

Resource Pool Management with Direct Remote Services

This document contains the following sections:

- **Feature Overview** on page 1
- **Benefits** on page 16
- **Restrictions** on page 17
- **Related Features and Technologies** on page 17
- **Related Documents** on page 17
- **Supported Platforms** on page 18
- **Supported MIBs and RFCs** on page 18
- **Prerequisites** on page 19
- **Configuration Tasks** on page 19
- **Configuration Examples** on page 28
- **Command Reference** on page 42

Feature Overview

Cisco Resource Pool Manager (RPM) enables telephone companies and Internet service providers (ISPs) to share dial resources for wholesale and retail dial network services in a single network access server (NAS) or across multiple NAS stacks. With Cisco RPM, service providers can count, control, and manage dial resources and provide accounting for shared resources when implementing different service-level agreements.

This document presents the single, standalone NAS version of Cisco RPM. For information on the Cisco Resource Pool Manager Server (RPMS) solution, see the Cisco Connection Online location at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/rpms/rpms_1-0/index.htm.

Cisco RPM is ideal for combining retail and wholesale dial services using Cisco AS5200, AS5300, and AS5800 network access servers. The Cisco RPM can be configured in one or more standalone Cisco NASs, or, optionally, across multiple NAS stacks by using one or more external Cisco Resource Pool Manager Servers (RPMSs). Call management and call discrimination can be configured to occur before the call is answered.

For call management, dial customers are differentiated by the use of configurable customer profiles. Each profile is based on the Dialed Number Information Service (DNIS) and the call type determined at the time of an incoming call.

When using call discrimination, the DNIS and call type are matched against a table of disallowed calls. When a call arrives at the NAS, if the DNIS and call type match an entry in this table, the call is rejected. Call discrimination can be used to manage the billing of calls to different types of resources.

When management by virtual private dialup network (VPDN) is configured, a VPDN group includes the information needed to set up or reject a VPDN session. VPDN setup can be based on the DNIS received during call setup, or on the domain name after the call is answered. Load balancing is used to achieve full usage of VPDN tunnels. The VPDN group can also serve as the “customer profile” when all calls are answered and sessions are identified and limited by domain name instead of DNIS.

To support data over voice bearer service (DoVBS), service providers use DNIS to direct calls to the appropriate resource. When a digital call arrives at the NAS through the voice network, it terminates on a High-Level Data Link Control (HDLC) controller rather than on a modem. In this application, the customer profile that the DNIS group is assigned has the associated call type of **speech** and the resource group directs the call to the HDLC controller.

Standalone Network Access Server (NAS)

A single NAS using Cisco RPM can provide:

- wholesale virtual private dialup network (VPDN) dial service to corporate customers
- direct remote services
- retail dial service to end users

Figure 1 and Figure 2 show multiple connections to a Cisco AS5300 NAS. Incoming calls to the NAS can use ISDN Private Rate Interface (PRI) signaling, channel associated signaling (CAS), or SS7 signaling protocol. Figure 1 shows incoming calls that are authenticated locally for retail dial services, or forwarded through VPDN tunnels for wholesale dial services.

Note This implementation does not use Cisco RPMS. If you are not using Cisco RPMS and you have more than one Cisco NAS, you must manually configure each NAS by using Cisco IOS commands. Resource usage information is not shared between NASs.

Figure 1 Retail Dial Service Using Resource Pool Management

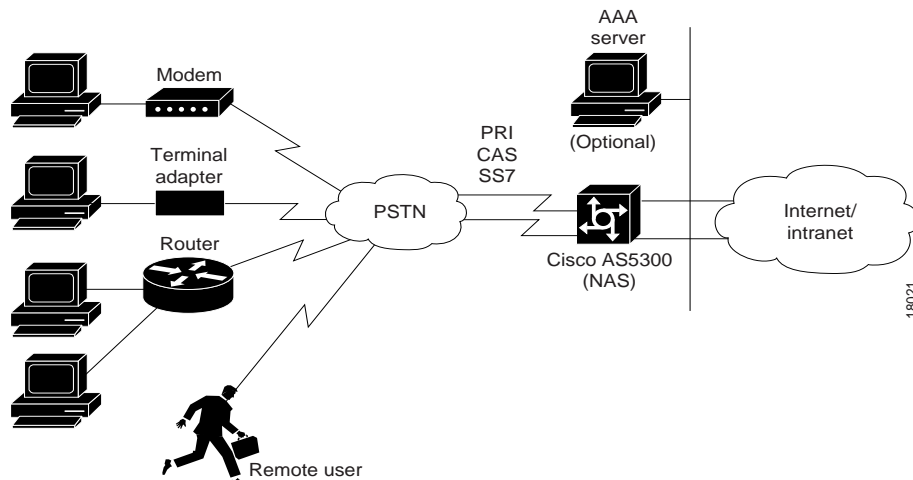
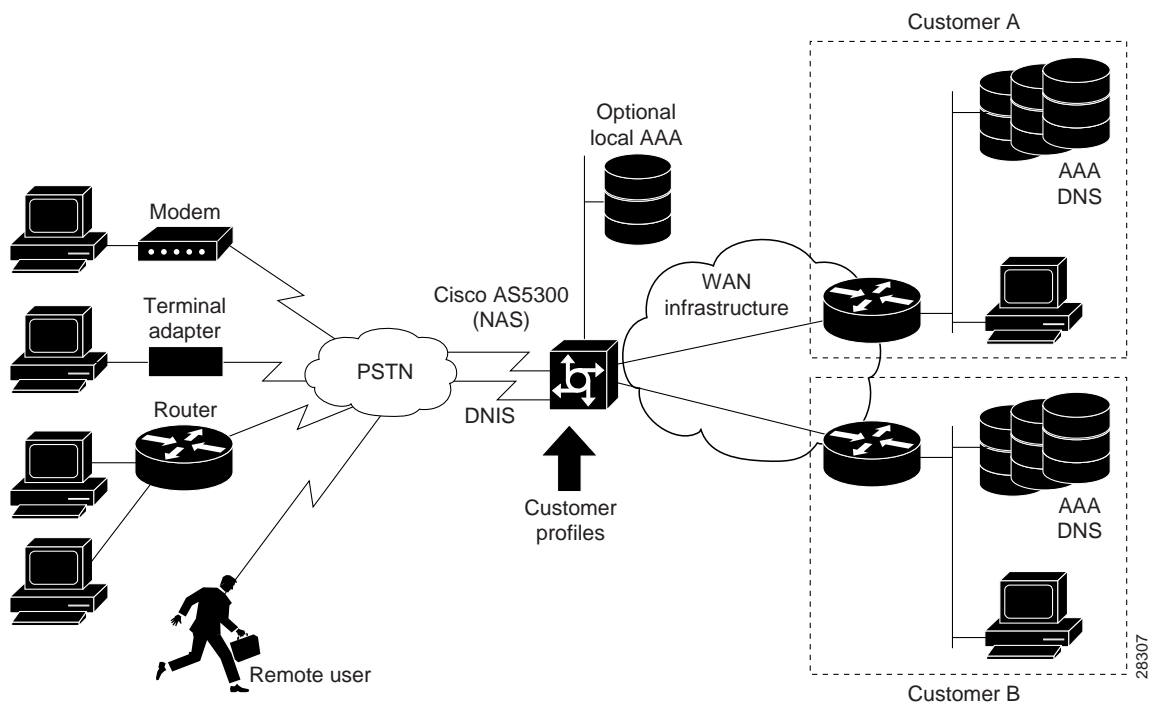


Figure 2 shows a method of implementing wholesale dial services without using VPDN tunnels. This is done by creating individual customer profiles consisting of authentication, authorization, and accounting (AAA) groups and Point-to-Point Protocol (PPP) configurations. The AAA groups provide IP addresses of AAA servers for authentication and accounting. The PPP configurations enable you to set different PPP parameter values on each customer profile. A customer profile typically includes the following PPP parameters:

- Applicable IP address pools or a default local list of IP addresses
- Primary and secondary domain name server (DNS) or Windows internet naming service (WINS)
- Authentication method (PAP, CHAP, MSCHAP)
- Number of links allowed for each call using Multilink PPP

Note The AAA and PPP integration applies to a single NAS environment; the external RPMS solution is not supported.

Figure 2 Resource Pool Management with Direct Remote Services



Components of Incoming and Outgoing Call Management

Cisco RPM manages both incoming calls and outgoing sessions. Cisco RPM differentiates dial customers through configured customer profiles based on the Dialed Number Information Service (DNIS) and call type determined when an incoming call comes in.

The components of incoming call management in the Cisco RPM are:

- Customer profiles
- DNIS groups
- Call types
- Resource groups
- Resource services

The components of outgoing session management in the Cisco RPM are:

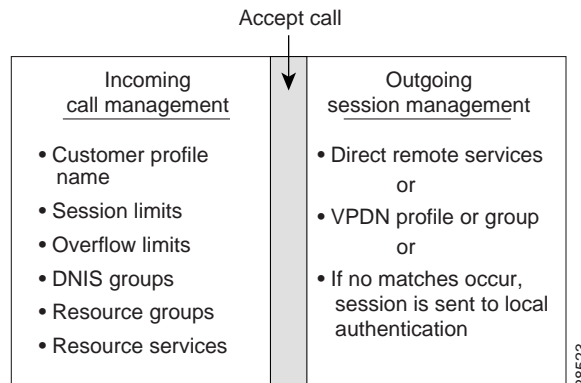
- VPDN groups
- VPDN profiles
- Direct remote services

Customer Profiles

A customer profile defines how and when a call is answered. Customer profiles include the following components (see Figure 3):

- Customer profile name
- Session limits—Maximum number of standard sessions
- Overflow limits—Maximum number of overflow sessions
- DNIS groups
- Resource groups
- Resource services
- VPDN profiles or groups
- Direct remote services source template

Figure 3 Components of a Customer Profile



The following types of customer profiles can be used on a NAS:

- DNIS-based customer profile—Associated with a specific DNIS group and used for a single NAS solution.
- Default customer profile—Associated with the default DNIS group and also used for a single NAS solution. This is most useful with domain-based VPDN services and for combining retail dial services with VPDN services. You can use up to four default customer profiles, each differentiated by the call type (speech, digital, V.110, V.120).
- Backup customer profile—Functionally the same as the two profiles above, except that the backup customer profile is applicable with an RPMS solution and is used only when connectivity between a NAS and the RPMS is lost. When the connection is restored, the call counters may not be synchronized.

See the RPMS documentation for a review of the RPMS fault tolerance and recovery mechanisms.

DNIS Groups

A DNIS group is a configured list of DNIS numbers that correspond to the numbers dialed to access particular customers, service offerings, or both. The Cisco RPM checks the DNIS number of inbound calls against the configured DNIS groups and selects a customer profile based on the following criteria:

- If Cisco RPM finds a match, it uses the configured information in the customer profile to which the DNIS group is assigned.
- If Cisco RPM does not find a match, it uses the configured information in the customer profile to which the default DNIS group is assigned.

The DNIS/call type sequence can only be associated with one customer profile.

Call Types

The following call types are supported in the Cisco RPM:

- Speech
- Digital
- V.110
- V.120

Note Voice over IP, Fax over IP, and dial-out calls are not currently supported.

Call types are used within a customer profile to assign calls to the appropriate resource based on:

- Q.931 bearer capability for ISDN PRI and SS7 calls
- Static DNIS group configuration for CAS (CT1, CT3, and CE1) calls

Note For information on SS7 implementation for RPM, see *Cisco Resource Pool Manager Server 1.0 SS7 Implementation* on Cisco Connection Online (CCO) at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/rpms/rpms_1-0/rpmsnote.htm.

Resource Groups

Resource groups represent groupings of similar hardware and/or firmware that are static and do not change on a per-call basis. Resource groups can be used to define resources that are port-based or non-port-based.

- Port-based resources are identified by physical location, such as a range of port/slot numbers (for example, modems or terminal adapters).
- Non-port-based resources are identified by a single size parameter (for example, HDLC framers or V.120 terminal adapters). Note that V.120 terminal adapters are currently implemented as part of the Cisco IOS software.

The Cisco RPM:

- Enables you to configure resource groups on a Cisco NAS and apply them to a customer profile to maximize the use of available shared resources and thus support service-level agreements for various resource allocation schemes.
- Allows you to combine your Cisco NAS resource groups with call types (speech, digital, V.110, and V.120) and optional resource modem services. Resource groups and services are assigned to incoming calls through DNIS groups and call types.

Note Resources not configured in the NAS as part of a resource group and not assigned to a customer profile cannot be used by Cisco RPM or Cisco RPMS.

Note To support ISDN Data over Voice Bearer Service (DoVBS), use a DNIS group and a configured customer profile to direct the speech call to the appropriate digital resource. The resource group assigned to this customer profile is **digital resources** with a call type of **speech**, so the call will terminate on an HDLC controller rather than on a modem.

Resource Services

A resource service contains a finite series of resource command strings that can be used to dynamically configure an incoming connection.

Services supported by a resource group are determined by the combination of hardware and firmware installed. Currently, resource services:

- Can be configured and applied to resource groups containing only MICA modems.
- Can be configured to affect minimum and maximum speed, modulation, error correction, and compression as shown in Table 1.

Table 1 Resource Services for Resource Groups Containing MICA Modems

Service	Options	Comments
min-speed	<300—56000>, any	Must be a V.90 increment
max-speed	<300—56000>, any	Must be a V.90 increment
modulation	k56flex, v22bis, v32bis, v34, v90, any	
error-correction	lapm, mn14	Hidden command
compression	mmps, v42bis	Hidden command

VPDN Groups

A VPDN group contains the data required to build a VPDN tunnel from the Cisco RPM NAS L2TP Access Concentrator (LAC) to the L2TP Network Server (LNS). In the context of RPM, VPDN is authorized by first associating a customer profile with a VPDN group, and second by associating the VPDN group to the DNIS group used for that customer profile. VPDN groups are assigned to customer profiles as follows:

- For DNIS-based VPDN dial services, VPDN groups are assigned to customer profiles based on the configured DNIS groups.
- For domain-based VPDN dial services, VPDN groups are assigned to customer profiles with the default DNIS group and matching call-type assignment.

VPDN group data includes the endpoint IP addresses. Cisco RPM enables you to specify multiple IP endpoints for a VPDN group. If two or more IP endpoints are specified, Cisco RPM uses a load-balancing method to ensure traffic is distributed across the IP endpoints.

The VPDN group provides call management by allowing limits to be applied to both the number of multilink PPP bundles per tunnel and the number of links per multilink PPP bundle. Limits can also restrict the number of sessions per IP endpoint. If you require more granular control of VPDN counters, use VPDN profiles.

VPDN Profiles

VPDN profiles allow for session and overflow limits to be imposed for a particular customer profile. These limits are unrelated to the limits imposed by the customer profile. A customer profile is associated with a VPDN profile. A VPDN profile is associated with a VPDN group. VPDN profiles are required only when these additional counters are required for VPDN usage per customer profile.

Direct Remote Services

Direct remote services is an enhancement to Cisco resource pool management (RPM) implemented in Cisco IOS Release 12.0(7)T that enables service providers to implement wholesale dial services without using VPDN tunnels. A customer profile that has been preconfigured with a PPP template to define the unique PPP services for the wholesale dial customer is selected by the incoming DNIS and call type. At the same time, the DNIS is used to select AAA server groups for authentication/authorization and for accounting for the customer.

PPP Common Configuration Architecture (CCA) is the new component of the RPM customer profile that enables direct remote services. The full PPP command set available in Cisco IOS software is configurable per customer profile for wholesale dial applications. A customer profile typically includes the following PPP parameters:

- Local or named IP address pools
- Primary and secondary domain name server (DNS) or Windows internet naming service (WINS) addresses
- Authentication method (PAP, CHAP, MS-CHAP)
- Multilink PPP links per bundle limits

The AAA session information is selected by the incoming DNIS. AAA server lists provide the IP addresses of AAA servers for authentication, authorization, and accounting in the wholesale customer's local network. The server lists for both authentication and authorization and for accounting contain the server addresses, AAA server type, timeout, retransmission, and keys per server.

When direct remote services is implemented on a Cisco NAS, the following events occur:

- 1 The NAS sends an authorization request packet to the AAA server by using the authentication method (PAP, CHAP, MSCHAP) that has been configured through PPP.
- 2 The AAA server accepts the authorization request and returns one of the following items to the NAS:
 - (a) a specific IP address
 - (b) an IP address pool name
 - (c) nothing
- 3 Depending on the response from the AAA server, the NAS assigns one of the following items to the user through the DNS/WINS:
 - (a) the IP address returned by the AAA server
 - (b) an IP address randomly assigned from the named IP address pool
 - (c) an IP address from a pool specified in the customer profile template

Note If the AAA server sends back to the NAS a named IP address pool and that name does not exist on the NAS, the request for service is denied. If the AAA server does not send anything back to the NAS and there is an IP address pool name configured in the customer profile template, an address from that pool is used for the session.

Processes of Incoming and Outgoing Call Management

This section describes the following topics:

- Call Treatment
- Call Discrimination
- Base Session and Overflow Session Limits
- VPDN Session and Overflow Session Limits
- VPDN MLP Bundles and Links-Per-Bundle Limits
- VPDN Tunnel Limits
- Call Management Functional Descriptions

Call Treatment

Call treatment determines how calls are handled when certain events require the call to be rejected. For example, if the session and overflow limits for one of your customers has been exceeded, any additional calls receive a busy signal. Table 2 summarizes the various call treatment options.

Table 2 Call Treatment Events and Options

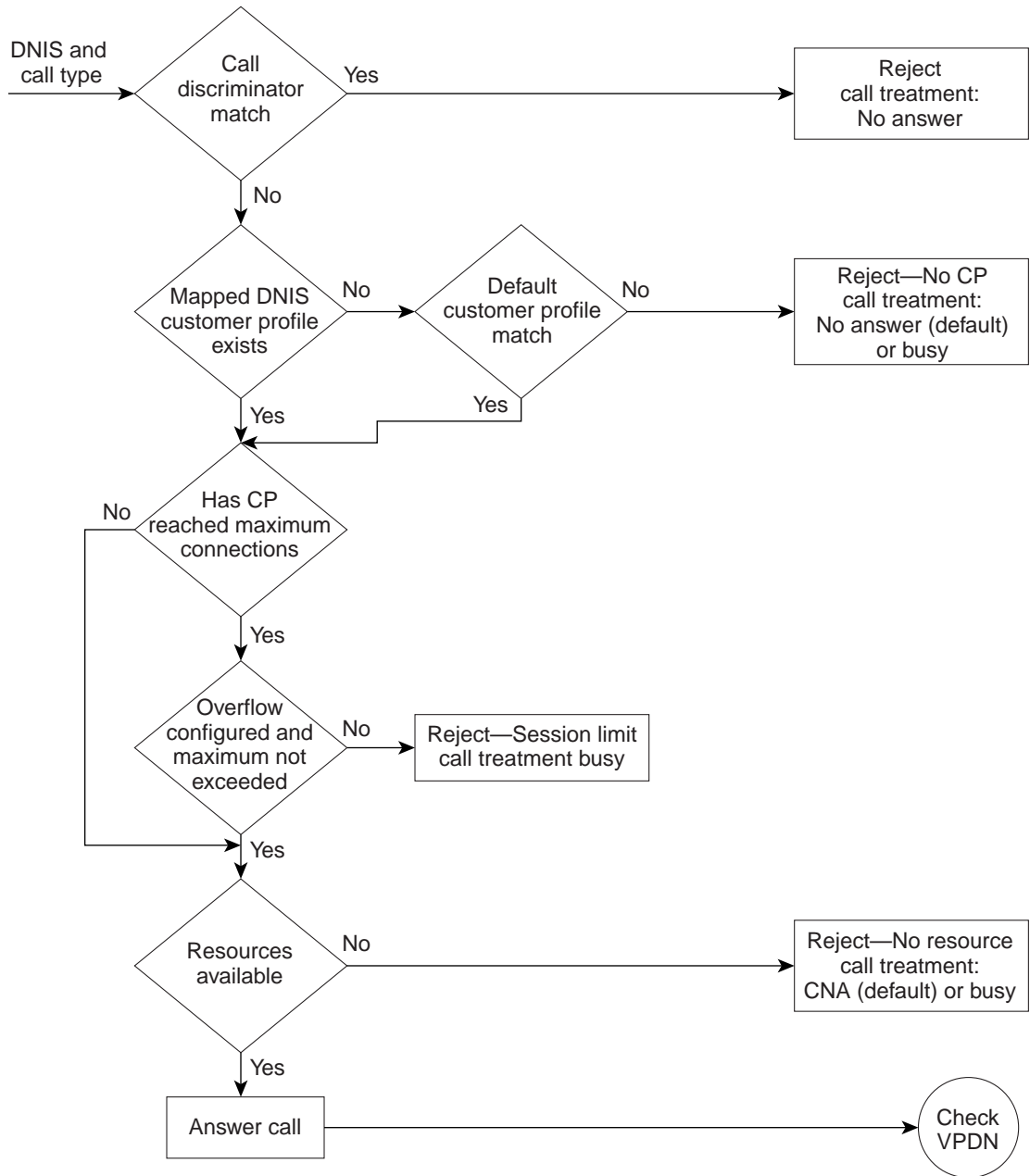
Event	Call Treatment Option	Results
Customer profile not found	No answer (default)	The caller receives rings until the switch eventually times out. Implies that the NAS was appropriate, but resources were unavailable. The caller should try later.
	Busy	The switch drops the call from the NAS and sends a busy signal back to the caller. The call is rejected based on not matching a DNIS group/call type and customer profile. Can be used to immediately reject the call and free up the circuit.
Customer profile limits exceeded	Busy	The switch drops the call from the NAS and sends a busy signal back to the caller.
NAS resource not available	Channel not available (default)	The switch sends the call to the next channel in the trunk group. The call can be answered, but the NAS does not have any available resources in the resource groups. Allows the switch to try additional channels until it gets to a different NAS in the same trunk group that has the available resources.
	Busy	The switch drops the call from the NAS and sends a busy signal back to the caller. Can be used when the trunk group does not span additional NASs.
Call discriminator match	No answer	The caller receives rings until the switch eventually times out.

Call Discrimination

Resource pool management offers a call discrimination feature that rejects calls based on a DNIS group and a call type filter. When a call arrives at the NAS, the DNIS and the call type are matched against a table of disallowed calls. If the DNIS and call type match entries in this table, the call is rejected before it is assigned Cisco NAS resources, or before any other Cisco RPM processing occurs.

