the Telnet connection will be reset. If the encryption negotiation is successful, the Telnet connection will be established, and the Telnet session will continue in encrypted mode (all Telnet traffic for the session will be encrypted).
/ipv4	Forces the use of IP version 4.
/ipv6	Forces the use of IP version 6.

Table 8 *connect Keyword Options (continued)*

Option	Description
/line	Enables Telnet line mode. In this mode, the Cisco IOS software sends no data to the host until you press the Enter key. You can edit the line using the standard Cisco IOS software command editing characters. The /line keyword is a local switch; the remote router is not notified of the mode change.
/noecho	Disables local echo.
/quiet	Prevents onscreen display of all messages from the Cisco IOS software.
/route path	Specifies loose source routing. The <i>path</i> argument is a list of host names or IP addresses that specify network nodes and ends with the final destination.
/source-interface	Specifies the source interface.
/stream	Turns on <i>stream</i> processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
bgp	Border Gateway Protocol.
chargen	Character generator.
cmd rcmd	Remote commands.
daytime	Daytime.
discard	Discard.
domain	Domain Naming Service.
echo	Echo.
exec	EXEC.
finger	Finger.
ftp	File Transfer Protocol.
ftp-data	FTP data connections (used infrequently).
gopher	Gopher.
hostname	Host name server.
ident	Ident Protocol.
irc	Internet Relay Chat.
klogin	Kerberos login.
kshell	Kerberos shell.
login	Login (rlogin).
lpd	Printer service.
nntp	Network News Transport Protocol.
node	Connect to a specific LAT node.
pop2	Post Office Protocol v2.
pop3	Post Office Protocol v3.
port	Destination LAT port name.
port-number	Port number.

Table 8 *connect Keyword Options (continued)*

Option	Description
smtp	Simple Mail Transport Protocol.
sunrpc	Sun Remote Procedure Call.
syslog	Syslog.
tacacs	Specify TACACS security.
talk	Talk.
telnet	Telnet.
time	Time.
uucp	UNIX-to-UNIX Copy Program.
whois	Nickname.
www	World Wide Web.

With the Cisco IOS software implementation of TCP/IP, you are not required to enter the **connect**, **telnet**, **lat**, or **rlogin** commands to establish a terminal connection. You can enter only the learned host name—as long as the host name is different from a command word in the Cisco IOS software. The Cisco IOS software assigns a logical name to each connection, and several commands use these names to identify connections. The logical name is the same as the host name, unless that name is already in use, or you change the connection name with the **name-connection EXEC** command. If the name is already in use, the Cisco IOS software assigns a null name to the connection. To display a list of the available hosts, use the **show hosts** command. To display the status of all TCP connections, use the **show tcp** command.

Examples

The following example establishes an encrypted Telnet session from a router to a remote host named host1:

```
Router> connect host1 /encrypt kerberos
```

The following example routes packets from the source system named host1 to router1.cisco.com, then to 10.1.0.11, and finally back to host1:

```
Router> connect host1 /route:router1.cisco.com 10.1.0.11 host1
```

The following example connects to a host with logical name host1:

```
Router> host1
```

The following example suppresses all onscreen messages from the Cisco IOS software during login and logout:

```
Router> connect host2 /quiet
```

The following example shows the limited messages displayed when connection is done using the optional **/quiet** keyword:

```
login:User2
```

```
Password:
```

```

Welcome to OpenVMS VAX version V6.1 on node CRAW
Last interactive login on Tuesday, 15-DEC-1998 11:01
Last non-interactive login on Sunday, 3-JAN-1999 22:32
```

Server3) **logout**

User2 logged out at 16-FEB-2000 09:38:27.85

Related Commands

Command	Description
kerberos clients mandatory	Causes the rsh , rcp , rlogin , and telnet commands to fail if they cannot negotiate the Kerberos Protocol with the remote server.
l2f ignore-mid-sequence	Specifies a connection to a particular LAT node that offers LAT services.
lat	Connects to a LAT host.
name-connection	Assigns a logical name to a connection.
rlogin	Logs in to a UNIX host using rlogin.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.
show tcp	Displays the status of TCP connections.
telnet	Logs in to a host that supports Telnet.

connection wait

To specify how users accessing a router using Telnet, Secure Shell (SSH), or the console port will be connected, use the **connection wait** command in transport map configuration mode. To restore the default setting of waiting for an IOS vty line to become available while also allowing the user to enter diagnostic mode if the connection that is waiting for the IOS vty line is interrupted, use the **no** or **default** form of the command.

connection wait [**allow** [**interruptable**]| **none** [**disconnect**]]

no connection wait [**allow** [**interruptable**]| **none** [**disconnect**]]

Syntax Description

allow	Specifies the Telnet or SSH connection will wait for the IOS process to become available, and will exit the router if interrupted. This option is not available for console port transport maps.
allow interruptable	Specifies the Telnet, SSH, or console port connection will wait for the IOS process to become available, and also will allow users to enter diagnostic mode by interrupting a Telnet connection waiting for the IOS process to become available.
none	Specifies the Telnet, SSH, or console port connection immediately enters diagnostic mode.
none disconnect	Specifies the Telnet or SSH connection will not wait for the IOS process and will not enter diagnostic mode, so all Telnet or SSH connections are rejected. This option is not available for console port transport maps.

Command Default

The default connection setting is **allow interruptable**.

Command Modes

Transport map configuration (config-tmap)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

When **connection wait allow interruptable** is configured, users enter diagnostic mode by sending a break signal while waiting to connect to the IOS process. The **Ctrl-C** or **Ctrl-Shift-6** sequences are used to send a break signal.

For a persistent Telnet connection to access IOS on the Cisco ASR 1000 Series Routers, local login authentication must be configured for the vty line (the **login** command in line configuration mode). If local login authentication is not configured, users will not be able to access IOS using a Telnet connection into the Management Ethernet interface with an applied transport map. Diagnostic mode will still be accessible in this scenario.

Examples

In the following example, a transport map that makes all Telnet connections wait for the IOS vty line to become active before connecting to the router, while also allowing the user to interrupt the process and enter diagnostic mode, is configured and applied to the Management Ethernet interface (interface gigabitethernet 0).

A diagnostic and a wait banner are also configured.

The transport map is then applied to the interface when the **transport type persistent telnet input** command is entered to enable persistent Telnet.

```
Router(config)# transport-map type persistent telnet telnethandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for IOS Process--
X

Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler
```

In the following example, a transport map to set console port access policies is created and attached to console port 0.

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
Welcome to diagnostic mode
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS prompt
X
Router(config-tmap)# exit

Router(config)# transport type console 0 input consolehandler
```

Related Commands

Command	Description
authentication-retries	Specifies the number of SSH authentication retries before dropping the connection when a persistent SSH transport map is applied to the receiving interface.
banner (transport map)	Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of the transport map configuration.
rsa keypair-name	Names the RSA keypair to be used for persistent SSH connections.
show platform software configuration access policy	Displays the access policy and banner settings for console, Telnet, and SSH connections.
time-out	Specifies the SSH timeout interval in seconds.
transport interface	Applies the transport map settings to the interface.

Command	Description
transport type persistent	Applies an already-configured persistent transport map to an interface.
transport-map type persistent	Creates and names a persistent transport map enters transport map configuration mode.

description (ruleset)

To add a description about a translation ruleset, use the **description** command in translate ruleset configuration mode. To remove the description, use the **no** form of this command.

description *text*

no description *text*

Syntax Description

<i>text</i>	One-line description of the ruleset, up to 240 characters.
-------------	--

Defaults

No default behavior or values

Command Modes

Translate ruleset configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Only one description line is accepted. If you reenter this command, the new description replaces the existing description.

Examples

The following example shows how to add a description to a ruleset:

```
translate ruleset A from pad to telnet
description Template A for site 101
skip dest-addr ^55554$ source-addr ^4444$
match dest-addr ^5555.$ source-addr ^4444$
set telnet dest-addr 10.2.2.1
substitute pad dest-addr ^5555(.) into telnet dest-port 23
```

Related Commands

Command	Description
match (ruleset)	Identifies a connection for processing by the translation ruleset.
options (ruleset)	Specifies protocol translation options in a translation ruleset.
set (ruleset)	Unconditionally sets one or more connection parameters to a fixed value for a translation ruleset.
show translate ruleset	Displays a summary of a specific or of all configured translation rulesets, behavioral parameters, and usage statistic.
skip (ruleset)	Identifies a connection for omission by the translation ruleset.

Command	Description
substitute (ruleset)	Matches an available protocol and substitutes another in a translation ruleset.
test (ruleset)	Tests parameter values in a translation ruleset using regular expressions.
test translate	Displays a trace of protocol translation behavior for a connection attempt.
translate ruleset	Defines a unique name for a translation ruleset, specifies translated protocols, and enters translate ruleset configuration mode.
x25 pvc translate ruleset	Configures PVCs that are valid for protocol translation rule set handling.

flush-at-activation

To discard any data or noise characters that are sitting in the input buffer of the asynchronous line before the line is activated, use the **flush-at-activation** command in line configuration mode. To keep any data or noise characters that are sitting in the input buffer of the asynchronous line before the line is activated, use the **no** form of this command.

flush-at-activation

no flush-at-activation

Syntax Description This command has no keywords or arguments.

Defaults Enabled by default.

Command Modes Line configuration

Command History	Release	Modification
	11.1(5)	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines For an incoming call on a line configured with modem control (using the **modem inout** and **modem dialin** commands), the line will be activated when the data set ready (DSR) signal goes high and will be dropped when the DSR signal goes low. While the line is idle, its input buffer may receive characters; for example, modem result codes such as “NO CARRIER” or “RING” or line noise. Such characters are not useful to the line application. Flushing the line input buffer when the DSR goes high using the **flush-at-activation** command is the preferred behavior.



Note

To know whether the DSR signal is going high or low, use the **debug modem** command or the **show line** command. Output of these commands displays the status of DSR signal.

On most Cisco IOS platforms, there may be up to a one-second delay between when the DSR signal goes high and Cisco IOS activates the line. Therefore, some valid data received from the line may be discarded when you issue the **flush-at-activation** command. If it is important to process this valid data rather than discarding it and the application is tolerant of receiving bad data, configure the **no flush-at-activation** command.

The application that is used determines whether the system can differentiate the valid data from the bad data or the system is tolerant of receiving any data. For example, consider that the application used is TCP over IP over PPP. PPP uses a Frame Check Sequence (FCS) in a data frame format to verify the integrity of the received data. If an invalid data pattern is delivered to a PPP receiver, PPP will discard

it as a framing or FCS error. So the bad data will not be delivered to the higher layers. Even if some data is delivered up to IP and TCP, TCP has its own FCS which will reject bad data. Therefore, the application is tolerant of receiving the bad data that the line delivers.

Consider another application where incoming character data received from the line is delivered as TCP payload to a server running a pager application. Unless the pager application has implemented its own protocol to verify data integrity, this bad data may cause the pager not to be delivered, or to deliver bad data within the message payload to the receiving pager. So the bad data should not be delivered as payload to the line.

Where an upper-layer framed protocol such as PPP or Serial Line Internet Protocol (SLIP) is always used (asynchronous mode dedicated), the framed protocol may reach link status more quickly when you issue the **no flush-at-activation** command. Since the framed protocol discards any erroneous data received, you do not have to use the **flush-at-activation** command.

If the line application is not tolerant of receiving bad data; for example, when you are using character-mode username/password authentication, always use the **flush-at-activation** command. Otherwise, the bad data may trigger an application failure.

**Note**

Prior to Cisco IOS Release 12.2, the **no flush-at-activation** command was the default on AS5000 platforms with modem ISDN channel aggregation (MICA) and NextPort modems. However, from Cisco IOS Release 12.3 and later, there is no longer any significant delay between when the modem link reaches steady state (DSR high) and when the line is activated so you do not need to use the **no flush-at-activation** command.

The modem state STEADY_STATE is mapped to DSR high and TERMINATING is mapped to DSR low when asynchronous lines are the internal digital modem ports.

Examples

The following example shows how to configure lines 1/0 through 1/59 to flush any data in their input buffers when the lines are activated:

```
Router(config)# line 1/0 1/59
Router(config-line)# flush-at-activation
```

Related Commands

Command	Description
activation-character	Defines the character entered at a vacant terminal to begin a terminal session.
debug modem	Observes modem line activity on an access server.
modem dialin	Configures a line to enable a modem attached to the router to accept incoming calls only.
modem inout	Configures a line for both incoming and outgoing calls.
show line	Displays parameters of a terminal line.

ip alias

To assign an IP address to the service provided on a TCP port, use the **ip alias** command in interface configuration mode. To remove the specified address for the router, use the **no** form of this command.

ip alias *ip-address tcp-port*

no ip alias *ip-address*

Syntax Description

<i>ip-address</i>	Specifies the IP address for the service.
<i>tcp-port</i>	Specifies the number of the TCP port.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A user attempting to establish a connection is connected to the first free line in a rotary group using the Telnet protocol.

The IP address must be on the same network or subnet as the main address of the terminal server, and must not be used by another host on that network or subnet. Connecting to the IP address has the same effect as connecting to the main address of the router, using the argument *tcp-port* as the TCP port.

You can use the **ip alias** command to assign multiple IP addresses to the router. For example, in addition to the primary alias address, you can specify addresses that correspond to lines or rotary groups. Using the **ip alias** command in this way makes connection to a specific rotary group transparent to the user.

When asynchronous mode is implemented, the Cisco IOS software creates the appropriate IP aliases, which map the asynchronous addresses for the lines to which they are connected. This process is automatic and does not require configuration.

Examples

The following example configures connections to IP address 172.30.42.42 to act identically to connections made to the primary IP address of the server on TCP port 3001. In other words, a user is connected to the first free line on port 1 of the rotary group that uses the Telnet protocol.

```
ip alias 172.30.42.42 3001
```

ipx nasi-server enable

To enable NetWare Asynchronous Services Interface (NASI) clients to connect to asynchronous devices attached to your router, use the **ipx nasi-server enable** command in global configuration mode. To prevent NASI clients from connecting to asynchronous devices through a router, use the **no** form of this command.

ipx nasi-server enable

no ipx nasi-server enable

Syntax Description This command has no arguments or keywords.

Command Default NASI is not enabled.

Command Modes Global configuration

Command History	Release	Modification
	11.1	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines When you enter this command, NASI clients can connect to any port on the router, other than the console port, to access network resources. When the user on the NASI client uses the Windows or DOS application to connect to the router, a list of available tty and vty lines appear, beginning with tty1. The user can select the desired outgoing tty or vty port.

To to enable a username and password prompt for authentication, authorization, and accounting purposes, you can configure TACACS+ security on the router, after the user on the NASI client selects a tty or vty port.

Examples The following example shows a minimum configuration to enable NASI clients dial-in access with TACACS+ authentication:

```
ipx routing
ipx internal-network ncs001
interface ethernet 0
    ipx network 1
ipx nasi-server enable
! enable TACACS+ authentication for NASI clients using the list name swami
aaa authentication nasi swami tacacs+
line 1 8
    modem inout
```

 **ipx nasi-server enable****Related Commands**

Command	Description
aaa authentication nasi	Specifies AAA authentication for NASI clients connecting through the access server.
nasi authentication	Enables AAA authentication for NASI clients connecting to a router.
show ipx nasi connections	Displays the status of NASI connections.
show ipx spx-protocol	Displays the status of the Sequenced Packet Exchange (SPX) protocol stack and related counters.

keymap

To define specific characteristics of keyboard mappings, use the **keymap** command in global configuration mode. To remove the named keymap from the current image of the configuration file, use the **no** form of this command.

keymap *keymap-name* *keymap-entry*

no keymap *keymap-name*

Syntax Description

<i>keymap-name</i>	Name of the file containing the keyboard mappings. The name can be up to 32 characters long and must be unique.
<i>keymap-entry</i>	Commands that define the keymap.

Defaults

VT100 keyboard emulation

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **keymap** command maps individual keys on a non-TN3270 keyboard to perform the function defined for the TN3270 keyboard. Use the **show keymap EXEC** command to test for the availability of a keymap.

Do not use the name “default” for a ttycap entry filename or the Cisco IOS software will adopt the newly defined entry as the default.

The guidelines for creating a keymap follow.

The Keymap Entry Structure

A keymap is a keyboard map file. A keymap consists of an entry for a keyboard. The first part of a keymap lists the names of the keyboards that use that entry. These names will often be the same as in the ttycaps (terminal emulation) file, and often the terminals from various ttycap entries will use the same keymap entry. For example, both 925 and 925vb (for 925 with visual bells) terminals would probably use the same keymap entry. There are other circumstances in which it is necessary to specify a keyboard name as the name of the entry (for example, if a user requires a custom key layout).

After the names, which are separated by vertical bars (|), comes an open brace ({), the text that forms the definitions, the a close brace (}), as follows:

```
ciscodefault{
clear = '^z';\
flinp = '^x';\
```

```

enter = '^m';\
delete = '^d' | '^?';\
synch = '^r';\
ebcdic_xx='string'
reshow = '^v';
eof = '^e';\
tab = '^i';\
btab = '^b';\
nl = '^n';\
left = '^h';\
right = '^l';\
up = '^k';\
down = '^j';\
einp = '^w';\
reset = '^t';\
ferase = '^u';\
insrt = '\E';\
pa1 = '^p1'; pa2 = '^p2'; pa3 = '^p3';\
pfk1 = '\E1'; pfk2 = '\E2'; pfk3 = '\E3'; pfk4 = '\E4';\
pfk5 = '\E5'; pfk6 = '\E6'; pfk7 = '\E7'; pfk8 = '\E8';\
pfk9 = '\E9'; pfk10 = '\E0'; pfk11 = '\E-'; pfk12 = '\E=';\
pfk13 = '\E!'; pfk14 = '\E@'; pfk15 = '\E#'; pfk16 = '\E$';\
pfk17 = '\E%'; pfk18 = '\E'; pfk19 = '\E&'; pfk20 = '\E*';\
pfk21 = '\E('; pfk22 = '\E)'; pfk23 = '\E_'; pfk24 = '\E+';\
}

```

Each definition consists of a reserved keyword, which identifies the TN3270 function, followed by an equal sign (=), followed by the various ways to generate this particular function, followed by a semicolon (;), as follows:

```
pa1 = '^p1'; pa2 = '^p2'; pa3 = '^p3';\
```

Each alternative way to generate the function is a sequence of ASCII characters enclosed inside single quotes (' '); the alternatives are separated by vertical bars (|), as follows:

```
delete = '^d' | '^?';\
```

Inside the single quotes, a few characters are special. A caret (^) specifies that the next character is a control (Ctrl) character. The two-character string caret-a (^a) represents Ctrl-a. The caret-A sequence (^A) generates the same code as caret-a (^a). To generate Delete (or DEL), enter the caret-question mark (^?) sequence.


Note

The Ctrl-caret combination (Ctrl-^), used to generate a hexadecimal 1E, is represented as two caret symbols in sequence (^ ^)—not as a caret-backslash-caret combination (^ \ ^).

In addition to the caret, a letter can be preceded by a backslash (\). Because this sequence has little effect for most characters, its use is usually not recommended. In the case of a single quote ('), the backslash prevents that single quote from terminating the string. In the case of a caret (^), the backslash prevents the caret from having its special meaning. To include the backslash in the string, place two backslashes (\\) in the keymap. [Table 9](#) lists other supported special characters.

Table 9 *Special Characters Supported by TN3270 Keymap Capability*

Character	Description
\E	Escape character
\n	Newline

Table 9 *Special Characters Supported by TN3270 Keymap Capability (continued)*

Character	Description
\t	Tab
\r	Carriage return

Each character in a string needs not be enclosed within single quotes. For example, `\E\E\E` means three escape characters.

To enter a keymap, provide a unique name for it and explicitly define all special keys you intend to include in it within open and close braces. Also, except for the last line, each line must be terminated with a backslash symbol (`\`). The last line ends with the closing bracket (`}`) symbol and an end-of-line character.

Keymap Restrictions

When IBM-style TN3270 terminals are emulated, a mapping must be performed between sequences of keys pressed at an ASCII keyboard and the keys available on a TN3270 keyboard. For example, a TN3270 keyboard has a key labeled EEOF that erases the contents of the current field from the location of the cursor to the end. To accomplish this function, the terminal user and a program emulating a TN3270 keyboard must agree on which keys will be typed to invoke the function. The requirements for these sequences follow:

- The first character of the sequence must be outside of the standard ASCII printable characters.
- No sequence can be a complete subset of another sequence (although sequences can share partial elements).

Following are examples of acceptable keymap entries:

```
pfk1 = '\E1';
pfk2 = '\E2';
```

Following are examples of unacceptable keymap entries:

```
pfk1 = '\E1';
pfk11 = '\E11';
```

In the acceptable example, the keymap entry for pfk1 is not completely included in the keymap entry for pfk2. By contrast, in the unacceptable, or conflicting keymap pair, the sequence used to represent pfk1 is a complete subset of the sequence used to represent pfk11. See the keymap entry provided later in the Examples section of how various keys can be represented to avoid this kind of conflict.

[Table 10](#) lists TN3270 key names that are supported in this keymap. Note that some of the keys do not exist on a TN3270 keyboard. An unsupported function will cause the Cisco IOS software to send a (possibly visual) bell sequence to the terminal.

Table 10 *TN3270 Key Names Supported by Defaults Keymap*

TN3270 Key Name	Functional Description
LPRT	Local print ¹
DP	Duplicate character
FM	Field mark character
CURSEL	Cursor select
CENTSIGN	EBCDIC cent sign

Table 10 ***TN3270 Key Names Supported by Defaults Keymap (continued)***

TN3270 Key Name	Functional Description
RESHOW	Redisplay the screen
EINP	Erase input
EEOF	Erase end of field
DELETE	Delete character
INSRT	Toggle insert mode
TAB	Field tab
BTAB	Field back tab
COLTAB	Column tab
COLBAK	Column back tab
INDENT	Indent one tab stop
UNDENT	Undent one tab stop
NL	New line
HOME	Home the cursor
UP	Up cursor
DOWN	Down cursor
RIGHT	Right cursor
LEFT	Left cursor
SETTAB	Set a column tab
DELTAB	Delete a column tab
SETMRG	Set left margin
SETHOM	Set home position
CLRTAB	Clear all column tabs
APLON	Apl on ¹
APLOFF	Apl off ¹
APLEND ¹	Treat input as ASCII
PCON	Xon/xoff on ¹
PCOFF	Xon/xoff off ¹
DISC	Disconnect (suspend) ¹
INIT	New terminal type ¹
ALTK	Alternate keyboard dvorak ¹
FLINP	Flush input
ERASE	Erase last character
WERASE	Erase last word ¹
FERASE	Erase field
SYNCH	In synchronization with the user
RESET	Reset key—unlock keyboard

Table 10 *TN3270 Key Names Supported by Defaults Keymap (continued)*

TN3270 Key Name	Functional Description
MASTER_RESET	Reset, unlock, and redisplay
XOFF	Please hold output ¹
XON	Please give me output ¹
WORDTAB	Tab to beginning of next word ¹
WORDBACKTAB	Tab to beginning of current or last word ¹
WORDEND	Tab to end of current or next word ¹
FIELDEND	Tab to last nonblank of current or next unprotected (writable) field ¹
PA1	Program attention 1
PA2	Program attention 2
PA3	Program attention 3
CLEAR	Local clear of the TN3270 screen
TREQ	Test request
ENTER	Enter key
PFK1 to PFK30	Program function key 1 program function key 30
ATTN	Attention
SYSREQ	System request

1. Not supported by the Cisco TN3270 implementation.

[Table 11](#) lists the proper keys used to emulate each TN3270 function when default key mappings are used.

Table 11 *Keys Used to Emulate Each TN3270 Function with Defaults Keymap*

Key Types	IBM TN3270 Key	Defaults Keys
Cursor movement keys	New Line	Ctrl-n or Home
	Tab	Ctrl-i
	Back Tab	Ctrl-b
	Back Tab	Ctrl-b
	Cursor Left	Ctrl-h
	Cursor Right	Ctrl-l
	Cursor Up	Ctrl-k
	Cursor Down	Ctrl-j or LINE FEED
Edit control keys	Delete Char	Ctrl-d or RUB
	Erase EOF	Ctrl-e
	Erase Input	Ctrl-w
	Insert Mode	ESC-Space ¹
	End Insert	ESC-Space

Table 11 *Keys Used to Emulate Each TN3270 Function with Defaults Keymap (continued)*

Key Types	IBM TN3270 Key	Defaults Keys
Program function keys	PF1	ESC 1
	PF2	ESC 2
	...	...
	PF10	ESC 0
	PF11	ESC -
	PF12	ESC =
	PF13	ESC !
	PF14	ESC @
	...	...
	PF24	ESC +
Program attention keys	PA1	Ctrl-p 1
	PA2	Ctrl-p 2
	PA3	Ctrl-p 3
Local control keys	Reset After Error	Ctrl-r
	Purge Input Buffer	Ctrl-x
	Keyboard Unlock	Ctrl-t
	Redisplay Screen	Ctrl-v
Other keys	Enter	Return
	Clear	Ctrl-z
	Erase current field	Ctrl-u

1. ESC refers to the Escape key.

Examples

The following example is the default entry used by the TN3270 emulation software when it is unable to locate a valid keymap in the active configuration image. [Table 10](#) lists the key names supported by the default Cisco TN3270 keymap.

```
keymap ciscodefault{
  clear = '^z';\
  flinp = '^x';\
  enter = '^m';\
  delete = '^d' | '^?';\
  synch = '^r';\
  reshow = '^v';\
  ebcdic_xx='string'
  eof = '^e';\
  tab = '^i';\
  btab = '^b';\
  nl = '^n';\
  left = '^h';\
  right = '^l';\
  up = '^k';\
  down = '^j';\
  einp = '^w';\
}
```

```

reset = '^t';\
ferase = '^u';\
insrt = '\E '; \
pa1 = '^p1'; pa2 = '^p2'; pa3 = '^p3';\
pfk1 = '\E1'; pfk2 = '\E2'; pfk3 = '\E3'; pfk4 = '\E4';\
pfk5 = '\E5'; pfk6 = '\E6'; pfk7 = '\E7'; pfk8 = '\E8';\
pfk9 = '\E9'; pfk10 = '\E0'; pfk11 = '\E-'; pfk12 = '\E=';\
pfk13 = '\E!'; pfk14 = '\E@'; pfk15 = '\E#'; pfk16 = '\E$';\
pfk17 = '\E%'; pfk18 = '\E'; pfk19 = '\E&'; pfk20 = '\E*';\
pfk21 = '\E('; pfk22 = '\E)'; pfk23 = '\E_'; pfk24 = '\E+';\
}

```

The following keymap statement maps the “|” character to send EBCDIC 0x6A:

```

keymap mykeys{
ebcdic_6f='|'
}

```

Related Commands

Command	Description
keymap-type	Specifies the keyboard map for a terminal connected to the line.
show keymap	Tests the availability of a keymap after a connection on a router takes place.
terminal-type	Specifies the type of terminal connected to a line.

keymap-type

To specify the keyboard map for a terminal connected to the line, use the **keymap-type** command in line configuration mode. To reset the keyboard type for the line to the default, use the **no** form of this command.

keymap-type *keymap-name*

no keymap-type

Syntax Description

<i>keymap-name</i>	Name of a keymap defined within the configuration file of the router. The TN3270 terminal-type negotiations use the specified keymap type when setting up a connection with the remote host.
--------------------	--

Defaults

VT100

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command must follow the corresponding **keymap** global configuration entry in the configuration file. The TN3270 terminal-type negotiations use the specified keymap type when setting up a connection with the remote host.

Setting the keyboard to a different keymap requires that a keymap be defined with the Cisco IOS software configuration either by obtaining a configuration file over the network that includes the keymap definition or by defining the keyboard mapping using the **keymap** global configuration command.

Use the command **show keymap EXEC** command to test for the availability of a keymap.

Examples

The following example sets the keyboard mapping to a keymap named vt100map:

```
line 3
 keymap-type vt100map
```

Related Commands

Command	Description
keymap	Defines specific characteristics of keyboard mappings.

Command	Description
show keymap	Tests the availability of a keymap after a connection on a router takes place.
ttycap	Defines characteristics of a terminal emulation file.

lat

To connect to a local-area transport (LAT) host, use the **lat** command in EXEC mode.

lat *name* [**node** *nodename* | **port** *portname* | **/debug**]

Syntax Description

<i>name</i>	LAT-learned service name.
node <i>nodename</i>	(Optional) Specifies a connection to a particular LAT node that offers a service. If you do not include the node name option, the node with the highest rating offering the service is used. Use the show lat nodes EXEC command to display information about all known LAT nodes.
port <i>portname</i>	(Optional) Specifies a destination LAT port name. This keyword is ignored in most time-sharing systems, but is used by routers and network access servers offering <i>reverse LAT</i> services. Reverse LAT involves connecting to one router from another, so that the target router runs the host portion of the protocol. Enter the port name in the format of the remote system as the <i>portname</i> argument.
/debug	(Optional) Enables a switch to display parameter changes and other special messages.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

After entering the **lat** command, you can quit the connection by pressing Ctrl-C, or complete the connection by entering the password for a given service.

You can have several concurrent LAT sessions open and switch between them. To open a subsequent session, first enter the escape sequence (**Ctrl-Shift-6** then **x** [**Ctrl^x**] by default) to suspend the current session. Then open a new session.

To list the available LAT services, use the **show lat services** EXEC command.

You can temporarily define the list of services to which you or another user can connect. To do so, use the **terminal lat out-group** command to define the group code lists used for connections from specific lines.

To exit a session, simply log off the remote system. Then terminate an active LAT session by entering the **exit** command.

If your preferred transport is set to **lat**, you can use the **connect** command in place of the **lat** command. Refer to the chapter “Configuring Terminal Operating Characteristics for Dial-In Sessions” in the *Cisco IOS Terminal Services Configuration Guide* for more information about configuring a preferred transport type. When your preferred transport is set to **none** or to another protocol, you must use the **lat** command to connect to a LAT host.

Examples

The following sample command and output shows a LAT connection from the router named Router_A to host eng2:

```
Router_A> lat eng2
Trying ENG2...Open
      ENG2 - VAX/VMS V5.2
Username: User1
Password:
      Welcome to VAX/VMS version V5.2 on node ENG2
      Last interactive login on Friday, 1-APR-1994 19:46
```

The system informs you of its progress by displaying the messages “Trying <system>...” and then “Open.” If the connection attempt is not successful, you receive a failure message.

The following sample command establishes a LAT connection from the router named Router_B to a device named our-modems and specifies port 24, which is a special modem:

```
Router_B> lat our-modems port 24
```

The following sample command establishes a LAT connection from the router named Router_C to a device named our-modems and specifies a node named eng:

```
Router_C> lat our-modems node eng
```

The following sample command and output shows the LAT session debugging capability:

```
Router_D> lat Eng2 /debug
Trying ENG2...Open
      ENG2 - VAX/VMS V5.2
Username: User1
Password:
      Welcome to VAX/VMS version V5.2 on node ENG2
      Last interactive login on Tuesday, 5-APR-1994 19:02
[Set Flow out off, Flow in on, Format 8:none, Speed 9600/9600]
[Set Flow out off, Flow in on, Format 8:none, Speed 9600/9600]
$ set ter/speed=2400
[Set Flow out off, Flow in on, Format 8:none, Speed 2400/2400]
```

A variety of LAT events are reported, including all requests by the remote system to set local line parameters. The messages within brackets ([]) are the messages produced by the remote system setting line characteristics to operating system defaults.

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
ip alias	Assigns an IP address to the service provided on a TCP port.
show lat services	Displays information about learned LAT services in the Cisco IOS software.
terminal lat out-group	Temporarily defines the list of services to which you or another user can connect.

lat access-list

To specify access conditions to nodes on the local-area transport (LAT) network, use the **lat access-list** command in global configuration mode. To remove a specified access list number, use the **no** form of this command.

lat access-list *number* {**permit** | **deny**} *nodename*

no lat access-list *number*

Syntax Description

<i>number</i>	Specifies a number ranging from 1 to 199 assigned to the line using the access-class line configuration command.
permit	Allows any matching node name to access the line.
deny	Denies access to any matching node name.
<i>nodename</i>	Specifies the name of the LAT node, with or without regular expression pattern matching characters, with which to compare for access. The UNIX-style regular expression characters allow for pattern matching of characters and character strings in the node name.

Defaults

No access conditions are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Regular expressions are case sensitive. Because LAT node names are always in all uppercase letters, make sure you use only all uppercase regular expressions.

[Table 12](#) and [Table 13](#) list pattern and character matching symbols and their use. A more complete description of the pattern matching characters is found in the “Regular Expressions” appendix in the *Cisco IOS Terminal Services Configuration Guide*.

Table 12 *Pattern Matching*

Character	Description
\0	Replaces the entire original address.
\1..9	Replaces the strings that match the first through ninth parenthesized part of X.121 address.
*	Matches 0 or more sequences of the regular expressions.

Table 12 **Pattern Matching**

Character	Description
+	Matches 1 or more sequences of the regular expressions.
?	Matches the regular expression of the null string.

Table 13 **Character Matching**

Character	Description
^	Matches the null string at the beginning of the input string.
\$	Matches the null string at the end of the input string.
\char	Matches char.
.	Matches any single character.

Examples

The following example permits all packets destined for any LAT node named WHEEL:

```
lat access-list 1 permit WHEEL
```

The following example denies all packets destined for any LAT node name beginning with the BLDG1-prefix:

```
lat access-list 2 deny ^BLDG1-
```

Related Commands

Command	Description
accept dialin	Defines access list restrictions on incoming and outgoing connections.

lat enabled

To enable local-area transport (LAT), use the **lat enabled** command in interface configuration mode. To disable LAT, use the **no** form of this command.

lat enabled

no lat enabled

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables LAT on Ethernet interface 0:

```
interface ethernet 0
 lat enabled
```

The following example disables LAT on Ethernet interface 0:

```
interface ethernet 0
 no lat enabled
```

lat group-list

To allow a name to be assigned to the group list, use the **lat group-list** command in global configuration mode. To remove the specified group list, use the **no** form of this command.

lat group-list *groupname* { *number* | *range* | **all** } [**enabled** | **disabled**]

no lat group-list *groupname* { *number* | *range* | **all** } [**enabled** | **disabled**]

Syntax Description	<i>groupname</i>	Specifies a group code name.
	<i>number</i>	Specifies a group code number. You can enter both a group code name and group code numbers.
	<i>range</i>	Specifies a hyphenated range of numbers.
	all	Specifies the range from 0 to 255.
	enabled	(Optional) Allows incremental changes to the list; that is, you can add a group code without retyping the entire command.
	disabled	(Optional) Allows selective removal of a group code from the list.

Defaults None. A group list is any combination of group names, numbers, or ranges. No group names are assigned to the list by default.

Command Modes Global configuration

Command History	Release	Modification
	11.1	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Specifying a name for a group list simplifies the task of entering individual group codes. In other words, a name makes it easier to refer to a long list of group code numbers. The group list must already exist. Use the **show lat groups EXEC** command to see a list of existing groups.

Examples The following example creates the new group named stockroom and defines it to include the group numbers 71 and 99:

```
lat group-list stockroom 71 99
```

The following example adds group code 101 to the group named stockroom:

```
lat group-list stockroom 101 enabled
```

The following example deletes the group named Bldg-2:

■ lat group-list

```
no lat group-list Bldg-2
```

Related Commands

Command	Description
lat out-group	Defines a group list for the outgoing user-initiated connections for a line.
lat service-group	Specifies a group code mask to use when advertising all services for this node and to control incoming services.
show lat groups	Displays the groups that were defined in the Cisco IOS software.

lat host-buffers

To set the number of receive buffers that will be negotiated when the router is acting as a local-area transport (LAT) host, use the **lat host-buffers** command in global configuration mode. To return to the default of one receive buffer, use the **no** form of this command.

lat host-buffers *receive-buffers*

no lat host-buffers *receive-buffers*

Syntax Description	<i>receive-buffers</i> Specifies the number of receive buffers that will be negotiated. Valid values range from 1 to 128.							
Defaults	One receive buffer							
Command Modes	Global configuration							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>10.0</td><td>This command was introduced.</td></tr><tr><td>12.2SX</td><td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td></tr></table>		Release	Modification	10.0	This command was introduced.	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Release	Modification							
10.0	This command was introduced.							
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.							
Usage Guidelines	Before LAT Version 5.2, LAT allowed only one outstanding message at a time on a virtual circuit. This restriction could limit the performance of large routers. For example, only one Ethernet packet of data could be in transit at a time. With LAT Version 5.2, nodes can indicate that they are willing to receive more than one message at a time. During virtual circuit startup, each side communicates to the other how many outstanding messages it is willing to accept.							
Examples	The following example enables LAT and configures the LAT host to negotiate 100 receive buffers: <pre>lat enabled lat host-buffers 100</pre>							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>lat server-buffers</td><td>Sets the number of receive buffers that will be negotiated when the router is acting as a LAT server.</td></tr></table>		Command	Description	lat server-buffers	Sets the number of receive buffers that will be negotiated when the router is acting as a LAT server.		
Command	Description							
lat server-buffers	Sets the number of receive buffers that will be negotiated when the router is acting as a LAT server.							

lat ka-timer

To set the rate of the keepalive timer, use the **lat ka-timer** command in global configuration mode. To restore the default, use the **no** form of this command.

lat ka-timer *seconds*

no lat ka-timer

Syntax Description	<i>seconds</i>	Timer rate, in seconds. Valid values for the timer rate range from 10 to 255 seconds.
--------------------	----------------	---

Defaults	20 seconds
----------	------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	The keepalive timer sets the rate that messages are sent in the absence of actual traffic between the router and the remote node. The server uses keepalive messages to detect when communication with a remote node is disrupted or when the remote node has crashed.
------------------	--

Examples	The following example sets the keepalive timer rate to 5 seconds: <pre>lat ka-timer 5</pre>
----------	--

lat node

To change the local-area transport (LAT) node name without changing the system host name, use the **lat node** command in global configuration mode.

lat node *node-name*

Syntax Description

<i>node-name</i>	Name of the LAT node.
------------------	-----------------------

Defaults

No default LAT node name

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command allows you to give the server a node name that is different from the host name. Use the **show entry EXEC** command to determine which LAT hosts have queue entries for printers on the servers. Use the **clear entry EXEC** command to delete entries from the queue.

Examples

The following example specifies the LAT node name as DEC2:

```
lat node DEC2
```

Related Commands

Command	Description
clear entry	Deletes an entry from the list of queued host-initiated connections.
hostname	Specifies or modifies the host name for the network server.
show entry	Displays the list of queued host-initiated connections to a router.

lat out-group

To define a group list for outgoing user-initiated connections on a line, use the **lat out-group** command in line configuration mode. To return to the default value, use the **lat out-group 0** command.

lat out-group {*group-name number* | *range* | **all**}

Syntax Description

<i>group-name</i>	Group code name.
<i>number</i>	Group code number. You can also enter both a group code name and group code numbers.
<i>range</i>	Hyphenated range of numbers.
all	Range from 0 to 255.

Defaults

The default group code number is 0.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can have values for one, two, or all three arguments. If the **all** keyword is specified, no arguments can be used. You can enter the *group-name*, *number*, and *range* values in any order.

Use the **show lat groups EXEC** command to display group numbers. If the host node and router do not share a common group number, the host services will not be displayed.

Examples

The following example defines the services for lines 1 through 7, 10 through 17, and 20 through 24. Access to systems on the first set of lines is limited to groups 12 and 18 through 23; the second set is limited to group 12; the third set is limited to group codes 12, 18 through 23, and 44. All other lines use the default of group 0.

```
line 1 7
  lat out-group 12 18-23
line 10 17
  lat out-group 12
line 20 24
  lat out-group 12 18-23 44
```

Related Commands

Command	Description
lat group-list	Allows a name to be assigned to the group list, which is any combination of group names, numbers, or ranges.
show lat groups	Displays the groups that were defined in the Cisco IOS software with the lat group-list command.

lat remote-modification

To enable remote local-area transport (LAT) modification of line characteristics (for example, baud rate), use the **lat remote-modification** command in line configuration mode. To disable remote LAT modification of line characteristics, use the **no** form of this command.

lat remote-modification

no lat remote-modification

Syntax Description

This command has no arguments or keywords.

Defaults

Remote modification is disabled.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Enabling the line for remote modification allows the remote LAT node to change line characteristics (for example, baud rate, parity, and so on).

Examples

The following example enables remote LAT modification on line 4:

```
line 4
 lat remote-modification
```

lat retransmit-limit

To set the number of times that local-area transport (LAT) resends a message before declaring the remote system unreachable, use the **lat retransmit-limit** command in global configuration mode. To restore the default retry value, use the **no** form of this command.

lat retransmit-limit *number*

no lat retransmit-limit

Syntax Description	<i>number</i>	Number of retries. Valid values range from 4 to 255 retries.
---------------------------	---------------	--

Defaults	8 retries
-----------------	-----------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	Assigning larger values to the number of tries increases the robustness of the LAT service at the cost of longer delays when communications are disrupted. Because LAT generally resends messages once per second, the value is approximately the number of seconds that LAT connections will survive connection disruption.
-------------------------	--

If you bridge LAT, the retransmission limit should be set to at least 20 tries for LAT sessions to survive a worst-case spanning-tree reconfiguration, because the time for bridging spanning-tree reconfiguration to be completed can be up to 15 seconds.

Examples	The following example sets the retransmission limit to 30 tries, enough time to sustain the downtime incurred when the system must reconfigure a spanning-tree topology:
-----------------	--

```
lat retransmit-limit 30
```

lat server-buffers

To set the number of receive buffers that will be negotiated when the router is acting as a local-area transport (LAT) server, use the **lat server-buffers** command in global configuration mode. To return to the default of one receive buffer, use the **no** form of this command.

lat server-buffers *receive-buffers*

no lat server-buffers *receive-buffers*

Syntax Description

receive-buffers Specifies the number of receive buffers that will be negotiated. Valid values range from 1 to 128 receive buffers. The default value is 1 receive buffer.

Defaults

1 receive buffer

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before LAT Version 5.2, LAT allowed only one outstanding message on a virtual circuit at a time. This restriction could limit the performance of large routers because only one Ethernet packet of data could be in transit at a time. With LAT Version 5.2, nodes can indicate that they are willing to receive more than one message at a time. During virtual circuit startup, each side communicates to the other how many outstanding messages it is willing to accept.

Examples

The following example enables LAT and configures the server to negotiate 25 receive buffers:

```
lat enabled
lat server-buffers 25
```

Related Commands

Command	Description
lat host-buffers	Sets the number of receive buffers that will be negotiated when the router is acting as a LAT host.

lat service enabled

To enable inbound connections to the specified service and enable the advertisement of this service to routers on the network, use the **lat service enabled** command in global configuration mode. To delete the named service, use the **no** form of this command.

lat service *service-name* **enabled**

no lat service *service-name* **enabled**

Syntax Description

service-name Name of the service.

Defaults

No services are enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In the simplest form, this command creates a service that gives connecting users access to a vty port on the server.

Use the **lat service enabled** command after commands that define a service so that users do not connect to a service before all the parameters are set.

Deleting a service does not disconnect existing connections.

Examples

The following example enables inbound connections to the service named WHEEL:

```
lat service WHEEL enabled
```

lat service-host

To statically define local-area transport (LAT) services, use the **lat service-host** command in interface configuration mode. To remove the statically defined LAT services, use the **no** form of this command.

lat service-host *node-name service-name MACaddress*

no lat service-host

Syntax Description

<i>node-name</i>	The remote node providing this service.
<i>service-name</i>	The name of the service.
<i>MAC address</i>	MAC address entered as three hexadecimal numbers of four digits separated by a period MAC address of the remote node.

Command Default

LAT services are not statically defined.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use the **show running-config** command to verify if the LAT services have been configured.

Examples

The following example shows how to statically define LAT services:

```
Router# configure terminal
Router(config)# interface FastEthernet0/0
Router(config-if)# lat service-host node1 service1 0000.fc08.12ab
```

Related Commands

Command	Description
show running-config	Displays the running configuration.

lat service ident

To set the local-area transport (LAT) service identification for a specified service, use the **lat service ident** command in global configuration mode. To remove the identification, use the **no** form of this command.

lat service *service-name* **ident** *identification*

no lat service *service-name* **ident**

Syntax Description

<i>service-name</i>	Name of the service.
<i>identification</i>	Descriptive name (text only) that identifies the service.

Defaults

No LAT service identification is set for specific services.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The identification is advertised to other servers on the network and is displayed along with the list of name services on the LAN.

Examples

The following example specifies the identification “Welcome to Gateway-A” on the service named host1:

```
lat service host1 ident Welcome to Gateway-A
```

lat service password

To set up a local-area transport (LAT) password for a service, use the **lat service password** command in global configuration mode. To remove the password, use the **no** form of this command.

lat service *service-name* **password** *password*

no lat service *service-name* **password**

Syntax Description

<i>service-name</i>	Name of the service.
<i>password</i>	Password used to gain access to the service.

Defaults

No default LAT service passwords

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The connecting user will be required to enter the password to complete the connection. The password is obtained through the LAT password mechanism.

Examples

The following example specifies a service named `host1` and the password `secret`:

```
lat service host1 password secret
```

lat service rating

To set a static service rating for the specified service, use the **lat service rating** command in global configuration mode. To remove the service rating, use the **no** form of this command.

lat service *service-name* **rating** *static-rating*

no lat service *service-name* **rating**

Syntax Description	<i>service-name</i>	Name of the service.
	<i>static-rating</i>	Static service rating. The rating must be in the range from 1 to 255.

Defaults	Dynamic rating
-----------------	----------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	If this command is not entered, the Cisco IOS software calculates a dynamic rating based on the number of free ports that can handle connections to the service. Setting a static rating overrides this calculation and causes the specified value to be used.
-------------------------	--

Examples	The following example specifies a service rating of 84 on the service named WHEEL: lat service WHEEL rating 84
-----------------	---

lat service rotary

To associate a rotary group with a service, use the **lat service rotary** command in global configuration mode. To remove the association, use the **no** form of this command.

lat service *service-name* **rotary** *group-number*

no lat service *service-name* **rotary**

Syntax Description

<i>service-name</i>	Name of the service.
<i>group-number</i>	Rotary group number.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Establish rotary groups using the **rotary** line configuration command.

When an inbound connection is received for this service, the router establishes a reverse local-area transport (LAT) connection to a terminal in that rotary group.

If the rotary option is not set, the connection will be to a virtual terminal session on the router.

Examples

The following example creates a service named MODEM to establish a rotary group:

```
lat services MODEM rotary 1
```

Related Commands

Command	Description
rotary	Defines a group of lines consisting of one or more lines.

lat service-announcements

To reenable local-area transport (LAT) broadcast service announcements, use the **lat service-announcements** command in global configuration mode. To disable the sending of LAT service announcements, use the **no** form of this command.

lat service-announcements

no lat service-announcements

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If this command is enabled, the LAT code will periodically broadcast service advertisements. If the command is disabled, the LAT code will not send service announcements, so solicit information messages must be used to look up node information.



Note

You should only disable service announcements if all of the nodes on the LAN support the service responder feature.

Examples

The following example reenables the sending of broadcast service announcements:

```
lat service-announcements
```

Related Commands

Command	Description
lat service-responder	Configures a node to act as proxy for other nodes when a solicit-information multicast message is received.

lat service-group

To specify a group code mask to use when advertising all services for this node and to control incoming services, use the **lat service-group** command in global configuration mode. To remove the group code mask specified, use the **no** form of this command.

lat service-group {[*groupname*] [*number*] [*min-max*] | **all**} [**enabled** | **disabled**]

no lat service-group {[*groupname*] [*number*] [*min-max*] | **all**} [**enabled** | **disabled**]

Syntax Description

<i>groupname</i>	Specifies a group code name. Multiple group code names can be specified.
<i>number</i>	Specifies a group code number. Multiple group code numbers can be specified. Valid values for the <i>number</i> argument range from 0 to 255.
<i>min-max</i>	Specifies a hyphenated range of numbers. Multiple group code number ranges can be specified. Valid values for the <i>min</i> and <i>max</i> arguments range from 0 to 255.
all	Specifies the group number range from 0 to 255.
enabled	(Optional) Allows incremental changes to the list; you can add a group code without retyping the entire command.
disabled	(Optional) Allows selective removal of a group code from the list.

Defaults

If no service group is specified, the Cisco IOS software defaults to advertising to group 0.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When this command is written to NVRAM (using the **write memory EXEC** command), the system looks for an exact match on a group code name. If it finds one, it uses that name in the command. Otherwise, it writes out a list of numbers, using the range syntax whenever possible.

Examples

The following example specifies groups 100 through 103, then defines engineering as the group code list to advertise:

```
lat group-list engineering 100-103
lat service-group engineering enabled
```

The following example specifies the groups 1, 5, 20 through 36, and 52:

```
lat service-group 1 5 20-36 52
```

Related Commands

Command	Description
lat group-list	Allows a name to be assigned to the group list, which is any combination of group names, numbers, or ranges.

lat service-responder

To configure a node to act as proxy for other nodes when a solicit-information multicast message is received, use the **lat service-responder** command in global configuration mode. To remove any proxy definition set up using the **lat service-responder** command, use the **no** form of this command.

lat service-responder

no lat service-responder

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Cisco IOS software can be configured to support the service responder feature that is part of the latest LAT Version 5.2 specification.

Specifically, the DECserver90L+, which has less memory than other Digital Equipment Corporation servers, does not maintain a cache of learned services. Instead, the DECserver90L+ solicits information about services as they are needed.

LAT Version 5.2 nodes can respond for themselves; however LAT Version 5.1 nodes, for example, VMS Version 5.4 or earlier nodes, cannot respond for themselves. Instead, a LAT Version 5.2 node configured as a service responder must respond in proxy for the LAT Version 5.1 nodes.

The Cisco IOS software can be configured as a LAT service responder. If all your nodes are LAT Version 5.2 nodes, you need not enable the service responder features.

Examples

The following example configures a node to act as a proxy for a node when a solicit-information multicast message is received. The node configured with this command will respond to solicit messages.

