JUNIPER NETWORKS

Application-Level Gateways for JSF

Published: 2012-07-02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Table of Contents

About the Documentation ix
Documentation and Release Notes ix
Supported Platforms ix
Using the Examples in This Manual ix
Merging a Full Example x
Merging a Snippet x
Documentation Conventions xi
Documentation Feedback xiii
Requesting Technical Support xiii
Self-Help Online Tools and Resources xiii
Opening a Case with JTAC xiv

Part 1 Overview

Chapter 1 **Application-Level Gateways 3**

Application-Level Gateways for JSF 3
ALG Descriptions 4
Supported ALGs 4
ALG Support Details 5
Basic TCP ALG 5
Basic UDP ALG 6
DCE RPC Services 6
DNS 6
FTP 6
MSRPC 7
ONC RPC Services 7
PPTP 7
RPC and RPC Portmap Services 7
RTSP 9
SIP 9
SQLNet 10
Talk 10
UNIX Remote-Shell Services 10
Verifying the Output of ALG Sessions 10
System Log Messages 10
System Log Configuration 11
System Log Output 11
Junos Default Groups 12
Examples: Referencing the Preset Statement from the Junos Default Group 17

Part 2 Configuration

Chapter 2 Configuration Tasks 21

Configuring Application Protocol Properties 21
Configuring an Application Protocol 22
Configuring the Network Protocol 23
Configuring the ICMP Code and Type 24
Configuring Source and Destination Ports 26
Configuring the Inactivity Timeout Period 29
Configuring an SNMP Command for Packet Matching 29
Configuring an RPC Program Number 29
Configuring the TTL Threshold 29
Configuring a Universal Unique Identifier 30
Configuring Application Sets 30
Configuring Juniper Service Framework – Application-Level Gateways, Rules, and Services Set 30
Configuring the JSF Application-Level Gateways Package 30
Configuring Stateful Firewall with ALGs 33
Configuring Network Address Translation with ALGs 34

Chapter 3 Example 39

Examples: Configuring Application Protocols 39

Chapter 4 Configuration Statements 41

application 41
application-protocol 42
application-set 43
applications 43
destination-port 44
icmp-code 44
icmp-type 45
inactivity-timeout 45
learn-sip-register 45
protocol 46
rpc-program-number 47
sip-call-hold-timeout 47
snmp-command 48
source-port (Applications) 48
ttl-threshold 49
uuid 49

Part 3 Administration

Chapter 5 ALG Operational Mode Commands 53

clear services alg statistics 54
show services alg conversations 55
show services alg statistics 59
show services sessions 68

Part 4 Index

Index 77

List of Tables

About the Documentation ix

Table 1: Notice Icons xi
Table 2: Text and Syntax Conventions xi

Part 1 Overview

Chapter 1 Application-Level Gateways 3

Table 3: ALGs Supported Under JSF 4
Table 4: Supported RPC Services 8

Part 2 Configuration

Chapter 2 Configuration Tasks 21

Table 5: Application Protocols Supported by Services Interfaces 22
Table 6: Network Protocols Supported by Services Interfaces 23
Table 7: ICMP Codes and Types Supported by Services Interfaces 25
Table 8: Port Names Supported by Services Interfaces 26

Part 3 Administration

Chapter 5 ALG Operational Mode Commands 53

Table 9: show services alg conversations Output Fields 56
Table 10: show services alg statistics Output Fields 59
Table 11: show services sessions Output Fields 70

About the Documentation

- Documentation and Release Notes on page ix
- Supported Platforms on page ix
- Using the Examples in This Manual on page ix
- Documentation Conventions on page xi
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiii

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books .

Supported Platforms

For the features described in this document, the following platforms are supported:

- M Series
- T Series
- MX Series
- J Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

   ```
   [edit]
   user@host# edit system scripts
   [edit system scripts]
   ```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

   ```
   [edit system scripts]
   user@host# load merge relative /var/tmp/ex-script-snippet.conf
   load complete
   ```

For more information about the **load** command, see the *Junos OS CLI User Guide*.

Documentation Conventions

Table 1 on page xi defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the**configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Italic text like this	• Introduces or emphasizes important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub <default-metric** ***metric*****>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/

- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html .

PART 1

Overview

- Application-Level Gateways on page 3

CHAPTER 1

Application-Level Gateways

- Application-Level Gateways for JSF on page 3
- ALG Descriptions on page 4
- Verifying the Output of ALG Sessions on page 10
- Junos Default Groups on page 12

Application-Level Gateways for JSF

An *Application Layer Gateway (ALG)* is a software component that is designed to manage specific protocols such as FTP on Juniper Networks devices running Junos OS. The ALG module is responsible for Application-Layer aware packet processing.

ALG functionality can be triggered either by a service or application configured in the security policy:

- A *service* is an object that identifies an application protocol using Layer 4 information (such as standard and accepted TCP and UDP port numbers) for an application service (such as Telnet, FTP, SMTP, and HTTP).
- An *application* specifies the Layer 7 application that maps to a Layer 4 service.

A predefined service already has a mapping to a Layer 7 application. However, for custom services, you must link the service to an application explicitly, especially if you want the policy to apply an ALG.

ALGs for packets destined to well-known ports are triggered by service type. The ALG intercepts and analyzes the specified traffic, allocates resources, and defines dynamic policies to permit the traffic to pass securely through the device:

1. When a packet arrives at the device, the flow module forwards the packet according to the security rule set in the policy.
2. If a policy is found to permit the packet, the associated service type or application type is assigned and a session is created for this type of traffic.
3. If a session is found for the packet, no policy rule match is needed. The ALG module is triggered if that particular service or application type requires the supported ALG processing.

The ALG also inspects the packet for embedded IP address and port information in the packet payload, and performs Network Address Translation (NAT) processing if necessary. The ALG also opens a gate for the IP address and port number to permit data exchange for the session. The control session and data session can be coupled to have the same timeout value, or they can be independent.

ALGs are supported on chassis clusters.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

ALG Descriptions

This topic provides details about Application Layer Gateways (ALGs) supported under the Junos OS Service Framework (JSF). It includes the following:

- Supported ALGs on page 4
- ALG Support Details on page 5

Supported ALGs

Table 3 on page 4 lists ALGs supported by JSF.

