

vpdn aaa attribute

To enable reporting of network access server (NAS) authentication, authorization, and accounting (AAA) attributes related to a virtual private dialup network (VPDN) to the AAA server, use the **vpdn aaa attribute** command in global configuration mode. To disable reporting of AAA attributes related to VPDN, use the **no** form of this command.

```
vpdn aaa attribute {nas-ip-address vpdn-nas | nas-port vpdn-nas}
```

```
no vpdn aaa attribute {nas-ip-address vpdn-nas | nas-port}
```

Syntax Description	
nas-ip-address vpdn-nas	Enable reporting of the VPDN NAS IP address to the AAA server.
nas-port vpdn-nas	Enable reporting of the VPDN NAS port to the AAA server.

Command Default AAA attributes are not reported to the AAA server.

Command Modes Global configuration

Command History	Release	Modification
	11.3 NA	This command was introduced.
	11.3(8.1)T	This command was integrated into Cisco IOS Release 11.3(8.1)T.

Usage Guidelines This command can be used with RADIUS or TACACS+, and is applicable only on the VPDN tunnel server.

Examples The following example configures VPDN on a tunnel server and enables reporting of VPDN AAA attributes to the AAA server:

```
vpdn enable
vpdn-group 1
  accept-dialin
  protocol any
  virtual-template 1
!
  terminate-from hostname nas1
  local name ts1
!
vpdn aaa attribute nas-ip-address vpdn-nas
vpdn aaa attribute nas-port vpdn-nas
```

vpdn aaa override-server

To specify an authentication, authorization, and accounting (AAA) server to be used for virtual private dialup network (VPDN) tunnel authorization other than the default AAA server, use the **vpdn aaa override-server** global configuration command. To return to the default setting, use the **no** form of this command.

```
vpdn aaa override-server {aaa-server-ip-address | aaa-server-name}
```

```
no vpdn aaa override-server {aaa-server-ip-address | aaa-server-name}
```

Syntax Description

<i>aaa-server-ip-address</i>	The IP address of the AAA server to be used for tunnel authorization.
<i>aaa-server-name</i>	The name of the AAA server to be used for tunnel authorization.

Defaults

If the AAA server is not specified, the default AAA server configured for network authorization is used.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

This command can be used with RADIUS or TACACS+, and is applicable only on the VPDN network access server (NAS). Configuring this command restricts tunnel authorization to the specified AAA servers only. This command can be used to specify multiple AAA servers.

For TACACS+ configuration, the **tacacs-server directed-request** command must be configured using the **restricted** keyword, or authorization will continue with all configured TACACS+ servers.

Examples

The following example enables AAA attributes and specifies the AAA server to be used for VPDN tunnel authorization:

```
aaa new-model
aaa authorization network default group radius
vpdn aaa override-server 10.1.1.1
vpdn enable
radius-server host 10.1.1.2 auth-port 1645 acct-port 1646
radius-server key Secret
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA access control model.
	tacacs-server directed-request	Sends only a username to a specified server when a direct request is issued.
	vpdn enable	Enables VPDN on the router and directs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.

vpngn authen-before-forward

To configure a network access server (NAS) to request authentication of a complete username before making a forwarding decision for all dial-in Layer 2 Tunnel Protocol (L2TP) or Layer 2 Forwarding (L2F) tunnels, use the **vpngn authen-before-forward** command in global configuration mode. To disable this configuration, use the **no** form of this command.

vpngn authen-before-forward

no vpngn authen-before-forward

Syntax Description This command has no arguments or keywords.

Command Default L2TP or L2F tunnels are forwarded to the tunnel server without first requesting authentication of the complete username.

Command Modes Global configuration

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines To configure the NAS to perform authentication of all dial-in L2TP or L2F sessions before the sessions are forwarded to the tunnel server, configure the **vpngn authen-before-forward** command in global configuration mode.

To configure the NAS to perform authentication of dial-in L2TP or L2F sessions belonging to a specific VPDN group before the sessions are forwarded to the tunnel server, use the **authen-before-forward** command in VPDN group configuration mode.

Enabling the **vpngn authen-before-forward** command instructs the NAS to authenticate the complete username before making a forwarding decision based on the domain portion of the username. A user may be forwarded or terminated locally depending on the information contained in the users RADIUS profile. Users with forwarding information in their RADIUS profile are forwarded based on that information. Users without forwarding information in their RADIUS profile are either forwarded or terminated locally based on the Service-Type in their RADIUS profile. The relationship between forwarding decisions and the information contained in the users RADIUS profile is summarized in Table 154.

Table 154 Forwarding Decisions Based on RADIUS Profile Attributes

Forwarding Information Is	Service-Type Is Outbound	Service-Type Is Not Outbound
Present in RADIUS profile	Forward User	Forward User
Absent from RADIUS profile	Check Domain	Terminate Locally

Examples

The following example configures the NAS to request authentication of all dial-in L2TP or L2F sessions before the sessions are forwarded to the tunnel server:

```
vpdn authen-before-forward
```

Related Commands

Command	Description
authen-before-forward	Configures a NAS to request authentication of a complete username before making a forwarding decision for dial-in L2TP or L2F tunnels belonging to a VPDN group.

vpng authorize directed-request

To enable virtual private dialup network (VPDN) authorization for directed-request users, use the **vpng authorize directed-request** command in global configuration mode. To disable VPDN authorization for directed request users, use the **no** form of this command.

vpng authorize directed-request

no vpng authorize directed-request

Syntax Description This command has no keywords or arguments.

Defaults VPDN authorization for directed-request users is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1	This command was introduced.

Usage Guidelines When a username includes both a username and a domain portion, such as user@site.com, directed request configuration allows the authorization request to be sent to a specific RADIUS or TACACS+ server based on the domain name portion of the username (site.com). The **vpng authorize directed-request** command must be enabled to allow VPDN authorization of any directed request user.

Directed request for RADIUS users is enabled by issuing the **radius-server directed-request** command. Directed request for TACACS+ users is enabled by default, and may be disabled using the **no tacacs-server directed request** command. The **ip host** command must be configured to enable directed requests to RADIUS or TACACS+ servers.

The **vpng authorize directed-request** command is usually configured on the L2TP network server (LNS). When directed-requests are used on an L2TP access concentrator (LAC) in conjunction with per-user VPDN configuration, the **authen before-forward** command must be enabled.

Examples The following example enables VPDN authorization and RADIUS directed requests on an LNS:

```
ip host site.com 10.1.1.1
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server directed-request
vpng authorize directed-request
```

The following example enables VPDN authorization and TACACS+ directed requests on an LNS:

```
ip host site.com 10.1.1.1
tacacs-server host 10.1.1.1
tacacs-server directed-request
vpng authorize directed-request
```

The following example enables per-user VPDN and enables VPDN authorization for directed request users on a LAC:

```
vpdn-group 1
 request-dialin
  protocol l2f
  domain site.com
 !
 initiate-to ip 10.1.1.1
 local name local1
 authen before-forward
 !
 ip host site.com 10.1.1.1
 vpdn authorize directed-request
 !
 radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
 radius-server directed-request
```

Related Commands

Command	Description
authen before-forward	Specifies that the VPDN sends the entire structured username to the AAA server the first time the router contacts the AAA server.
ip host	Defines a static host name-to-address mapping in the host cache.
radius-server directed-request	Allows users logging into a Cisco NAS to select a RADIUS server for authentication.
tacacs-server directed-request	Sends only a username to a specified server when a direct request is issued.

vpng domain-delimiter

To specify the characters to be used to delimit the domain prefix or domain suffix, use the **vpng domain-delimiter** command in global configuration mode.

vpng domain-delimiter *characters* [**suffix** | **prefix**]

Syntax Description

characters One or more specific characters to be used as suffix or prefix delimiters. Available characters are %, -, @, \, #, and /.

If a backslash (\) is the last delimiter in the command line, enter it as a double backslash (\\).

suffix | **prefix** (Optional) Usage of the specified characters.

Defaults

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

You can enter one **vpng domain-delimiter** command to list the suffix delimiters and another **vpng domain-delimiter** command to list the prefix delimiters. However, no character can be both a suffix delimiter and a prefix delimiter.

This command allows the network access server to parse a list of home gateway DNS domain names and addresses sent by an AAA server. The AAA server can store domain names or IP addresses in the following AV pair:

```
cisco-avpair = "lcp:interface-config=ip address 1.1.1.1 255.255.255.255.0",
```

```
cisco-avpair = "lcp:interface-config=ip address bigrouter@excellentinc.com,
```

Examples

The following example lists three suffix delimiters and three prefix delimiters:

```
vpng domain-delimiter %-@ suffix
vpng domain-delimiter #/\ prefix
```

This example allows the following host and domain names:

```
cisco.com#houstondrr
houstondrr@cisco.com
```

Related Commands	Command	Description
	vpdn enable	Enables virtual private dialup networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
	vpdn-group	Sets the failure history table depth beyond the default value of 20 entries.
	vpdn history failure	Enables logging of VPDN failures to the history failure table or to set the failure history table size.
	vpdn profile	Specifies how the network access server for the service provider is to perform VPDN tunnel authorization searches.

vpdn enable

To enable virtual private dialup networking on the router and inform the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present, use the **vpdn enable** command in global configuration mode.

vpdn enable

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines To disable a VPN tunnel, use the command **clear vpdn tunnel** in EXEC mode. The command **no vpdn enable** does not automatically disable a VPN tunnel.

Examples The following example enables virtual private dialup networking on the router:

```
vpdn enable
```

Related Commands	Command	Description
	vpdn-group	Sets the failure history table depth beyond the default value of 20 entries.
	vpdn history failure	Enables logging of VPDN failures to the history failure table or to set the failure history table size.

vpdn force-local-chap

To cause the home gateway to issue its own Challenge Handshake Authentication Protocol (CHAP) challenge even if one has already been issued from the network access server, use the **vpdn force-local-chap** command in global configuration mode. Use the **no** form of this command to prevent the home gateway from issuing its own CHAP challenge.

vpdn force-local-chap

no vpdn force-local-chap

Syntax Description This command has no arguments or keywords.

Defaults The home gateway does not issue its own CHAP challenge:

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Examples The following example configures a virtual template interface on the home gateway and then enables VPDN and forces the home gateway to issue its own CHAP challenge.

```
interface virtual-template 1
ip unnumbered ethernet 0
encapsulation ppp
ppp authentication chap
!
vpdn enable
vpdn incoming world12 troll virtual-template 1
vpdn force-local-chap
```

vpngroup

To associate a virtual private dialup network (VPDN) group with a customer or VPDN profile, use the **vpngroup** command in customer profile or VPDN profile configuration mode. To disassociate a VPDN group from a customer or VPDN profile, use the **no** form of this command.

vpngroup *name*

no vpngroup *name*

Syntax Description

name

Name of the VPDN group.

Note This name should match the name defined for the VPDN group configured with the **vpngroup** command.

Defaults

No default behavior or values.

Command Modes

Customer profile configuration
VPDN profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.

Usage Guidelines

Use the **vpngroup** command in customer profile configuration mode or VPDN profile configuration mode to associate a VPDN group with a customer profile or a VPDN profile, respectively.

VPDN groups are created using the **vpngroup** command in global configuration mode.

Examples

The following example creates the VPDN groups named l2tp and l2f, and associates both VPDN groups with the VPDN profile named profile32:

```
Router(config)# vpngroup l2tp
Router(config-vpngroup)#
!
Router(config)# vpngroup l2f
Router(config-vpngroup)#
!
Router(config)# resource-pool profile vpngroup profile32
Router(config-vpngroup-profile)# vpngroup l2tp
Router(config-vpngroup-profile)# vpngroup l2f
```

The following example creates two VPDN groups and configures them under a customer profile named company2:

```
Router(config)# vpdn-group mygroup
Router(config-vpdn)#
!
Router(config)# vpdn-group yourgroup
Router(config-vpdn)#
!
Router(config)# resource-pool profile vpdn company2
Router(config-vpdn-profile)# vpdn group mygroup
Router(config-vpdn-profile)# vpdn group yourgroup
```

Related Commands

Command	Description
resource-pool profile customer	Creates a customer profile and enters customer profile configuration mode.
resource-pool profile vpdn	Creates a VPDN profile and enters VPDN profile configuration mode.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn profile	Associates a VPDN profile with a customer profile.

vpdn history failure

To enable logging of virtual private dialup network (VPDN) failures to the history failure table or to set the failure history table size, use the **vpdn history failure** command in global configuration mode. To disable logging of VPDN history failures or to restore the default table size, use the **no** form of this command.

vpdn history failure [*table-size entries*]

no vpdn history failure [*table-size*]

Syntax Description

table-size entries (Optional) Sets the number of entries in the history failure table. Valid entries range from 20 to 50.

Defaults

VPDN failures are logged by default.
table size: 20 entries

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Logging of VPDN failure events is enabled by default. You can disable the logging of VPDN failure events by issuing the **no vpdn history failure** command.

The logging of a failure event to the history table is triggered by event logging by the syslog facility. The syslog facility creates a failure history table entry, which keeps records of failure events. The table starts with 20 entries, and the size of the table can be expanded to a maximum of 50 entries using the **vpdn history failure table-size entries** command. You may configure the **vpdn history failure table-size entries** command only if VPDN failure event logging is enabled.

All failure entries for the user are kept chronologically in the history table. Each entry records the relevant information of a failure event. Only the most recent failure event per user, unique to its name and tunnel client ID (CLID), is kept.

When the total number of entries in the table reaches the configured table size, the oldest record is deleted and a new entry is added.

Examples

The following example disables logging of VPDN failures to the history failure table:

```
no vpdn history failure
```

The following example enables logging of VPDN failures to the history table and sets the history failure table size to 40 entries:

```
vpdn history failure
vpdn history failure table-size 40
```

Related Commands

Command	Description
show vpdn history failure	Displays the content of the failure history table.

vpdn incoming

To specify the local name to use for authenticating and the virtual template to use for building interfaces for incoming connections when a Level 2 Forwarding (tunnel) connection is requested from a certain remote host, use the **vpdn incoming** command in global configuration mode.

vpdn incoming *remote-name local-name virtual-template number*

Syntax Description

<i>remote-name</i>	Case-sensitive name of the remote host (the network access server) requesting the connection.
<i>local-name</i>	Case-sensitive local name (of the home gateway) to use when authenticating back to the remote host.
virtual-template <i>number</i>	Virtual template to use for building interfaces for incoming calls.

Defaults

Disabled. No host name, IP address, or local name for authentication are provided.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The *remote-name* and *local-name* arguments are case sensitive.

This command is usually used on a home gateway, not on the network access server in the ISP or public data network.

Examples

The following partial example specifies use of local host `go_blue` and virtual template interface 6 for connections with remote host `dallas_wan`:

```
vpdn incoming dallas_wan go_blue virtual-template 6
```

vpdn logging

To enable the logging of virtual private dialup network (VPDN) events, use the **vpdn logging** command in global configuration mode. To disable the logging of VPDN events, use the **no** form of this command.

vpdn logging [local | remote | user]

no vpdn logging [local | remote | user]

Syntax Description	local	(Optional) Enables logging of VPDN events to the syslog locally.
	remote	(Optional) Enables logging of VPDN events to the syslog of the remote tunnel endpoint.
	user	(Optional) Enables logging of VPDN user events to the syslog.

Defaults All VPDN event logging is disabled.

Command Modes Global configuration

Command History	Release	Modification
	11.3T	This command was introduced.
	12.1	The user keyword was introduced in Cisco IOS Release 12.1.

Usage Guidelines This command controls the logging of VPDN events. By default, all VPDN event logging is disabled. To enable the logging of VPDN events to the system message logging (syslog) of the local or remote tunnel endpoint router, issue the **vpdn logging** command with the **local** or **remote** keyword. To log VPDN user events to the syslog, you must configure the **vpdn logging** command with the **user** keyword. You may configure as many types of VPDN event logging as you want.

Examples The following example enables VPDN logging locally:

```
vpdn logging local
```

The following example disables VPDN event logging locally, enables VPDN event logging at the remote tunnel endpoint, and enables the logging of VPDN user events to the syslog of the remote router:

```
no vpdn logging local
vpdn logging remote
vpdn logging user
```

Related Commands	Command	Description
	vpdn history failure	Enables logging of VPDN failures to the history failure table or sets the failure history table size.

vpdn multihop

To enable virtual private dialup network (VPDN) multihop, use the **vpdn multihop** global configuration command. To disable VPDN multihop capability, use the **no** form of this command.

vpdn multihop

no vpdn multihop

Syntax Description This command has no arguments or keywords.

Defaults Multihop is not enabled.

Command Modes Global configuration

Command History	Release	Modification
	11.3(5)T	This command was introduced.

Usage Guidelines

The Cisco Multihop VPDN feature allows you to perform Multichassis Multilink Point-to-Point Protocol (MMP) on a home gateway (HGW) or Layer 2 Tunneling Protocol (L2TP) network server (LNS) in a VPDN scenario. This feature allows sharing tunnel resources between the HGW and LNS routers, and the possibility to offload by default to another router in the network.

The VPDN multihop feature also allows a router configured as a tunnel switch to terminate tunnels from Layer 2 access concentrators (LACs) and forward the sessions through up to four newly established L2TP tunnels. The tunnels are selected using client-supplied matching criteria configured by the **vpdn search-order** global configuration command.

Before using the **vpdn multihop** command, refer to the *Dial Services Configuration Guide: Network Services*, to learn more about Multilink PPP and MMP.

Examples

The following example shows a configuration where a packet traverses a VPDN tunnel over a service provider link, and then a second tunnel by traversing a hop between home gateways on the corporate network. The bundle owner is Home-Gateway1 and the stack group peer, Home-Gateway2, is specified as a peer (10.10.1.2).

```
vpdn multihop
username stack password hellothere
multilink virtual-template 1

sgbp group stack
sgbp member Home-Gateway2 10.10.1.2

interface virtual-template 1
ip unnumbered e0
ppp multilink
ppp auth chap
```

The following example also shows how to configure the Cisco Multihop VPDN feature:

```

!
vpngroup enable
vpngroup multihop
vpngroup search-order domain
!
vpngroup-group 1
  request-dialin
  protocol l2tp
  domain cisco.com
  initiate-to ip 172.22.53.144 priority 1
  initiate-to ip 172.22.53.145 priority 1
!
l2tp tunnel password 7 <deleted>
!

```

Related Commands

Command	Description
vpngroup enable	Enables VPDN networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpngroup search-order	Specifies how the service provider's network access server is to perform VPDN tunnel authorization searches.

vpdn outgoing

To specify use of Dialed Number Information Service (DNIS) or use of a domain name when selecting a tunnel for forwarding traffic to the remote host (the home gateway) on a Virtual Private Dialup Network (VPDN), use the **vpdn outgoing** command in global configuration mode.

vpdn outgoing word | **dnis** *dialed-number*

Syntax Description	word	Case-sensitive name of the gateway domain for forwarding traffic.
	dnis <i>dialed-number</i>	Dialed number to be used for selecting a specific tunnel to be used for forwarding traffic to a home gateway.

Defaults Disabled. No remote names and local names are defined.

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines

The **word** argument is case sensitive.

This command is usually used on a network access server, not on a home gateway.

When use of the Dialed Number Information Service is enabled and a dialed number is provided, the network service provider can use the dialed number to select a specific tunnel destination.

The domain name can be used to choose a tunnel destination. For example, if a user dials in as “joe@company-a.com,” then matching on “company-a.com,” a tunnel destination can be chosen.

If both DNIS information and a CHAP or PAP name map to a valid tunnel, the DNIS information is used.

If TACACS+ is used to get tunnel information, the string “dnis:” is prepended to the phone number before attempting to look up the information in AAA.

Examples The following example selects a tunnel destination based on the domain name:

```
vpdn outgoing chicago-main go-blue
```

The following example selects a tunnel destination based on the use of DNIS and a specific dialed number:

```
vpdn outgoing dnis 2387765 gocardinal
```

Related Commands	Command	Description
	vpdn enable	Enables virtual private dialup networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
	vpdn-group	Sets the failure history table depth beyond the default value of 20 entries.

vpdn profile

To associate a virtual private dialup network (VPDN) profile with a customer profile, use the **vpdn profile** command in customer profile configuration mode. To remove a VPDN profile from a customer profile, use the **no** form of this command.

vpdn profile *name*

no vpdn profile *name*

Syntax Description	<i>name</i>	VPDN profile name.
--------------------	-------------	--------------------

Defaults	No default behavior or values.
----------	--------------------------------

Command Modes	Customer profile configuration
---------------	--------------------------------

Command History	Release	Modification
	12.0(4)XI	This command was introduced.
12.0(5)T	Support for this command was integrated into Cisco IOS Release 12.0(5)T.	

Usage Guidelines	Use the vpdn profile command to associate a VPDN profile with a customer profile.
------------------	--

VPDN profiles can be used to combine session counting over multiple VPDN groups. This ability can be applied to customer profiles by configuring multiple VPDN groups under a VPDN profile, then associating the VPDN profile with the customer profile using the **vpdn profile** command.

Examples	The following example shows how to create two VPDN groups, configure the VPDN groups under a VPDN profile named profile1, then associates the VPDN profile with a customer profile named customer12:
----------	--

```
Router(config)# vpdn-group 1
Router(config-vpdn)#
!
Router(config)# vpdn-group 2
Router(config-vpdn)#
!
Router(config)# resource-pool profile vpdn profile1
Router(config-vpdn-profile)# vpdn group 1
Router(config-vpdn-profile)# vpdn group 2
!
Router(config)# resource-pool profile customer customer12
Router(config-vpdn-customer)# vpdn profile profile1
```

Related Commands	Command	Description
	resource-pool profile customer	Creates a customer profile.
	resource-pool profile vpdn	Creates a VPDN profile and enters VPDN profile configuration mode.
	vpdn group	Associates a VPDN group with a customer or VPDN profile.
	vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

vpdn search-order

To specify how the service provider's network access server is to perform Virtual Private Dialup Network (VPDN) tunnel authorization searches, use the **vpdn search-order** command in global configuration mode. Use the **no** form of the command to remove a prior specification.

vpdn search-order { dnis domain | domain dnis | domain | dnis }

no vpdn search-order

Syntax Description

dnis domain	Search first on the Dialed Number Information Service (DNIS) information provided on ISDN lines and then search on the domain name.
domain dnis	Search first on the domain name and then search on the DNIS information.
domain	Search on the domain name only.
dnis	Search on the DNIS information only.

Defaults

When this command is not used, the default is to search first on the Dialed Number Information Service (DNIS) information provided on ISDN lines and then search on the domain name. This is equivalent to using the **vpdn search-order dnis domain** command.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

VPDN authorization searches are performed only as specified.

The configuration shows the **vpdn search-order** command setting only if the command is explicitly configured.

Examples

The following example configures a network access server to select a tunnel destination based on the use of DNIS and a specific dialed number and to perform tunnel authorization searches based on the DNIS information only.

```
vpdn enable
vpdn outgoing dnis 2387765 gocardinal ip 170.16.44.56
vpdn search-order dnis
```

Related Commands

Command	Description
vpdn outgoing	Specifies to use either DNIS or a domain name when selecting a tunnel for forwarding traffic to the remote host (the home gateway) on a VPDN.

vpdn source-ip

To set the source IP address of the network access server, use the **vpdn source-ip** command in global configuration mode.

vpdn source-ip *address*

Syntax Description	<i>address</i>	IP address of the network access server.
---------------------------	----------------	--

Defaults	This command is disabled. No default IP address is provided.
-----------------	--

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

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines	One source IP address is configured on the network access server. The source IP address is configured per network access server, not per domain.
-------------------------	--

Examples	<p>This example enables VPDN on the network access server and sets an IP source address of 171.4.48.3:</p> <pre>vpdn enable vpdn source-ip 171.4.48.3</pre>
-----------------	---

Related Commands	Command	Description
	vpdn enable	Enables virtual private dialup networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.

vpngroup

To create a virtual private dialup network (VPDN) group and to enter VPDN group configuration mode, use the **vpngroup** command in global configuration mode. To delete a VPDN group, use the **no** form of this command.

vpngroup *name*

no vpngroup *name*

Syntax Description	<i>name</i>	Name of the VPDN group.
--------------------	-------------	-------------------------

Defaults No VPDN groups are defined.

Command Modes Global configuration

Command History	Release	Modification
	12.0(4)XI	This command was introduced.
	12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.

Usage Guidelines Issuing the **vpngroup** command creates a VPDN group with the specified name and enters VPDN group configuration mode. If a VPDN group with the specified name already exists, issuing the **vpngroup** command will enter VPDN group configuration mode and allow configuration of that VPDN group.

A VPDN group can be associated with a customer profile or a VPDN profile by issuing the **vpngroup** command in customer profile configuration mode or VPDN profile configuration mode.

Examples The following example creates the VPDN group named l2tp and enters VPDN group configuration mode:

```
Router(config)# vpngroup l2tp
Router(config-vpngroup)#
```

The following example associates the VPDN group created in the preceding example with the VPDN profile named profile1:

```
Router(config)# resource-pool profile vpngroup profile1
Router(config-vpngroup-profile)# vpngroup l2tp
```

The following example creates a VPDN group named l2f and associates it with the customer profile named customer1:

```
Router(config)# vpngroup l2f
!
Router(config)# resource-pool profile customer customer1
Router(config-customer-profile)# vpngroup l2f
```

Related Commands	Command	Description
	resource-pool profile customer	Creates a customer profile and enters customer profile configuration mode.
	resource-pool profile vpdn	Creates a VPDN profile and enters VPDN profile configuration mode.
	vpdn group	Associates a VPDN group with a customer or VPDN profile.

vty-async

To configure all virtual terminal lines on a router to support asynchronous protocol features, use the **vty-async** command in global configuration mode. Use the **no** form of this command to disable asynchronous protocol features on virtual terminal lines.

vty-async

no vty-async

Syntax Description

This command has no arguments or keywords.

Defaults

Asynchronous protocol features are not enabled by default on virtual terminal lines.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The **vty-async** command extends asynchronous protocol features from physical asynchronous interfaces to virtual terminal lines. Normally, SLIP and PPP can function only on asynchronous interfaces, not on virtual terminal lines. However, extending asynchronous functionality to virtual terminal lines permits you to run SLIP and PPP on these *virtual asynchronous interfaces*. One practical benefit is the ability to tunnel SLIP and PPP over X.25 PAD, thus extending remote node capability into the X.25 area. You can also tunnel SLIP and PPP over Telnet or LAT on virtual terminal lines. To tunnel SLIP and PPP over X.25, LAT, or Telnet, you use the protocol translation feature in the Cisco IOS software.

To tunnel SLIP or PPP inside X.25, LAT, or Telnet, you can use two-step protocol translation or one-step protocol translation, as follows:

- If you are tunnelling SLIP or PPP using the two-step method, you need to first enter the **vty-async** command. Next, you perform two-step translation.
- If you are tunnelling SLIP or PPP using the one-step method, you do not need to enter the **vty-async** command. You only need to issue the **translate** command with the SLIP or PPP keywords, because the **translate** command automatically enables asynchronous protocol features on virtual terminal lines.

Examples

The following example enables asynchronous protocol features on virtual terminal lines:

```
vty-async
```

Related Commands

Command	Description
ppp	Starts an asynchronous connection using PPP.
slip	Starts a serial connection to a remote host using SLIP.
translate [slip ppp]	Enables asynchronous protocol features on virtual terminal lines.

vty-async dynamic-routing

To enable dynamic routing on all virtual asynchronous interfaces, use the **vty-async dynamic-routing** command in global configuration mode. Use the **no** form of this command to disable asynchronous protocol features on virtual terminal lines and, therefore, disable routing on virtual terminal lines.

vty-async dynamic-routing

no vty-async dynamic-routing

Syntax Description

This command has no arguments or keywords.

Defaults

Dynamic routing is not enabled on virtual asynchronous interfaces.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This feature enables IP routing on virtual asynchronous interfaces. When you issue this command and a user later makes a connection to another host using SLIP or PPP, the user must specify **/routing** on the SLIP or PPP command line.

If you had not previously entered the **vty-async** command, the **vty-async dynamic-routing** command creates virtual asynchronous interfaces, then enables dynamic routing on them.

Examples

The following example enables dynamic routing on virtual asynchronous interfaces:

```
vty-async dynamic-routing
```

Related Commands

Command	Description
async dynamic routing	Enables manually configured routing on an asynchronous interface.

vty-async header-compression

To compress the headers of all TCP packets on virtual asynchronous interfaces, use the **vty-async header-compression** command in global configuration mode. Use the **no** form of this command to disable virtual asynchronous interfaces and header compression.

vty-async header-compression [passive]

no vty-async header-compression

Syntax Description

passive	(Optional) Specifies that outgoing packets to be compressed only if TCP incoming packets on the same virtual asynchronous interface are compressed. For SLIP, if you do not specify this option, the Cisco IOS software will compress all traffic. The default is no compression. For PPP, the Cisco IOS software always negotiates header compression.
----------------	---

Defaults

Header compression is not enabled on virtual asynchronous interfaces.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This feature compresses the headers on TCP/IP packets on virtual asynchronous connections to reduce the size of the packets and to increase performance. This feature only compresses the TCP header, so it has no effect on UDP packets or other protocol headers. The TCP header compression technique, described fully in RFC 1144, is supported on virtual asynchronous interfaces using SLIP or PPP encapsulation. You must enable compression on both ends of a connection.

Examples

The following example compresses outgoing TCP packets on virtual asynchronous interfaces only if incoming TCP packets are compressed:

```
vty-async header-compression passive
```

Related Commands

Command	Description
async dynamic routing	Enables manually configured routing on an asynchronous interface.

vty-async ipx ppp-client loopback

To enable IPX-PPP on virtual terminal lines, use the **vty-async ipx ppp-client loopback** command in global configuration mode. Use the **no** form of this command to disable IPX-PPP sessions on virtual terminal lines.

vty-async ipx ppp-client loopback *number*

no vty-async ipx ppp-client loopback

Syntax Description	<i>number</i>	Number of the loopback interface configured for IPX to which the virtual terminal lines are assigned.
---------------------------	---------------	---

Defaults IPX over PPP is not enabled on virtual terminal lines.

Command Modes Global configuration

Command History	Release	Modification
	11.0	This command was introduced.

Usage Guidelines This command enables users to log into the router from a device running a virtual terminal protocol, then issue the PPP command at the EXEC prompt to connect to a remote device.

A loopback interface must already have been defined and an IPX network number must have been assigned to the loopback interface before the **vty-async ipx ppp-client loopback** command will permit IPX-PPP on virtual terminal lines.

Examples The following example enables IPX over PPP on virtual terminal lines:

```
ipx routing ramana
interface loopback0
 ipx network 12345
vty-async ipx ppp-client loopback0
```

Related Commands	Command	Description
	interface loopback	Creates a loopback interface.
	ipx network	Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).

vtty-async keepalive

To change the frequency of keepalive packets on all virtual asynchronous interfaces, use the **vtty-async keepalive** command in global configuration mode. Use the **no vty-async** command to disable asynchronous protocol features on virtual terminal lines, or the **vtty-async keepalive 0** command to disable keepalive packets on virtual terminal lines.

vtty-async keepalive *seconds*

no vty-async keepalive

vtty-async keepalive 0

Syntax Description	<i>seconds</i>	Frequency, in seconds, with which the Cisco IOS software sends keepalive messages to the other end of a virtual asynchronous interface. To disable keepalive packets, use a value of 0. The active keepalive interval range is 1 to 32,767 seconds. Keepalive is disabled by default.
---------------------------	----------------	---

Defaults	Keepalive is disabled.
-----------------	------------------------

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

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines	Use this command to change the frequency of keepalive updates on virtual asynchronous interfaces, or to disable keepalive updates. To determine if keepalive is enabled on an interface, use the show running-config EXEC command. If the router has not received a keepalive packet after three update intervals have passed, the connection is considered down.
-------------------------	--

Examples The following example sets the keepalive interval to 30 seconds:

```
vtty-async keepalive 30
```

The following example sets the keepalive interval to 0 (off):

```
vtty-async keepalive 0
```

Related Commands	Command	Description
	keepalive	Sets the keepalive timer for a specific interface.

vty-async mtu

To set the maximum transmission unit (MTU) size on virtual asynchronous interfaces, use the **vty-async mtu** command in global configuration mode. Use the **no** form of this command to disable asynchronous protocol features on virtual terminal lines.

vty-async mtu *bytes*

no vty-async

Syntax Description	<i>bytes</i> MTU size of IP packets that the virtual asynchronous interface can support. The default MTU is 1500 bytes, the minimum MTU is 64 bytes, and the maximum is 1,000,000 bytes.
---------------------------	--

Defaults	1500 bytes
-----------------	------------

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

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines Use this command to modify the MTU for packets on a virtual asynchronous interfaces. You might want to change to a smaller MTU size for IP packets transmitted on a virtual terminal line configured for asynchronous functions for any of the following reasons:

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

Do not change the MTU size unless the SLIP or PPP implementation running on the host at the other end of the virtual asynchronous interface supports reassembly of IP fragments. Because each fragment occupies a spot in the output queue, it might also be necessary to increase the size of the SLIP or PPP hold queue if your MTU size is such that you might have a high amount of packet fragments in the output queue.

Examples The following example sets the MTU for IP packets to 256 bytes:

```
vty-async mtu 256
```

Related Commands	Command	Description
	mtu	Adjusts the maximum packet size or MTU size.

vty-async ppp authentication

To enable PPP authentication on virtual asynchronous interfaces, use the **vty-async ppp authentication** command in global configuration mode. Use the **no** form of this command to disable PPP authentication.