```
lat service-responder
```

Related Commands	Command	Description
	lat service-announcements	Reenables LAT broadcast service announcements.

lat service-timer

To adjust the time between local-area transport (LAT) service advertisements, use the **lat service-timer** command in global configuration mode. To return to the default setting, use the **no** form of this command.

lat service-timer *seconds*

no lat service-timer

Syntax Description	<i>seconds</i>	Number of seconds between service announcements. Note that the granularity offered by this command is 10-second intervals, and the <i>seconds</i> value is rounded up.
---------------------------	----------------	--

Defaults	20 seconds
-----------------	------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.1	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	This command adjusts the time, in seconds, between LAT service announcements for services offered by the router. This function is useful in large networks with many LAT services and limited bandwidth.
-------------------------	--

Examples	The following example sets the interval between LAT service advertisements to 11, and it illustrates the rough granularity of the lat service-timer command:
-----------------	---

```
! The time between LAT service advertisements is set to 11. Because the
! granularity is in ten-second intervals, the actual time between advertisement
! is 20 seconds.
lat service-timer 11
! 20 seconds between updates.
lat service-timer 19
! 120 seconds between updates.
lat service-timer 120
```

lat vc-sessions

To set the maximum number of sessions to be multiplexed onto a single local-area transport (LAT) virtual circuit, use the **lat vc-sessions** command in global configuration mode. To remove the definition of a prior session, use the **no** form of this command.

lat vc-sessions *maximum-number*

no lat vc-sessions *maximum-number*

Syntax Description

maximum-number Specifies the number of sessions that will be multiplexed onto a single LAT virtual circuit. This number cannot be greater than 255.

Defaults

255 sessions per virtual circuit

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Setting the number of sessions to a lower number can increase throughput if many sessions are running on one host, especially with routers with many physical ports. It can also increase overhead if the same host has little traffic but a large number of sessions.

Examples

The following example sets the maximum number of sessions to be multiplexed onto a single LAT virtual circuit at 100:

```
lat vc-sessions 100
```

lat vc-timer

To set the interval of time local-area transport (LAT) waits before sending any traffic, use the **lat vc-timer** command in global configuration mode. To remove a timer definition, use the **no** form of this command.

lat vc-timer *milliseconds*

no lat vc-timer *milliseconds*

Syntax Description

<i>milliseconds</i>	Specifies the amount of time LAT will wait before sending traffic. Acceptable values range from 10 to 1000 milliseconds.
---------------------	--

Defaults

80 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Smaller timer values increase the overhead on both the router and the host. However, you can use smaller values to correct buffer overflows, which happen when the router receives more data than it can buffer during a virtual circuit timer interval.

Larger values increase the need for buffering and can cause noticeable echoing delay. However, increased values can reduce traffic. In environments with slow bridging, retransmissions can be reduced if you increase the value to at least three times the worst-case, round-trip interval.

Examples

The following example sets the time between sending messages to 500 milliseconds:

```
lat vc-timer 500
```

line

To identify a specific line for configuration and enter line configuration collection mode, use the **line** command in global configuration mode.

line [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]

Syntax Description

aux	(Optional) Auxiliary EIA/TIA-232 DTE port. Must be addressed as relative line 0. The auxiliary port can be used for modem support and asynchronous connections.
console	(Optional) Console terminal line. The console port is DCE.
tty	(Optional) Standard asynchronous line.
vty	(Optional) Virtual terminal line for remote console access.
<i>line-number</i>	Relative number of the terminal line (or the first line in a contiguous group) that you want to configure when the line type is specified. Numbering begins with zero.
<i>ending-line-number</i>	(Optional) Relative number of the last line in a contiguous group that you want to configure. If you omit any keyword, then <i>line-number</i> and <i>ending-line-number</i> are absolute rather than relative line numbers.

Defaults

There is no default line.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can address a single line or a consecutive range of lines with the **line** command. A line number is necessary, though, and you will receive an error message if you forget to include it.

Entering the **line** command with the optional line type (**aux**, **console**, **tty**, or **vty**) designates the line number as a relative line number. For example, to configure line parameters for line 7 (a TTY line), you could enter the following:

```
line tty 7
```

You also can use the **line** command without specifying a line type. In this case, the line number is treated as an absolute line number. For example, to configure line parameters for line 5, which can be of any type, you could enter the following:

```
line 5
```

Absolute line numbers increment consecutively and can be difficult to manage on large systems. Relative line numbers are a shorthand notation used in configuration. Internally, the Cisco IOS software uses absolute line numbers. You cannot use relative line numbers everywhere, but you can use absolute line numbers everywhere.

The absolute line number of the auxiliary port is 1. The relative line number of the auxiliary port is 0. See the **modem** line configuration command to set up modem support on the auxiliary port.

The software keeps a table of absolute and relative line numbers that you can display with the **show users all** EXEC command. A sample display follows:

```
Router> show users all
```

Line	User	Host(s)	Idle	Location
0 con 0				con2 console
1 tty 1				Engineering printer
2 tty 2				
3 tty 3		HOST1	1:07	Employee1 x1111
4 tty 4				Console E3-D
5 tty 5				Mkt. demo area
6 tty 6				
7 tty 7		HOST1	14	Employee2 x1112
10 tty 10				
.				
.				
.				
135 tty 135				
136 tty 136				
137 tty 137				rp4-printer
140 tty 140				Braille printer
141 aux 0				
142 vty 0	User1	idle		ROUTER-MAC.CISCO.COM
143 vty 1	User2	idle		0 HOST1.CISCO.COM
144 vty 2				
145 vty 3				
146 vty 4				
147 vty 5				

The absolute line numbers are listed at the far left, followed by the line type, and then the relative line number. Relative line numbers always begin numbering at zero and define the type of line. Addressing the second virtual terminal line as line VTY 1, for example, is easier than remembering it as line 143—its absolute line number.

The line types are ranked as follows in the line table:

1. Console 0 (con 0)
2. Standard asynchronous line (TTY)
3. Auxiliary port (aux)
4. Virtual terminal line (VTY)
5. Printer

The terminal from which you locally configure the router is attached to the console port. To configure line parameters for the console port, enter the following:

```
line console 0
```

The console relative line number must be 0.

Virtual terminal lines are used to allow remote access to the router. A virtual terminal line is not associated with either the auxiliary or console port. The router has five virtual terminal lines by default. However, you can create additional virtual terminal lines as described in the chapter “Configuring Protocol Translation and Virtual Asynchronous Devices” in the *Cisco IOS Terminal Services Configuration Guide*.

Configuring the console port or virtual terminal lines allows you to perform such tasks as setting communication parameters, specifying autobaud connections, and configuring terminal operating parameters for the terminal you are using.

Examples

The following example starts configuration for virtual terminal lines 0 to 4:

```
line vty 0 4
```

In the following example, the user creates and configures the maximum 100 virtual terminal lines with the **no login** command:

```
line vty 0 99
no login
```

In the following example, the user eliminates virtual terminal line number 5 and all higher-numbered virtual terminal lines. Only virtual terminal lines 0 to 4 will remain.

```
no line vty 5
```

In the following example, the user configures console line 0, auxiliary line 0, and virtual terminal lines 0 to 4:

```
line vty 0 4
login
line console 0
password secretWord
line aux 0
password Mypassword
no exec
access-class 1 in
speed 19200
line vty 0
exec-timeout 0 0
password Mypassword
line vty 1
exec-timeout 0 0
password Mypassword
line vty 2
exec-timeout 0 0
password Mypassword
line vty 3
password Mypassword
line vty 4
password Mypassword
```

Related Commands

Command	Description
show line	Displays the parameters of a terminal line.
show users	Displays information about the active lines on the router.

login (EXEC)

To change a login username, use the **login** command in EXEC mode.

login

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	You can change a login username if you must match outgoing access list requirements or other login prompt requirements. When you enter this command, the Cisco IOS software prompts you for a username and password. Enter the new username and the original password. If the username does not match, but the password does, the Cisco IOS software updates the session to the new username with which the login command attempt was made. If no username and password prompts appear when you enter this command, the network administrator did not specify that a username and password be required at login time. If both the username and password are entered correctly, the session becomes associated with the specified username. When you access a system using TACACS security with this command, enter your login name and specify a TACACS server using the <i>user@tacacs-server</i> syntax when the “Username:” prompt appears. The TACACS server must be one of those defined in a Cisco IOS software configuration file. For more information, refer to the sections about specifying a TACACS host in the <i>Cisco IOS Security Configuration Guide</i>, or refer to the tacacs-server host command in the <i>Cisco IOS Security Command Reference</i>. If you do not specify a host, the Cisco IOS software tries each of the TACACS servers in the list until it receives a response. If you do specify a host that does not respond, no other TACACS server is queried. The Cisco IOS software will deny access or function according to the action specified by the tacacs-server last-resort command, if one is configured. If you specified a TACACS server host with the <i>user@tacacs-server</i> command, the TACACS server specified will be used for all subsequent authentication or notification queries, with the possible exception of Serial Line Internet Protocol (SLIP) address queries.
-------------------------	---

Examples

The following example shows how login usernames and passwords can be changed. In this example, a user currently logged in under the username user1 attempts to change that login name to user2. After entering the **login** command, the user enters the new username, but enters an incorrect password. Because the password does not match the original password, the system rejects the attempt to change the username.

```
Router> login
Username: user2
Password:
% Access denied
Still logged in as "user1"
```

Next, the user attempts the login change again, with the username user2, but enters the correct (original) password. This time the password matches the current login information, the login username is changed to user2, and the user is allowed access to the EXEC at the user level.

```
Router> login
Username: user2
Password:
Router>
```

Related Commands

Command	Description
line-power	Sets up a temporary password on a line.
lockable	Enables the lock EXEC command.
password	Specifies a password on a line.
tacacs-server host	Specifies a TACACS+ host.

login (line)

To enable password checking at login, use the **login** command in line configuration mode. To disable password checking and allow connections without a password, use the **no** form of this command.

login [**local** | **tacacs**]

no login

Syntax Description

local	(Optional) Selects local password checking. Authentication is based on the username specified with the username global configuration command.
tacacs	(Optional) Selects the TACACS-style user ID and password-checking mechanism.

Defaults

Virtual terminals require a password. If you do not set a password for a virtual terminal, it responds to attempted connections by displaying an error message and closing the connection.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you specify the **login** command without the **local** or **tacacs** option, authentication is based on the password specified with the **password** line configuration command.



Note

This command cannot be used with AAA/TACACS+. Cisco recommends that you use the **login authentication** command instead of the **login (line)** configuration command. Refer to the *Cisco IOS Security Command Reference* for a description of the **login authentication** command.

Examples

The following example sets the password letmein on vty 4:

```
line vty 4
 password letmein
 login
```

The following example enables the TACACS-style user ID and password-checking mechanism:

```
line 0
 password mypassword
 login tacacs
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
virtual-profile aaa	Enables virtual profiles by AAA configuration.

login-string

To define a string of characters that is sent to a host after a successful Telnet connection, use the **login-string** command in global configuration mode. To remove the login string, use the **no** form of this command.

login-string *host-name d message [%secp] [%secw] [%b] [%m] d*

no login-string *host-name*

Syntax Description

<i>host-name</i>	Specifies the name of the host.
<i>d</i>	Sets a delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the busy message.
<i>message</i>	Specifies the login string.
<i>%secp</i>	(Optional) Sets a pause in seconds. To insert pauses into the login string, embed a percent sign (%) followed by the number of seconds to pause and the letter “p.”
<i>%secw</i>	(Optional) Prevents users from issuing commands or keystrokes during a pause.
<i>%b</i>	(Optional) Sends a Break character.
<i>%m</i>	(Optional) Supports TN3270 terminals. Sends only CR and no LINE FEED.

Defaults

No login strings are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character. To use a percent sign in the login string, precede it with another percent sign; that is, type the characters “%%.” The options can be used anywhere within the message string.

This command applies only to rlogin and Telnet sessions.

Examples

In the following example, the value *%5p* causes a 5-second pause:

```
login-string office #ATDT 555-0134
%5p hello
#
```

match (ruleset)

To identify a connection for processing by a protocol translation ruleset, use the **match** command in translate ruleset configuration mode. To remove the match statement, use one of the two **no** forms of this command.

match [*#line-number*] *incoming-connection-parameter regular-expression* [*#line-number incoming-connection-parameter regular-expression* [...]]

no match *incoming-connection-parameter regular-expression* [*incoming-connection-parameter regular-expression* [...]]

no match *#line-number* [...]

Syntax Description	<i>#line-number</i>	(Optional) The line in the ruleset to test for a match operation. The # character must be entered.
	<i>incoming-connection-parameter</i>	An incoming protocol parameter to test for; parameters are available for packet assembler/disassembler (PAD) and Telnet connections and are listed in Table 14 and Table 15 .
	<i>regular-expression</i>	Regular expression pattern to match.
	[...]	(Optional) Specifies that multiple entries can be made as follows: - Up to six match tests can be written on one command line. - Multiple line numbers can be specified using the second no form of this command.

Defaults No default behavior or values

Command Modes Translate ruleset configuration

Command History	Release	Modification
	12.3(8)T	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Up to six match tests can be written on one command line. The ellipses in the format shown above means multiple match test statements can be specified.

The **match** command is specific to the identified ruleset. A connection can be identified for processing by the ruleset match operation where tests written using keywords from [Table 14](#) and [Table 15](#), such as **dest-addr** and **dest-port**, match a regular expression.

Each protocol translation ruleset must have at least one match statement. If an incoming connection does not match any tests written in this template, it is not selected for processing by the ruleset.

The ordered set of commands in the template have line numbers that can be displayed using the **show translate EXEC** command.

Cisco regular expressions are described in Appendix A, “Regular Expressions,” in the *Cisco IOS Terminal Services Configuration Guide*.

Table 14 and Table 15 lists the protocol parameter keywords that can be specified in the match test statements for incoming PAD and Telnet connections.

Table 14 Match Keywords for Incoming PAD Connections

Keyword	Description
cud <i>ASCII-string</i>	Call user data (CUD) that occurs after the protocol identification (PID). For outgoing PAD connections, this is the optional, user-specified text included in the outgoing call request packet following the protocol identification bytes. The CUD is entered as an ASCII string.
dest-addr <i>address</i>	Destination X.121 address entered as a number from 0 to 15 digits long.
dest-addr-ext <i>address</i>	Network service access point (NSAP) destination address extension.
dlci <i>number</i>	Frame Relay data-link connection identifier (DLCI) of an Annex G service entered as a number from one to seven digits in length, although a size of two to four digits is more likely, or the NULL string if not received on an Annex G service.
interface <i>type number</i>	Interface to be used for the circuit, entered using standard Cisco IOS interface designations: Serial1/0:1, for example.
mac <i>address</i>	Connection-Mode Network Service (CMNS) service remote host MAC address entered as three hexadecimal numbers of four digits separated by a period (0000.fc08.12ab, for example) or the NULL string if not received on a CMNS service.
packetsize <i>size</i>	X.25 maximum data packet sizes to request, entered as two numbers from the following choices: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096.
pid <i>byte-string</i>	Protocol identification (PID) string specified in ASCII or hexadecimal. A hexadecimal PID must be prefixed by “0x.” For example, 0x01000000 is the standard PAD PID. Although it is available for specifying a nonstandard Call PID, this parameter is not restricted to the common PID length and can be used to specify the entire user data field.
reversed <i>flag</i>	Flag to indicate whether a reverse charged Call is permitted. This flag applies to a switched virtual circuit (SVC) and is entered as a single character, Y or N , for yes or no.
source-addr <i>address</i>	Source X.121 address.
source-addr-ext <i>address</i>	NSAP source address extension.
window size <i>size</i>	X.25 window sizes to request, entered as two numbers in a range from 1 to 127.
xot-dest-addr <i>address</i>	Destination IP address of an X.25 over TCP (XOT) service entered in standard IP address dotted decimal notation (10.0.0.127, for example) or the NULL string if not received on an XOT service.
xot-source-addr <i>address</i>	Source IP address of an XOT service entered in standard IP address dotted decimal notation (10.0.0.127, for example) or the NULL string if not received on an XOT service.

Table 15 Match Keywords for Incoming Telnet Connections

Keyword	Description
dest-addr <i>address</i>	Destination IP address entered in standard IP address dotted decimal notation: 10.0.0.127, for example.
dest-port <i>port</i>	Destination port entered as a decimal number from one to five digits long.
source-addr <i>address</i>	Source IP address entered in standard IP address dotted decimal notation: 10.0.0.127, for example.

Examples

The following example shows how to write match and skip tests to ignore connection attempts from any subnetwork address starting with 10 and match only those with a specific IP address and destination port number:

```
translate ruleset customer-case-1 from telnet to pad
! Ignore an incoming Telnet attempt from any subnetwork address starting with 10
skip source-addr ^10\.
! Match an incoming Telnet attempt destined for an IP addresses starting
! with 172.18., and a 5-digit port starting with 10 or 11
match dest-addr ^172\.18\.* dest-port ^1[0-1]...$
! Or match an incoming Telnet attempt destined an IP addresses starting
! with 172.18., and a 5-digit port starting with 120 through 127
match dest-addr ^172\.18\.* dest-port ^12[0-7]..$
```

The following example shows how to write match and skip tests to skip connection attempts from destination 55554 and to match only those with destination addresses from 55550 to 55553 and from 55556 to 55559:

```
translate ruleset A from pad to telnet
skip dest-addr ^55554$
match dest-addr ^5555.$
```

Related Commands

Command	Description
description (ruleset)	Adds a description about a translation ruleset.
options (ruleset)	Specifies protocol translation options in a translation ruleset.
set (ruleset)	Unconditionally sets one or more connection parameters to a fixed value for a translation ruleset.
show translate ruleset	Displays a summary of a specific or of all configured translation rulesets, behavioral parameters, and usage statistic.
skip (ruleset)	Identifies a connection for omission by the translation ruleset.
substitute (ruleset)	Matches an available protocol and substitutes another in a translation ruleset.
test (ruleset)	Tests parameter values in a translation ruleset using regular expressions.
test translate	Displays a trace of protocol translation behavior for a connection attempt.
translate ruleset	Defines a unique name for a translation ruleset, specifies translated protocols, and enters translate ruleset configuration mode.
x25 pvc translate ruleset	Configures PVCs that are valid for protocol translation rule set handling.

monitor traffic line

To monitor inbound or outbound asynchronous character mode traffic on another terminal line, use the **monitor traffic line** command in privileged EXEC mode.

monitor traffic line [**aux** | **tty**] *line-number* [**in** | **out**] [**control-char**] [**interactive**]

Syntax Description		
aux	(Optional) Auxiliary EIA/TIA-232 DTE port. Must be addressed as relative line 0. The auxiliary port can be used for modem support and asynchronous connections.	
tty	(Optional) Standard asynchronous line.	
<i>line-number</i>	Relative number of the terminal line that you want to monitor when the line type is specified. Numbering begins with zero. Absolute number of the terminal line that you want to monitor when the line type is not specified. The acceptable range of this value is platform dependent.	
in	(Optional) Inbound traffic is monitored.	
out	(Optional) Outbound traffic is monitored.	
control-char	(Optional) Control characters are displayed along with asynchronous character mode traffic. Control character display is turned off by default.	
interactive	(Optional) Commands entered on the remote monitoring station are displayed to the user of the terminal line being monitored. By default, commands entered at the remote monitoring station are not displayed on the station being monitored (the keyboard lock is on).	

Defaults	Outbound traffic is monitored.
-----------------	--------------------------------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(4)T	This command was introduced.
	12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
	12.3(8)T	The control-char and interactive keywords were introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	The monitor traffic line command allows for the monitoring of only tty and auxiliary lines. The monitoring of console or vty lines is not permitted.
-------------------------	---

You can monitor only a single line with the **monitor traffic line** command. A line number is necessary, though, and you will receive an error message if you forget to include it.

To disable asynchronous line monitoring, enter the escape sequence (Ctrl-Shift-6, then x [Ctrl^x] by default).

Entering the **monitor traffic line** command with the optional line type (**aux** or **tty**) designates the line number as a relative number. For example, to configure line monitoring for line 7 (a tty line), you could enter the following:

```
monitor traffic line tty 7
```

You can also use the **monitor traffic line** command without specifying a line type. In this case, the line number is treated as an absolute line number. For example, to configure line traffic monitoring for line 5, which can be of **aux** or **tty** type, you could enter the following:

```
monitor traffic line 5
```

The **monitor traffic line** command starts displaying the asynchronous characters traversing the line that is being monitored. To stop monitoring traffic, enter the escape sequence (Ctrl-Shift-6, then x [Ctrl^x] by default).

You can issue the **control-char** keyword with the **monitor traffic line** command to configure the display of control characters along with the asynchronous character traffic on the line that is being monitored.



Note

The **monitor traffic line** command inserts a linefeed (LF) character in the character stream immediately after a carriage return (CR) character if the CR character is not immediately followed by an LF character in the original character stream.

In releases prior to Cisco IOS Release 12.3(8)T, when the **monitor traffic line** command is running and the asynchronous characters are being displayed (the user has not yet entered the escape sequence to stop traffic monitoring), the Asynchronous Line Monitoring feature allows the user of the remote monitoring station to enter more commands on this line. The output of the additional commands are displayed not only to the user of the remote monitoring station but also to the user of the terminal line that is being monitored. To prevent this display of command output on the terminal line that is being monitored, the user of the remote monitoring station must be careful not to enter more commands while the **monitor traffic line** command is still running.

In Release 12.3(8)T, the default behavior of the **monitor traffic line** command was changed so that commands entered by the user on the remote monitoring station are not displayed to the user on the terminal line being monitored (the keyboard lock is on). The **interactive** keyword turns off the keyboard lock, enabling the display of commands entered on the remote monitoring station to the user of the terminal line being monitored.

Examples

The following example allows the user to monitor inbound asynchronous character mode traffic on tty line 10:

```
Router# monitor traffic line tty 10 in
```

The following example allows the user to monitor inbound asynchronous character mode traffic, including control characters, on tty line 10:

```
Router# monitor traffic line tty 10 in control-char
```

The following example allows the user to monitor inbound asynchronous character mode traffic on line 5. The **interactive** keyword turns off the keyboard lock, specifying that commands entered at the remote monitoring station will be displayed to the user of the line being monitored.

```
Router# monitor traffic line 5 in interactive
```


options (ruleset)

To specify protocol translation options in a translation ruleset, use the **options** command in translate ruleset configuration mode. To remove or change the option, use the **no** form of this command.

options *rule-option* [*rule-option* [...]]

no options [...]

Syntax Description

rule-option [...] One of the protocol translation option keywords listed in [Table 16](#) followed, for some keywords, by a value for the option. More than one option can be listed on a command line.

Defaults

No default behavior or values

Command Modes

Translate ruleset configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to set the supported options listed in [Table 16](#). The ellipses in the format shown above means multiple options statements can be specified. The ruleset-defined options are overwritten each time the **options** command is entered. A connection that matches a ruleset, but fails the ruleset's configured option test, will be rejected.

Table 16 Options for Translation Rulesets

Options Keyword	Description
access-class <i>number</i>	Access class number that the incoming source hosts must match, and that must already have been defined in an access list. Standard access list numbers are in the range from 1 to 99; expanded standard access lists numbers are in the range from 1300 to 1999.
login	Require a login on the incoming connection before the outgoing connection is attempted. No value is required for this keyword.
max-users <i>number</i>	Defines the maximum number of concurrent users allowed per ruleset. When the maximum user limit has been reached, subsequent connection attempts and a test with test translate command will be refused.
quiet	Suppress translation information messages on the session. No value is required for this keyword.

Examples

The following example limits the number of simultaneous ruleset users to 10 and requires that the user log in before the outgoing connection is made:

```
translate ruleset customer-case-1 from telnet to pad
! Match an incoming Telnet attempt destined for IP addresses starting
! with 172.18., and a 5-digit port starting with 120 through 127
match dest-addr ^172\18\.* dest-port ^12[0-7]..$
! Once the correct network is matched, specify that this ruleset is limited
! to ten concurrent users and requires a login exchange
options max-users 10 login
```

Related Commands

Command	Description
description (ruleset)	Adds a description about a translation ruleset.
match (ruleset)	Identifies a connection for processing by the translation ruleset.
set (ruleset)	Unconditionally sets one or more connection parameters to a fixed value for a translation ruleset.
show translate ruleset	Displays a summary of a specific or of all configured translation rulesets, behavioral parameters, and usage statistic.
skip (ruleset)	Identifies a connection for omission by the translation ruleset.
substitute (ruleset)	Matches an available protocol and substitutes another in a translation ruleset.
test (ruleset)	Tests parameter values in a translation ruleset using regular expressions.
test translate	Displays a trace of protocol translation behavior for a connection attempt.
translate ruleset	Defines a unique name for a translation ruleset, specifies translated protocols, and enters translate ruleset configuration mode.
x25 pvc translate ruleset	Configures PVCs that are valid for protocol translation rule set handling.

pad

To log in to a packet assembler/disassembler (PAD), use the **pad** command in EXEC mode.

pad {*x121-address* | *host-name*} [/**cud** *text*] [/**debug**] [/**profile** *name*] [/**quiet** *message*] [/**reverse**] [/**use-map**]

Syntax Description

<i>x121-address</i>	Specifies the X.121 address of the X.25 host.
<i>host-name</i>	Specifies the X.25 host name if the host-to-address mapping has been set with the X.25 host command.
/ cud <i>text</i>	(Optional) Includes the specified <i>text</i> in the Call User Data (CUD) field of the outgoing Call Request Packet. The / character is required.
/ debug	(Optional) Displays the informational level of logging messages whenever the remote host changes an X.3 parameter setting or sends any other X.29 control packet. The / character is required.
/ profile <i>name</i>	(Optional) Sets X.3 PAD parameters for the <i>name</i> script. Using this keyword and profile name argument is the same as issuing the x29 profile global configuration command when translating X.25. If the X.29 profile is set to default , the profile is applied to all incoming X.25 PAD calls, including the calls used for protocol translation. The / character is required.
/ quiet <i>message</i>	(Optional) Suppresses information messages. Replace the <i>message</i> argument with the actual message that you want to suppress. The / character is required.
/ reverse	(Optional) Causes reverse-charge calls to be accepted on a per-call (rather than a per-interface) basis. The / character is required.
/ use-map	(Optional) Applies x25 map pad command entry options (such as CUD and idle) and facilities (such as packet in, packet out, win in, and win out) to the outgoing PAD call. This function occurs only if a matching X.121 destination address exists in an x25 map pad command entry. The / character is required.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **pad** command supports one-word connections. You need not enter the **pad** command; entering the address is enough to start the connection. A PAD can also be accessed and X.3 parameters configured with the **x28 EXEC** command, which uses the standard X.28 user interface.

You can have several PAD connections open at the same time and switch between them. You also can exit a connection and return to the user EXEC prompt at any point. To open a new connection, first exit the current connection by entering the escape sequence (**Ctrl-Shift-6** then **x** [**Ctrl^x**] by default) to

return to the EXEC prompt, then open the new connection. If the **/use-map** option is selected on the outgoing **pad** command, the **x25 map pad** command entries are searched for a matching X.121 destination address. If a match is found, the **x25 map pad** command entry options (such as CUD and idle) and facilities (such as packet in, packet out, win in, and win out) are applied to the outgoing PAD call.

To display information about packet transmission and X.3 PAD parameter settings, use the **show x25 pad** command. To exit a session, simply log out of the remote system. Then, terminate the active session by entering the **exit** command.

Examples

Use the **?** command to display **pad** command options, as shown in the following example:

```
Router# pad / ?
/cud      Call user data
/debug    Debugging option
/profile   Use a defined X.3 profile
/quiet     Suppress informational messages
/reverse   X25 Address reverse
/use-map   Use x25 map pad command facilities for outgoing Calls
```

The following example starts a PAD session:

```
Router> pad 123456789
Trying 123456789...Open
Router>
```

You can also access a PAD using standard X.28 commands. The following example enters X.28 mode with the **x28 EXEC** command and configures a PAD with the **set** X.3 parameter command. The **set** command sets the idle time delay to 40 seconds.

```
Router# x28
* set 4:40
```

The following example uses the **/use-map** option to configure a larger window and packet size than the default specified on the interface, and it sets the virtual circuit idle time to 2 seconds. Notice that the map values are used rather than the interface default values.

```
Router-A(config-if)# x25 map pad 2194441 cud user1 windowsize 7 7 packetsize 1024 1024
idle 2
Router-A(config-if)# end
Router-A#
%SYS-5-CONFIG_I: Configured from console by console.
```

```
Router-A# pad 2194441 /cud user1 /use-map
Trying 2194441....Open
```

```
06:31:12: pad_open_connection: found a matching x25 map pad
06:31:12: Serial1: X.25 O R1 Call (22) 8 lci 1024
06:31:12:   From(7): 2191111 To(7): 2194441
06:31:12:   Facilities: (6)
06:31:12:     Packet sizes: 1024 1024
06:31:12:     Window sizes: 7 7
06:31:12:   Call User Data (12): 0x01000000 (pad)
06:31:12: Serial1: X.25 I R1 Call Confirm (5) 8 lci 1024
06:31:12:   From(0): To(0):
06:31:12:   Facilities: (0)
06:31:12: PAD0: Call completed
```

Related Commands	Command	Description
	show x25 pad	Displays information about current open connections, including packet transmissions, X.3 parameter settings, and the current status of virtual circuits.
	translate x25	Automatically translates the request to another outgoing protocol connection type when an X.25 connection request to a particular destination address is received.
	x25 map pad	Configures an X.121 address mapping for PAD access over X.25.
	x28	Enters X.28 mode and accesses an X.25 network or sets X.3 PAD parameters.

resume (setting X.3 PAD parameters)

To set X.3 parameters, use the **resume** command in EXEC mode.

resume [*connection*] [/set *parameter:value*]

Syntax Description

<i>connection</i>	(Optional) The name or number of the connection; the default is the most recent connection.
<i>/set parameter:value</i>	(Optional) Sets the X.3 connection options and packet assembler/disassembler (PAD) parameters for the Cisco IOS software. See Table 17 in the Usage Guidelines for the PAD parameter numbers. Refer to the chapter “Configuring the Cisco PAD Facility for X.25 Connections” of the <i>Cisco IOS Terminal Services Configuration Guide</i> for a list of these connection options.

Defaults

For outgoing connections, the X.3 parameters default to the following:

2:1, 3:2, 4:1, 7:4, 16:127, 17:21, 18:19

All other parameters default to zero, but can be changed using the **/set** switch option with either the **resume** command or the **x3** command.

For incoming PAD connections, the software sends an X.29 SET PARAMETER packet to set only the following parameters:

2:0, 4:1, 7:21, 15:0

Command Modes

EXEC

Command History

Release	Modification
9.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Table 17 summarizes the X.3 PAD Parameters supported on Cisco devices. Refer to the “X.3 PAD Parameters” appendix in the *Cisco IOS Terminal Services Configuration Guide* for more complete information about these parameters.

Table 17 **Supported X.3 PAD Parameters**

Parameter Number	ITU-T Parameter Name	ITU-T X.3 and Cisco Values
1	PAD recall using a character	Minimum value: 0; maximum value: 126; X.28 PAD user emulation mode default: 1. Note Not supported by PAD EXEC user interface.
2	Echo	Minimum value: 0; maximum value: 1; PAD EXEC mode and X.28 PAD user emulation mode default: 1.
3	Selection of data forwarding character	Minimum value: 0; maximum value: 255; PAD EXEC mode default: 2 (CR); X.28 PAD user emulation mode default: 126 (~).
4	Selection of idle timer delay	Minimum value: 0; maximum value: 255; PAD EXEC mode default: 1; X.28 PAD user emulation mode default: 0.
5	Ancillary device control	Minimum value: 0; maximum value: 2; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 1.
6	Control of PAD service signals	Minimum value: 0; maximum value: 255; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 2. Note Not supported by PAD EXEC user interface.
7	Action upon receipt of a BREAK signal	Minimum value: 0; maximum value: 31; PAD EXEC mode default: 4; X.28 PAD user emulation mode default: 2.
8	Discard output	Minimum value: 0; maximum value: 1; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
9	Padding after Return	Minimum value: 0; maximum value: 255; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
10	Line folding	Not supported.
11	DTE speed (binary speed of start-stop mode DTE)	Minimum value: 0; maximum value: 18; PAD EXEC mode and X.28 PAD user emulation mode default: 14.
12	Flow control of the PAD by the start-stop DTE	Minimum value: 0; maximum value: 1; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 1.
13	Line feed insertion (after a Return)	Minimum value: 0; maximum value: 7; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
14	Line feed padding	Minimum value: 0; maximum value: 255; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
15	Editing	Minimum value: 0; maximum value: 1; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
16	Character delete	Minimum value: 0; maximum value: 127; PAD EXEC mode and X.28 PAD user emulation mode default: 127 (DEL).
17	Line delete	Minimum value: 0; maximum value: 127; PAD EXEC mode default: 21 (NAK or Ctrl-U); X.28 PAD user emulation mode default: 24 (CAN or Ctrl-X).

Table 17 **Supported X.3 PAD Parameters (continued)**

Parameter Number	ITU-T Parameter Name	ITU-T X.3 and Cisco Values
18	Line display	Minimum value: 0; maximum value: 127; PAD EXEC mode and X.28 PAD user emulation mode default: 18 (DC2 or Ctrl-R).
19	Editing PAD service signals	Minimum value: 0; maximum value: 126; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 2. Note Not supported by PAD EXEC user interface.
20	Echo mask	Minimum value: 0; maximum value: 255; PAD EXEC mode and X.28 PAD user emulation mode default: 0. Note Not supported by PAD EXEC user interface.
21	Parity treatment	Minimum value: 0; maximum value: 4; PAD EXEC mode and X.28 PAD user emulation mode default: 0. Note For additional values that can be selected for parameter 21, including parity treatment to conform to the French Transpac public switched data network and its technical specification and utilization of networks standards (STUR), see Appendix A, “X.3 PAD Parameters,” in the <i>Cisco IOS Terminal Services Configuration Guide</i> .

The **/set** switch sets the X.3 parameters defined by parameter number and value, separated by a colon. You set one or more X.3 PAD parameters, as follows:

-
- Step 1** Escape out of the current session by pressing the escape sequence (**Ctrl-Shift-6** then **x** [**Ctrl^x**] by default) and return to the EXEC prompt.
- Step 2** Issue the **where** command, to list the open sessions. All open sessions associated with the current terminal line are displayed.
- Step 3** Enter the **resume** command, followed by the parameter, a colon, and then the value to be set.
-

Examples

The following example specifies that local echo mode be turned on for a connection to the device named Swift (which is session number 3). As shown in Table 7, “local echo on” uses the parameter 2 and the value 1 (represented as 2:1 in this example):

```
Swift% ^^X
Router> resume 3 /set 2:1
Swift%
```


Related Commands

Command	Description
where	Lists the open sessions.

resume (switching sessions)

To switch to another open Telnet, rlogin, local-area transport (LAT), or packet assembler/disassembler (PAD) session, use the **resume** command in EXEC mode.

resume [*connection*] [*keyword*] [/set *parameter:value*]

Syntax Description

<i>connection</i>	(Optional) The name or number of the connection; the default is the most recent connection.
<i>keyword</i>	(Optional) One of the options listed in Table 8.
/set <i>parameter:value</i>	(Optional) Sets PAD parameters for the Cisco IOS software (see Table 7).

Command Modes

EXEC

Command History

Release	Modification
9.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

[Table 18](#) lists Telnet and rlogin resume options.

Table 18 *Telnet and rlogin resume Options*

Option	Description
/debug	Displays parameter changes and messages. In the Cisco IOS software, this option displays informational messages whenever the remote host changes an X.3 parameter, or sends an X.29 control packet.
/echo	Performs local echo.
/line	Enables line-mode editing.
/nodebug	Cancels printing of parameter changes and messages.
/noecho	Disables local echo.
/noline ¹	Disables line mode and enables character-at-a-time mode, which is the default.
/nostream	Disables stream processing.
/set <i>parameter:value</i>	Sets X.3 connection options. Refer to the chapter “Configuring the Cisco PAD Facility for X.25 Connections” of the <i>Cisco IOS Terminal Services Configuration Guide</i> for a list of these connection options.
/stream	Enables stream processing.

1. **/noline** is the default keyword.

You can have several concurrent sessions open and switch between them. The number of sessions that can be open is defined by the **session-limit** command.

You can switch between sessions by escaping one session and resuming a previously opened session, as follows:

-
- Step 1** Escape out of the current session by pressing the escape sequence (**Ctrl-Shift-6** then **x** [**Ctrl^x**] by default) and return to the EXEC prompt.
 - Step 2** Enter the **where** command, to list the open sessions. All open sessions associated with the current terminal line are displayed.
 - Step 3** Enter the **resume** command and the session number to make the connection.

You also can resume the previous session by pressing the **Return** key.

The **Ctrl^x**, **where**, and **resume** commands are available with all supported connection protocols.

Examples

The following example shows how to escape out of a connection and to resume connection 2:

```
Swift% ^^X
Router> resume 2
```

You can omit the command name and simply enter the connection number to resume that connection. The following example illustrates how to resume connection 3:

```
Router> 3
```

Related Commands

Command	Description
session-limit	Sets the maximum number of terminal sessions per line.
show tn3270 ascii-hexval	Displays ASCII-hexadecimal character mappings.
where	Lists open sessions associated with the current terminal line.

rlogin

To log in to a UNIX host using rlogin, use the **rlogin** command in EXEC mode.

rlogin *host* [-**I** *username*] [**/user** *username*] [**/quiet**] [**debug**]

Syntax Description		
<i>host</i>		Specifies the host name or IP address.
-I <i>username</i>		(Optional) The Berkeley Standard Distribution (BSD) UNIX syntax that specifies a username for the remote login. If you do not use this option, the remote username is your local username.
/user <i>username</i>		(Optional) The EXEC command syntax that specifies a remote username in the initial exchange with the remote host. The rlogin protocol will not present you with the <code>login</code> prompt. The <code>/</code> character must be entered.
/quiet		(Optional) Prevents onscreen display of all messages from the Cisco IOS software. The <code>/</code> character must be entered.
debug		(Optional) Enables debugging output from the rlogin protocol.

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	10.0	This command was introduced.
	12.1	The /quiet keyword was added.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can have several concurrent rlogin connections open and switch between them. To open a new connection, first suspend the current connection by pressing the escape sequence (**Ctrl-Shift-6** then **x** [**Ctrl^x**] by default) to return to the EXEC prompt. Then open a new connection. A user cannot automatically log in to a UNIX system from the router, but must provide a user ID and a password for each connection.

If your preferred transport is set to **rlogin**, you can use the **connect** command in place of the **rlogin** command. Refer to the chapter “Configuring Terminal Operating Characteristics for Dial-In Sessions” in the *Cisco IOS Terminal Services Configuration Guide* for more information about configuring a preferred transport type. When your preferred transport is set to **none** or to another protocol, you must use the **rlogin** command to connect to a host.

To terminate an active rlogin session, enter one of the following commands at the UNIX prompt of the device to which you are connecting:

- **close**
- **disconnect**
- **exit**
- **logout**

- **quit**

Examples

The following example illustrates how a user with the login name jsmith can use the **rlogin ?** help command and the **debug** command mode to establish and troubleshoot a remote connection to the host named Alvise:

```
Router> rlogin ?
WORD IP address or hostname of a remote system
Router> rlogin system1 ?
-l Specify remote username
/quiet Suppress login/logout messages
/user Specify remote username
debug Enable rlogin debugging output
<cr>
Router> rlogin system1 -l ?
WORD Remote user name
Router> rlogin system1 -l username?
debug Enable rlogin debugging output
<cr>
Router> rlogin system1 -l username debug
```

The following example illustrates debug return on the host named router1 by the user named user1:

```
Router# rlogin router1.cisco.com -l staff debug
Trying router1.cisco.com (171.69.63.31)... Open
RLOGIN: local username is: ciscoTS
RLOGIN: remote username is: user1
Password:
Last login: Wed Jun 24 06:15:36 from itech-view3.cisc
1 zipper> uptime
1:40pm up 42 day(s), 20:53, 80 users, load average: 1.44, 2.67, 3.39
2 zipper> logout
[Connection to router1.cisco.com closed by foreign host]
Router#
```

The following example makes an rlogin connection to a host at address 10.30.21.2 for a user named user2 and enables the message mode for debugging:

```
Router> rlogin 10.30.21.2 -l user2 debug
```

The following example makes an rlogin connection to a host named headquarters for the user named admin:

```
Router> rlogin headquarters -l admin
```

The following example suppresses all onscreen messages from the Cisco IOS software during login and logout:

```
Router> rlogin host2 /quiet
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
telnet	Logs in to a host that supports Telnet.

rlogin trusted-localuser-source

To choose an authentication method for determining the local username to send to the remote rlogin server, use the **rlogin trusted-localuser-source** command in global configuration mode. To restore the default rlogin behavior, use the **no** form of this command.

rlogin trusted-localuser-source [local | radius | tacacs]

no rlogin trusted-localuser-source [local | radius | tacacs]

Syntax Description

local	(Optional) Uses local username from any authentication method.
radius	(Optional) Uses local username from RADIUS authentication.
tacacs	(Optional) Uses local username from TACACS authentication.

Defaults

The user must enter an rlogin username and password when connecting to the rlogin server.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to define which of the sources for local usernames are valid.

The rlogin protocol passes three types of information: the remote username, the local username, and the local host name of the router. The **rlogin trusted-localuser-source** command allows you to configure one of three behaviors for making connections to the rlogin server, as follows:

- The user must enter a login username and password to connect (default).
- The Cisco IOS-authenticated username can be passed to the rlogin server so the user need only enter a password to connect.
- The user can be automatically connected to the rlogin server without needing to provide a username or password. This configuration is made by using both the **rlogin trusted-localuser-source** and **rlogin trusted-remoteuser-source local** commands where both the Cisco IOS authenticated username and the rlogin server username are the same.

Examples

The following example uses the local username from RADIUS authentication:

```
Router# configure terminal
Router(config)# rlogin trusted-localuser-source ?
  local    Use local username from any authentication method
  radius   Use local username from radius authentication
```

```
tacacs Use local username from tacacs authentication
Router(config)# rlogin trusted-localuser-source radius
```

Related Commands

Command	Description
ip alias	Assigns an IP address to the service provided on a TCP port.
retry keepalive	Logs in to a UNIX host using rlogin.
rlogin trusted-remoteuser-source local	Determines the remote username to send to the remote rlogin server.
template	Temporarily defines the list of services to which you or another user can connect.

rlogin trusted-remoteuser-source local

To determine the remote username to send to the remote rlogin server, use the **rlogin trusted-remoteuser-source local** command in global configuration mode. To restore the default rlogin behavior, which is to prompt the user for the remote username, use the **no** form of this command.

rlogin trusted-remoteuser-source local

no rlogin trusted-remoteuser-source local

Syntax Description

This command has no arguments or keywords.

Defaults

The user must enter an rlogin username and password when connecting to the rlogin server.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The current username is used only if the **rlogin host /user username** command is not enabled. If the current username is not known, rlogin falls back to providing the “login:” prompt to discover a remote username.

After you issue the **rlogin trusted-remoteuser-source local** command, you will not be prompted for a username. The first response you see is the password prompt from the remote system. For example, when this command is not enabled, you must enter your username twice (once at initial system login and once for the **rlogin** command).



Caution

Configuring the remote host to consider the Cisco router a “trusted” host should be considered a security hole.

Examples

The following sample output shows the two prompts a user must reply to when the **rlogin trusted-remoteuser-source local** command is not set:

User Access Verification

Username: **user1**

Password: **xxxxxx**

Router> **rlogin router**

Trying router.cisco.com (172.16.3.154)... Open


```
login: user1
Password: xxxxxx
```

The following example shows that after you issue the **rlogin trusted-remoteuser-source local** command, you no longer need to specify the username after the **rlogin** command. The username is automatically copied from the user ID of the router:

```
Router# enable
Password: xxxxxx
Router# configure terminal
Router(config)# rlogin ?
    trusted-localuser-source  Allowed authentication types for local username
    trusted-remoteuser-source Method used to get remote username
Router(config)# rlogin trusted-remoteuser-source local
Router(config)# ^Z
Router# rlogin router
Trying router.cisco.com (172.16.3.154)... Open
Password: xxxxxx
```

The following example uses the **/user root** keyword option as an override:

```
Router# rlogin router /user root
Trying router.cisco.com (172.16.3.154)... Open
Password: xxxxxx
login:
```

Related Commands

Command	Description
ip alias	Assigns an IP address to the service provided on a TCP port.
retry keepalive	Logs in to a UNIX host using rlogin.
rlogin trusted-localuser-source	Chooses an authentication method for determining the local username to send to the remote rlogin server.
template	Temporarily defines the list of services to which you or another user can connect.

rsa keypair-name

To name the Rivest, Shamir, and Adelman (RSA) keypair to be used for a persistent Secure Shell (SSH) connection, use the **rsa keypair-name** command in transport map configuration mode command. To restore the default setting of no configured RSA keypair name, use the **no** form of the command.

rsa keypair-name *rsa-keypair-name*

no rsa keypair-name

Syntax Description

<i>rsa-keypair-name</i>	The name of the RSA keypair to be used for a persistent SSH connection.
-------------------------	---

Command Default

No RSA keypair names for persistent SSH are specified by default.

Command Modes

Transport map configuration (config-tmap)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

For persistent SSH connections, the RSA keypair name must be defined using this command in transport map configuration mode. The RSA keypair definitions defined elsewhere on the router, such as through the use of the **ip ssh rsa keypair-name** command, do not apply to persistent SSH connections.

The generation of an RSA keypair, by default, starts the IOS internal SSH server. If you do not want to generate an SSH keypair using IOS, configure the **ip ssh rsa keypair-name** as a value that would never generate a connection (such as **ip ssh rsa keypair-name none**, **ip ssh rsa keypair-name never**, or any other name that will never generate a connection)

Examples

In the following example, a transport map that will make all SSH connections wait for the IOS process to become active before connecting to the router is configured and applied to the Management Ethernet interface (interface gigabitethernet 0). The RSA keypair is named “sshkeys”.

This example only uses the commands required to configure persistent SSH.

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# transport interface gigabitethernet 0
```

In the following example, a transport map is configured that applies the following settings to any users attempting to access the Management Ethernet port via SSH:

- Users using SSH wait for the IOS process to become active, but enter diagnostic mode if the attempt to access IOS is interrupted.
- The RSA keypair name is “sshkeys”

- The connection allows one authentication retry.
- The banner “--Welcome to Diagnostic Mode--” appears if diagnostic mode is entered as a result of SSH handling through this transport map.
- The banner “--Waiting for IOS Process--” appears if the connection is waiting for the IOS process to become active.