Table 3: ALGs Supported Under JSF

ALGs Supported	v4 - v4	v4 - v6	v6 - v6
Basic TCP ALG	Yes	No	No
Basic UPD ALG	Yes	No	No
DCE RPC Services	Yes	No	No
DNS	Yes	No	No
FTP	Yes	No	No
MSRPC	Yes	No	No
PPTP	Yes	No	No
Sun RPC and RPC Port Map Services	Yes	No	No
RTSP	Yes	No	No
SIP	Yes	No	No
SQLNET	Yes	No	No
TALK	Yes	No	No
Unix Remote Shell Service	Yes	No	No

ALG Support Details

ALG support includes managing pinholes and parent-child relationships for the supported all ALGs. This section includes details about the following ALGs:

- Basic TCP ALG on page 5
- Basic UDP ALG on page 6
- DCE RPC Services on page 6
- DNS on page 6
- FTP on page 6
- MSRPC on page 7
- ONC RPC Services on page 7
- PPTP on page 7
- RPC and RPC Portmap Services on page 7
- RTSP on page 9
- SIP on page 9
- SQLNet on page 10
- Talk on page 10
- UNIX Remote-Shell Services on page 10

Basic TCP ALG

This ALG performs basic sanity checking on TCP packets. If it finds errors, it generates the following anomaly events and system log messages:

- TCP source or destination port zero
- TCP header length check failed
- TCP sequence number zero and no flags are set
- TCP sequence number zero and FIN/PSH/RST flags are set
- TCP FIN/RST or SYN(URG|FIN|RST) flags are set

The TCP ALG performs the following steps:

1. When the router receives a SYN packet, the ALG creates TCP forward and reverse flows and groups them in a *conversation*. It tracks the TCP three-way handshake.
2. The SYN-defense mechanism tracks the TCP connection establishment state. It expects the TCP session to be established within a small time interval (currently 4 seconds). If the TCP three-way handshake is not established in that period, the session is terminated.
3. A keepalive mechanism detects TCP sessions with nonresponsive endpoints.
4. Internet Control Message Protocol (ICMP) errors are allowed only if there is a flow that matches the selector information specified in the ICMP data.

Basic UDP ALG

This ALG performs basic sanity checking on UDP headers. If it finds errors. it generates the following anomaly events and system log messages:

- UDP source or destination port 0
- UDP header length check failed

The UDP ALG performs the following steps:

1. When it receives the first packet, the ALG creates bidirectional flows to accept forward and reverse UDP session traffic.
2. If the session is idle for more than the maximum allowed idle time (the default is 30 seconds), the flows are deleted.
3. ICMP errors are allowed only if there is a flow that matches the selector information specified in the ICMP data.

DCE RPC Services

Distributed Computing Environment (DCE) Remote Procedure Call (RPC) services are mainly used by Microsoft applications. The ALG uses well-known TCP port 135 for port mapping services. and uses the universal unique identifier (UUID) instead of the program number to identify protocols. The main application-based DCE RPC is the Microsoft Exchange Protocol.

Support for stateful firewall and network address translation (NAT) services requires that you configure the DCE RPC portmap ALG on TCP port 135. The DCE RPC ALG uses the TCP protocol with application-specific UUIDs.

DNS

The Domain Name Service (DNS) ALG handles data associated with locating and translating domain names into IP addresses. The ALG typically runs on port 53. The ALG monitors DNS query and reply packets and supports only UDP traffic. The ALG does not support payload translations. The DNS ALG will only close the session when a reply is received or an idle timeout is reached.

FTP

FTP is the File Transfer Protocol, specified in RFC 959. In addition to the main control connection, data connections are also made for any data transfer between the client and the server; and the host, port, and direction are negotiated through the control channel.

For non-passive-mode FTP, the Junos OS stateful firewall service scans the client-to-server application data for the PORT command, which provides the IP address and port number to which the server connects. For passive-mode FTP, the Junos OS stateful firewall service scans the client-to-server application data for the PASV command and then scans the server-to-client responses for the 227 response, which contains the IP address and port number to which the client connects.

There is an additional complication: FTP represents these addresses and port numbers in ASCII. As a result, when addresses and ports are rewritten, the TCP sequence number might be changed, and thereafter the NAT service needs to maintain this delta in SEQ and ACK numbers by performing sequence NAT on all subsequent packets.

Support for stateful firewall and NAT services requires that you configure the FTP ALG on TCP port 21 to enable the FTP control protocol. The ALG performs the following tasks:

- Automatically allocates data ports and firewall permissions for dynamic data connection
- Creates flows for the dynamically negotiated data connection
- Monitors the control connection in both active and passive modes
- Rewrites the control packets with the appropriate NAT address and port information

MSRPC

MSRPC is a modified version of DCE/RPC. Additions include support for Unicode strings, implicit handles, inheritance of interfaces.

ONC RPC Services

Open Networks Computing (ONC) RPC services function similarly to DCE RPC services. However, the ONC RPC ALG uses TCP/UDP port 111 for port mapping services and uses the program number to identify protocols rather than the UUID.

Support for stateful firewall and NAT services requires that you configure the ONC RPC portmap ALG on TCP port 111. The ONC RPC ALG uses the TCP protocol with application-specific program numbers.

PPTP

The Point-to-Point Tunneling Protocol (PPTP) ALG is a TCP-based ALG. PPTP allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP defines a client-server architecture, a PPTP Network Server, and a PPTP Access Concentrator. The PPTP ALG requires a control connection and a data tunnel. The control connection uses TCP to establish and disconnect PPP sessions, and runs on port 1723. The data tunnel carries PPP traffic in generic routing encapsulated (GRE) packets that are carried over IP.

RPC and RPC Portmap Services

The Remote Procedure Call (RPC) ALG uses well-known ports TCP 111 and UDP 111 for port mapping, which dynamically assigns and opens ports for RPC services. The RPC Portmap ALG keeps track of port requests and dynamically opens the firewall for these requested ports. The RPC ALG can further restrict the RPC protocol by specifying allowed program numbers.

The ALG includes the RPC services listed in Table 4 on page 8.