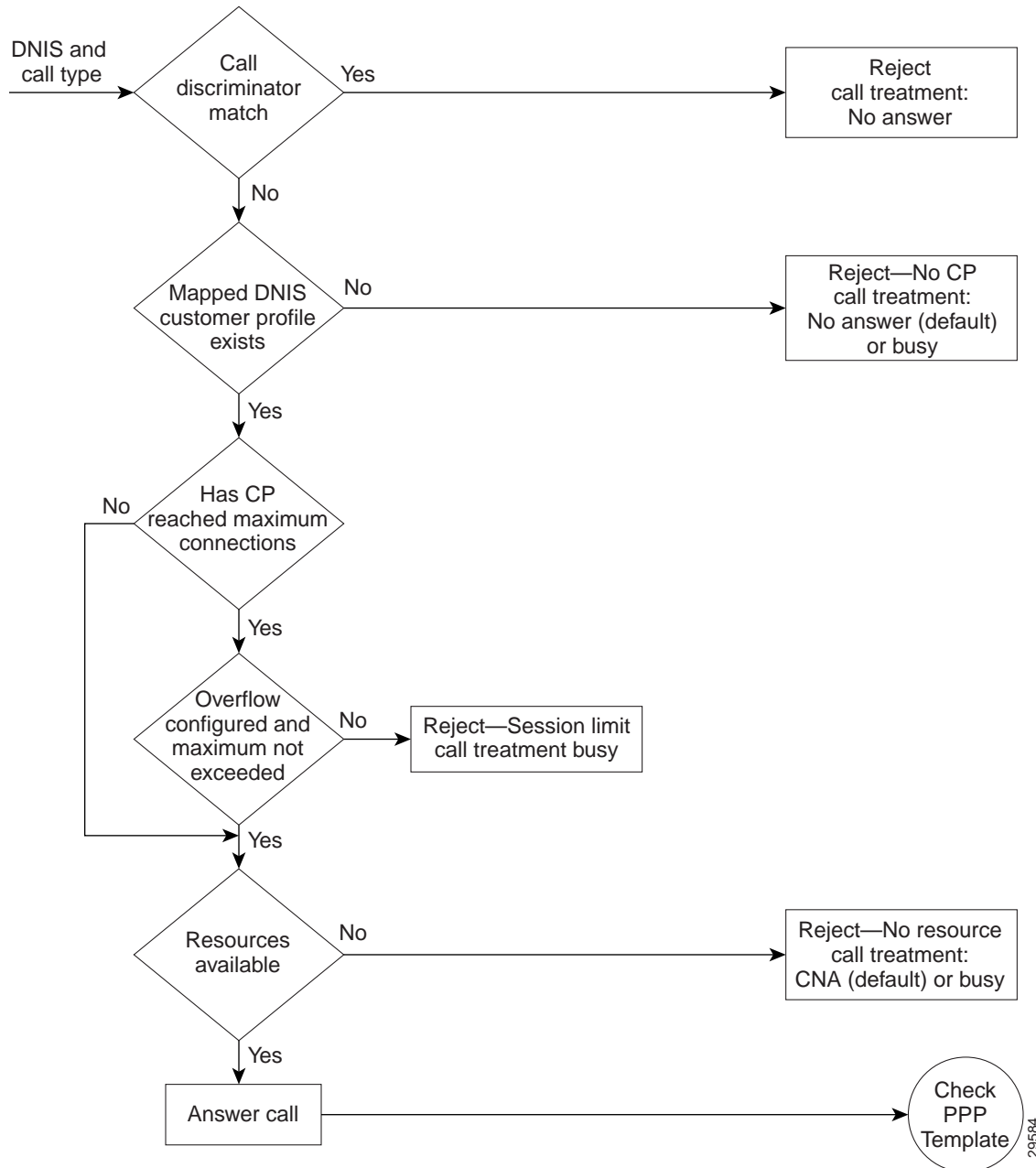
Figure 4 and Figure 5 show the sequence of call discrimination/call processing events which take place when an incoming call arrives at the Cisco NAS. Figure 4 shows the sequence for a Cisco NAS that is not using direct remote services. Figure 5 shows the sequence that occurs when direct remote services is being used.

Figure 4 RPM Call-Processing Flowchart for a Standalone NAS



22609

Figure 5 RPM Call-Processing Flowchart for a Standalone NAS with Direct Remote Services

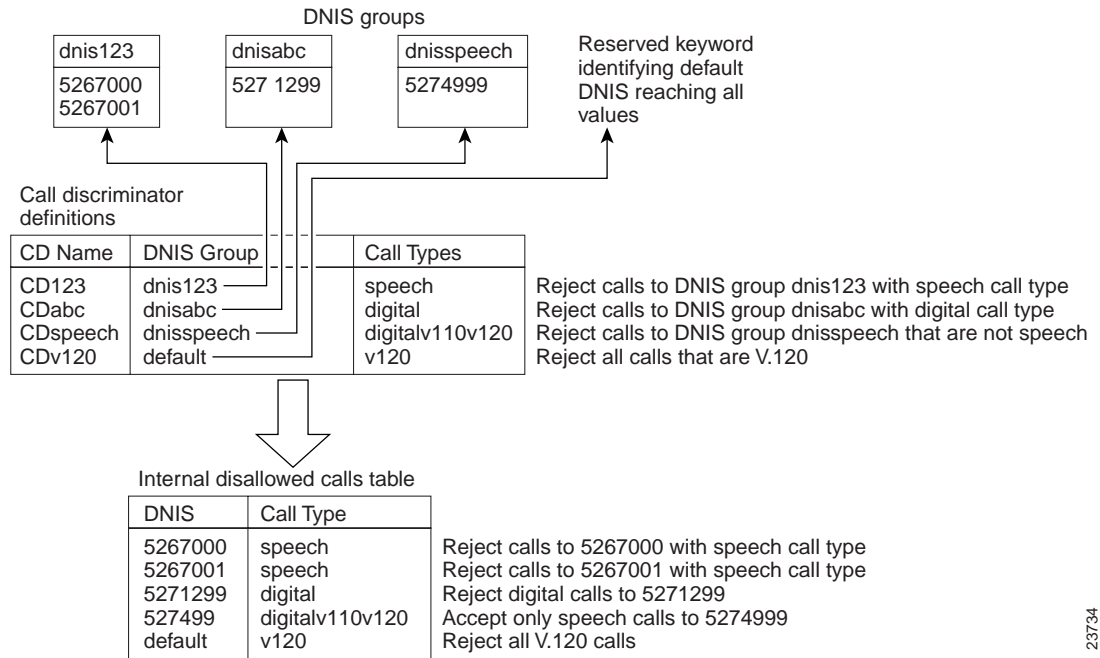


You can use call discrimination to manage billing of calls to different types of resources. If you have a different billing structure for modem calls and for digital calls, each call type is assigned a different DNIS. When a user calls the DNIS, the call type must be of the allowed call type or the call is rejected.

For example, to restrict a specific DNIS group to modem calls only, create call discrimination settings for the DNIS group and the other call types (digital, V.110, and V.120) as shown in Figure 6.

Note Supported call types are speech, digital, V.110, and V.120.

Figure 6 Call Discrimination



23734

Base Session and Overflow Session Limits

The Cisco RPM enables you to set base and overflow session limits in each customer profile.

The base session limit determines the maximum number of non-overflow sessions supported for a customer profile. When the base session limit is reached, any new calls are rejected unless overflow sessions are enabled. If overflow sessions are enabled, new sessions up to the session overflow limit are processed and marked as overflow for call handling and accounting. The RPM call counters and AAA accounting records indicate whether a call is considered overflow for tracking and billing.

The overflow session limit determines the allowable number of sessions above the session limit. If the overflow session limit is greater than zero, overflow sessions are enabled. The maximum number of allowed sessions is the base session limit plus the overflow session limit. When the overflow session limit is reached, any new calls are rejected.

Enabling overflow sessions is useful for allocating extra sessions for preferred customers at premium rates. Overflow sessions can also be useful for encouraging customers to adequately forecast bandwidth usage or for special events when normal session usage is exceeded. For example, if a customer has a corporate-wide program and many people are expected to request remote access, you can enable many overflow sessions and charge a premium rate for the extra bandwidth used.

Note An overflow call is a call received when the base session limit is exceeded and is in an overflow state. When a call is identified as an overflow call, the call maintains the overflow status throughout its duration—even if the number of current sessions returns below the base session limit.

Table 3 Effects of Session Limit and Session Overflow Limit Settings Combinations

Base Session Limit	Session Overflow Limit	Call Handling
0	0	Reject all calls.
10	0	Accept up to 10 sessions.
10	10	Accept up to 20 sessions and mark sessions 11 to 20 as overflow sessions.
0	10	Accept up to 10 sessions and mark session 1 to 10 overflow sessions.
All	0	Accept all calls.
0	All	Accept all calls and mark all calls as overflow.

VPDN Session and Overflow Session Limits

The Cisco RPM enables you to configure base and overflow session limits per VPDN profile for managing VPDN sessions.

Note The VPDN session and overflow session limits are independent of the limits set in the customer profiles.

The base VPDN session limit determines the maximum number of non-overflow sessions supported for a VPDN profile. When the base VPDN session limit is reached, any new VPDN calls using the VPDN profile sessions are disconnected unless overflow sessions are enabled. If overflow sessions are enabled, new sessions up to the overflow session limit are processed and marked as overflow for VPDN accounting.

The VPDN overflow session limit determines the number of sessions above the base session limit allowed in the VPDN group. If the overflow session limit is greater than zero, overflow sessions are enabled. The maximum number of allowed sessions is the base session limit plus the overflow session limit. When the overflow session limit is reached, any new calls are disconnected.

VPDN MLP Bundles and Links-Per-Bundle Limits

To ensure resources are not consumed by a few users with multilink PPP (MLP) connections, the Cisco RPM also enables you to specify the maximum number of MLP bundles that can be opened in a VPDN group. In addition, you can specify the maximum number of links for each MLP bundle.

For example, if standard ISDN users access the VPDN profile, limit this setting to two links per bundle. If video conferencing is used, increase this setting to accommodate the necessary bandwidth (usually six links). These limits have no overflow options and are configured under the VPDN group component.

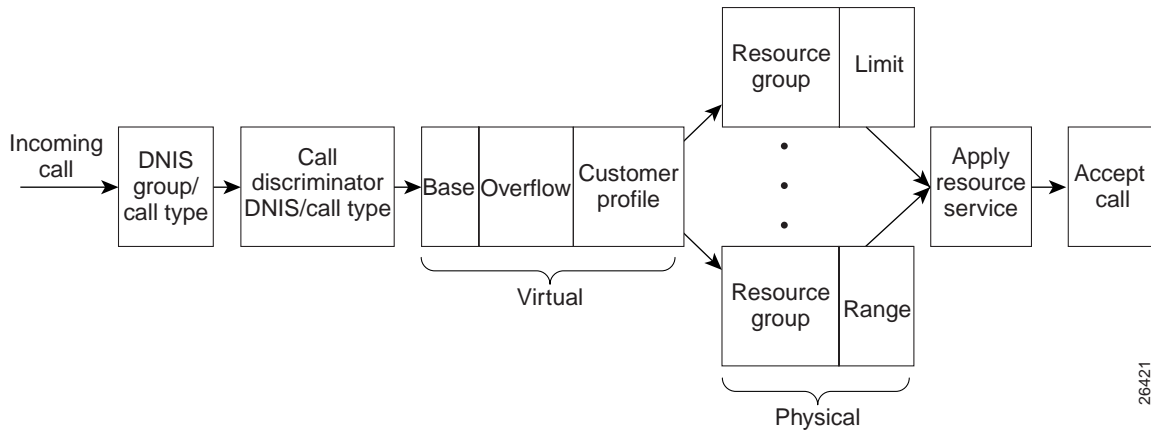
VPDN Tunnel Limits

For increased VPDN tunnel management, the Cisco RPM enables you to set an IP endpoint session limit for each IP endpoint. IP endpoints are configured for VPDN groups.

Call Management Functional Descriptions

Figure 7 and Figure 8 depict the processes of incoming and outgoing call management that have been described in the previous sections.

Figure 7 RPM Functional Description for Incoming Call Management



26421

When a DNIS call comes in, the Cisco NAS chooses an authentication/authorization server and an accounting server.

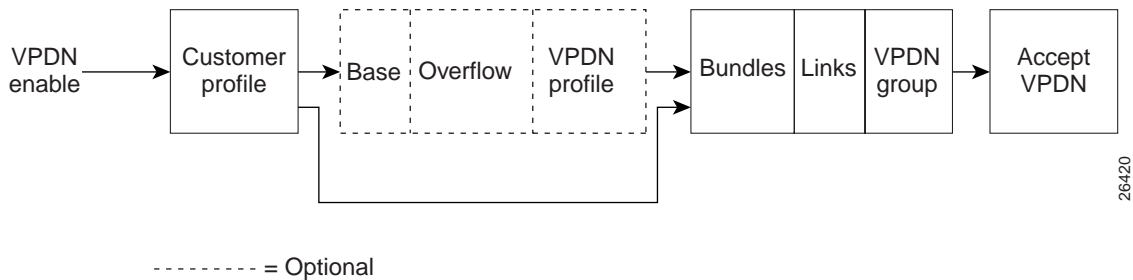
For information on RADIUS multiple UDP ports support for RPM, see *Configuring RADIUS for Multiple UDP Ports Support*. For information on AAA server groups based on DNIS implementation for RPM, see *Selecting AAA Server Groups Based on DNIS*.

Incoming call management includes the following processes:

- The incoming DNIS is mapped to a DNIS group; if there is no incoming DNIS number, or the DNIS number provided does not match any configured DNIS group, the DNIS group *default* is used.
- The mapped DNIS group is checked against configured call discriminator profiles to confirm if this DNIS group/call type combination is disallowed. If there is a match, the call is immediately rejected.
- Once a DNIS group or a default DNIS group is identified, the customer profile associated with that DNIS group and call type (from the bearer capability for ISDN calls; statically configured for CAS calls) is selected. If there is no corresponding customer profile, the call is rejected.
- The customer profile includes a base session limit value and an overflow session limit value. If these thresholds have not already been met, the call is assigned the appropriate resource defined in the customer profile. If the thresholds have been met, the call is rejected.
- If resources are available from the resource group defined in the customer profile, the call is answered. Otherwise, the call is rejected.
- As sessions start and end, the session counters increase and decrease, so the customer profile call counters are kept current.

Outgoing call management is depicted in Figure 8.

Figure 8 RPM Functional Description for Outgoing Call Management



Outgoing call management includes the following processes:

- After the call is answered and if VPDN is enabled, the Cisco RPM checks the customer profile for an assigned VPDN group or profile.
- If a VPDN profile is found, the limits for number of multilink bundles and number of links per bundle are checked:
 - If the limits have not been exceeded, the VPDN group data associated with that VPDN profile is used to build a VPDN tunnel.
 - If the VPDN limits have been exceeded, the call is disconnected.
- If a VPDN group is found within the customer profile, the VPDN group data is used to build a VPDN tunnel:
 - If the VPDN group limits for number of multilink bundles and number of links per bundle have not been exceeded, a VPDN tunnel is built.
 - If the limits have been reached, the call is disconnected.
- The outgoing session management of the customer profile directs the answered call to the appropriate destination:
 - To a PPP command set/feature set and AAA server group for direct remote services.
 - To a tunnel that is established between the NAS or L2TP Access Concentrator (LAC) and a wholesale (VPDN) dial customer's home gateway (HGW) or L2TP Network Server (LNS) using L2F or L2TP tunneling technology.
 - To a local AAA server of retail dial applications and Internet and intranet access.
- If no VPDN profile is assigned to the customer profile and VPDN is enabled, non-RPM VPDN service is attempted. If this non-RPM VPDN service fails, the call is processed as a retail dial service call if local AAA service is available.

Accounting Data

You can generate accounting data for network dial service usage in NAS AAA attribute format. You can configure the Cisco NAS to generate AAA accounting records for access to an external AAA server. The accounting start and stop records in AAA attribute format are sent to the external AAA server by using either RADIUS or TACACS+ protocols for accounting data storage. Table 4 lists the new fields in the AAA accounting packets.

Table 4 AAA Accounting Records

Accounting Start Record	Accounting Stop Record
Call-Type	Disconnect-Cause
CAS-Group-Name	Modem-Speed-Receive
Customer-Profile-Name	Modem-Speed-Transmit
Customer-Profile-Active-Sessions	MLP-Session-ID
DNIS-Group-Name	
Overflow	
MLP-Session_ID	
Modem-Speed-Receive	
Modem-Speed-Transmit	
VPDN-Domain-Name	
VPDN-Tunnel-ID	
VPDN-HomeGateway	
VPDN-Group-Active-Sessions	

Data over Voice Bearer Services

Data over Voice Bearer Services (DoVBS) is a dial service that uses a customer profile and an associated resource group of digital resources to direct data calls with a speech call type to HDLC controllers.

To support ISDN DoVBS, use a DNIS group and a configured customer profile to direct the speech call to the appropriate digital resource.

The resource group assigned to this customer profile is **digital resources**; the call type is **speech**. The call terminates on an HDLC controller rather than on a modem.

Benefits

Cisco Resource Pool Manager with direct remote services gives data network service providers the capability to:

- Manage customer use of shared resources, such as modems or HDLC controllers for data calls.
- Offer advanced wholesale dial-up services directly to customers. Because the PPP and AAA feature sets are selected by the incoming DNIS, the service provider no longer needs tunneling technology to provide unique service-level agreements to wholesale dial customers.
- Efficiently use resource groups, such as modems to offer differing over-subscription rates and dial service-level agreements.
- Deploy Data over Voice Bearer Service (DoVBS).
- Accept or reject a call based on the incoming DNIS number before answering the call.
- Include local retail dial services in the same NAS with the wholesale dial customers.

The Cisco RPM customer profile template provides a strong, single NAS solution with the following benefits for providers of wholesale dial services:

- Call acceptance is determined by the Cisco RPM before call answering by using the configured size limits and resource availability.
- The answered call uses the PPP configuration defined in the template to initiate authentication, obtain an IP address, and select a DNS or WINS that is located at the customer's site.
- The same DNIS that was used to choose the customer profile selects the servers for authentication/authorization and accounting that are located at the wholesale customer's site.

Restrictions

- Ear and Mouth Feature Group B (E&M-FGB) is the only signaling type supported for channel associated signaling (CAS) on T1 and T3 facilities; R2 is supported for E1 facilities. Feature Group (FG) D is not currently supported.
- The Cisco IOS software collects DNIS digits for E&M-FGB CAS signaling. For all other CAS signaling types, use the default DNIS group customer profiles.
- The Resource Pool Manager application requires the NPE 300 processor when implemented on the Cisco AS5800.
- Use resource pool management services with MICA modems only.
- Modem pooling and resource pool management are not compatible.

Related Features and Technologies

- Authentication, Authorization, and Accounting (AAA)
- Point-to-Point Protocol (PPP)
- Virtual Private Dial-up Network (VPDN)
- SS7 Signaling

Related Documents

- *Cisco AS5200 Universal Access Server Software Configuration Guide*
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5200/52swcfg2/index.htm
- *Cisco AS5300 Software Configuration Guide*
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/53swcf2/index.htm
- *Cisco AS5800 Access Server Software ICG*
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/58sw_icg/index.htm
- *Cisco Access VPN Solutions Using Tunneling Technology*
http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/vpn_soln/index.htm
- *Cisco Resource Pool Manager Server Configuration Guide*
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/rpms/rpms_1-0/rpmsconf/index.htm
- *Cisco Resource Pool Manager Server Installation Guide*
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/rpms/rpms_1-0/rpms_ins/index.htm

- *Cisco Resource Pool Manager Server Solutions Guide*
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/rpms/rpms_1-0/rpms_sol/index.htm
- *Dial Solutions Quick Configuration Guide (Cisco IOS Release 12.0)*
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12supdoc/dsqcg3/index.htm>
- *Redundant Link Manager*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113aa/113aa_7/rlm_rel2.htm
- *Release Notes for Cisco Resource Pool Manager Server Release 1.0*
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/rpms/rpms_1-0/rpmsnote.htm
- *SS7 Continuity Testing for Network Access Servers*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113aa/113aa_5/cot.htm
- *SS7 Dial Solution System Integration*
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/iosinfo/ios_mods/5420.htm
- *Configuring RADIUS for Multiple User Datagram Protocol Ports*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/rad_udp6.htm
- *Selecting AAA Server Groups Based on DNIS*
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/serdnis6.htm>

Supported Platforms

The following platforms support resource pool management in NAS standalone and external server scenarios for this Cisco IOS release:

- Cisco AS5200
- Cisco AS5300
- Cisco AS5800

Supported MIBs and RFCs

MIBs

- CALL-RESOURCE-POOL-MIB
- CISCO-VPDN-MANAGEMENT-MIB

For descriptions of supported MIBs and how to use MIBs, see Cisco's MIB web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

None

Prerequisites

- For the Cisco AS5200 and Cisco AS5300, Cisco IOS Release 12.0(4)XI1 or later releases must be running on the NAS.
- For the Cisco AS5800, Cisco IOS Release 12.0(5)T or later releases must be running on the NAS.
- A minimum of 64 MB must be available on the DMM cards.
- Before configuring resource pool management, verify the operation of the following features as described in the appropriate documentation listed in “Related Documents”:
 - Ensure AAA operation (if enabled)
 - Ensure PPP operation
 - Ensure VPDN operation (if enabled)

See *Configuring the NAS for Basic Dial Access* for more information:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/vpn_soln/l2fcase/l2ftask1.htm

Configuration Tasks

The following configuration tasks are used to configure a Cisco NAS for resource pool management:

- Enabling Resource Pool Management
- Configuring DNIS Groups
- Configuring Discriminator Profiles
- Configuring Resource Groups
- Configuring Service Profiles
- Configuring Customer Profiles
- Configuring Customer Profile Templates
- Configuring AAA Server Groups
- Configuring VPDN Profiles
- Configuring VPDN Groups

These tasks are described in the following sections:

Enabling Resource Pool Management

To enable resource pool management on a Cisco NAS, perform the following steps, beginning from global configuration mode.

Step	Command	Purpose
1	Router(config)# resource-pool { <i>enable</i> <i>disable</i> }	Enable resource pool management (RPM).
2	Router(config)# resource-pool call treatment resource { <i>busy</i> <i>channel-not-available</i> }	Specify the desired call treatment when resource allocation fails to connect an incoming call.
3	Router(config)# resource-pool call treatment profile { <i>busy</i> <i>no-answer</i> }	Specify the desired call treatment when profile authorization fails for an incoming call.
4	Router(config)# resource-pool aaa protocol (<i>local</i> <i>group name</i>)	Specify the authentication/authorization and accounting protocol for RPM. Group name specifies an authorization method that is not local; for example, an external AAA server group.

Example

The following example shows the commands used to enable resource pool management and establish the call treatments for incoming calls when resource allocation fails to connect (channel-not-available) and when profile authorization fails (no-answer). It also shows that local AAA has been chosen for the RPM configuration:

```
Router(config)# resource-pool enable
Router(config)# resource-pool call treatment resource channel-not-available
Router(config)# resource-pool call treatment profile no-answer
Router(config)# resource-pool aaa protocol local
```

Note that with RPM disabled, the resource groups will still take effect (that is, modem pooling will not be possible).

Note If you have an RPMS, you do not need to define VPDN groups and profiles, customer profiles, or DNIS groups on the NAS—you only need to define resource groups. Configure the remaining items by using the RPMS system.

Configuring DNIS Groups

This configuration task is optional. For default DNIS service, no DNIS group configuration is required. The following characteristics and restrictions apply to DNIS group configuration:

- Each DNIS group/call type combination can apply to only one customer profile.
- You can use up to four default DNIS groups (one for each call type).
- You must statically configure CAS call types.
- You can use x, X or . as wildcards within each DNIS number.

To configure DNIS groups for RPM implementations, perform the following steps, beginning from global configuration mode.