The transport map is then applied to the interface when the **transport type persistent ssh input** command is entered to enable persistent SSH.

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# authentication-retries 1
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for IOS Process--
X
Router(config-tmap)# time-out 30
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit

Router(config)# transport type persistent ssh input sshhandler
```

Related Commands

Command	Description
authentication-retries	Specifies the number of SSH authentication retries before dropping the connection when a persistent SSH transport map is applied to the receiving interface.
banner (transport map)	Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of the transport map configuration.
connection wait	Specifies how an incoming connection will be handled.
time-out	Specifies the SSH timeout interval in seconds.
transport interface	Applies the transport map settings to the interface.
transport type persistent	Applies an already-configured persistent transport map to an interface.
transport-map type persistent	Creates and names a persistent transport map and enters transport map configuration mode.

rxspeed

To set the terminal receive speed (how fast the terminal receives information from the modem), use the **rxspeed** command in line configuration mode. To reset the default value, use the **no** form of this command.

rxspeed *bps*

no rxspeed

Syntax Description	<i>bps</i>	Baud rate in bits per second (bps). The default value is 9600 bps.
---------------------------	------------	--

Defaults	9600 bps
-----------------	----------

Command Modes	Line configuration
----------------------	--------------------

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	Set the speed to match the baud rate of whatever device you have connected to the port. Some baud rates available on devices connected to the port might not be supported on the system. The system will indicate if the speed you select is not supported.
-------------------------	---



Note

If the line was previously configured for automatic baud rate detection (autobaud), disable autobaud by entering the **no autobaud** command before entering the **rxspeed** command to fix the speed of the port.

Examples	The following example sets the line 5 receive rate to 2400 bps: <pre>line 5 rxspeed 2400</pre>
-----------------	---

Related Commands	Command	Description
	source template	Sets the flow control start character.
	terminal rxspeed	Sets the terminal receive speed (how fast information is sent to the terminal) for the current line and session.
	txspeed	Sets the terminal transmit speed (how fast the terminal sends information to the modem).

secure-server

To enable the secure HTTP (HTTPS) server for a web user interface transport map, use the **secure-server** command in transport map configuration mode. To disable the HTTPS secure server for a web user interface transport map, use the **no** form of this command.

secure-server

no secure-server

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	No server is enabled in a web user interface transport map by default.
------------------------	--

Command Modes	Transport map configuration (config-tmap)
----------------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines	This command is used to enable the secure HTTPS web server for web user interface traffic. The other choice is the server option, which configures HTTP as the web server. Both web servers can be configured at the same time.
-------------------------	---

When this command is entered, the router decides which port to use for HTTPS traffic based on the **ip http secure-server** or **ip http secure-port** configuration. Therefore, **ip http secure-server**, which configures the router to use the default port of 443 for HTTPS traffic, or **ip http secure-port**, which specifies a user-defined port for HTTPS traffic, must be configured when the **secure-server** command is used.

Examples	In the following example, the web user interface using the default HTTPS port is enabled:
-----------------	---

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip http secure-server
Router(config)# transport-map type persistent webui https-webui
Router(config-tmap)# secure-server
Router(config-tmap)# exit
Router(config)# transport type persistent webui input https-webui
*Apr 22 02:38:43.597: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd: Server wui has been notified to start
```

Related Commands

Command	Description
ip http secure-server	Enables the HTTPS server on a router using the default HTTPS port.
ip http secure-port	Enables the HTTPS server on a router using a user-specified port.
server (transport map)	Enables the HTTP server for a persistent web user interface transport map.
transport type persistent	Applies an already-configured persistent transport map to an interface.
transport-map type persistent	Creates and names a transport map and enters transport map configuration mode.

server (transport map)

To enable the HTTP server for a web user interface transport map, use the **server** command in transport map configuration mode. To disable the HTTP server for a web user interface transport map, use the **no** form of this command.

server

no server

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	No server is enabled in a web user interface transport map by default.
------------------------	--

Command Modes	Transport map configuration (config-tmap)
----------------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines	This command is used to enable the HTTP web server for web user interface traffic. The other choice is the secure-server option, which configures HTTPS as the web server. Both web servers can be configured at the same time.
-------------------------	---

When this command is entered, the router decides which port to use for HTTP traffic based on the **ip http server** or **ip http port** configuration. Therefore, **ip http server**, which configures the router to use the default port of 80 for HTTP traffic, or **ip http port**, which specifies a user-defined port for HTTP traffic, must be configured when the **server** command is used.

Examples	In the following example, the web user interface using the default HTTP port is enabled:
-----------------	--

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip http server
Router(config)# transport-map type persistent webui http-webui
Router(config-tmap)# server
Router(config-tmap)# exit
Router(config)# transport type persistent webui input http-webui
*Apr 22 02:43:55.798: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd: Server wui has been notified to start
```

Related Commands

Command	Description
ip http server	Enables the HTTP server on a router using the default HTTP port.
ip http port	Enables the HTTP server on a router using a user-specified port.
secure-server	Enables the secure HTTP (HTTPS) server for a persistent web user interface transport map.
transport type persistent	Applies an already-configured persistent transport map to an interface.
transport-map type persistent	Creates and names a transport map and enters transport map configuration mode.

service exec-callback

To enable call back to clients who request a callback from the EXEC level, use the **service exec-callback** command in global configuration mode.

service exec-callback

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	Callback is not enabled.
-----------------	--------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.1	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	This command enables the Cisco IOS software to return a call to a device that dials in, connects to the EXEC, and requests callback.
-------------------------	--

Examples	The following example enables EXEC level callback: service exec-callback
-----------------	---

Related Commands	Command	Description
	arap callback	Enables an ARA client to request a callback from an ARA client.
	debug callback	Displays callback events when the router is using a modem and a chat script to call back on a terminal line.
	debug confmodem	Displays information associated with the discovery and configuration of the modem attached to the router.
	ppp callback (PPP client)	Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.
	script arap-callback	Specifies that a chat script start on a line when an ARA client requests a callback.
	username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

service old-slip-prompts

To provide backward compatibility for client software scripts expecting Serial Line Internet Protocol (SLIP) and PPP dialogs to be formatted with Cisco IOS software Release 9.1 or earlier releases, use the **service old-slip-prompts** command in global configuration mode. To disable this function, use the **no** form of this command.

service old-slip-prompts

no service old-slip-prompts

Syntax Description This command has no arguments or keywords.

Defaults The prompts and information sent by SLIP and PPP are formatted with the current release of Cisco IOS software.

Command Modes Global configuration

Command History	Release	Modification
	11.1	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines This command provides backward compatibility for client software scripts expecting SLIP and PPP dialogs to be formatted with Cisco IOS software Release 9.1 or earlier releases.

Examples The following example shows the output of a SLIP command after the **service old-slip-prompts** command is enabled:

```
Router# configure terminal
Router(config)# service old-slip-prompts
Router(config)# exit
Router# slip
IP address or hostname: 10.2.2.2
Entering SLIP mode.
Your IP address is 10.2.2.2. MTU is 1500 bytes
```

service pt-vty-logging

To log the X.121 calling address, Call User Data (CUD), and IP address assigned to a vty asynchronous connection, use the **service pt-vty-logging** command in global configuration mode. To disable this function, use the **no** form of this command.

service pt-vty-logging

no service pt-vty-logging

Syntax Description

This command has no arguments or keywords.

Defaults

This feature is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command permits you to log the X.121 calling address, CUD, and IP address assigned to a vty asynchronous connection and direct this information to the console, an internal buffer, or a UNIX syslog server, depending on the logging configuration command you use. This authentication information can be used to associate an incoming packet assembler/disassembler (PAD) vty-asynchronous connection with an IP address.



Note

By default, the Cisco IOS software displays all messages to the console terminal.

Examples

The following example enables you to log the X.121 calling address, CUD, and IP address assigned to a vty asynchronous connection and save this information to a syslog server:

```
service pt-vty-logging
```

The following is sample output from the **service pt-vty-logging** command:

```
01:24:31: PAD18: call from 00011890 on LCI 10 PID 1 0 0 0 CUD "xyz"
```

[Table 19](#) describes the fields shown in the output.

Table 19 *service pt-vty-logging Field Descriptions*

Field	Description
01:24:31:	Time stamp.
PAD18:	Active vty line number using the PAD connection.
00011890	The source or calling address.
on LCI 10	Incoming call is initiated on Logical Channel 10.
PID 1 0 0 0	The PAD Protocol Identifier is "01000000."
CUD "xyz"	CUD "xyz." If no CUD is available, this field will appear as follows: CUD " "

Related Commands

Command	Description
logging	Logs messages to a syslog server host.
logging buffered	Logs messages to an internal buffer.

session-limit

To set the maximum number of terminal sessions per line, use the **session-limit** command in line configuration mode. To remove any specified session limit, use the **no** form of this command.

session-limit *session-number*

no session-limit

Syntax Description

<i>session-number</i>	Specifies the maximum number of sessions.
-----------------------	---

Defaults

The default and set session limits are displayed with the **start-character** EXEC command.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example limits the number of sessions to eight on a ten-line range:

```
line 2 12
 session-limit 8
```

Related Commands

Command	Description
line vty	Specifies a virtual terminal for remote console access.
start-character	Sets the flow control start character.

session-timeout

To set the interval for closing the connection when there is no input or output traffic, use the **session-timeout** command in line configuration mode. To remove the timeout definition, use the **no** form of this command.

session-timeout *minutes* [**output**]

no session-timeout

Syntax Description

<i>minutes</i>	Specifies the timeout interval in minutes.
output	(Optional) Specifies that when traffic is sent to an asynchronous line from the router (within the specified interval), the connection is retained.

Defaults

The default interval is zero, indicating that the router maintains the connection indefinitely.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command sets the interval that the Cisco IOS software waits for traffic before closing the connection to a remote computer and returning the terminal to an idle state.

If only the **session timeout** command is specified, the session timeout interval is based solely on detected input from the user.

If the **session timeout** command is specified with the **output** keyword, the interval is based on both input and output traffic. You can specify a session timeout on each port.

The **session-timeout** command behaves slightly differently on virtual (vty) terminals than on physical console, auxiliary (aux), and terminal (tty) lines. When a timeout occurs on a vty, the user session returns to the EXEC prompt. When a timeout occurs on physical lines, the user session is logged out and the line returned to the idle state.

You can use a combination of the **exec-timeout** and **session-timeout** line configuration commands, set to approximately the same values, to get the same behavior from virtual lines that the **session-timeout** command causes on physical lines.

Examples

The following example sets an interval of 20 minutes and specifies that the timeout is subject to traffic detected from the user (input only):

```
line 5
```

```
session-timeout 20
```

The following example sets an interval of 10 minutes, subject to traffic on the line in either direction:

```
line 5
 session-timeout 10 output
```

Related Commands	Command	Description
	absolute-timeout	Sets the interval for closing the connection on a virtual terminal line.
	exec-timeout	Sets the interval that the EXEC command interpreter waits until user input is detected.

set (ruleset)

To unconditionally set one or more connection parameters to a fixed value for a translation ruleset, use the **set** command in translate ruleset configuration mode. To remove the ruleset, use one of the **no** forms of this command.

set [*#line-number*] {**pad** | **telnet**} *variable-parameter* [{**pad** | **telnet**} *variable-parameter* [...]]

no set {**pad** | **telnet**} *variable-parameter* [{**pad** | **telnet**} *variable-parameter* [...]]

no set *#line-number* [...]

Syntax Description	<i>#line-number</i>	(Optional) The line in the ruleset template the command should occupy. The # character must be entered.
	{ pad telnet }	Specifies the incoming or outgoing protocol, which controls the parameters that are available in the next element of this command.
	<i>variable-parameter</i>	A parameter that varies depending upon the protocol selected, either pad or telnet , and its role, either incoming or outgoing. Protocol parameter values are available to modify the incoming or outgoing connection behavior during protocol translation session setup. Up to six parameters can be entered on one command line. Table 20 indicates the supported Telnet and PAD incoming and outgoing connection parameter keywords with an X.
	[...]	(Optional) Specifies that multiple entries can be made as follows: - Up to six set specifications can be entered on one command line. - Multiple line numbers can be specified using the second no form of this command.

Defaults No default behavior or values

Command Modes Translate ruleset configuration

Command History	Release	Modification
	12.3(8)T	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Up to six **set** specifications can be entered on one command line. The ellipses in the format shown above means multiple set statements can be specified.

When you use the first **no** form of this command, specify the full set of parameters and expressions in the command to be removed. The second **no** form must specify the correct **set** command and line number within the ruleset template.

Once an incoming connection has been matched for processing, the ruleset generates the protocol translation parameters using a template that unconditionally sets a value defined by a set statement. It is also possible that the incoming connection could conditionally set a value based on a test of parameter values using regular expressions. This is a **test** and **set** operation. The ruleset template could then substitute one parameter into another from a regular expression pattern match. These command combinations provide the network administrator with much flexibility in determining the protocol parameter values to use when establishing a protocol translation session.

As an example of **set**, **test**, and **substitute** command usage, an incoming TCP connection to an outgoing PAD connection might unconditionally set the PAD's profile identifier as follows:

```
set pad profile Bldg-1-5ess
```

The incoming connection might conditionally set the profile identifier from a test of the destination information, as follows:

```
test telnet dest-addr \.11$ telnet dest-port ^10000$ set pad profile ess
```

Finally, the command might substitute a portion of the TCP destination port into the profile identifier, as follows:

```
substitute telnet dest-port ^1000(.)$ pad profile Bldg-1-5ess-\1
```

To combine the **test** and **set** commands, use the backslash character (\) to concatenate the command lines. The following statements test conditional parameters and then set appropriate parameters:

```
test telnet dest-addr ^172\18\0\.* telnet dest-port ^10.00 \  
set pad pvc 1 telnet binary T
```

The protocol parameters for the incoming connection attempt are available for match expressions in the test, set and substitute statements. The values of the incoming connection attempt cannot be modified, though. For example, an incoming PAD connection has source and destination addresses that can be tested and used to modify other parameters, but the incoming connection addresses themselves cannot be modified.

Configuration errors are not detected when translation ruleset commands are entered. They are tested when the connection is attempted and the **test (ruleset)** command is used. In the following example, the translation ruleset **set** command unconditionally sets the PAD's profile name to a profile that does not exist in the configuration:

```
set pad profile Bldg-1-5ess
```

This command would be accepted at the command-line interpreter, and validated only upon a connection attempt or with the **test translate EXEC** command. When the error is detected, the following messages display:

```
">%PT-3-PARAMRESULTERR: PT ruleset test protocol pad parameter profile parse error:  
Bldg-1-5ess.
```

```
-Process= "PAD InCall", ipl= 3, pid= 94
```

```
*PAD: ruleset translation not generated Cause: 9 Diag: 0
```

[Table 20](#) lists the PAD and Telnet parameters that can be set, as indicated by an X. PAD outgoing service routing information (interface, CMNS MAC address, X.25 over TCP or XOT parameters, for example) are available for both switched virtual circuit (SVC) and permanent virtual circuit (PVC) service, and will take precedence over the X.25 routing table. If no routing information is specified, the X.25 routing

table will be used. Entering an incomplete specification of routing information or the Connection-Mode Network Service (CMNS) MAC address, or omitting an interface specification for an Annex G data-link connection identifier (DLCI), will result in an error.

Table 20 **Set Connection Parameter Keywords**

Parameter	Description	Incoming PAD	Outgoing Telnet	Outgoing PAD	Incoming Telnet
authorize-method <i>ASCII-string</i>	Connection authorization method to use that must match one of a fixed set of values.	X	—	—	X
authorize-tag <i>ASCII-string</i>	Connection authorization identity to supply, entered as an ASCII string.	X	—	—	X
binary flag	Flag that specifies whether 8-bit binary data is required, entered as one of the following characters to specify binary mode: Y, y, 1–9, T, t .	—	X	—	X
cud <i>ASCII-string</i>	Call user data (CUD) that occurs after the protocol identification (PID). For X.29 service, this is the optional, user-specified text included in the command to place a call.	—	—	X	—
dest-addr <i>address</i>	Destination IP (Telnet) or X.121 (PAD) address.	—	X	X	—
dest-addr-ext <i>address</i>	Network service access point (NSAP) destination address extension.	—	—	X	—
dest-port <i>port</i>	Destination port entered as a decimal number from one to five digits long.	—	X	—	
dldi <i>number</i>	Frame Relay data-link connection identifier (DLCI) of an Annex G service entered as a number from one to seven digits in length, although a size of two to four digits is more likely, or the NULL string if not received on an Annex G service.	—	—	X	—
eor <i>specification</i>	A character set defining the End-of-Record (EOR) string for the protocol translation session, entered as an ASCII or hexadecimal specification from one to four bytes in length, aaa or 0x19, as examples.	—	X	—	X

Table 20 **Set Connection Parameter Keywords (continued)**

Parameter	Description	Incoming PAD	Outgoing Telnet	Outgoing PAD	Incoming Telnet
eor-insert <i>flag</i>	Flag specifying that the EOR character set should be inserted for PAD data being forwarded to a Telnet session, and is entered as a single character. Use one of the following characters to specify EOR insertion: Y, y, 1–9, T, t .	—	X	—	X
hostname <i>address</i>	Destination host name for Domain Name System (DNS) resolution entered as an ASCII string.	—	X	—	—
idle <i>seconds</i>	Number of seconds the PAD connection can be idle before being cleared.	X	—	X	—
interface <i>type number</i>	Interface to be used for the circuit, entered using standard Cisco IOS interface designations; Serial1/0:1, for example.	—	—	X	—
keepalive-period <i>seconds</i>	Indicates the number of seconds between TCP keepalives for the X.25 over TCP (XOT) connection. TCP keepalive information applies only when a ruleset is configured to match an XOT destination address. Example: match dest-addr ^5555.\$ xot-dest-addr 5.5.5.2	X	—	X	—
keepalive-tries <i>number</i>	Indicates the number of TCP keepalives to send before the XOT connection is declared dead. TCP keepalive information applies only when a ruleset is configured to match an XOT destination address. Example: match dest-addr ^5555.\$ xot-dest-addr 5.5.5.2	X	—	X	—
local <i>flag</i>	Flag specifying that Telnet control sequences should be forwarded, not processed, and is entered as a single character. Use one of the following characters to specify local mode: Y, y, 1–9, T, t .	—	X	—	X

Table 20 **Set Connection Parameter Keywords (continued)**

Parameter	Description	Incoming PAD	Outgoing Telnet	Outgoing PAD	Incoming Telnet
mac address	Connection-Mode Network Service (CMNS) service remote host MAC address entered as three hexadecimal numbers of four digits separated by a period, (0000.fc08.12ab, for example) or the NULL string if not received on a CMNS service.	—	—	X	—
no-reset	Suppress a PVC Reset packet at session startup.	X	—	X	—
packetsize size	X.25 maximum data packet sizes to request, entered as two numbers from the following choices: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096.	—	—	X	—
pid byte-string	PID string specified in ASCII or hexadecimal. A hexadecimal PID must be prefixed by "0x." For example, 0x01000000 is the standard PAD PID. Although it is available for specifying a nonstandard Call PID, this parameter is not restricted to the common PID length and can be used to specify the entire user data field.	—	—	X	—
printer flag	Printer access mode. Flag specifying that the outgoing connection should be brought up before the incoming connection is confirmed. Use one of the following characters to specify printer mode: Y , y , 1–9 , T , t . An unsuccessful outgoing connection attempt results in the incoming connection to the ruleset being refused, rather than being accepted and then closed, which is the default behavior. Note that using this keyword will force the ruleset quiet keyword to be applied to the translation.	X	—	—	X
profile name	Named PAD profile to use.	X	—	X	—

Table 20 Set Connection Parameter Keywords (continued)

Parameter	Description	Incoming PAD	Outgoing Telnet	Outgoing PAD	Incoming Telnet
pvc <i>circuit-number</i>	Permanent virtual circuit (PVC) entered as a number from 1 to 4095, or the null string if not a PVC.	—	—	X	—
reverse	Request reverse charging.	—	—	X	—
reversed <i>flag</i>	Flag to indicate whether a reverse charged Call is permitted. This flag applies to a switched virtual circuit (SVC) and is entered as a single character, Y or N , for yes or no.	—	—	—	—
rotor	Modifies the behavior of the host-name keyword by allowing one of the IP addresses defined by the ip host configuration command to be chosen randomly. If one address fails, another will be tried until a connection is made or all address choices are exhausted.	—	X	—	—
source-addr <i>address</i>	Source X.121 address.	—	—	X	—
source-addr-ext <i>address</i>	NSAP source address extension.	—	—	X	—
source-ifc <i>type number</i>	Interface from which to take the source IP address, entered using standard Cisco IOS interface designations, Loopback0, for example.	—	X	X	—
stream <i>flag</i>	Flag that specifies whether Telnet negotiation should be sent or accepted, entered as one of the following characters to specify stream mode: Y , y , 1–9 , T , t .	—	X	—	X

Table 20 Set Connection Parameter Keywords (continued)

Parameter	Description	Incoming PAD	Outgoing Telnet	Outgoing PAD	Incoming Telnet
swap flag	X.29 role reversal. Flag that indicates the PAD connection should not initiate X.29 commands when first connected. Use one of the following characters to swap behavior: Y , y , 1–9 , T , t . This parameter enables incoming and outgoing PAD connections to be swapped so that a protocol translation is treated like a PAD when it accepts a call. By default, the protocol translation functions like a PAD for calls that it initiates, and like an X.25 host for calls it accepts.	X	—	X	—
use-map map	Use the map defined for PAD service.	—	—	X	—
window size size	X.25 window sizes to request, entered as two numbers in a range from 1 to 127.	—	—	X	—
xot-dest-addr address	Destination IP address of an X.25 over TCP (XOT) service entered in standard IP address dotted decimal notation (10.0.0.127, for example) or the NULL string if not received on an XOT service.	—	—	X	—
xot-source-addr address	Source IP address of an XOT service entered in standard IP address dotted decimal notation (10.0.0.127, for example) or the NULL string if not received on an XOT service.	—	—	—	—

Examples

The following example shows how to build a ruleset by writing a match statement, specifying protocol translation options, setting parameters for incoming Telnet connections, then testing and setting appropriate parameters for incoming PAD connections. Note use of the backslash character to combine the test and set statements.

```
translate ruleset customer-case-1 from telnet to pad
! Match an incoming Telnet attempt destined for IP addresses starting
! with 172.18., and a 5-digit port starting with 120 through 127
match dest-addr ^172\18\.* dest-port ^12[0-7]..$
! Once the correct network is matched, specify that this ruleset is limited
! to ten concurrent users and requires a login exchange
options max-users 10 login
! Set Telnet options
set telnet printer Y telnet binary Y
```

```

! Set PAD options
set pad profile cust-profile-one
! Test conditional parameters and make appropriate settings
test telnet dest-addr ^172\.18\.0\.* telnet dest-port ^10.00 \
set pad pvc 1 telnet binary T

```

Related Commands

Command	Description
description (ruleset)	Adds a description about a translation ruleset.
match (ruleset)	Identifies a connection for processing by the translation ruleset.
options (ruleset)	Specifies protocol translation options in a translation ruleset.
show translate ruleset	Displays a summary of a specific or of all configured translation rulesets, behavioral parameters, and usage statistic.
skip (ruleset)	Identifies a connection for omission by the translation ruleset.
substitute (ruleset)	Matches an available protocol and substitutes another in a translation ruleset.
test (ruleset)	Tests parameter values in a translation ruleset using regular expressions.
test translate	Displays a trace of protocol translation behavior for a connection attempt.
translate ruleset	Defines a unique name for a translation ruleset, specifies translated protocols, and enters translate ruleset configuration mode.
x25 pvc translate ruleset	Configures PVCs that are valid for protocol translation ruleset handling.

show arap

To display information about a running AppleTalk Remote Access Protocol (ARAP) connection, use the **show arap** command in EXEC mode.

show arap [*line-number*]

Syntax Description	<i>line-number</i>	(Optional) Number of the line on which an ARAP connection is established and active.
--------------------	--------------------	--

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	Use the show arap command with no arguments to display a summary of the ARAP traffic since the router was last booted.
------------------	---

Examples	The following is sample output from the show arap command:
----------	---

```
Router# show arap
```

```
Statistics are cumulative since last reboot
Total ARAP connections: 2
Total Appletalk packets output: 157824
Total Appletalk packets input: 12465
```

These fields refer to the sum of all of the ARA connections since the box was last reloaded.

The following sample output results in a display of information about ARA activity on a specific line (line 3):

```
Router# show arap 3
```

```
Active for 23 minutes
"Unlimited time left" or "22 minutes left"
"Doing smartbuffering" or "Smartbuffering disabled"
Appletalk packets output: 157824
Appletalk packets input: 12465
Appletalk packets overflowed: 1642
Appletalk packets dropped: 586
V42bis compression efficiency (incoming/outgoing): {percentage/percentage}
MNP4 packets received: 864
MNP4 packets sent: 1068
MNP4 garbled packets received: 4
MNP4 out of order packets received: 0
```



```
MNP4 packets resent: 0
MNP4 nobuffers: 0
```

Table 21 describes the significant fields shown in the display.

Table 21 *show arap Field Descriptions*

Field	Description
Active for <i>integer</i> minutes	Number of minutes since ARAP started on the line.
Unlimited time left or <i>integer</i> minutes left	Remaining time limit on the line, if applicable on the line.
Doing smartbuffering or Smartbuffering disabled	Obsolete. Always says “Doing smartbuffering.”
Appletalk packets output:	Number of AppleTalk packets that have been received from the Apple Macintosh and out to the network during this connection.
Appletalk packets input:	Number of AppleTalk packets that have been received from the network and sent to the Apple Macintosh during this connection.
Appletalk packets overflowed:	Number of packets from the network that have been dropped because the link to the Apple Macintosh was congested.
Appletalk packets dropped:	Number of packets from the network that have been dropped because it was unnecessary to pass them (frequently RTMP).
V42bis compression efficiency (incoming/outgoing):	Performance of the v42bis protocol underneath ARA, expressed as a percentage of incoming/percentage outgoing. If the efficiency is low, a network user is probably copying already compressed files across the link. Generally, low efficiency means slow performance.
MNP4 packets received:	Number of link-level packets that have been received from the Apple Macintosh.
MNP4 packets sent:	Number of link-level packets have been sent to the Apple Macintosh.
MNP4 garbled packets received:	Number of garbled packets that have been received from the Apple Macintosh.
MNP4 out of order packets received:	Number of out-of-order packets that have been received from the Apple Macintosh.
MNP4 packets resent:	Number of times packets have been re-sent. ¹
MNP4 nobuffers:	Number of times MNP4 has run out of buffers. This field should be zero.

1. Each of these fields indicates line noise. The higher the value, the higher the noise.

show entry

To display the list of queued host-initiated connections to a router, use the **show entry** command in EXEC mode.

show entry

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.1	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines You can also use this command to determine which local-area transport (LAT) hosts have queue entries for printers on routers.

Examples The following is sample output from the **show entry** command. The display shows that two LAT connections are waiting for access to port 5. The list is ordered so that the lower-numbered entry has been waiting longer, and will use the line next.

Router# **show entry**

```
1 waiting 0:02:22 for port 5 from LAT node BLUE
2 waiting 0:00:32 for port 5 from LAT node STELLA
```

[Table 22](#) describes the fields in the first line of output shown in the display.

Table 22 *show entry Field Descriptions*

Field	Description
1	Number assigned to the queued connection attempt.
waiting 0:02:22	Interval (hours:minutes:seconds) during which the connection attempt has been waiting.
for port 5	Port for which the connection attempt is waiting.
from LAT node BLUE	Name of the user (BLUE) attempting to make the connection.

show keymap

To test for the availability of a keymap after a connection on a router takes place, use the **show keymap** command in EXEC mode.

show keymap [*keymap-name* | **all**]

Syntax Description

<i>keymap-name</i>	(Optional) Name of the keymap.
all	(Optional) Lists the names of all defined keymaps. The name of the default keymap is not listed.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Cisco IOS software searches for the specified keymap in its active configuration image and lists the complete entry if found. If the keymap is not found, an appropriate “not found” message appears.

If you do not use any arguments with the **show keymap** command, then the keymap currently used for the terminal is displayed.

Examples

The following is sample output from the **show keymap** command:

```
Router# show keymap

ciscodefault { clear = '^z'; flinp = '^x'; enter = '^m';\
  delete = '^d' | '^?';\
  synch = '^r'; reshow = '^v'; eof = '^e'; tab = '^i';\
  btab = '^b'; nl = '^n'; left = '^h'; right = '^l';\
  up = '^k'; down = '^j'; einp = '^w'; reset = '^t';\
  xoff = '^s'; xon = '^q'; escape = '^c'; ferase = '^u';\
  insrt = '^E';\
  pa1 = '^p1'; pa2 = '^p2'; pa3 = '^p3';\
  pfk1 = '^E1'; pfk2 = '^E2'; pfk3 = '^E3'; pfk4 = '^E4';\
  pfk5 = '^E5'; pfk6 = '^E6'; pfk7 = '^E7'; pfk8 = '^E8';\
  pfk9 = '^E9'; pfk10 = '^E0'; pfk11 = '^E-'; pfk12 = '^E=';\
  pfk13 = '^E!'; pfk14 = '^E@'; pfk15 = '^E#'; pfk16 = '^E$';\
  pfk17 = '^E%'; pfk18 = '^E^'; pfk19 = '^E&'; pfk20 = '^E*';\
  pfk21 = '^E('; pfk22 = '^E)'; pfk23 = '^E_'; pfk24 = '^E+';\
}
```

Refer to the **keymap** command for more information about keyboard mappings and keymap entry structures.

■ show keymap

Related Commands

Command	Description
keymap	Defines specific characteristics of keyboard mappings.

show lat advertised

To display the local-area transport (LAT) services a router offers to other systems running LAT on the network, use the **show lat advertised** command in EXEC mode.

show lat advertised

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Advertised services are created with the **lat service** commands. The display includes the service rating, rotary group if present, and whether the service is enabled for incoming connections.

Examples The following is sample output from the **show lat advertised** command:

```
Router# show lat advertised

service Name      Rating      Rotary  Flags
service1          4 (Dynamic)  None   Enabled
  Autocommand: telnet service1
Service2           0 (Dynamic)   12   Enabled
  Ident: service2 modem services
service3           4 (Dynamic)  None   Enabled
  Ident: service3...
```

The display shows output from a router named router1 that has three services defined: service1, service2, and service3.

[Table 23](#) describes the fields shown in the display.

Table 23 *show lat advertised Field Descriptions*

Field	Description
Service Name	Lists the LAT service name.
Rating	Lists the static service rating set, if any.
Rotary	Lists the associated rotary service.
Flags	Lists whether a service is enabled.

Table 23 *show lat advertised Field Descriptions*

Field	Description
Autocommand	Defines the autocommand associated with the service.
Ident	Lists the advertised identification for the service.

show lat groups

To display the groups that were defined in the Cisco IOS software with the **lat group-list** command, use the **show lat groups** command in EXEC mode.

show lat groups

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples The following is sample output from the **show lat groups** command:

Router# **show lat groups**

Group Name	Len	Groups
cafeteria	3	13 15 23
engineering	7	55
manufacturing	10	70 71 72

[Table 24](#) describes the fields shown in the display.

Table 24 *show lat groups Field Descriptions*

Field	Description
Group Name	Assigned group name.
Len	Size of internal data structure used to contain the group code map.
Groups	Group codes associated with the learned group.

Related Commands	Command	Description
	lat group-list	Allows a name to be assigned to the group list, which is any combination of group names, numbers, or ranges.

show lat nodes

To display information about all known local-area transport (LAT) nodes, use the **show lat nodes** command in EXEC mode.

show lat nodes

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples The following is sample output from the **show lat nodes** command:

```
Router# show lat nodes

Node "service1", usage -1, Interface Ethernet0, Address 0000.0c01.0509
  Timer 89, sequence 188, changes 131, flags 0x0, protocol 5.1
  Facility 0, Product code 0, Product version 0
  Recv 0/0/0, Xmit 0/0/0, 0 Dups, 0 ReXmit
  Bad messages: 0, Bad slots: 0, Solicits accepted: 0
  Solicits rejected: 0, Multiple nodes: 0
  Groups: 0
  Service classes: 1
Node "service2", usage -1, Local
  Timer 99, sequence 4, changes 151, flags 0x0, protocol 5.2
  Facility 0, Product code 0, Product version 0
  Recv 0/0/0, Xmit 0/0/0, 0 Dups, 0 ReXmit
  Bad messages: 0, Bad slots: 0, Solicits accepted: 0
  Solicits rejected: 0, Multiple nodes: 0
  Groups: 0
  Service classes: 1
Node "service3", usage -1, Interface Ethernet0, Address 0000.0cff.c9ed
  Timer 99, sequence 9, changes 159, flags 0x0, protocol 5.1
  Facility 0, Product code 0, Product version 0
  Recv 0/0/0, Xmit 0/0/0, 0 Dups, 0 ReXmit
  Bad messages: 0, Bad slots: 0, Solicits accepted: 0
  Solicits rejected: 0, Multiple nodes: 0
  Groups: 0
  Service classes: 1
Node "service4", usage -1, Interface Ethernet0, Address 0000.0c02.c7c1
  Timer -10351, sequence 1, changes 131, flags 0x40, protocol 5.2
  Facility 0, Product code 0, Product version 0
  Recv 0/0/0, Xmit 0/0/0, 0 Dups, 0 ReXmit
  Bad messages: 0, Bad slots: 0, Solicits accepted: 0
  Solicits rejected: 0, Multiple nodes: 0
  Groups: 0
```



```
Service classes: 1
```

Table 25 describes the significant fields shown in the display.

Table 25 *show lat nodes Field Descriptions*

Field	Description
Node	The node name as reported by the host computer.
usage	The number of virtual circuits currently active to this node.
Interface	Node interface type and number.
Address	The MAC address of the Ethernet interface for the node.
Timer	The number of seconds remaining until the service advertisement message for this node will time out; this value is set to three times the nodes multicast timer value whenever a new service advertisement message is received.
sequence	The sequence number received in the last service advertisement message received. Nodes increment their sequence number when the contents of the service advertisement change.
changes	The internal representation of what changed in the multicast message the last time the sequence number changed.
flags	The internal representation of various state information about the node.
protocol	The LAT protocol version used by the node.
Facility	The remote facility number.
Product code	The remote product code.
Product version	The remote product version.
Recv and Xmit	The number of messages, slots, and bytes received or sent to the node. The number of messages is the number of LAT virtual circuit messages. Each virtual circuit message contains some number of slots, which contain actual terminal data or control information. Bytes is the number of data bytes (input or output characters) exchanged.
Dups	The number of duplicate virtual circuit messages received.
ReXmit	The number of virtual circuit messages resent.
Bad messages	The number of bad messages received.
Bad slots	The number of bad slots received.
Solicits accepted	The number of solicit-information requests accepted.
Solicits rejected	The number of solicit-information requests rejected.
Multiple nodes	The total of multiple nodes seen.
Groups	The list of group codes advertised by the service-advertisement message of the node.
Service classes	The number of service classes.

show lat services

To display information about learned local-area transport (LAT) services in the Cisco IOS software, use the **show lat services** command in EXEC mode.

```
show lat services [service-name]
```

Syntax Description	service-name (Optional) Name of a specific LAT service.
--------------------	---

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	11.2	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show lat services** command:

```
Router# show lat services

Service Name      Rating  Interface  Node (Address)
ABCDEFGHIJ         5       Ethernet0  SERVICE1 (0000.0c00.391f)
GLAD              84      Ethernet0  SERVICE2 (aa00.0400.9205)
  Ident: Welcome to Gateway
WHEEL            83      Ethernet0  SERVICE3 (aa00.0400.9005)
ZXYW              5       Ethernet0  SERVICE4 (0000.0c00.391f)
```

[Table 26](#) describes the significant fields shown in the display.

Table 26 show lat services Field Descriptions

Field	Description
Service Name	LAT service name.
Rating	Rating of the service. If a single service is provided by more than one host, the Cisco IOS software connects to the one with the highest rating.
Interface	Interface type.
Node	Connection address.
(Address)	Advertised identification for the service.

Related Commands	Command	Description
	show lat sessions	Displays active LAT sessions.
	show resource-pool call	Displays specific LAT learned services.

show lat sessions

To display active local-area transport (LAT) sessions, use the **show lat sessions** command in EXEC mode.

show lat sessions [*line-number*]

Syntax Description	<i>line-number</i> (Optional) Displays an active LAT session on a specific line.						
Command Modes	EXEC						
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>11.2</td><td>This command was introduced.</td></tr><tr><td>12.2SX</td><td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td></tr></table>	Release	Modification	11.2	This command was introduced.	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Release	Modification						
11.2	This command was introduced.						
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.						

Examples

The following is sample output from the **show lat sessions** command. In this example, information about all active LAT sessions is displayed. The output is divided into three sections for each session (in this case two sessions): TTY data, session data, and remote node data.

```
Router> show lat sessions
```

```
tty0, connection 1 to service TERM1
```

```
TTY data:
```

```
Name "0", Local usage 1/0, Remote usage disabled
```

```
Flags: Local Connects, Enabled
```

```
Type flags: none
```

```
Config flags: -FlowOut, -FlowIn, Parameter Info
```

```
Flow control ^S/^Q in ^S/^Q out, Mode Normal, Parity None, databits 8
```

```
Groups: 0
```

```
Session data:
```

```
Name TERM1, Remote Id 1, Local Id 1
```

```
Remote credits 2, Local credits 0, Advertised Credits 2
```

```
Flags: none
```

```
Max Data Slot 255, Max Attn Slot 255, Stop Reason 0
```

```
Remote Node data:
```

```
Node "TERM1", Address 0000.0C00.291F, usage 1
```

```
Timer 59, sequence 5, changes 159, flags 0x0, protocol 5.1
```

```
Recv 56/22/83, Xmit 41/23/14, 0 Dups, 0 ReXmit
```

```
Groups: 0
```

```
tty10, connection 1 to service ENG2
```

```
TTY data:
```

```
Name "10", Local usage 1/0, Remote usage disabled
```

```
Flags: Local Connects, Enabled
```

```
Type flags: none
```

```
Config flags: -FlowOut, +FlowIn, Set Parameters, 0x40000000
```

```
Flow control ^S/^Q in ^S/^Q out, Mode Normal, Parity None, databits 8
```

```
Groups: 0
```

```
Session data:
```

```
Name ENG2, Remote Id 1, Local Id 1
```

show lat sessions

```

Remote credits 1, Local credits 0, Advertised Credits 2
Flags: none
Max Data Slot 255, Max Attn Slot 255, Stop Reason 0
Remote Node data:
Node "ENG2", Address AA00.0400.34DC, usage 1
  Timer 179, sequence 60, changes 255, flags 0x0, protocol 5.1
  Recv 58/29/186, Xmit 50/36/21, 0 Dups, 0 ReXmit
  Groups: 0

```

The following sample output displays information about active LAT sessions on one line (line 10). The output is divided into three sections: TTY data, session data, and remote node data.

```

Router> show lat sessions 10

tty10, connection 1 to service ENG2
TTY data:
  Name "10", Local usage 1/0, Remote usage disabled
  Flags: Local Connects, Enabled
  Type flags: none
  Config flags: -FlowOut, +FlowIn, Set Parameters, 0x40000000
  Flow control ^S/^Q in ^S/^Q out, Mode Normal, Parity None, databits 8
  Groups: 0
Session data:
  Name ENG2, Remote Id 1, Local Id 1
  Remote credits 1, Local credits 0, Advertised Credits 2
  Flags: none
  Max Data Slot 255, Max Attn Slot 255, Stop Reason 0
Remote Node data:
Node "ENG2", Address AA00.0400.34DC, usage 1
  Timer 189, sequence 61, changes 247, flags 0x0, protocol 5.1
  Recv 60/29/186, Xmit 52/36/21, 0 Dups, 0 ReXmit
  Groups: 0

```

Table 27 describes the fields shown in the displays.

Table 27 *show lat sessions Field Descriptions*

Field	Description
TTY data	Summary of the LAT-oriented terminal-line-specific data.
Name	Name used for this port as a port identification string. The name is reported to remote systems, which can display it in some operating-system dependent manner. This value is also used for targets of host-initiated connections. Currently, this value is hard-wired to be the line number of the associated terminal line.
Local/Remote usage	Current status of the terminal. The number is reported as current/maximum, where current is the current number of sessions of a given type, and maximum is the maximum number of sessions allowed (or zero if there is no maximum). If a terminal is being used for outgoing sessions, the local usage is equal to the number of current LAT sessions. If the terminal is being used for incoming sessions, local usage is disabled, and the remote count and maximum is one.
Flags	Current state of the line, and whether there are any queued host-initiated connections.
Type flags	Report flags not used in the current software release.
Config flags	Current port state as reflected by the most recent configuration message exchange.

Table 27 *show lat sessions Field Descriptions (continued)*

Field	Description
Flow control	Lists set flow control characters.
Groups	Group code list currently in use for the line.
Session data	Reports various parameters about the connection.
Name	For the outbound connection, the name of the remote service to which it is connected. For inbound connections, this field is currently unused.
Remote/Local Id	Slot IDs being used to uniquely identify the session multiplexed over the underlying LAT virtual circuit.
Remote/Local/ Advertised Credits	Number of flow control credits that the Cisco IOS software will be sending to the host as soon as possible. The advertised credits are the number of credits that have already been sent.
Flags	Transient conditions in the LAT-state machine dealing with the current connection status.
Max Data Slot	Maximum number of characters that can be sent in a single data slot.
Max Attn Slot	Maximum amount of data that can be sent in an attention message. Current LAT implementations only send 1-byte attention messages (attention messages are used to flush buffered output). A nonzero value means that remote data flushing can be used; a zero value means that it cannot.
Stop Reason	Reason the session was stopped, if it was stopped but not deleted. This value is usually zero, indicating that the session has not yet been stopped. If a session persists for a long time with a nonzero stop reason, there is probably a problem in the local LAT software.
Remote Node data	Reports information about the remote node. The data includes the same fields as those from the show lat nodes output.
Node	Node name as reported by the host computer.
Address	MAC address of the Ethernet interface for the node.
usage	Number of virtual circuits currently active to the node.
Timer	Number of seconds remaining until the service advertisement message for the node will time out; this value is set to three times greater than the node multicast timer value whenever a new service-advertisement message is received.
sequence	Sequence number received in the last service-advertisement message. Nodes increment their sequence number when the contents of the service-advertisement change.
changes	Internal representation of what changed in the multicast message the last time the sequence number changed.
flags	Internal representation of various state information about the node.
protocol	LAT protocol version used by the node.
Recv and Xmit	Number of messages, slots, and bytes received or sent to the node. The number of messages is the number of LAT virtual circuit messages. Each virtual circuit message contains some number of slots, which contain actual terminal data or control information.
Dups	Number of duplicate virtual circuit messages received.

Table 27 *show lat sessions Field Descriptions (continued)*

Field	Description
ReXmit	Number of virtual circuit messages resent.
Groups	Group codes advertised by the service-advertisement message of the node.

Related Commands

Command	Description
show lat services	Displays information about learned LAT services in the Cisco IOS software.
show resource-pool call	Displays specific LAT learned services.

show lat traffic

To display information about traffic and resource utilization statistics on all active lines, use the **show lat traffic** command in EXEC mode.

show lat traffic

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples The following is sample output from the **show lat traffic** command:

```
Router# show lat traffic
```

```
Local host statistics:
  0/100 circuits, 0/500 sessions, 1/500 services
  100 sessions/circuit, circuit timer 80, keep-alive timer 5
Recv:  335535 messages (2478 duplicates),  161722 slots, 1950146 bytes
       0 bad circuit messages,  3458 service messages (52 used)
Xmit:  182376 messages (2761 retransmit),  146490 slots, 36085 bytes
       1 circuit timeouts
Total: 23 circuits created, 38 sessions
```

[Table 28](#) describes the significant fields shown in the display.

Table 28 *show lat traffic Field Descriptions*

Field	Description
Local host statistics	Information about the router.
circuits	Current number and maximum support number of virtual circuits.
sessions	Current and maximum number of sessions.
services	Current number of known remote services, and the maximum supported.
sessions/circuit	Number of sessions per virtual circuit supported by the software.
circuit timer	Value of the virtual circuit timer parameter defined by the lat vc-timer global configuration command.
keep-alive timer	Value defined by the lat ka-timer global configuration command.
Recv	Statistics about local node receive totals.
messages	Total count of virtual circuit messages received.

Table 28 *show lat traffic Field Descriptions (continued)*

Field	Description
duplicates	Number of duplicate virtual circuit messages received.
slots	Number of slots received.
bytes	Number of data bytes received.
bad circuit messages	Count of invalid messages received.
service messages	Number of service advertisement multicast messages received.
used	Number of multicast messages that caused the local node information to be updated.
Xmit	Various transmission totals.
messages	Total number of virtual circuit messages sent.
retransmit	Number of virtual circuit messages resent due to the lack of an acknowledgment.
slots	Number of data and control slots sent.
bytes	Count of user data bytes sent.
circuit timeouts	Count of times that a virtual circuit timed out because the remote node stopped responding (due to a node failure or communications failure).
Total	Count of virtual circuits and sessions that have existed since the router booted or rebooted.

show line

To display parameters of a terminal line, use the **show line** command in user EXEC or privileged EXEC mode.