Table 4: Supported RPC Services

Name	Description	Comments
rpc-mountd	Network File Server (NFS) mount daemon; for details, see the UNIX man page for **rpc.mountd(8)**.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050).
rpc-nfsprog	Used as part of NFS. For details, see RFC 1094. See also RFC1813 for NFS v3.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050).
rpc-nisplus	Network Information Service Plus (NIS+), designed to replace NIS; it is a default naming service for Sun Solaris and is not related to the old NIS. No protocol information is available.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050).
rpc-nlockmgr	Network lock manager.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, **rpc-nlockmgr** service can be allowed or blocked based on RPC program 100021.
rpc-pcnfsd	Kernel statistics server. For details, see the UNIX man pages for **rstatd** and **rpc.rstatd**.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, **rpc-rstat** service can be allowed or blocked based on RPC program 150001.
rpc-rwall	Used to write a message to users; for details, see the UNIX man page for **rpc.rwalld**.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, **rpc-rwall** service can be allowed or blocked based on RPC program 150008.
rpc-ypbind	NIS binding process. For details, see the UNIX man page for **ypbind**.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, **rpc-ypbind** service can be allowed or blocked based on RPC program 100007.
rpc-yppasswd	NIS password server. For details, see the UNIX man page for **yppasswd**.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, **rpc-yppasswd** service can be allowed or blocked based on RPC program 100009.
rpc-ypserv	NIS server. For details, see the UNIX man page for **ypserv**.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, **rpc-ypserv** service can be allowed or blocked based on RPC program 100004.
rpc-ypupdated	Network updating tool.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, **rpc-ypupdated** service can be allowed or blocked based on RPC program 100028.
rpc-ypxfrd	NIS map transfer server. For details, see the UNIX man page for **rpc.ypxfrd**.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, **rpc-ypxfrd** service can be allowed or blocked based on RPC program 100069.

Support for stateful firewall and NAT services that use port mapping requires that you configure the RPC portmap ALG on TCP/UDP destination port 111 and the RPC ALG for both TCP and UDP. You can specify one or more **rpc-program-number** values to further restrict allowed RPC protocols.

RTSP

The Real-Time Streaming Protocol (RTSP) controls the delivery of data with real-time properties such as audio and video. The streams controlled by RTSP can use RTP, but it is not required. Media can be transmitted on the same RTSP control stream. This is an HTTP-like text-based protocol, but both client and server maintain session information. A session is established using the SETUP message and terminated using the TEARDOWN message. The transport (the media protocol, address, and port numbers) is negotiated in the setup and the setup-response.

NOTE: **RTSP interleaved mode is not supported.**

Support for stateful firewall and NAT services requires that you configure the RTSP ALG for TCP port 554.

The ALG monitors the control connection, opens flows dynamically for media (RTP/RTSP) streams, and performs NAT address and port rewrites.

SIP

The Session Initiation Protocol (SIP) is an application layer protocol that can establish, maintain and terminate media sessions. It is a widely used voice over IP (VoIP) signaling protocol. The SIP ALG monitors SIP traffic and dynamically creates and manages pinholes on the signaling and media paths. The ALG only allows packets with the correct permissions. The SIP ALG also performs the following functions:

- Manages parent-child session relationships.
- Enforces security policies.
- Manages pinholes for VoIP traffic.

Starting with Junos OS Release 11.4, the SIP ALG supports Network Address Translation (NAT) and stateful firewall configuration on JSF. The SIP ALG supports the following features:

- Stateful firewall
- Static source NAT
- Dynamic address only source NAT
- Network Address Port Translation (NAPT)

NOTE: **The SIP ALG does not support destination NAT, class of service (CoS), or multicast.**

At present, the SIP ALG does not support the following features:

- Encryption and authentication of SIP messages
- Transport of SIP messages over TCP

SQLNet

The SQLNet protocol is used by Oracle SQL servers to execute SQL commands from clients, including load balancing and application-specific services.

Support of stateful firewall and NAT services requires that you configure the SQLNet ALG for TCP port 1521.

The ALG monitors the control packets, opens flows dynamically for data traffic, and performs NAT address and port rewrites.

Talk

The Talk protocol is used for interactive communication between two users. The Talk ALG on the caller negotiates with the Talk program on the receiver about the socket that will be used for the data connection. The Talk ALG has the capability to parse Talk packets, perform Network Address Translation (NAT), and open TCP and UDP gates. The payload contains only client address and port information.

UNIX Remote-Shell Services

UNIX remote-shell service is supported. Remote command execution; enables a user on the client system to execute a command on the remote system. The first command from client (**rcmd**) to server (**rshd**) uses well-known TCP port 514. A second TCP connection can be opened at the request of **rcmd**. The client port number for the second connection is sent to the server as an ASCII string.

Support of stateful firewall services requires that you configure the Shell ALG on TCP port 514. NAT remote-shell services require that any dynamic source port assigned be within the port range 512 through 1023. If you configure a NAT pool, this port range is reserved exclusively for remote shell applications. NAPT is not supported for remote-shell.

Verifying the Output of ALG Sessions

This section contains information on configuration of system logs. You can compare the logs from your sessions to check whether the configurations are functioning correctly.

- System Log Messages on page 10

System Log Messages

Enabling system log generation and checking the system log are helpful for analysis of ALG flows. This section contains the following:

- System Log Configuration on page 11
- System Log Output on page 11

System Log Configuration

You can configure the enabling of system log messages at a number of different levels in the Junos OS CLI. As shown in the following sample configurations, the choice of level depends on how specific you want the event logging to be and what options you want to include. For details on the configuration options, see the *Junos OS System Basics Configuration Guide* (system level) or the *Junos OS Services Interfaces Configuration Guide* (all other levels).

1. At the topmost global level:

```
user@host# show system syslog
file messages {
    any any;
}
```

2. At the service set level:

```
user@host# show services service-set svc_set
syslog {
    host local {
        services any;
    }
}
stateful-firewall-rules allow_rtsp;
interface-service {
    service-interface ms-3/2/0;
}
```

3. At the service rule level:

```
user@host# show services stateful-firewall rule allow_rtsp
match-direction input-output;
term 0 {
    from {
        applications junos-rtsp;
    }
    then {
        accept;
        syslog;
    }
}
```

System Log Output

System log messages are generated during flow creation, as shown in the following examples:

The following system log message indicates that the ASP matched an accept rule:

```
Oct 25 16:11:37 (FPC Slot 3, PIC Slot 2) {svc_set}[FWNAT]: ASP_SFW_RULE_ACCEPT:
  proto 6 (TCP) application: rtsp, ge-2/0/1.0:1.1.1.2:35595 -> 2.2.2.2:554, Match SFW accept
  rule-set: , rule: allow_rtsp, term: 0
```

For a complete listing of system log messages, see the *Junos OS System Log Messages Reference*.