```
vty-async ppp authentication {chap | pap}
```

```
no vty-async ppp authentication {chap | pap}
```

Syntax Description

chap	Enable CHAP on all virtual asynchronous interfaces.
pap	Enable PAP on all virtual asynchronous interfaces.

Defaults

No CHAP or PAP authentication for PPP.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command configures the virtual asynchronous interface to either authenticate CHAP or PAP while running PPP. After you have enabled CHAP or PAP, the local router requires a password from remote devices. If the remote device does not support CHAP or PAP, no traffic will be passed to that device.

Examples

The following example enables CHAP authentication for PPP sessions on virtual asynchronous interfaces:

```
vty-async ppp authentication chap
```

Related Commands

Command	Description
ppp bap call	Sets PPP BACP call parameters.
ppp use-tacacs	Enables TACACS for PPP authentication.
vty-async	Configures all virtual terminal lines on a router to support asynchronous protocol features.
vty-async ppp use-tacacs	Enables TACACS authentication for PPP on virtual asynchronous interfaces.

vty-async ppp use-tacacs

To enable TACACS authentication for PPP on virtual asynchronous interfaces, use the **vty-async ppp use-tacacs** command in global configuration mode. Use the **no** form of this command to disable TACACS authentication on virtual asynchronous interfaces.

vty-async ppp use-tacacs

no vty-async ppp use-tacacs

Syntax Description This command has no arguments or keywords.

Defaults TACACS for PPP is disabled.

Command Modes Global configuration

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines This command requires the extended TACACS server.

After you have enabled TACACS, the local router requires a password from remote devices.

This feature is useful when integrating TACACS with other authentication systems that require a clear-text version of a user's password. Such systems include one-time password systems and token card systems.

If the username and password are contained in the CHAP password, then the CHAP secret is not used by the router. Because most PPP clients require that a secret be specified, you can use any arbitrary string; the Cisco IOS software ignores it.

You cannot enable TACACS authentication for SLIP on asynchronous or virtual asynchronous interfaces.

Examples The example enables TACACS authentication for PPP sessions:

```
vty-async ppp use-tacacs
```

Related Commands	Command	Description
	ppp use-tacacs	Enables TACACS for PPP authentication.
	vty-async ppp authentication	Enables PPP authentication on virtual asynchronous interfaces.

vty-async virtual-template

To configure virtual terminal lines to support asynchronous protocol functions based on the definition of a virtual interface template, use the **vty-async virtual-template** command in global configuration mode. Use the **no** form of this command to disable virtual interface templates for asynchronous functions on virtual terminal lines.

vty-async virtual-template *number*

no vty-async virtual-template

Syntax Description	<i>number</i>	The virtual interface number.
Defaults	Asynchronous protocol features are not enabled by default on virtual terminal lines.	
Command Modes	Global configuration	
Command History	Release	Modification
	10.3	The vty-async command was introduced.
	11.3	The vty-async virtual-template command was introduced.

Usage Guidelines

The **vty-async virtual-template** command enables you to support tunneling of SLIP or PPP across X.25, TCP, or LAT networks by using two-step protocol translation.

Before issuing the **vty-async virtual-template** command, create and configure a virtual interface template by using the **interface virtual-template** command. Configure this virtual interface as a regular asynchronous serial interface. That is, assign the virtual interface template the IP address of the Ethernet interface, and configure addressing, just as on an asynchronous interface. You can also enter commands in interface configuration mode that compress TCP headers or configure CHAP authentication for PPP.

After creating a virtual interface template, apply it by issuing the **vty-async virtual-template** command. When a user dials in through a virtual terminal line, the router creates a virtual access interface, which is a temporary interface that supports the asynchronous protocol configuration specified in the virtual interface template. This virtual access interface is created dynamically, and is freed up as soon as the connection drops.

Before virtual templates were implemented, you could use the **vty-async** command to extend asynchronous protocol functions from physical asynchronous interfaces to virtual terminal lines. However, in doing so, you created a virtual asynchronous interface, rather than the virtual access interface. The difference is that the virtual asynchronous interfaces are allocated permanently, whereas the virtual access interfaces are created dynamically when a user calls in and closed down when the connection drops.

You can have up to 25 virtual templates interfaces, but you can apply only one template to vty-async interfaces on a router. There can be up to 300 virtual access interfaces on a router.

Examples

The following example enables asynchronous protocol features on virtual terminal lines:

```
vty-async
vty-async Virtual-Template 1
vty-async dynamic-routing
vty-async header-compression
!
interface Virtual-Template1
 ip unnumbered Ethernet0
 encapsulation ppp
 no peer default ip address
 ppp authentication chap
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
ppp	Starts an asynchronous connection using PPP.
slip	Starts a serial connection to a remote host using SLIP.
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.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection.

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 first appeared in a release prior to Cisco IOS Release 10.0.

Usage Guidelines The **where** command displays all open sessions associated with the current terminal line. The **Ctrl^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 155 describes significant fields shown in the display.

Table 155 *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
	protocol (VPDN)	Sets X.3 parameters for PAD connections.
	show sessions	Displays information about open LAT, Telnet, or rlogin connections.

x25 aodi

To enable the Always On/Dynamic ISDN (AO/DI) client on an interface, use the **x25 aodi** command in interface configuration mode. Use the **no** form of this command to remove AO/DI client functionality.

x25 aodi

no x25 aodi

Syntax Description This command has no arguments or keywords.

Defaults AO/DI client is not enabled.

Command Modes Interface configuration

Command History	Release	Modification
	11.3T	This command was introduced.

Usage Guidelines Use this command to enable the AO/DI client on an interface.

Examples The following example enables the AO/DI client on the interface running X.25, using the **x25 aodi** command:

```
interface bri0
  isdn x25 dchannel
  isdn x25 static-tei 8
interface bri0:0
  x25 aodi
  x25 address 12135551234
  x25 htc 4
  x25 win 3
  x25 wout 3
  x25 map ppp 12135556789 interface dialer 1
```

**Note**

Configuring the BRI interface with the **isdn x25 dchannel** command creates a configurable interface (bri 0:0) for other necessary X.25 commands. Refer to the *Cisco IOS Dial Services Configuration Guide: Terminal Services* publication for additional information about this command.

x25 map ppp

To enable a PPP session over the X.25 protocol, use the **x25 map ppp** command in interface configuration mode. Use the **no** form of this command to remove a prior mapping.

x25 map ppp x121-address interface *cloning-interface* no-outgoing

no x25 map ppp x121-address interface *cloning-interface* no-outgoing

Syntax Description		
x121 address	The X.121 address as follows:	<ul style="list-style-type: none"> Client side—The calling number. Server side—The called number.
interface <i>cloning-interface</i>	The interface to be used for cloning the configuration.	
no-outgoing	Ensures that the X.25 map does not originate calls.	

Defaults	
Disabled	

Command Modes	
Interface configuration	

Command History	Release	Modification
	11.3T	This command was introduced.

Usage Guidelines	
Use x25 map ppp command to allow a PPP session to run over X.25.	
The interface keyword refers to the interface that will be used to clone the configuration.	



Note

For the **x25 map** command used in standard X.25 implementations, refer to the *Cisco IOS Wide-Area Networking Command Reference* publication.