Step	Command	Purpose
1	Router(config)# dialer dnis group { <i>dnis-group-name</i> }	Create a DNIS group with a name of your choice. The name you specify in this step must be used when configuring the customer profile (see “Configuring Customer Profiles” on page 23).
2	Router(config-dnis-group)# call-type cas { <i>digital</i> <i>speech</i> }	Statically set the call-type override for incoming CAS calls to either digital or speech.
3	Router(config-dnis-group)# number <i>number</i>	Add a DNIS number to the dialer DNIS group to be used in the customer profile. The DNIS number may have up to 65 characters; wildcards may be used.

Example

The following example shows the commands used to configure a DNIS group named *cisco* with a call type override for incoming CAS calls of *speech* and the DNIS numbers of *5552221210* through *5552221219*:

```
Router(config)# dialer dnis group cisco
Router(config-dnis-group)# call-type cas speech
Router(config-dnis-group)# number 555222121x
```

Configuring Discriminator Profiles

Discriminator profiles enable you to process calls differently based on the call type and DNIS combination. To configure discriminator profiles for RPM implementation, perform the following steps, beginning from global configuration mode.

Step	Command	Purpose
1	Router(config)# resource-pool profile discriminator <i>name</i>	Create a call discriminator profile and assign it a name of up to 23 characters.
2	Router(config-call-discrimin)# call-type { <i>all</i> <i>digital</i> <i>speech</i> <i>v110</i> <i>v120</i> }	Specify the type of calls you want to block. The NAS will not answer the call-type you specify.
3	Router(config-call-discrimin)# dnis group { <i>dnis-group-name</i> <i>default</i> }	Enter the name of the DNIS group to be rejected by this call discriminator profile.

Note To create a call discriminator profile, you must specify both a call-type and a DNIS group. Once a DNIS group is associated with a call type in a discriminator, it cannot be used in any other discriminator.

Example

The following example shows a call discriminator named *blocked1* being created and configured to block speech calls from the DNIS group named *remotephone*:

```
Router(config)# resource-pool profile discriminator blocked1
Router(config-call-discrimin)# call-type speech
Router(config-call-discrimin)# dnis group remotephone
```

Configuring Resource Groups

Note For external Cisco RPMS environments, configure resource groups on the NAS before defining them on external RPMS servers. For standalone NAS environments, first configure resource groups before using them in customer profiles.

- Resource groups can apply to multiple customer profiles.
- You can separate the physical resources into different resource groups.

Note Do not put heterogenous resources in the same group. Do not put MICA modems in the same group as Microcom modems. Do not put modems and HDLC controllers in the same resource group. Do not configure "port" and "limit" parameters in the same resource group.

To configure resource groups for RPM implementations, perform the following steps, beginning from global configuration mode.

Step	Command	Purpose
1	Router(config)# resource-pool group resource name	Create a resource group and assign it a name of up to 23 characters.
2	Router(config-resource-group)# range {port {slot/port slot/port} {limit number}	Associate a range of modems or other physical resources with this resource group. <ul style="list-style-type: none"> • For port-based resources, use the physical locations of the resources. • For non-port-based resources, use a single integer limit—Specify the maximum number of simultaneous connections supported by the resource group. Up to 192 connections may be supported depending on the hardware configuration of the access server.

Example

The following example shows the creation of a resource group *modem1* with ports set ranging from 0 to 47:

```
Router(config)# resource-pool group resource modems1
Router(config-resource-group)# range port 1/0 1/47
```

The following example shows the creation of a resource group named *hdlc1* supporting a range limit set for 48 simultaneous connections:

```
Router(config)# resource-pool group resource hdlc1
Router(config-resource-group)# range limit 48
```

Configuring Service Profiles

Service profiles are used to configure modem service parameters for MICA modems. Note the following characteristics of service profiles:

- Service profiles apply only to MICA modems (speech or V.110).

- Error-correction and compression are hidden parameters that may be included in a service profile. For more information, see “modem min-speed max-speed” on page 70.

To configure service profiles for RPM implementations, perform the following steps, beginning from global configuration mode.

Step	Command	Purpose
1	Router(config)# resource-pool profile service <i>name</i>	Create a service profile and assign it a name of up to 23 characters.
2	Router(config-service-profil)# modem { min-speed { <i>speed</i> <i>any</i> } } { max-speed { <i>speed</i> <i>any</i> } } [modulation (<i>k56flex</i> <i>v22bis</i> <i>v32bis</i> <i>v32terbo</i> <i>v34</i> <i>v90</i> <i>any</i>)] [error-correction { <i>mnp4</i> <i>lapm</i> <i>any</i> <i>none</i> }] [compression { <i>mnp5</i> <i>v42bis</i> <i>any</i> <i>none</i> }]	Specify the desired modem parameter values. The range for min-speed and max-speed is from 300 to 56000 bps.

Example

The following example shows the creation of a service profile named *mical*. The minimum modem speed is set for 28800 bps; maximum speed is 56000 bps; the modulation is set to v32bis; error correction is not configured; compression is set to v42bis.

```
Router(config)# resource-pool profile service mical
Router(config-service-profil)# modem min-speed 28800 max-speed 56000 modulation v32bis
compression v42bis
```

Configuring Customer Profiles

Customer profiles are used so that service providers can assign different service characteristics to different customers. Note the following characteristics of customer profiles:

- Multiple resources of the same call type are used sequentially.
- The limits imposed are per customer (DNIS)—not per resource.
- A digital resource with a call type of **speech** allows for data over speech bearer service (DoSBS).

To configure customer profiles for RPM implementations, perform the following steps, beginning from global configuration mode.

Step	Command	Purpose
1	Router(config)# resource-pool profile customer <i>name</i>	Create a customer profile and assign it a name of up to 23 characters.
2	Router(config-customer-profi)# dnis group <i>dnis-group-name</i>	Assign a previously-created DNIS group to this customer profile (see “Configuring DNIS Groups” on page 20).
3	Router(config-customer-profi)# limit base-size { <i>number</i> <i>all</i> }	Specify the maximum number of simultaneous base sessions to be allowed for this customer under the terms of the service-level agreement (SLA). The range is from 0 to 1000 sessions. If all sessions are to be designated as base sessions, specify all .
4	Router(config-customer-profi)# limit overflow-size { <i>number</i> <i>all</i> }	Specify the maximum number of overflow sessions to be allowed for this customer under the terms of the service-level agreement (SLA). The range is from 0 to 1000. If all sessions are to be designated as overflow sessions, specify all .

Step	Command	Purpose
5	Router(config-customer-profi)# resource WORD {digital speech v110 v120} [service WORD]	Assign a name to a group of physical resources inside the customer profile. Select which type of calls this group of resources will accept. Specify the name of a service profile if you have configured a service profile for MICA modems.

Example

The following example shows a customer profile called *corporate1* being created and configured. It is using the DNIS group named *cisco* with no limits on the base size or on the overflow size (accepting all sessions). The customer profile is set to use the configured resource *modems1* for digital calls using the configured service named *mical*:

```
Router(config)# resource-pool profile customer corporate1
Router(config-customer-profi)# dnis group cisco
Router(config-customer-profi)# limit base-size all
Router(config-customer-profi)# limit overflow-size all
Router(config-customer-profi)# resource modems1 digital service mical
```

Configuring Customer Profile Templates

Customer profile templates provide a way to keep each customer's unique PPP configuration values separate for both security and accountability. This is an optional configuration.

Note To configure a template and place it in a customer profile, ensure that all basic configurations including the resource pool management configurations have been completed and verified.

To configure a customer profile template for RPM implementations, perform the following steps, beginning from global configuration mode.

Step	Command	Purpose
1	Router(config)# template name	Create a customer profile template and assign a unique name that relates to the customer that will be receiving it. Note Steps 2, 3, and 4 are optional. Enter multilink, peer, and ppp commands appropriate to the customer's application requirements.
2	Router(config-template)# peer default ip address pool pool-name	Optional command. Specify that the customer profile to which this template is attached will use a local IP address pool with the specified name.
3	Router(config-template)# ppp authentication chap	Optional command. Set the PPP link authentication method.
4	Router(config-template)# ppp multilink	Optional command. Enable multilink PPP for this customer profile.
5	Router(config-template)# exit	Exit from template configuration mode; return to global configuration mode.
6	Router(config)# resource-pool profile customer name	Enter customer profile configuration mode for the customer to which you wish to assign this template.
7	Router(config-customer-profi)# source template name	Attach the customer profile template you have just configured to the customer profile.

When you create a customer profile template and enter template configuration mode, the following commands are available:

```
Router(config)# template acme_direct
Template Configuration Commands:
  default      Set a command to its defaults
  exit         Exit from resource-manager configuration mode
  multilink    Configure multilink parameters
  no           Negate a command or set its defaults
  peer        Peer parameters for point to point interfaces
  ppp         Point-to-Point Protocol
```

For more information about the PPP command set, refer to Release 12.0, *Cisco IOS Dial Solutions Command Reference* and *Dial Solutions Configuration Guide*.

Example

The following example shows the creation and configuration of a customer profile template named *acme-direct* and its subsequent assignment to the customer profile *acme1*:

```
Router(config)# template acme-direct
Router(config-template)# multilink max-fragments 10
Router(config-template)# peer match aaa-pools
Router(config-template)# peer default ip address pool acme-numbers
Router(config-template)# ppp ipcp dns 10.1.1.1 10.2.2.2
Router(config-template)# ppp multilink
Router(config-template)# exit
Router(config)# resource-pool profile customer acme1
Router(config-customer-profi)# source template acme-direct
```

Configuring AAA Server Groups

AAA server groups are lists of AAA server hosts of a particular type. The Cisco RPM currently supports Remote Authentication Dial In User Service (RADIUS) server hosts and Terminal Access Controller Access Control System Plus (TACACS+) server hosts. A AAA server group lists the IP addresses of the selected server hosts.

You can use a AAA server group to define a distinct list of AAA server hosts and apply this list to the Cisco RPM application. Note that the AAA server group feature works only when the server hosts in a group are of the same type.

To configure AAA server groups for RPM implementations, perform the following steps, beginning from global configuration mode.

Step	Command	Purpose
1	Router(config)# aaa new-model	Enable AAA on the NAS.
2	Router(config)# radius-server key key or Router(config)# tacacs-server key key	Set the authentication and encryption key used for all RADIUS or TACACS+ communications between the NAS and the RADIUS or TACACS+ daemon.
3	Router(config)# radius-server host {hostname ip-address key} [auth-port port acct-port port] or Router(config)# tacacs-server host ip-address key	Specify the hostname or IP address of the server host before configuring the AAA server group. You can also specify the UDP destination ports for authentication and for accounting.
4	Router(config)# aaa group server {radius tacacs+} group-name	Select the AAA server type you want to place into a server group and assign a server group name.

Configuration Tasks

Step	Command	Purpose
5	Router(config-sg radius)# server <i>ip-address</i>	Specify the IP address of the selected server type. This must be the same IP address that was assigned to the server host in Step 2.
6	Router(config-sg radius)# exit	Return to global configuration mode.
7	Router(config)# resource-pool profile <i>customer name</i>	Enter customer profile configuration mode for the customer to which you wish to assign this AAA server group.
8	Router(config-customer-profi)# aaa group-configuration <i>group-name</i>	Associate this AAA server group (named in Step 4) with the customer profile named in Step 7.

For more information about the AAA command set, refer to *AAA Server Group*, a Cisco IOS Release 12.0(5)T feature, and Release 12.0, *Cisco IOS Dial Solutions Command Reference* and *Dial Solutions Configuration Guide*.

Example

The following example shows a RADIUS AAA server group configured with a hostname of *serverhostname* for the customer profile named *acmeprofile* in the AAA group configuration of *acme1*:

```
Router(config)# aaa new-model
Router(config)# radius-server key key
Router(config)# radius-server host serverhostname
Router(config)# aaa group server radius acme1
Router(config-sg radius)# server ip-address
Router(config-sg radius)# exit
Router(config)# resource-pool profile customer acmeprofile1
Router(config-customer-profi)# aaa group-configuration acme1
```

Configuring VPDN Profiles

VPDN profiles are used to combine session counting for VPDN groups with session counting for DNIS groups. A VPDN profile is required only if you want to impose VPDN tunnel limits that are different from the base session and overflow session limits that are configured for the customer profile containing the VPDN sessions.

To configure VPDN profiles for RPM implementations, perform the following steps, beginning from global configuration mode.

Step	Command	Purpose
1	Router(config)# resource-pool profile <i>vpdn profile-name</i>	Create a VPDN profile and assign it a profile name.
2	Router(config-vpdn-profile)# limit base-size <i>{number all}</i>	Specify the maximum number of simultaneous base VPDN sessions to be allowed for this VPDN group under the terms of the service-level agreement (SLA). The range is from 0 to 1000 sessions. If all sessions are to be designated as base VPDN sessions, specify all .
3	Router(config-vpdn-profile)# limit overflow-size <i>{number all}</i>	Specify the maximum number of simultaneous overflow VPDN sessions to be allowed for this VPDN group under the terms of the service-level agreement (SLA). The range is from 0 to 1000 sessions. If all sessions are to be designated as overflow VPDN sessions, specify all .
4	Router(config-vpdn-profile)# exit	Return to global configuration mode.
5	Router(config)# resource-pool profile <i>customer name</i>	Enter customer profile configuration mode for the customer to which you wish to assign this VPDN group.

Step	Command	Purpose
6	<pre>Router(config-customer-profi)# vpdn profile profile-name or Router(config-customer-profi)# vpdn group group-name</pre>	Attach the VPDN profile you have just configured to the customer profile to which it belongs, or, if the limits imposed by the VPDN profile are not required, attach VPDN group instead (see “Configuring VPDN Groups” on page 27).

Example

The following example shows the commands used to configure the VPDN profile *cust1profile* for the customer named *cust1*. The base-size limit has been set to 25, the overflow size limit has been set to 20. After the VPDN profile *cust1profile* has been configured, it is then assigned to the customer *cust1*:

```
Router(config)# resource-pool profile vpdn cust1profile
Router(config-vpdn-profile)# limit base-size 25
Router(config-vpdn-profile)# limit overflow-size 20
Router(config-vpdn-profile)# exit
Router(config)# resource-pool profile customer cust1
Router(config-customer-profi)# vpdn profile cust1profile
```

Configuring VPDN Groups

A VPDN group consists of VPDN sessions that are combined together and placed into a customer profile or a VPDN profile. Note the following characteristics of VPDN groups:

- The *dnis-group-name* is required to authorize the VPDN group with RPM.
- A VPDN group placed in a customer profile allows VPDN connections for the customer using that profile.
- A VPDN group placed in a VPDN profile allows the session limits configured for that profile to apply to all of the VPDN sessions within that VPDN group.
- VPDN data includes an associated domain name or DNIS, an endpoint IP address, the maximum number of MLP bundles, and the maximum number of links per MLP bundle; this data can optionally be on a AAA server.

To configure VPDN groups for RPM implementations, perform the following steps, beginning from global configuration mode.

Step	Command	Purpose
1	<pre>Router(config)# vpdn enable</pre>	Enable VPDN sessions on the NAS.
2	<pre>Router(config)# vpdn-group group-name</pre>	Create a VPDN group and assign it a unique name. Each VPDN group can have multiple endpoints (HGW/LNSs).
3	<pre>Router(config-vpdn)# request dialin {l2f l2tp} {ip ip-address} {domain domain-name dnis dnis-number}</pre>	Specify the tunneling protocol to be used to reach the remote peer defined by a specific IP address if a dial-in request is received for the specified domain name or DNIS number. The IP address that qualifies the session is automatically generated and does not need to be entered again.
4	<pre>Router(config-vpdn)# multilink {bundle number link number}</pre>	Specify the maximum number of bundles and links for all multilink users in the VPDN group. The range for both bundles and links is from 0 to 32767. In general, each user requires one bundle.

Configuration Examples

Step	Command	Purpose
5	Router(config-vpdn)# loadsharing ip <i>ip-address</i> [limit number]	Configure the endpoints for loadsharing. This router will loadshare IP traffic with the first router specified in Step 2. The limit keyword limits the number of simultaneous sessions that are sent to the remote endpoint (HGW/LNS). This limit can be between 0 and 32767 sessions.
6	Router(config-vpdn)# backup ip <i>ip-address</i> [limit number] [priority number]	Set up a backup HGW/LNS router. The number of sessions per backup can be limited. The priority number can be between 2 and 32767. The highest priority is 2, which is the first HGW/LNS router to receive backup traffic. The lowest priority, which is the default, is 32767.
7	Router(config-vpdn)# exit	Return to global configuration mode.
8	Router(config)# resource-pool profile vpdn <i>profile-name</i> or Router(config)# resource-pool profile customer name	Enter either VPDN profile configuration mode or customer profile configuration mode, depending on whether you want to allow VPDN connections for a customer profile, or allow combined session counting on all of the VPDN sessions within a VPDN profile.
9	Router(config-vpdn-profile)# vpdn group <i>group-name</i> or Router(config-customer-profi)# vpdn group <i>group-name</i>	Attach the VPDN group to either the VPDN profile or the customer profile specified in Step 7.

Example

The following example shows the configuration of a VPDN group named *vpdn4commerce* and how it was associated with the customer profile *johndoe1*:

```
Router(config)# vpdn enable
Router(config)# vpdn-group vpdn4commerce
Router(config-vpdn)# request dialin l2f ip 10.10.1.1 domain 5552221212
Router(config-vpdn)# multilink bundle number 10
Router(config-vpdn)# loadsharing ip 10.10.1.1 25
Router(config-vpdn)# backup ip 10.10.1.2 20
Router(config-vpdn)# exit
Router(config)# resource-pool profile customer johndoe1
Router(config-customer-profi)# vpdn group vpdn4commerce
```

Configuration Examples

This section provides the following configuration examples:

- Sample Configuration for Resource Pool Management
- Sample Direct Remote Services Configuration
- Sample Customer Profile Configuration for Data Over Voice Bearer Service
- Sample VPDN Configuration
- Sample VPDN Load Sharing and Backup Configuration

Sample Configuration for Resource Pool Management

The following example configuration illustrates the general use of RPM:

```
resource-pool enable
```

```
resource-pool call treatment resource busy
resource-pool call treatment profile no-answer
!
resource-pool group resource isdn-ports
  range limit 46
resource-pool group resource MICA-modems
  range port 1/0 2/23
!
resource-pool profile customer ACME
  limit base-size 30
  limit overflow-size 10
  resource isdn-ports digital
  resource MICA-modems speech service gold
  dnis group ACME_dnis_numbers
```

Note Replace **resource isdn-ports digital** above with **resource isdn-ports speech** to set up DoVBS. See the section, “Sample Direct Remote Services Configuration” for more information.

```
!
resource-pool profile customer DEFAULT
  limit base-size 10
  resource MICA-modems speech service silver
  dnis group default
```

```
resource-pool profile discriminator deny_DNIS
  call-type digital
  dnis group bye-bye
!
resource-pool profile service gold
  modem min-speed 33200 max-speed 56000 modulation v90
resource-pool profile service silver
  modem min-speed 19200 max-speed 33200 modulation v34
!
resource-pool aaa protocol local
!
dialer dnis group ACME_dnis_numbers
  number 301001
dialer dnis group bye-bye
  number 301005
```

Note the following characteristics of the sample configuration:

- Digital calls to 301001 are associated with the customer ACME by using the resource group “isdn-ports”.
- Speech calls to 301001 are associated with the customer ACME by using the resource group “MICA-modems.” In the ACME customer profile, this resource group uses service profile “gold,” which allows V.90 connections (anything less than a V.90 connection is also allowed).
- Digital calls to 301005 are denied.
- All other speech calls to any other DNIS number are associated with the customer profile “DEFAULT” by using the resource group “MICA-modems.” In the DEFAULT customer profile, this resource group uses service profile “silver,” which allows V.34 connections (anything more than V.34 is not allowed; anything less than V.34 is allowed).
- All other digital calls to any other DNIS number are not associated with a customer profile and are therefore not allowed.
- In this case, the customer profile named “DEFAULT” serves as the default customer profile for speech calls only. If the solution uses an external RPMS server, this same configuration can be used for backup resource pooling if communication is lost between the NAS and the RPMS.

Sample Direct Remote Services Configuration

The following example configuration illustrates the use of direct remote services with RPM:

```
resource-pool profile customer ACME
  limit base-size 30
  limit overflow-size 10
  resource isdn-ports digital
  resource MICA-modems speech service gold
  dnis group ACME_dnis_numbers
  aaa group-configuration tahoe
  source template acme_direct
!
resource-pool profile customer DEFAULT
  limit base-size 10
  resource MICA-modems speech service silver
  dnis group default
resource-pool profile discriminator deny_DNIS
  call-type digital
  dnis group bye-bye
!
```

```

resource-pool profile service gold
  modem min-speed 33200 max-speed 56000 modulation v90
resource-pool profile service silver
  modem min-speed 19200 max-speed 33200 modulation v34
!
resource-pool aaa protocol local
!
template acme_direct
  peer default ip address pool tahoe
  ppp authentication chap isdn-users
  ppp multilink
!
dialer dnis group ACME_dnis_numbers
  number 301001
dialer dnis group bye-bye
  number 301005

```

Sample Customer Profile Configuration for Data Over Voice Bearer Service

To allow ISDN calls with a speech bearer capability to be directed to digital resources, make the following change (highlighted in bold) to the configuration shown in the section “Sample Configuration for Resource Pool Management”:

```

resource-pool profile customer ACME
  limit base-size 30
  limit overflow-size 10
  resource isdn-ports speech
  dnis group ACME_dnis_numbers

```

This change causes ISDN speech calls (in addition to ISDN digital calls) to be directed to the resource “isdn-ports”; thus, ISDN speech calls provide Data Over Voice Bearer Service.

Sample VPDN Configuration

Adding the following commands to the “Sample Configuration for Resource Pool Management” section allows you to use VPDN by setting up a VPDN profile and a VPDN group.