```
show line [line-number [upper-line-number] | [{aux | console | vty} line-number
[upper-line-number]] [summary]
```

Syntax Description

<i>line-number</i>	(Optional) Absolute line number of the line for which you want to list parameters.
<i>upper-line-number</i>	(Optional) Specifies the upper limit of a range.
aux	(Optional) Auxiliary line.
console	(Optional) Primary terminal line.
vty	(Optional) Virtual terminal line.
summary	(Optional) Line status summary.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.3(1)T	The summary keyword was added.
12.0	The vty keyword was added.
12.1	Output from this command was modified to show the transport method configured.
12.2(13)T	This command was modified to indicate when support for closed user group (CUG) security is enabled on the line.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If Closed User Group (CUG) security is configured on a line, the **show line** command used with the *line-number* argument causes “CUG Security Enabled” to be displayed in the Capabilities field of the output.

The **show line** command used with the **summary** keyword provides line status summary details such as whether there were modem calls or character mode calls.

Examples

The following sample output from the **show line vty4** command shows that virtual terminal line 4 has a send and receive rate of 9600 bits per second (bps). Also shown are the terminal screen width and length, modem state, preferred transport method, and other characteristics.

Router# **show line vty4**

```

      Tty Typ      Tx/Rx      A Modem  Roty AccO AccI      Uses   Noise  Overruns
      22 VTY              -   -      -   -   -         0       0      0/0 -

Line 22, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600
Status: No Exit Banner
Capabilities: CUG Security Enabled
Modem state: Idle
Special Chars: Escape Hold Stop Start Disconnect Activation
                ^^x   none  -   -           none
Timeouts:      Idle EXEC Idle Session Modem Answer Session
Dispatch
                never      never      none      not set
                Idle Session Disconnect Warning
                never
                Login-sequence User Response
                00:00:30
                Autoselect Initial Wait
                not set

Modem type is unknown.
Session limit is not set.
Time since activation: never
Editing is enabled.
History is enabled, history size is 10.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed input transports are none.
Allowed output transports are pad v120 telnet rlogin udptn.
Preferred transport is telnet.
No output characters are padded
No special data dispatching characters

```

Table 29 describes the significant fields shown in the report displayed by the **show line** command (and may not match the previous example).

Table 29 *show line Field Descriptions*

Field	Description
Tty	Line number.
Typ	Type of line. In this case, a virtual terminal line, which is active, in asynchronous mode denoted by the preceding “A.” All possible values follow: • VTY—virtual terminal line • CTY—console • AUX—auxiliary port • TTY—asynchronous terminal port • lpt—parallel printer
Tx/Rx	Transmit rate/receive rate of the line.
A	Indicates whether autobaud has been configured for the line. A value of F indicates that autobaud has been configured; a hyphen indicates that it has not been configured.

Table 29 **show line Field Descriptions (continued)**

Field	Description
Modem	Types of modem signals that have been configured for the line. Possible values follow: • callin • callout • cts-req • DTR-Act • inout • RIisCD
Roty	Rotary group configured for the line, if set.
AccO, AccI	Output or input access list number configured for the line.
Uses	Number of connections established to or from the line since the system was restarted.
Noise	Number of times noise has been detected on the line since the system restarted.
Overruns	Hardware Universal Asynchronous Receiver/Transmitter (UART) overruns or software buffer overflows, both defined as the number of overruns or overflows that have occurred on the specified line since the system was restarted. Hardware overruns are buffer overruns; the UART chip has received bits from the software faster than it can process them. A software overflow occurs when the software has received bits from the hardware faster than it can process them.
A (or I or *)	An A at the upper left of the display indicates that the user is running an asynchronous interface; an I indicates that the line has an asynchronous interface available; an asterisk (*) indicates that the line is otherwise active (in character mode).
Line	Definition of the specified protocol and address of the line.
Location	Location of the current line.
Type	Type of line, as specified by the line global configuration command.
Length	Length of the terminal or screen display, in rows.
Width	Width of the terminal or screen display, in columns.
Baud rate (TX/RX)	Transmit rate/receive rate of the line, in bps.
Status	State of the line: ready or not, connected or disconnected, active or inactive, exit banner or no exit banner, asynchronous interface active or inactive.
Capabilities	Current terminal capabilities.
Modem state	Modem control state. Although the sample output shows the modem state Idle, this field should always say READY.

Table 29 *show line Field Descriptions (continued)*

Field	Description
Special Chars	Current settings of special characters that were input by the user (or taken by default) from the following global configuration commands: • escape-character • hold-character • stop-character • start-character • disconnect-character • activation-character
Timeouts	Current settings that were input by the user (or taken by default) from the following global configuration commands: • exec-timeout • session-timeout • dispatch-timeout • modem answer-timeout • session-disconnect-warning • timeout login response • autoselect timeout
Session limit	Maximum number of sessions.
Time since activation	Last time start_process was run.
Editing	Whether command-line editing is enabled.
History	Current history list size, set by the user (or taken by default) from the history configuration command.
DNS resolution in show commands is	Whether Open Shortest Path First (OSPF) is configured to look up Domain Name System (DNS) names for use in show EXEC command displays.
Full user help	Whether full user help has been set by the user with the terminal full-help EXEC command or by the administrator with the full-help line configuration command.
Allowed input transports are	Current set transport method, set by the user (or taken by default) from the transport input line configuration command.
Allowed output transports are	Current set transport method, set by the user (or taken by default) from the transport output line configuration command.
Preferred transport is	Current set transport method, set by the user (or taken by default) from the transport preferred line configuration command.
...characters are padded	Current set padding, set by the user (or taken by default) from the padding line configuration command.
...data dispatching characters	Current dispatch character set by the user (or taken by default) from the dispatch-character line configuration command.

Table 29 *show line Field Descriptions (continued)*

Field	Description
Modem type is unknown	No modemcap has been applied to this line, that means either modem autoconfigure has not been configured for the line, or modem autoconfigure discovery is configured. Autoconfigure is unable to discover the modem type.
Dispatch	Displays the current configured dispatch-timeout value.

The following sample output from the **show line summary** command shows line summary status for lines 1/3/36 through 1/3/102. Each row of output represents 36 lines, and the line status characters in groups of four for readability. For example, the first row represents information on rows 1/3/36 through 1/3/71, and the first line status character “U” corresponds to line 1/3/36.

Router# **show line summary**

```
1/3/36: U??? ---- ---- ---- --u- ---- ???? ....
1/3/72: ---- ???? ---- ???? ???? MMMM MMMM MMMM MMMM
```

```
2  character mode users.          (U)
19 lines never used.             (?)
31 lines used, but currently idle. (-)
4  lines do not exist.           (.)
16 lines in use by modem management (M)
```

```
18 total lines in use, 1 not authenticated (lowercase)
```

Table 30 describes the possible line status characters that can be shown in output from the **show line summary** command.

Table 30 *Line Status Character Descriptions*

Line Status Character	Description
?	Line has never been used.
-	Lines has been used but is currently idle.
.	Line does not exist.
A	Line in use by a packet mode user such as asynchronous PPP, Serial Line Internet Protocol (SLIP), Appletalk Remote Access Protocol (ARAP), or Serial Tunneling (STUN).
D	Line in use by a digit mode user such as V.110 or V.120.
F	Line in use by a TCP fast-stream user.
M	Line in use by modem management.
U	Line in use by character mode user, such as an EXEC user making an outbound packet connection using Telnet, rlogin, local-area transport (LAT), packet assembler/disassembler (PAD), or normal (nonfast-stream) TCP clear.
V	Line in use by a voice mode user.

Related Commands

Command	Description
modem enable	Enables backup dial capability through the console port (changes the console port into an auxiliary port).

show line autodetect

To detect the type of device connected on the console line, use the **show line autodetect** command in user EXEC or privileged EXEC mode.

show line autodetect

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.2(13)ZG	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Use this command to detect the type of device connected on the console line.

Examples The following example shows the command used to configure console autodetect mode:

```
Router(config-line)# modem enable autodetect
```

Use the **show line autodetect** command to determine when a modem or a console has been detected:

```
Router# show line autodetect  
Detection State: Feature not enabled
```

```
Router# show line autodetect  
Detection State: Nothing Attached
```

```
Router# show line autodetect  
Detection State: Init State
```

```
Router# show line autodetect  
Detection State: Console Attached
```

```
Router# show line autodetect  
Detection State: Modem Attached
```

[Table 31](#) describes the significant fields shown in the display.

Table 31 *show line autodetect Field Descriptions*

Field	Description
Detection State: Feature not enabled	No device connection is detected.
Detection State: Nothing Attached	No cable is attached to the EIA/TIA-232 port on the router.
Detection State: Init State	Autodetection has been enabled, but no changes have been detected.
Detection State: Console Attached	A DTE console or terminal device is attached.
Detection State: Modem Attached	A DCE asynchronous modem device is attached.

Related Commands

Command	Description
modem enable	Enables backup dial capability through the console port (changes the console port into an auxiliary port).

show node

To display information about local-area transport (LAT) nodes, use the **show node** command in EXEC mode.

```
show node [all | node-name] [counters | status | summary]
```

Syntax Description

all	(Optional) Specifies all nodes.
node-name	(Optional) Indicates the name of the node for which status is required.
counters	(Optional) Specifies the various node counters.
status	(Optional) Specifies detailed node status. This is the default if a node name is specified.
summary	(Optional) Specifies a status summary for the node. This is the default if no node name is specified.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Entering the **show node** command with no arguments is the same as entering the **show node all summary** command and shows a one-line summary of all known nodes.

You can enter the **show node** command with either a specific node name or the **all** keyword, but not both.

The **show node** command displays three different sets of information about a node: the node counters, the node status, or a one-line summary of the node status.

You can enter the **show node** command with only one of the **counters**, **status**, or **summary** keywords. If you enter **show node** and two of these keywords without specifying a node name, the first keyword is treated as a node name, causing an error. If you enter the **show node node-name** command and two of these keywords, the second keyword will be treated as ambiguous.

The **show node** command with a *node-name* argument but no **counters**, **status**, or **summary** keyword defaults to **show node node-name status**.

Examples

The following is sample output from the **show node** command with no further keywords (the same as the **show node all summary** command):

```
Router> show node

Node Name      Status      Identification
-----
CHAOS          Reachable
MUDDY-RIVER    Reachable
```



```
TARMAC          Reachable
WHEEL           Reachable    Welcome to VAX/VMS V5.4-2
```

Table 32 describes the significant fields shown in the display.

Table 32 *show node Field Descriptions*

Field	Description
Node Name	Lists the names of the nodes.
Status	Indicates whether the node is reachable or not.
Identification	Identification string for the node.

The following is sample output from the **show node** output that defaults to **show node chaos status**. It results in a display of the detailed status of node chaos.

```
Router> show node chaos

Node: CHAOS      Address: 00-00-0C-01-05-09
LAT Protocol: V5.1  Data Link Frame Size: 1500
Identification:
Node Groups: 0
Service Name  Status    Rating  Identification
CHAOS        Available  80
```

Table 33 describes the significant fields shown in the display.

Table 33 *show node status Field Descriptions*

Field	Description
Node	Lists the node name as reported by the host computer.
Address	Identifies the MAC address of the node Ethernet interface.
LAT protocol	Lists the version of the LAT protocol used by the node.
Data Link Frame Size	Lists the size of the largest packet that can be sent to the LAT host.
Identification	Lists the identification string for the node.
Node Groups	Lists the group code list that is advertised by the remote node, which comes from the service advertisement of the remote node.
Service Name	Lists the LAT service name.
Status	Indicates whether the node is currently available on the network.
Rating	Indicates the rating of the service: an integer from 0 to 255, with the highest number being the preferred service. Used for load balancing.

The following sample output displays the counter information for a specific node:

```
Router> show node tarmac counters

Node: tarmac
Seconds Since Zeroed: 100 Multiple Node Addresses: 0
Messages Received: 0 Duplicates Received: 0
Messages Transmitted: 0 Messages Re-transmitted: 0
Slots Received: 0 Illegal Messages Received: 0
Slots Transmitted: 0 Illegal Slots Received: 0
Bytes Received: 0 Solicitations Accepted: 0
```

Bytes Transmitted: 0 Solicitations Rejected: 0

In the following sample command and output displays, the **status** keyword is treated as the node name:

```
Router> show node status counters
```

Local -710- Node STATUS not known

In the following example, the second keyword **counters** is treated as ambiguous:

```
Router> show node lager status counters
```

Local -702- Keyword "COUNTERS" not known or ambiguous

show platform software configuration access policy

To view the access policies and banners for users entering the router using Telnet, Secure Shell (SSH), or the console port, enter the **show platform software configuration access policy** command in privileged EXEC and diagnostic mode.

show platform software configuration access policy

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	No default behavior or values.
------------------------	--------------------------------

Command Modes	Privileged EXEC (#) Diagnostic (diag)
----------------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines	Access policies for the console port, Telnet, and SSH are set through the use of transport maps. If no transport maps are applied for a particular access method, the router uses the default settings. Transport maps are configured by entering the transport-map type command, then setting the configuration of the transport map in transport map configuration mode. Transport maps are then enabled using the transport type global configuration command.
-------------------------	---

Examples	In the following example, the connection policy and banners are set for a persistent Telnet transport map, and the transport map is enabled.
-----------------	---

The **show platform software configuration access policy** output is given both before the new transport map is enabled and after the transport map is enabled so the changes to the Telnet configuration are illustrated in the output.

```
Router# show platform software configuration access policy
The current access-policies
```

```
Method      : telnet
Rule        : wait
Shell banner:
Wait banner :
```

```
Method      : ssh
Rule        : wait
Shell banner:
Wait banner :
```

```
Method      : console
```

■ show platform software configuration access policy

```

Rule          : wait with interrupt
Shell banner:
Wait banner :

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# transport-map type persistent telnet telnethandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# banner diagnostic X
Enter TEXT message.  End with the character 'X'.
Welcome to Diagnostic Mode
X
Router(config-tmap)# banner wait X
Enter TEXT message.  End with the character 'X'.
Waiting for IOS process
X
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit

Router(config)# transport type persistent telnet input telnethandler

Router# show platform software configuration access policy
The current access-policies

Method       : telnet
Rule         : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS process

Method       : ssh
Rule         : wait
Shell banner:
Wait banner :

Method       : console
Rule         : wait with interrupt
Shell banner:
Wait banner :

```

In the following example, the connection policy and banners are set for a persistent SSH transport map, and the transport map is enabled.

The **show platform software configuration access policy** output is given both before the new transport map is enabled and after the transport map is enabled so the changes to the SSH configuration are illustrated in the output.

```

Router# show platform software configuration access policy
The current access-policies

Method       : telnet
Rule         : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS process

```

```
Method      : ssh
Rule        : wait
Shell banner:
Wait banner :
```

```
Method      : console
Rule        : wait with interrupt
Shell banner:
Wait banner :
```

Router# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# **transport-map type persistent ssh sshhandler**

Router(config-tmap)# **connection wait allow interruptable**

Router(config-tmap)# **banner diagnostic X**

Enter TEXT message. End with the character 'X'.

Welcome to Diag Mode

X

Router(config-tmap)# **banner wait X**

Enter TEXT message. End with the character 'X'.

Waiting for IOS

X

Router(config-tmap)# **rsa keypair-name sshkeys**

Router(config-tmap)# **transport interface gigabitethernet 0**

Router(config-tmap)# **exit**

Router(config)# **transport type persistent ssh input sshhandler**

Router(config)# **exit**

Router# **show platform software configuration access policy**

The current access-policies

```
Method      : telnet
Rule        : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode
```

```
Wait banner :
Waiting for IOS process
```

```
Method      : ssh
Rule        : wait with interrupt
Shell banner:
Welcome to Diag Mode
```

```
Wait banner :
Waiting for IOS
```

```
Method      : console
Rule        : wait with interrupt
Shell banner:
Wait banner :
```

 show platform software configuration access policy**Related Commands**

Command	Description
banner (transport-map)	Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of the transport map configuration.
connection wait	Specifies how an incoming connection will be handled.
transport interface	Applies the transport map settings to the interface.
transport type persistent	Applies an already-configured persistent transport map to an interface.
transport-map type persistent	Creates and names a persistent transport map and enters transport map configuration mode.

show service

To display specific local-area transport (LAT) learned services, use the **show service** command in EXEC mode.

show service [*service-name*]

Syntax Description

service-name (Optional) The name of a specific LAT service.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show service** command without a service name displays a list of known LAT learned services. When entered with the *service-name* argument, it displays a more-detailed status of the named service. If no LAT learned service by the specified name is known, then a lookup is done for an IP host of that name.

Examples

The following is sample output from the **show service** command:

```
Router> show service
```

Service Name	Status	Identification
BLUE	Available	Welcome to VAX/VMS V5.4
CHAOS	Available	
MRL12	Available	
MUDDY-RIVER	Available	
STELLA-BLUE	Available	Welcome to VAX/VMS V5.4

The following is sample output of the **show service** command for a specific service:

```
Router> show service blue
```

```
Service BLUE - Available
Node Name   Status   Rating   Identification
BLUE        reachable 84       Welcome to VAX/VMS V5.4
```

[Table 34](#) describes the significant fields shown in the two previous displays.

Table 34 *show service Field Descriptions*

Field	Description
Service	Name of the service.
Node Name	Name of the nodes advertising the service.

Table 34 *show service Field Descriptions (continued)*

Field	Description
Status	Status of the service: Available or Unknown when a command is entered without a service name. Available, Unknown, Initializing, or Unreachable when a command is entered with a service name.
Rating	Rating of the service: An integer from 0 to 255, with the highest number being the preferred service. Used for load balancing.
Identification	Identification string.

show terminal

To obtain information about the terminal configuration parameter settings for the current terminal line, use the **show terminal** command in EXEC mode.

show terminal

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show terminal** command:

```
Router# show terminal
```

```
Line 2, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600
Status: Ready, Active, No Exit Banner
Capabilities: Enabled
Modem state: Ready
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
                ^^x   none  -    -      none
Timeouts:      Idle EXEC  Idle Session  Modem Answer  Session  Dispatch
                never    never          0:00:15      not imp  not set
Session limit is not set.
Allowed transports are telnet rlogin. Preferred is telnet
No output characters are padded
```

[Table 35](#) describes the fields in the first three lines of the **show terminal** output.

Table 35 *show terminal Field Descriptions—First Three Lines of Output*

Field	Description
Line 2	Current terminal line.
Location: ""	Location of the current terminal line, as specified using the location line configuration command.
Type: ""	Type of the current terminal line, as specified using the line global configuration command.
Length: 24 lines	Length of the terminal display.

Table 35 *show terminal Field Descriptions—First Three Lines of Output*

Field	Description
Width: 80 columns	Width of the terminal display, in character columns.
Baud rate (TX/RX) is 9600/9600	Transmit rate/receive rate of the line.

The following line of output indicates the status of the line:

Status: Ready, Active, No Exit Banner

Table 36 describes possible values for the Status field.

Table 36 *show terminal Field Descriptions—Status Field Values*

Field	Description
Active	A process is actively using the line.
Autobauding	The line is running the autobaud process.
Carrier Dropped	Some sense of “carrier” has been dropped, so the line process should be killed.
Connected	The line has at least one active connection.
Dialing Out	A dial-on-demand routing (DDR) asynchronous interface is dialing a remote site on this line.
Echo Off	The line is not echoing what the user types in (for example, because a password must be entered).
Escape Started	The first character of the escape sequence has been typed.
Escape Typed	Both characters of the escape sequence have been typed.
Hanging Up	The line state is “hanging up.”
Hardware XON/XOFF	The line uses a Universal Asynchronous Receiver/Transmitter (UART) that supports XON/XOFF flow control in hardware. (This does not mean that the line is currently using software flow control.)
Hold Typed	The user typed the “hold character” (and the line is paused).
Idle	The line modem state is “idle” (see modem state diagrams).
Idle Timeout	An idle timeout has occurred.
Input Stopped	The input has been turned off because of hardware flow control or overflow.
No Exit Banner	The normal exit banner will not be displayed on this line.
PSI Enabled	The line is paying attention to typed escape characters.
Rcvd BREAK	A BREAK sequence has been received on the line.
Rcvd Command	The line has received a special command sequence (for example, ^B for send break).
Rcvd CR	The last character received was a carriage return.
Ready	The line state is “ready.”
Ring Transition	A transition has occurred on the RING signal of the line.
Send Break Soon	Send a BREAK on the line soon.
Send XOFF Soon	Buffers are full and an XOFF should be sent soon.

Table 36 *show terminal Field Descriptions—Status Field Values*

Field	Description
Sending Break	A BREAK sequence is being sent on the line.
Sent XOFF	Buffers were full, so an XOFF was sent.
SLIP Mode	The line is running SLIP or PPP.

The following line of output indicates the status of the capabilities of the line. These capabilities correspond closely to configurable parameters that can be set using configuration commands.

Capabilities: Enabled

Table 37 describes possible values for the Capabilities field.

Table 37 *show terminal Field Descriptions—Capabilities Field Values*

Field	Description
Autobaud Full Range	Corresponds to the autobaud command.
Character Padding	At least one pad c x configuration command has been used.
Enabled	The user has “enabled” successfully.
EXEC Suppressed	Corresponds to the no exec command.
Hangup on Last Close	Corresponds to the autohangup command.
Hardware Flowcontrol In	Corresponds to the flowcontrol hardware in command.
Hardware Flowcontrol Out	Corresponds to the flowcontrol hardware out command.
Insecure	Corresponds to the insecure command.
Lockable	Corresponds to the lockable command.
Modem Callin	Corresponds to the modem callin command.
Modem Callout	Corresponds to the modem callout command.
Modem CTS-Required	Corresponds to the modem cts-required command.
Modem DTR-Active	Corresponds to the modem dtr-active command.
Modem RI is CD	Corresponds to the modem ri-is-cd command.
No Login Banner	Corresponds to the no exec-banner command.
Notification Set	Corresponds to the notify command.
Output Non-Idle	Corresponds to the session-timeout command.
Permanent SLIP	Corresponds to the slip-dedicated command
Private Line	Corresponds to the private command.
Refuse Suppress-GA	Corresponds to the telnet refuse command.
Receives Logging Output	Corresponds to the monitor command.
Refuse Telnet Echo	Corresponds to the telnet refuse command.
Send BREAK on IP	Corresponds to the telnet break-on-ip command.
SLIP allowed	Corresponds to the slip address command.
Software Flowcontrol In	Corresponds to the flowcontrol software in command.

Table 37 *show terminal Field Descriptions—Capabilities Field Values*

Field	Description
Software Flowcontrol Out	Corresponds to the flowcontrol software out command.
Telnet Transparent Mode	Corresponds to the telnet transparent command.

The following line of output indicates the modem state. Values include Autobauding, Carrier Dropped, Hanging Up, Idle, and Ready.

```
Modem state: Ready
```

The following lines of output indicate the special characters that can be entered to activate various terminal operations. The none or hyphen (-) values imply that no special characters are set.

```
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
                  ^^x    none  -    -          none
```

The following lines of output indicate the timeout values that have been configured for the line:

```
Timeouts:      Idle EXEC      Idle Session  Modem Answer  Session  Dispatch
                  never          never          0:00:15      not imp   not set
```

[Table 38](#) describes the fields in the preceding lines of output.

Table 38 *show terminal Field Descriptions—Timeouts*

Field	Description
Idle EXEC	Interval that the EXEC command interpreter waits for user input before resuming the current connection; or if no connections exist, returning the terminal to the idle state and disconnecting the incoming session. This interval is set using the exec-timeout command.
Idle Session	Interval that the Cisco IOS software waits for traffic before closing the connection to a remote computer and returning the terminal to an idle state. This interval is set using the session-timeout command.
Modem Answer	Interval during which the software raises DTR in response to RING and the modem response to CTS. This interval is set using the modem answer-timeout command.
Session	Not implemented in this release.
Dispatch	Number of milliseconds the software waits after putting the first character into a packet buffer before sending the packet. This interval is set using the dispatch-timeout command.

The following lines of output indicate how various options have been configured:

```
Session limit is not set.
Allowed transports are telnet rlogin. Preferred is telnet
No output characters are padded
```

show tn3270 ascii-hexval

To determine ASCII-hexadecimal character mappings, use the **show tn3270 ascii-hexval** command in EXEC mode.

show tn3270 ascii-hexval

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.3	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Use the **show tn3270 ascii-hexval** command to display the hexadecimal value of a character on your keyboard. After you enter the **show tn3270 ascii-hexval** command, you will be prompted to press a key. The hexadecimal value of the ASCII character is displayed. This command is useful for users who do not know the ASCII codes associated with various keys or do not have manuals for their terminals.

Examples The following is sample output from the **show tn3270 ascii-hexval** command:

```
Router> show tn3270 ascii-hexval

Press key> 7 - hexadecimal value is 0x37.

Router> show tn3270 ascii-hexval
Press key> f - hexadecimal value is 0x66.

Router> show tn3270 ascii-hexval
Press key> not printable - hexadecimal value is 0xD.
```

Related Commands	Command	Description
	show tn3270 character-map	Displays character mappings between ASCII and EBCDIC.
	tn3270 character-map	Converts incoming EBCDIC characters into ASCII characters for TN3270 connections.

show tn3270 character-map

To display character mappings between ASCII and EBCDIC, use the **show tn3270 character-map** command in EXEC mode.

show tn3270 character-map {**all** | *ebcdic-in-hex*}

Syntax Description

all	Displays all nonstandard character mappings.
<i>ebcdic-in-hex</i>	Displays the ASCII mapping for a specific EBCDIC character.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show tn3270 character-map** command:

```
Router# show tn3270 character-map all
```

```
EBCDIC 0x81 <=> 0x78 ASCII
EBCDIC 0x82 <=> 0x79 ASCII
EBCDIC 0x83 <=> 0x7A ASCII
```

Refer to the **tn3270 character-map** command for more information about EBCDIC and ASCII character mappings.

Related Commands

Command	Description
show tn3270 ascii-hexval	Displays ASCII-hexadecimal character mappings.
tn3270 character-map	Converts incoming EBCDIC characters into ASCII characters for TN3270 connections.

show translate

To display translation sessions that have been configured, use the **show translate** command in privileged EXEC mode.

show translate

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.3	This command was introduced.
	12.3(2)T	Output fields were added to display information about translation sessions configured to use an End-of-Record (EOR) marker.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines The display from this command shows each translation session set up on the router. It shows the incoming device and virtual terminal protocol, and the outgoing device and protocol.

Examples The following **show translate** sample output is based on the following **translate** command configuration:

```
translate x25 3131415912345 ppp ip-pool scope-name router1 keepalive 0
```

If the previous **translate** command is enabled, the following output is created by the **show translate** command:

```
Router# show translate
```

```
Translate From: x25 3131415912345
              To:   PPP ip-pool scope-name router1 keepalive 0
                  1/1 users active, 1 peak, 1 total, 0 failures
```

[Table 39](#) describes the significant fields shown in the display.

Table 39 *show translate Field Descriptions—X.25 to IP Translation*

Field	Description
Translate From: x25 3131415912345	Protocol (X.25) and address (3131415912345) of the incoming device.
To: PPP	The virtual terminal protocol (PPP).
ip-pool	Obtain an IP address from a DHCP proxy client or a local pool.

Table 39 *show translate Field Descriptions—X.25 to IP Translation (continued)*

Field	Description
scope-name router1	Specific local scope name (router1) from which to obtain an IP address.
keepalive 0	Indicates that keepalive updates have been disabled for the current translation session.
1/1 users active	Number of users active over the total number of users.
1 peak	Maximum number of translate sessions up at any given time.
1 total	Total number of translation sessions.
0 failures	Number of failed translation attempts resulting from this configuration.

The following **show translate** sample output is based on the following **translate** command configuration:

```
translate x25 31301234 PPP 192.168.14.23 ipx-client Loopback0
```

If the previous **translate** command is enabled, the following output is created by the **show translate** command:

```
Router# show translate
```

```
Translate From: x25 31301234
               To:   PPP 192.168.14.23 ipx-client Loopback0
               1/1 users active, 1 peak, 1 total, 0 failures
```

[Table 40](#) describes the significant fields shown in the display.

Table 40 *show translate Field Descriptions—X.25 to IPX Translation*

Field	Description
Translate From: x25 31301234	Protocol (X.25) and address (31301234) of the incoming device.
To: PPP 192.168.14.23	The virtual terminal protocol (PPP) and IP address of the outgoing device.
ipx-client Loopback0	Indicates that loopback interface 0 has been configured in client mode.
1/1 users active	Number of users active over the total number of users.
1 peak	Maximum number of translate sessions up at any given time.
1 total	Total number of translation sessions.
0 failures	Number of failed translation attempts resulting from this configuration.

The following **show translate** sample output is based on the following **translate** command configuration:

```
translate tcp 10.60.155.63 x25 12345678 pvc 3 dynamic eor 0x19 insert
```

If the previous **translate** command is enabled, the following output is created by the **show translate** command:

```
Router# show translate
```

```
Translate From: TCP 10.60.155.63 Port 23
               To: X25 12345678 Pvc 3 dynamic
```



```
EOR 0x19 Insert
1/1 users active, 1 peak, 1 total, 0 failures
```

Table 41 describes the significant fields shown in the display.

Table 41 *show translate Field Descriptions—TCP to X.25 Translation*

Field	Description
Translate From: TCP 10.60.155.63 Port 23	Protocol (TCP) and address (10.60.155.63) of the incoming device.
To: X25 12345678	The virtual terminal protocol (X.25) and X.121 destination address of the outgoing device.
Pvc 3	The outgoing connection is using permanent virtual circuit (PVC) 3.
dynamic	Terminate the TCP-to-X.25 PVC session when the interface goes down.
EOR 0x19 Insert	Indicates that EOR functionality is configured and that the EOR marker (0x19) will be inserted into the TCP stream after each received X.25 packet that does not contain the More-bit set.
1/1 users active	Number of users active over the total number of users.
1 peak	Maximum number of translate sessions up at any given time.
1 total	Total number of translation sessions.
0 failures	Number of failed translation attempts resulting from this configuration.

show translate ruleset

To display a summary of a specific or of all configured translate rulesets, behavioral parameters, and usage statistics, use the **show translate ruleset** command in user or privileged EXEC mode.

show translate ruleset [*name*]

Syntax Description

name (Optional) Ruleset name.

Defaults

Displays all one-line **translate** command and ruleset configuration and connection information.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is useful for maintaining and updating ruleset statements. The output of this command identifies **match**, **skip**, **set**, **test**, and **substitute** statement lines and numbers them. The line number can be used to reconfigure or remove any of these statements.

When the optional *name* argument is used, the display includes only the configured ruleset and does not include information about the standard one-line translate commands.

Examples

Specific Ruleset Information

The following example shows specific information about the ruleset named A:

```
Router# show translate ruleset A
```

```
PT ruleset A, from pad to telnet.
administrative locks: 2 (2 readers, 0 writers).
translations: 0 created, 0 active, 0 failed, 0 created for test.
match/skip lines: 2.
#1 match on 1 pad test: dest-addr ^5555(.)$.
#2 skip on 1 pad test: dest-addr ^5555[89]$.
options: limited to 10 active sessions.
set/test/substitute lines: 3.
#1 set 1 parameter: telnet/dest-addr 10.2.2.1.
#2 substitute from: pad/dest-addr ^5555(.)$ into telnet/dest-port 200\1.
#3 test 1 parameter: telnet/dest-port 2004; to set 1: telnet/dest-port 2010.
```

Information About All Rulesets

The following example shows information about all protocol translation rulesets configured on the device:

```
Router# show translate ruleset
```

```
Protocol translation rulesets: 27 created, 25 deleted, 25 freed, 0 failed.
2 active rulesets.
in/out: telnet 1/1, pad 1/1, ppp -/0, autocommand -/0, virtual-template -/0.
PT ruleset A, from telnet to pad.
administrative locks: 2 (2 readers, 0 writers).
translations: 2 created, 0 active, 0 failed, 4 created for test.
match/skip lines: 1.
#1 match on 1 telnet test: dest-addr 10.2.2.3.
options: none configured.
set/test/substitute lines: 4.
#1 test 1 parameter: telnet/dest-addr 10.2.2.3; to set 1: pad/dest-addr 4444.
#2 test 1 parameter: pad/dest-addr 4444; to set 1: pad/source-addr-ext 11.2222.2.
#3 substitute from: pad/source-addr-ext 11.2222.2 into pad/source-addr-ext 11.2222.3.
#4 test 1 parameter: pad/source-addr-ext ^11.2222.3$; to set 1: telnet/binary 1.
PT ruleset B, from pad to telnet.
administrative locks: 2 (2 readers, 0 writers).
translations: 0 created, 0 active, 0 failed, 0 created for test.
match/skip lines: 2.
#1 match on 1 pad test: dest-addr ^5555(.)$.
#2 skip on 1 pad test: dest-addr ^55551$
set/test/substitute lines: 3.
#1 set 1 parameter: telnet/dest-addr 10.2.2.1.
#2 substitute from: pad/dest-addr ^5555(.) into telnet/dest-port 2000.
#3 test 1 parameter: pad/dest-addr ^5555[6-9]
```

Table 42 describes *all* significant fields seen that may be reported by this command.

Table 42 *show translate ruleset Field Descriptions*

Field	Description
Protocol translation rulesets:	Describes ruleset memory management statistics. In the sample output seen in the “Information About All Rulesets” section, there were 27 total translate rulesets created, 25 rulesets deleted from the configuration, 25 rulesets freed, and 0 ruleset creation failure.
active ruleset:	Total number of current configured ruleset (rulesets created - rulesets deleted).
in/out:	Ruleset translation protocol counts, by incoming and outgoing protocol.
PT ruleset	Shows the defined name of the ruleset. In the sample output seen in the “Information About All Rulesets” section, the ruleset named A is configured to translate from a Telnet connection to PAD a connection.
administrative locks:	Describes the total ruleset administrative locks.
readers:	Total count of administrative locks.
writers:	Total count of configuration editors (rulesets being edited).
	Note Editing a ruleset changes the behavior of the set as a whole; an incoming connection will not be processed against a ruleset with an editor lock.

Table 42 *show translate ruleset Field Descriptions (continued)*

Field	Description
translations:	Describes ruleset memory management statistics for the dynamic one-line translate command, generated for and used by the protocol translation operation.
created:	Total number of translation sessions created by this ruleset.
test function translations:	Total number of translations created by the test (ruleset) command.
active:	Total number of active connections through this translation.
failed:	Total number of attempted translation connections that failed. Example of failures: number of maximum users limit has reached, a destination host not responding, an access failure, login failure, no resources, and so on.
(0 max-user):	Total number of connections refused due to reaching maximum users limit; (zero, in this example).
match/skip lines:	Total number of match and skip lines configured for the ruleset.
#1 match #2 skip	The line number within the block of match and skip commands.
options:	Options configured for ruleset processing.
set/test/substitute lines:	Total number of set, test, and substitute lines configured for the ruleset.
#1 set #2 substitute #3 test	Reports the line number within the block of set , substitute , and test commands and describes the commands configured for the ruleset.
#line number substitute from:	Reports the line number within the block of set , test , and substitute commands and describes the substitute command configured for the ruleset.
#line number [set/test] parameter:	Reports the line number within the block of set and test commands and describes the set and test parameters configured for the ruleset.

Related Commands

Command	Description
description (ruleset)	Adds a description about a translation ruleset.
match (ruleset)	Identifies a connection for processing by the translation ruleset.
options (ruleset)	Specifies protocol translation options in a translation ruleset.
set (ruleset)	Unconditionally sets one or more connection parameters to a fixed value for a translation ruleset.
skip (ruleset)	Identifies a connection for omission by the translation ruleset.
substitute (ruleset)	Matches an available protocol and substitutes another in a translation ruleset.
test (ruleset)	Tests parameter values in a translation ruleset using regular expressions.
test translate	Displays a trace of protocol translation behavior for a connection attempt.

Command	Description
translate ruleset	Defines a unique name for a translation ruleset, specifies translated protocols, and enters translate ruleset configuration mode.
x25 pvc translate ruleset	Configures PVCs that are valid for protocol translation ruleset handling.

show transport-map

To view the transport map configuration details on your router, enter the **show transport-map** EXEC or privileged EXEC command.

```
show transport map [all | name transport-map-name | type [console | persistent [ssh | telnet | webui]]]
```

Syntax Description		
all		Specifies information on all transport maps.
name <i>transport-map-name</i>		Specifies information on a specific transport map, where <i>transport-map-name</i> is the name of the specific transport map.
type [console persistent [ssh telnet webui]]		Specifies information on all transport maps of a specific type on the router. Options include: console—specifies information on all console port transport maps. persistent ssh—specifies information on all persistent ssh transport maps. persistent telnet—specifies information on all persistent telnet transport maps. persistent webui—specifies information on all web user interface transport maps.

Command Modes	EXEC (>) Privileged EXEC (#)
---------------	---------------------------------

Command Default	No default behavior or values.
-----------------	--------------------------------

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines	This command is used to view information about transport map configurations. If you are unable to access the IOS CLI in diagnostic mode and want transport map configuration information, the show platform software configuration access policy command is available in diagnostic mode and provides some of the information displayed in this command output for console port, Telnet, and SSH connections.
------------------	--

Examples	In the following example, the router has a console port transport map named consolehandler, a persistent SSH transport map named sshhandler, and a persistent Telnet transport map named telnethandler. The show transport-map all, show transport-map type, and show transport-map name command are all used throughout the example to gather information on the transport maps.
----------	---

```
Router#show transport-map all
Transport Map:
  Name: consolehandler
  Type: Console Transport

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for the IOS CLI

  Bshell banner:

Welcome to Diagnostic Mode

Transport Map:
  Name: sshhandler
  Type: Persistent SSH Transport

Interface:
  GigabitEthernet0

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for IOS prompt

  Bshell banner:

Welcome to Diagnostic Mode

SSH:
  Timeout: 120
  Authentication retries: 5
  RSA keypair: sshkeys

Transport Map:
  Name: telnethandler
  Type: Persistent Telnet Transport

Interface:
  GigabitEthernet0

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for IOS process

  Bshell banner:

Welcome to Diagnostic Mode

Transport Map:
  Name: telnethandling1
  Type: Persistent Telnet Transport

Connection:
  Wait option: Wait Allow
```

```
Router#show transport-map type console
```

```
Transport Map:
```

```
  Name: consolehandler
```

```
  Type: Console Transport
```

```
Connection:
```

```
  Wait option: Wait Allow Interruptable
```

```
  Wait banner:
```

```
Waiting for the IOS CLI
```

```
  Bshell banner:
```

```
Welcome to Diagnostic Mode
```

```
Router#show transport-map type persistent ssh
```

```
Transport Map:
```

```
  Name: sshhandler
```

```
  Type: Persistent SSH Transport
```

```
Interface:
```

```
  GigabitEthernet0
```

```
Connection:
```

```
  Wait option: Wait Allow Interruptable
```

```
  Wait banner:
```

```
Waiting for IOS prompt
```

```
  Bshell banner:
```

```
Welcome to Diagnostic Mode
```

```
SSH:
```

```
  Timeout: 120
```

```
  Authentication retries: 5
```

```
  RSA keypair: sshkeys
```

```
Router#show transport-map type persistent telnet
```

```
Transport Map:
```

```
  Name: telnethandler
```

```
  Type: Persistent Telnet Transport
```

```
Interface:
```

```
  GigabitEthernet0
```

```
Connection:
```

```
  Wait option: Wait Allow Interruptable
```

```
  Wait banner:
```

```
Waiting for IOS process
```

```
  Bshell banner:
```

```
Welcome to Diagnostic Mode
```

```
Transport Map:
```

```
  Name: telnethandling1
```

```
  Type: Persistent Telnet Transport
```



```
Connection:
  Wait option: Wait Allow

Router#show transport-map name telnethandler
Transport Map:
  Name: telnethandler
  Type: Persistent Telnet Transport

Interface:
  GigabitEthernet0

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for IOS process

  Bshell banner:

Welcome to Diagnostic Mode

Router#show transport-map name telnethandler1
% No transport map telnethandler1
Router#show transport-map name consolehandler
Transport Map:
  Name: consolehandler
  Type: Console Transport

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for the IOS CLI

  Bshell banner:

Welcome to Diagnostic Mode

Router#show transport-map name sshhandler
Transport Map:
  Name: sshhandler
  Type: Persistent SSH Transport

Interface:
  GigabitEthernet0

Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:

Waiting for IOS prompt

  Bshell banner:

Welcome to Diagnostic Mode

SSH:
  Timeout: 120
  Authentication retries: 5
  RSA keypair: sshkeys
```

■ show transport-map

Router#

In the following example, a transport map that has enabled both the HTTP server and the secure HTTP server is viewed using this command.

```
Router# show transport-map type persistent webui
Transport Map:
  Name: webui_http_https
  Type: Persistent Webui Transport

Webui:
  Server:          enabled
  Secure Server:  enabled
```

Table 43 *show transport-map Field Descriptions*

Field	Description
Name:	Specifies the name of the transport map. A transport-map is named when the transport-map type command is entered in global configuration mode to create a transport map.
Type:	Specifies the type of transport map. The possibilities include Console Transport for console port transport maps, Persistent SSH for Persistent SSH transport maps, and Persistent Telnet for persistent Telnet transport maps, Persistent WebUI Transport for web user interface transport maps.
Wait option:	Displayed the connection policy. The connection policy is defined using the connection wait transport map configuration command, and can include allow (wait for an IOS vty line, or exit router if send break signal is sent), allow interruptable (wait for an IOS vty line, and enter diagnostic mode if a send break signal is sent), none (immediately enter diagnostic mode if no IOS vty line is available, or none disconnect (immediately leave router if no IOS vty line is available).
Wait banner:	Specifies the banner seen when a user is waiting for an IOS vty line. The wait banner is defined using the banner wait transport map configuration mode command. If no text is seen, there is no wait banner.
Bshell banner:	Specifies the banner seen when a user is waiting for an diagnostic mode. The wait banner is defined using the banner diagnostic transport map configuration mode command. If no text is seen, there is no wait banner.
Interface:	Specifies the interface where the transport map will be applied if it is enabled or once it is enabled. The interface is defined using the transport interface transport map configuration mode command.
Timeout:	The login SSH timeout value, in seconds. The login timeout value can be set for SSH transport maps using the time-out transport map configuration command and has a default of 120 seconds.
Authentication-retries:	The number of authentication retries before dropping the connection for a persistent SSH connection attempt. This value can be set using the authentication-retries transport map configuration command.

Table 43 *show transport-map Field Descriptions (continued)*

Field	Description
RSA keypair:	The RSA keypair name, which is set using the rsa keypair-name transport map configuration command.
Server	The HTTP server. This value tells users if the HTTP server is enabled or disabled when a particular web user interface transport map is used.
Secure Server	The secure HTTP (HTTPS) server. This value tells users if the secure HTTP server is enabled or disabled when a particular web user interface transport map is used.

Related Commands

Command	Description
authentication-retries	Specifies the number of SSH authentication retries before dropping the connection when a persistent SSH transport map is applied to the receiving interface.
banner (transport map)	Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of the transport map configuration.
connection wait	Specifies how an incoming connection will be handled.
rsa keypair-name	Names the RSA keypair to be used for persistent SSH connections.
secure-server	Enables the secure HTTP (HTTPS) server for a persistent web user interface transport map.
server	Enables the HTTP server for a persistent web user interface transport map.
show platform software configuration access policy	Displays the access policy and banner settings for console, Telnet, and SSH connections.
time-out	Specifies the SSH timeout interval in seconds.
transport interface	Applies the transport map settings to the interface.
transport type persistent	Applies an already-configured persistent transport map to an interface.
transport-map type persistent	Creates and names a persistent transport map and enters transport map configuration mode.

show ttycap

To test for the availability of a ttycap after a connection on a router takes place, use the **show ttycap** command in EXEC mode.

show ttycap [*ttycap-name* | **all**]

Syntax Description

<i>ttycap-name</i>	(Optional) Name of a ttycap.
all	(Optional) Lists the names of all defined ttycaps. The name of the default ttycap is not listed.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Cisco IOS software searches for the specified ttycap in its active configuration image, and lists the complete entry if found. If it is not found, an appropriate “not found” message appears.

If you do not include any arguments with the **show ttycap** command, then the current keymap used for the terminal is displayed.

Examples

The following is sample output from the **show ttycap** command:

```
Router# show ttycap
```

```
d0|vt100|vt100-am|vt100am|dec vt100:do=^J:co#80:li#24:\
cl=50^[[;H^[[2J:bs:am:cm=5^[[%i%d;%dH:nd=2^[[C:up=2^[[A:\
ce=3^[[K:so=2^[[7m:se=2^[[m:us=2^[[4m:ue=2^[[m:md=2^[[1m:\
me=2^[[m:ho=^[[H:xn:sc=^[7:rc=^[8:cs=^[[%i%d;%dr:
```

```
Router# show ttycap all
```

```
ttycap3    d0|vt100|vt100-am|vt100am|dec vt100
ttycap2    d1|vt200|vt220|vt200-js|vt220-js|dec vt200 series with jump scroll
ttycap1    ku|h19-u|h19u|heathkit with underscore cursor
```

```
Router# show ttycap ttycap1
```

```
ttycap1    ku|h19-u|h19u|heathkit with underscore cursor:\:vs@:ve@:tc=h19-b:\
:al=1*\EL:am:le=^H:bs:cd=\EJ:ce=\EK:cl=\EE:cm=\EY%+ %+\
:co#80:dc=\EN:\:dl=1*\EM:do=\EB:ei=\EO:ho=\EH\
:im=\E@:li#24:mi:nd=\EC:as=\EF:ae=\EG:\
:ms:pt:sr=\EI:se=\Eq:so=\Ep:up=\EA:vs=\Ex4:ve=\Ey4:\
:kb=^h:ku=\EA:kd=\EB:kl=\ED:kr=\EC:kh=\EH:kn#8:ke=\E>:ks=\E=:\
:k1=\ES:k2=\ET:k3=\EU:k4=\EV:k5=\EW:\
```

```
:l6=blue:l7=red:l8=white:k6=\EP:k7=\EQ:k8=\ER:\
:es:hs:ts=\Ej\Ex5\Ex1\EY8%+ \Eo:fs=\Ek\Ey5:ds=\Ey1:
```

Refer to the **ttycap** command for more information about keyboard mappings and keymap entry structures.

Related Commands

Command	Description
keymap	Defines characteristics of a terminal emulation file.

show users

To display information about the active lines on the router, use the **show users** command in privileged EXEC mode.

show users [**all**] [**lawful-intercept**]

Syntax Description

all	(Optional) Specifies that all lines be displayed, regardless of whether anyone is using them.
lawful-intercept	(Optional) Displays lawful-intercept users.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	The lawful-intercept keyword was introduced.
12.2(33)SRB	The lawful-intercept keyword was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command displays the line number, connection name, idle time, hosts (including virtual access interfaces), and terminal location. An asterisk (*) indicates the current terminal session.

If the **lawful-intercept** keyword is issued, the names of all users who have access to a configured lawful intercept view will be displayed. To access the **show users lawful-intercept** command, you must be an authorized lawful-intercept-view user.

Examples

The following is sample output from the **show users** command:

```
Router# show users
      Line      User      Host(s)      Idle Location
      0 con 0           idle
*    2 vty 0      user1      idle          0  SERVICE1.CISCO.COM
```

The following is sample output identifying an active virtual access interface:

```
Router# show users

Line      User      Host(s)      Idle   Location
*  0 con 0           idle        01:58
   10 vty 0      Virtual-Access2      0      1212321
```

The following is sample output from the **show users all** command:

```
Router# show users all
      Line      User      Host(s)      Idle   Location
```

```
* 0 vty 0 user1 idle 0 SERVICE1.CISCO.COM
1 vty 1
2 con 0
3 aux 0
4 vty 2
```

Table 44 describes the significant fields shown in the displays.

Table 44 *show users Field Descriptions*

Field	Description
Line	Contains three subfields: - The first subfield (0 in the sample output) is the absolute line number. - The second subfield (vty in the sample output) indicates the type of line. Possible values follow: - con—console - aux—auxiliary port - tty—asynchronous terminal port - vty—virtual terminal - The third subfield (0 in the * sample output) indicates the relative line number within the type.
User	User using the line. If no user is listed in this field, no one is using the line.
Host(s)	Host to which the user is connected (outgoing connection). A value of idle means that there is no outgoing connection to a host.
Idle	Interval (in minutes) since the user has entered something.
Location	Either the hard-wired location for the line or, if there is an incoming connection, the host from which incoming connection came.

The following sample output from the **show users lawful intercept** command, shows three LI-View users on the system—li_admin, li-user1, and li-user2”:

```
Router# show users lawful-intercept
li_admin
li-user1
li-user2
Router#
```

Related Commands

Command	Description
line	Identifies a specific line for configuration and starts the line configuration command collection mode.
li-view	Creates a lawful intercept view.
show line	Displays the parameters of a terminal line.
username	Establishes a username-based authentication system.

show x25 pad

To display information about current open connections, including packet transmissions, X.3 parameter settings, and the current status of virtual circuits, use the **show x25 pad** command in EXEC mode.

show x25 pad

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples The following is sample output from the **show x25 pad** command:

```
Router# show x25 pad

tty2, Incoming PAD connection
Total input: 61, control 6, bytes 129. Queued: 0 of 7 (0 bytes).
Total output: 65, control 6, bytes 696.
Flags: 1, State: 3, Last error: 1
ParamsIn: 1:1, 2:0, 3:2, 4:1, 5:1, 6:0, 7:21,
          8:0, 9:0, 10:0, 11:14, 12:0, 13:0, 14:0, 15:1,
          16:127, 17:21, 18:18, 19:0, 20:0, 21:0, 22:0,
ParamsOut: 1:1, 2:1, 3:2, 4:1, 5:0, 6:0, 7:4,
           8:0, 9:0, 10:0, 11:14, 12:0, 13:0, 14:0, 15:0,
           16:127, 17:21, 18:18, 19:0, 20:0, 21:0, 22:0,
LCI: 1, State: D1, Interface: Serial0
Started 0:11:10, last input 0:00:16, output 0:00:16
Connected to 313700540651
Window size input: 7, output: 7
Packet size input: 512, output: 512
PS: 1 PR: 5 ACK: 5 Remote PR: 1 RCNT: 0 RNR: FALSE
Retransmits: 0 Timer (secs): 0 Reassembly (bytes): 0
Held Fragments/Packets: 0/0
Bytes 696/129 Packets 65/61 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

[Table 45](#) describes the fields shown in the display.

Table 45 *show x25 pad Field Descriptions*

Field	Description
Total input/output	Number of packets received or sent for the connection.
control	Number of packets with Qbit set (X.29 control packets).
bytes	Number of bytes in each direction.