Client Examples

The following example enables the AO/DI client on the interface and configures the D channel (BRI interface 0:0) with the x25 map statement in order to allow PPP sessions over X.25 encapsulation with the configured AO/DI server:

```
interface BRI0:0
  x25 address 16193368208
  x25 aodi
  x25 htc 4
  x25 win 3
  x25 wout 3
  x25 map ppp 16193368209 interface dialer 1
```

Server Examples

The following example enables the AO/DI server to receive calls from the AO/DI client and configures the D channel (BRI0:0) with the x25 map statement which allows PPP sessions over X.25 encapsulation with the configured AO/DI client. The **no-outgoing** option is used with the x.25 map command since the AO/DI server is receiving, versus initiating, calls.

```
interface BRI0:0
x25 address 16193368209
x25 htc 4
x25 win 3
x25 wout 3
x25 map ppp 16193368208 interface dialer 1 no-outgoing
```



Note

Configuring the BRI interface with the **isdn x25 dchannel** command creates a configurable interface (bri 0:0).

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. Use the **no** form of this command to disable subaddressing.

```
x25 subaddress {line | number}
```

```
no x25 subaddress {line | number}
```

Syntax Description

line	The physical port number for the indicated line will be appended to the X.121 address as the subaddress.
<i>number</i>	Numeric variable assigned to a specific line.

Defaults

No default behavior or values.

Command Modes

Line configuration

Command History

Release	Modification
11.2F	This command was introduced.

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.

Examples

The following example shows how to configure subaddressing on vty 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
```

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 EXEC** command. Use the **no** form of this command to exit X.28 mode.

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 network user identification facility of the call request. Instead it 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
	11.2F	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 156 lists the commands available in both standard and extended command syntax.

Table 156 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 158.)
iclr	iclear	Request the remote device to clear the call.
int	interrupt	Send an Interrupt Packet.
par? par	parameter read	Show the current values of local parameters (see Table 157).
prof	profile <i>file-name</i>	Load a standard or a named profile.
reset		Reset the call.
rpar?	rread	Show 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 157.)
set?	setread	Change and then read 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 157 lists the different types of parameters you can set using the **set parameter-number: new-value** PAD command signal from X.28 mode.

Table 157 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 157 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.
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.

Table 157 Supported X.3 PAD Parameters (continued)

Parameter Number	ITU-T Parameter Name	ITU-T X.3 and Cisco Values
21	Parity treatment	Minimum value: 0; maximum value: 4; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
22	Page wait	Not supported.

**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 158 lists the options for the X.28 **help** command.

Table 158 X.28 help Command 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 number	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 name	Shows the specified parameter's name and current value.
help any-PAD-command	Describes the specified PAD command signal.

You can issue call requests from X.28 mode without using standard X.28 commands. To do this, use the following command syntax:

```
facilities-x121-addressDcall-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 call user data 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 call user data field, the call is placed to the X.121 address.

- While using standard command syntax, one or more facility request codes can be entered, followed by the code value. Additional facility request codes and values can also be entered; separate each entry with a comma, followed by a dash. An X.121 address and optional call user data 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 dash (-) followed by a string of digits (the X.121 address). The call request can be optionally terminated by an asterisk (*), a “P,” or a “D,” followed by some data.
- While using extended command syntax, 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 159 shows examples of parsed call requests.

Table 159 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

Use 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.

x3

To set X.3 packet assembler/disassembler (PAD) parameters, use the **x3** EXEC command.

x3 *parameter:value*

Syntax Description

parameter:value Sets the PAD parameters. (See Table 157 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, refer to the appendix titled “X.3 PAD Parameters” in this publication.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

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 back and forth 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**, **where**, and **resume** commands, which are available with all supported connection protocols, to do this.

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 Router-A. The remote host is 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.

xremote

To prepare the router for manual startup and initiate an XRemote connection, use the **xremote** EXEC command. This command begins the instructions that prompt you through the connection.

xremote

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes EXEC

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines If you do not use a host computer that supports XDMCP or LAT, you must use manual session startup. Manual session startup involves the following steps:

- Step 1** Enable XRemote manually on the router's port.
- Step 2** Connect to the host computer by using a **telnet**, **lat**, or **rlogin** command, then log on as usual.
- Step 3** Set the location of the X display.
- Step 4** Start client applications.
- Step 5** Return to the EXEC prompt.
- Step 6** Enter the **xremote** command to enable XRemote manually again on the server port.



Note In manual operation, the server and X terminal remain in XRemote mode until all clients disconnect or the access server receives a reset request from the X terminal. A session might terminate during startup because you invoked transient X clients that set some parameters (such as **xset** or **xmodmap**) and then disconnected. There must always be one session open or the connection resets.

Refer to the *Cisco IOS Dial Services Configuration Guide: Terminal Services* for more information about how to establish XRemote sessions between servers.

Examples

The following example starts a manual XRemote session:

```
dialup> xremote
XRemote enabled; your display is dialup:2006
Start your clients and type XRemote again
```

The router replies with a message informing you of your X display location. Use this information to tell the XRemote host the location of your X display server. If no clients are found, you see the following message:

```
No X clients waiting - check that your display is darkstar:2006
```

The following example shows a connection from an X display terminal through a router to a host running client programs:

```
dialup> xremote

XRemote enabled; your display is dialup:2006
Start your clients and type XRemote again

dialup> telnet eureka
Trying EUREKA.NOWHERE.COM (252.122.1.55)... Open

SunOS UNIX (eureka)

login: deal
Password:

Last login: Fri Apr 1 17:17:46 from dialup.nowhere.com
SunOS Release (SERVER+FDDI+DBE.patched) #14: Fri Apr 8 10:37:29 PDT 1994

eureka% setenv DISPLAY dialup:2006
eureka% xterm &
[1] 15439

eureka% logout

[Connection to EUREKA closed by foreign host]

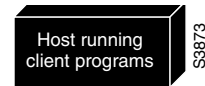
dialup> xremote
Entering XRemote
```

The following procedure shows how an XRemote connection is established for a configuration like the one shown in Figure 4. This example assumes that the administrator has set the user's display environment variable to identify the user's X display terminal.

-
- Step 1** From the PCX, MacX, or UNIX machine in Figure 4, the user connects to port 9003 on AccessServer1. If your administrator has configured a rotary number 7, the user connects to port 10007. For more information about rotary groups, refer to the *Cisco IOS Dial Services Configuration Guide: Terminal Services*.
 - Step 2** AccessServer1 connects the user to a modem.
 - Step 3** The modem calls AccessServer2.
 - Step 4** The user enters **xremote** at the AccessServer2 prompt.
 - Step 5** The user connects to the host from AccessServer2 using the **telnet** command.
 - Step 6** The user starts the X client program that will run on the host and display on the X display server (PCX, MacX, or UNIX host).