Note If the limits imposed by the VPDN profile are not required, do not configure the VPDN profile. Replace the command **vpdn profile ACME_VPDN** under the customer profile ACME with the command **vpdn group outgoing-2**.

```

resource-pool profile vpdn ACME_VPDN
  limit base-size 6
  limit overflow-size 0
  vpdn group outgoing-2
!
resource-pool profile customer ACME
  limit base-size 30
  limit overflow-size 10
  resource isdn-ports digital
  resource MICA-modems speech service gold
  dnis group ACME_dnis_numbers
  vpdn profile ACME_VPDN

```

```

vpdn enable
!
vpdn-group outgoing-2
 request dialin 12f ip 172.16.1.9 dnis ACME_dnis_numbers
 local name HQ-NAS
 multilink bundle 1
 multilink link 2
 dnis ACME_dnis_numbers
!
dialer dnis group ACME_dnis_numbers
 number 301001

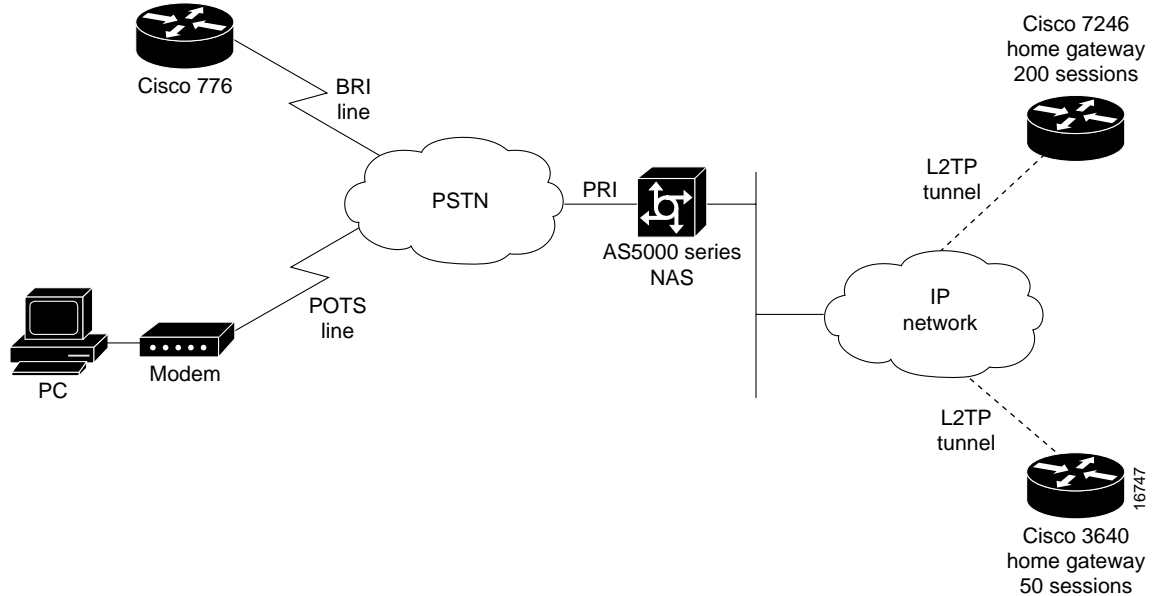
```

Sample VPDN Load Sharing and Backup Configuration

The Cisco IOS software enables you to balance and back up VPDN sessions across multiple tunnel endpoints (HGW/LNS). When a user or session comes into the NAS/LAC, a VPDN load-balancing algorithm is triggered and applied to the call, which is then passed to an available HGW/LNS. You can modify this function by limiting the number of sessions supported on an HGW/LNS router and limiting the number of MLP bundles and links.

Figure 9 shows an example of one NAS/LAC directing calls to two HGW/LNS routers by using the L2TP tunneling protocol. Each router has a different number of supported sessions and works at a different speed. The NAS/LAC is counting the number of active simultaneous sessions sent to each HGW/LNS.

Figure 9 Home Gateway Load Sharing and Backup



In a standalone NAS environment (no RPMS server is used), the NAS has complete knowledge of the status of tunnel endpoints. Load balancing across endpoints is done by a “least-filled tunnel” or a “next-available round robin” approach. In an RPMS-controlled environment, RPMS has the complete knowledge of tunnel endpoints. However, the NAS still controls those tunnel endpoints selected by RPMS.

When load-balancing traffic across multiple endpoints (HGW/LNS), a standalone NAS uses the following search criteria:

- 1 Selects any idle endpoint—an HGW/LNS with no active sessions.
- 2 Selects an active endpoint that currently has a tunnel established with the NAS.
- 3 If all specified load-sharing routers are busy, the NAS selects the backup HGW.
If all endpoints are busy, the NAS reports that it cannot find an IP address to establish the call.

Note This default search order criteria is independent of the Cisco Resource Pool Manager Server application scenario. A standalone NAS uses a different load-sharing algorithm than the Cisco Resource Pool Manager Server. This search criteria will change as future enhancements become available.

The following example configuration shows the use of VPDN load-sharing and backup with RPM:

```
vpdn enable
!
vpdn-group outgoing-2
 request dialin l2tp ip 172.16.1.9 dnis ACME_dnis_numbers
 local name HQ-NAS
 loadsharing ip 172.16.1.9 limit 200
 loadsharing ip 172.16.2.17 limit 50
 backup ip 172.16.3.22
```

Verifying Call-Counter and Call-Detail Output

The following commands provide call-counter and call-detail output for the different RPM components. An example for each command follows.

- **show resource-pool call**
- **show resource-pool customer**
- **show resource-pool discriminator**
- **show resource-pool resource**
- **show dialer dnis {group | number} WORD**
- **show resource-pool vpdn {group | profile} WORD**
- **clear resource-pool {customer | discriminator | resource} {WORD | all}**

show resource-pool call

The following output of the **show resource-pool call** command shows the details for all current calls, including the customer profile and resource group, and the matched DNIS group:

```
Router# show resource-pool call
Shelf 0, slot 0, port 0, channel 15, state RM_RPM_RES_ALLOCATED
 Customer profile ACME, resource group isdn-ports
 DNIS number 301001
Shelf 0, slot 0, port 0, channel 14, state RM_RPM_RES_ALLOCATED
 Customer profile ACME, resource group isdn-ports
 DNIS number 301001
Shelf 0, slot 0, port 0, channel 11, state RM_RPM_RES_ALLOCATED
 Customer profile ACME, resource group MICA-modems
 DNIS number 301001
```

show resource-pool customer

If you enter the **show resource-pool customer** command without including a customer profile name, a list of the current customer profile names appears. If you enter a customer profile name with the **show resource-pool customer** command, as in the example below, the call counters for the selected customer profile appear. These counters include historical data and can be cleared:

```
Router# show resource-pool customer ACME
 3 active connections
41 calls accepted
 3 max number of simultaneous connections
11 calls rejected due to profile limits
 2 calls rejected due to resource unavailable
 0 minutes spent with max connections
 5 overflow connections
 1 overflow states entered
11 overflow connections rejected
10 minutes spent in overflow
214 minutes since last clear command
```

show resource-pool discriminator

If you enter the **show resource-pool discriminator** command without including a call discriminator name, a list of the current call discriminator profiles appears. If you enter a call discriminator profile name with the **show resource-pool discriminator** command, the number of calls rejected by the selected call discriminator appears:

```
Router# show resource-pool discriminator
List of Call Discriminator Profiles:
 deny_DNIS
Router# show resource-pool discriminator deny_DNIS
 1 calls rejected
```

show resource-pool resource

If you enter the **show resource-pool resource** command without including a resource name, a list of the current resource names appears. If you enter a resource name is entered with the **show resource-pool resource** command, the call counters for the selected resource appear. These counters include historical data and can be cleared:

```
Router# show resource-pool resource
List of Resources:
 isdn-ports
 MICA-modems

Router# show resource-pool resource isdn-ports
46 resources in the resource group
 2 resources currently active
 8 calls accepted in the resource group
 2 calls rejected due to resource unavailable
 0 calls rejected due to resource allocation errors
```

show dialer dnis

The following sample output of the **show dialer dnis** command shows the call counters for a given DNIS group. These counters include historical data and can be cleared:

```
Router# show dialer dnis group ACME_dnis_numbers
DNIS Number:301001
  11 total connections
  5 peak connections
  0 calltype mismatches
```

show resource-pool vpdn

The following sample output of the **show resource-pool vpdn profile** command shows the call counters for a given VPDN profile. These counters include historical data and can be cleared:

```
Router# show resource-pool vpdn profile ACME_VPDN
  2 active connections
  2 max number of simultaneous connections
  0 calls rejected due to profile limits
  0 calls rejected due to resource unavailable
  0 overflow connections
  0 overflow states entered
  0 overflow connections rejected
  215 minutes since last clear command
```

The following sample output of the **show resource-pool vpdn group** command shows tunnel information for a given VPDN group:

```
Router# show resource-pool vpdn group outgoing-2
VPDN Group outgoing-2 found under VPDN Profiles:  ACME_VPDN

Tunnel (L2F)
-----
dnis:301001
dnis:ACME_dnis_numbers

Endpoint      Session Limit Priority Active Sessions Status Reserved Sessions
-----
172.16.1.9   *           1         2             OK          -
-----
Total        *           2         2             0
```

clear resource-pool

This command clears the call counters in the access server. Depending on what keywords you use, you can clear all resource pool counter statistics, or you can limit the clearing to specific parameters within different customer profiles, discriminators, or physical resources:

```
Router# clear resource-pool customer customer1

Router# clear resource-pool discriminator customer3

Router# clear resource-pool resource all
```

Troubleshooting Resource Pool Management

Test and verify that ISDN, CAS, SS7, PPP, AAA, and VPDN are working properly before implementing RPM. Once RPM is implemented, the only commands needed for troubleshooting RPM are:

- **debug resource-pool**
- **debug aaa authorization**

Use the **debug resource-pool** command as the first step to ensure proper operation. It is usually sufficient in most cases. Use the **debug aaa authorization** command for troubleshooting VPDN and modem service problems.

When using the direct remote services implementation, first make sure the RPM is working. Then check the dial-in caller and users.

The following problems may occur:

- No DNIS group found, or no customer profile uses a default DNIS
- Call discriminator blocks the DNIS
- Customer profile limits have been exceeded
- Resource group limits have been exceeded

Note Always enable the debug and log timestamps when troubleshooting RPM.

Checking the Resource Pool Connection

The following sample output of **debug resource-pool** shows a successful RPM connection. The entries in bold are of particular importance:

```
*Mar 1 02:14:57.439: RM state:RM_IDLE event:DIALER_INCALL DS0:0:0:0:21
*Mar 1 02:14:57.439: RM: event incoming call
*Mar 1 02:14:57.443: RM state:RM_DNIS_AUTHOR event:RM_DNIS_RPM_REQUEST DS0:0:0:0:21
*Mar 1 02:14:57.447: RM:RPM event incoming call
*Mar 1 02:14:57.459: RPM profile ACME found
*Mar 1 02:14:57.487: RM state:RM_RPM_RES_AUTHOR event:RM_RPM_RES_AUTHOR_SUCCESS
DS0:0:0:0:21
*Mar 1 02:14:57.487: Allocated resource from res_group isdn-ports
*Mar 1 02:14:57.491: RM:RPM profile "ACME", allocated resource "isdn-ports"
successfully
*Mar 1 02:14:57.495: RM state:RM_RPM_RES_ALLOCATING event:RM_RPM_RES_ALLOC_SUCCESS
DS0:0:0:0:21
*Mar 1 02:14:57.603: %LINK-3-UPDOWN: Interface Serial0:21, changed state to up
*Mar 1 02:15:00.879: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0:21,
changed state to up
```

Troubleshooting DNIS Group Problems

The following output of the **debug resource-pool** command shows a customer profile that is not found for a particular DNIS group:

```
*Mar 1 00:38:21.011: RM state:RM_IDLE event:DIALER_INCALL DS0:0:0:0:3
*Mar 1 00:38:21.011: RM: event incoming call
*Mar 1 00:38:21.015: RM state:RM_DNIS_AUTHOR event:RM_DNIS_RPM_REQUEST DS0:0:0:0:3
*Mar 1 00:38:21.019: RM:RPM event incoming call
*Mar 1 00:38:21.103: RPM no profile found for call-type digital in default DNIS number
*Mar 1 00:38:21.155: RM:RPM profile rejected do not allocate resource
*Mar 1 00:38:21.155: RM state:RM_RPM_RES_AUTHOR event:RM_RPM_RES_AUTHOR_FAIL
DS0:0:0:0:3
*Mar 1 00:38:21.163: RM state:RM_RPM_DISCONNECTING event:RM_RPM_DISC_ACK DS0:0:0:0:3
```

Troubleshooting Call Discriminator Problems

The following output of the **debug resource-pool** command shows an incoming call that is matched against a call discriminator profile:

```
*Mar 1 00:35:25.995: RM state:RM_IDLE event:DIALER_INCALL DS0:0:0:0:4
*Mar 1 00:35:25.999: RM: event incoming call
*Mar 1 00:35:25.999: RM state:RM_DNIS_AUTHOR event:RM_DNIS_RPM_REQUEST DS0:0:0:0:4
*Mar 1 00:35:26.003: RM:RPM event incoming call
*Mar 1 00:35:26.135: RM:RPM profile rejected do not allocate resource
*Mar 1 00:35:26.139: RM state:RM_RPM_RES_AUTHOR event:RM_RPM_RES_AUTHOR_FAIL
DS0:0:0:0:4
*Mar 1 00:35:26.143: RM state:RM_RPM_DISCONNECTING event:RM_RPM_DISC_ACK DS0:0:0:0:4
```

Troubleshooting Customer Profile Counts

The following output of the **debug resource-pool** command shows what happens once a customer profile's limits have been reached:

```
*Mar 1 00:43:33.275: RM state:RM_IDLE event:DIALER_INCALL DS0:0:0:0:9
*Mar 1 00:43:33.279: RM: event incoming call
*Mar 1 00:43:33.279: RM state:RM_DNIS_AUTHOR event:RM_DNIS_RPM_REQUEST DS0:0:0:0:9
*Mar 1 00:43:33.283: RM:RPM event incoming call
*Mar 1 00:43:33.295: RPM count exceeded in profile ACME
*Mar 1 00:43:33.315: RM:RPM profile rejected do not allocate resource
*Mar 1 00:43:33.315: RM state:RM_RPM_RES_AUTHOR event:RM_RPM_RES_AUTHOR_FAIL
DS0:0:0:0:9
*Mar 1 00:43:33.323: RM state:RM_RPM_DISCONNECTING event:RM_RPM_DISC_ACK DS0:0:0:0:9
```

Troubleshooting Resource Group Counts

The following output of the **debug resource-pool** command shows the resources all in use within a resource group:

```
*Mar 1 00:52:34.411: RM state:RM_IDLE event:DIALER_INCALL DS0:0:0:0:19
*Mar 1 00:52:34.411: RM: event incoming call
*Mar 1 00:52:34.415: RM state:RM_DNIS_AUTHOR event:RM_DNIS_RPM_REQUEST DS0:0:0:0:19
*Mar 1 00:52:34.419: RM:RPM event incoming call
*Mar 1 00:52:34.431: RPM profile ACME found
*Mar 1 00:52:34.455: RM state:RM_RPM_RES_AUTHOR event:RM_RPM_RES_AUTHOR_SUCCESS
DS0:0:0:0:19
*Mar 1 00:52:34.459: All resources in res_group isdn-ports are in use
*Mar 1 00:52:34.463: RM state:RM_RPM_RES_ALLOCATING event:RM_RPM_RES_ALLOC_FAIL
DS0:0:0:0:19
*Mar 1 00:52:34.467: RM:RPM failed to allocate resources for "ACME"
```

Checking the RPM/VPDN Connection

The following sample output of **debug resource-pool** shows a successful RPM/VPDN connection. The entries in bold are of particular importance:

```
*Mar 1 00:15:53.639: Se0:10 RM/VPDN/rm-session-request: Allocated vpdn info for domain
NULL MLP Bundle SOHO
*Mar 1 00:15:53.655: RM/VPDN/ACME_VPDN: VP LIMIT/ACTIVE/RESERVED/OVERFLOW are now
6/0/0/0
*Mar 1 00:15:53.659: RM/VPDN/ACME_VPDN: Session reserved for outgoing-2
*Mar 1 00:15:53.695: Se0:10 RM/VPDN: Session has been authorized using
dnis:ACME_dnis_numbers
*Mar 1 00:15:53.695: Se0:10 RM/VPDN/session-reply: NAS name HQ-NAS
*Mar 1 00:15:53.699: Se0:10 RM/VPDN/session-reply: Endpoint addresses 172.16.1.9
*Mar 1 00:15:53.703: Se0:10 RM/VPDN/session-reply: VPDN tunnel protocol l2f
*Mar 1 00:15:53.703: Se0:10 RM/VPDN/session-reply: VPDN Group outgoing-2
*Mar 1 00:15:53.707: Se0:10 RM/VPDN/session-reply: VPDN domain dnis:ACME_dnis_numbers
*Mar 1 00:15:53.767: RM/VPDN: MLP Bundle SOHO Session Connect with 1 Endpoints:
*Mar 1 00:15:53.771: IP 172.16.1.9 OK
*Mar 1 00:15:53.771: RM/VPDN/rm-session-connect/ACME_VPDN: VP
LIMIT/ACTIVE/RESERVED/OVERFLOW are now 6/1/0/0
*Mar 1 00:15:54.815: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0:10,
changed state to up
*Mar 1 00:15:57.399: %ISDN-6-CONNECT: Interface Serial0:10 is now connected to SOHO
```

Following are some VPDN problems that typically might occur:

- Customer profile is not associated with a VPDN profile or VPDN group (the call will be locally terminated in this case. Regular VPDN can still succeed even if RPM/VPDN fails).
- VPDN profile limits have been reached (call answered but disconnected).
- VPDN group limits have been reached (call answered but disconnected).
- VPDN end point is not reachable (call answered but disconnected).

Troubleshooting Customer/VPDN Profile

The following sample output of **debug resource-pool** indicates that there is no VPDN group associated with an incoming DNIS group. However, the output of **debug resource-pool**, as shown here, does not effectively reflect the problem:

```
*Mar 1 03:40:16.483: Se0:15 RM/VPDN/rm-session-request: Allocated vpdn info for domain
NULL MLP Bundle SOHO
*Mar 1 03:40:16.515: Se0:15 RM/VPDN/rm-session-request: Authorization failed
*Mar 1 03:40:16.527: %VPDN-6-AUTHORERR: L2F NAS HQ-NAS cannot locate a AAA server for
Se0:15 user SOHO
*Mar 1 03:40:16.579: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
*Mar 1 03:40:17.539: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0:15,
changed state to up
*Mar 1 03:40:17.615: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up
*Mar 1 03:40:19.483: %ISDN-6-CONNECT: Interface Serial0:15 is now connected to SOHO
```

Note Whenever the **debug resource-pool** command offers no further assistance besides the indication that authorization has failed, enter the **debug aaa authorization** command to further troubleshoot the problem.

The following sample shows output for the **debug aaa authorization** command:

```
*Mar 1 04:03:49.846: Se0:19 RM/VPDN/rm-session-request: Allocated vpdn info for domain
NULL MLP Bundle SOHO
*Mar 1 04:03:49.854: Se0:19 AAA/AUTHOR/RM vpdn-session (3912941997):
Port='DS0:0:0:0:19' list='default' service=RM
*Mar 1 04:03:49.858: AAA/AUTHOR/RM vpdn-session: Se0:19 (3912941997) user='301001'
*Mar 1 04:03:49.862: Se0:19 AAA/AUTHOR/RM vpdn-session (3912941997): send AV
service=resource-management
*Mar 1 04:03:49.866: Se0:19 AAA/AUTHOR/RM vpdn-session (3912941997): send AV
protocol=vpdn-session
*Mar 1 04:03:49.866: Se0:19 AAA/AUTHOR/RM vpdn-session (3912941997): send AV
rm-protocol-version=1.0
*Mar 1 04:03:49.870: Se0:19 AAA/AUTHOR/RM vpdn-session (3912941997): send AV
rm-nas-state=3278356
*Mar 1 04:03:49.874: Se0:19 AAA/AUTHOR/RM vpdn-session (3912941997): send AV
rm-call-handle=27
*Mar 1 04:03:49.878: Se0:19 AAA/AUTHOR/RM vpdn-session (3912941997): send AV
multilink-id=SOHO
*Mar 1 04:03:49.878: Se0:19 AAA/AUTHOR/RM vpdn-session (3912941997): found list
"default"
*Mar 1 04:03:49.882: Se0:19 AAA/AUTHOR/RM vpdn-session (3912941997): Method=LOCAL
*Mar 1 04:03:49.886: Se0:19 AAA/AUTHOR/RM/local (3912941997): Received AV
service=resource-management
*Mar 1 04:03:49.890: Se0:19 AAA/AUTHOR/RM/local (3912941997): Received AV
protocol=vpdn-session
*Mar 1 04:03:49.890: Se0:19 AAA/AUTHOR/RM/local (3912941997): Received AV
rm-protocol-version=1.0
*Mar 1 04:03:49.894: Se0:19 AAA/AUTHOR/RM/local (3912941997): Received AV
rm-nas-state=3278356
*Mar 1 04:03:49.898: Se0:19 AAA/AUTHOR/RM/local (3912941997): Received AV
rm-call-handle=27
*Mar 1 04:03:49.902: Se0:19 AAA/AUTHOR/RM/local (3912941997): Received AV
multilink-id=SOHO
*Mar 1 04:03:49.906: Se0:19 AAA/AUTHOR/VPDN/RM/LOCAL: Customer ACME has no VPDN group
for session dnis:ACME_dnis_numbers
*Mar 1 04:03:49.922: Se0:19 AAA/AUTHOR (3912941997): Post authorization status = FAIL
```

Troubleshooting VPDN Profile Limits

The following output of the **debug resource-pool** command shows that VPDN profile limits have been reached:

```
*Mar 1 04:57:53.762: Se0:13 RM/VPDN/rm-session-request: Allocated vpdn info for domain
NULL MLP Bundle SOHO
*Mar 1 04:57:53.774: RM/VPDN/ACME_VPDN: VP LIMIT/ACTIVE/RESERVED/OVERFLOW are now
0/0/0/0
*Mar 1 04:57:53.778: RM/VPDN/ACME_VPDN: Session outgoing-2 rejected due to Session
Limit
*Mar 1 04:57:53.798: Se0:13 RM/VPDN/rm-session-request: Authorization failed
*Mar 1 04:57:53.802: %VPDN-6-AUTHORFAIL: L2F NAS HQ-NAS, AAA authorization failure for
Se0:13 user SOHO; At Session Max
*Mar 1 04:57:53.866: %ISDN-6-DISCONNECT: Interface Serial0:13 disconnected from
SOHO, call lasted 2 seconds
*Mar 1 04:57:54.014: %LINK-3-UPDOWN: Interface Serial0:13, changed state to down
*Mar 1 04:57:54.050: RM state:RM_RPM_RES_ALLOCATED event:DIALER_DISCON DS0:0:0:13
*Mar 1 04:57:54.054: RM:RPM event call drop
*Mar 1 04:57:54.054: Deallocated resource from res_group isdn-ports
```

Troubleshooting VPDN Group Limits

The following output of the **debug resource-pool** command shows that VPDN group limits have been reached. From this output, it is not readily obvious what the problem is. Enable the **debug aaa authorization** command to troubleshoot further (see “Using the debug aaa authorization Command” on page 40 for more information):

```
*Mar 1 05:02:22.314: Se0:17 RM/VPDN/rm-session-request: Allocated vpdn info for domain
NULL MLP Bundle SOHO
*Mar 1 05:02:22.334: RM/VPDN/ACME_VPDN: VP LIMIT/ACTIVE/RESERVED/OVERFLOW are now
5/0/0/0
*Mar 1 05:02:22.334: RM/VPDN/ACME_VPDN: Session reserved for outgoing-2
*Mar 1 05:02:22.358: Se0:17 RM/VPDN/rm-session-request: Authorization failed
*Mar 1 05:02:22.362: %VPDN-6-AUTHORFAIL: L2F NAS HQ-NAS, AAA authorization failure for
Se0:17 user SOHO; At Multilink Bundle Limit
*Mar 1 05:02:22.374: %ISDN-6-DISCONNECT: Interface Serial0:17 disconnected from
SOHO, call lasted 2 seconds
*Mar 1 05:02:22.534: %LINK-3-UPDOWN: Interface Serial0:17, changed state to down
*Mar 1 05:02:22.570: RM state:RM_RPM_RES_ALLOCATED event:DIALER_DISCON DS0:0:0:0:17
*Mar 1 05:02:22.574: RM:RPM event call drop
*Mar 1 05:02:22.574: Deallocated resource from res_group isdn-ports
```

Troubleshooting VPDN Endpoint Problems

The following output of the **debug resource-pool** command shows that the IP endpoint for the VPDN group is not reachable:

```
*Mar 1 05:12:22.330: Se0:21 RM/VPDN/rm-session-request: Allocated vpdn info for domain
NULL MLP Bundle SOHO
*Mar 1 05:12:22.346: RM/VPDN/ACME_VPDN: VP LIMIT/ACTIVE/RESERVED/OVERFLOW are now
5/0/0/0
*Mar 1 05:12:22.350: RM/VPDN/ACME_VPDN: Session reserved for outgoing-2
*Mar 1 05:12:22.382: Se0:21 RM/VPDN: Session has been authorized using
dnis:ACME_dnis_numbers
*Mar 1 05:12:22.386: Se0:21 RM/VPDN/session-reply: NAS name HQ-NAS
*Mar 1 05:12:22.386: Se0:21 RM/VPDN/session-reply: Endpoint addresses 172.16.1.99
*Mar 1 05:12:22.390: Se0:21 RM/VPDN/session-reply: VPDN tunnel protocol l2f
*Mar 1 05:12:22.390: Se0:21 RM/VPDN/session-reply: VPDN Group outgoing-2
*Mar 1 05:12:22.394: Se0:21 RM/VPDN/session-reply: VPDN domain dnis:ACME_dnis_numbers
*Mar 1 05:12:25.762: %ISDN-6-CONNECT: Interface Serial0:21 is now connected to SOHO
*Mar 1 05:12:27.562: %VPDN-5-UNREACH: L2F HGW 172.16.1.99 is unreachable
*Mar 1 05:12:27.578: RM/VPDN: MLP Bundle SOHO Session Connect with 1 Endpoints:
*Mar 1 05:12:27.582: IP 172.16.1.99 Destination unreachable
```

Using the debug aaa authorization Command

In general, the **debug aaa authorization** command is not required for RPM troubleshooting—unless **debug resource-pool** is too vague.