Table 45 *show x25 pad Field Descriptions (continued)*

Field	Description
Queued	Number of unread packets waiting for the connection.
Waiting to send	Local data packet bit not sent (part of a line).
Flags, State, Last error	Displays data for detecting errors and tracing initialization status. Only useful to your Cisco-certified technical support personnel.
ParamsIn	Parameters read from the PAD at the start of the connection.
ParamsOut	Active X.3 parameters.
LCI, State, Interface	Status of the X.25 virtual circuit associated with the PAD connection. This is the same display that the show x25 vc command shows.

skip (ruleset)

To identify a connection to ignore by the translation ruleset, use the **skip** command in translate ruleset configuration mode. To remove the test operation, use one of the two **no** forms of this command.

skip [*#line-number*] *incoming-connection-parameter regular-expression* [*#line-number incoming-connection-parameter regular-expression* ...]

no skip *incoming-connection-parameter regular-expression* [*incoming-connection-parameter regular-expression* ...]

no skip *#line-number* [...]

Syntax Description	<i>#line-number</i>	(Optional) The line in the translation ruleset to test for a skip operation. The # character must be entered.
	<i>incoming-connection-parameter</i>	Incoming protocol parameter to test for; up to six skip tests can be written on one command line. Parameters are available for packet assembler/disassembler (PAD) and Telnet connections, and are listed in Table 46 and Table 47 .
	<i>regular-expression</i>	Pattern with regular expression to test for ignoring.
	[...]	(Optional) Specifies that multiple entries can be made as follows: - Up to six skip tests can be written on one command line. - Multiple line numbers can be specified using the second no form of this command.

Defaults No default behavior or values

Command Modes Translate ruleset configuration

Command History	Release	Modification
	12.3(8)T	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Up to six skip tests can be written on one command line. The ellipses in the format shown above means multiple skip tests can be written in a translation ruleset statement.

For incoming connection attempts, a template is configured, and within the template a connection can be identified by tests written using Cisco regular expressions and a pattern that is ignored (skipped).

The translation ruleset templates have line numbers that can be displayed using the **show translate ruleset EXEC** command.

Cisco regular expressions are described in Appendix A, “Regular Expressions,” in the *Cisco IOS Terminal Services Configuration Guide*.

Table 46 and Table 47 list the protocol parameter keywords and arguments that can be specified in the skip statements for incoming PAD and Telnet connections.

Table 46 Skip Keywords for Incoming PAD Connections

Keyword	Description
cud <i>ASCII-string</i>	Call user data (CUD) that occurs after the protocol identification (PID). For outgoing PAD connections, this is the optional, user-specified text included in the outgoing call request packet after the protocol identification bytes. The CUD is entered as an ASCII string.
dest-addr <i>address</i>	Destination X.121 address entered as a number from 0 to 15 digits long.
dest-addr-ext <i>address</i>	Network service access point (NSAP) destination address extension.
dlci <i>number</i>	Frame Relay data-link connection identifier (DLCI) of an Annex G service entered as a number from one to seven digits, although a size of two to four digits is more likely, or the NULL string if not received on an Annex G service.
interface <i>type number</i>	Interface to be used for the circuit, entered using standard Cisco IOS interface designations: Serial1/0:1, for example.
mac <i>address</i>	Connection-Mode Network Service (CMNS) service remote host MAC address entered as three hexadecimal numbers of four digits separated by a period, 0000.fc08.12ab, for example, or the NULL string if not received on a CMNS service.
packetsize <i>size</i>	X.25 maximum data packet sizes to request, entered as two numbers from the following choices: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096.
pid <i>byte-string</i>	PID string specified in ASCII or hexadecimal. A hexadecimal PID must be prefixed by “0x.” For example, 0x01000000 is the standard PAD PID. Although it is available for specifying a nonstandard Call PID, this parameter is not restricted to the common PID length and can be used to specify the entire user data field.
reversed <i>flag</i>	Flag to indicate whether a reverse charged Call is permitted. This flag applies to a switched virtual circuit (SVC) and is entered as a single character, Y or N, for yes or no.
source-addr <i>address</i>	Source X.121 address.
source-addr-ext <i>address</i>	NSAP source address extension.
window-size <i>size</i>	X.25 window sizes to request, entered as two numbers in a range from 1 to 127.
xot-dest-addr <i>address</i>	Destination IP address of an X.25 over TCP (XOT) service entered in standard IP address dotted decimal notation (10.0.0.127, for example) or the NULL string if not received on an XOT service.
xot-source-addr <i>address</i>	Source IP address of an XOT service entered in standard IP address dotted decimal notation (10.0.0.127, for example) or the NULL string if not received on an XOT service.

Table 47 **Skip Keywords for Incoming Telnet Connections**

Keyword	Description
dest-addr <i>address</i>	Destination IP address entered in standard IP address dotted decimal notation: 10.0.0.127, for example.
dest-port <i>port</i>	Destination port entered as a decimal number from one to five digits long.
source-addr <i>address</i>	Source IP address entered in standard IP address dotted decimal notation: 10.0.0.127, for example.

Examples

The following example shows how to write match and skip tests to skip connection attempts from any subnetwork address starting with 10 or 11 and match only those with a specific IP address and destination port number:

```
translate ruleset customer-case-1 from telnet to pad
! Ignore an incoming Telnet attempt from any subnetwork address starting with 10
skip source-addr ^10\.
! Match an incoming Telnet attempt destined for an IP addresses starting
! with 172.18., and a 5-digit port starting with 10 or 11
match dest-addr ^172\.18\.* dest-port ^1[0-1]...$
! Or match an incoming Telnet attempt destined an IP addresses starting
! with 172.18., and a 5-digit port starting with 120 through 127
match dest-addr ^172\.18\.* dest-port ^12[0-7]..$
```

The following example shows how to write match and skip tests to skip connection attempts from destination 55554 and to match only those with destination addresses from 55550 to 55553 and from 55556 to 55559:

```
translate ruleset A from pad to telnet
skip dest-addr ^55554$
match dest-addr ^5555.$
```

Related Commands

Command	Description
description (ruleset)	Adds a description about a translation ruleset.
match (ruleset)	Identifies a connection for processing by the translation ruleset.
options (ruleset)	Specifies protocol translation options in a translation ruleset.
set (ruleset)	Unconditionally sets one or more connection parameters to a fixed value for a translation ruleset.
show translate ruleset	Displays a summary of a specific or of all configured translation rulesets, behavioral parameters, and usage statistic.
substitute (ruleset)	Matches an available protocol and substitutes another in a translation ruleset.
test (ruleset)	Tests parameter values in a translation ruleset using regular expressions.
test translate	Displays a trace of protocol translation behavior for a connection attempt.
translate ruleset	Defines a unique name for a translation ruleset, specifies translated protocols, and enters translate ruleset configuration mode.
x25 pvc translate ruleset	Configures PVCs that are valid for protocol translation ruleset handling.

slip

To start a serial connection to a remote host by using Serial Line Internet Protocol (SLIP), use the **slip** command in EXEC mode.

slip [/default] {remote-ip-address | remote-name} [@tacacs-server] [/routing] [/compressed]

Syntax Description

/default	(Optional) Makes a SLIP connection when a default address has been configured.
<i>remote-ip-address</i>	IP address of the client workstation or PC.
<i>remote-name</i>	Name of the client workstation or PC.
<i>@tacacs-server</i>	(Optional) IP address or IP host name of the TACACS server to which your TACACS authentication request is sent.
/routing	(Optional) Indicates that the remote system is a router. Line must be configured for asynchronous routing using SLIP encapsulation.
/compressed	(Optional) Indicates that IP header compression should be negotiated.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced in a release prior to Cisco IOS Release 10.0.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you connect from a remote node computer to the EXEC facility on a router and want to connect from the router to a device on the network, issue the **slip** command.

If you specify an address for the TACACS server by using **/default** or *tacacs-server* arguments, the address must be the first parameter in the command after you enter **slip**. If you do not specify an address or enter **/default**, you are prompted for an IP address or host name. You can enter the **/default** keyword at this point.

If you do not use the *tacacs-server* argument to specify a TACACS server for SLIP address authentication, the TACACS server specified at login (if any) is used for the SLIP address query.

To optimize bandwidth on a line, SLIP enables compression of the SLIP packets using Van Jacobson TCP header compression as defined in RFC 1144.

Your system administrator must configure the system with the **ip tcp header-compression passive** command for the **/compressed** command option to be valid in EXEC mode. The **ip tcp header-compression** command forces header compression on or off. The default is to not compress the packets. The configuration file must have header compression on and the **slip /compressed** EXEC command must be entered for header compression to occur.

To terminate a session initiated with the **slip** command, disconnect from the device on the network using the command specific to that device. Then, exit from EXEC mode by using the **exit** command.

Examples

The following example makes a connection when a default IP address is assigned. Once a correct password is entered, you are placed in SLIP mode, and the IP address is displayed.

```
Router> slip
Password:
Entering SLIP mode.
Your IP address is 192.168.7.28, MTU is 1524 bytes
```

The following example illustrates the prompts displayed and the response required when you use dynamic addressing to assign the SLIP address:

```
Router> slip
IP address or hostname? 192.168.6.15
Password:
Entering SLIP mode
Your IP address is 192.168.6.15, MTU is 1524 bytes
```

In the preceding example, the address 172.31.6.15 has been assigned as the default. Password verification is still required before SLIP mode can be enabled.

```
Router> slip /default
Password:
Entering SLIP mode
Your IP address is 192.168.6.15, MTU is 1524 bytes
```

The following example illustrates the implementation of header compression on the interface with the IP address 172.24.2.1:

```
Router> slip 172.24.2.1 /compressed
Password:
Entering SLIP mode.
Interface IP address is 172.24.2.1, MTU is 1500 bytes.
Header compression will match your system.
```

In the preceding example, the interface is configured for the **ip tcp header-compression passive** command, which permits the user to enter the **/compressed** keyword at the EXEC mode prompt. The message “Header compression will match your system” indicates that the user specified compression. If the line was configured for the **ip tcp header-compression on** command, this line would read “Header compression is On.”

The following example specifies a TACACS server named server1 for address authentication:

```
Router> slip 10.0.0.1@server1
Password:
Entering SLIP mode.
Interface IP address is 10.0.0.1, MTU is 1500 bytes
Header compression will match your system.
```

Related Commands

Command	Description
ip tcp header-compression	Enables TCP header compression.

substitute (ruleset)

To match an available protocol and substitute another in a translation ruleset, use the **substitute** command in translate ruleset configuration mode. To change or remove the substitution statement, use one of the **no** forms of this command.

```
substitute [#line-number] {pad | telnet} variable-parameter reg-exp-match [#line-number {pad | telnet} variable-parameter reg-exp-match [...]] into {pad | telnet} variable-parameter [reg-exp-write]
```

```
no substitute {pad | telnet} variable-parameter reg-exp-match into {pad | telnet} variable-parameter [reg-exp-write]
```

```
no substitute #line-number [...]
```

Syntax Description		
<i>#line-number</i>	(Optional) The line in the translation ruleset to test for substitution. The # character must be entered.	
{ pad telnet }	Identifies the incoming or outgoing protocol and controls which parameters are available in the next element of this command.	
<i>variable-parameter</i>	A parameter that varies depending upon the protocol selected, either pad or telnet , and its role, either incoming or outgoing. Protocol parameters that modify the incoming or outgoing connection behavior during protocol translation session setup are indicated in Table 48 with an X.	
<i>reg-exp-match</i>	A standard Cisco regular expression match specification.	
into	Makes the substitution into an available protocol parameter.	
<i>reg-exp-write</i>	(Optional) A standard Cisco regular expression write specification that uses information from a match specification.	
[...]	(Optional) Specifies that multiple entries can be made as follows: - Up to six substitute statements can be written on one command line. - Multiple line numbers can be specified using the second no form of this command.	

Defaults No default behavior or values

Command Modes Translate ruleset configuration

Command History	Release	Modification
	12.3(8)T	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Up to six substitute specifications can be entered on one command line. The ellipses in the format shown above means multiple **substitute** statements can be specified in a translation ruleset statement.

When you use the first **no** form of this command, specify the full set of parameters and expressions in the command to be removed. The second **no** form must specify the correct **substitute** command and line number within the translation ruleset template.

This command is used to substitute between protocol parameters using regular expressions to match elements with a test string, and to substitute parameters into another string that can take elements from the matched string.

Cisco regular expressions are described in Appendix A, “Regular Expressions,” in the *Cisco IOS Terminal Services Configuration Guide*.

A substitute ... into statement will perform a regular expression match on any available protocol parameter and, if matched, substitute into any available protocol parameter. The regular expression write specification is optional. If the specification is omitted, the current value of the parameter will be taken as the regular expression write specification. This latter provision is a way of using multiple parameter values to set another parameter value. As an example, two successive substitute statements from a Telnet destination address and destination port into a packet assembler/disassembler (PAD) destination address could be specified using the following statements:

```
substitute telnet dest-addr ^10\.\0\.\0\.$ into pad dest-addr 111100\1\1
substitute telnet dest-addr ^10\.\0\.\0\.$ into pad dest-addr 111100\1\1
substitute telnet dest-port ^10(...)$ into pad dest-addr
```

If these successive substitutions were performed using an incoming Telnet connection from IP address 10.0.0.9/10234, the PAD destination address after the first substitution would be 111009\1, and after the second substitution would be 1111009234.

The following statements construct a switched virtual circuit (SVC) source address from the Telnet source information, starting with the source IP address in the form 172.18.###, which allows for a subsequent substitution of one field (notice the use of the backslash to concatenate the substitute and into statements):

```
substitute telnet source-addr ^172\.\18\.\.\.\.$ into pad source-addr 98\1\2\1
```

You can add in elements extracted from the Telnet destination port, where the rewrite pattern is taken from the current value of PAD source address, as follows:

```
substitute telnet dest-port ^(...). into pad source-addr
```

[Table 48](#) lists the PAD and Telnet parameters that can be set, as indicated by an X.

Table 48 *Substitute Connection Parameter Keywords*

Parameter	Description	Incoming PAD	Outgoing Telnet	Outgoing PAD	Incoming Telnet
authorize-method <i>ASCII-string</i>	Connection authorization method to use that must match one of a fixed set of values.	X	—	—	X
authorize-tag <i>ASCII-string</i>	Connection authorization identity to supply, entered as an ASCII string.	X	—	—	X

Table 48 *Substitute Connection Parameter Keywords (continued)*

Parameter	Description	Incoming PAD	Outgoing Telnet	Outgoing PAD	Incoming Telnet
binary <i>flag</i>	Flag that specifies whether 8-bit binary data is required, entered as one of the following characters to specify binary mode: Y , y , 1–9 , T , t .	—	X	—	X
cud <i>ASCII-string</i>	Call user data (CUD) that occurs after the protocol identification (PID). For X.29 service, this is the optional, user-specified text included in the command to place a call.	X	—	X	—
dest-addr <i>address</i>	Destination IP (Telnet) or X.121 (PAD) address.	X	X	X	X
dest-addr-ext <i>address</i>	Network service access point (NSAP) destination address extension.	X	—	X	—
dest-port <i>port</i>	Destination port entered as a decimal number from one to five digits long.	—	X	—	X
dldci <i>number</i>	Frame Relay data-link connection identifier (DLCI) of an Annex G service entered as a number from one to seven digits in length, although a size of two to four digits is more likely, or the NULL string if not received on an Annex G service.	X	—	X	—
eor <i>specification</i>	A character set defining the End-of-Record (EOR) string for the protocol translation session, entered as an ASCII or hexadecimal specification from one to four bytes in length, aaa or 0x19, as examples.	—	X	—	X
eor-insert <i>flag</i>	Flag specifying that the EOR character set should be inserted for PAD data being forwarded to a Telnet session, and entered as a single character. Use one of the following characters to specify EOR insertion: Y , y , 1–9 , T , t .	—	X	—	X
hostname <i>address</i>	Destination host name for Domain Name System (DNS) resolution entered as an ASCII string.	—	X	—	—

Table 48 **Substitute Connection Parameter Keywords (continued)**

Parameter	Description	Incoming PAD	Outgoing Telnet	Outgoing PAD	Incoming Telnet
idle <i>seconds</i>	Number of seconds the PAD connection can be idle before being cleared.	X	—	X	—
interface <i>type number</i>	Interface to be used for the circuit, entered using standard Cisco IOS interface designations; Serial1/0:1, for example.	X	—	X	—
keepalive-period <i>seconds</i>	A number that indicates the number of seconds between TCP keepalives for the X.25 over TCP (XOT) connection. TCP keepalive information applies only when a ruleset is configured to match an XOT destination address. Example: match dest-addr ^5555.\$ xot-dest-addr 5.5.5.2	X	—	X	—
keepalive-tries <i>number</i>	A number that indicates the number of TCP keepalives to send before the XOT connection is declared dead. TCP keepalive information applies only when a ruleset is configured to match an XOT destination address. Example: match dest-addr ^5555.\$ xot-dest-addr 5.5.5.2	X	—	X	—
local <i>flag</i>	Flag specifying that Telnet control sequences should be forwarded, not processed, and entered as a single character. Use one of the following characters to specify local mode: Y, y, 1–9, T, t .	—	X	—	X
mac <i>address</i>	Connection-Mode Network Service (CMNS) service remote host MAC address entered as three hexadecimal numbers of four digits separated by a period, (0000.fc08.12ab, for example) or the NULL string if not received on a CMNS service.	X	—	X	—
no-reset	Suppress a PVC Reset packet at session startup.	X	—	X	—

Table 48 **Substitute Connection Parameter Keywords (continued)**

Parameter	Description	Incoming PAD	Outgoing Telnet	Outgoing PAD	Incoming Telnet
packetsize <i>size</i>	X.25 maximum data packet sizes to request, entered as two numbers from the following choices: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096.	X	—	X	—
pid <i>byte-string</i>	PID string specified in ASCII or hexadecimal. A hexadecimal PID must be prefixed by "0x." For example, 0x01000000 is the standard PAD PID. Although it is available for specifying a nonstandard Call PID, this parameter is not restricted to the common PID length and can be used to specify the entire user data field.	X	—	X	—
printer <i>flag</i>	Printer access mode. Flag specifying that the outgoing connection should be brought up before the incoming connection is confirmed. Use one of the following characters to specify printer mode: Y , y , 1–9 , T , t . An unsuccessful outgoing connection attempt results in the incoming connection to the ruleset being refused, rather than being accepted and then closed, which is the default behavior. Note that using this keyword will force the ruleset quiet keyword to be applied to the translation.	X	—	—	X
profile <i>name</i>	Named PAD profile to use.	X	—	X	—
pvc <i>circuit-number</i>	Permanent virtual circuit (PVC) entered as a number from 1 to 4095, or the null string if not a PVC.	—	—	X	—
reverse	Request reverse charging.	—	—	X	—
reversed <i>flag</i>	Flag to indicate whether a reverse charged Call is permitted. This flag applies to a switched virtual circuit (SVC) and is entered as a single character, Y or N , for yes or no.	X	—	—	—

Table 48 **Substitute Connection Parameter Keywords (continued)**

Parameter	Description	Incoming PAD	Outgoing Telnet	Outgoing PAD	Incoming Telnet
rotor	Modifies the behavior of the host-name keyword by allowing one of the IP addresses defined by the ip host configuration command to be chosen randomly. If one address fails, another will be tried until a connection is made or all address choices are exhausted.	—	X	—	—
source-addr address	Source X.121 address.	X	—	X	X
source-addr-ext address	NSAP source address extension.	X	—	X	—
source-ifc type number	Interface from which to take the source IP address, entered using standard Cisco IOS interface designations: Loopback0, for example.	—	X	X	—
stream flag	Flag that specifies whether Telnet negotiation should be sent or accepted, entered as one of the following characters to specify stream mode: Y, y, 1–9, T, t .	—	X	—	X
swap flag	X.29 role reversal. Flag that indicates the PAD connection should not initiate X.29 commands when first connected. Use one of the following characters to swap behavior: Y, y, 1–9, T, t . This parameter enables incoming and outgoing PAD connections to be swapped so that a protocol translation is treated like a PAD when it accepts a call. By default, the protocol translation functions like a PAD for calls that it initiates, and like an X.25 host for calls it accepts.	X	—	X	—
use-map map	Use the map defined for PAD service.	—	—	X	—
window size size	X.25 window sizes to request, entered as two numbers in a range from 1 to 127.	X	—	X	—

Table 48 *Substitute Connection Parameter Keywords (continued)*

Parameter	Description	Incoming PAD	Outgoing Telnet	Outgoing PAD	Incoming Telnet
xot-dest-addr <i>address</i>	Destination IP address of an X.25 over TCP (XOT) service entered in standard IP address dotted decimal notation (10.0.0.127, for example) or the NULL string if not received on an XOT service.	X	—	X	—
xot-source-addr <i>address</i>	Source IP address of an XOT service entered in standard IP address dotted decimal notation (10.0.0.127, for example) or the NULL string if not received on an XOT service.	X	—	—	—

Examples

The following example shows how to build a translation ruleset template by starting with a match connection test, specifying protocol translation options, and setting specific parameters for incoming Telnet connections. The translation ruleset goes on to test and set appropriate parameters for incoming PAD connections, and to construct an SVC source address from Telnet information starting with the source IP address expressed using regular expression characters that allow for subsequent substitution in its last two fields. The translation ruleset is completed by adding in elements extracted from the Telnet destination port; the rewrite pattern is taken from the current value of PAD source address. Note use of the backslash character to construct the test ... set and substitute ... into statements.

```
translate ruleset customer-case-1 from telnet to pad
! Match an incoming Telnet attempt destined for IP addresses starting
! with 172.18., and a 5-digit port starting with the numbers 120 through 127.
match dest-addr ^172\.18\.* dest-port ^12[0-7]..$
! Once the correct network is matched, specify that this ruleset is limited
! to ten concurrent users and requires a login exchange.
options max-users 10 login
! Set Telnet options:
set telnet printer Y telnet binary Y
! Set PAD options:
set pad profile cust-profile-one
! Test conditional parameters and make appropriate settings:
test telnet dest-addr ^172\.18\.0\.* telnet dest-port ^10.00 \
  set pad pvc 1 telnet binary T
! Construct an SVC source address from the Telnet source information;
! start with the source IP address in the form 172.18.##.##, allowing
! for substitutions in the last two fields:
substitute telnet source-addr ^172\.18\.(.)\.(.)\
  into pad source-addr 98\1\2\1
! Now add in an extract from the Telnet destination port,
! where the rewrite pattern is taken from the current value of the PAD
! source address:
substitute telnet dest-port ^.(...). into pad source-addr
```

Related Commands

Command	Description
description (ruleset)	Adds a description about a translation ruleset.
match (ruleset)	Identifies a connection for processing by the translation ruleset.

Command	Description
options (ruleset)	Specifies protocol translation options in a translation ruleset.
set (ruleset)	Unconditionally sets one or more connection parameters to a fixed value for a translation ruleset.
show translate ruleset	Displays a summary of a specific or of all configured translation rulesets, behavioral parameters, and usage statistic.
skip (ruleset)	Identifies a connection for omission by the translation ruleset.
test (ruleset)	Tests parameter values in a translation ruleset using regular expressions.
test translate	Displays a trace of protocol translation behavior for a connection attempt.
translate ruleset	Defines a unique name for a translation ruleset, specifies translated protocols, and enters translate ruleset configuration mode.
x25 pvc translate ruleset	Configures PVCs that are valid for protocol translation ruleset handling.

telnet

To log in to a host that supports Telnet, use the **telnet** command in user EXEC or privileged EXEC mode.

telnet *host* [*port*] [*keyword*]

Syntax Description	<i>host</i>	A hostname or an IP address.
	<i>port</i>	(Optional) A decimal TCP port number, or port name; the default is the Telnet router port (decimal 23) on the host.
	<i>keyword</i>	(Optional) One of the keywords listed in Table 49 .

Command Modes	User EXEC
	Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(21)ST	The /ipv4 and /ipv6 keywords were added.
	12.1	The /quiet keyword was added.
	12.2(2)T	The /ipv4 and /ipv6 keywords were added.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	Table 49 lists the optional telnet command keywords.
------------------	---

Table 49 *telnet Keyword Options*

Option	Description
/debug	Enables Telnet debugging mode.
/encrypt kerberos	Enables an encrypted Telnet session. This keyword is available only if you have the Kerberized Telnet subsystem. If you authenticate using Kerberos Credentials, the use of this keyword initiates an encryption negotiation with the remote server. If the encryption negotiation fails, the Telnet connection will be reset. If the encryption negotiation is successful, the Telnet connection will be established, and the Telnet session will continue in encrypted mode (all Telnet traffic for the session will be encrypted).
/ipv4	Specifies version 4 of the IP protocol. If a version of the IP protocol is not specified in a network that supports both the IPv4 and IPv6 protocol stacks, IPv6 is attempted first and is followed by IPv4.
/ipv6	Specifies version 6 of the IP protocol. If a version of the IP protocol is not specified in a network that supports both the IPv4 and IPv6 protocol stacks, IPv6 is attempted first and is followed by IPv4.
/line	Enables Telnet line mode. In this mode, the Cisco IOS software sends no data to the host until you press the Enter key. You can edit the line using the standard Cisco IOS software command-editing characters. The /line keyword is a local switch; the remote router is not notified of the mode change.
/noecho	Disables local echo.
/quiet	Prevents onscreen display of all messages from the Cisco IOS software.
/route: path	Specifies loose source routing. The <i>path</i> argument is a list of hostnames or IP addresses that specify network nodes and ends with the final destination.
/source-interface	Specifies the source interface.
/stream	Turns on <i>stream</i> processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
<i>port-number</i>	Port number.
bgp	Border Gateway Protocol.
chargen	Character generator.
cmd rcmd	Remote commands.
daytime	Daytime.
discard	Discard.
domain	Domain Name Service.
echo	Echo.
exec	EXEC.
finger	Finger.
ftp	File Transfer Protocol.
ftp-data	FTP data connections (used infrequently).
gopher	Gopher.

Table 49 *telnet Keyword Options (continued)*

Option	Description
hostname	Hostname server.
ident	Ident Protocol.
irc	Internet Relay Chat.
klogin	Kerberos login.
kshell	Kerberos shell.
login	Login (rlogin).
lpd	Printer service.
nntp	Network News Transport Protocol.
pim-auto-rp	Protocol Independent Multicast (PIM) auto-rendezvous point (RP).
node	Connect to a specific Local-Area Transport (LAT) node.
pop2	Post Office Protocol v2.
pop3	Post Office Protocol v3.
port	Destination local-area transport (LAT) port name.
smtp	Simple Mail Transfer Protocol.
sunrpc	Sun Remote Procedure Call.
syslog	Syslog.
tacacs	Specifies TACACS security.
talk	Talk (517).
telnet	Telnet (23).
time	Time (37).
uucp	UNIX-to-UNIX Copy Program (540).
whois	Nickname (43).
www	World Wide Web (HTTP, 80).

With the Cisco IOS implementation of TCP/IP, you are not required to enter the **connect** or **telnet** command to establish a terminal connection. You can enter only the learned hostname—as long as the following conditions are met:

- The hostname is different from a command word for the router.
- The preferred transport protocol is set to **telnet**.

To display a list of the available hosts, use the **show hosts** command. To display the status of all TCP connections, use the **show tcp** command.

The Cisco IOS software assigns a logical name to each connection, and several commands use these names to identify connections. The logical name is the same as the hostname, unless that name is already in use, or you change the connection name with the **name-connection EXEC** command. If the name is already in use, the Cisco IOS software assigns a null name to the connection.

The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter the escape sequence and then a command character. The default escape sequence is Ctrl-^ (press

and hold the Ctrl and Shift keys and the 6 key). You can enter the command character as you hold down Ctrl or with Ctrl released; you can use either uppercase or lowercase letters. [Table 50](#) lists the special Telnet escape sequences.

Table 50 *Special Telnet Escape Sequences*

Escape Sequence ¹	Purpose
Ctrl-^ b	Break
Ctrl-^ c	Interrupt Process (IP and IPv6)
Ctrl-^ h	Erase Character (EC)
Ctrl-^ o	Abort Output (AO)
Ctrl-^ t	Are You There? (AYT)
Ctrl-^ u	Erase Line (EL)

1. The caret (^) symbol refers to Shift-6 on your keyboard.

At any time during an active Telnet session, you can list the Telnet commands by pressing the escape sequence keys followed by a question mark at the system prompt:

Ctrl-^ ?

A sample of this list follows. In this sample output, the first caret (^) symbol represents the Ctrl key, and the second caret represents Shift-6 on your keyboard:

```
router> ^^?
[Special telnet escape help]
^^B  sends telnet BREAK
^^C  sends telnet IP
^^H  sends telnet EC
^^O  sends telnet AO
^^T  sends telnet AYT
^^U  sends telnet EL
```

You can have several concurrent Telnet sessions open and switch among them. To open a subsequent session, first suspend the current connection by pressing the escape sequence (Ctrl-Shift-6 then x [Ctrl^x] by default) to return to the system command prompt. Then open a new connection with the **telnet** command.

To terminate an active Telnet session, enter any of the following commands at the prompt of the device to which you are connecting:

- **close**
- **disconnect**
- **exit**
- **logout**
- **quit**

Examples

The following example establishes an encrypted Telnet session from a router to a remote host named host1:

```
router> telnet host1 /encrypt kerberos
```

The following example routes packets from the source system *host1* to *example.com*, then to *10.1.0.11*, and finally back to *host1*:

```
router> telnet host1 /route:example.com 10.1.0.11 host1
```

The following example connects to a host with the logical name *host1*:

```
router> host1
```

The following example suppresses all onscreen messages from the Cisco IOS software during login and logout:

```
router> telnet host2 /quiet
```

The following example shows the limited messages displayed when connection is made using the optional **/quiet** keyword:

```
login:User2
Password:
      Welcome to OpenVMS VAX version V6.1 on node CRAW
      Last interactive login on Tuesday, 15-DEC-1998 11:01
      Last non-interactive login on Sunday,  3-JAN-1999 22:32

Server3)logout
      User2          logged out at  16-FEB-2000 09:38:27.85
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
kerberos clients mandatory	Causes the rsh , rcp , rlogin , and telnet commands to fail if they cannot negotiate the Kerberos Protocol with the remote server.
name connection	Assigns a logical name to a connection.
rlogin	Logs in to a UNIX host using rlogin.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.
show tcp	Displays the status of TCP connections.

telnet break-on-ip

To cause the system to generate a hardware BREAK signal on the EIA/TIA-232 line that is associated with a reverse Telnet connection when a Telnet Interrupt-Process command is received on that connection, use the **telnet break-on-ip** command in line configuration mode.

telnet break-on-ip

Syntax Description

This command has no arguments or keywords.

Defaults

No hardware BREAK signal is generated when an Interrupt-Process command is received.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command causes the system to generate a hardware BREAK signal on the EIA/TIA-232 line that is associated with a reverse Telnet connection. It is useful when a Telnet Interrupt-Process command is received on that connection because it can control the translation of Telnet Interrupt-Process commands into X.25 BREAK indications. It is also a useful workaround in the following situations:

- Several user Telnet programs send an Interrupt-Process command, but cannot send a Telnet BREAK signal.
- Some Telnet programs implement a BREAK signal that sends an Interrupt-Process command.
- Some EIA/TIA-232 hardware devices use a hardware BREAK signal for various purposes.

A hardware BREAK signal is generated when a Telnet BREAK command is received.

Examples

In the following example, line 5 is configured with the **telnet break-on-ip** command. The location text notes that this line is the location of the high-speed modem. The **telnet transparent** command sets end-of-line handling.

```
line 5
location high-speed modem
telnet transparent
telnet break-on-ip
```

Related Commands	Command	Description
	connect	Logs in to a host that supports Telnet, rlogin, or LAT.
	telnet	Logs in to a host that supports Telnet.
	telnet transparent	Configures the Cisco IOS software to send a CARRIAGE RETURN (CR) as a CR followed by a NULL instead of a CR followed by a LINE FEED (LF).
	terminal telnet break-on-ip	Causes the access server to generate a hardware Break signal on the EIA/TIA-232 line, which is associated with a reverse Telnet connection, for the current line and sessions.

telnet refuse-negotiations

To set a line using Telnet to refuse to negotiate full-duplex, remote echo requests on incoming connections, use the **telnet refuse-negotiations** command in line configuration mode. To disable this function, use the **no** form of this command.

telnet refuse-negotiations

no telnet refuse-negotiations

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Line configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Use this command on reverse Telnet connections to allow the Cisco IOS software to refuse full-duplex, remote echo option connection requests from the other end. This command suppresses negotiation of the Telnet Remote Echo and Suppress Go Ahead options.

This command does not apply to protocol translation configurations. It is intended for applications in which the router is functioning as a terminal server to allow terminal connections to remote devices through the asynchronous terminal ports of the router. Terminal server connections are those where the user types a command similar to the following to access network resources:

```
telnet access-server 2005
```

where access-server is the host name of the Cisco router functioning as a terminal server, and 2005 is the port number on the router to which the remote terminal is connected.

Examples The following example shows how to set line 5 to refuse full-duplex, remote echo requests:

```
line 5
telnet refuse-negotiations
```

Related Commands	Command	Description
	connect	Logs in to a host that supports Telnet, rlogin, or LAT.

Command	Description
telnet	Logs in to a host that supports Telnet.
terminal telnet refuse-negotiations	Sets the current line to refuse to negotiate full-duplex, remote echo options on incoming connections for current sessions.

telnet speed

To allow negotiation of the transmission speed of the line to a connected device, use the **telnet speed** command in line configuration mode. To disable this function, use the **no** form of this command.

telnet speed *default-speed* *maximum-speed*

no telnet speed

Syntax Description	<i>default-speed</i>	Line speed, in bits per second, that the Cisco IOS software will use if the device on the other end of the connection has not specified a speed.
	<i>maximum-speed</i>	Maximum speed, in bits per second, that the device on the port will use.

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	Line configuration
----------------------	--------------------

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	Negotiates speeds on reverse Telnet lines. You can match line speeds on remote systems in reverse Telnet, on host machines hooked up to a router used to access the network, or on a group of console lines hooked up to the router, when disparate line speeds are in use at the local and remote ends of the connection. Line speed negotiation adheres to the Remote Flow Control option defined in RFC 1080.
-------------------------	--

Examples	The following example allows a router to negotiate a bit rate on the line using the Telnet option. If no speed is negotiated, the line will run at 2400 bits per second (bps). If the remote host requests a speed of greater than 9600 bps, then 9600 will be used.
-----------------	--

```
line 5
 telnet speed 2400 9600
```

Related Commands	Command	Description
	connect	Logs in to a host that supports Telnet, rlogin, or LAT.
	telnet	Logs in to a host that supports Telnet.
	terminal telnet speed	Allows the access server to negotiate transmission speed for the current line and session.

telnet sync-on-break

To configure the Cisco IOS software to cause an incoming connection to send a Telnet Synchronize signal when it receives a Telnet BREAK signal, use the **telnet sync-on-break** command in line configuration mode. To disable this function, use the **no** form of this command.

telnet sync-on-break

no telnet sync-on-break

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Line configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines This command causes a reverse Telnet line to send a Telnet Synchronize signal when it receives a Telnet BREAK signal. This option is used very rarely to ensure the ordering of BREAK reception with respect to data characters sent after the BREAK.

Examples The following example configures the AUX line with the **telnet sync-on-break** command:

```
line aux 0
telnet sync-on-break
```

Related Commands	Command	Description
	connect	Logs in to a host that supports Telnet, rlogin, or LAT.
	telnet	Logs in to a host that supports Telnet.
	terminal telnet sync-on-break	Causes the access server to send a Telnet Synchronize signal when it receives a Telnet Break signal on the current line and session.

telnet transparent

To configure the Cisco IOS software to send a CARRIAGE RETURN (CR) as a CR followed by a NULL instead of a CR followed by a LINE FEED (LF), use the **telnet transparent** command in line configuration mode. To return to the default setting, use the **no** form of this command.

telnet transparent

no telnet transparent

Syntax Description

This command has no arguments or keywords.

Defaults

CARRIAGE RETURN followed by a LINE FEED.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is useful for coping with different interpretations of end-of-line handling in the Telnet protocol specification.

Examples

The following example causes the Cisco IOS software, when sending a CR, to send a CR followed by a NULL character:

```
line 7
 telnet transparent
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
telnet	Logs in to a host that supports Telnet.
terminal telnet transparent	Causes the current terminal line to send a Return character (CR) as a CR followed by a NULL instead of a CR followed by a LINE FEED (LF) for the current session.

terminal lat out-group

To temporarily define the list of services to which you or another user can connect, use the **terminal lat out-group** command in user EXEC mode.

terminal lat out-group *group-number* [*start-end*] {**disabled** | **enabled**}

Syntax Description

<i>group-number</i>	Number of the group that has access to the system through the specified line. This number is identified by the system administrator. You also can specify a range of group numbers. Separate the beginning and end of the range with a hyphen.
[<i>start-end</i>]	(Optional) You can specify a range of group numbers for the <i>group-number</i> argument. Separate the beginning and end of the range with a hyphen.
disabled	Incrementally removes specified groups from a list.
enabled	Incrementally adds specified groups to a list.

Command Modes

User EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To temporarily define the list of services to which you or another user can connect, you define the group code lists used for connections from specific lines. You limit the connection choices for an individual line by defining the group code lists for an outgoing connection. When a user initiates a connection with a local-area transport (LAT) host, the line must share a common group number with the remote LAT host before a connection can be made.

The group code range entered in this command must fall within the group code range already configured for the line.

Examples

The following example defines a group code list for the outgoing group 4:

```
Router> terminal lat out-group 4, 6-189
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
l2f ignore-mid-sequence	Specifies a connection to a particular LAT node that offers LAT services.

terminal lat remote-modification

To set a line running local-area transport (LAT) to be remotely modifiable, use the **terminal lat remote-modification** command in privileged EXEC mode.

terminal lat remote-modification

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples The following example sets line 6 to be remotely modifiable:

```
Router# terminal lat remote-modification 6
```

Related Commands	Command	Description
	connect	Logs in to a host that supports Telnet, rlogin, or LAT.
	l2f ignore-mid-sequence	Specifies a connection to a particular LAT node that offers LAT services.

terminal transport preferred

To specify the preferred protocol to use for the current session when a command does not specify one, use the **terminal transport preferred** command in EXEC mode.

terminal transport preferred {all | lat | mop | nasi | none | pad | rlogin | telnet | v120}

Syntax Description		
all		Specifies all recognized protocols.
lat		Specifies the local-area transport (LAT) protocol.
mop		Specifies the Maintenance Operation Protocol (MOP).
nasi		Specifies the NetWare Asynchronous Services Interface (NASI) protocol.
none		Prevents any protocol selection on the line. The router default is that any unrecognized command is a host name. If the preferred protocol is set to none, the router will not attempt any connections if the command is not recognized.
pad		Specifies X.3 packet assembler/disassembler (PAD), which is used most often to connect a server product to X.25 hosts.
rlogin		Specifies UNIX rlogin.
telnet		Specifies the TCP/IP Telnet protocol.
v120		Selects the V.120 protocol for incoming asynchronous connections over ISDN .

Defaults	lat (if LAT is not supported, telnet)
-----------------	--

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	10.0	This command first appeared in a release prior to Cisco IOS Release 10.0.
	11.2	The following keywords were added: • all • lat • mop • nasi • pad • preferred • rlogin • v120
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures the console so that it does not connect when an unrecognized command is entered:

```
Router# terminal transport preferred none
```

Related Commands

Command	Description
transport preferred	Specifies the transport protocol that the Cisco IOS software uses if the user does not specify one when initiating a connection.

test (ruleset)

To test parameter values in a translation ruleset using regular expressions, use the **test** command in translate ruleset configuration mode. To change or remove the specification, use one of the two **no** forms of this command.

```
test [#line-number] {pad | telnet} variable-parameter reg-exp-match [{pad | telnet}  
variable-parameter reg-exp-match [...]] set {pad | telnet} variable-parameter
```

```
no test {pad | telnet} variable-parameter reg-exp-match [{pad | telnet} variable-parameter  
reg-exp-match [...]] set {pad | telnet} variable-parameter
```

```
no test #line-number [...]
```

Syntax Description		
#line-number	(Optional) The line in the translation ruleset to test for substitution. The # character must be entered.	
{pad telnet}	Identifies the incoming or outgoing protocol and controls which parameters are available in the next element of this command.	
variable-parameter	A parameter that varies depending upon the protocol selected, either pad or telnet , and its role, either incoming or outgoing. Protocol parameters are available to modify the incoming or outgoing connection behavior during protocol translation session setup. Up to six parameters can be entered on one command line. Table 51 indicates supported incoming and outgoing PAD and Telnet connection parameter keywords for the test command with an X.	
reg-exp-match	A standard Cisco regular expression match specification.	
set	Conditionally sets the specified protocol parameters to a fixed value.	
[...]	(Optional) Specifies that multiple entries can be made as follows: - Up to six test statements can be written on one command line. - Multiple line numbers can be specified using the second no form of this command.	

Defaults No default behavior or values

Command Modes Translate ruleset configuration

Command History	Release	Modification
	12.3(8)T	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Up to six test statements can be entered on one command line. The ellipses in the format shown above means multiple test statements can be specified in a translation ruleset template.

The **test** command is useful for working with conditional parameters.

A test ... set ... statement conditionally sets one or more connection parameters to a given value, but only after a successful comparison of one or more connection parameters against a regular expression.

Cisco regular expressions are described in Appendix A, “Regular Expressions,” in the *Cisco IOS Terminal Services Configuration Guide*.

When you use the first **no** form of this command, specify the full set of parameters and expressions in the command to be removed. The second **no** form must specify the correct **test** command and line number within the translation ruleset template.

Table 51 Test Connection Parameter Keywords

Parameter	Description	Incoming PAD	Outgoing Telnet	Outgoing PAD	Incoming Telnet
authorize-method <i>ASCII-string</i>	Connection authorization method to use that must match one of a fixed set of values.	X	—	—	X
authorize-tag <i>ASCII-string</i>	Connection authorization identity to supply, entered as an ASCII string.	X	—	—	X
binary flag	Flag that specifies whether 8-bit binary data is required, entered as one of the following characters to specify binary mode: Y, y, 1–9, T, t .	—	X	—	X
cud <i>ASCII-string</i>	Call user data (CUD) that occurs after the protocol identification (PID). For X.29 service, this is the optional, user-specified text included in the command to place a call.	X	—	X	—
dest-addr <i>address</i>	Destination IP (Telnet) or X.121 (PAD) address.	X	X	X	X
dest-addr-ext <i>address</i>	Network service access point (NSAP) destination address extension.	X	—	X	—
dest-port <i>port</i>	Destination port entered as a decimal number from one to five digits long.	—	—	—	X
dldci <i>number</i>	Frame Relay data-link connection identifier (DLCI) of an Annex G service entered as a number from one to seven digits in length, although a size of two to four digits is more likely, or the NULL string if not received on an Annex G service.	X	—	X	—

Table 51 **Test Connection Parameter Keywords (continued)**

Parameter	Description	Incoming PAD	Outgoing Telnet	Outgoing PAD	Incoming Telnet
eor <i>specification</i>	A character set defining the End-of-Record (EOR) string for the protocol translation session, entered as an ASCII or hexadecimal specification from one to four bytes in length, aaa or 0x19, as examples.	—	X	—	X
eor-insert <i>flag</i>	Flag specifying that the EOR character set should be inserted for PAD data being forwarded to a Telnet session, and entered as a single character. Use one of the following characters to specify EOR insertion: Y , y , 1–9 , T , t .	—	X	—	X
hostname <i>address</i>	Destination host name for Domain Name System (DNS) resolution entered as an ASCII string.	—	X	—	—
idle <i>seconds</i>	Number of seconds the PAD connection can be idle before being cleared.	X	—	X	—
interface <i>type</i> <i>number</i>	Interface to be used for the circuit, entered using standard Cisco IOS interface designations; Serial1/0:1, for example.	X	—	X	—
keepalive-period <i>seconds</i>	A number that indicates the number of seconds between TCP keepalives for the X.25 over TCP (XOT) connection. TCP keepalive information applies only when a ruleset is configured to match an XOT destination address. Example: match dest-addr ^5555.\$ xot-dest-addr 5.5.5.2	X	—	X	—
keepalive-tries <i>number</i>	A number that indicates the number of TCP keepalives to send before the XOT connection is declared dead. TCP keepalive information applies only when a ruleset is configured to match an XOT destination address. Example: match dest-addr ^5555.\$ xot-dest-addr 5.5.5.2	X	—	X	—

Table 51 **Test Connection Parameter Keywords (continued)**

Parameter	Description	Incoming PAD	Outgoing Telnet	Outgoing PAD	Incoming Telnet
local <i>flag</i>	Flag specifying that Telnet control sequences should be forwarded, not processed, and entered as a single character. Use one of the following characters to specify local mode: Y , y , 1–9 , T , t .	—	X	—	X
mac <i>address</i>	Connection-Mode Network Service (CMNS) service remote host MAC address entered as three hexadecimal numbers of four digits separated by a period, (0000.fc08.12ab, for example) or the NULL string if not received on a CMNS service.	X	—	X	—
no-reset	Suppress a PVC Reset packet at session startup.	X	—	X	—
packetsize <i>size</i>	X.25 maximum data packet sizes to request, entered as two numbers from the following choices: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096.	X	—	X	—
pid <i>byte-string</i>	PID string specified in ASCII or hexadecimal. A hexadecimal PID must be prefixed by "0x." For example, 0x01000000 is the standard PAD PID. Although it is available for specifying a nonstandard Call PID, this parameter is not restricted to the common PID length and can be used to specify the entire user data field.	X	—	X	—

Table 51 **Test Connection Parameter Keywords (continued)**

Parameter	Description	Incoming PAD	Outgoing Telnet	Outgoing PAD	Incoming Telnet
printer flag	Printer access mode. Flag specifying that the outgoing connection should be brought up before the incoming connection is confirmed. Use one of the following characters to specify printer mode: Y , y , 1–9 , T , t . An unsuccessful outgoing connection attempt results in the incoming connection to the ruleset being refused, rather than being accepted and then closed, which is the default behavior. Note that using this keyword will force the ruleset quiet keyword to be applied to the translation.	X	—	—	X
profile name	Named PAD profile to use.	X	—	X	—
pvc circuit-number	Permanent virtual circuit (PVC) entered as a number from 1 to 4095, or the null string if not a PVC.	—	—	X	—
reverse	Request reverse charging.	—	—	X	—
reversed flag	Flag to indicate whether a reverse charged Call is permitted. This flag applies to a switched virtual circuit (SVC) and is entered as a single character, Y or N , for yes or no.	X	—	—	—
rotor	Modifies the behavior of the host-name keyword by allowing one of the IP addresses defined by the ip host configuration command to be chosen randomly. If one address fails, another will be tried until a connection is made or all address choices are exhausted.	—	X	—	—
source-addr address	Source X.121 address.	X	—	X	X
source-addr-ext address	NSAP source address extension.	X	—	X	—
source-ifc type number	Interface from which to take the source IP address, entered using standard Cisco IOS interface designations: Loopback0, for example.	—	X	X	—

Table 51 Test Connection Parameter Keywords (continued)

Parameter	Description	Incoming PAD	Outgoing Telnet	Outgoing PAD	Incoming Telnet
stream <i>flag</i>	Flag that specifies whether Telnet negotiation should be sent or accepted, entered as one of the following characters to specify stream mode: Y , y , 1–9 , T , t .	—	X	—	X
swap <i>flag</i>	X.29 role reversal. Flag that indicates the PAD connection should not initiate X.29 commands when first connected. Use one of the following characters to swap behavior: Y , y , 1–9 , T , t . This parameter enables incoming and outgoing PAD connections to be swapped so that a protocol translation is treated like a PAD when it accepts a call. By default, the protocol translation functions like a PAD for calls that it initiates, and like an X.25 host for calls it accepts.	X	—	X	—
use-map <i>map</i>	Use the map defined for PAD service.	—	—	X	—
window size <i>size</i>	X.25 window sizes to request, entered as two numbers in a range from 1 to 127.	X	—	X	—
xot-dest-addr <i>address</i>	Destination IP address of an X.25 over TCP (XOT) service entered in standard IP address dotted decimal notation (10.0.0.127, for example) or the NULL string if not received on an XOT service.	X	—	X	—
xot-source-addr <i>address</i>	Source IP address of an XOT service entered in standard IP address dotted decimal notation (10.0.0.127, for example) or the NULL string if not received on an XOT service.	X	—	—	—

Examples

The following example shows how to integrate a test into a translation ruleset template. The translation ruleset begins with the required match connection test, specifies protocol translation options, and sets specific parameters for incoming Telnet connections. The translation ruleset goes on to test and set appropriate parameters for incoming PAD connections, and to construct an SVC source address from Telnet information, starting with the source IP address. The translation ruleset is completed by adding

in elements extracted from the Telnet destination port; the rewrite pattern is taken from the current value of PAD source address. The backslash character is used to construct the test ... set and substitute ... into statements.