Junos Default Groups

The Junos OS provides a default, hidden configuration group called **junos-defaults** that is automatically applied to the configuration of your router. The **junos-defaults** group contains preconfigured statements that contain predefined values for common applications. Some of the statements must be referenced to take effect, such as applications like FTP or Telnet. Other statements are applied automatically, such as terminal settings. All of the preconfigured statements begin with the reserved name **junos-**.

NOTE: You can override the Junos default configuration values, but you cannot delete or edit them. If you delete a configuration, the defaults return when a new configuration is added.

You cannot use the **apply-groups** statement with the Junos defaults group.

To view the full set of available preset statements from the Junos default group, issue the **show groups junos-defaults** configuration mode command. The following example displays a partial list of Junos default groups that use application protocols (ALGs).

NOTE: Some ALGs listed under **junos-defaults** may not be supported. For the complete list of supported ALGs, see "ALG Descriptions" on page 4.

```
user@host# show groups junos-defaults
... output for other groups defined at the  [edit groups junos-defaults] hierarchy level ...
applications {
   # File Transfer Protocol
   application junos-ftp {
      application-protocol ftp;
      protocol tcp;
      destination-port 21;
   }
   # Trivial File Transfer Protocol
   application junos-tftp {
      application-protocol tftp;
      protocol udp;
      destination-port 69;
   }
   # RPC port mapper on TCP
   application junos-rpc-portmap-tcp {
      application-protocol rpc-portmap;
      protocol tcp;
      destination-port 111;
   }
   # RPC port mapper on UDP
   application junos-rpc-portmap-udp {
      application-protocol rpc-portmap;
      protocol udp;
      destination-port 111;
```

```
}
# IP Protocol
application junos-ip {
   application-protocol ip;
}
# remote exec
application junos-rexec {
   application-protocol exec;
   protocol tcp;
   destination-port 512;
}
# remote login
application junos-rlogin {
   application-protocol login;
   protocol tcp;
   destination-port 513;
}
# remote shell
application junos-rsh {
   application-protocol shell;
   protocol tcp;
   destination-port 514;
}
# Real-Time Streaming Protocol
application junos-rtsp {
   application-protocol rtsp;
   protocol tcp;
   destination-port 554;
}
# Oracle SQL servers use this protocol to execute SQL commands
# from clients, load balance, use application-specific servers, and so on.
application junos-sqlnet {
   application-protocol sqlnet;
   protocol tcp;
   destination-port 1521;
}
# H.323 Protocol for audio/video conferencing
protocol tcp;
   destination-port 1720;
}
# Internet Inter-ORB Protocol is used for CORBA applications.
# The ORB protocol in Java virtual machine uses port 1975 as a default.
protocol tcp;
   destination-port 1975;
}
# Internet Inter-ORB Protocol is used for CORBA applications.
# ORBIX is a CORBA framework from Iona Technologies that uses
# port 3075 as a default.
protocol tcp;
   destination-port 3075;
}
# This was the original RealPlayer protocol.
# RTSP is more widely used by RealPlayer,
protocol tcp;
   destination-port 7070;
}
```



```
# Traceroute application
application junos-traceroute {
   application-protocol traceroute;
   protocol udp;
   destination-port 33435-33450;
   ttl-threshold 30;
}
# Traceroute application that stops at device supporting firewall
# (packets with ttl > 1 will be discarded).
application junos-traceroute-ttl-1 {
   application-protocol traceroute;
   protocol udp;
   destination-port 33435-33450;
   ttl-threshold 1;
}
# The full range of known RPC programs using UDP.
# Specific program numbers are assigned to certain applications.
application junos-rpc-services-udp {
   application-protocol rpc;
   protocol udp;
   rpc-program-number 100001-400000;
}
# The full range of known RPC programs using TCP.
# Specific program numbers are assigned to certain applications.
application junos-rpc-services-tcp {
   application-protocol rpc;
   protocol tcp;
   rpc-program-number 100001-400000;
}
# All ICMP traffic
# This can be made more restrictive by specifying ICMP type and code.
application junos-icmp-all {
   application-protocol icmp;
}
# ICMP ping; the echo reply is allowed upon return.
application junos-icmp-ping {
   application-protocol icmp;
   icmp-type echo-request;
}
# Protocol used by Windows Media Server and Windows Media Player
application junos-netshow {
   application-protocol netshow;
   protocol tcp;
   destination-port 1755;
}
# NetBIOS, the networking protocol used on Windows networks;
# includes name service port, both UDP and TCP.
application junos-netbios-name-udp {
   application-protocol netbios;
   protocol udp;
   destination-port 137;
}
application junos-netbios-name-tcp {
   protocol tcp;
   destination-port 137;
}
```

```
# NetBIOS, the networking protocol used on Windows networks;
# includes datagram service port.
application junos-netbios-datagram {
  application-protocol netbios;
  protocol udp;
  destination-port 138;
}
# NetBIOS, the networking protocol used on Windows networks;
# includes session service port.
application junos-netbios-session {
  protocol tcp;
  destination-port 139;
}
# DCE-RPC port mapper on TCP
application junos-dce-rpc-portmap {
  application-protocol dce-rpc-portmap;
  protocol tcp;
  destination-port 135;
}
# MS Exchange requires these three UUID values.
application junos-dcerpc-endpoint-mapper-service {
  application-protocol dce-rpc;
  protocol tcp;
  uuid e1af8308-5d1f-11c9-91a4-08002b14a0fa;
}
application junos-ssh {
  protocol tcp;
  destination-port 22;
}
application junos-telnet {
  protocol tcp;
  destination-port 23;
}
application junos-smtp {
  protocol tcp;
  destination-port 25;
}
application junos-dns-udp {
  protocol udp;
  destination-port 53;
}
application junos-dns-tcp {
  protocol tcp;
  destination-port 53;
}
application junos-tacacs {
  protocol tcp;
  destination-port 49;
}
# TACACS Database Service
application junos-tacacs-ds {
  protocol tcp;
  destination-port 65;
}
application junos-dhcp-client {
  protocol udp;
```

```
    destination-port 68;
}
application junos-dhcp-server {
    protocol udp;
    destination-port 67;
}
application junos-bootpc {
    protocol udp;
    destination-port 68;
}
application junos-bootps {
    protocol udp;
    destination-port 67;
}
application junos-http {
    protocol tcp;
    destination-port 80;
}
application junos-https {
    protocol tcp;
    destination-port 443;
}
# " junos-algs-outbound" defines a set of all applications
# requiring an ALG. Useful for defining a rule for an untrusted
# network to allow trusted network users to use all the
# Junos-supported ALGs initiated from the trusted network.
application-set junos-algs-outbound {
    application junos-ftp;
    application junos-tftp;
    application junos-rpc-portmap-tcp;
    application junos-rpc-portmap-udp;
    application junos-snmp-get;
    application junos-snmp-get-next;
    application junos-snmp-response;
    application junos-snmp-trap;
    application junos-rexec;
    application junos-rlogin;
    application junos-rsh;
    application junos-rtsp;
    application junos-sqlnet;
    application junos-traceroute;
    application junos-rpc-services-udp;
    application junos-rpc-services-tcp;
    application junos-icmp-all;
    application junos-netshow;
    application junos-netbios-name-udp;
    application junos-netbios-datagram;
    application junos-dce-rpc-portmap;
    application junos-dcerpc-msexchange-directory-rfr;
    application junos-dcerpc-msexchange-information-store;
    application junos-dcerpc-msexchange-directory-nsp;
}
# " junos-management-inbound" represents the group of applications
# that might need access to the trusted network from the untrusted
# network for management purposes.
# The set is intended for a UI to display management choices.
```

```
    # NOTE: It is not recommended that you use the entire set directly in
    # a firewall rule and open up firewall to all of these
    # applications. Also, you should always specify the source
    # and destination prefixes when using each application.
    application-set junos-management-inbound {
      application junos-snmp-get;
      application junos-snmp-get-next;
      application junos-snmp-response;
      application junos-snmp-trap;
      application junos-ssh;
      application junos-telnet;
      application junos-http;
      application junos-https;
      application junos-xnm-ssl;
      application junos-xnm-clear-text;
      application junos-icmp-ping;
      application junos-traceroute-ttl-1;
    }
  }
  }
  }
```