Typically, **debug aaa authorization** is more useful for troubleshooting with RPMS:

```
Router# debug aaa authorization
AAA Authorization debugging is on
Router# show debug
General OS:
  AAA Authorization debugging is on
Resource Pool:
  resource-pool general debugging is on
```

The following output of the **debug resource-pool** and **debug aaa authorization** commands shows a successful RPM connection:

```

*Mar 1 06:10:35.450: AAA/MEMORY: create_user (0x723D24) user='301001'
ruser='port='DS0:0:0:0:12' rem_addr='102' authn_type=NONE service=NONE priv=0
*Mar 1 06:10:35.462: DS0:0:0:0:12 AAA/AUTHOR/RM call-accept (2784758907):
Port='DS0:0:0:0:12' list='default' service=RM
*Mar 1 06:10:35.466: AAA/AUTHOR/RM call-accept: DS0:0:0:0:12 (2784758907) user=
'301001'
*Mar 1 06:10:35.470: DS0:0:0:0:12 AAA/AUTHOR/RM call-accept (2784758907): send AV
service=resource-management
*Mar 1 06:10:35.470: DS0:0:0:0:12 AAA/AUTHOR/RM call-accept (2784758907): send AV
protocol=call-accept
*Mar 1 06:10:35.474: DS0:0:0:0:12 AAA/AUTHOR/RM call-accept (2784758907): send AV
rm-protocol-version=1.0
*Mar 1 06:10:35.478: DS0:0:0:0:12 AAA/AUTHOR/RM call-accept (2784758907): send AV
rm-nas-state=7513368
*Mar 1 06:10:35.482: DS0:0:0:0:12 AAA/AUTHOR/RM call-accept (2784758907): send AV
rm-call-type=speech
*Mar 1 06:10:35.486: DS0:0:0:0:12 AAA/AUTHOR/RM call-accept (2784758907): send AV
rm-request-type=dial-in
*Mar 1 06:10:35.486: DS0:0:0:0:12 AAA/AUTHOR/RM call-accept (2784758907): send AV
rm-link-type=isdn
*Mar 1 06:10:35.490: DS0:0:0:0:12 AAA/AUTHOR/RM call-accept (2784758907): found list
"default"
*Mar 1 06:10:35.494: DS0:0:0:0:12 AAA/AUTHOR/RM call-accept (2784758907): Method=LOCAL
*Mar 1 06:10:35.498: DS0:0:0:0:12 AAA/AUTHOR/RM/local (2784758907): Received
DNIS=301001
*Mar 1 06:10:35.498: DS0:0:0:0:12 AAA/AUTHOR/RM/local (2784758907): Received CLID=102
*Mar 1 06:10:35.502: DS0:0:0:0:12 AAA/AUTHOR/RM/local (2784758907): Received
Port=DS0:0:0:0:12
*Mar 1 06:10:35.506: DS0:0:0:0:12 AAA/AUTHOR/RM/local (2784758907): Received AV
service=resource-management
*Mar 1 06:10:35.510: DS0:0:0:0:12 AAA/AUTHOR/RM/local (2784758907): Received AV
protocol=call-accept
*Mar 1 06:10:35.510: DS0:0:0:0:12 AAA/AUTHOR/RM/local (2784758907): Received AV
rm-protocol-version=1.0
*Mar 1 06:10:35.514: DS0:0:0:0:12 AAA/AUTHOR/RM/local (2784758907): Received AV
rm-nas-state=7513368
*Mar 1 06:10:35.518: DS0:0:0:0:12 AAA/AUTHOR/RM/local (2784758907): Received AV
rm-call-type=speech
*Mar 1 06:10:35.522: DS0:0:0:0:12 AAA/AUTHOR/RM/local (2784758907): Received AV
rm-request-type=dial-in
*Mar 1 06:10:35.526: DS0:0:0:0:12 AAA/AUTHOR/RM/local (2784758907): Received AV
rm-link-type=isdn
*Mar 1 06:10:35.542: AAA/AUTHOR (2784758907): Post authorization status = PASS_REPL
*Mar 1 06:10:35.546: DS0:0:0:0:12 AAA/AUTHOR/RM/call-accept (2784758907): Processing
AV service=resource-management
*Mar 1 06:10:35.550: DS0:0:0:0:12 AAA/AUTHOR/RM/call-accept (2784758907): Processing
AV protocol=call-accept
*Mar 1 06:10:35.554: DS0:0:0:0:12 AAA/AUTHOR/RM/call-accept (2784758907): Processing
AV rm-protocol-version=1.0
*Mar 1 06:10:35.558: DS0:0:0:0:12 AAA/AUTHOR/RM/call-accept (2784758907): Processing
AV rm-response-code=overflow
*Mar 1 06:10:35.558: DS0:0:0:0:12 AAA/AUTHOR/RM/call-accept (2784758907): Processing
AV rm-call-handle=47
*Mar 1 06:10:35.562: DS0:0:0:0:12 AAA/AUTHOR/RM/call-accept (2784758907): Processing
AV rm-call-count=2
*Mar 1 06:10:35.566: DS0:0:0:0:12 AAA/AUTHOR/RM/call-accept (2784758907): Processing
AV rm-cp-name=ACME
*Mar 1 06:10:35.570: DS0:0:0:0:12 AAA/AUTHOR/RM/call-accept (2784758907): Processing
AV rm-rg-name#0=MICA-modems
*Mar 1 06:10:35.574: DS0:0:0:0:12 AAA/AUTHOR/RM/call-accept (2784758907): Processing
AV rm-rg-service-name#0=gold
*Mar 1 06:10:35.578: DS0:0:0:0:12 AAA/AUTHOR/RM/call-accept (2784758907): Processing
AV rm-call-treatment=busy
*Mar 1 06:10:35.582: DS0:0:0:0:12 AAA/AUTHOR/RM/call-accept (2784758907): Processing
AV rm-call-type=speech

```

Command Reference

This section documents the new or modified commands for the resource pool management feature. All other commands are documented in the *Cisco IOS Release 12.0 Command Reference*.

- **aaa group-configuration** on page 44
- **backup** on page 46
- **call progress tone** on page 48
- **call-type** on page 50
- **call-type cas** on page 52
- **clear dialer dnis** on page 53
- **clear resource-pool** on page 55
- **dialer dnis group** on page 57
- **dnis** on page 59
- **dnis group** on page 61
- **domain** on page 63
- **limit base-size** on page 65
- **limit overflow-size** on page 67
- **loadsharing** on page 68
- **modem min-speed max-speed** on page 70
- **multilink** on page 72
- **number** on page 74
- **ppp ipcp** on page 75
- **range** on page 77
- **request dialin** on page 79
- **resource** on page 82
- **resource-pool** on page 84
- **resource-pool aaa accounting ppp** on page 85
- **resource-pool aaa protocol** on page 87
- **resource-pool call treatment** on page 88
- **resource-pool group resource** on page 89
- **resource-pool profile customer** on page 91
- **resource-pool profile discriminator** on page 93
- **resource-pool profile service** on page 94
- **resource-pool profile vpdn** on page 95
- **show call progress tone** on page 96
- **show dialer dnis** on page 99
- **show resource-pool call** on page 102

- **show resource-pool customer** on page 104
- **show resource-pool discriminator** on page 106
- **show resource-pool resource** on page 108
- **show resource-pool vpdn** on page 110
- **show vpdn domain** on page 113
- **show vpdn group** on page 114
- **show vpdn multilink** on page 117
- **source template** on page 119
- **template** on page 120
- **vpdn group** on page 121
- **vpdn profile** on page 123
- **debug resource-pool** on page 125

aaa group-configuration

To associate a AAA server group with an interface or customer profile, enter the **aaa group-configuration** interface or customer profile sub-command. To disable the configuration, enter the **no** form of this command.

```
aaa group-configuration aaa-group-name  
no aaa group-configuration aaa-group-name
```

Syntax Description

aaa-group-name Character string used to name the group of AAA servers.

Defaults

No default behavior or values.

Command Modes

Interface
Customer profile subcommand

Command History

Release	Modification
12.0(6)T	This command was introduced.

Usage Guidelines

The AAA server group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

A server group is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts and TACACS+ server hosts. A server group is used with a global server host list. The server group lists the IP addresses of the selected server hosts.

Example

The following example shows a AAA server group by the name of **radius-3** being associated with a customer profile by the name of **acme**.

```
Router(config)# resource-pool profile customer acme  
Router(config-customer-profi)# aaa group-configuration radius-3
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security when RADIUS or TACACS+ is used.
aaa authentication login	Sets AAA authentication at login.
aaa authorization	Sets parameters that restrict network access to a user.
aaa new model	Enables the AAA access control model.
radius-server-host	Specifies and defines the IP address of the RADIUS server host before configuring a AAA server group.
tacacs-server-host	Specifies and defines the IP address of the TACACS+ server host before configuring a AAA server group.

backup

To configure an IP backup endpoint address, enter the **backup** VPDN group configuration command. To remove this function, enter the **no** form of this command.

backup ip *ip-address* [**limit number** [**priority number**]]

no backup ip *ip-address* [**limit number** [**priority number**]]

Syntax Description

ip <i>ip-address</i>	IP address of the HGW/LNS at the other end of the tunnel. This is the IP endpoint at the end of the tunnel, which is an HGW/LNS router.
limit number	(Optional) Limits sessions per backup. The limit can range from 0 to 32767. The default is no limit set.
priority number	(Optional) Priority level. Loadsharing is priority 1. Backup priority is between 2 and 32,767. The highest priority is 2, which is the first home gateway router to receive backup traffic. The lowest priority is 32,767. The priority group is used to support multiple levels of loadsharing and backup. The default is the lowest priority.

Defaults

No default behavior or values. This function is used only if it is configured.

Command Modes

VPDN group configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced in Cisco IOS Release 12.0(4)XI1 and applies to Cisco AS5200s and Cisco AS5300s only.

Usage Guidelines

Use the **backup** VPDN group configuration command to configure an IP backup endpoint address.

Examples

The following example shows that the **backup** command is not available in the command line interface until you enter the **request dialin** command:

```
Router(config)# vpdn-group customer1-vpdngroup
Router(config-vpdn)# ?
VPDN group configuration commands:
  accept  Accept a tunnel open request
  default Set a command to its defaults
  exit    Exit from VPDN group configuration mode
  no      Negate a command or set its defaults
  request Request to open a tunnel

Router(config-vpdn)# request dialin l2tp ip 10.2.2.2 domain customerx
Router(config-vpdn)# ?
VPDN group configuration commands:
  backup      Add backup address
  default     Set a command to its defaults
  dnis        Accept a DNIS tunnel
  domain      Accept a domain tunnel
  exit        Exit from VPDN group configuration mode
  force-local-chap Force a CHAP challenge to be instigated locally
  l2tp        L2TP specific commands
  lcp         LCP specific commands
  loadsharing Add loadsharing address
  local       local information, like name
  multilink   Configure limits for Multilink
  no          Negate a command or set its defaults
  request     Request to open a tunnel
```

The following example shows an IP backup endpoint address of 10.1.1.1 configured with a backup session limit of 5:

```
Router(config-vpdn)# backup ip 10.1.1.1 limit 5
```

Related Commands

Command	Description
request dialin	Specifies a dial-in L2F or L2TP tunnel to a remote peer if a dial-in request is received for a specified domain or Dialed Number Information Service (DNIS).

call progress tone

To specify the country code for retrieving the call progress tone parameters from the call progress tone database, enter the **call progress tone** configuration mode command. To cancel the previous setting and to generate the call progress tones according to modem settings, enter the **no** version of this command.

call progress tone country *country-name*

no call progress tone country *country-name*

Syntax Description

country	Selects default call progress tones (ring and cadence settings) for the specified country.
<i>country-name</i>	Valid entries are: argentina, australia, austria, belgium, brazil, canada, china, colombia, cyprus, czech-republic, denmark, finland, france, germany, greece, hongkong, hungary, iceland, india, indonesia, ireland, israel, italy, japan, korea, luxembourg, malaysia, mexico, netherlands, peru, philippines, poland, portugal, russia, singapore, slovakia, slovenia, south-africa, spain, sweden, switzerland, taiwan, thailand, turkey, unitedkingdom, usa, and venezuela.

Defaults

Modem default settings. (Generally *northamerica* for Cisco IOS Release versions earlier than release 12.0(3)XG; *us* for 12.0(3)XG and later releases.)

Command Modes

Configuration mode

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **call progress tone** configuration command to specify the country for call progress tone generation. While in many cases the country is chosen automatically based on the modem setting, automatic selection won't work for all users because many modems do not support all countries and many users choose the "us" or "default-t1" or "default-e1" setting on their modem.

This command affects the tones generated at the local interface and does not affect any information passed to the remote end of a connection or any tones generated at the remote end of a connection.

For dial platforms (AS5200, AS5300, and AS5800), call progress tones are used only for the resource pool management application. Resource pool management assumes that the call progress tone selection is global. Select only one call progress tone set for the whole box, and it will globally override country settings on all ports.

Examples

The following example shows the call progress tone set for Japan tone parameters:

```
Router(config)# call progress tone country japan
Router(config)# exit
```

Related Commands

Command	Description
show call progress	Displays the contents of the internal call progress tone database.

call-type

To reject particular types of calls, enter the **call-type** call discriminator command. Enter the **no** form of this command to disable this feature.

```
call-type {all | digital | speech | v110 | v120}
no call-type {all | digital | speech | v110 | v120}
```

Syntax Description

all	Rejects all calls.
digital	Rejects digital calls.
speech	Rejects speech calls.
v110	Rejects V.110 calls.
v120	Rejects V.120 calls.

Defaults

All calls are accepted by the network access server.

Command Modes

Call discriminator profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **call-type** call discriminator command to reject particular types of calls. Call type “all” is mutually exclusive for all other call types. If call type “all” is set in the discriminator, no other call types are allowed. Also, once a DNIS is associated with a call type in a discriminator, it cannot be used in any other discriminator.

Examples

The following example shows the call discriminator being configured to reject speech calls for the call discriminator profile named *userd3*:

```
Router(config)# resource-pool profile discriminator userd3
Router(config-call-discrim)# call-type speech
Router(config-call-discrim)#
```

Related Commands

None

call-type cas

To statically set the call-type override for incoming channel-associated signalling (CAS) calls, enter the **call-type cas** DNIS group configuration command. Enter the **no** form of this command to disable this service.

```
call-type cas { digital | speech }
no call-type cas { digital | speech }
```

Syntax Description

digital	Override call type to digital. The incoming call with the DNIS in the called group is treated as a digital call type.
speech	Override call-type to speech. The incoming call with the DNIS in the called group is treated as a speech call type.

Default

None.

Command Mode

DNIS group configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **call-type cas** DNIS group configuration command to set the call-type override. From the resource pooling call-type perspective, use CT1 (CAS) to support either analog calls (speech) or digital calls (switched 56K).

Switched 56K calls are digital calls that connect to HDLC framers. Unlike ISDN, it is impossible to communicate the call type in CT1. Therefore, switched 56K services in CT1 can be differentiated by the DNIS numbers. This command identifies that the call arriving with the DNIS in the DNIS group is assigned to the call type specified in the command.

Examples

The following example shows the DNIS group configuration mode being accessed to use the **call-type cas** command to set the call type override for CAS to *speech*:

```
Router(config)# dialer dnis group modem-group1
Router(config-called-group)# call-type cas speech
```

Related Commands

None

clear dialer dnis

To reset the counter statistics associated with a specific DNIS group or number, enter the **clear dialer dnis** EXEC command. There is no **no** form of this command.

```
clear dialer dnis {group name | number number}
```

Syntax Description

group <i>name</i>	Clears dialer DNIS group statistics.
number <i>number</i>	Clears dialer DNIS number statistics.

Defaults

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **clear dialer dnis** EXEC command to reset the counter statistics associated with a specific DNIS group or number. This command clears the counters for a DNIS group to reset the counter statistics associated with a specific DNIS group or number. If an ISP is charging a customer for the number of calls to a DNIS, it can clear the number after a week or month by using this command.

Examples

The following example shows the result of using the **clear dialer dnis** command for the DNIS group named *dgl*. Note that the counters have been cleared after the **clear dialer dnis** command has been entered:

```
Router# show dialer dnis group dgl
DNIS Number:71028
  4 total connections
  3 peak connections
  1 calltype mismatches
DNIS Number:4156266541
  8 total connections
  5 peak connections
  0 calltype mismatches
DNIS Number:4085541628
  3 total connections
  2 peak connections
  0 calltype mismatches
DNIS Number:71017
  2 total connections
  1 peak connections
  0 calltype mismatches
```

```
Router# clear dialer dnis group dgl
```

```
Router# show dialer dnis group dgl
DNIS Number:71028
  0 total connections
  0 peak connections
  0 calltype mismatches
DNIS Number:4156266541
  0 total connections
  0 peak connections
  0 calltype mismatches
DNIS Number:4085541628
  0 total connections
  0 peak connections
  0 calltype mismatches
DNIS Number:71017
  0 total connections
  0 peak connections
  0 calltype mismatches
```

Related Commands

Command	Description
show dialer dnis	Displays how many calls a specific DNIS group has had.

clear resource-pool

To reset the counter statistics associated with a specific customer profile, call discriminator, or physical resource, enter the **clear resource-pool** privileged EXEC command. There is no **no** version of this command.

```
clear resource-pool { customer | discriminator / resource } { name | all }
```

Syntax Description

customer	Clears a customer profile.
discriminator	Clears a call discriminator.
resource	Clears a physical resource. Checks the counters maintained for resource groups.
<i>name</i>	Clears a specific customer profile, discriminator, or physical resource in the access server.
all	Clears all customer profiles, discriminators, or physical resources in the access server.

Defaults

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Enter the **clear resource-pool** privileged EXEC command to reset the counter statistics associated with a specific customer profile, call discriminator, or physical resource.

Examples

The following example shows the use of the **clear resource-pool** command for the specific customer named *customer-isp*:

```
Router# clear resource-pool customer ?
      WORD  Customer profile name
      all   Clear all customer profiles

Router# clear resource-pool customer customer_isp
Router#
```

clear resource-pool

Related Commands

Command	Description
show resource-pool customer	Displays the contents of one or more customer profiles.
show resource-pool resource	Displays the resource groups set up in the access server.
show resource-pool call	Displays all active call information for all customer profiles and resource groups.

dialer dnis group

To create a DNIS group, enter the **dialer dnis group** global configuration command. Enter the **no** form of this command to remove a specific DNIS group from the running configuration.

dialer dnis group *name*

no dialer dnis group *name*

Syntax Description

name Assigns a name to the DNIS group number.

Defaults

A dialer DNIS group named *default*.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **dialer dnis group** global configuration command to create a DNIS group. This command enables you to create and populate a DNIS group, which is then added to a profile (customer or discriminator) by using the **dnis group** command within that profile's configuration mode.

Examples

The following example shows a specific DNIS group named *modem-group1* being created with the options available for further configuration:

```
Router(config)# dialer dnis group modem-group1
Router(config-dnis-group)# ?
Dialer Called Configuration Commands:
  call-type  set call-type override
  default    Set a command to its defaults
  exit       Exit from dialer configuration mode
  help       Description of the interactive help system
  no        Negate a command or set its defaults
  number     Enter number in dnis group
```

In the following example, a customer profile called `isp_1` is created, a DNIS group called `dnis_isp_1` is associated with the customer profile, and DNIS numbers 1234 and 5678 are assigned to the DNIS group. Only DNIS numbers 1234 and 5678 are allocated physical resources by the `isp_1` customer profile, which counts and manages the resources for these two DNIS numbers and ignores all other DNIS numbers:

```
Router(config)# resource-pool profile customer isp_1
Router(config-customer-pro)# dnis group dnis_isp_1
Router(config-customer-pro)# exit
Router(config)# dialer dnis group dnis_isp_1
Router(config-called-group)# number 1234
Router(config-called-group)# number 5678
```

Related Commands

Command	Description
resource-pool profile	Creates a customer profile.
dnis group	Includes a group of DNIS numbers in a customer profile.

dnis

To support additional DNIS for a specific VPDN tunnel, enter the **dnis** VPDN group configuration command. To remove a DNIS from a VPDN group, enter the **no** form of this command.

Note When resource pool management is enabled, this command uses the keyword designator *dnis-group-name*. When resource pool management is disabled, this command uses the keyword designator *dnis-number*.

dnis *dnis-group-name*

no dnis *dnis-group-name*

Syntax Description

<i>dnis-group-name</i>	DNIS group name—If resource pool management is enabled and the VPDN group is configured under the incoming customer profile, <i>dnis-group-name</i> is used.
<i>dnis-number</i>	DNIS group number—If resource pool management is disabled, the <i>dnis-number</i> is used. Or, if a call is associated with a customer profile without any VPDN group configured for the customer profile, <i>dnis-number</i> is used.

Default

Disabled.

Command Mode

VPDN group configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **dnis** VPDN group configuration command to support additional DNIS for a specific VPDN tunnel. The **dnis** command is available in the command line interface after you enter the **request dialin** command for the first time. DNIS allows a VPDN tunnel to be authorized by using the DNIS number or DNIS group name.

Note Configure the **vpdn group** command with the **request dialin** command to enable VPDN. The requestor initiates a dial-in tunnel. The acceptor accepts a request for a dial-in tunnel.

Examples

The following example shows multiple DNISs tunneling to one HGW/LNS router at 10.1.1.1. Note that the **dnis** command does not appear in the command line interface until you enter the **request dialin** command:

```
Router(config)# vpdn-group california_users
Router(config-vpdn)# ?
VPDN group configuration commands:
  accept  Accept a tunnel open request
  default Set a command to its defaults
  exit    Exit from VPDN group configuration mode
  no      Negate a command or set its defaults
  request Request to open a tunnel

Router(config-vpdn)# request dialin l2tp ip 10.1.1.1 dnis 1234
Router(config-vpdn)# ?
VPDN group configuration commands:
  backup      Add backup address
  default     Set a command to its defaults
  dnis       Accept a DNIS tunnel
  domain     Accept a domain tunnel
  exit       Exit from VPDN group configuration mode
  force-local-chap Force a CHAP challenge to be instigated locally
  l2tp       L2TP specific commands
  lcp        LCP specific commands
  loadsharing Add loadsharing address
  local      local information, like name
  multilink  Configure limits for Multilink
  no         Negate a command or set its defaults
  request    Request to open a tunnel
Router(config-vpdn)# dnis 5678
Router(config-vpdn)# dnis 9101
Router(config-vpdn)# dnis 1121
Router(config-vpdn)# ^Z
```

Related Commands

Command	Description
request dialin	Specifies a dial-in L2F or L2TP tunnel to a remote peer if a dial-in request is received for a specified domain or Dialed Number Information Service (DNIS).

dnis group

To include a group of DNIS numbers in a customer profile, enter the **dnis group** customer profile configuration command. Enter the **no** form of this command to remove a DNIS group from a customer profile.

dnis group { **default** | **name** *name* }

no dnis group { **default** | **name** *name* }

Syntax Description

default	Allows a specified customer profile to accept all DNIS numbers coming into the access server. For example, a stray DNIS number not listed in any customer profile passes through this default DNIS group. Most customer profiles do not have this option configured.
name	Assigns a name to a DNIS group.
<i>name</i>	The name can have up to 23 characters.

Defaults

No DNIS groups are associated with a customer profile.

Command Modes

Customer profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **dnis group** customer profile configuration command to include a group of DNIS numbers in a customer profile or discriminator:

Examples

The following example includes the DNIS group called “customer1dnis” in the “customer1” customer profile:

```
router(config)# resource-pool profile customer customer1
router(config-customer-profile)# dnis group customer1dnis
```

dnis group

Related Commands

Command	Description
dialer dnis group	Creates a DNIS group.
resource-pool profile	Creates a customer profile.

domain

To support additional domain names for a specific VPDN group, enter the **domain** VPDN group configuration command. To remove a domain name from a VPDN group, enter the **no** form of this command.

domain *name*

no domain *name*

Syntax Description

name Domain name.

Defaults

This function will be used if it is configured. Otherwise, it is disabled.

Command Modes

VPDN group configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **domain** VPDN group configuration command to support additional domain names for a specific VPDN group. The **domain** command becomes available in the command line interface after you enter the **request dialin** command for the first time. The **domain** command allows a VPDN tunnel to be authorized by using the domain name.

Note Configure the **vpdn group** command with the **request dialin** command to enable VPDN. The requestor initiates a dial-in tunnel.

Examples

The following example shows multiple domains tunneling to one HGW/LNS router at 10.1.1.1. Note that the **domain** command does not appear in the command line interface until you enter the **request dialin** command:

```
Router(config)# vpdn-group california_users
Router(config-vpdn)# ?
VPDN group configuration commands:
  accept  Accept a tunnel open request
  default Set a command to its defaults
  exit    Exit from VPDN group configuration mode
  no      Negate a command or set its defaults
  request Request to open a tunnel

Router(config-vpdn)# request dialin l2tp ip 10.1.1.1 domain la.com
Router(config-vpdn)# ?
VPDN group configuration commands:
  backup      Add backup address
  default     Set a command to its defaults
  dnis        Accept a DNIS tunnel
  domain      Accept a domain tunnel
  exit        Exit from VPDN group configuration mode
  force-local-chap Force a CHAP challenge to be instigated locally
  l2tp        L2TP specific commands
  lcp         LCP specific commands
  loadsharing Add loadsharing address
  local       local information, like name
  multilink   Configure limits for Multilink
  no          Negate a command or set its defaults
  request     Request to open a tunnel
Router(config-vpdn)# domain sandiego.com
Router(config-vpdn)# domain sanjose.com
Router(config-vpdn)# domain sf.com
```

Related Commands

Command	Description
request dialin	Specifies a dial-in L2F or L2TP tunnel to a remote peer if a dial-in request is received for a specified domain or Dialed Number Information Service (DNIS).

limit base-size

To define the base number of simultaneous connections that can be done in a single customer or VPDN profile, enter the **limit base-size** customer profile configuration command. Enter the **no** form of this command to remove the limitation.

limit base-size {*number* | **all**}

no limit base-size {*number* | **all**}

Syntax Description

<i>number</i>	Sets the maximum number of simultaneous connections or sessions that can be used in a specified customer or VPDN profile.
all	Accepts all calls. Use this command if you don't want to limit or apply overflow session counting to a customer or VPDN profile.

Defaults

No limits are set for a customer profile. The base size is set to **all**.

Command Modes

Customer profile configuration/VPDN profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **limit base-size** customer or VPDN profile configuration command to define the base number of simultaneous connections in a single customer or VPDN profile. The session limit applies to all the physical resource groups and pools configured in a single customer profile. If you want to define the number of overflow calls granted to a customer profile by using the command **limit overflow-size**, do *not* set the command **limit base-size** to "all." Instead, specify a number for **limit base-size**.

Examples

The following example shows the limits of the total number of simultaneous connections to a base size of 48:

```
router(config)# resource-pool profile customer customer1_isp
router(config-customer-profile)# limit base-size 48
```

limit base-size

Related Commands

Command	Description
resource-pool profile	Creates a customer profile.
limit overflow-size	Defines the number of overflow sessions allowed by a single customer profile.

limit overflow-size

To define the number of overflow calls granted to one customer or VPDN profile, enter the **limit overflow-size** customer profile configuration command. Enter the **no** form of this command to remove the overflow configuration.

limit overflow-size {*number* | **all**}

no limit overflow-size {*number* | **all**}

Syntax Description

<i>number</i>	Specifies the number of overflow calls.
all	Allows an unlimited number of overflow calls.

Defaults

The overflow size is set to 0.

Command Modes

Customer profile configuration/VPDN profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **limit overflow-size** customer or VPDN profile configuration command to define the number of overflow calls granted to one customer or VPDN profile. The overflow is not applied if the **limit base-size** command is set to “all”.

Examples

The following example shows 20 overflow calls granted to the customer profile called customer1_isp:

```
router(config)# resource-pool profile customer customer1_isp
router(config-customer-profile)# limit overflow-size 20
```

Related Commands

Command	Description
resource-pool profile	Creates a customer profile.
limit base-size	Defines the base number of simultaneous standard sessions allowed by a single customer profile.

loadsharing

To configure endpoints for loadsharing, enter the **loadsharing** VPDN group configuration command. To remove this function, enter the **no** form of this command.

loadsharing ip *ip-address* [**limit** *number*]

no loadsharing ip *ip-address* [**limit** *number*]

Syntax Description

ip <i>ip-address</i>	IP address of the HGW/LNS at the other end of the tunnel. This is the IP endpoint at the end of the tunnel, which is a HGW/LNS router.
limit <i>number</i>	(Optional) Limits sessions per loadshare. The limit has a range from 0 to 32,767 sessions. The default is no limit set.

Defaults

This function is not used when not configured.

Command Modes

VPDN group configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **loadsharing** VPDN group configuration command to configure endpoints for loadsharing.

Examples

In the following example, one VPDN group called customer1-vpdng is created. L2TP IP traffic is loadshared between two HGW/LNSs. The IP addresses for the HGW/LNS's WAN ports are 172.21.9.67 and 172.21.9.68. The characteristics for 172.21.9.67 are defined by using the **request dialin** command. The characteristics for 172.21.9.68 are defined by using the **loadsharing** command.

A backup home-gateway router is specified at 172.21.9.69 by using the **backup** command. This router serves as a backup device for two load-sharing HGW/LNS:

```
!  
vpdn-group customer1-vpdng  
  request dialin l2tp ip 172.21.9.67 domain cisco.com  
  loadsharing ip 172.21.9.68 limit 100  
  backup ip 172.21.9.69 priority 5  
  domain cisco2.com  
!
```

Related Commands

Command	Description
request dialin	Specifies a dial-in L2F or L2TP tunnel to a remote peer if a dial-in request is received for a specified domain or Dialed Number Information Service (DNIS).

modem min-speed max-speed

To configure various modem-service parameters, enter the **modem min-speed max-speed** service profile configuration command. Enter the **no** form of this command to remove modem parameters.

modem min-speed {*speed* | **any**} **max-speed** {*speed* | **any** [**modulation value**]}

no modem min-speed {*speed* | **any**} **max-speed** {*speed* | **any** [**modulation value**]}

Syntax Description

min-speed	Configures the minimum modem speed for all the modems used by this service profile.
<i>speed</i>	Specifies the minimum and maximum bps rate for the modems, which can be between 300 and 56,000 bps. Must be in V.90 increments.
any	Specifies any minimum or maximum speed.
max-speed	Configures the maximum modem speed for all the modems used by this service profile. Must be in V.90 increments.
modulation value	(Optional) Specifies the maximum negotiated speed. Replace the value argument with one of the following choices: any , k56flex , v22bis , v34 , or v90 .
error-correction	(Hidden command) lapm , mn14
compression	(Hidden command) mnps , v42bis

Defaults

No modem service parameters are defined by default. Any default services provided by the modems will be available.

Command Modes

Service profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **modem min-speed max-speed** service profile configuration command to configure various modem-service parameters:

Examples

The following example shows the modem service parameters for the service profile named *user1sample* configured for a minimum speed of *any*, a maximum speed of *any*, and a modulation of *k56flex*.

```
Router(config)# resource-pool profile service user1sample
Router(config-service-prof)# modem min-speed any max-speed any modulation k56flex
```

Related Commands

None

multilink

To limit sessions authorized for all multilink users, enter the **multilink** VPDN group configuration command. To remove this function, enter the **no** form of this command.

```
multilink {bundle number | link number}
no multilink {bundle number | link number}
```

Syntax Description

bundle number	Configures the number of bundles supported for a VPDN group. In general, each user requires one bundle. The limit has a range from 0 to 32,767.
link number	Configures the number of links or sessions supported for each bundle. The limit has a range from 0 to 32,767.

Defaults

No limit is set.

Command Modes

VPDN group configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **multilink** VPDN group configuration command to limit sessions authorized for all multilink users. Each user requires one bundle—regardless if the user is a remote modem client or an ISDN client.

One modem client using one B channel requires one link. One ISDN BRI node may require up to two links for one BRI line connection. The second B channel of an ISDN BRI node comes up when the maximum threshold is exceeded.

Examples

The following example shows a VPDN group called `joe_eastcoast`. An L2TP tunnel is set up to the home gateway router at IP address 10.2.2.2. You can authorize ten MLPPP bundles for ten users. Each user dials in to the domain called `bostonjoe.com`. Each bundle is authorized to support a maximum of 5 links. This means that all 10 users can consume a maximum of 50 simultaneous sessions dialing in to `bostonjoe.com`:

```
Router(config)# vpdn-group joe_eastcoast
Router(config-vpdn)# request dialin l2tp ip 10.2.2.2 domain bostonjoe.com
Router(config-vpdn)# multilink bundle 10
Router(config-vpdn)# multilink link 5
```

Related Commands

Command	Description
request dialin	Specifies a dial-in L2F or L2TP tunnel to a remote peer if a dial-in request is received for a specified domain or Dialed Number Information Service (DNIS).

number

To add a DNIS number to a dialer DNIS group, enter the **number** DNIS group configuration command followed by the specifying number. Enter the **no** form of this command to remove a DNIS number from a DNIS group.

number *number*

no number *number*

Syntax Description

number Specifies a DNIS number, which can have up to 65 digits.

Defaults

None.

Command Modes

DNIS group configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **number** DNIS group configuration command to enter a DNIS number to a dialer DNIS group. The Cisco IOS software also includes a feature that streamlines the DNIS configuration process. By replacing any digit with an X (for example, issuing the **number 555222121x** command), clients dialing different numbers, such as 5552221214 or 5552221215, are automatically mapped to the same customer profile. The X variable is a place holder for the digits 1 through 9.

Examples

The following example shows a DNIS group called `dnis_isp_1` and DNIS numbers 1234 and 5678 assigned to the DNIS group.

```
Router(config)# dialer dnis group dnis_isp_1
Router(config-called-group)# number 1234
Router(config-called-group)# number 5678
```

Related Commands

Command	Description
dnis group	Includes a group of DNIS numbers in a customer profile.

ppp ipcp

To configure the primary and secondary domain name server (DNS) addresses, or the primary and secondary WINS server addresses to be supplied to the peer during IPCP negotiation, enter the **ppp ipcp** template configuration command. To delete a **ppp ipcp** configuration, enter the **no** form of this command.

```
ppp ipcp {accept-address}|{dns [(primary dns ip address | secondary dns ip address)] }|
{ignore-map}|{(wins [primary wins ip address> | secondary wins ip address])}
```

```
no ppp ipcp {accept-address}|{dns [(primary dns ip address | secondary dns ip address)] }|
{ignore-map}|{(wins [primary wins ip address> | secondary wins ip address])}
```

Syntax Description

accept-address	Accept any non-zero IP address from the peer.
dns	Domain name server.
primary dns	Primary domain name server. Specify DNS address to provide.
<i>ip address</i>	IP address of the primary or secondary DNS or WINS server.
secondary dns	Secondary domain name server.
ignore-map	Ignore dialer map when negotiating peer IP address.
wins	Windows Internet naming service. Specify WINS address to provide.
primary wins	Primary Windows Internet naming service.
secondary wins	Secondary Windows Internet naming service.

Defaults

No servers are configured.

Command Modes

Template configuration

Command History

Release	Modification
12.0(6)T	This command was introduced.

Usage Guidelines

All PPP and peer-default commands are allowed under this grouping.

Examples

```
Router(config-template)# ppp ipcp accept-address  
  
Router(config-template)# ppp ipcp dns 10.1.1.1 10.1.1.2  
  
Router(config-template)# ppp ipcp ignore-map  
  
Router(config-template)# ppp ipcp wins 10.1.1.1 10.1.1.2  
  
Router(config-template)# no ppp ipcp wins 10.1.1.1 10.1.1.2
```

Related Commands

None

range

To associate a range of modems or other physical resources with a resource group, enter the **range** resource configuration command. To remove a range of modems or other physical resources, enter the **no** form of this command.

```
range {limit number | port range }
no range {limit number | port range }
```

Syntax Description

limit <i>number</i>	Specifies the maximum number of simultaneous connections supported by the resource group. Replace the <i>number</i> argument with the session limit you want to assign. Your access server's hardware configuration determines the maximum value of this limit. Applicable to ISDN B-channels or HDLC controllers.
port <i>range</i>	Specifies the range of resource ports to use in the resource group. For the Cisco AS5200 and AS5300, replace the <i>range</i> variable with <i>slot/port slot/port</i> .

Defaults

No range is configured.

Command Modes

Resource group configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **range** resource configuration command to associate a range of modems or other physical resources with a resource group.

Specify the range for port-based resources by using the resource's physical location. Do not identify non-port-based resource ranges by using a location. Rather, specify the size of the resource group with a single integer limit.

Specify non-contiguous ranges by using multiple **range port** commands within the same resource group. Do not configure the same ports in more than one resource group and do not overlap multiple port ranges.

For resources that are not pooled and have a 1-to-1 correspondence between DS0s, B channels, and HDLC framers, use the **range limit number** command. Circuit-switched data calls and V.120 calls use these kinds of resources.

Note Do not put heterogenous resources in the same group. Do not put MICA modems in the same group as Microcom modems. Do not put modems and HDLC controllers in the same resource group. Do not configure "port" and "limit" parameters in the same resource group.

Examples

The following example shows the range limit set for 48 simultaneous connections being supported by the resource group:

```
router# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
router(config)# resource-pool group resource hdlc1  
router(config-resource-group)# range limit 48
```

The following example shows the ports set for modem 1 ranging from port 0 to port 47:

```
router(config)# resource-pool group modem1  
router(config-resource-group)# range port 1/0 1/47
```

Related Commands

None

request dialin

To specify a dial-in L2F or L2TP tunnel to a remote peer if a dial-in request is received for a specified domain or Dialed Number Information Service (DNIS), enter the **request dialin** VPDN group configuration command. To remove this function, enter the **no** form of this command.

```
request dialin {l2f / l2tp} {ip ip-address} {domain domain-name / dnis dnis-number / dnis-group-name}
```

```
no request dialin {l2f / l2tp} {ip ip-address} {domain domain-name / dnis dnis-number / dnis-group-name}
```

Syntax Description

dnis <i>group-name</i>	Name of the DNIS group.
dnis <i>dnis-number</i>	Dialed number used for authorizing a specific tunnel that forwards traffic to the HGW/LNS.
domain <i>domain-name</i>	Case-sensitive name of the domain to tunnel.
ip <i>ip-address</i>	IP address (www.xxx.yyy.zzz) of the HGW/LNS at the other end of the tunnel.
l2f l2tp	Select L2F or L2TP tunnel protocol.

Defaults

None. **request dialin** must be explicitly configured.

Command Modes

VPDN group configuration

Command History

Release	Modification
11.3(5)AA	This command appeared in Cisco IOS Release 11.3(5)AA.
12.0(4)XI	The command request dialin modified for 12.0.

Usage Guidelines

Use the **request dialin** VPDN group configuration command to specify a dial-in L2F or L2TP tunnel to a remote peer if a dial-in request is received for a specified domain or Dialed Number Information Service (DNIS).

This command starts a tunnel to a remote peer defined by a specific IP address if a dial-in tunnel is received for users under a specific domain name, or if a specific DNIS is called. Configure the VPDN group command to use **request dialin**, which indicates a dial-in tunnel is requested.

Note Configure the **vpdn group** command with the **request dialin** command to enable VPDN. The requestor initiates a dial-in tunnel. The acceptor accepts a request for a dial-in tunnel.

To add additional domain names or DNIS to a VPDN group, enter the **domain** and **dnis** commands, which are available in the CLI after you enter the **request dialin** command for the first time.

Examples

The following example shows a request for an L2TP dial-in tunnel to a remote peer at IP address 172.17.33.125 for a user in domain partner.com:

```
request dialin l2tp ip 172.17.33.125 partner.com
```

The following example shows multiple domains tunneling to one LNS (for L2TP) router at 10.1.1.1. Note that the **domain** and **dnis** commands do not appear in the command line interface until you enter the **request dialin** command:

```
Router(config)# vpdn-group california_users
Router(config-vpdn)# ?
VPDN group configuration commands:
  accept  Accept a tunnel open request
  default Set a command to its defaults
  exit    Exit from VPDN group configuration mode
  no     Negate a command or set its defaults
  request Request to open a tunnel

Router(config-vpdn)# request dialin l2tp ip 10.1.1.1 domain la.com
Router(config-vpdn)# ?
VPDN group configuration commands:
  backup      Add backup address
  default     Set a command to its defaults
  dnis        Accept a DNIS tunnel
  domain      Accept a domain tunnel
  exit        Exit from VPDN group configuration mode
  force-local-chap Force a CHAP challenge to be instigated locally
  l2tp        L2TP specific commands
  lcp         LCP specific commands
  loadsharing Add loadsharing address
  local       local information, like name
  multilink   Configure limits for Multilink
  no         Negate a command or set its defaults
  request     Request to open a tunnel
Router(config-vpdn)# domain sandiego.com
Router(config-vpdn)# domain sanjose.com
Router(config-vpdn)# domain sf.com
Router(config-vpdn)# ^z
Router# show running
Building configuration...

Current configuration:
!
---- cut ----
!
vpdn-group california_users
  request dialin l2tp ip 10.1.1.1 domain la.com
  domain sandiego.com
  domain sanjose.com
  domain sf.com
!
---- cut ----
```

Related Commands

Command	Description
accept dialin	Sets up a tunnel on the HGW/LNS side.

resource

To assign resources and supported call-types to a customer profile, enter the **resource** customer profile configuration command. Enter the **no** form of this command to disable this function.

resource *name* { **digital** | **speech** | **v110** | **v120** } [*service name*]

no resource *name* { **digital** | **speech** | **v110** | **v120** } [*service name*]

Syntax Description

resource <i>name</i>	Assigns a name to a group of physical resources inside the access server. This name can have up to 23 characters.
digital	Accepts digital calls. Specifies circuit-switched data calls that terminate on a HDLC framers (unlike asynchronous analog modem call that use start and stop bits).
speech	Accepts speech calls. Specifies normal voice calls, such as calls started by analog modems and standard telephones.
v110	Accepts V.110 calls.
v120	Accepts V.120 calls. By specifying this keyword, the access server begins counting the number of v120 software encapsulations occurring in the system.
service <i>name</i>	(Optional) Configures a service profile. This option is not supported for digital or V.120 calls.

Defaults

No resources are assigned to the customer profile by default.

Command Modes

Customer profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource** customer profile configuration command to assign resources and supported call-types to a customer profile. This command specifies a group of physical resources to be used in answering an incoming call of a particular type for a particular customer profile. For example, calls started by analog modems are reciprocated with the **speech** keyword.

Examples

The following example shows a physical resource group called “modem1”. Forty-eight integrated modems are then assigned to modem1, which is linked to the customer profile called “customer1_isp”:

```
Router(config)# resource group resource modem1
Router(config-resource-gro)# range port 1/0 1/47
Router(config-resource-gro)# exit
Router(config)# resource-pool profile customer customer1_isp

Router(config-customer-pro)# resource modem1 ?
  digital  Accept digital calls
  speech   Accept speech calls
  v110     Accept V.110 calls
  v120     Accept V.120 calls
Router(config-customer-pro)# resource modem1 speech
```

Related Commands

Command	Description
resource-pool profile	Creates a customer profile.

resource-pool

To enable or disable resource pool management, enter the **resource-pool** global configuration command. There is no **no** form of this command.

resource-pool { enable | disable }

Syntax Description

enable	Enables resource pool management.
disable	Disables resource pool management.

Defaults

Resource management is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource-pool** global configuration command to enable and disable the resource pool management feature.

Examples

```
Router(config)# resource-pool enable  
Router(config)# resource-pool disable
```

Related Commands

None

resource-pool aaa accounting ppp

To include enhanced start/stop resource manager records to AAA accounting, enter the **resource-pool aaa accounting ppp** global configuration command. Enter the **no** form of this command to disable this feature.

resource-pool aaa accounting ppp

no resource-pool aaa accounting ppp

Syntax Description

This command has no additional keyword options.

Defaults

Disabled. The default of the **resource-pool enable** command is to *not* enable these new accounting records.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource-pool aaa accounting ppp** global configuration command to include enhanced start/stop resource manager records to AAA accounting. The **resource-pool aaa accounting ppp** command adds new resource pool management fields to the AAA accounting start/stop records. The new attributes in the start records are also in the stop records—in addition to those new attributes added exclusively for the stop records.

If you have configured your regular AAA accounting, this command directs additional information from the resource manager into your accounting records.

Note If you configure only this command and do not configure AAA accounting, nothing happens. The default functionality for the resource-pool enable command does not include this functionality.

The following new fields are added to the start and stop records:

New Start Record Fields	New Stop Record Fields
Call-type	ModemSpeed-receive
Customer-profile-name	ModemSpeed-transmit
Customer-profile-active-sessions	MLP-session-ID (multilink users)
MLP-session-ID (multilink users)	
Resource-group-name	
Overflow-flag	
VPDN-tunnel-ID (VPDN users)	
VPDN-homegateway (VPDN users)	
VPDN-domain-name (VPDN users)	
VPDN-group-active-session (VPDN users)	



Caution This list of newly supported start and stop fields is not exhaustive. Cisco reserves the right to enhance this list of records at any time. Use the **show accounting** command to see the contents of each active session.

Note Cisco recommends that you *thoroughly* understand how these new start/stop records affect your current accounting structure *before* you enter this command.

Examples

The following example shows the new AAA accounting start/stop records inserted into an existing AAA accounting infrastructure:

```
Router(config)# resource-pool aaa accounting ppp
```

Related Commands

Command	Description
show accounting	Steps through all active sessions and displays all accounting records for actively accounted functions.

resource-pool aaa protocol

To specify which protocol to use for resource management, enter the **resource-pool aaa protocol** global configuration command. Enter the **no** form of this command to disable this feature and go to local.

resource-pool aaa protocol { **local** | **group** *name* }

no resource-pool aaa protocol

Syntax Description

local	Specifies local authorization.
group <i>name</i>	Specifies an authorization method that is not local; for example, using an external AAA server group. The Resource Pool Management Server(s) (RPMS) is defined in a AAA server group.

Defaults

Defaults to local.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource-pool aaa protocol** global configuration command to specify which protocol to use for resource management. The AAA server group is most useful when you want to have multiple RPMSs configured as a fall-back mechanism.

Examples

```
Router(config)# resource-pool aaa protocol local
```

Related Commands

None

resource-pool call treatment

To set up the signal sent back to the telco switch in response to incoming calls, enter the **resource-pool call treatment** global configuration command. Enter the **no** form of this command to disable this function.