```
translate ruleset customer-case-1 from telnet to pad
! Match an incoming Telnet attempt destined for IP addresses starting
! with 172.18., and a 5-digit port starting with the numbers 120 through 127.
match dest-addr ^172\18\.* dest-port ^12[0-7]..$
! Once the correct network is matched, specify that this ruleset is limited
! to ten concurrent users and requires a login exchange.
options max-users 10 login
! Set Telnet options:
set telnet printer Y telnet binary Y
! Set PAD options:
set pad profile cust-profile-one
! Test conditional parameters and make appropriate settings:
test telnet dest-addr ^172\18\.0\.* telnet dest-port ^10.00 \
  set pad pvc 1 telnet binary T
! Construct an SVC source address from the Telnet source information;
! start with the source IP address in the form 172.18.###, allowing
! for a following substitute of one field:
substitute telnet source-addr ^172\18\.(.)\.(.)\
  into pad source-addr 98\1\2\1
! Now add in an extract from the Telnet destination port,
! where the rewrite pattern is taken from the current value of the PAD
! source address:
substitute telnet dest-port ^.(...). into pad source-addr
```

Related Commands

Command	Description
description (ruleset)	Adds a description about a translation ruleset.
match (ruleset)	Identifies a connection for processing by the translation ruleset.
options (ruleset)	Specifies protocol translation options in a translation ruleset.
set (ruleset)	Unconditionally sets one or more connection parameters to a fixed value for a translation ruleset.
show translate ruleset	Displays a summary of a specific or of all configured translation rulesets, behavioral parameters, and usage statistic.
skip (ruleset)	Identifies a connection for omission by the translation ruleset.
substitute (ruleset)	Matches an available protocol and substitutes another in a translation ruleset.
test translate	Displays a trace of protocol translation behavior for a connection attempt.
translate ruleset	Defines a unique name for a translation ruleset, specifies translated protocols, and enters translate ruleset configuration mode.
x25 pvc translate ruleset	Configures PVCs that are valid for protocol translation ruleset handling.

test translate

To display a trace of protocol translation behavior for a connection attempt, use the **test translate** command in user or privileged EXEC mode.

test translate {**pad** | **telnet** | **parameter** *parameter*} [**detail**]

Syntax Description

pad	Tests a trace of a packet assembler/disassembler (PAD) connection attempt.
telnet	Tests a trace of a Telnet connection attempt.
parameter <i>parameter</i>	Tests one of the following translation ruleset parameters in interactive mode: • boolean—Boolean expression parameter. True if at least one character is present and the first character is one of Y, y, 1–9, T, or t; otherwise, false. • hexstring—Hex string parameter. A standard hexadecimal string representation starting with 0x, such as 0x14000F0000. • integer—Integer parameter. A standard decimal number from 0 to 65535. • interface—Two-integer parameter. A character string, possibly with embedded white space, identifying an existing interface, such as Serial 1, on the router. • ip—IP address parameter. A standard four-byte dotted decimal IP address such as 10.0.0.127. • mac—MAC address parameter. A standard set of three 4-digit hexadecimal words in dotted MAC address form such as 0001.00a8.1f2c. • nsap—Network service access point (NSAP) address parameter. • string—String parameter. A null-terminated ASCII string. • two-integer—Two-integer parameter. • x121—X.121 address parameter. A standard X.121 address from 1 to 15 decimal digits long.
detail	(Optional) Provides a more detailed test report.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command will traverse the set of protocol translation configurations in the order they are listed in the translation ruleset, and report all events that take place. The **detail** keyword shows each line being evaluated and detailed translation test information.

The translation ruleset operations to test, set, and substitute protocol parameter values use strings, and the ruleset generates the set of protocol parameter values as a set of strings. When entered with the optional **parameter** keyword and parameter type, the **test translate** command becomes interactive and queries for incoming connection parameter values. For a given protocol parameter there may be additional validation tests that apply. If the application of a translation ruleset results in an invalid value for a parameter (whether a violation of the basic type rule or the more specific validation tests for the parameter), the protocol translation operation will fail with an informative message.

Configuration errors are not detected when translation ruleset commands are entered. They are tested when the connection is attempted or when you use the **test (ruleset)** command. In the following example, the **set** translation ruleset command unconditionally sets the PAD's profile name to a profile that does not exist in the configuration:

```
set pad profile Bldg-1-5ess
```

This command would be accepted at the command-line interpreter, but not tested until a connection attempt or with the **test translate EXEC** command. When the error is detected, the following messages display:

```
*%PT-3-PARAMRESULTERR: PT ruleset test protocol pad parameter profile parse error:
Bldg-1-5ess.
-Process= "PAD InCall", ipl= 3, pid= 94
*PAD: ruleset translation not generated Cause: 9 Diag: 0
```

Examples

The following example shows a sample of the self-explanatory report from the **test translate** command:

```
Router# test translate pad

dest-addr (X.121 address): 55555
Ruleset A match/skip line 1 compared: match
Ruleset A; pad parameter read:
  pad/dest-addr: 55555
Parameters set:
  telnet/dest-addr: 10.2.2.1

Translate From: PAD 55555
To:   Telnet 10.2.2.1 Port 23
Ruleset A
0/1 users active
```

The following is a sample of a detailed report:

```
Router# test translate pad detail

PAD translate command 1 PVC match not required
```

```

dest-addr (X.121 address): 55555
Normalized PAD dest-addr: 55555
PAD translate command 1 skipped, destination address 55555 doesn't match 12345
PAD translate command 2 PVC match not required
PAD translate command 2 skipped, destination address 55555 doesn't match 55551
No PAD translate command matched
(Testing translate command A ...)
Ruleset A match/skip line 1 compared: match
  (processing set/test/substitute line 1)
  (set/test/subst line 1, item 1, parameter dest-addr set to 10.2.2.1)
  (parsed telnet parameter dest-addr: 10.2.2.1)
Ruleset A; pad parameter read:
  pad/dest-addr: 55555
Parameters set:
  telnet/dest-addr: 10.2.2.1
  (translation requires 0 bytes variable-sized memory)

Translate From: PAD 55555
To: Telnet 10.2.2.1 Port 23
Ruleset A
0/1 users active

```

The following example tests the **boolean** translate ruleset parameter in interactive mode:

```

Router# test translate parameter boolean

Enter parameter value (boolean): Y

Enter encode buffer size (integer): 10
Encoded into Y
Router#

```

Related Commands

Command	Description
description (ruleset)	Adds a description about a translation ruleset.
match (ruleset)	Identifies a connection for processing by the translation ruleset.
options (ruleset)	Specifies protocol translation options in a translation ruleset.
set (ruleset)	Unconditionally sets one or more connection parameters to a fixed value for a translation ruleset.
show translate ruleset	Displays a summary of a specific or of all configured translation rulesets, behavioral parameters, and usage statistic.
skip (ruleset)	Identifies a connection for omission by the translation ruleset.
substitute (ruleset)	Matches an available protocol and substitutes another in a translation ruleset.
test (ruleset)	Tests parameter values in a translation ruleset using regular expressions.
translate ruleset	Defines a unique name for a translation ruleset, specifies translated protocols, and enters translate ruleset configuration mode.
x25 pvc translate ruleset	Configures PVCs that are valid for protocol translation ruleset handling.

time-out

To specify the Secure Shell (SSH) login timeout interval in seconds for a persistent SSH connection, use the **time-out** command in transport map configuration mode command. To restore the default setting of 120 seconds, use the **no** form of the command.

time-out *timeout-interval*

no time-out

Syntax Description	<i>timeout-interval</i> Specifies the SSH login timeout interval in seconds.
--------------------	--

Command Default	The default <i>timeout-interval</i> is 120 seconds.
-----------------	---

Command Modes	Transport map configuration (config-tmap)
---------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines	This command is used to specify the SSH timeout interval.
------------------	---

Examples	In the following example, a transport map is configured that applies the following settings to any users attempting to access the Management Ethernet port via SSH: • Users using SSH waits for the IOS process to become active, but enters diagnostic mode if the attempt to access IOS is interrupted. • The RSA keypair name is “sshkeys”. • The connection allows one authentication retry. • The banner “--Welcome to Diagnostic Mode--” appears if diagnostic mode is entered as a result of SSH handling through this transport map. • The banner “--Waiting for IOS Process--” appears if the connection is waiting for the IOS process to be come active.
----------	--

The transport map is then applied to the interface when the **transport type persistent ssh input** command is entered to enable persistent SSH.

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# authentication-retries 1
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
```

```

Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for IOS Process--
X
Router(config-tmap)# time-out 30
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit

Router(config)# transport type persistent ssh input sshhandler

```

Related Commands

Command	Description
authentication-retries	Specifies the number of SSH authentication retries before dropping the connection when a persistent SSH transport map is applied to the receiving interface.
banner (transport map)	Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of the transport map configuration.
connection wait	Specifies how an incoming connection will be handled.
rsa keypair-name	Names the RSA keypair to be used for persistent SSH connections.
transport interface	Applies the transport map settings to the interface.
transport type persistent	Applies an already-configured persistent transport map to an interface.
transport-map type persistent	Creates and names a persistent transport map and enters transport map configuration mode.

tn3270

To begin a TN3270 session, use the **tn3270** command in EXEC mode.

tn3270 *host*

Syntax Description	<i>host</i>	Name or IP address of a specific host on a network that can be reached by the router. The default terminal emulation mode allows access using a VT100 emulation.
---------------------------	-------------	--

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	11.1	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	Unlike Telnet and local-area transport (LAT) connections, you <i>must</i> enter the tn3270 command to make a connection to an IBM TN3278 host. To terminate an active TN3270 session, enter the escape sequence (Ctrl-Shift-6 then x [Ctrl^x] by default) and enter the disconnect command at the EXEC prompt. Or log off the remote system by issuing the command specific to that system (such as exit, logout, quit, close, or disconnect).
-------------------------	--

Examples	The following example establishes a terminal session with an IBM TN3270 host named finance: <pre>tn3270 finance</pre>
-----------------	--

tn3270 8bit display

To configure the Cisco IOS software to use the mask set by the **data-character-bits {7 | 8}** command in line configuration mode or the **terminal data-character bits {7 | 8}** EXEC command, use the **tn3270 8bit display** command in line configuration mode. To restore the default 7-bit mask used for TN3270 connections, use the **no** form of this command.

tn3270 8bit display

no tn3270 8bit display

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Line configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Use the **tn3270-character-map** command to map between extended EBCDIC or extended ASCII characters.

Examples The following example configures the Cisco IOS software to use the mask set by the **data-character-bits** line configuration and EXEC commands on line 5:

```
line 5
tn3270 8bit display
```

Related Commands	Command	Description
	data-character-bits	Sets the number of data bits per character that are interpreted and generated by the Cisco IOS software.
	terminal data-character-bits	Sets the number of data bits per character that are interpreted and generated by the Cisco IOS software for the current line and session.

tn3270 8bit transparent-mode

To configure the Cisco IOS software to use the mask set by the **data-character-bits {7 | 8}** command in line configuration mode or the **terminal data-character bits {7 | 8}** EXEC command, use the **tn3270 8bit transparent-mode** command in line configuration mode. To restore the default 7-bit mask used for TN3270 connections, use the **no** form of this command.

tn3270 8bit transparent-mode

no tn3270 8bit transparent-mode

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	Disabled
-----------------	----------

Command Modes	Line configuration
----------------------	--------------------

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	This command is needed if you are using a file transfer protocol such as Kermit in 8-bit mode or you are using 8-bit graphics, both of which rely on transparent mode.
-------------------------	--

Examples	The following example configures the software to use the mask set by the data-character-bits line configuration and EXEC commands on line 5:
-----------------	---

```
line 5
tn3270 8bit transparent-mode
```

Related Commands	Command	Description
	data-character-bits	Sets the number of data bits per character that are interpreted and generated by the Cisco IOS software.
	terminal data-character-bits	Sets the number of data bits per character that are interpreted and generated by the Cisco IOS software for the current line and session.

tn3270 character-map

To convert incoming EBCDIC characters into ASCII characters, use the **tn3270 character-map** command in global configuration mode. To restore default character mappings, use the **no** form of this command.

tn3270 character-map *ebcdic-in-hex* *ascii-in-hex*

no tn3270 character-map {**all** | *ebcdic-in-hex*} [*ascii-in-hex*]

Syntax Description

<i>ebcdic-in-hex</i>	Hexadecimal value of an EBCDIC character.
<i>ascii-in-hex</i>	Hexadecimal value of an ASCII character.
all	Indicates all character mappings.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to print international characters that are EBCDIC characters not normally printed, including umlauts (¨) and tildes (~). The command first restores default mapping for both EBCDIC and ASCII characters. In the **no** form of the command, the **all** keyword resets all character mappings to Cisco defaults.

[Table 52](#) shows the default character mappings between ASCII and EBCDIC in decimal and hexadecimal format.

To convert outgoing ASCII characters into EBCDIC characters, use the **keymap** command to modify the keymap structure with the tag *ebcdic_xx=string*, where *xx* is a hexadecimal value and *string* is the sequence of characters that send the EBCDIC character.

Table 52 Default ASCII, EBCDIC Character Mappings

Character	ASCII Decimal	ASCII Hexadecimal	EBCDIC Decimal	EBCDIC Hexadecimal
!	33	0x21	90	0x5a
"	34	0x22	127	0x7f
#	35	0x23	123	0x7b
\$	36	0x24	91	0x5b

Table 52 *Default ASCII, EBCDIC Character Mappings (continued)*

Character	ASCII Decimal	ASCII Hexadecimal	EBCDIC Decimal	EBCDIC Hexadecimal
%	37	0x25	108	0x6c
&	38	0x26	80	0x50
'	39	0x27	125	0x7d
(	40	0x28	77	0x4d
)	41	0x29	93	0x5d
*	42	0x2a	92	0x5c
+	43	0x2b	78	0x4e
,	44	0x2c	107	0x6b
-	45	0x2d	96	0x60
.	46	0x2e	75	0x4b
/	47	0x2f	97	0x61
0	48	0x30	240	0xf0
1	49	0x31	241	0xf1
2	50	0x32	242	0xf2
3	51	0x33	243	0xf3
4	52	0x34	244	0xf4
5	53	0x35	245	0xf5
6	54	0x36	246	0xf6
7	55	0x37	247	0xf7
8	56	0x38	248	0xf8
9	57	0x39	249	0xf9
:	58	0x3a	122	0x7a
;	59	0x3b	94	0x5e
<	60	0x3c	76	0x4c
=	61	0x3d	126	0x7e
>	62	0x3e	110	0x6e
?	63	0x3f	111	0x6f
@	64	0x40	124	0x7c
A	65	0x41	193	0xc1
B	66	0x42	194	0xc2
C	67	0x43	195	0xc3
D	68	0x44	196	0xc4
E	69	0x45	197	0xc5
F	70	0x46	198	0xc6
G	71	0x47	199	0xc7
H	72	0x48	200	0xc8

Table 52 *Default ASCII, EBCDIC Character Mappings (continued)*

Character	ASCII Decimal	ASCII Hexadecimal	EBCDIC Decimal	EBCDIC Hexadecimal
I	73	0x49	201	0xc9
J	74	0x4a	209	0xd1
K	75	0x4b	210	0xd2
L	76	0x4c	211	0xd3
M	77	0x4d	212	0xd4
N	78	0x4e	213	0xd5
O	79	0x4f	214	0xd6
P	80	0x50	215	0xd7
Q	81	0x51	216	0xd8
R	82	0x52	217	0xd9
S	83	0x53	226	0xe2
T	84	0x54	227	0xe3
U	85	0x55	228	0xe4
V	86	0x56	229	0xe5
W	87	0x57	230	0xe6
X	88	0x58	231	0xe7
Y	89	0x59	232	0xe8
Z	90	0x5a	233	0xe9
[	91	0x5b	173	0xad
\	92	0x5c	224	0xe0
]	93	0x5d	189	0xbd
^	94	0x5e	95	0x5f
_	95	0x5f	109	0x6d
`	96	0x60	121	0x79
a	97	0x61	129	0x81
b	98	0x62	130	0x82
c	99	0x63	131	0x83
d	100	0x64	132	0x84
e	101	0x65	133	0x85
f	102	0x66	134	0x86
g	103	0x67	135	0x87
h	104	0x68	136	0x88
i	105	0x69	137	0x89
j	106	0x6a	145	0x91
k	107	0x6b	146	0x92
l	108	0x6c	147	0x93

Table 52 *Default ASCII, EBCDIC Character Mappings (continued)*

Character	ASCII Decimal	ASCII Hexadecimal	EBCDIC Decimal	EBCDIC Hexadecimal
m	109	0x6d	148	0x94
n	110	0x6e	149	0x95
o	111	0x6f	150	0x96
p	112	0x70	151	0x97
q	113	0x71	152	0x98
r	114	0x72	153	0x99
s	115	0x73	162	0xa2
t	116	0x74	163	0xa3
u	117	0x75	164	0xa4
v	118	0x76	165	0xa5
w	119	0x77	166	0xa6
x	120	0x78	167	0xa7
y	121	0x79	168	0xa8
z	122	0x7a	169	0xa9
{	123	0x7b	192	0xc0
	124	0x7c	79	0x4f
}	125	0x7d	208	0xd0
~	126	0x7e	161	0xa1

Examples

The following example creates a two-way binding between an EBCDIC character and an ASCII character:

```
tn3270 character-map 0x81 0x78
```

Related Commands

Command	Description
show tn3270 ascii-hexval	Displays ASCII-hexadecimal character mappings.
show tn3270 character-map	Displays character mappings between ASCII and EBCDIC.

tn3270 datastream

To enable the TN3270 extended datastream, use the **tn3270 datastream** command in global configuration mode. To return to the normal TN3270 datastream, use the **no** form of this command.

tn3270 datastream {extended | normal}

no tn3270 datastream

Syntax Description

extended	Extended datastream.
normal	Normal datastream.

Defaults

Normal datastream

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command causes an “-E” to be appended to the terminal type string sent to the IBM host, which allows you to use the extended TN3270 features.

Examples

The following example shows the supported TN3270 datastream options:

```
tn3270 datastream ?
  extended  Use extended TN3270 datastream
  normal    Use normal TN3270 datastream
```

tn3270 null-processing

To specify how NULL signals are handled, use the **tn3270 null-processing** command in global configuration mode. To return to 7171 NULL processing, use the **no** form of this command.

tn3270 null-processing [3270 | 7171]

no tn3270 null-processing [3270 | 7171]

Syntax Description	3270	(Optional) NULLs are compressed out of the string, as on a 3278-x terminal.
	7171	(Optional) NULLs are converted to spaces, as on a 7171 controller.

Defaults	7171 NULL processing
----------	----------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	10.3	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	If a user enters data, uses an arrow key to move the cursor to the right on the screen, and then enters more data, the intervening spaces are filled with NULLs. To specify how NULLs are handled, enter the tn3270 null-processing command either with the 3270 argument, where NULLs are compressed out of the string (as on a real 3278-x terminal) or the 7171 argument, where NULLs are converted to spaces as on a 7171 controller. Enter this command in global configuration.
------------------	--

Examples	The following example shows the two available null processing methods:
----------	--

```
tn3270 null-processing ?  
 3270 Use 3270-style null processing  
 7171 Use 7171-style null processing
```

tn3270 optimize-cursor-move

To increase performance between a remote user and a TN3270 host by limiting cursor movement information that is sent to user terminals, use the **tn3270 optimize-cursor-move** command in global configuration mode. To ensure that all cursor movement information is sent between the terminal and the TN3270 host, use the **no** form of this command.

tn3270 optimize-cursor-move

no tn3270 optimize-cursor-move

Syntax Description

This command has no arguments or keywords.

Defaults

Cursor movement escape strings are sent to the terminal.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Issuing this command increases the speed of information transfer between users and TN3270 hosts through an access server.

If you do not issue this command, virtually every byte of information between the terminal and the TN3270 host is prepended and trailed by cursor-movement strings.

Examples

The following example disables status messages to users connected to 3278 terminals:

```
tn3270 optimize-cursor-move
```

Related Commands

Command	Description
tn3270 status-message	Reenables the display of status messages after they have been disabled.

tn3270 reset-required

To lock a terminal after input error until the user resets the terminal, use the **tn3270 reset-required** command in global configuration mode. To return to the default of no reset required, use the **no** form of this command.

tn3270 reset-required

no tn3270 reset-required

Syntax Description This command has no arguments or keywords.

Defaults No reset is required.

Command Modes Global configuration

Command History	Release	Modification
	10.3	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines On a 3278-x terminal, the keyboard is locked and further input is not permitted after input error (due to field overflow, invalid entry, and so on) until the user presses the RESET key. Most TN3270 implementations leave the keyboard unlocked and remove any error message on the next key input after the error. Use this command to lock the keyboard until the user performs a reset.

Examples The following example enables keyboard locking after an input error:

```
tn3270 reset-required
```

tn3270 status-message

To reenable the display of status messages after they have been disabled, use the **tn3270 status-message** command in global configuration mode. To save bandwidth on asynchronous lines by not displaying status messages, use the **no** form of this command.

tn3270 status-message

no tn3270 status-message

Syntax Description This command has no arguments or keywords.

Defaults Status messages appear.

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Status messages appear on the console by default. These messages include “System Locked,” “Field error,” and “System UnLocked” messages. These messages are sent back to the terminal via the TTY line on the access server.

Disabling status messages saves bandwidth on asynchronous lines, which have very low bandwidth.

Examples The following example disables status messages to users connected to 3270 terminals:

```
no tn3270 status-message
```

Related Commands	Command	Description
	tn3270 optimize-cursor-move	Increases performance between a remote user and a TN3270 host by limiting cursor movement information that is sent to user terminals.

tn3270 typeahead

To buffer keyboard data when a 3278 server is in locked mode, use the **tn3270 typeahead** command in global configuration mode. To disable the typeahead function, use the **no** form of this command.

tn3270 typeahead

no tn3270 typeahead

Syntax Description This command has no arguments or keywords.

Defaults Typeahead is disabled.

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines When typeahead is enabled, the TN3270 client implementation in the Cisco IOS software permits you to continue typing while the system is trying to obtain a response from the TN3270 server. Information you type while a “System Locked” message appears on the terminal is stored in a buffer. After the “System Locked” message disappears, the information is then used as though it were just typed.

Examples The following example saves user information when “System Locked” messages appear on the screen:

```
tn3270 typeahead
```

Related Commands	Command	Description
	tn3270 reset-required	Locks a terminal after input error until the user resets the terminal.

translate lat

To translate a connection request to another protocol connection type when receiving a local-area transport (LAT) request, use the **translate lat** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

translate lat *incoming-service-name* [*incoming-options*] *protocol* *outgoing-address*
[*outgoing-options*] [*global-options*]

no translate lat *incoming-service-name* [*incoming-options*] *protocol* *outgoing-address*
[*outgoing-options*] [*global-options*]

Syntax Description

<i>incoming-service-name</i>	A LAT service name. When used on the incoming portion of the command, <i>incoming-service-name</i> is the name of the service that users specify when trying to make a translated connection. This name can match the name of the final destination resource, but is not required to. This argument is useful when making remote translated connections.
<i>incoming-options</i>	(Optional) An incoming connection request option. For LAT, the only option currently supported is: • unadvertised—Prevents service advertisements from being broadcast to the network. This keyword can be useful, for example, when you define translations for many printers, and you do not want these services advertised to other LAT terminal servers. (VMS systems will be able to connect to the service even though it is not advertised.)
<i>protocol</i> <i>outgoing-address</i>	A protocol name followed by an address or host name. Protocol translation choices are: ppp , slip , tcp , and x25 . Note The host name is resolved to an address during configuration, unless you are translating to TCP and use the host-name keyword, which allows the host name to be resolved at connection time instead of configuration time. See Table 55 for more information about the host-name keyword. Additional keywords that can be entered with the protocol are as follows: • autocommand—Specifies an EXEC command for an outgoing connection. The command executes upon connection to a host. You can issue any EXEC command and any switch or host name as an argument to the autocommand command. If the string following autocommand has one or more spaces as part of the string, you must place quotation marks (“ ”) around the string. If you want to enable AppleTalk Remote Access (ARA) on an outgoing connection, specify the autocommand arap keywords. These keywords are necessary for ARA because ARA does not use addressing, and this option permits you to invoke the ARA string. • virtual-template—Associates a virtual template with a virtual access interface. See the translate lat (virtual access interfaces) command description for more information.

<i>outgoing-options</i>	(Optional) Outgoing connection request options. Choices depend upon the protocol or command entered. See Table 53 , Table 54 , Table 55 , and Table 56 for more information.
<i>global-options</i>	(Optional) One or more of the following translation options can be used by any connection type: • access-class <i>number</i>—Allows the incoming call to be used by source hosts that match the access list parameters. The argument <i>number</i> is an integer previously assigned to an access list. Standard access list numbers are in the range from 1 to 99; expanded standard access lists numbers are in the range 1300 to 1999. • local—Allows Telnet protocol negotiations to <i>not</i> be translated. • login—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the login command. • max-users <i>number</i>—Limits the number of simultaneous users of the translation to <i>number</i> (an integer you specify). • quiet—Suppresses printing of user-information messages.

Defaults

No default translation parameters

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1	The no-reset permanent virtual circuits (PVC) subkeyword was added to support outgoing PVCs.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You define protocol translation connections by supplying a protocol keyword and the address, host name, or service name. A LAT protocol translation command can be as simple as the following example:

```
Router(config)# translate lat LAT-1 X.25 1236672
```

However, the Cisco IOS software provides a broad range of options that support protocol translations in many networking environments. [Table 53](#), [Table 54](#), [Table 55](#), and [Table 56](#) list the **translate lat** translation options by protocol.

You can also use the Cisco IOS command-line interface to help you understand how these keywords are entered. In global configuration mode, begin entering the **translate** command and add a question mark at each portion of the command to display the options available. Some examples follow:

```
Router(config)# translate lat ?
```

```
WORD LAT service name
```

```
Router(config)# translate lat LSVC ?
```

```
autocommand      Associate a command with a translation on this connections
lat              DEC LAT protocol
ppp              Virtual async PPP
slip              Virtual async SLIP
tcp              TCP/IP Telnet
unadvertised      Prevent service advertisements from being broadcast to the
                  network
virtual-template  Associate a virtual template with virtual access interface
x25              X.25
```

```
Router(config)# translate lat LSVC tcp ?
```

```
Hostname or A.B.C.D  IP address
```

```
Router(config)# translate lat LSVC tcp 10.1.1.1 ?
```

```
access-class      Allow access list parameters to be used by source hosts
binary            Negotiate Telnet binary mode on the connection
host-name         Store the host name rather than its IP address
local             Allow Telnet protocol negotiations not to be translated
login             Require that the user log in before the outgoing connection
                  is made
max-users          Limit the number of simultaneous users of the translation
multibyte-IAC     Always treat multiple IACs as telnet command
port              Port Number
quiet             Suppress printing of user-information messages
source-interface  Specify source interface
stream            Treat telnet escape characters as data
```

**Note**

If you plan to translate to X.25 on a permanent virtual circuit (PVC), see the description for the [translate x25](#) command for important configuration notes.

Table 53 ***LAT-to-PPP Outgoing Translation Options***

Outgoing PPP Translation

ppp {*ip-address* | **ip-pool** [**scope-name** *name*]}

Translates from LAT to virtual asynchronous PPP. Supply an IP address as a standard, four-part dotted decimal IP address.

The **ip-pool** keyword obtains an IP address from a Dynamic Host Configuration Protocol (DHCP) proxy client or a local pool. If the optional **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

Outgoing PPP Connection Request Options

Add any of the following keywords to configure PPP connection requests:

- **authentication** {**pap** | **chap**}—Sets Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication for PPP on virtual asynchronous interfaces. If you specify both keywords, order is significant; the system will try to use the first authentication type, then the second.
 - **header-compression**—Implements header compression on IP packets only.
-

Table 53 **LAT-to-PPP Outgoing Translation Options (continued)**

-
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP to connect through virtual terminal lines on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the virtual terminal line. The virtual terminal line is assigned to the loopback interface.
 - **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on Serial Line Internet Protocol (SLIP) and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.
 - **mtu** *bytes*—Sets the interface maximum transmission unit (MTU) of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
 - **routing**—Permits routing updates between connections. This keyword is required if the destination device is not on a subnet connected to one of the interfaces on the router.
 - **use-tacacs**—Uses TACACS to verify PPP authentications for CHAP or PAP on virtual asynchronous interfaces.
-

Table 54 **LAT-to-SLIP Outgoing Translation Options****Outgoing SLIP Translation**

slip { *ip-address* | **ip-pool** [**scope-name** *name*] }

Translates from LAT to virtual asynchronous SLIP. Supply an IP address as a standard, four-part dotted decimal IP address.

The **ip-pool** keyword obtains an IP address from a DHCP proxy client or a local pool. If the optional **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

Note The **slip** argument applies only to outgoing connections; SLIP is not supported on incoming protocol translation connections.

Table 54 *LAT-to-SLIP Outgoing Translation Options (continued)***Outgoing SLIP Connection Request Options**

Add any of the following keywords to configure SLIP connection requests:

- **header-compression** [**passive**]—Implements header compression on IP packets only. The **passive** keyword permits compression on outgoing packets only if incoming TCP packets on the same virtual asynchronous interface are compressed. The default (without the **passive** keyword) permits compression on all traffic.
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP to connect through virtual terminal lines on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the virtual terminal line. The virtual terminal line is assigned to the loopback interface.
- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on SLIP and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.
- **mtu** *bytes*—Sets the interface MTU of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
- **routing**—Permits routing updates between connections. This keyword is required if the destination device is not on a subnet connected to one of the interfaces on the router.

Table 55 *LAT-to-TCP Outgoing Options***Outgoing TCP Translation****tcp** *ip-address*

Translates LAT to TCP/IP Telnet. Supply an IP address as a standard, four-part dotted decimal IP address, the name of an IP host that can be resolved by the Domain Name System (DNS), or explicit specification in an **ip host** command (refer to the description for the **host-name** keyword in the “Outgoing TCP Connection Request Options” section).

Outgoing TCP Connection Request Options

Any of the following optional keywords can be used to configure TCP connection requests:

- **binary**—Negotiates Telnet binary mode on the connection.
- **host-name**—Stores the host name rather than its IP address, thereby allowing the host name to be resolved at connection time instead of configuration time. There is also a **rotor** keyword suboption that you can use to modify the behavior of the **host-name** keyword by allowing one of the IP addresses defined by the **ip host** configuration command to be chosen randomly. If one address fails, another one will be tried, and so on until all address choices are exhausted. You can use the **rotor** keyword, therefore, to provide basic load sharing of the IP destinations.
- **multibyte-IAC**—Always treat multiple Interpret as Command (IAC) escape character codes as a Telnet command.
- **port** *number*—For outgoing connections, enter the number of the port to match. The default is port 23 (Telnet).

Table 55 LAT-to-TCP Outgoing Options (continued)

- **source-interface**—Specifies the source address used for Telnet connections initiated by the router.
- **stream**—Performs stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process or generate any Telnet options, and also prevents Telnet processing of the data stream. This keyword might be useful for connections to ports running the UNIX-to-UNIX Copy Program (UUCP) or other non-Telnet protocols, or to ports connected to printers. For ports connected to printers using Telnet, the **stream** keyword prevents some of the problems associated with using Telnet for printers, such as unusual events happening to carriage returns or line feeds and echoing of data back to VMS systems.

Table 56 LAT-to-X.25 Outgoing Translation Options**Outgoing X.25 Translation****x25** *x.121-address*

Translates LAT to the X.25 protocol. Supply an X.121 address that conforms to the specifications provided in the *CCITT 1984 Red Book*, or the name of an X.25 host that can be resolved by the DNS, or explicit specification in an **x25 host** command.

The address number generally consists of a portion that is administered by the public data network (PDN) and a portion that is locally assigned. You must be sure that the numbers that you assign agree with the addresses assigned to you by the X.25 service provider. The X.121 addresses generally will be subaddresses of the X.121 address for the X.25 network interface.

Outgoing X.25 Connection Request Options

Any of the following optional keywords can be used to configure X.25 connection requests:

- **cud** *c-u-data*—Sends the specified X.25 Call User Data (CUD) text as part of an outgoing call request after the protocol identification bytes.
- **no-reverse**—Specifies that outgoing calls not request the X.25 reverse charge facility, when the interface default is that all outgoing calls are reverse charged.
- **profile** *profile*—Sets the X.3 packet assembler/disassembler (PAD) parameters as defined in the profile created by the **x29 profile** command.
- **pvc** *number* [**interface** *serial number* | **packet-size** *in-size out-size* | **window-size** *in-size out-size* | **no-reset**]—Specifies that the outgoing connection is actually a PVC. The *number* argument specifies the virtual circuit channel number of the connection, which must be less than the virtual circuits assigned to the switched virtual circuit (SVC). Only one session is allowed per PVC. Use the following optional keywords to further define the connection:
 - **interface** *serial number*—Specifies a PVC interface on which to set up the PVC connection.
 - **packet-size** *in-size out-size*—Specifies the input packet size (*in-size*) and output packet size (*out-size*) for the PVC. Valid packet size values are: 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096.
 - **window-size** *in-size out-size*—Specifies the packet count for input windows (*in-size*) and output windows (*out-size*) for the outgoing translation. Values of *in-size* and *out-size* range from 1 to 127 and must not be greater than the value set for the **x25 modulo** command. You must specify the same value for *in-size* and *out-size*.
 - **no-reset**—Causes the Cisco router to send a no Reset packet request at startup of a TCP or LAT to permanent virtual circuit (PVC) translation session.

Table 56 LAT-to-X.25 Outgoing Translation Options (continued)

- **reverse**—Provides reverse charging for X.25 on a per-call rather than a per-interface basis. Requests reverse charges on a specified X.121 address, even if the serial interface is not configured to request reverse charge calls.
- **use-map**—Applies **x25 map pad** command entry options (such as CUD and idle) and facilities (such as packet in, packet out, win in, and win out) to the outgoing protocol translation call. When the **use-map** keyword is specified on the **translate** command, the Destination address and optional PAD Protocol Identification (PID), CUD, and facilities are checked against a configured list of **x25 map pad** entries. If a match is found, the map entry PID, CUD, and facilities are applied to the outgoing protocol translation call. The X.25 map facilities applied to the outgoing translation can be displayed with the **show translation** command throughout the duration of the translation session.

Examples

The following example illustrates incoming LAT to outgoing TCP translations. The **unadvertised** keyword prevents broadcast of service advertisements to other servers in the network. Outgoing translated packets are sent to IP host Host1, TCP port 4005.

```
translate lat pt-printer1 unadvertised tcp Host1 port 4005
```

The following example translates LAT on an incoming line to SLIP on an outgoing line. It uses header compression only if incoming TCP packets on the same interface are compressed.

```
translate lat Service1 slip 10.0.0.4 header-compression
```

The following example first shows how to disable keepalive packets on a PPP line using the **translate lat** command, then shows translated session output from the **show translate EXEC** command indicating keepalive packets have been turned off.

```
translate lat Service2 ppp 172.21.2.2 keepalive 0
.
.
.
Router# show translate

Translate From: LAT Service2
           To:   PPP 172.21.2.2 keepalive 0
           0/0 users active, 0 peak, 0 total, 0 failures
```

Related Commands

Command	Description
show translate	Displays configured translation sessions.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the translate command.

translate ruleset

To define a unique name for a translation ruleset, specify the translated protocols, and enable translate ruleset configuration mode, use the **translate ruleset** command in global configuration mode. To remove the ruleset, use the **no** form of this command.

translate ruleset *name* **from** *incoming-protocol* **to** *outgoing-protocol*

no translate ruleset *name* **from** *incoming-protocol* **to** *outgoing-protocol*

Syntax Description

<i>name</i>	Unique name for the protocol translation ruleset.
from <i>incoming-protocol</i>	Specifies the incoming protocol that will be translated, and can be one of the following: • pad—X.25 PAD • telnet—TCP/IP Telnet
to <i>outgoing-protocol</i>	Specifies the outgoing protocol or option to translate the incoming protocol to, and can be one of the following: • pad—X.25 PAD • telnet—TCP/IP Telnet

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command places the shell into the translate ruleset configuration mode to create the ruleset template of protocol translation criteria.

The translation ruleset compares an incoming connection attempt to the set of criteria to determine whether it is eligible for protocol translation processing, then uses additional information to complete the transaction.

Existing one-line translate command protocol translation configurations (using the **translate tcp** and **translate x25** commands, for example) take precedence over a protocol translation ruleset. This rule is reinforced when the configuration is generated by placing all one-line **translate** command protocol translation configurations *before* protocol translation ruleset configurations.

Some protocol translation options available with the one-line protocol translation commands are not available with this command.

An incoming PAD call with a standard protocol identification (PID) value that cannot be identified as PAD (for example, its first four bytes indicate IP encapsulation) will not be eligible for protocol translation.

Incoming TCP connections must be made on standard Telnet port 23; otherwise, the connection is not eligible for protocol translation.

If a ruleset is deleted, it will not affect an established protocol translation session, but a new, incoming connection attempt may terminate, depending upon how far along it is in the connection process.

Examples

The following example shows how to start the translate ruleset configuration mode:

```
Router(config)# translate ruleset Pad-Telnet from pad to telnet
```

```
Router(cfg-pt-ruleset)# ?
```

Protocol Translation ruleset configuration commands:

description	User-specified description of the ruleset
exit	Exit from PT ruleset configuration mode
match	Define a pattern of input parameters for a connection to process
no	Negate or set default values of a command
options	Define the ruleset options
set	Define parameter values
skip	Define a pattern of input parameters for a connection to skip
substitute	Define a parameter pattern match and substitute into another
test	Define parameter pattern(s) to test for conditionally setting parameters

Related Commands

Command	Description
description (ruleset)	Adds a description about a translation ruleset.
match (ruleset)	Identifies a connection for processing by the translation ruleset.
options (ruleset)	Specifies protocol translation options in a translation ruleset.
set (ruleset)	Unconditionally sets one or more connection parameters to a fixed value for a translation ruleset.
show translate ruleset	Displays a summary of a specific or of all configured translation rulesets, behavioral parameters, and usage statistic.
skip (ruleset)	Identifies a connection for omission by the translation ruleset.
substitute (ruleset)	Matches an available protocol and substitutes another in a translation ruleset.
test (ruleset)	Tests parameter values in a translation ruleset using regular expressions.
test translate	Displays a trace of protocol translation behavior for a connection attempt.
x25 pvc translate ruleset	Configures PVCs that are valid for protocol translation ruleset handling.

translate lat (virtual access interfaces)

When receiving a local-area transport (LAT) connection request to a service name, to set up the Cisco router to automatically translate the request to another outgoing protocol connection type, use the **translate lat** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

translate lat *incoming-service-name* [*incoming-options*] **virtual-template** *number*
[*global-options*]

no translate lat *incoming-service-name* [*incoming-options*] **virtual-template** *number*
[*global-options*]

Syntax Description	
<i>incoming-service-name</i>	A LAT service name. When used on the incoming portion of the translate lat command, <i>service-name</i> is the name of the service that users specify when trying to make a translated connection. This name can match the name of the final destination resource, but this match is not required. Such matches can be useful when making remote translated connections.
<i>incoming-options</i>	(Optional) An incoming connection request option. For LAT, the only keyword currently supported is: • unadvertised—Prevents service advertisements from being broadcast to the network. This keyword can be useful, for example, when you define translations for many printers, and you do not want these services advertised to other LAT terminal servers. (VMS systems will be able to connect to the service even though it is not advertised.)
virtual-template <i>number</i>	Applies the virtual interface template specified by the <i>number</i> argument in place of outgoing options.
<i>global-options</i>	(Optional) Translation options that can be used by any connection type and can be one or more of the following: • access-class <i>number</i>—Allows the incoming call to be used by source hosts that match the access list parameters. The argument <i>number</i> is an integer previously assigned to an access list. Standard access list numbers are in the range from 1 to 99; expanded standard access lists numbers are in the range 1300 to 1999. • max-users <i>number</i>—Limits the number of simultaneous users of the translation to <i>number</i> (an integer you specify). • local—Allows Telnet protocol negotiations to <i>not</i> be translated. • login—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the login command. • quiet—Suppresses printing of user-information messages.

Defaults No default translation parameters

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The command syntax documented here shows how to apply a virtual interface template in place of outgoing **translate** options. If you are using virtual templates for protocol translation, all outgoing options are defined in the virtual interface template. [Table 57](#) lists all outgoing options and their corresponding interface configuration commands.

You define the protocol translation connections by choosing a protocol keyword and supplying the appropriate address, host name, or service name. The protocol connection information is followed by optional features for that connection, as appropriate. For example, the **binary** keyword is only appropriate with TCP/IP connections. The global options, in general, apply to all the connection types, but there are exceptions.

Rather than specifying outgoing translation options in the **translate** command, configure these options as interface configuration commands under the virtual interface template, then apply the virtual interface template to the **translate** command. [Table 57](#) maps outgoing **translate** command options to interface commands you can configure in the virtual interface template.

Table 57 Mapping Outgoing translate lat Options to Interface Commands

translate lat Command Options	Corresponding Interface Configuration Command
ip-pool	peer default ip address {ip-address dhcp pool [poolname]}
header-compression	ip tcp header compression [on off passive]
routing	ip routing or ipx routing
mtu	mtu
keepalive	keepalive
authentication {chap pap}	ppp authentication {chap pap}
ppp use-tacacs	ppp use-tacacs
ipx loopback	ipx ppp-client loopback <i>number</i>

Examples

The following example configures PPP tunneling from a PC across a LAT network. The remote PC is given the IP address 10.12.118.12 when it dials in. The **unadvertised** keyword prevents broadcast of service advertisements to other servers.

```
interface Virtual-Template1
 ip unnumbered Ethernet0
 peer default ip address 10.12.118.12
 ppp authentication chap
!
translate lat pt-printer1 unadvertised virtual-template 1
```

Related Commands

Command	Description
show translate	Displays configured translation sessions.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the translate command.

translate tcp

To translate a connection request to another protocol connection type when receiving a TCP connection request to a particular destination address or host name, use the **translate tcp** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

translate tcp *incoming-address* [*incoming-options*] *protocol* *outgoing-address* [*outgoing-options*] [*global-options*]

no translate tcp *incoming-address* [*incoming-options*] *protocol* *outgoing-address* [*outgoing-options*] [*global-options*]

Syntax Description

<i>incoming-address</i>	Standard IP address in standard, four-part dotted decimal notation. The IP address cannot be in use by other routers, and it should be on a connected subnet.
<i>incoming-options</i>	(Optional) An incoming connection request option. Choices are as follows: • binary—Negotiates Telnet binary mode on the Telnet connection. (This was the default in previous versions of the protocol translation software and is set automatically when you enter a translate command in the previous format.) • port number—The number of the port to match for incoming connections. The default is port 23 (Telnet). For outgoing connections, enter the number of the port to use. The default is port 23. • printer—Supports local-area transport (LAT) and X.25 printing over a TCP network among multiple sites. This keyword causes the protocol translation software to delay the completion of an incoming Telnet connection until after the outgoing protocol connection (to LAT or X.25) has been established. An unsuccessful outgoing connection attempt results in the TCP connection to the router being refused, rather than being accepted and then closed, which is the default behavior. Note that using this keyword will force the global quiet keyword to be applied to the translation. • stream—Performs stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process or generate any Telnet options, and also prevents Telnet processing of the data stream. This keyword might be useful for connections to ports running the UNIX-to-UNIX Copy Program (UUCP) or other non-Telnet protocols, or to ports connected to printers. For ports connected to printers using Telnet, the stream keyword prevents some of the problems associated with using Telnet for printers, such as unusual events happening to carriage returns or line feeds and echoing of data back to VPN/Security Management Solution (VMS) systems.

<i>protocol</i>	A protocol name followed by an address or host name. Protocol translation choices are: lat , ppp , slip , and x25 .
<i>outgoing-address</i>	Additional keywords that can be entered instead of a protocol name are as follows: • autocommand—Specifies an EXEC command for an outgoing connection. The command executes upon connection to a host. You can issue any EXEC command and any switch or host name as an argument to the autocommand keyword. If the string following autocommand has one or more spaces as part of the string, you must place quotation marks (“ ”) around the string. If you want to enable AppleTalk Remote Access (ARA) on an outgoing connection, specify the autocommand arap keywords. These keywords are necessary for ARA because ARA does not use addressing, and this option permits you to invoke the ARA string. • virtual-template—Associates a virtual template with a virtual access interface. See the translate tcp (virtual access interfaces) command description for more information.
<i>outgoing-options</i>	(Optional) Outgoing connection request options. Choices depend upon the protocol or command entered. See Table 58 , Table 59 , Table 60 , and Table 61 for more information.

<i>global-options</i>	(Optional) One or more of the following translation options can be used by any connection type: • access-class <i>number</i>—Allows the incoming call to be used by source hosts that match the access list parameters. The <i>number</i> argument is an integer previously assigned to an access list. Standard access list numbers are in the range from 1 to 99; expanded standard access lists numbers are in the range from 1300 to 1999. • authorize <i>method-list tag</i>—Enables authorization for protocol translation sessions. The <i>method-list</i> argument is the list of authorization methods defined by the aaa authorization command with the translate keyword. The <i>method-list</i> argument may have the value of the <i>list-name</i> argument or the default keyword. The <i>tag</i> argument is an alphanumeric string of up to 64 characters. The <i>tag</i> argument need not be unique; more than one instance of the translate command can specify identical values for the <i>tag</i> argument. The authorize option is available only if the outgoing protocol keyword is x25 or autocommand. • eor <i>marker</i> [insert]—Defines the End-of-Record (EOR) marker for the translation session. The <i>marker</i> argument may be any set of characters from 1 to 4 in length. Nonprintable characters must be entered in hexadecimal format. Printable characters may be typed in. The insert keyword allows the EOR marker to be inserted into the TCP stream after each X.25 packet without a More-bit (M-bit) set is received. • local—Allows Telnet protocol negotiations to <i>not</i> be translated. • login—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the login command. • max-users <i>number</i>—Limits the number of simultaneous users of the translation to <i>number</i> (an integer you specify). • quiet—Suppresses printing of user-information messages. • swap—Valid for TCP-to-X.25 translations only, and allows X.3 parameters to be set on the router by the host originating the X.25 call, or by an X.29 profile. This configuration enables incoming and outgoing X.25 connections to be swapped so that the device is treated like a packet assembler/disassembler (PAD) when it accepts a call. By default, the router functions like a PAD for calls that it initiates, and like an X.25 host for calls it accepts. The swap keyword allows connections from an X.25 host that wants to connect to the router, and then treats it like a PAD.
-----------------------	---

Defaults

No default translation parameters

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1	The no-reset permanent virtual circuits (PVCs) subkeyword was added to support outgoing PVCs.
12.2(13)T	The dynamic keyword was added to support a backup interface.
12.3(2)T	The authorize method-list tag keyword and arguments were added to support authorization of protocol translation sessions. The eor marker [insert] keywords and argument were added to support the EOR function for DCNs.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You define protocol translation connections by supplying a protocol keyword and the address, host name, or service name. A TCP protocol translation command can be as simple as the following example:

```
Router(config)# translate tcp 10.1.1.1 x25 1236672
```

However, the Cisco IOS software provides a broad range of options that support protocol translations in many networking environments. [Table 58](#), [Table 59](#), [Table 60](#), and [Table 61](#) list the **translate tcp** translation options by protocol.