To reference statements available from the **junos-defaults** group, include the selected **junos-*default-name*** statement at the applicable hierarchy level. To configure application protocols, see "Configuring Application Protocol Properties" on page 21; for details about a specific protocol, see "ALG Descriptions" on page 4.

Examples: Referencing the Preset Statement from the Junos Default Group

The following example is a preset statement from the Junos default groups that is available for FTP in a stateful firewall:

```
[edit]
groups {
  junos-defaults {
    applications {
      application junos-ftp { # Use FTP default configuration
      application-protocol ftp;
      protocol tcp;
      destination-port 21;
    }
  }
}
```

To reference a preset Junos default statement from the Junos default groups, include the **junos-*default-name*** statement at the applicable hierarchy level. For example, to reference the Junos default statement for FTP in a stateful firewall, include the **junos-ftp** statement at the **[edit services stateful-firewall rule *rule-name* term *term-name* from applications]** hierarchy level.

```
[edit]
services {
  stateful-firewall {
    rule my-rule {
      term my-term {
        from {
```

```
            applications junos-ftp; #Reference predefined statement, junos-ftp,
          }
        }
      }
    }
  }
```

The following example shows configuration of the default Junos IP ALG:

```
[edit]
services {
  stateful-firewall {
    rule r1 {
      match-direction input;
      term t1 {
        from {
          applications junos-ip;
        }
        then {
          accept;
          syslog;
        }
      }
    }
  }
}
```

If you configure the IP ALG in the stateful firewall rule, it is matched by any IP traffic, but if there is any other more specific application that matches the same traffic, the IP ALG will not be matched. For example, in the following configuration, both the ICMP ALG and the IP ALG are configured, but traffic is matched for ICMP packets, because it is the more specific match.

```
[edit]
services {
  stateful-firewall {
    rule r1 {
      match-direction input;
      term t1 {
        from {
          applications [ junos-ip junos-icmp-all ];
        }
        then {
          accept;
          syslog;
        }
      }
    }
  }
}
```

PART 2

Configuration

- Configuration Tasks on page 21
- Example on page 39
- Configuration Statements on page 41

CHAPTER 2

Configuration Tasks

- Configuring Application Protocol Properties on page 21
- Configuring Application Sets on page 30
- Configuring Juniper Service Framework – Application-Level Gateways, Rules, and Services Set on page 30

Configuring Application Protocol Properties

To configure application properties, include the **application** statement at the **[edit applications]** hierarchy level:

```
[edit applications]
application application-name {
    application-protocol protocol-name;
    destination-port port-number;
    icmp-code value;
    icmp-type value;
    inactivity-timeout value;
    learn-sip-register;
    protocol type;
    rpc-program-number number;
    sip-call-hold-timeout seconds;
    snmp-command command;
    source-port port-number;
    ttl-threshold value;
    uuid hex-value;
}
```

You can group application objects by configuring the **application-set** statement; for more information, see "Configuring Application Sets" on page 30.

This section includes the following tasks for configuring applications:

- Configuring an Application Protocol on page 22
- Configuring the Network Protocol on page 23
- Configuring the ICMP Code and Type on page 24
- Configuring Source and Destination Ports on page 26
- Configuring the Inactivity Timeout Period on page 29
- Configuring an SNMP Command for Packet Matching on page 29

- Configuring an RPC Program Number on page 29
- Configuring the TTL Threshold on page 29
- Configuring a Universal Unique Identifier on page 30