- Step 7** The user escapes from the host back to the AccessServer2, or logs out if clients were run in the background, and enters **xremote** command at the AccessServer2 prompt.
- You can use the master indexes or search online to find documentation of related commands.
-

Figure 4 XRemote Session Between Servers



The following example shows how to make an XRemote connection between servers. The number 9016 in the first line of the display indicates a connection to individual line 16. If the administrator had configured a rotary connection, the user enters 10000 plus the number of the rotary instead of 9016.

```
router% telnet golden-road 9016

Trying 192.31.7.84 ...
Connected to golden-road.cisco.com.
Escape character is '^]'.

User Access Verification

Password:
Password OK
```

```

--- Outbound XRemote service ---
Enter X server name or IP address: innerspace
Enter display number [0]:

Connecting to tty16... please start up XRemote on the remote system

atdt 13125554141
DIALING
RING
CONNECT 14400

User Access Verification
Username: deal
Password:
Welcome to the cisco dial-up access server.

dialup> xremote
XRemote enabled; your display is dialup:2006
Start your clients and type XRemote again

dialup> telnet sparks
Trying SPARKS.NOWHERE.COM (252.122.1.55)... Open

SunOS UNIX (sparks)

login: deal
Password:
Last login: Fri Apr 1 17:17:46 from dialup.nowhere.com
SunOS Release (SERVER+FDDI+DBE.patched) #14: Fri Apr 8 10:37:29 PDT 1994

sparks% setenv DISPLAY dialup:2006
sparks% xterm &
[1] 15439

sparks% logout

[Connection to SPARKS closed by foreign host]

dialup> xremote
Entering XRemote

```

Related Commands

Command	Description
xremote lat	Initiates a DEC window session over a LAT connection.
xremote xdm	Activates automatic session startup for an XRemote connection.

xremote lat

To initiate a DECwindow session over a local-area transport (LAT) connection, use the **xremote lat** EXEC command.

xremote lat *service*

Syntax Description	<i>service</i>	Name of the desired LAT service.
Command Modes	EXEC	
Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines If your host computer supports DECwindows login sessions, you can use automatic session startup to make an XRemote session connection. Once the system administrator at the remote host configures support for DECwindows over LAT, use the **xremote lat** EXEC command to initiate the connection. After you issue this command, the following events occur:

- The XRemote font server down-line loads several initial fonts for the DECwindows login display.
- The terminal displays the DIGITAL logo and DECwindows login box.

Log on to the host. Upon completion of login, more fonts are loaded, and the remote session begins.



Note

Because of heavy font usage, DECwindows applications can take longer than expected to start when using XRemote. Once the application starts, performance and access times should be as expected.

To exit XRemote sessions, you must quit all active X connections, usually with a command supported by your X client system. Usually, when you quit the last connection (when all client processes are stopped), XRemote closes and you return to the EXEC prompt. However, your X client system determines how the session closes.

Examples The following example begins connection with a LAT service named service1:

```
xremote lat service1
```

Related Commands	Command	Description
	xremote	Prepares the router for manual startup and initiates an XRemote connection.
	xremote xdm	Activates automatic session startup for an XRemote connection.

xremote tftp buffersize

To change the buffer size used for loading font files, use the **xremote tftp buffersize** command in global configuration mode. Use the **no** form of this command to restore the buffer size to the default value.

xremote tftp buffersize *buffersize*

no xremote tftp buffersize

Syntax Description	<i>buffersize</i>	Buffer size in bytes. This is a decimal number in the range from 4096 to 70000 bytes. The default is 70000.
---------------------------	-------------------	---

Defaults	70000 bytes
-----------------	-------------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	When the X terminal requests that a font file be loaded, the Cisco IOS software must first load the font file into an internal buffer before passing it to the X terminal. The default value of 70000 bytes is adequate for most font files, but the size can be increased as necessary for nonstandard font files.
-------------------------	---

The buffer size can be set as low as 4096 bytes and as large as the available memory on the router will allow. If you are using LAT font access, you should not lower the buffer size below the default, because the font directory for all of the LAT fonts (created internally) requires 70000 bytes.

This command applies to both TFTP and LAT font access.

Examples	The following example sets the buffer size to 20000 bytes:
-----------------	--

```
xremote tftp buffersize 20000
```

xremote tftp host

To add a specific Trivial File Transfer Protocol (TFTP) font server as a source of fonts for the terminal, use the **xremote tftp host** command in global configuration mode. Use the **no** form of this command to remove a font server from the list.

xremote tftp host *hostname*

no xremote tftp host *hostname*

Syntax Description	<i>hostname</i>	IP address or name of the host containing fonts.
---------------------------	-----------------	--

Defaults	No TFTP font server is specified.
-----------------	-----------------------------------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	Each time a new host name is entered, the list in the Cisco IOS software is updated. Font servers are queried in the order of their definition when the X terminal requests a font.
-------------------------	---

Examples	The following example sets the host IBM-1 as an XRemote TFTP font server:
-----------------	---

```
xremote tftp host IBM-1
```

The following example sets the host with IP address 10.0.0.7 as an XRemote TFTP font server:

```
xremote tftp host 10.0.0.7
```

xremote tftp retries

To specify the number of retries the font loader will attempt before declaring an error condition, use the **xremote tftp retries** command in global configuration mode. Use the **no** form of this command to restore the default retries number.

xremote tftp retries *retries*

no xremote tftp retries

Syntax Description	<i>retries</i>	(Optional) Number of retries. Acceptable values are decimal numbers in the range from 1 to 15.
---------------------------	----------------	--

Defaults	3 retries
-----------------	-----------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	Under certain conditions, you might need to increase the number of retries, particularly if the font servers are known to be heavily loaded.
-------------------------	--

Examples	<p>The following example sets the font loader retries to 5:</p> <pre>xremote tftp retries 5</pre>
-----------------	---

xremote xdm

To activate automatic session startup for an XRemote connection, use the **xremote xdm** EXEC command.

```
xremote xdm [hostname]
```

Syntax Description	<i>hostname</i> (Optional) Host computer name or IP address.
---------------------------	--

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

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines If your host computer supports a server running XDMCP (such as the *xdm* program included in X11R4 or later), you can use automatic session startup to make an XRemote session connection. To do so, use the **xremote xdm** EXEC command.

This command sends an X Display Manager Control Protocol (XDMCP) session startup request to the host computer. If you do not specify a host name or IP address, a broadcast message is sent to all hosts. The first host to respond by starting up a session is used.

The XRemote (the host) server and X terminal stay in XRemote mode until either the display manager terminates the session or the XRemote server receives a reset request from the X terminal.

To exit XRemote sessions, you must quit all active X connections, usually with a command supported by your X client system. Usually, when you quit the last connection (all client processes are stopped), XRemote closes and you return to the EXEC prompt. However, your remote X client system determines how the session closes.

To terminate a session, disconnect from the device on the network using the command specific to that device. Then, exit from the EXEC by using the **exit** command.

Examples The following example starts a session with a remote host named host1:

```
xremote xdm host1
```

Related Commands	Command	Description
	xremote	Prepares the router for manual startup and initiates an XRemote connection.
	xremote lat	Initiates a DEC window session over a LAT connection.

xremote xdm