You can also use the Cisco IOS command-line interface (CLI) to help you understand how these keywords are entered. In global configuration mode, begin entering the **translate** command and add a question mark at each portion of the command to display the options available. Some examples follow:

```
Router(config)# translate tcp ?
```

```
Hostname or A.B.C.D IP address
```

```
Router(config)# translate tcp 10.1.1.1 ?
```

```
autocommand      Associate a command with a translation on this connections
binary           Negotiate Telnet binary mode on the connection
lat              DEC LAT protocol
port             Port Number
ppp              Virtual async PPP
printer          Enable non-interactive (implies global quiet)
slip             Virtual async SLIP
stream           Enable stream processing
tcp              TCP/IP Telnet
virtual-template Associate a virtual template with virtual access interface
x25              X.25
```

```
Router(config)# translate tcp 10.1.1.1 lat LAT-1 ?
```

```
access-class      Allow access list parameters to be used by source hosts
local            Allow Telnet protocol negotiations not to be translated
login            Require that the user log in before the outgoing connection is
                 made
max-users         Limit the number of simultaneous users of the translation
node             LAT node name
port             LAT port name
quiet            Suppress printing of user-information messages
unadvertised      Prevent service advertisements from being broadcast to the
```

network

**Note**

If you plan to translate to X.25 on a PVC, see the description for the [translate x25](#) command for important configuration notes.

Table 58 *TCP-to-LAT Outgoing Options*

Outgoing LAT Translation

lat *service-name*

Translates TCP to the LAT protocol. The software must learn the service name through LAT service advertisements before it can use the service.

Outgoing LAT Connection Request Options

Any of the following optional keywords can be used to configure LAT connection requests:

- **node** *name*—Connects to the specified node that offers a LAT service. By default, the connection is made to the highest-rated node that offers the service.
 - **port** *name*—Destination LAT port name in the format of the remote system. This parameter is usually ignored in most time-sharing systems, but is used by terminal servers that offer reverse-LAT services.
 - **unadvertised**—Prevents LAT service advertisements from being broadcast to the network.
-

Table 59 *TCP-to-PPP Outgoing Options*

Outgoing PPP Translation

ppp { *ip-address* | **ip-pool** [**scope-name** *name*] }

Translates from TCP to virtual asynchronous PPP. Supply an IP address as a standard, four-part dotted decimal IP address.

The **ip-pool** keyword obtains an IP address from a Dynamic Host Configuration Protocol (DHCP) proxy client or a local pool. If the **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

Outgoing PPP Connection Request Options

Any of the following optional keywords can be used to configure PPP connection requests:

- **authentication** { **pap** | **chap** }—Sets Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication for PPP on virtual asynchronous interfaces. If you specify both keywords, order is significant; the system will try to use the first authentication type, then the second.
 - **header-compression** [**passive**]—Implements header compression on IP packets only. The **passive** keyword permits compression on outgoing packets only if incoming TCP packets on the same virtual asynchronous interface are compressed. The default (without the **passive** keyword) permits compression on all traffic.
 - **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP to connect through vtys on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the vty. The vty is assigned to the loopback interface.
-

Table 59 *TCP-to-PPP Outgoing Options (continued)*

- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on Serial Line Internet Protocol (SLIP) and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.
- **mtu** *bytes*—Sets the interface maximum transmission unit (MTU) of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
- **routing**—Permits routing updates between connections. This keyword is required if the destination device is not on a subnet connected to one of the interfaces on the router.
- **use-tacacs**—Uses TACACS to verify PPP authentications for CHAP or PAP on virtual asynchronous interfaces.

Table 60 *TCP-to-SLIP Outgoing Options***Outgoing SLIP Translation**

slip {*ip-address* | **ip-pool** [**scope-name** *name*]}

Translates from TCP to virtual asynchronous SLIP. Supply an IP address as a standard, four-part dotted decimal IP address.

The **ip-pool** keyword obtains an IP address from a DHCP proxy client or a local pool. If the optional **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

Note The **slip** keyword applies only to outgoing connections; SLIP is not supported on incoming protocol translation connections.

Outgoing SLIP Connection Request Options

Any of the following optional keywords can be used to configure SLIP connection requests:

- **header-compression** [**passive**]—Implements header compression on IP packets only. The **passive** keyword permits compression on outgoing packets only if incoming TCP packets on the same virtual asynchronous interface are compressed. The default (without the **passive** keyword) permits compression on all traffic.
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP over X.25 to connect through vtys on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the vty. The vty is assigned to the loopback interface.
- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on SLIP and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.

Table 60 *TCP-to-SLIP Outgoing Options (continued)*

-
- **mtu bytes**—Sets the interface MTU of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
 - **routing**—Permits routing updates between connections. This keyword is required if the destination device is not on a subnet connected to one of the interfaces on the router.
-

Table 61 *TCP-to-X.25 Outgoing Options***Outgoing X.25 Translation****x25** *x.121-address*

Translates TCP to the X.25 protocol. Supply an X.121 address that conforms to the specifications provided in the *CCITT 1984 Red Book*, or the name of an X.25 host that can be resolved by the DNS, or explicit specification in an **x25 host** command.

The address number generally consists of a portion that is administered by the public data network (PDN) and a portion that is locally assigned. You must be sure that the numbers that you assign agree with the addresses assigned to you by the X.25 service provider. The X.121 addresses generally will be subaddresses of the X.121 address for the X.25 network interface.

Outgoing X.25 Connection Request Options

Any of the following optional keywords can be used to configure X.25 connection requests:

- **cud c-u-data**—Sends the specified X.25 Call User Data (CUD) text as part of an outgoing call request after the protocol identification bytes.
 - **no-reverse**—Specifies that outgoing calls not request the X.25 reverse charge facility, when the interface default is that all outgoing calls are reverse charged.
 - **profile profile**—Sets the X.3 PAD parameters as defined in the profile created by the **x29 profile** command.
 - **pvc number [interface serial number | packet-size in-size out-size | window-size in-size out-size | no-reset | dynamic]**—Specifies that the outgoing connection is actually a PVC. The *number* argument specifies the virtual circuit channel number of the incoming connection, which must be less than the virtual circuits assigned to the switched virtual circuit (SVC). Only one session is allowed per PVC. Use the following optional keywords to further define the connection:
 - **interface serial number**—Specifies a PVC interface on which to set up the PVC connection.
 - **packet-size in-size out-size**—Specifies the input packet size (*in-size*) and output packet size (*out-size*) for the PVC. Valid packet size values are: 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096.
 - **window-size in-size out-size**—Specifies the packet count for input windows (*in-size*) and output windows (*out-size*) for the outgoing translation. Values of *in-size* and *out-size* range from 1 to 127 and must not be greater than the value set for the **x25 modulo** command. You must specify the same value for the *in-size* and *out-size* arguments.
 - **no-reset**—Causes the Cisco router to send a no reset packet request at startup of a TCP or LAT-to-PVC translation session.
 - **dynamic**—Causes the TCP-to-X25 PVC session to terminate when the interface goes down. The default behavior is to keep the PVC in existence as long as it is configured.
-

Table 61 *TCP-to-X.25 Outgoing Options (continued)*

-
- **reverse**—Provides reverse charging for X.25 on a per-call rather than a per-interface basis. Requests reverse charges on a specified X.121 address, even if the serial interface is not configured to request reverse charge calls.
 - **use-map**—Applies **x25 map pad** command entry options (such as CUD and idle) and facilities (such as packet in, packet out, win in, and win out) to the outgoing protocol translation call. When the **use-map** keyword is specified on the **translate** command, the Destination address and optional PAD Protocol Identification (PID), CUD, and facilities are checked against a configured list of **x25 map pad** command entries. If a match is found, the map entry PID, CUD, and facilities are applied to the outgoing protocol translation call. The X.25 map facilities applied to the outgoing translation can be displayed with the **show translation** command throughout the duration of the translation session.
-

Examples

Dynamic PVCs to Support Primary and Secondary Interfaces Example

The following partial example shows how to configure the PVC dynamic option. The **dynamic** keyword allows an X.25 PVC to be created on a backup interface when the primary interface goes down. The example configures a primary serial interface (serial 0/0) for X.25 encapsulation and assigns a secondary serial interface (serial 1/1) as backup for the primary. Comments explain the configuration.

```
interface serial 0/0
 encapsulation x25
 backup active interface Serial1/1
!
interface serial 1/1
 encapsulation x25
!
! Configure an X.25 route specifying the primary interface on which the router
! should create the dynamic PVCs.
x25 route ^10 interface serial 0/0
!
! Configure a second X.25 route specifying the secondary backup interface on which
! the router can recreate the PVCs should the primary go down.
x25 route ^10 interface serial 1/1
!
! Configure the translate commands with the PVC dynamic option.
translate tcp 10.60.150.128 port 1031 x25 10 pvc 1 dynamic
.
.
.
translate tcp 10.60.150.128 port 1036 x25 10 pvc 6 dynamic
!
```

When the primary interface serial 0/0 is the active link and it is operational (up), the PVCs will be created on that interface.

If the primary interface goes down, the following will occur:

- The TCP sessions associated with the X.25 PVCs on serial interface 0/0 will be terminated.
- The X25 PVCs created on serial interface 0/0 will be deleted.
- The primary link on serial interface 0/0 will go into the TESTING state.
- The backup link on serial interface 1/1 will change from the X.25 TESTING state to the UP state.
- This change of the interface state (from TESTING to UP) will cause the secondary link on serial interface 1/1 to become active.

- The X.25 PVCs will be recreated on the secondary link on serial interface 1/1 based on the configuration of the second **x25 route** command.
- Incoming TCP connections will be reestablished with the X.25 PVCs on serial interface 1/1.

TCP-to-X.25 PVC connections will remain on the backup secondary interface (serial 1/1) even when the primary interface (serial 0/0) becomes operational. Only when the backup interface (serial 1/1) fails does the process described repeat and move the TCP-to-X25 PVC connections back to the primary interface (serial 0/0).

Incoming TCP Connection to a Printer Example

The following example illustrates the use of the TCP incoming protocol **printer** keyword for an incoming TCP connection:

```
translate tcp 172.19.32.250 printer x25 5678
```

IPX-PPP Client Connects to a Server Running PPP Example

The following example permits clients running IPX-PPP to connect through the device virtual terminal lines to a server running PPP:

```
interface loopback0
  no ip address
  ipx network 544
  ipx sap-interval 2000
!
translate tcp 172.21.14.67 port 1234 ppp 10.0.0.2 ipx loopback0
```

Configuring the EOR Marker for a TCP-to-X.25 Protocol Translation Session Example

The following example configures a TCP-to-X.25 protocol translation session to insert an EOR marker in a TCP packet after each received X.25 packet that does not contain the M-bit set. The EOR marker in this example consists of nonprintable characters and is entered in hexadecimal format.

```
translate tcp 10.60.155.63 x25 12345678 pvc 3 dynamic eor 0x19 insert
```

Configuring Translation Authorization for a TCP-to-X.25 Protocol Translation Session Example

The following example uses an authorization method list named mygroup. Serial interfaces 2/0 and 2/1 connect to X.25 hosts, each of which provides multiple services at different X.25 subaddresses. Some of the translate statements specify unique authorization tags so the services can be individually controlled; others specify generic tags (perhaps because they are less critical, such as a monitoring service rather than one which permits configuration changes).

```
aaa authorization network mygroup group tacacs+
x25 routing
!
interface Ethernet0/0
  ip address 10.60.155.30 255.255.255.0
!
interface Serial2/0
  encapsulation x25 dce
  x25 ltc 30
!
interface Serial2/1
  encapsulation x25 dce
  x25 ltc 30
!
x25 route ^13033 interface Serial2/0
x25 route ^13133 interface Serial2/1
!
translate tcp 10.60.155.36 port 2001 x25 1303301 login authorize mygroup a-port01
translate tcp 10.60.155.36 port 2002 x25 1303302 login authorize mygroup a-port02
```

```

translate tcp 10.60.155.36 port 2003 x25 1303303 login authorize mygroup monitor
translate tcp 10.60.155.36 port 2004 x25 1303304 login authorize mygroup monitor
translate tcp 10.60.155.36 port 2005 x25 13033 pvc 1 login authorize mygroup a-admin01
!
translate tcp 10.60.155.36 port 2101 x25 1313301 login authorize mygroup b-port01
translate tcp 10.60.155.36 port 2102 x25 1313302 login authorize mygroup b-port02
translate tcp 10.60.155.36 port 2103 x25 1313303 login authorize mygroup monitor
translate tcp 10.60.155.36 port 2104 x25 1313304 login authorize mygroup monitor

```

With this configuration, the router accepts Telnet requests to 10.60.155.36 at any of the TCP ports listed. The user is required to log in, then the router sends an authorization request specifying “translate” as the value of the “service” AV pair, and the authorization tag from the corresponding **translate** command as the value of the “azn-tag” AV pair. The user id and remote address of the Telnet session are also included in the authorization request. If the authorization server approves the request, the connection to the specified X.25 address is attempted; if the request is denied, the Telnet connection is closed.

The authorization server would not be able to distinguish between connections to 10.60.155.36 port 2003 and 10.60.155.36 port 2104, because they specify the same authorization tag.

Related Commands

Command	Description
aaa	Sets parameters that restrict user access to a network.
authorization	
show translate	Displays configured translation sessions.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the translate command.

translate tcp (virtual access interfaces)

When receiving a TCP connection request to a particular destination address or host name, to set up the Cisco router to automatically translate the request to another outgoing protocol connection type, use the **translate tcp** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

translate tcp *incoming-address* [*incoming-options*] **virtual-template** *number* [*global-options*]

no translate tcp *incoming-address* [*incoming-options*] **virtual-template** *number* [*global-options*]

Syntax Description

<i>incoming-address</i>	TCP/IP Telnet and a standard IP address or host name. The <i>ip-address</i> argument is a standard, four-part dotted decimal IP address or the name of an IP host that can be resolved by the Domain Name System (DNS) or explicit specification in an ip host command.
<i>incoming-options</i>	(Optional) Incoming connection request options. These arguments can have the following values: • binary—Negotiates Telnet binary mode on the Telnet connection. (This was the default in previous versions of the Cisco IOS software and is set automatically when you enter a translate command in the old format.) • port number—For incoming connections, enter the number of the port to match. The default is port 23 (Telnet). For outgoing connections, enter the number of the port to use. The default is port 23. • printer—Supports LAT and X.25 printing over a TCP network among multiple sites. This keyword causes the protocol translation software to delay the completion of an incoming Telnet connection until after the outgoing protocol connection (to LAT or X.25) has been successfully established. An unsuccessful outgoing connection attempt results in the TCP connection to the router being refused, rather than being accepted and then closed, which is the default behavior. Note that using this keyword will force the global quiet keyword to be applied to the translation. • stream—Performs stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process or generate any Telnet options, and also prevents Telnet processing of the data stream. This keyword might be useful for connections to ports running the UNIX-to-UNIX Copy Program (UUCP) or other non-Telnet protocols, or to ports connected to printers. For ports connected to printers using Telnet, the stream keyword prevents some of the problems associated with using Telnet for printers, such as unusual events happening to carriage returns or line feeds and echoing of data back to VMS systems.
virtual-template <i>number</i>	Applies the virtual interface template specified by the <i>number</i> argument in place of outgoing options.

<i>global-options</i>	(Optional) One or more of the following translation options can be used by any connection type: • access-class <i>number</i>—Allows the incoming call to be used by source hosts that match the access list parameters. The argument <i>number</i> is an integer previously assigned to an access list. Standard access list numbers are in the range from 1 to 99; expanded standard access lists numbers are in the range 1300 to 1999. • local—Allows Telnet protocol negotiations to <i>not</i> be translated. • login—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the login command. • max-users <i>number</i>—Maximum number of simultaneous users of the translation. • quiet—Suppresses printing of user-information messages. • swap—Valid for TCP-to-X.25 translations only, and allows X.3 parameters to be set on the router by the host originating the X.25 call, or by an X.29 profile. This configuration enables incoming and outgoing X.25 connections to be swapped so that the device is treated like a PAD when it accepts a call. By default, the router functions like a PAD for calls that it initiates, and like an X.25 host for calls it accepts. The swap keyword allows connections from an X.25 host that wants to connect to the router, and then treats it like a PAD.
-----------------------	--

Defaults

No default translation parameters

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The command syntax documented here shows how to apply a virtual interface template in place of outgoing **translate** options. If you are using virtual templates for protocol translation, all outgoing options are defined in the virtual interface template.

You define the protocol translation connections by choosing a protocol keyword and supplying the appropriate address, host name, or service name. The protocol connection information is followed by optional features for that connection, as appropriate. For example, the **binary** keyword is only appropriate with TCP/IP connections. The global options, in general, apply to all the connection types, but there are exceptions.

Examples

The following example illustrates the use of the TCP incoming **printer** keyword for an incoming TCP connection:

```
interface virtual-template1
 ip unnumbered Ethernet0
 peer default ip address 10.12.108.1
 ppp authentication chap

translate tcp 172.19.32.250 printer virtual-template1
```

Related Commands

Command	Description
show translate	Displays configured translation sessions.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the translate command.

translate use telnet

To specify the required IP address in a Telnet-to-PAD protocol translation ruleset, use the **translate use telnet** command in global configuration mode. To disable the address, use the **no** form of this command.

translate use telnet *ip-address*

no translate use telnet *ip-address*

Syntax Description	<i>ip-address</i>	Incoming Telnet IP address used by translation rulesets.
---------------------------	-------------------	--

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.3(8)T	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	An IP address must be specified for the protocol translator to respond to Address Resolution Protocol (ARP) attempts for that address. The IP address that the protocol translation software listens for must be on a connected subnet; it cannot be used by another interface unless you also specify a TCP port number, and there cannot be another host that responds to ARPs for that address.
-------------------------	--

Examples	The following example sets the IP address for a translation ruleset: <pre> translate use telnet 10.10.1.5 ! translate ruleset T_to_P from telnet to pad description Sitel 10.10.1.5 Area Code 555 exchg 900 match dest-addr ^10.10.1.5\$ dest-port ^[1-5]...\$ substitute telnet dest-port ^1(...) into pad dest-addr 555900\1 . . . </pre>
-----------------	--

Related Commands	Command	Description
	description (ruleset)	Adds a description about a translation rule set.
	match (ruleset)	Identifies a connection for processing by the translation rule set.
	options (ruleset)	Specifies protocol translation options in a translation rule set.

Command	Description
set (ruleset)	Unconditionally sets one or more connection parameters to a fixed value for a translation rule set.
show translate ruleset	Displays a summary of a specific or of all configured translation rule sets, behavioral parameters, and usage statistic.
skip (ruleset)	Identifies a connection for omission by the translation rule set.
substitute (ruleset)	Matches an available protocol and substitutes another in a translation rule set.
test (ruleset)	Tests parameter values in a translation rule set using regular expressions.
test translate	Displays a trace of protocol translation behavior for a connection attempt.
translate ruleset	Defines a unique name for a translation rule set, specifies translated protocols, and enters translate ruleset configuration mode.
x25 pvc translate ruleset	Configures PVCs that are valid for protocol translation rule set handling.

translate x25

To translate a connection request to another protocol connection type when receiving an X.25 connection request to a particular destination address or host name, use the **translate x25** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

translate x25 *incoming-address* [*incoming-options* [**pvc** *number* [*pvc-options*]]] *protocol*
outgoing-address [*outgoing-options*] [*global-options*]

no translate x25 *incoming-address* [*incoming-options* [**pvc** *number* [*pvc-options*]]] *protocol*
outgoing-address [*outgoing-options*] [*global-options*]

Syntax Description

<i>incoming-address</i>	An X.25 and X.121 address that conforms to specifications provided in the <i>CCITT 1984 Red Book</i>. This address generally consists of a portion that is administered by the public data network (PDN) and a portion that is locally assigned. You must be sure that the numbers that you assign agree with the addresses assigned to you by the X.25 service provider. The X.121 addresses generally will be subaddresses of the X.121 address for the X.25 network interface. Typically, the interface address will be a 12-digit number. Any additional digits are interpreted as a subaddress. The PDN still routes these calls to the interface, and the Cisco IOS software is responsible for interpreting the extra digits. Do not use the same address on the interface and for translation.
<i>incoming-options</i>	(Optional) An incoming connection request option. Choices are as follows: • accept-reverse—Accepts reverse charged calls on an X.121 address even if the serial interface is not configured to accept reverse charged calls. • cud c-u-data—Specifies the Call User Data (CUD) field to match in the X.25 Incoming Call packet. If the cud keyword is not configured, the CUD in the Incoming Call packet must be blank. • idle minutes—Specifies the number of minutes the virtual circuit is idle. This keyword enables the protocol translation function to clear a switched virtual circuit (SVC) after a set period of inactivity, where <i>minutes</i> is the number of minutes in the period. Calls either originated or terminated are cleared. The maximum value of the <i>minutes</i> argument is 255. The default value of the <i>minutes</i> argument is zero. • printer—Supports local-area transport (LAT) and TCP printing over an X.25 network among multiple sites. Provides an “interlock mechanism” between the acceptance of an incoming X.25 connection and the opening of an outgoing LAT or TCP connection. This keyword causes the Cisco IOS software to delay the call confirmation of an incoming X.25 call request until after the outgoing protocol connection (to TCP or LAT) has been established. An unsuccessful outgoing connection attempt to the router results in the incoming X.25 connection being refused, rather than being accepted and then closed, which is the default behavior. Note that using this keyword will force the global quiet keyword to be applied to the translation. • profile profile—Sets the X.3 packet assembler/disassembler (PAD) parameters as defined in the profile created by the x29 profile command.

pvc number [pvc-options]	• pvc number [interface serial number packetsize in-size out-size window-size in-size out-size]—Specifies that the outgoing connection is actually a PVC. The <i>number</i> argument specifies the virtual circuit channel number of the connection, which must be less than the virtual circuits assigned to the SVC. Only one session is allowed per PVC. Use the following optional keywords to further define the connection: – interface serial number—Specifies a PVC interface on which to set up the PVC connection. – packetsize in-size out-size—Specifies the input packet size (<i>in-size</i>) and output packet size (<i>out-size</i>) for the PVC. Valid packet size values are as follows: 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096. – window-size in-size out-size—Specifies the packet count for input windows (<i>in-size</i>) and output windows (<i>out-size</i>) for the outgoing translation. Values of <i>in-size</i> and <i>out-size</i> range from 1 to 127 and must not be greater than the value set for the x25 modulo command. You must specify the same value for the <i>in-size</i> and <i>out-size</i> arguments. Note When the incoming connection is a PVC, the login and authorize global options and the autocommand option for the outbound protocol are not available.
<i>protocol</i> <i>outgoing-address</i>	A protocol name followed by an address or host name. Protocol translation choices are lat, ppp, slip, and tcp. Note The host name is translated to an address during configuration, unless you are translating to TCP and use the host-name keyword, which allows the host name to be resolved at connection time instead of configuration time. See Table 65 for more information about the host-name keyword. Additional keywords that can be entered instead of a protocol name are as follows: • autocommand—Specifies an EXEC command for an outgoing connection. The command executes upon connection to a host. You can issue any EXEC command and any switch or host name as an argument to the autocommand keyword. If the string following autocommand has one or more spaces as part of the string, you must place quotation marks (“ ”) around the string. If you want to enable AppleTalk Remote Access (ARA) on an outgoing connection, specify the autocommand arap keywords. These keywords are necessary for ARA because ARA does not use addressing, and this option permits you to invoke the ARA string. Note The autocommand option is not available when the incoming connection is a PVC. • virtual-template—Associates a virtual template with a virtual access interface. See the translate x25 (virtual access interfaces) command description for more information.
<i>outgoing-options</i>	(Optional) Outgoing connection request option. Choices depend upon the protocol or command entered. See Table 62, Table 63, Table 64, and Table 65 for a list of outgoing protocol translation options.

global-options

(Optional) One or more of the following translation options can be used by any connection type:

- **access-class** *number*—Allows the incoming call to be used by source hosts that match the access list parameters. The *number* argument is an integer previously assigned to an access list. Standard access list numbers are in the range from 1 to 99; expanded standard access lists numbers are in the range from 1300 to 1999.
- **authorize** *method-list tag*—Enables authorization for protocol translation sessions. The *method-list* argument is the list of authorization methods defined by the **aaa authorization** command with the **translate** keyword. The *method-list* argument may have the value of the *list-name* argument or the **default** keyword. The *tag* argument is an alphanumeric string of up to 64 characters. The *tag* argument need not be unique; more than one instance of the **translate** command can specify identical values for the *tag* argument.

Note The **authorize** option is not available when the incoming connection is a PVC.

- **eor marker** [**insert**]—Defines the End-of-Record (EOR) marker for the translation session. The *marker* argument may be any set of characters from 1 to 4 in length. Nonprintable characters must be entered in hexadecimal format. Printable characters may be typed in. The **insert** keyword allows the EOR marker to be inserted into the TCP stream after each X.25 packet without a More-bit (M-bit) set is received.
- **local**—Allows Telnet protocol negotiations to *not* be translated.
- **login**—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the **login** command.

Note The **login** option is not available when the incoming connection is a PVC.

- **max-users** *number*—Limits the number of simultaneous users of the translation to *number* (an integer you specify).
- **quiet**—Suppresses printing of user-information messages.
- **swap**—Valid for X.25-to-TCP translations only, and allows X.3 parameters to be set on the router by the host originating the X.25 call, or by an X.29 profile. This configuration enables incoming and outgoing X.25 connections to be swapped so that the device is treated like a PAD when it accepts a call. By default, the router functions like a PAD for calls that it initiates, and like an X.25 host for calls it accepts. The **swap** keyword allows connections from an X.25 host that wants to connect to the router, and then treats it like a PAD.

Defaults

No default translation parameters.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(2)T	The authorize method-list tag keyword and arguments were added to support authorization of protocol translation sessions. The eor marker [insert] keywords and argument were added to support the EOR function for DCNs.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You define protocol translation connections by supplying a protocol keyword and the address, host name, or service name. An X.25 protocol translation command can be as simple as the following example:

```
Router(config)# translate X.25 1236672 tcp 10.1.1.1
```

However, the Cisco IOS software provides a broad range of options that support protocol translations in many networking environments. [Table 62](#), [Table 63](#), [Table 64](#), and [Table 65](#) lists the **translate x25** translation options by protocol.

You can also use the Cisco IOS command-line interface to help you understand how these keywords are entered. In global configuration mode, begin entering the **translate** command and add a question mark at each portion of the command to display the options available. Some examples follow:

```
Router(config)# translate x25 ?
```

```
WORD X.121 Address pattern
```

```
Router(config)# translate x25 66666 ?
```

```
accept-reverse  Accept reverse charge on a per-call basis
autocommand     Associate a command with a translation on this connections
cud             Specify the Call User Data (CUD)
idle            Specify VC idle timer
lat             DEC LAT protocol
ppp             Virtual async PPP
printer         Enable non-interactive (implies global quiet)
profile         Use a defined X.3 profile
pvc             An incoming connection is actually a PVC
slip            Virtual async SLIP
tcp             TCP/IP Telnet
virtual-template Associate a virtual template with virtual access interface
x25            X.25
```

```
Router(config)# translate x25 66666 tcp 10.1.1.1 ?
```

```
access-class    Allow access list parameters to be used by source hosts
binary          Negotiate Telnet binary mode on the connection
host-name       Store the host name rather than its IP address
local           Allow Telnet protocol negotiations not to be translated
login           Require that the user log in before the outgoing connection
                is made
max-users       Limit the number of simultaneous users of the translation
multibyte-IAC   Always treat multiple IACs as telnet command
port            Port Number
quiet           Suppress printing of user-information messages
source-interface Specify source interface
stream          Treat telnet escape characters as data
swap           Allow X.3 parameters to be set on the protocol translator
                by the host originating the X.25 call
```

Table 62 *X.25-to-LAT Outgoing Options***Outgoing LAT Translation***lat service-name*

Translates X.25 to the LAT protocol. The software must learn the service name through LAT service advertisements before it can use the service.

Outgoing LAT Connection Request Options

Any of the following optional keywords can be used to configure LAT connection requests:

- **node** *name*—Connects to the specified node that offers a LAT service. By default, the connection is made to the highest-rated node that offers the service.
- **port** *name*—Destination LAT port name in the format of the remote system. This parameter is usually ignored in most time-sharing systems, but is used by terminal servers that offer reverse-LAT services.
- **unadvertised**—Prevents LAT service advertisements from being broadcast to the network.

Table 63 *X.25-to-PPP Outgoing Options***Outgoing PPP Translation****ppp** [*ip-address* | **ip-pool** [**scope-name** *name*]]

Translates from X.25 to virtual asynchronous PPP. Supply an IP address as a standard, four-part dotted-decimal IP address.

The **ip-pool** keyword obtains an IP address from a Dynamic Host Configuration Protocol (DHCP) proxy client or a local pool. If the optional **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

Outgoing PPP Connection Request Options

Any of the following optional keywords can be used to configure PPP connection requests:

- **authentication** {**pap** | **chap**}—Sets Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication for PPP on virtual asynchronous interfaces. If you specify both options, order is significant; the system will try to use the first authentication type, then the second.
- **header-compression**—Configures header compression on IP packets only.
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP over X.25 to connect through vtys on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the vty. The vty is assigned to the loopback interface.
- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on Serial Line Internet Protocol (SLIP) and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.

Table 63 X.25-to-PPP Outgoing Options (continued)

- **mtu bytes**—Sets the interface MTU of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
- **routing**—Permits routing updates between connections. This option is required if the destination device is not on a subnet connected to one of the interfaces on the router.
- **use-tacacs**—Uses TACACS to verify PPP authentications for CHAP or PAP on virtual asynchronous interfaces.

Table 64 X.25-to-SLIP Outgoing Options**Outgoing SLIP Translation**

slip {*ip-address* | **ip-pool** [*scope-name name*]}

Translates from X.25 to virtual asynchronous SLIP. Supply an IP address as a standard, four-part dotted-decimal IP address.

The **ip-pool** keyword obtains an IP address from a DHCP proxy client or a local pool. If the optional **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

Note The **slip** argument applies only to outgoing connections; SLIP is not supported on incoming protocol translation connections.

Outgoing SLIP Connection Request Options

Any of the following optional keywords can be used to configure SLIP connection requests:

- **header-compression** [**passive**]—Implements header compression on IP packets only. The **passive** keyword permits compression on outgoing packets only if incoming TCP packets on the same virtual asynchronous interface are compressed. The default (without the **passive** keyword) permits compression on all traffic.
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP over X.25 to connect through vty's on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the vty. The vty is assigned to the loopback interface.
- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on SLIP and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.
- **mtu bytes**—Sets the interface MTU of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
- **routing**—Permits routing updates between connections. This keyword is required if the destination device is not on a subnet connected to one of the interfaces on the router.

Table 65 **X.25-to-TCP Outgoing Options****Outgoing TCP Translation****tcp** *ip-address*

Translates X.25 to TCP/IP Telnet. Supply an IP address as a standard, four-part dotted-decimal IP address, or the name of an IP host that can be resolved by the DNS, or explicit specification in an **ip host** command (see the description for the **host-name** keyword in the “Outgoing TCP Connection Request Options” section).

Outgoing TCP Connection Request Options

Any of the following optional keywords can be used to configure TCP connection requests:

- **binary**—Negotiates Telnet binary mode on the connection.
- **host-name**—Stores the host name rather than its IP address, thereby allowing the host name to be resolved at connection time instead of configuration time. There is also a **rotor** keyword suboption that you can use to modify the behavior of the **host-name** keyword by allowing one of the IP addresses defined by the **ip host** configuration command to be chosen randomly. If one address fails, another one will be tried, and so on until all address choices are exhausted. You can use the **rotor** keyword, therefore, to provide basic load sharing of the IP destinations.
- **multibyte-IAC**—Always treat multiple Interpret as Command (IAC) escape character codes as a Telnet command.
- **port number**—For incoming connections, enter the number of the port to match. The default is port 23 (Telnet).
- **source-interface**—Specifies the source address used for Telnet connections initiated by the router.
- **stream**—Performs stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process or generate any Telnet options, and also prevents Telnet processing of the data stream. This option might be useful for connections to ports running UNIX-to-UNIX Copy Program (UUCP) or other non-Telnet protocols, or to ports connected to printers. For ports connected to printers using Telnet, the **stream** keyword prevents some of the problems associated with using Telnet for printers, such as unusual events happening to carriage returns or line feeds and echoing of data back to VPN/Security Management Solution (VMS) systems.

Protocol Translation and X.25 PVCs Functional Description

This section describes how the protocol translator works with X.25 PVCs. It will help you understand the overall behavior of incoming and outgoing X.25 PVCs associated with a **translate** command, enabling you to correctly configure protocol translator PVCs for your application.

Configuring X.25 PVCs

When the **translate x25** command is configured with a PVC, an attempt is made to create the PVC. The following conditions can cause this attempt to fail:

- The PVC number in the **translate x25** command is not within the range of logical channels defined for use by PVCs in the interface configuration.
- The PVC number in the **translate x25** command is already in use.
- An X.25 destination in a **translate x25** command is routed to X.25 over TCP/IP (XOT), Connection Mode Network Service (CMNS), or Annex G, which do not support translated PVCs.

PVC numbers must be unique across an X.25 connection; however, PVC 1 on serial interface 1/0 is different (and therefore unique) from PVC 1 on serial interface 2/1.

If, once the **translate x25** command is accepted, the X.25 interface on which the PVC is created goes down, the PVC enters an inactive state, the TCP or LAT connection is terminated, but the existing PAD context remains inactive.

An incoming TCP or LAT connection associated with a down outgoing PVC (displaying a “P/Inactive message”) will be rejected by the protocol translator.

If any X.25 traffic is received while the corresponding TCP or LAT connection is terminated, and if a data packet is received in state D1, a reset with a diagnostic message will be displayed, similar to the following:

```
20:17:11.809: Serial2: X.25 O D1 Reset (5) 8 lci 4
20:17:11.809: Cause 29, Diag 113 (Network out of order (PVC)/Remote network problem)
```

The number of outgoing and incoming protocol translation PVCs is limited only by the number of vtys supported on the Cisco router. Remember that each protocol translation session uses a vty, which lowers the number of vtys available for Telnet sessions.

By default, the Cisco router sends a reset packet with the cause “PVC Network Operational” and diagnostic “Maintenance action” messages at the start of a TCP or LAT to PVC translation session, to announce that the connection is established and that the PVC is able to handle data traffic. To suppress the PVC reset packet at TCP or LAT session startup, configure the **no-reset** outgoing PVC keyword as shown in the following example:

```
translate tcp 192.168.22.102 port 5 x25 333 pvc 5 no-reset profile tcl
```

Changing or Removing a translate Command PVC Configuration

Removing a **translate** command with an outgoing PVC specified is allowed only when there no active connection is associated with the outgoing PVC. An attempt to remove an active translation results in the following message:

```
Translate: Can't delete/add entry - Connection(s) are currently active
```

For example, if PVC 5 is assigned to a **translate** command as shown in the following example:

```
translate tcp 10.0.155.61 port 5 x25 5 pvc 5 interface Serial2/0
```

And you want PVC 5 to be assigned under an X.25 interface instead of the **translate** command, as shown in the following example:

```
interface serial2/0
  x25 pvc 5 int s4/0 pvc 25
```

Perform the following steps to configure this reassignment:

-
- Step 1** Check whether a PVC is associated with a serial connection using the **show x25 EXEC** command, as follows:

```
Router# show x25 vc 5

PVC 5, State:D1, Interface:Serial2/0
Started ...

Line:230 vty 4 Location:Host:nmos3m1
connected to PAD <--> X25
```

- Step 2** If the PVC is associated with a TCP connection, terminate the connection by disconnecting the TCP session or by using the **clear line EXEC** command as shown in the following example:

```
Router# clear line vty 4
```

Step 3 Enter configuration mode, delete the **translate** command, and reassign PVC 5 to an interface:

```
Router(config)# no translate tcp 10.0.155.61 port 5 x25 5 pvc 5 interface Serial12/0
Router(config)# interface serial12/0
Router(config-if)# x25 pvc 5 int s4/0 pvc 25
```

If you want to modify the **translate** command and change the PVC number from 5 to 12, follow steps 1 and 2, and modify the **translate** command with PVC 12, as follows:

```
Router(config)# translate tcp 10.0.155.61 port 12 x25 12 pvc 12 interface Serial12/0
```

Understanding the X.25 Address and the PVC Interface Option on a translate Command

The protocol translator locates the X.121 destination address in the X.25 route table to determine the interface on which to establish the PVC. A more up-to-date, simpler approach uses the **translate** command with the **interface** keyword, which ignores the status of the interface by avoiding referencing the X.25 route table.

For example, instead of configuring an **x25 route** command for each translated PVC, and entering a long X.121 address on the **translate** command, as shown this example:

```
x25 route ^32785223344502 interface Serial1/5
translate tcp 10.0.155.61 port 2502 x25 32785223344502 pvc 1
```

You can enter one **translate** command that links the IP port number with the X.121 address and specifies the interface on which to establish the PVC, as follows:

```
translate tcp 10.0.155.61 port 2502 x25 2502 pvc 1 interface Serial 1/5
```

This is the recommended approach and should be adopted in place of **translate** commands that cause the destination address to be looked up in the route table.

Examples

The following example shows how to use the **translate** global configuration command to translate from an X.25 PAD to a LAT device on Network A. It is applied to Router-A. The configuration example includes an access list that limits remote LAT access through Router-A to connections from PAD-C. This example typifies the use of access lists in the Cisco IOS software. The first two lines define the scope of access list 1. The first line specifies that access list 1 will permit all calls from X.121 address 44444. The caret symbol (^) specifies that the first number 4 is the beginning of the address number. The second line of the definition explicitly denies calls from any other number. (Refer to the appendix “Regular Expressions” in the *Cisco IOS Terminal Services Configuration Guide* for details concerning the use of special characters in defining X.121 addresses.)

```
! Define X25 access list to only allow pad-c.
x29 access-list 1 permit ^44444
x29 access-list 1 deny .*
!
! Set up translation.
translate x25 1111101 lat LAT-A access-class 1
```

The following example shows a simple X.25-to-TCP **translate x25** command. Packets coming in X.25 address 652365123 arrive via PVC 1 and are translated to TCP packets and sent out IP address 172.16.1.1.

```
translate x25 652365123 pvc 1 tcp 172.16.1.1
```

The following example shows a more complex configuration that calls an X.29 profile and swaps the default PAD operation of the router to that of an X.25 host. The name of the profile is fullpackets.

```
x29 profile fullpackets 2:0 3:0 4:100 7:21
translate x25 217536124 profile fullpackets tcp Host1 port 4006 swap
```

The following example shows the use of the X.25 incoming protocol **printer** keyword for an incoming X.25 connection:

```
translate x25 55555 printer tcp 172.16.1.1
```

The following examples causes the protocol translator to try connecting to IP address 172.16.1.1 and if that failed, to try IP address 172.16.2.1, and so on through all IP addresses listed in the **ip host** command:

```
ip host my-hosts 172.16.1.1 172.16.2.1 172.16.3.1
translate x25 55555 tcp my-hosts host-name
```

The following example uses the **rotor** keyword to cause the protocol translator to randomly choose one of the IP address listed in the **ip host** command and if it fails to connect, to try another IP address, until all are exhausted:

```
ip host my-hosts 172.16.1.1 172.16.2.1 172.16.3.1
translate x25 55555 tcp my-hosts host1 rotor
```

The following example translates X.25 packets to PPP. It enables routing updates between the two connections:

```
translate x25 12345678 ppp 10.0.0.2 routing
```

The following example permits clients running AppleTalk Remote Access (ARA) to connect through the virtual terminal lines of the device to an AppleTalk network:

```
appletalk routing
translate x25 12345678 autocommand arap
  arap enable
  arap dedicated
  arap timelimit 45
  arap warningtime 5
  arap noguest
  arap require-manual-password
  arap net-access-list 614
```

The following example specifies IP pooling from a DHCP server named D-Server1. It then specifies that incoming TCP traffic be translated to SLIP. The DHCP server will dynamically assign IP addresses on the outgoing sessions.

```
ip address-pool dhcp-proxy-client
ip dhcp-server D-Server1
translate x25 5467835 ppp ip-pool scope-name D-Server1
```

The following example specifies a local IP pool named Pool2 with IP addresses ranging from 172.18.10.10 to 172.18.10.110. It then specifies that incoming X.25 traffic be translated to PPP. The local IP pool Pool2 will be used to dynamically assign IP addresses on the outgoing sessions.

```
ip-pool Pool2 172.18.10.10 172.18.10.110
translate x25 1234567 ppp ip-pool scope-name Pool2
```

The following example shows how to set the idle timer. X.25 calls are cleared if they are idle for the configured time.

```
translate x25 1234 idle 2 lat Service3
```

The following example configures an X.25-to-TCP protocol translation session to insert an EOR marker in a TCP packet after each received X.25 packet that does not contain the M-bit set. The EOR marker in this example consists of printable characters.

```
translate x25 12345678 pvc 3 tcp 10.60.155.63 eor AAA insert
```

The following example uses the default authorization method list. Incoming PAD calls to the router on serial interface 1/1 are translated to Telnet calls to various destinations based on the X.25 subaddress. Use of the first two translate statements is restricted to users that are approved by the authorization server for access to group1; the third translate statement will complete the connection only if the authorization server grants access to group2.

```
aaa authorization network default group tacacs+
!
interface Serial1/1
 encapsulation x25
 x25 address 5551088
!
translate x25 555108801 tcp 10.60.155.1 login authorize default group1
translate x25 555108802 tcp 10.60.155.2 login authorize default group1
translate x25 555108803 tcp 10.60.155.3 login authorize default group2
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.
show translate	Displays configured translation sessions.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the translate command.

translate x25 (virtual access interfaces)

When receiving an X.25 connection request to a particular destination address, to set up the Cisco router to automatically translate the request to another outgoing protocol connection type, use the **translate x25** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

translate x25 *incoming-address* [*incoming-options* [**pvc number** [*pvc-options*]]] **virtual-template number** [*global-options*]

no translate x25 *incoming-address* [*incoming-options* [**pvc number** [*pvc-options*]]] **virtual-template number** [*global-options*]

Syntax Description	
<i>incoming-address</i>	An X.25 and X.121 address that conform to specifications provided in the <i>CCITT 1984 Red Book</i>. This address generally consists of a portion that is administered by the public data network (PDN) and a portion that is locally assigned. You must be sure that the numbers that you assign agree with the addresses assigned to you by the X.25 service provider. The X.121 addresses generally will be subaddresses of the X.121 address for the X.25 network interface. Typically, the interface address will be a 12-digit number. Any additional digits are interpreted as a subaddress. The PDN still routes these calls to the interface, and the Cisco IOS software is responsible for interpreting the extra digits. Do not use the same address on the interface and for translation.
<i>incoming-options</i>	(Optional) Incoming connection request keywords and arguments, as follows: • accept-reverse—Accepts reverse charged calls on an X.121 address even if the serial interface is not configured to accept reverse charged calls. This is an incoming option only. • cud c-u-data—Specifies the Call User Data (CUD) field to match in the X.25 Incoming Call packet. If not configured, the CUD in the Incoming Call packet must be blank. • printer—Supports LAT and TCP printing over an X.25 network among multiple sites. Provides an “interlock mechanism” between the acceptance of an incoming X.25 connection and the opening of an outgoing LAT or TCP connection. The printer keyword causes the protocol translation software to delay the call confirmation of an incoming X.25 call request until the outgoing protocol connection (to TCP or LAT) has been successfully established. An unsuccessful outgoing connection attempt to the router results in the incoming X.25 connection being refused, rather than being confirmed and then cleared, which is the default behavior. Note that using this keyword will force the global quiet keyword to be applied to the translation. • profile profile—Sets the X.3 PAD parameters as defined in the profile created by the x29 profile command.

pvc number [pvc-options]	• pvc number [interface serial number packetsize in-size out-size window-size in-size out-size]—Specifies that the outgoing connection is actually a PVC. The <i>number</i> argument specifies the virtual circuit channel number of the connection, which must be less than the virtual circuits assigned to the switched virtual circuit (SVC). Only one session is allowed per PVC. Use the following optional keywords and arguments to further define the connection: – interface serial number—Specifies a PVC interface on which to set up the PVC connection. – packetsize in-size out-size—Specifies the input packet size (<i>in-size</i>) and output packet size (<i>out-size</i>) for the PVC. Valid packet size values are as follows: 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096. – window-size in-size out-size—Specifies the packet count for input windows (<i>in-size</i>) and output windows (<i>out-size</i>) for the outgoing translation. Values of <i>in-size</i> and <i>out-size</i> range from 1 to 127 and must not be greater than the value set for the x25 modulo command. You must specify the same value for <i>in-size</i> and <i>out-size</i>.
virtual-template number	Applies the virtual interface template specified by the <i>number</i> argument in place of outgoing options.
<i>global-options</i>	(Optional) Translation options that can be used by any connection type and can be one or more of the following: • access-class number—Allows the incoming call to be used by source hosts that match the access list parameters. The argument <i>number</i> is an integer previously assigned to an access list. Standard access list numbers are in the range from 1 to 99; expanded standard access list numbers are in the range 1300 to 1999. • local—Allows Telnet protocol negotiations to <i>not</i> be translated. • login—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the login command. • max-users number—Limits the number of simultaneous users of the translation to <i>number</i> (an integer you specify). • quiet—Suppresses printing of user-information messages. • swap—Valid for X.25-to-TCP translations only, and allows X.3 parameters to be set on the router by the host originating the X.25 call, or by an X.29 profile. This keyword allows incoming and outgoing X.25 connections to be swapped so that the device is treated like a PAD when it accepts a call. By default, the router functions like a PAD for calls that it initiates, and like an X.25 host for calls it accepts. The swap keyword allows connections from an X.25 host that wants to connect to the router, and then treats it like a PAD.

Defaults

No default translation parameters.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The command syntax documented here shows how to apply a virtual interface template in place of outgoing **translate x25** options. If you are using virtual templates for protocol translation, all outgoing options are defined in the virtual interface template. [Table 66](#) lists all outgoing options and their corresponding interface configuration commands.

You define the protocol translation connections by choosing a protocol keyword and supplying the appropriate address or service name. The protocol connection information is followed by optional features for that connection, as appropriate. The global options, in general, apply to all the connection types, but there are exceptions. The **swap** keyword, for example, is for X.25- to-TCP translations only. See the example for more explanations on how to enter this command.

Rather than specifying outgoing translation options in the **translate** command, configure these options as interface configuration commands under the virtual interface template, then apply the virtual interface template to the **translate** command. [Table 66](#) maps outgoing **translate** command options to interface commands you can configure in the virtual interface template.

Table 66 Mapping Outgoing translate x25 Options to Interface Commands

translate x25 Command Options	Corresponding Interface Configuration Command
ip-pool	peer default ip address {ip-address dhcp pool [poolname]}
header-compression	ip tcp header compression [on off passive]
routing	ip routing or ipx routing
mtu	mtu
keepalive	keepalive
authentication {chap pap}	ppp authentication {chap pap}
ppp use-tacacs	ppp use-tacacs
ipx loopback	ipx ppp-client loopback number

Examples

The following example shows a virtual template with PPP encapsulation specified by default (not explicit). It also specifies CHAP authentication and an X.29 access list.

```
x29 access-list 1 permit ^5555
!
interface Virtual-Template1
 ip unnumbered Ethernet0
 peer default ip address 172.16.2.129
 ppp authentication chap
!
translate x25 5555667 virtual-template 1 access-class 1
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
show translate	Displays configured translation sessions.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection type.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection type.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the translate command.

transport-map type console

To create and name a transport map for console port access and enter transport map configuration mode, use the **transport-map type console** command in global configuration mode. To delete a transport map for console port access that was previously created, use the **no** form of this command.

transport-map type console *transport-map-name*

no transport-map type console *transport-map-name*

Syntax Description	<i>transport-map-name</i> Specifies the name of the transport map.				
Command Default	No transport maps are configured by default.				
Command Modes	Global configuration (config)				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>Cisco IOS XE Release 2.1</td><td>This command was introduced on the Cisco ASR 1000 Series Routers.</td></tr> </table>	Release	Modification	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.
Release	Modification				
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.				