Configuring an Application Protocol

The **application-protocol** statement allows you to specify which of the supported application protocols (ALGs) to configure and include in an application set for service processing. To configure application protocols, include the **application-protocol** statement at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
application-protocol protocol-name;
```

Table 5 on page 22 shows the list of supported protocols. For more information about specific protocols, see "ALG Descriptions" on page 4.

Table 5: Application Protocols Supported by Services Interfaces

Protocol Name	CLI Value	Comments
Distributed Computing Environment (DCE) remote procedure call (RPC)	**dce-rpc**	Requires the **protocol** statement to have the value **udp** or **tcp**. Requires a **uuid** value. You cannot specify **destination-port** or **source-port** values.
DCE RPC portmap	**dce-rpc-portmap**	Requires the **protocol** statement to have the value **udp** or **tcp**. Requires a **destination-port** value.
Domain Name System (DNS)	**dns**	Requires the **protocol** statement to have the value **udp**. This application protocol closes the DNS flow as soon as the DNS response is received.
FTP	**ftp**	Requires the **protocol** statement to have the value **tcp** or to be unspecified. Requires a **destination-port** value.
PPTP	**pptp**	Requires the **protocol** statement to have the value **tcp** or to be unspecified. Requires a **destination-port** value.
RPC User Datagram Protocol (UDP) or TCP	**rpc**	Requires the **protocol** statement to have the value **udp** or **tcp**. Requires a **rpc-program-number** value. You cannot specify **destination-port** or **source-port** values.
RPC port mapping	**rpc-portmap**	Requires the **protocol** statement to have the value **udp** or **tcp**. Requires a **destination-port** value.
Real-Time Streaming Protocol (RTSP)	**rtsp**	Requires the **protocol** statement to have the value **tcp** or to be unspecified. Requires a **destination-port** value.
SQLNet	**sqlnet**	Requires the **protocol** statement to have the value **tcp** or to be unspecified. Requires a **destination-port** or **source-port** value.
Talk	**talk**	Requires the **protocol** statement to have the value **tcp** or **udp**. Requires a **destination-port** value.

Table 5: Application Protocols Supported by Services Interfaces *(continued)*

Protocol Name	CLI Value	Comments
UNIX Remote Shell	**shell**	Requires the **protocol** statement to have the value **tcp** or to be unspecified. Requires a **destination-port** value.

Configuring the Network Protocol

The **protocol** statement allows you to specify which of the supported network protocols to match in an application definition. To configure network protocols, include the **protocol** statement at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
protocol type;
```

You specify the protocol type as a numeric value; for the more commonly used protocols, text names are also supported in the command-line interface (CLI). Table 6 on page 23 shows the list of the supported protocols.

Table 6: Network Protocols Supported by Services Interfaces

Network Protocol Type	CLI Value	Comments
IP Security (IPsec) authentication header (AH)	**ah**	–
External Gateway Protocol (EGP)	**egp**	–
IPsec Encapsulating Security Payload (ESP)	**esp**	–
Generic routing encapsulation (GR)	**gre**	–
ICMP	**icmp**	Requires an **application-protocol** value of **icmp**.
Internet Group Management Protocol (IGMP)	**igmp**	–
IP in IP	**ipip**	–
OSPF	**ospf**	–
Protocol Independent Multicast (PIM)	**pim**	–
Resource Reservation Protocol (RSVP)	**rsvp**	–
TCP	**tcp**	Requires a **destination-port** or **source-port** value unless you specify **application-protocol rcp** or **dce-rcp**.
UDP	**udp**	Requires a **destination-port** or **source-port** value unless you specify **application-protocol rcp** or **dce-rcp**.

Table 6: Network Protocols Supported by Services Interfaces *(continued)*

Network Protocol Type	CLI Value	Comments
Virtual Router Redundancy Protocol (VRRP)	**vrrp**	–

For a complete list of possible numeric values, see RFC 1700, *Assigned Numbers (for the Internet Protocol Suite)*.

NOTE: IP version 6 (IPv6) is not supported as a network protocol in application definitions.

By default, the twice NAT feature can affect IP, TCP, and UDP headers embedded in the payload of ICMP error messages. You can include the **protocol tcp** and **protocol udp** statements with the application statement for twice NAT configurations.

Configuring the ICMP Code and Type

The ICMP code and type provide additional specification, in conjunction with the network protocol, for packet matching in an application definition. To configure ICMP settings, include the **icmp-code** and **icmp-type** statements at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
icmp-code value;
icmp-type value;
```

You can include only one ICMP code and type value. The **application-protocol** statement must have the value **icmp**. Table 7 on page 25 shows the list of supported ICMP values.

Table 7: ICMP Codes and Types Supported by Services Interfaces

CLI Statement	Description
icmp-code	This value or keyword provides more specific information than **icmp-type**. Because the value's meaning depends upon the associated **icmp-type** value, you must specify **icmp-type** along with **icmp-code**. For more information, see the *Junos OS Policy Framework Configuration Guide*. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed). The keywords are grouped by the ICMP type with which they are associated: parameter-problem: **ip-header-bad** (0), **required-option-missing** (1) redirect: **redirect-for-host** (1), **redirect-for-network** (0), **redirect-for-tos-and-host** (3), **redirect-for-tos-and-net** (2) time-exceeded: **ttl-eq-zero-during-reassembly** (1), **ttl-eq-zero-during-transit** (0) unreachable: **communication-prohibited-by-filtering** (13), **destination-host-prohibited** (10), **destination-host-unknown** (7), **destination-network-prohibited** (9), **destination-network-unknown** (6), **fragmentation-needed** (4), **host-precedence-violation** (14), **host-unreachable** (1), **host-unreachable-for-TOS** (12), **network-unreachable** (0), **network-unreachable-for-TOS** (11), **port-unreachable** (3), **precedence-cutoff-in-effect** (15), **protocol-unreachable** (2), **source-host-isolated** (8), **source-route-failed** (5)
icmp-type	Normally, you specify this match in conjunction with the **protocol** match statement to determine which protocol is being used on the port. For more information, see the *Junos OS Policy Framework Configuration Guide*. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): **echo-reply** (0), **echo-request** (8), **info-reply** (16), **info-request** (15), **mask-request** (17), **mask-reply** (18), **parameter-problem** (12), **redirect** (5), **router-advertisement** (9), **router-solicit** (10), **source-quench** (4), **time-exceeded** (11), **timestamp** (13), **timestamp-reply** (14), or **unreachable** (3).

NOTE: If you configure an interface with an input firewall filter that includes a reject action and with a service set that includes stateful firewall rules, the router executes the input firewall filter before the stateful firewall rules are run on the packet. As a result, when the Packet Forwarding Engine sends an ICMP error message out through the interface, the stateful firewall rules might drop the packet because it was not seen in the input direction.

Possible workarounds are to include a forwarding-table filter to perform the reject action, because this type of filter is executed after the stateful firewall in the input direction, or to include an output service filter to prevent the locally generated ICMP packets from going to the stateful firewall service.

Configuring Source and Destination Ports

The TCP or UDP source and destination port provide additional specification, in conjunction with the network protocol, for packet matching in an application definition. To configure ports, include the **destination-port** and **source-port** statements at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
destination-port port-number;
source-port port-number;
```

You must define one source or destination port. Normally, you specify this match in conjunction with the **protocol** match statement to determine which protocol is being used on the port; for constraints, see Table 5 on page 22.