```
resource-pool call treatment {profile {busy | no-answer} | resource {busy | channel-not-available}}
```

```
no resource-pool call treatment {profile {busy | no-answer} | resource {busy | channel-not-available}}
```

Syntax Description

busy	Answers the call; then, sends a busy signal when profile authorization or resource allocation fails.
no-answer	Does not answer the call when profile authorization fails.
profile	Call treatment when profile authorization fails.
resource	Call treatment when resource allocation fails.
channel-not-available	Send "channel not available" code when resource allocation fails.

Defaults

No answer for a customer profile; CNA for a resource.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource-pool call treatment** global configuration command to set up the signal sent back to the telco switch in response to incoming calls.

Examples

```
res_pool(config)# resource-pool call treatment profile ?
  busy          Send busy code when profile authorization fails
  no-answer     Don't answer when profile authorization fails
```

Related Commands

None

resource-pool group resource

To create a resource group for resource management, enter the **resource-pool group resource** global configuration command. Enter the **no** form of this command to remove a resource group from the running configuration.

resource-pool group resource *name*

no resource-pool group resource *name*

Syntax Description

resource *name* Assigns a name to a group of physical resources inside the access server. This name can have up to 23 characters.

Defaults

No resource groups are set up.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource-pool group resource** global configuration command to create a resource group for resource management. When calls come into the access server, they are allocated physical resources as specified within resource groups and customer profiles.

See the **range** command for more information.

If some physical resources are not included in any resource groups, then these remaining resources are not used and are considered to be part of the default resource group. These resources can be used in certain cases to answer calls before profile allocation occurs, but the resources are not used other than in the connection phase.

Note For standalone NAS environments, configure resource groups before using them in customer profiles. For external RPMS environments, configure resource groups on the NAS before defining them on external RPMS servers.

When enabling RPM for SS7 signaling, like resources in the NAS must be in a single group:

- All modems must be in one group.
- All HDLC controllers must be in a different group.
- All V.110 ASICs must be put into another group.

- All V.120 resources must be in a separate group.

All resource group types must have the same number of resources and that number must equal the number of interface channels available from the public network switch. This grouping scheme prevents the signal “Channel Not Available” (CNA) from being sent to the signaling point. For SS7 signaling, Microcom and MICA modems must be in the *same* group. If SS7 signaling is not used, Cisco recommends assigning Microcom and MICA modems to separate groups to avoid introducing errors in RPM statistics.

Examples

The following example shows the configuration options within a resource group:

```
Router(config)# resource-pool group resource modem1
Router(config-resource-group)# ?
Resource Group Configuration Commands:
  default  Set a command to its defaults
  exit     Exit from resource-manager configuration mode
  help     Description of the interactive help system
  no       Negate a command or set its defaults
  range    Configure range for resource

Router(config-resource-group)# range ?
  limit    Configure the maximum limit
  port     Configure the resource ports

Router(config-resource-group)# range limit ?
<1-192>   Maximum number of connections allowed

Router(config-resource-group)# range port ?
<0-246>   First Modem TTY Number
x/y       Slot/Port for Internal Modems
```

Related Commands

None

resource-pool profile customer

To create a customer profile, enter the **resource-pool profile customer** global configuration command. Enter the **no** form of this command to delete a customer profile from the running configuration.

resource-pool profile customer *name*

no resource-pool profile customer *name*

Syntax Description

name Name of the customer profile. This name can have up to 23 characters.

Defaults

No customer profiles are set up.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource-pool profile customer** global configuration command to create a customer profile.

Examples

The following example shows the creation of a customer profile called “isp-abc”. By entering the **?** command, you can see the options you can set within the customer profile:

```
Router(config)# resource-pool profile customer isp-abc
Router(config-customer-pro)# ?
Customer Profile Configuration Commands:
  dnis      Assign dnis group with this profile
  default   Set a command to its defaults
  exit      Exit from resource-manager configuration mode
  help      Description of the interactive help system
  limit     Configure limits for the profile
  no        Negate a command or set its defaults
  resource  Assign resource and supported call-type
  vpdn     Assign VPDN group/profile with this profile
```

Related Commands

Command	Description
resource-pool group	Creates a resource group for resource management.
limit base-size	Defines the base number of simultaneous standard sessions allowed by a single customer profile.
limit overflow-size	Defines the number of overflow sessions allowed by a single customer profile.
dnis group	Includes a group of DNIS numbers in a customer profile.
resource	Assigns resources and supported call-types to a customer profile.

resource-pool profile discriminator

To create a call discrimination profile, enter the **resource-pool profile discriminator** global configuration command. Enter the **no** form of this command to remove a profile from the running configuration.

resource-pool profile discriminator *name*

no resource-pool profile discriminator *name*

Syntax Description

name Name of the call discriminator profile. This name can have up to 23 characters.

Defaults

No discrimination of calls.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource-pool profile discriminator** global configuration command to create a call discrimination profile.

Examples

The following example shows how to create a discrimination profile called “user1”:

```
res_pool(config)# resource-pool profile discriminator user1
```

Related Commands

Command	Description
dnis group	Includes a group of DNIS numbers in a discriminator profile.
call-type	Rejects particular types of calls.

resource-pool profile service

To set up the service profile configuration, enter the **resource-pool profile service** global configuration command. Enter the **no** form of this command to disable this function.

resource-pool profile service *name*

no resource-pool profile service *name*

Syntax Description

name Name of the service profile. This name can have up to 23 characters.

Defaults

No service profiles are set up.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource-pool profile service** global configuration command to set up the service profile configuration.

Examples

The following example shows the creation of a service profile called “user1”:

```
Router(config)# resource-pool profile service user1
```

Related Commands

None

resource-pool profile vpdn

To set up for VPDN session counting for one or more VPDN groups and to limit sessions that can be authorized for VPDN groups, enter the **resource-pool profile vpdn** global configuration command. Enter the **no** form of this command to disable this function.

resource-pool profile vpdn *name*

no resource-pool profile vpdn *name*

Syntax Description

name Name of the VPDN profile.

Defaults

No VPDN profiles are set up.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource-pool profile vpdn** global configuration command to set up VPDN session counting for one or more VPDN groups and to limit sessions that can be authorized for VPDN groups.

Examples

The following example shows the creation of a VPDN session counter at the VPDN group named “lg-hmgate”:

```
Router(config)# resource-pool profile vpdn lg-hmgate
```

Related Commands

Command	Description
limit base-size	Defines the base number of simultaneous standard sessions allowed by a single customer profile.
limit overflow-size	Defines the number of overflow sessions allowed by a single customer profile.

show call progress tone

To display the contents of the internal call progress (CP) tone database for a specific country, enter the **show call progress tone** EXEC mode command. There is no **no** version of this command.

show call progress tone *country* [*tone-type*]

Syntax Description

<i>country</i>	(Optional) Enter the country code for the country's call progress tone database you want to see.
<i>tone-type</i>	(Optional) Enter the tone type parameters you want to see. Options are: <ul style="list-style-type: none">• busy—Busy tone• congestion—Congestion tone• dialtone—Dial tone• disconnect—Disconnect tone• error—Error tone• off-hook-alert—Off-hook alert tone• off-hook-notice—Off-hook notice tone• pbx-dialtone—PBX dialtone• ringback—Ringback tone• routing—Routing tone

Defaults

The default provided by the modem.

Command Modes

Configuration mode.

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Using this command enables you to see the exact settings as they are programmed in the call-progress-tone database.

Examples

When you enter the **show call progress tone** command, the contents of the internal call progress tone database for a specific country appears as in the following example:

```
Router>show call progress tone japan
Call progress tone: Japan

Dial tone:
0   Forever          425Hz -15.0/-15.0/-15.0 dBm0

PBX Dial tone:
0   Forever          425Hz -15.0/-15.0/-15.0 dBm0

Busy tone:
0   250ms           425Hz -20.0/-20.0/-20.0 dBm0
1   250ms           Silence

Congestion tone:
0   250ms           425Hz -20.0/-20.0/-20.0 dBm0
1   250ms           Silence

Error tone:
0   330ms           950Hz -15.0/-15.0/-15.0 dBm0
1   330ms           1400Hz -15.0/-15.0/-15.0 dBm0
2   330ms           1800Hz -15.0/-15.0/-15.0 dBm0
3   5000ms          Silence

Routing tone:
0   125ms           600Hz -24.0/-24.0/-24.0 dBm0
1   125ms           Silence
2   125ms           600Hz -24.0/-24.0/-24.0 dBm0
3   Forever          Silence

Disconnect tone:
0   330ms           600Hz -15.0/-15.0/-15.0 dBm0
1   330ms           Silence
2   330ms           600Hz -15.0/-15.0/-15.0 dBm0
3   Forever          Silence

Ringback tone:
0   1000ms          425Hz -19.0/-19.0/-19.0 dBm0
1   4000ms          Silence

Off-hook Notice tone:
0   100ms 1400x2040Hz -24.0/-24.0/-24.0 dBm0 -24.0/-24.0/-24.0 dBm0
1   100ms           Silence

Off-hook Alert tone:
0   100ms 1400x2040Hz -15.0/-15.0/-15.0 dBm0 -15.0/-15.0/-15.0 dBm0
1   100ms           Silence
```

Table 5 show show call progress tone Display Field Description

Field	Description
Cadence number	Call progress tones consist of cadences—periods of sound or silence with certain parameters that do not change during the cadence. The cadence number shows the number of a particular cadence within the call progress tone definition. Cadence numbers start at the number 0.
Cadence duration	Cadence duration in “Forever” means that the sound or silence can be heard forever, like in a dialtone.

Table 5 show show call progress tone Display Field Description

Field	Description
Cadence type	Silence—no tone is generated 440Hz—a single frequency is generated. 440x530Hz—two frequencies are added (mixed).
Amplitudes for corresponding frequency components	Amplitudes for the corresponding frequency components. Different amplitudes are used on different trunk types.

The following example shows a specific call progress tone (Japan, busy):

```
Router# show call progress tone japan busy
Busy tone for Japan:
0      2000ms  440x480 Hz -17.0/-17.0/-19.0 dBm0 -17.0/-17.0/-19.0 dBm0
1      4000ms      Silence
```

Related Commands

Command	Description
call progress tone	Specifies the country code for retrieving call progress tone parameters from the call progress tone database.

show dialer dnis

To see how many calls DNIS groups have had, enter the **show dialer dnis** privileged EXEC command. There is no **no** form of this command.

```
show dialer dnis {group [name] | number [number]}
```

Syntax Description

group	Displays DNIS group statistics.
<i>name</i>	(Optional) DNIS group name.
number	Displays DNIS group number statistics.
<i>number</i>	(Optional) DNIS group number.

Defaults

None. If no DNIS groups are configured and resource pooling is enabled, then no calls are accepted. All calls are identified by calltype/DNIS combinations.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **show dialer dnis** EXEC command to see how many calls DNIS groups have had or how many calls a specific DNIS group has had. You can configure each DNIS group with multiple numbers. Using this command shows tables of statistics for each DNIS number received at the NAS.

Examples

The following example shows the **show dialer dnis** command being used to display DNIS group and DNIS number statistics:

```

Router# show dialer dnis ?
  group  DNIS group statistics
  number DNIS number statistics

Router# show dialer dnis group
List of DNIS Groups:
  default
  mdm_grp1

Router# show dialer dnis group mdm_grp1
DNIS Number:2001
  0 total connections
  0 peak connections
  0 calltype mismatches
DNIS Number:2002
  0 total connections
  0 peak connections
  0 calltype mismatches
DNIS Number:2003
  0 total connections
  0 peak connections
  0 calltype mismatches
DNIS Number:2004
  0 total connections
  0 peak connections
  0 calltype mismatches

Router# show dialer dnis number
List of Numbers:
  default
  2001
  2002
  2003
  2004

Router# show dialer dnis number 2001
DNIS Number:2001
  0 connections total
  0 peak connections
  0 call-type mismatches
    
```

Table 6 show dialer dnis Field Descriptions

Field	Description
List of DNIS Groups	List of DNIS groups assigned.
List of Numbers	List of DNIS numbers currently assigned.
DNIS Number	Dialed Number Information Service number assigned to specific customers.
Total connections	Cumulative number of connections since the last clear command was used.
Peak connections	Cumulative number of peak connections since the last clear command was used.
Calltype mismatches	Cumulative number of calltype mismatches since the last clear command was used.

Related Commands

Command	Description
clear dialer dnis	Resets the counter for statistics associated with DNIS groups or numbers.

show resource-pool call

To display all active call information for all customer profiles and resource groups, enter the **show resource-pool call** EXEC command. There is no **no** form of this command.

show resource-pool call

Syntax Description

There are no keywords or arguments for this command.

Defaults

If no calls are up, there is no output. Enter the command to see valid information for all current calls.

Command Modes

User and privileged EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **show resource-pool call** EXEC command to see all active call information for all customer profiles and resource groups. Use this command to see output when one call is up.

Examples

The following example shows output for the **show resource-pool call** command:

```
Router# show resource-pool call
Shelf 0, slot 0, port 0, channel 2, state RM_RPM_RES_ALLOCATED
Customer profile cp1, resource group isdn1
DNIS number 71017
```

Table 7 show resource-pool call Field Descriptions

Field	Description
Shelf	The shelf number where the call is being handled.
Slot	The slot number where the call is being handled.
Port	The port number where the call is being handled.
Channel	The channel number where the call is being handled.
State	The state of the call.
Customer profile	The customer profile name (alphanumeric).
Resource group	The name of the resource group being used for the call.
DNIS number	The DNIS number for the call.

Related Commands

None

show resource-pool customer

To display the contents of one or more customer profiles, enter the **show resource-pool customer** EXEC command. There is no **no** form of this command.

show resource-pool customer [*name*]

Syntax Description

name (Optional) Specifies the name of a specific customer profile. The name can have up to 23 characters.

Defaults

None.

Command Modes

User and privileged EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **show resource-pool customer** EXEC command to see the contents of one or more customer profiles.

Examples

```
Router# show resource-pool customer customer1_isp
 5 active connections
 3 calls accepted
 8 max number of simultaneous connections
 0 calls rejected due to profile limits
 0 calls rejected due to resource unavailable
 0 overflow connections
 0 overflow states entered
 0 minutes spent in overflow
28 minutes since last clear command
```

Table 8 show resource-pool customer Field Descriptions

Field	Description
Active connections	Lists the number of active connections in the specified customer profile.
Calls accepted	Cumulative number of calls accepted since the last clear command in the customer profile—regardless of the call type.
Max number of simultaneous connections	Maximum number of simultaneous connections assigned for this customer profile.

Field	Description
Calls rejected due to profile limits	Cumulative number of calls rejected since the last clear command because the maximum number of allowable simultaneous connections was exceeded. You can configure each customer profile to not exceed a simultaneous call limit. This feature stops a single customer profile from consuming all the system resources.
Calls rejected due to resource unavailable	Cumulative number of calls rejected since the last clear command because no system resources were available to accept the call (such as a free modem for an analog call or an HDLC framer for a circuit switched data call).
Overflow connections	Number of overflow connections active since the last clear command.
Overflow states entered	Number of overflow states processed since the last clear command.
Minutes spent in overflow	Number of minutes that the overflow session has been in process since the last clear command.
Minutes since last clear command	Number of minutes since the clear command has been used.
List of Customer Profiles	Lists the customer profiles set up on the access server.

Related Commands

None

show resource-pool discriminator

To see how many times an incoming call has been rejected due to a specific DNIS/call-type combination, enter the **show resource-pool discriminator** EXEC command. There is no **no** form of this command.

show resource-pool discriminator [*name*]

Syntax Description

name (Optional) Specifies the name of the specific DNIS/call-type that will be rejected. The name can have up to 23 characters.

Defaults

None. You must configure a call discriminator for it to work or appear.

Command Modes

User and privileged EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **show resource-pool discriminator** EXEC command to see how many times an incoming call has been rejected due to a specific DNIS/call-type combination.

Examples

Example 1

```
Router# show resource-pool discriminator
List of Call Discriminator Profiles:
  cd1
  cd2
  cd3
  cd4
Router# show resource-pool discriminator cd1
0 calls rejected
```

Table 9 show resource-pool discriminator Command Field Descriptions

Field	Description
List of Call Discriminator Profiles	A list of the Call Discriminator Profile names currently assigned.
Calls rejected	Number of calls rejected since the last clear command was used (This is cumulative).

Related Commands

None

show resource-pool resource

To see the resource groups configured in the network access server (NAS), enter the **show resource-pool resource** EXEC command. There is no **no** form of this command.

show resource-pool resource [*name*]

Syntax Description

name (Optional) Displays the contents of a specifically named resource group, which was set up by using the **resource-pool group resource name** command. The name can have up to 23 characters.

Defaults

None.

Command Modes

User and privileged EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **show resource-pool resource** EXEC command to see the resource groups configured in the network access server (NAS). To see the contents of a specific resource group, use the **show resource-pool resource name** command.

Examples

The following example shows the output for the **show resource-pool resource** EXEC command:

```
Router# show resource-pool resource
List of Resources:
  modem1
  rgl
  hi

Router# show resource-pool resource modem-group-1
  2 resources in the resource group
  0 resources currently active
  0 calls accepted in the resource group
  0 calls rejected due to resource unavailable
  0 calls rejected due to resource allocation errors
```

Table 10 show resource-pool resource name Command Field Descriptions

Field	Description
Resources in the resource group	Number of resources allocated to this pool. For example, you can limit a range of modems to five. You can limit a range of circuit-switched data calls to 50.
Resources currently active	Number of resources that are currently used in the resource group.
Calls accepted in the resource group	Number of calls accepted in the resource group (This is cumulative).
Calls rejected due to resource unavailable	Number of calls rejected because a resource was not available (This is cumulative).
Calls rejected due to resource allocation errors	Number of times the access server had an available resource, but the resource had an error when the access server tried to allocate it (for example, a bad modem). Therefore, the call was rejected. (This is cumulative.)

Related Commands

None

show resource-pool vpdn

To see the contents of a specific VPDN group or specific VPDN profile, enter the **show resource-pool vpdn** EXEC command. There is no **no** form of this command.

show resource-pool vpdn {**group** | **profile**} [*name*]

Syntax Description

group	Displays all the VPDN groups configured inside the NAS.
profile	Displays all the VPDN profiles configured inside the NAS.
<i>name</i>	(Optional) Specifies the name of a specific VPDN group or profile.

Defaults

None.

Command Modes

User and privileged EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Enter the **show resource-pool vpdn** EXEC command to see the contents of a specific VPDN group or specific VPDN profile.

Examples

Enter the **show resource-pool vpdn group** *name* command to see the contents of a specific VPDN group. This example contains one domain name, one DNIS group, and one end point:

Example 1

```
Router# show resource-pool vpdn group customer2-vpdng
VPDN Group customer2-vpdng found under Customer Profiles: customer2

Tunnel (LTP)
-----
dnis:customer2-calledg
hp.com

Endpoint          Session Limit Priority Active Sessions Status Reserved Sessions
-----
172.21.9.97      *              1           0                OK                -----
Total            *              0           0                0                -----
```

Example 2

```
Router# show resource-pool vpdn group
List of VPDN Groups under Customer Profiles
Customer Profile user1: big
Customer Profile user2: green
List of VPDN Groups under VPDN Profiles
VPDN Profile lggate: vpdnlgate
VPDN Profile yellow: hi
```

Table 11 show resource-pool vpdn group Command Field Descriptions

Field	Description
Endpoint	IP address of HGW/LNS router.
Session Limit	Number of sessions permitted for the designated endpoint.
Priority	Loadsharing HGW/LNSs are always marked with a priority of 1.
Active Sessions	Number of active sessions on the NAS. These are sessions successfully established with endpoints (not reserved sessions).
Status	Only two status types are possible: OK and busy.
Reserved Sessions	Authorized sessions that are waiting to see if they can successfully connect to endpoints. Essentially, these sessions are queued calls. In most cases, reserved sessions become active sessions.
*	No limit is set.
List of VPDN Groups under Customer Profiles	A list of VPDN groups that are assigned to customer profiles. The customer profile name is listed first, followed by the name of the VPDN group assigned to it.
List of VPDN Groups under VPDN Profiles	A list of VPDN groups that are assigned to customer profiles. The VPDN profile name is listed first, followed by the VPDN group assigned to it.

Example 3

```
Router# show resource-pool vpdn profile
% List of VPDN Profiles:
lg-hmgate
lggate
yellow
```

Example 4

```
Router# show resource-pool vpdn profile lggate
0 active connections
0 max number of simultaneous connections
0 calls rejected due to profile limits
0 calls rejected due to resource unavailable
0 overflow connections
0 overflow states entered
0 overflow connections rejected
3003 minutes since last clear command
```

Table 12 show resource-pool vpdn profile Command Field Descriptions

Field	Description
List of VPDN Profiles	A list of the VPDN profiles that have been assigned.
Active connections	Number of active VPDN connections counted by the VPDN profile.
Max number of simultaneous connections	Maximum number of VPDN simultaneous connections counted by the VPDN profile. This value helps you determine how many VPDN sessions to subscribe to a specific profile.
Calls rejected due to profile limits	Number of calls rejected since the last clear command because the profile limit has been exceeded.
Calls rejected due to resource unavailable	Number of calls rejected since the last clear command because the assigned resource was unavailable.
Overflow connections	Number of overflow connections used since the last clear command.
Overflow states entered	Number of overflow states entered since the last clear command.
Overflow connections rejected	Number of overflow connections rejected since the last clear command.
Minutes since last clear command	Number of minutes elapsed since the last clear command was used.

Related Commands

None

show vpdn domain

To view all VPDN domains and DNIS groups configured on the NAS, enter the **show vpdn domain** EXEC command. There is no **no** form of this command.

show vpdn domain

Syntax Description

There are no keywords or arguments used with this command.

Defaults

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **show vpdn domain** EXEC command to see all VPDN domains and DNIS groups configured on the NAS.

Examples

```
Router# show vpdn domain
Tunnel          VPDN Group
-----
dnis:cg2        vgdnis (L2F)
domain:twu-ultra test (L2F)
```

Table 13 show vpdn domain Command Field Descriptions

Field	Description
Tunnel	The assigned name of the tunnel endpoint.
VPDN Group	The assigned name of the VPDN group using the tunnel.

Related Commands

None

show vpdn group

To see a summary of the relationships among VPDN groups and customer/VPDN profiles, or to summarize the configuration of a VPDN group including domain/DNIS, loadsharing information and current session information, enter the **show vpdn group** EXEC command. There is no **no** form of this command.

show vpdn group *name* [**domain** | **endpoint**]

Syntax Description

<i>name</i>	Name of vpdn-group.
domain	DNIS/domain information.
endpoint	Endpoint session information.

Defaults

None.

Command Modes

User and privileged EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **show vpdn group** EXEC command to see a summary of the relationships among VPDN groups and customer/VPDN profiles, or to summarize the configuration of a VPDN group including domain/DNIS, loadsharing information, and current session information. To summarize relationships among VPDN groups and Customer/VPDN profiles, use the syntax **show vpdn group** group-name.

Examples

```
Router > show vpdn group

VPDN Group  Customer Profile  VPDN Profile
-----
1           -             -
2           -             -
3           -             -
lisun       cp1             -
outgoing-2 -             -
test       -             -
*vg1       cpdnis         -
*vg2       cpdnis         -
vgdnis     +cp1          vp1
vnumber    -             -
vp1        -             -

* VPDN group not configured
+ VPDN profile under Customer profile
```

Note VPDN group is marked with “*” if it doesn't exist, but is used under customer/VPDN profile.

Note Customer profiles are marked with “+” if the corresponding VPDN group is not directly configured under a customer profile. Instead, the corresponding VPDN profile is configured under the customer profile.