Usage Guidelines	The characteristics of the transport map are defined in transport map configuration mode. The following options can be configured in transport map configuration mode: • connection wait—Specifies how a persistent Telnet or persistent SSH connection will be handled using this transport map. • banner [diagnostic wait]—Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of the persistent Telnet or persistent SSH configuration. See the command references for the individual options for additional information on a specific option. The transport map is not actively managing incoming console port connections until it is enabled using the transport type console <i>console-line-number</i> input <i>transport-map-name</i> global configuration command. The connection and banner settings of the transport map applied to the console port can be seen by entering the show platform software configuration access policy command.
-------------------------	---

Examples	In the following example, a transport map to set console port access policies is created and attached to console port 0.
-----------------	--

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
Welcome to diagnostic mode
```

```

X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS prompt
X
Router(config-tmap)# exit

Router(config)# transport type console 0 input consolehandler

```

Related Commands

Command	Description
banner (transport map)	Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of the transport map configuration.
connection wait	Specifies how an incoming connection will be handled.
show platform software configuration access policy	Displays the access policy and banner settings for console, Telnet, and SSH connections.
transport type console	Applies an already-configured console port transport map to a console interface.

transport-map type persistent

To create and name a transport map for persistent Telnet, SSH, or web user interface connections and enter transport map configuration mode, use the **transport-map type persistent** command in global configuration mode. To delete a previously created transport map for persistent Telnet, SSH, or web user interface connections, use the **no** form of this command.

transport-map type persistent [ssh | telnet | webui] *transport-map-name*

no transport-map type persistent [ssh | telnet | webui] *transport-map-name*

Syntax Description	ssh	Specifies a persistent SSH transport map.
	telnet	Specifies a persistent Telnet transport map.
	webui	Specifies a persistent web user interface transport map.
	<i>transport-map-name</i>	Specifies the name of the transport map.

Command Default No transport maps are configured by default.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

The characteristics of the transport map are defined in transport map configuration mode.

The following commands can be configured in persistent Telnet and SSH transport map configuration mode:

- **connection wait**—Specifies how a persistent Telnet or persistent SSH connection will be handled using this transport map.
- **rsa keypair-name**—Names the RSA keypair to be used for persistent SSH connections.
- **banner [diagnostic | wait]**—Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of the persistent Telnet or persistent SSH configuration.
- **time-out**—Specifies the SSH timeout interval in seconds.
- **transport interface**—Applies the transport map settings to the interface. For the Cisco ASR 1000 Series Routers, transport maps for persistent Telnet or persistent SSH handling can only be attached to the Management Ethernet interface, so the only possible value for this option is **transport interface gigabitethernet 0**. This is a required step for persistent SSH and persistent Telnet transport maps.
- **authentication-retries**—Specifies the number of authentication retries before dropping the connection.

The following commands can be configured in persistent web user interface transport map configuration mode:

- **server**—Enables the HTTP server for the transport map.
- **secure-server**—Enables the secure HTTP (HTTPS) server for the transport map.

The transport map is not actively managing incoming Telnet or SSH connections until it is applied to an interface and enabled. This command is used to apply a transport map to an interface, and the **transport type persistent telnet input** global configuration command is used to enable the transport map.

This command is currently only available for Cisco ASR 1000 Series Routers, and transport maps can be applied only to the Management Ethernet interface (interface gigabitethernet 0) on Cisco ASR 1000 Series Routers.

Examples

In the following example, a transport map that will make all Telnet connections wait for the IOS process to become active before connecting to the router, while also allowing the user to interrupt the process and enter diagnostic mode, is configured and applied to the Management Ethernet interface (interface gigabitethernet 0).

A diagnostic and a wait banner are also configured.

The transport map is then applied to the interface when the **transport type persistent telnet input** command is entered to enable persistent Telnet.

```
Router(config)# transport-map type persistent telnet telnethandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for IOS Process--
X

Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler
```

In the following example, a transport map is configured that applies the following settings to any users attempting to access the Management Ethernet port via SSH:

- Users using SSH wait for the IOS process to become active, but enter diagnostic mode if the attempt to access IOS is interrupted.
- The RSA keypair name is “sshkeys.”
- The connection allows one authentication retry.
- The banner “--Welcome to Diagnostic Mode--” appears if diagnostic mode is entered as a result of SSH handling through this transport map.
- The banner “--Waiting for IOS Process--” appears if the connection is waiting for the IOS process to become active.

The transport map is then applied to the interface when the **transport type persistent ssh input** command is entered to enable persistent SSH.

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# rsa keypair-name sshkeys
```

```

Router(config-tmap)# authentication-retries 1
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for IOS Process--
X
Router(config-tmap)# time-out 30
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit

Router(config)# transport type persistent ssh input sshhandler

```

In the following example, this command is used to create a web user interface transport map using the default HTTP port.

```

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip http server
Router(config)# transport-map type persistent webui http-webui
Router(config-tmap)# server
Router(config-tmap)# exit
Router(config)# transport type persistent webui input http-webui
*Apr 22 02:43:55.798: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd: Server wui has been
notified to start

```

Related Commands

Command	Description
authentication-retries	Specifies the number of SSH authentication retries before dropping the connection when a persistent SSH transport map is applied to the receiving interface.
banner (transport map)	Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of the transport map configuration.
connection wait	Specifies how an incoming connection will be handled.
rsa keypair-name	Names the RSA keypair to be used for persistent SSH connections.
server (transport map)	Enables the HTTP server for a persistent web user interface transport map.
secure-server	Enables the HTTPS server for a persistent web user interface transport map.
show platform software configuration access policy	Displays the access policy and banner settings for console, Telnet, and SSH connections.
time-out	Specifies the SSH timeout interval in seconds.
transport interface	Applies the transport map settings to the interface.
transport type persistent	Applies an already-configured persistent transport map to an interface.

transport input

To define which protocols to use to connect to a specific line of the router, use the **transport input** command in line configuration mode. To change or remove the protocol, use the **no** form of this command.

transport input {all | lat | mop | nasi | none | pad | rlogin | ssh | telnet | v120}

no transport input {all | lat | mop | nasi | none | pad | rlogin | ssh | telnet | v120}

Syntax Description

all	Selects all protocols.
lat	Selects the digital (Local-Area Transport) LAT protocol and specifies both incoming reverse LAT and host-initiated connections.
mop	Selects Maintenance Operation Protocol (MOP).
nasi	Select NetWare Access Servers Interface (NASI) as the input transport protocol.
none	Prevents any protocol selection on the line. This makes the port unusable by incoming connections.
pad	Selects X.3 packet assembler/disassembler (PAD) incoming connections.
rlogin	Selects the UNIX rlogin protocol.
ssh	Selects the Secure Shell (SSH) protocol.
telnet	Specifies all types of incoming TCP/IP connections.
v120	Selects the V.120 protocol for incoming asynchronous connections over ISDN.

Defaults

No protocols allowed on the line (**none**).

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1	The none keyword was added and became the default. Before Cisco IOS Release 11.1, the default keyword was all .
12.3(4)T	The ssh keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Cisco routers do not accept incoming network connections to asynchronous ports (TTY lines) by default. You must specify an incoming transport protocol or specify the **transport input all** command before the line will accept incoming connections. For example, if you are using your router as a terminal server to make console-port connections to routers or other devices, you will not be able to use Telnet to connect to these devices. You will receive the message “Connection Refused.” This behavior is new as of

Cisco IOS software Release 11.1. Previous to Release 11.1, the default was the **transport input all** command, and the **all** keyword restored pre-Cisco IOS software Release 11.0 defaults. If you are upgrading to Cisco IOS software Release 11.1(1) or later releases from earlier Cisco IOS software releases, you must configure the **transport input** {*protocol* | **all**} command, or you will be locked out of your router.

You can specify one protocol, multiple protocols, all protocols, or no protocols. To specify multiple protocols, enter the keyword for each protocol, separated by a space.

This command can be useful in distributing resources among different types of users, or in making certain that only specific hosts can access a particular port. When using two-step protocol translation, the **transport input** command is useful in controlling exactly which protocols can be translated to other protocols.

Access lists for each individual protocol can be defined in addition to the allowances created by the **transport input** command. Any settings made with the **transport input** command override settings made with the **transport preferred** command.

Examples

The following example sets the incoming protocol to Telnet for virtual terminal lines 0 to 32:

```
line vty 0 32
 transport input telnet
```

Related Commands

Command	Description
transport output	Determines the protocols that can be used for outgoing connections from a line.
transport preferred	Specifies the transport protocol that the Cisco IOS software uses if the user does not specify one when initiating a connection.

transport interface

To specify the interface where a transport map should be applied, use the **transport interface** command in transport map configuration mode command. To restore the default setting where no interface is associated with the transport map, use the **no** form of this command.

transport interface *interface-type interface-number*

no transport interface *interface-type interface-number*

Syntax Description

<i>interface-type</i>	Specifies the type of interface where the transport map will be applied. For persistent Telnet and persistent SSH on the Cisco ASR 1000 Series Routers, transport maps can only be attached to the Management Ethernet interface (gigabitethernet 0). Therefore, gigabitethernet is the only available <i>interface-type</i> for persistent SSH and persistent Telnet on the Cisco ASR 1000 Series Routers.
<i>interface-number</i>	Specifies the interface number. For persistent Telnet and persistent SSH on the Cisco ASR 1000 Series Routers, transport maps can only be attached to the Management Ethernet interface (gigabitethernet 0). Therefore, 0 is the only available <i>interface-number</i> for persistent SSH and persistent Telnet on the Cisco ASR 1000 series routers.

Command Default

No transport maps are associated with any interfaces by default.

Command Modes

Transport map configuration (config-tmap)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

For persistent SSH and persistent Telnet on the Cisco ASR 1000 Series Router, the only interface that can accept a persistent SSH or persistent Telnet transport map is **gigabitethernet 0**.

For a transport map to be associated with an interface, this command must specify the interface for the transport map, and the **transport type persistent** global configuration must be entered to enable the transport map. If this command is not used in a transport map, the transport map is not applied to any interface and therefore has no effect on the handling of any incoming persistent Telnet or persistent SSH traffic.

Examples

In the following example, a transport map that will make all Telnet connections wait for the IOS process to become active before connecting to the router, while also allowing the user to interrupt the process and enter diagnostic mode, is configured and applied to the Management Ethernet interface (interface gigabitethernet 0).

A diagnostic and a wait banner are also configured.

The transport map is then applied to the interface when the **transport type persistent telnet input** command is entered to enable persistent Telnet.

```
Router(config)# transport-map type persistent telnet telnethandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for IOS Process--
X

Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler
```

In the following example, a transport map is configured that applies the following settings to any users attempting to access the Management Ethernet port via SSH:

- Users using SSH wait for the IOS process to become active, but enter diagnostic mode if the attempt to access IOS is interrupted.
- The RSA keypair name is “sshkeys”.
- The connection allows one authentication retry.
- The banner “--Welcome to Diagnostic Mode--” appears if diagnostic mode is entered as a result of SSH handling through this transport map.
- The banner “--Waiting for IOS Process--” appears if the connection is waiting for the IOS process to be come active.

The transport map is then applied to the interface when the **transport type persistent ssh input** command is entered to enable persistent SSH.

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# authentication-retries 1
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for IOS Process--
X
Router(config-tmap)# time-out 30
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit

Router(config)# transport type persistent ssh input sshhandler
```

Related Commands

Command	Description
authentication-retries	Specifies the number of SSH authentication retries before dropping the connection when a persistent SSH transport map is applied to the receiving interface.
banner (transport map)	Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of the transport map configuration.
connection wait	Specifies how an incoming connection will be handled.
rsa keypair-name	Names the RSA keypair to be used for persistent SSH connections.
show platform software configuration access policy	Displays the access policy and banner settings for console, Telnet, and SSH connections.
time-out	Specifies the SSH timeout interval in seconds.
transport type persistent	Applies an already-configured persistent transport map to an interface.
transport-map type persistent	Creates and names a persistent transport map and enters transport map configuration mode.

transport output

To determine the protocols that can be used for outgoing connections from a line, use the **transport output** command in line configuration mode. To change or remove the protocol, use the **no** form of this command.

transport output { **all** | **lat** | **mop** | **nasi** | **none** | **pad** | **rlogin** | **telnet** | **v120** }

no transport output { **all** | **lat** | **mop** | **nasi** | **none** | **pad** | **rlogin** | **telnet** | **v120** }

Syntax Description		
all		Selects all protocols.
lat		Selects the Digital LAT protocol, which is the protocol used most often to connect routers to Digital hosts.
mop		Selects Maintenance Operation Protocol (MOP).
nasi		Selects NetWare Access Server Interface (NASI) as the output transport protocol.
none		Prevents any protocol selection on the line. The system normally assumes that any unrecognized command is a host name. If the protocol is set to none , the system no longer makes that assumption. No connection will be attempted if the command is not recognized.
pad		Selects X.3 packet assembler/disassembler (PAD), used most often to connect routers to X.25 hosts.
rlogin		Selects the UNIX rlogin protocol for TCP connections. The rlogin setting is a special case of Telnet. If an rlogin attempt to a particular host has failed, the failure will be tracked, and subsequent connection attempts will use Telnet instead.
telnet		Selects the TCP/IP Telnet protocol. It allows a user at one site to establish a TCP connection to a login server at another site.
v120		Selects the V.120 protocol for outgoing asynchronous connections over ISDN.

Defaults	Telnet
-----------------	--------

Command Modes	Line configuration
----------------------	--------------------

Command History	Release	Modification
	10.0	This command was introduced.

Release	Modification
11.1	The following keywords were added: • all • lat • pad • rlogin • v120
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can specify one protocol, multiple protocols, all protocols, or no protocols. To specify multiple protocols, enter the keyword for each protocol, separated by a space.

Any settings made with the **transport output** command override settings made with the **transport preferred** command.

Examples

The following example prevents any protocol selection:

```
transport output none
```

Related Commands

Command	Description
transport input	Defines which protocols to use to connect to a specific line of the router.
transport preferred	Specifies the transport protocol that the Cisco IOS software uses if the user does not specify one when initiating a connection.

transport preferred

To specify the transport protocol that the Cisco IOS software uses if the user does not specify one when initiating a connection, use the **transport preferred** command in line configuration mode. To change or remove the protocol, use the **no** form of this command.

transport preferred {lat | mop | nasi | none | pad | rlogin | telnet | v120}

no transport preferred {lat | mop | nasi | none | pad | rlogin | telnet | v120}

Syntax Description		
lat		Selects the Digital LAT protocol, which is the protocol used most often to connect routers to Digital hosts.
mop		Selects Maintenance Operation Protocol (MOP).
nasi		Selects NetWare Access Server Interface (NASI) protocol.
none		Prevents any protocol selection on the line. The system normally assumes that any unrecognized command is a host name. If the protocol is set to none , the system no longer makes that assumption. No connection is attempted if the command is not recognized.
pad		Selects X.3 packet assembler/disassembler (PAD), used most often to connect routers to X.25 hosts.
rlogin		Selects the UNIX rlogin protocol for TCP connections. The rlogin setting is a special case of Telnet. If an rlogin attempt to a particular host has failed, the failure will be tracked, and subsequent connection attempts will use Telnet instead.
telnet		Selects the TCP/IP Telnet protocol. It allows a user at one site to establish a TCP connection to a login server at another site.
v120		Selects the asynchronous protocols over ISDN.

Defaults	Telnet
-----------------	--------

Command Modes	Line configuration
----------------------	--------------------

Command History	Release	Modification
	10.0	This command was introduced.
	11.1	The following keywords were added: • lat • pad • rlogin
	12.4	The all keyword is no longer supported.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Specify the **transport preferred none** command to prevent errant connection attempts.

Any settings made with the **transport input** or **transport output** commands override settings made with the **transport preferred** command.

Examples

The following example sets the preferred protocol to Telnet on physical terminal line 1:

```
line tty 1
  transport preferred telnet
```

Related Commands

Command	Description
terminal transport preferred	Specifies the preferred protocol to use for the current session when a command does not specify one.
transport input	Defines which protocols to use to connect to a specific line of the router.
transport output	Determines the protocols that can be used for outgoing connections from a line.

transport type console

To enable an already configured console port transport map, use the **transport type console** command in global configuration mode. To disable a previously enabled console port transport map, use the **no** form of this command.

transport type console *console-line-number* **input** *transport-map-name*

no transport type console *console-line-number* **input**

Syntax Description

<i>console-line-number</i>	The console port or line number.
input	Specifies that the transport map settings are applied to traffic entering the interface. Transport maps for console port handling are only applied in the input direction.
<i>transport-map-name</i>	Specifies the name of the transport map to attach to the interface.

Command Default

No transport maps are configured or applied to interfaces by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

A transport map is not actively managing incoming console port connections until it is enabled. This command enables the transport map.

Transport maps for console ports are created using the **transport-map type console** command. The *transport-map-name* in the **transport -map type console** command and this command must match in order to properly apply the transport map to the console interface.

Examples

In the following example, a transport map to set console port access policies is created and attached to console port 0.

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
Welcome to diagnostic mode
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS prompt
X
```



```
Router(config-tmap)# exit
```

```
Router(config)# transport type console 0 input consolehandler
```

Related Commands

Command	Description
banner (transport map)	Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of the transport map configuration.
connection wait	Specifies how an incoming connection will be handled.
show platform software configuration access policy	Displays the access policy and banner settings for console, Telnet, and SSH connections.
transport-map type console	Creates and names a transport map for the console port and enters transport map configuration mode.

transport type persistent

To enable an already configured persistent Telnet, SSH, or web user interface transport map, use the **transport type persistent** command in global configuration mode. To disable a previously enabled persistent Telnet, SSH, or web user interface transport map, use the **no** form of this command.

transport type persistent [ssh | telnet | webui] **input** *transport-map-name*

no transport type persistent [ssh | telnet | webui] **input**

Syntax Description	ssh	Specifies a persistent SSH transport map.
	telnet	Specifies a persistent Telnet transport map.
	webui	Specifies a persistent web user interface transport map.
	input	Specifies that the transport map settings are only applied to traffic entering the interface. Transport maps for persistent SSH or persistent Telnet handling are only applied in the input direction.
	<i>transport-map-name</i>	Specifies the name of the transport map to attach to the interface.

Command Default No transport maps are configured or applied to interfaces by default.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

A transport map is not actively managing incoming Telnet, SSH, or web user interface traffic until it is enabled. This command enables the transport map.

Transport maps for persistent SSH, Telnet, or the web user interface are created using the **transport-map type persistent** command. The *transport-map-name* in the **transport-map type persistent** command and this command must match in order to properly apply the transport map to the interface.

For a persistent Telnet or SSH transport map to be active, the **transport interface** transport map configuration command must define the interface for the transport map, and this command must be entered to enable the transport map. The **transport interface** step is not part of the process for persistent web user interface transport maps.

This command is currently only available for Cisco ASR 1000 Series Routers, and transport maps can be applied only to the Management Ethernet interface (**interface gigabitethernet 0**) on Cisco ASR 1000 Series Routers.

Examples

In the following example, a transport map that will make all Telnet connections wait for the IOS process to become active before connecting to the router, while also allowing the user to interrupt the process and enter diagnostic mode, is configured and applied to the Management Ethernet interface (interface gigabitethernet 0).

A diagnostic and a wait banner are also configured.

The transport map is then applied to the interface when the **transport type persistent telnet input** command is entered to enable persistent Telnet.

```
Router(config)# transport-map type persistent telnet telnethandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for IOS Process--
X

Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler
```

In the following example, a transport map is configured that applies the following settings to any users attempting to access the Management Ethernet port via SSH:

- Users using SSH wait for the IOS process to become active, but enter diagnostic mode if the attempt to access IOS is interrupted.
- The RSA keypair name is “sshkeys.”
- The connection allows one authentication retry.
- The banner “--Welcome to Diagnostic Mode--” appears if diagnostic mode is entered as a result of SSH handling through this transport map.
- The banner “--Waiting for IOS Process--” appears if the connection is waiting for the IOS process to become active.

The transport map is then applied to the interface when the **transport type persistent ssh input** command is entered to enable persistent SSH.

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# authentication-retries 1
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
--Waiting for IOS Process--
X
Router(config-tmap)# time-out 30
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit

Router(config)# transport type persistent ssh input sshhandler
```

In the following example, this command is used to enable a persistent web user interface transport map using the default HTTP port:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip http server
Router(config)# transport-map type persistent webui http-webui
Router(config-tmap)# server
Router(config-tmap)# exit
Router(config)# transport type persistent webui input http-webui
*Apr 22 02:43:55.798: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd: Server wui has been
notified to start
```

Related Commands

Command	Description
authentication-retries	Specifies the number of SSH authentication retries before dropping the connection when a persistent SSH transport map is applied to the receiving interface.
banner (transport map)	Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of the transport map configuration.
connection wait	Specifies how an incoming connection will be handled.
rsa keypair-name	Names the RSA keypair to be used for persistent SSH connections.
secure-server	Enables the secure HTTP (HTTPS) server for a persistent web user interface transport map.
server (transport map)	Enables the HTTP server for a persistent web user interface transport map.
show platform software configuration access policy	Displays the access policy and banner settings for console, Telnet, and SSH connections.
time-out	Specifies the SSH timeout interval in seconds.
transport interface	Applies the transport map settings to the interface.
transport-map type persistent	Creates and names a persistent transport map and enters transport map configuration mode.

ttycap

To define characteristics of a terminal emulation file, use the **ttycap** command in global configuration mode. To delete any named ttycap entry from the configuration file, the **no** form of this command.

ttycap *tycap-name termcap-entry*

no ttycap *tycap-name*

Syntax Description

<i>tycap-name</i>	Name of a file. It can be up to 32 characters long and must be unique.
<i>termcap-entry</i>	Commands that define the ttycap. Consists of two parts. (See the “Usage Guidelines” section for details.)

Defaults

VT100 terminal emulation

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ttycap EXEC** command to test for the availability of a ttycap.



Note

Do not type a ttycap entry filename “default” or the Cisco IOS software will adopt the newly defined entry as the default.

The *termcap-entry* argument consists of two parts: a name portion and a capabilities portion.

The name portion is a series of names that can be used to refer to a specific terminal type. Generally, these names should represent commonly recognized terminal names (such as VT100 and VT200). Multiple names can be used. Each name is separated by a vertical bar symbol (|). The series is terminated by a colon symbol (:).

The following example illustrates a name specification for a VT100 termcap:

```
d0|vt100|vt100-am|vt100am|dec vt100:
```

The capabilities portion of the termcap entry consists of a sequence of termcap capabilities. These capabilities can include Boolean flags, string sequences, or numeric sequences. Each individual capability is terminated using a colon symbol (:). A Boolean flag can be set to true by including the two-character capability name in the termcap entry. The absence of any supported flag results in the flag being set to false.

The following is an example of a backspace Boolean flag:

bs:

A string sequence is a two-character capability name followed by an equal sign (=) and the character sequence.

The following example illustrates the capability for homing the cursor:

ho=\E[H:

The sequence \E represents the ESC character.

Control characters can be represented in string sequences by entering a two-character sequence starting with a caret symbol (^), followed by the character to be used as a control character.

The following example illustrates the definition of a control character.

bc=^h:

In this example, the backspace is entered into the termcap entry as the string sequence as the characters “^h.”

A numeric sequence is a two-character capability name followed by a number symbol (#) and the number.

The following example represents the number of columns on a screen.

co#80:

Use the backslash symbol (\) to extend the definition to multiple lines. The end of the ttycap termcap entry is specified by a colon terminating a line followed by an end-of-line character and no backslash.

For the definitions of supported Boolean-flag ttycap capabilities, see [Table 67](#). For the definitions of supported string-sequence ttycap capabilities, see [Table 68](#). For the definitions of supported number-sequence ttycap capabilities, see [Table 69](#). For the definitions of supported color-sequence ttycap capabilities, see [Table 70](#).

Table 67 **Definitions of ttycap Capabilities: Boolean Flags**

Boolean Flag	Description
am	Automatic margin
bs	Terminal can backspace with bs
ms	Safe to move in standout modes
nc	No currently working carriage return
xn	NEWLINE ignored after 80 columns (Concept)
xs	Standout not erased by overwriting (Hewlett-Packard)

Table 68 **Definitions of ttycap Capabilities: String Sequences**

String Sequence	Description
AL	Add line below with cursor sequence
bc	Backspace if not ^h
bt	Backtab sequence
ce	Clear to end of line

Table 68 **Definitions of ttycap Capabilities: String Sequences (continued)**

String Sequence	Description
cl	Clear screen, cursor to upper left
cm	Move cursor to row number and column number
cr	Carriage return sequence
cs	Change scrolling region
DL	Delete the line the cursor is on
ei	End insert mode
ho	Home, move cursor to upper left
ic	Character insert
im	Begin insert mode
is	Initialization string (typically tab stop initialization)
ll	Move cursor to lower left corner
md	Turn on bold (extra bright) character attribute
me	Turn off all character attributes
nd	Nondestructive space
nl	Newline sequence
pc	Pad character if not NULL
rc	Restore cursor position
rs	Resets terminal to known starting state
sc	Save cursor position
se	End standout mode (highlight)
so	Start standout mode (highlight)
ta	Tab
te	End programs that use cursor motion
ti	Initialization for programs that use cursor motion
uc	Underline character at cursor
ue	End underline mode
up	Move cursor up
us	Begin underline mode
vb	Visual bell
vs	Visual cursor
ve	Normal cursor

Table 69 Definitions of ttycap Capabilities: Number Sequences

Number Sequence	Description
li	Lines on the screen
co	Columns on the screen
sg	Standout glitch, number of spaces printed when entering or leaving standout display mode
ug	Underline glitch, number of spaces printed when entering or leaving underline mode

Table 70 Definitions of ttycap Capabilities: Color Sequences

Color Sequence	Description
x0	Black
x1	Blue
x2	Red or orange
x3	Pink or purple
x4	Green, which is the default color
x5	Turquoise
x6	Yellow
x7	Gray or white

The ttycap database uses these color sequences to translate IBM directives into screen drawing commands. These color sequences control only foreground terminal colors. They do not control background color, which is configured to black by default.

Examples

The following is an example of a ttycap file. Refer to the “Configuring Dial-In Terminal Services” chapter in the *Cisco IOS Terminal Services Configuration Guide* and the *tn3270.examples* file in the *Cisco ftp@cisco.com* directory for more examples.

```

ttycap ttycap1\
d0|vt100|vt100-am|vt100am|dec vt100:do=^J:co#80:li#24:\
cl=50^[[;H^[[2J:bs:am:cm=5^[[;%i%d;%dH:nd=2^[[C:up=2^[[A:\
ce=3^[[K:so=2^[[7m:se=2^[[m:us=2^[[4m:ue=2^[[m:md=2^[[1m:\
me=2^[[m:ho=^[[H:xn:sc=^[[7:rc=^[[8:cs=^[[;%i%d;%dr:

```

Related Commands

Command	Description
keymap-type	Specifies the keyboard map for a terminal connected to the line.
terminal-type	Specifies the type of terminal connected to a line.

txspeed

To set the terminal transmit speed (how fast the terminal sends information to the modem), use the **txspeed** command in line configuration mode. To return to the default setting, use the **no** form of this command.

txspeed *bps*

no txspeed

Syntax Description	<i>bps</i>	Baud rate, in bits per second (bps). The default value is 9600 bps.
---------------------------	------------	---

Defaults	9600 bps
-----------------	----------

Command Modes	Line configuration
----------------------	--------------------

Command History	Release	Modification
	10.0	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	Set the speed to match the baud rate of whatever device you have connected to the port. Some baud rates available on devices connected to the port might not be supported on the router. The Cisco IOS software will indicate if the speed you select is not supported.
-------------------------	---

**Note**

If the line was previously configured for automatic baud rate detection (autobaud), disable autobaud by entering the **no autobaud** command before entering the **txspeed** command to fix the speed of the port.

Examples	The following example sets the transmit speed for line 5 to 2400 bps:
-----------------	---

```
line 5
txspeed 2400
```

Related Commands	Command	Description
	rotary-group	Sets the terminal receive speed (how fast the terminal receives information from the modem).
	source template	Sets the flow control start character.
	terminal txspeed	Sets the terminal transmit speed (how fast the terminal can send information) on the current line and session.

where

To list the open sessions, use the **where** command in EXEC mode.

where

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced in a release prior to Cisco IOS Release 10.0.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines The **where** command displays all open sessions associated with the current terminal line.

The break (Ctrl-Shift-6, x), **where**, and **resume** commands are available with all supported connection protocols.

Examples The following is sample output from the **where** command:

```
Router# where
Conn Host          Address           Byte    Idle  Conn Name
  1 MATHOM          192.31.7.21       0        0    MATHOM
* 2 CHAFF           131.108.12.19     0        0    CHAFF
```

The asterisk (*) indicates the current terminal session.

[Table 71](#) describes the fields shown in the display.

Table 71 *where Field Descriptions*

Field	Description
Conn	Name or address of the remote host to which the connection is made.
Host	Remote host to which the router is connected through a Telnet session.
Address	IP address of the remote host.
Byte	Number of unread bytes for the user to see on the connection.
Idle	Interval (in minutes) since data was last sent on the line.
Conn Name	Assigned name of the connection.

Related Commands

Command	Description
show line	Displays information about all lines on the system or the specified line.
show sessions	Displays information about open LAT, Telnet, or rlogin connections.

x25 pvc translate ruleset

To configure the permanent virtual circuits (PVCs) that are valid for protocol translation ruleset handling, use the **x25 pvc translate ruleset** command in interface configuration mode. To remove or change the configuration, use the **no** form of this command.

x25 pvc number translate ruleset [*name* | *x121-address* | **packetsize** *in-size out-size* | **window**
size in-size out-size]

no x25 pvc number translate ruleset [*name* | *x121-address* | **packetsize** *in-size out-size* |
window*size in-size out-size*]

Syntax Description		
	<i>number</i>	PVC number to reserve for protocol translation ruleset handling.
	<i>name</i>	(Optional) Ruleset name specified by the translate ruleset command that governs the PVC.
	<i>x121-address</i>	(Optional) Destination host address.
	packetsize <i>in-size out-size</i>	(Optional) Specifies the input packet size (<i>in-size</i>) and output packet size (<i>out-size</i>) for the PVC. Valid packet size values are: 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096.
	window <i>size in-size out-size</i>	(Optional) Specifies the packet count for input windows (<i>in-size</i>) and output windows (<i>out-size</i>) for the outgoing translation. Values of the <i>in-size</i> and <i>out-size</i> arguments range from 1 to 127 and must not be greater than the value set for the x25 modulo command.
	Note	You must specify the same value for the <i>in-size</i> and <i>out-size</i> arguments.

Defaults No default behavior or values

Command Modes Interface configuration

Command History	Release	Modification
	12.3(8)T	This command was introduced.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines If the optional name or X.121 address is given, PVC usage is restricted to the translation ruleset of that name.

Examples The following example shows how to reserve a PVC for protocol translation ruleset handling, and select the outbound X.25 serial interface and PVC number based on the IP port number:

```

interface serial 2/0
x25 pvc 4 translate ruleset port_to_pvc
!
translate use telnet 10.10.1.6
!
translate ruleset port_to_pvc from telnet to pad
match dest-addr ^10.10.1.6$ dest-port ^[12]00[0-7][1-3]$
substitute telnet dest-port ^..0([0-7]) into pad interface serial 0/\1
substitute telnet dest-port ^....(.) into pad pvc \1
test telnet dest-port ^.0... set pad profile TEMS
test telnet dest-port ^.1... set pad profile SQAS
test telnet dest-port ^.2... set pad profile NMA
substitute telnet dest-port (.)$ into pad dest-addr 876543\1

x.29 profile TEMS 2:0 3:128 4:0
x.29 profile SQAS 2:0 3:128 4:0
x.29 profile NMA 2:0 3:128 4:0

```

Related Commands

Command	Description
description (ruleset)	Adds a description about a translation ruleset.
match (ruleset)	Identifies a connection for processing by the translation ruleset.
options (ruleset)	Specifies protocol translation options in a translation ruleset.
set (ruleset)	Unconditionally sets one or more connection parameters to a fixed value for a translation ruleset.
show translate ruleset	Displays a summary of a specific or of all configured translation rulesets, behavioral parameters, and usage statistic.
skip (ruleset)	Identifies a connection for omission by the translation ruleset.
substitute (ruleset)	Matches an available protocol and substitutes another in a translation ruleset.
test (ruleset)	Tests parameter values in a translation ruleset using regular expressions.
test translate	Displays a trace of protocol translation behavior for a connection attempt.
translate ruleset	Defines a unique name for a translation ruleset, specifies translated protocols, and enters translate ruleset configuration mode.

x25 subaddress

To append either a physical port number or a value specified for a line as a subaddress to the X.121 calling address, use the **x25 subaddress** command in line configuration mode. To disable subaddressing, use the **no** form of this command.

x25 subaddress {*line* | *number*} [**no-zero-pad**]

no x25 subaddress {*line* | *number*}

Syntax Description

line	Physical port number for the indicated line to be appended to the X.121 address as the subaddress.
<i>number</i>	Numeric variable assigned to a specific line.
no-zero-pad	(Optional) Specifies that a leading zero should not be appended to subaddresses with a value of nine or lower (0–9).

Defaults

No default behavior or values

Command Modes

Line configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.3(2)T	The no-zero-pad keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **x25 subaddress line** command to create a unique X.121 calling address by adding either a physical port number or a numeric value for a line as a subaddress to the X.121 calling address.

Use the **no-zero-pad** option to eliminate the inclusion of a leading zero for subaddresses with a value of nine or lower (0–9).

Examples

The following example shows how to configure subaddressing on virtual terminal lines 10 through 20 by appending the line number as a subaddress to the X.121 calling address:

```
line vty 10 20
 x25 subaddress line
```

The following example shows how to configure subaddressing on the first five tty lines by appending the value 09 as a subaddress to the X.121 calling address of an X.28 connection originating on these lines:

```
line 1 5
x25 subaddress 9
autocommand x28
```

The following example configures a subaddress of 6 for a set of vty lines, and specifies that a leading zero should not be appended to the subaddress value:

```
line vty 0 9
x25 subaddress 6 no-zero-pad
```

Related Commands

Command	Description
line	Identifies a specific line for configuration and starts the line configuration command collection mode.

x28

To enter X.28 mode and access an X.25 network or set X.3 packet assembler/disassembler (PAD) parameters, use the **x28** command in EXEC mode. To exit X.28 mode, use the **no** form of this command.

x28 [**escape** *character-string*] [**noescape**] [**nuicud**] [**profile** *file-name*] [**reverse**] [**verbose**]

no x28 [**escape** *character-string*] [**noescape**] [**nuicud**] [**profile** *file-name*] [**reverse**] [**verbose**]

Syntax Description

escape <i>character-string</i>	(Optional) Specifies a character string to use to exit X.28 mode and return to EXEC mode. The character string can be any string of alphanumeric characters. The Ctrl key can be used in conjunction with the character string.
noescape	(Optional) Specifies that no escape character string is defined (user cannot return to EXEC mode). On the console line, the noescape option is ignored, and the default escape sequence is used (exit command).
nuicud	(Optional) Specifies the network user identification (NUI) data to not be placed in the NUI facility of the call request. Instead the data is placed in the Call User Data (CUD) area of the call request packet.
profile <i>file-name</i>	(Optional) Specifies using a user-configured profile of X.3 parameters. A profile is created with the x29 profile EXEC command.
reverse	(Optional) Specifies reverse charges for outgoing calls made from the local router to the destination device.
verbose	(Optional) Displays optional service signals such as the called DTE address, facility block, and CUD.

Defaults

Disabled. X.28 mode uses standard X.28 command syntax.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

If both the **escape** and **noescape** options are not set, the default escape sequence is used (**exit** command).

X.28 mode is identified with an asterisk (*) router prompt. After you enter this mode, the standard X.28 user interface (with the exception of the escape sequence) is available. From this interface, you can configure a PAD device using X.3 parameters, or you can access an X.25 network.

In X.28 mode, you can set PAD command signals using standard or extended command syntax. For example, you can enter the **clr** command or **clear** command to clear a virtual call. A command specified with standard command syntax is merely an abbreviated version of the extended syntax version.

[Table 72](#) lists the commands available in both standard and extended command syntax.

Table 72 Available PAD Command Signals

Standard Syntax	Extended Syntax	Description
break		Simulate an asynchronous break.
call		Place a virtual call to a remote device.
clr	clear	Clear a virtual call.
<i>command-signal¹</i>		Specifies a call request without using a standard X.28 command, which is entered with the following syntax: <i>facilities-x121-addressDcall-user-data</i> .
help		Display help information. (See Table 74 .)
iclr	iclear	Request the remote device to clear the call.
int	interrupt	Send an Interrupt Packet.
par? par	parameter read	Display the current values of local parameters. (See Table 73 .)
prof	profile <i>file-name</i>	Load a standard or a named profile.
reset		Reset the call.
rpar?	rread	Display the current values of remote parameters.
rset?	rsetread	Set and then read the values of remote parameters.
set		Change the values of local parameters. (See Table 73 .)
set?	setread	Change and then read the values of parameters.
stat	status	Request the status of a connection.
selection pad		Set up a virtual call.

1. This is an example of issuing a call request command: the **R,G23,P2-234234Duser1** command.

[Table 73](#) lists the different types of parameters you can set using the **set parameter-number:new-value** PAD command signal from X.28 mode. Refer to the “X.3 PAD Parameters” appendix in the *Cisco IOS Terminal Services Configuration Guide* for more complete information about these parameters. See [Table 34](#) in this publication for a list of ASCII characters.

Table 73 Supported X.3 PAD Parameters

Parameter Number	ITU-T Parameter Name	ITU-T X.3 and Cisco Values
1	PAD recall using a character	Minimum value: 0; maximum value: 126; X.28 PAD user emulation mode default: 1. Note Not supported by PAD EXEC user interface.
2	Echo	Minimum value: 0; maximum value: 1; PAD EXEC mode and X.28 PAD user emulation mode default: 1.
3	Selection of data forwarding character	Minimum value: 0; maximum value: 255; PAD EXEC mode default: 2 (CR); X.28 PAD user emulation mode default: 126 (~).
4	Selection of idle timer delay	Minimum value: 0; maximum value: 255; PAD EXEC mode default: 1; X.28 PAD user emulation mode default: 0.

Table 73 **Supported X.3 PAD Parameters (continued)**

Parameter Number	ITU-T Parameter Name	ITU-T X.3 and Cisco Values
5	Ancillary device control	Minimum value: 0; maximum value: 2; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 1.
6	Control of PAD service signals	Minimum value: 0; maximum value: 255; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 2. Note Not supported by PAD EXEC user interface.
7	Action upon receipt of a BREAK signal	Minimum value: 0; maximum value: 31; PAD EXEC mode default: 4; X.28 PAD user emulation mode default: 2.
8	Discard output	Minimum value: 0; maximum value: 1; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
9	Padding after Return	Minimum value: 0; maximum value: 255; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
10	Line folding	Not supported.
11	DTE speed (binary speed of start-stop mode DTE)	Minimum value: 0; maximum value: 18; PAD EXEC mode and X.28 PAD user emulation mode default: 14.
12	Flow control of the PAD by the start-stop DTE	Minimum value: 0; maximum value: 1; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 1.
13	Line feed insertion (after a Return)	Minimum value: 0; maximum value: 7; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
14	Line feed padding	Minimum value: 0; maximum value: 255; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
15	Editing	Minimum value: 0; maximum value: 1; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
16	Character delete	Minimum value: 0; maximum value: 127; PAD EXEC mode and X.28 PAD user emulation mode default: 127 (DEL).
17	Line delete	Minimum value: 0; maximum value: 127; PAD EXEC mode default: 21 (NAK or Ctrl-U); X.28 PAD user emulation mode default: 24 (CAN or Ctrl-X).
18	Line display	Minimum value: 0; maximum value: 127; PAD EXEC mode and X.28 PAD user emulation mode default: 18 (DC2 or Ctrl-R).
19	Editing PAD service signals	Minimum value: 0; maximum value: 126; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 2. Note Not supported by PAD EXEC user interface.

Table 73 **Supported X.3 PAD Parameters (continued)**

Parameter Number	ITU-T Parameter Name	ITU-T X.3 and Cisco Values
20	Echo mask	Minimum value: 0; maximum value: 255; PAD EXEC mode and X.28 PAD user emulation mode default: 0. Note Not supported by PAD EXEC user interface.
21	Parity treatment	Minimum value: 0; maximum value: 4; PAD EXEC mode and X.28 PAD user emulation mode default: 0. Note For additional values that can be selected for parameter 21, including parity treatment to conform to the French Transpac public switched data network and its technical specification and utilization of networks standards (STUR), see Appendix A, “X.3 PAD Parameters,” in the <i>Cisco IOS Terminal Services Configuration Guide</i> .

**Note**

Abbreviated X.121 addresses are not supported. Such addresses start with a period, are alphanumeric, and are mapped to a full X.121 address by the PAD.

Table 74 lists the options for the X.28 **help** command.

Table 74 **X.28 help Options**

Command	Description
help	Describes the help PAD command.
help command	Displays the list of available PAD command signals.
help parameter	Displays the list of available X.3 PAD parameters.
help parameter <i>number</i>	Displays the specified X.3 PAD parameter and its current value.
help list	Lists the available help subjects.
help profiles	Lists available profiles.
help profile <i>name</i>	Displays the specified parameter name and current value.
help <i>any-PAD-command</i>	Describes the specified PAD command signal.

You can issue call requests from X.28 mode without using standard X.28 commands by using the following command syntax:

*facilities-x121-address***D***call-user-data*

where:

facilities Applies X.25 facilities to the outgoing call. The hyphen is mandatory.

x121-address Specifies the address of the remote X.25 device.

D Facility request code that specifies CUD for the outgoing call.

call-user-data Specifies the data that accompanies the call request packet sent to the remote X.25 device.

The following rules apply to all call requests parsed in X.28 mode:

- When an X.121 address specified using standard command syntax is followed by an optional CUD field, the call is placed to the X.121 address.
- When standard command syntax is used, one or more facility request codes can be entered, followed by the code value. Additional facility request codes and values also can be entered. Separate each entry with a comma, followed by a dash. An X.121 address and optional CUD can follow this entry.
- If an X.28 command is not entered, a call request is assumed.
- Ensure that the call request begins with a facility code letter, and that it contains a hyphen (-) followed by a string of digits (the X.121 address). The call request can be terminated by an asterisk (*), a "P," or a "D," followed by some data.
- When using extended command syntax is used, the **call** command uses the facility codes and X.121 address as its operand.
- If facility codes are entered without an X.121 address, remember the codes for the next call. When a call is completed, forget the facility codes until they are once again set.

Table 75 shows examples of parsed call requests.

Table 75 Example X.28 Call Requests

Command	Description
123456789	Calls this X.121 address.
123456789*userdata	Calls this X.121 address, with specified data.
123456789Puserdata	Calls this X.121 address, with specified data.
123456789Duserdata	Calls this X.121 address, with specified data.
Nabcd-123456789	Calls this X.121 address, with NUI set to abcd.
Nabcd,R-123456789	Calls 123456789 with NUI of abcd, and with reverse charging.

Examples

The following example uses the **?** command to display the optional X.28 keywords:

Router# **x28 ?**

```

debug      Turn on Debug Messages for X28 Mode
escape     Set the string to escape from X28 PAD mode
noescape   Never exit x28 mode (use with caution)
nuicud     All calls with NUI, are normal charge with the NUI placed in Call
           User Data
profile     Use a defined X.3 Profile
reverse     All calls default to reverse charge
verbose     Turn on Verbose Messages for X28 Mode
<cr>
```

After you are in X.28 mode, use the **call** PAD signal command to place a virtual call:

```
Router# x28
```

```
* call 123456
```

The following example enters X.28 mode with the **x28** EXEC command and configures a PAD with the **set** X.3 parameter command. The **set** command sets the idle time delay to 40 seconds.

```
Router# x28
```

```
* set 4:40
```

Related Commands

Command	Description
pad	Logs in to a PAD.

x28 no-outgoing

To configure X.28 user emulation mode to prevent a network element from dialing out, use the **x28 no-outgoing** command in user EXEC, privileged EXEC, or line configuration mode. To disable the X.28 user emulation mode that is configured to prevent a network element from dialing out, use the **no** form of this command.

x28 no-outgoing

no x28 no-outgoing

Syntax Description This command has no arguments or keywords.

Command Default Network elements can dial out.

Command Modes

- User EXEC
- Privileged EXEC
- Line configuration

Command History	Release	Modification
	12.3(11)YN	This command was introduced.
	12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To configure X.28 user emulation mode on all lines connected to the router, use the **x28 no-outgoing** command in the user EXEC mode or the privileged EXEC mode.

The **x28 no-outgoing** command is used with the **autocommand** command in line configuration mode to configure the x28 user emulation mode on a per-line basis. See the "Examples" section.

Use of the **x28 no-outgoing** command on the console will lock the console. Unlock the console by logging in from a different tty or vty. If no line is available, reload the router.

Examples

The following example configures X.28 user emulation mode on all the lines connected to the router to prevent network elements from dialing out:

```
Router# x28 no-outgoing
```

The following example configures X.28 user emulation mode only on line 33, when used with the **autocommand** command, to prevent network elements from dialing out through that line:

```
Router# configure terminal  
Enter configuration commands, one per line.  End with CNTL/Z.  
Router(config)# line 33  
Router(config-line)# autocommand x28 no-outgoing  
Router(config-line)# exit
```

Related Commands

Command	Description
autocommand	Executes a command automatically when a user connects to a particular line.
pad	Logs in to a PAD.

x3

To set X.3 packet assembler/disassembler (PAD) parameters, use the **x3** command in EXEC mode.

x3 *parameter:value*

Syntax Description

parameter:value Sets the PAD parameters. (See [Table 73](#) in the **x28** command description.)

Defaults

For outgoing connections, the X.3 parameters default to the following:

2:1, 3:2, 4:1, 7:4, 16:127, 17:21, 18:19

All other parameters default to zero, but can be changed using the **/set** switch keyword with either the **resume** command or the **x3** command.

For incoming PAD connections, the software sends an X.29 SET PARAMETER packet to set only the following parameters:

2:0, 4:1, 7:21, 15:0

For a complete description of the X.3 PAD parameters, see the appendix titled “X.3 PAD Parameters” in the *Cisco IOS Terminal Services Configuration Guide*.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can have several PAD connections open at the same time and switch between them. You can also exit a connection and return to the user EXEC prompt at any point.

To open a new connection, first suspend the current connection by pressing the escape sequence (**Ctrl-Shift-6** then **x** [**Ctrl^x**] by default) to return to the system command prompt, then open the new connection with the **pad** command.

You can have several concurrent sessions open and switch between them. The number of PAD sessions that can be open is defined by the **session-limit** command.

To switch between sessions you must escape one session and resume a previously opened session. Use the **Ctrl^x** sequence to escape out of a connection, use the **where** EXEC command to check the connection number, and then use the **resume** command with the connection number to resume the suspended connection. These commands are available with all supported connection protocols.

You can issue any of the following commands to terminate a terminal session:

- **exit**

- **quit**
- **logout**

To display information about packet transmission and X.3 PAD parameter settings, use the **show x25 pad** command.

Examples

The following example shows how to change a local X.3 PAD parameter from a remote X.25 host using X.29 messages, which is a secure way to enable a remote host to gain control of local PAD. The local device is named Router-A. The remote host is named Router-B. The parameters listed in the ParamsIn field are incoming parameters, which are sent by the remote PAD. The parameters listed in the ParamsOut field are parameters sent by the local PAD.

```
Router-A# pad 123456
Trying 123456...Open

Router-B> x3 2:0
Router-B>
Router-A# show x25 pad

tty0, connection 1 to host 123456

Total input: 12, control 3, bytes 35. Queued: 0 of 7 (0 bytes).
Total output: 10, control 3, bytes 64.
Flags: 1, State: 3, Last error: 1
ParamsIn: 1:0, 2:0, 3:0, 4:0, 5:0, 6:0, 7:0,
          8:0, 9:0, 10:0, 11:0, 12:0, 13:0, 14:0, 15:0,
          16:0, 17:0, 18:0, 19:0, 20:0, 21:0, 22:0,
ParamsOut: 1:1, 2:0, 3:2, 4:1, 5:1, 6:0, 7:21,
          8:0, 9:1, 10:0, 11:14, 12:1, 13:0, 14:0, 15:0,
          16:127, 17:21, 18:18, 19:0, 20:0, 21:0, 22:0,
Router-A#
```

Related Commands

Command	Description
resume (X.3 PAD)	Sets X.3 parameters for PAD connections.