You can specify either a numeric value or one of the text synonyms listed in Table 8 on page 26.

Table 8: Port Names Supported by Services Interfaces

Port Name	Corresponding Port Number
afs	1483
bgp	179
biff	512
bootpc	68
bootps	67
cmd	514
cvspserver	2401
dhcp	67
domain	53
eklogin	2105
ekshell	2106
exec	512
finger	79
ftp	21
ftp-data	20

Table 8: Port Names Supported by Services Interfaces *(continued)*

Port Name	Corresponding Port Number
http	80
https	443
ident	113
imap	143
kerberos-sec	88
klogin	543
kpasswd	761
krb-prop	754
krbupdate	760
kshell	544
ldap	389
login	513
mobileip-agent	434
mobilip-mn	435
msdp	639
netbios-dgm	138
netbios-ns	137
netbios-ssn	139
nfsd	2049
nntp	119
ntalk	518
ntp	123
pop3	110
pptp	1723

Table 8: Port Names Supported by Services Interfaces *(continued)*

Port Name	Corresponding Port Number
printer	515
radacct	1813
radius	1812
rip	520
rkinit	2108
smtp	25
snmp	161
snmptrap	162
snpp	444
socks	1080
ssh	22
sunrpc	111
syslog	514
tacacs-ds	65
talk	517
telnet	23
tftp	69
timed	525
who	513
xdmcp	177
zephyr-clt	2103
zephyr-hm	2104

For more information about matching criteria, see the *Junos OS Policy Framework Configuration Guide*.

Configuring the Inactivity Timeout Period

You can specify a timeout period for application inactivity. If the software has not detected any activity during the duration, the flow becomes invalid when the timer expires. To configure a timeout period, include the **inactivity-timeout** statement at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
inactivity-timeout seconds;
```

The default value is 30 seconds. The value you configure for an application overrides any global value configured at the **[edit interfaces *interface-name* service-options]** hierarchy level.

Configuring an SNMP Command for Packet Matching

You can specify an SNMP command setting for packet matching. To configure SNMP, include the **snmp-command** statement at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
snmp-command value;
```

The supported values are **get**, **get-next**, **set**, and **trap**. You can configure only one value for matching. The **application-protocol** statement at the **[edit applications application *application-name*]** hierarchy level must have the value **snmp**. For information about specifying the application protocol, see "Configuring an Application Protocol" on page 22.

Configuring an RPC Program Number

You can specify an RPC program number for packet matching. To configure an RPC program number, include the **rpc-program-number** statement at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
rpc-program-number number;
```

The range of values used for DCE or RPC is from 100,000 through 400,000. The **application-protocol** statement at the **[edit applications application *application-name*]** hierarchy level must have the value **rpc**. For information about specifying the application protocol, see "Configuring an Application Protocol" on page 22.

Configuring the TTL Threshold

You can specify a trace route time-to-live (TTL) threshold value, which controls the acceptable level of network penetration for trace routing. To configure a TTL value, include the **ttl-threshold** statement at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
ttl-threshold value;
```

The **application-protocol** statement at the **[edit applications application *application-name*]** hierarchy level must have the value **traceroute**. For information about specifying the application protocol, see "Configuring an Application Protocol" on page 22.

Configuring a Universal Unique Identifier

You can specify a Universal Unique Identifier (UUID) for DCE RPC objects. To configure a UUID value, include the **uuid** statement at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
uuid hex-value;
```

The **uuid** value is in hexadecimal notation. The **application-protocol** statement at the **[edit applications application *application-name*** hierarchy level must have the value **dce-rpc**. For information about specifying the application protocol, see "Configuring an Application Protocol" on page 22. For more information on UUID numbers, see **http://www.opengroup.org/onlinepubs/9629399/apdxa.htm**.

Configuring Application Sets

You can group the applications you have defined into a named object by including the **application-set** statement at the **[edit applications]** hierarchy level with an **application** statement for each application:

```
[edit applications]
  application application-name {
}
```

For an example of a typical application set, see "Examples: Configuring Application Protocols" on page 39.

Configuring Juniper Service Framework – Application-Level Gateways, Rules, and Services Set

ALGs intercept and analyze specified traffic, allocate resources, and define dynamic policies to permit traffic to pass securely through a device. You may use JSF ALGs with the SFW and NAT.

To use JSF to run ALGs, you must configure the jservices-nat, jservices-alg, and jservices-sfw package at the hierarchy level. In addition, you must configure SFW rules and a services set with a Multiservice interface. This section includes the following tasks:

1. Configuring the JSF Application-Level Gateways Package on page 30
2. Configuring Stateful Firewall with ALGs on page 33
3. Configuring Network Address Translation with ALGs on page 34

Configuring the JSF Application-Level Gateways Package

To configure the JSF services:

1. In configuration mode, go to the following hierarchy level:


```
user@host# edit chassis
```

2. In the hierarchy level, configure the FPC and PIC.

```
[edit chassis]
user@host# edit fpc slot pic slot
```

In this example, the FPC is in slot 1 and the PIC is in slot 0:

```
[edit chassis]
user@host# edit fpc 1 pic 0
```

3. Configure the number of cores dedicated to run control functionality.

```
[edit chassis fpc slot pic slot]
user@host#  set adaptive-services service-package extension-provider control-cores
  control-cores
```

In this example, the number of control cores is 1.

```
[edit chassis fpc 1 pic 0]
user@host#  set adaptive-services service-package extension-provider control-cores
  1
```

4. Configure the number of processing cores dedicated to data.