```
Router > show vpdn group vgdnis

Tunnel (L2TP)
-----
dnis:cg1
dnis:cg2
dnis:jan
cisco.com

Endpoint          Session Limit Priority Active Sessions Status Reserved Sessions
-----
172.21.9.67      *              1           0              OK           -
-----
Total            *              0           0              0           0
```

Note Tunnel section lists all domain/DNIS (“dnis” appears before DNIS).

The session limit endpoint is the sum of the session limits of all endpoints and is marked with “*” if there is no limit (indicated by “*”) for any endpoint.

If the endpoint has no session limit, reserved sessions are marked with “-”.

show vpdn group

```
Router# show vpdn group

VPDN Group      Customer Profile  VPDN Profile
-----
customer1-vpdng customer1         customer1-profile
customer2-vpdng customer2         -

Router# show vpdn group customer1-vpdng

Tunnel (L2TP)
-----
cisco.com
cisco1.com
dnis:customer1-calledg

Endpoint        Session Limit  Priority  Active Sessions  Status  Reserved Sessions
-----
172.21.9.67    *              1        0                OK
172.21.9.68    100            1        0                OK
172.21.9.69    *              5        0                OK
-----
Total          *              0        0                0
```

Table 14 show vpdn group Command Field Descriptions

Field	Description
VPDN Group	The assigned name of the VPDN group using the tunnel.
Customer Profile	The name of the assigned customer profile.
VPDN Profile	The name of the assigned VPDN profile.
Tunnel	The assigned name of the tunnel endpoint.
Endpoint	IP address of HGW/LNS router.
Session Limit	Number of sessions permitted for the designated endpoint.
Priority	Loadsharing HGW/LNSs are always marked with a priority of 1.
Active Sessions	Number of active sessions on the NAS. These are sessions successfully established with endpoints (not reserved sessions).
Status	Only two status types are possible: OK and busy.
Reserved Sessions	Authorized sessions that are waiting to see if they can successfully connect to endpoints. Essentially, these sessions are queued calls. In most cases, reserved sessions become active sessions.

Related Commands

None

show vpdn multilink

To see the multilink sessions authorized for all VPDN groups, enter the **show vpdn multilink EXEC** command. There is no **no** form of this command.

show vpdn multilink

Syntax Description

There are no keywords or options for this command.

Defaults

None.

Command Modes

User and privileged EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **show vpdn multilink EXEC** command to see the multilink sessions authorized for all VPDN groups.

Examples

L2F Tunnel and Session Information (Total tunnels=1 sessions=1)

NAS	CLID	HGW	CLID	NAS Name	HGW Name	State
24		10		centi3_nas	twu253_hg	open
				172.21.9.46	172.21.9.67	

CLID	MID	Username	Intf	State
10	1	twu@twu-ultra.cisco.com	Se0:22	open

Router# **show vpdn multilink**

Multilink Bundle Name	VPDN Group	Active links	Reserved links	Bundle/Link Limit
twu@twu-ultra.cisco.com	vgdnis	1	0	*/*

Router#

Table 15 show vpdn multilink Command Field Descriptions

Field	Description
NAS CLID	The network access server (NAS) Caller Line Identification number (CLID).
HGW CLID	The home gateway (HGW) Caller Line Identification number (CLID).
NAS Name	The name assigned to the NAS.
HGW Name	Name assigned to the HGW.
State	Operational state of the designated piece of equipment.
CLID	Calling Line Identification number.
MID	Modem Identification.
Username	Assigned user name.
Intf	Type of interface.
State	Operational state of the designated piece of equipment.
Multilink Bundle Name	The name of the multilink bundle.
VPDN Group	Name of the VPDN group.
Active Links	Number of active links.
Reserved Links	Number of reserved links.
Bundle/Link limit	Limit of bundles or links available.

Related Commands

None

source template

To attach a configured customer profile template to a particular customer profile, enter the **source template** customer profile configuration command. There is no **no** form of this command.

source template *name*

Syntax Description

This command has no arguments or keywords.

Defaults

No templates are sourced or attached to a customer profile.

Command Modes

Customer profile configuration

Command History

Release	Modification
12.0(6)T	This command was introduced.

Usage Guidelines

All PPP and peer-default commands are allowed for a particular customer profile template under this grouping.

Examples

The following example shows the creation and configuration of a customer profile template named *acme-direct* and its subsequent assignment to the customer profile *acme1*:

```
Router(config)# template acme-direct
Router(config-template)# multilink {max-fragments num | max-links num | min-links num}
Router(config-template)# peer match aaa-pools
Router(config-template)# peer default ip address pool acme-numbers
Router(config-template)# ppp ipcp dns 10.1.1.1 10.2.2.2
Router(config-template)# ppp multilink
Router(config-template)# exit
Router(config)# resource-pool profile customer acme1
Router(config-customer-profi)# source template acme-direct
```

Related Commands

Command	Description
template	Assigns a group of PPP commands to a customer profile template.

template

To access the template configuration mode for configuring a particular customer profile template, enter the **template** global configuration command. Use the **no** form of this command to delete the template of the specified name.

```
template name {default | exit | multilink | no | peer | ppp}
no template name {default | exit | multilink | no | peer | ppp}
```

Syntax Description

<i>name</i>	A name that identifies the template.
default	Sets the command to its defaults.
exit	Exits from resource-manager configuration mode.
multilink	Configures multilink parameters.
no	Negates the command or its defaults.
peer	Accesses peer parameters for point-to-point interfaces.
ppp	Accesses Point-to-Point Protocol.

Defaults

No templates are configured.

Command Modes

Global configuration

Usage Guidelines

All PPP and peer-default commands are enabled for a particular customer profile template under this grouping.

Examples

The following example shows the creation and configuration of a customer profile template named *acme-direct* and its subsequent assignment to the customer profile *acme1*:

```
Router(config)# template acme-direct
Router(config-template)# multilink max-fragments 10
Router(config-template)# peer match aaa-pools
Router(config-template)# peer default ip address pool acme-numbers
Router(config-template)# ppp ipcp dns 10.1.1.1 10.2.2.2
Router(config-template)# ppp multilink
Router(config-template)# exit
Router(config)# resource-pool profile customer acme1
Router(config-customer-profi)# source template acme-direct
```

Related Commands

Command	Description
source template	Associates the template with a customer profile.

vpdn group

To associate a VPDN group to a customer or VPDN profile, enter the **vpdn group** configuration command. Enter the **no** form of this command to remove the VPDN group from a customer profile or VPDN profile.

vpdn group *name*

no vpdn group *name*

Syntax Description

name Name of the VPDN group.

Defaults

None.

Command Modes

Customer profile configuration/VPDN profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **vpdn group** configuration command to associate a VPDN group to a customer or VPDN profile. You can count the sessions for an entire VPDN group under a single VPDN profile.

To add a VPDN group to a customer profile or VPDN profile, use either the **vpdn profile** or the **vpdn group** command:

- VPDN group under customer profile allows VPDN connections for this customer profile.
- VPDN groups under VPDN profile allows combined session counting over these VPDN groups.

Examples

Example 1

```
Router(config)# resource profile vpdn lggate
Router(config-vpdn-profile)# vpdn group ?
WORD Enter name of VPDN group
```

Example 2

```
Router(config)# resource profile customer customer1

Router(config-customer-pro)# vpdn group ?
WORD Enter name of VPDN group
```

vpdn group

Related Commands

Command	Description
resource-pool profile	Creates a customer profile.

vpdn profile

To combine session counting over VPDN groups, enter the **vpdn profile** customer profile configuration command. Enter the **no** form of this command to remove a VPDN profile from a customer profile.

vpdn profile *name*

no vpdn profile *name*

Syntax Description

name Name of the VPDN profile.

Defaults

None.

Command Modes

Customer profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **vpdn profile** configuration command to combine session counting over VPDN groups. Configure VPDN groups under the VPDN profile only by using the **vpdn profile** command; then, link these VPDN groups to the customer profile by using the **vpdn group** VPDN profile configuration command.

Examples

Example 1

```
Router(config)# resource profile customer user1

Router(config-customer-pro)# vpdn profile ?
WORD  Enter name of VPDN group
```

Related Commands

Command	Description
resource-pool profile	Creates a customer profile.

Debug Commands

This section documents a new debug command. All other commands used with this feature are documented in the Cisco Release 12.0 command references.

- **debug resource pool**

debug resource-pool

To see and trace resource pool management activity, enter the **debug resource-pool** debug command. To disable this function, enter the **undebug** version of this command.

debug resource-pool

undebug resource-pool

Syntax Description

This command has no keywords or arguments.

Defaults

Disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Enter the **debug resource-pool** debug command to see and trace resource pool management activity:

Table 16 Resource Pooling States

State	Description
RM_IDLE	No call activity.
RM_RES_AUTHOR	Call waiting for authorization, message sent to AAA.
RM_RES_ALLOCATING	Call authorized, resource-grp-mgr allocating.
RM_RES_ALLOCATED	Resource allocated, connection acknowledgment sent to signaling state. Call should get connected and become active.
RM_AUTH_REQ_IDLE	Signaling module disconnected call while in RM_RES_AUTHOR. Waiting for authorization response from AAA.
RM_RES_REQ_IDLE	Signaling module disconnected call while in RM_RES_ALLOCATING. Waiting for resource allocation response from resource-group manager.
RM_DNIS_AUTHOR	An intermediate state before proceeding with RPM authorization.
RM_DNIS_AUTH_SUCCEEDED	DNIS authorization succeeded.
RM_DNIS_RES_ALLOCATED	DNIS resource allocated.
RM_DNIS_AUTH_REQ_IDLE	DNIS authorization request idle.
RM_DNIS_AUTHOR_FAIL	DNIS authorization failed.
RM_DNIS_RES_ALLOC_SUCCESS	DNIS resource allocation succeeded.
RM_DNIS_RES_ALLOC_FAIL	DNIS resource allocation failed.

Table 16 Resource Pooling States

State	Description
RM_DNIS_RPM_REQUEST	DNIS resource pool management requested.

You can use the resource-pool state to isolate problems. For example, if a call fails authorization in the RM_RES_AUTHOR state, investigate further with AAA authorization debugs to determine whether the problem lies in the resource-pool manager, AAA, or dispatcher.

Examples

The following example shows different instances where you can use the **debug resource-pool** command:

```

Router # debug resource-pool
RM general debugging is on

Router # show debug
General OS:
  AAA Authorization debugging is on
Resource Pool:
  resource-pool general debugging is on
Router #
Router # ping 21.1.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 21.1.1.10, timeout is 2 seconds:
*Jan 8 00:10:30.358: RM state:RM_IDLE event:DIALER_INCALL DS0:0:0:0:1
*Jan 8 00:10:30.358: RM: event incoming call

/* An incoming call is received by RM */

*Jan 8 00:10:30.358: RM state:RM_DNIS_AUTHOR event:RM_DNIS_RPM_REQUEST
DS0:0:0:0:1

/* Receives an event notifying to proceed with RPM authorization while
in DNIS authorization state */

*Jan 8 00:10:30.358: RM:RPM event incoming call
*Jan 8 00:10:30.358: RPM profile cpl found

/* A customer profile "cpl" is found matching for the incoming call, in
the local database */

*Jan 8 00:10:30.358: RM state:RM_RPM_RES_AUTHOR
event:RM_RPM_RES_AUTHOR_SUCCESS DS0:0:0:0:1

/* Resource authorization success event received while in resource
authorization state*/

*Jan 8 00:10:30.358: Allocated resource from res_group isdn1
*Jan 8 00:10:30.358: RM:RPM profile "cpl", allocated resource "isdn1"
successfully
*Jan 8 00:10:30.358: RM state:RM_RPM_RES_ALLOCATING
event:RM_RPM_RES_ALLOC_SUCCESS DS0:0:0:0:1

/* Resource allocation success event received while attempting to
allocate a resource */
*Jan 8 00:10:30.358: Se0:1 AAA/ACCT/RM: doing resource-allocated
(local) (nothing to do)
*Jan 8 00:10:30.366: %LINK-3-UPDOWN: Interface Serial0:1, changed state
to up
*Jan 8 00:10:30.370: %LINK-3-UPDOWN: Interface Serial0:1, changed state

```

```

to down
*Jan 8 00:10:30.570: Se0:1 AAA/ACCT/RM: doing resource-update (local)
cp1 (nothing to do)
*Jan 8 00:10:30.578: %LINK-3-UPDOWN: Interface Serial0:0, changed
state to up
*Jan 8 00:10:30.582: %DIALER-6-BIND: Interface Serial0:0 bound to
profile Dialer0...
Success rate is 0 percent (0/5)
Router #
*Jan 8 00:10:36.662: %ISDN-6-CONNECT: Interface Serial0:0 is now
connected to 71017
*Jan 8 00:10:52.990: %DIALER-6-UNBIND: Interface Serial0:0 unbound from
profile Dialer0
*Jan 8 00:10:52.990: %ISDN-6-DISCONNECT: Interface Serial0:0
disconnected from 71017 , call lasted 22 seconds
*Jan 8 00:10:53.206: %LINK-3-UPDOWN: Interface Serial0:0, changed state
to down
*Jan 8 00:10:53.206: %ISDN-6-DISCONNECT: Interface Serial0:1
disconnected from unknown , call lasted 22 seconds
*Jan 8 00:10:53.626: RM state:RM_RPM_RES_ALLOCATED event:DIALER_DISCON
DS0:0:0:0:1

/* Received Disconnect event from signalling stack for a call which
has a resource allocated. */

*Jan 8 00:10:53.626: RM:RPM event call drop

/* RM processing the disconnect event */

*Jan 8 00:10:53.626: Deallocated resource from res_group isdn1
*Jan 8 00:10:53.626: RM state:RM_RPM_DISCONNECTING
event:RM_RPM_DISC_ACK DS0:0:0:0:1

/* An intermediate state while the DISCONNECT event is being processed
by external servers, before RM goes back into IDLE state.
*/

```

Table 17 debug resource-pool Command Field Descriptions

Field	Description
RM state: RM_IDLE	Resource manager state that displays no active calls.
RM state: RM_RES_AUTHOR	Resource authorization state.
RES_AUTHOR_SUCCESS DS0: shelf:slot:port:channel	Actual physical resource that is used
Allocated resource from res_group	Physical resource group that accepts the call.
RM profile "x", allocated resource "x"	Specific customer profile and resource group names used to accept the call.
RM state: RM_RES_ALLOCATING	Resource manager state that unifies a call with a physical resource.

Related Commands

None

Glossary

Backup customer profile—Configured locally on the NAS to be used when the link between the NAS and RPMS is out of service, backup customer profiles allow the NAS to answer calls for specific customers when there is no connection to the Cisco RPMS. The backup customer profile can contain all elements defined in a standard customer profile, including base-size or overflow parameters. However, when the connection between the NAS and Cisco RPMS is out of service, session counting and session limits are not applied to incoming calls on the RPMS—they are applied only on the NAS. Also, after the connection is reestablished, there is no synchronization of call counters between the NAS and Cisco RPMS.

Call discrimination—Ability to reject a call before answering based on DNIS, call type (bearer capability), or DNIS and call type. The NAS or Cisco RPMS matches the call against the DNIS number and call type (bearer capability) restrictions. If a match is found, the call is rejected and a no answer call treatment is sent to the switch. Otherwise, call processing continues.

Call treatment—The signaling return code sent by resource pool management when a call is not accepted. Call treatments are:

- no answer—the caller receives rings until the switch eventually times out or the caller disconnects.
- busy—the NAS drops the switch, which sends a busy signal to the caller.
- channel not available—the NAS directs the switch to send the call to the next available channel in the trunk group.

Call type—Equivalent to a bearer capability in ISDN, but also applies to Channel Associated Signaling (CAS). The call type is used to differentiate calls (digital or analog) for call discrimination and to assign calls to appropriate resources. Call types are:

- Speech
- Digital
- V.110
- V.120

CHAP—Challenge Handshake Authentication Protocol. Security feature supported on lines using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines whether that user is allowed access.

Cisco RPMS—Cisco Resource Pool Manager Server. A central server that provisions customer profiles and group resources over several NASs.

CLI—Command line interface for the Cisco IOS software.

Customer profile—A customized configuration that identifies a customer and specifies the types of resources and services to be used by the customer's dial plan. Customer profiles allow for configuration and resource usage statistics for:

- active sessions
- session limit
- overflow sessions
- overflow session limit
- session counts
- DNIS groups

- domain groups
- call type
- resource groups
- resource services
- call treatment
- VPDN active sessions
- VPDN multilink bundles
- VPDN multilink sessions within each bundle
- VPDN endpoints
- VPDN groups
- VPDN session limits.

Default customer profile—Profile configured to accept unmapped calls—those calls with no DNIS information or with DNIS info that is not mapped to a standard customer profile.

- If this profile is configured, a call is answered automatically.
- If this profile is not configured, unmapped calls are rejected.

Configured by not entering the DNIS or domain group value, or by entering the reserved keyword value “default” for the DNIS or domain group. Identical to standard customer profile, but does not have any associated DNIS groups. Used to provide session counting, resource assignment, and VPDN tunnel creation for customers using domain-based or retail dial service rather than DNIS-based service. These calls are assigned to resources based only on call type and are answered. If a VPDN is used, during user authorization the domain information received by the NAS is compared with the VPDN tunnels associated with the default customer profile. If a match is found, a new tunnel is created, or the call is assigned to an existing tunnel, and VPDN session counting occurs. Otherwise, the call is rejected.

DNIS—Dialed Number Information Service or Dialed Number Identification Service. Also known as the called party number. The telephone number of the called party after translation occurs in the Public Switched Telephone Network (PSTN). A given destination can have a different DNIS number based on how the call is placed (for example, 800 or direct dial).

DNIS group—A collection of DNIS entries associated with a customer profile or call discriminator profile. Call types can also be associated with a DNIS group to support more than one call type, which can map to a specific resource and service group in a profile. There is no set limit on the number of DNIS groups or DNIS entries supported by a NAS.

DNS—domain name server. A DNS server is requested by a client during IPCP negotiation.

HGW—Home gateway. A NAS.

LAC—L2TP Access Concentrator.

LNS—L2TP Network Server.

Multilink PPP—A protocol that enables a user to accept incoming multilink calls.

NAS—Network access server. Any of Cisco’s access server line of products including the AS5200, the AS5300, and the AS5800.

Overflow billing—State assigned to calls that occur after the session limit has been reached. Once a call is identified as an overflow call, it maintains the overflow status throughout its duration—even if the current number of calls returns below the session limit.

PAP—Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and host name or username in the clear (unencrypted). PAP itself does not prevent unauthorized access, but merely identifies the remote end. The router or access server then determines if that user is allowed access. PAP is supported only on PPP lines.

Physical resources—Also called a resource group. Providers can configure these physical resources by specifying a range of ports. These resources groups can be shared between customer profiles.

PPP—Point-to-Point Protocol. A protocol that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. PPP was designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: Link Control Protocol and Network Control Protocol.

RADIUS—Remote Authentication Dial-In User Service. RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server containing all user authentication and network-service access information.

Resource groups—A group of similar NAS resources to access for incoming calls. For example, separate resource groups can be created for 56K modems, V.110 terminal adapters, and calls terminating on HDLC framers (ISDN). Resource groups used by Cisco RPMS must be configured on the NAS and the resource group names must match.

Resource Manager Protocol—A proprietary behind-the-scenes metaprotocol running between the NASs and RPMS that defines what information needs to be passed between the NAS and the RPMS. The RMP protocol displays in debug mode as AAA messages. Use the **debug aaa authorization**, **debug aaa accounting**, **debug resource-pool**, and **debug tacacs+** commands to see these parameters.

TACACS+—Terminal Access Controller Access Control System. TACACS+ is a protocol that provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is implemented through AAA and can be enabled only by using AAA commands.

VPDN group—For configured VPDN sessions, the home gateway and limit data required to set up or reject a VPDN session. This data includes an associated domain name or DNIS, endpoint IP address, maximum MLP bundles per VPDN group, and maximum links per MLP bundle.

VPDN session—A communication channel between a user and an HGW/LNS router.

VPDN tunnel—An IP connection established between a NAS/LAC and an HGW/LNS router.

WINS—Windows Internet Naming Service. A WINS server name is requested by a client during IPCP negotiation.

Note For a list of other internetworking terms, see the Internetworking Terms and Acronyms document available on the Documentation CD-ROM and Cisco Connection Online (CCO) at the following URL: <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm>.