```
[edit chassis fpc slot pic slot]
user@host# set adaptive-services service-package extension-provider data-cores
  data-cores
```

In this example, the number of data cores is 7.

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider data-cores 7
```

5. Configure the size of the object cache in MB. Only values in increments of 128 MB are allowed and the maximum value of object cache can be 1280 MB. On MS-100 the value is 512 MB. To configure the size of the cache:

```
[edit chassis fpc slot pic slot]
user@host# set adaptive-services service-package extension-provider
  object-cache-size object-cache-size
```

In this example, the size of the object cache is 1280 MB.

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider
  object-cache-size 1280
```

6. Configure the size of the policy database in MB.

```
[edit chassis fpc slot pic slot]
user@host# set adaptive-services service-package extension-provider policy-db-size
  policy-db-size
```

In this example, the size of the policy database is 64 MB.

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider policy-db-size
  64
```

7. Configure the package.

```
[edit chassis fpc slot pic slot]
user@host# set adaptive-services service-package extension-provider package
  package
```

In this example, the first package is **jservices-nat**, the second package is **jservices-alg**, and the third package is **jservices-sfw**.

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider package
  jservices-nat
user@host# set adaptive-services service-package extension-provider package
  jservices-alg
user@host# set adaptive-services service-package extension-provider package
  jservices-sfw
```

8. Configure the extension provider system log, to enable PIC system logging to record or view system log messages:

```
[edit chassis fpc slot pic slot]
user@host# set adaptive-services service-package extension-provider syslog syslog
```

In this example **syslog** is set to **daemon any** and **external any**:

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider syslog daemon
  any
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider syslog external
  any
```

9. Verify the configuration.

```
[edit chassis]
user@host# show chassis
fpc 1 {
    pic 0 {
        adaptive-services {
            service-package {
                extension-provider {
                    control-cores 1;
                    data-cores 7;
                    object-cache-size 1280;
                    policy-db-size 64;
                    package jservices-nat;
                    package jservices-alg;
                    package jservices-sfw;
                    syslog {
                        daemon any;
                        external any;
                    }
                }
            }
        }
    }
}
```

10. Verify for ALG errors in the configuration.

```
host@user# run show services alg statistics
Interface name: ms-1/1/0
FTP ALG statistics:
```



```
Packets dropped : 0
ALG parser errors : 0
Packets translated : 0

Interface name: ms-1/1/0
RPC ALG statistics:
Call packet with rpcbind2 : 2
Call packet with rpcbind3 : 0
Call packet with rpcbind4 : 0
Invalid rpcbind call : 0
Reply packet with rpcbind2: 2
Reply packet with rpcbind3: 0
Reply packet with rpcbind4: 0
Invalid rpcbind reply : 0
Copyright © 2011, Juniper Networks, Inc. 7
Packets fragmented : 0
Packets dropped : 0
Packets released : 0

Interface name: ms-0/1/0
RTSP ALG statistics:
Packets exceeded maximum length : 0
Packets dropped by ALG : 0
Number of describe messages received : 8
Number of setup messages received : 30
Number of teardown messages received : 7
```

Configuring Stateful Firewall with ALGs

To configure the stateful firewall rule:

1. In configuration mode, go to the following hierarchy level:

   user@host# edit services

2. Configure the Stateful Firewall rule.

   [edit services]
   user@host# set stateful-firewall rule *rule*

   In this example, the SFW rule is **rule1 match-direction input-output**.

   [edit services]
   user@host# set stateful-firewall rule rule1 match-direction input-output

3. Configure the rule input conditions for a rule to define the stateful firewall term.

   [edit services]
   user@host# set stateful-firewall rule *rule*

   In this example, the rule input conditions are **rule1 term term1 from applications junos-ftp**, **rule1 term term1 from applications junos-sqlnet**, **rule1 term term1 from applications junos-pptp**, **rule1 term term1 from applications junos-talk-udp**, **rule1 term term1 from applications junos-dns-udp**, **rule1 term term1 from applications junos-rtsp**, and **rule1 term term1 from applications junos-sip**.

   [edit services]
   user@host# set stateful-firewall rule rule1 term term1 from applications junos-ftp
   [edit services]
   user@host# set stateful-firewall rule rule1 term term1 from applications junos-sqlnet

```
[edit services]
user@host# set stateful-firewall rule rule1 term term1 from applications junos-pptp
[edit services]
user@host# set stateful-firewall rule rule1 term term1 from applications junos-talk-udp
[edit services]
user@host# set stateful-firewall rule rule1 term term1 from applications junos-dns-udp
[edit services]
user@host# set stateful-firewall rule rule1 term term1 from applications junos-rtsp
[edit services]
user@host# set stateful-firewall rule rule1 term term1 from applications junos-sip
```

4. Configure the rule for the stateful firewall term actions.

```
[edit services]
user@host# set stateful-firewall rule rule
```

In this example, the rule is **rule1 term term1 then accept**.

```
[edit services]
user@host# set stateful-firewall rule rule1 term term1 then accept
```

5. Verify the configuration.

```
[edit services]
stateful-firewall {
    rule rule1 {
        match-direction input-output;
        term term1 {
            from {
               applications [ junos-ftp junos-sqlnet junos-pptp junos-talk-udp
 junos-dns-udp junos-rtsp junos-sip ];
            }
            then {
                accept;
            }
        }
    }
}
```

Configuring Network Address Translation with ALGs

To configure the NAT pool and NAT rule:

1. In configuration mode, go to the following hierarchy level:

```
user@host# edit services
```

2. Configure the NAT pool.

```
[edit services]
user@host# set nat pool pool
```

In this example, the NAT pool is **p1**.

```
[edit services]
user@host# set nat pool p1
```

3. Configure the NAT pool address.

```
[edit services]
user@host# set nat pool p1 address address
```

In this example, the NAT pool address is **20.1.1.10/32**.

```
[edit services]
user@host# set nat pool p1 address 20.1.1.10/32;
```

4. Configure the NAT pool port.

```
[edit services]
user@host# set nat pool p1 port port;
```

In this example, the NAT pool port is **automatic**.

```
[edit services]
user@host# set nat pool p1 port automatic;
```

5. Configure the rule.

```
[edit services]
user@host# set nat rule rule
```

In this example, the rule is **r1**.

```
[edit services]
user@host# set nat rule r1
```

6. Configure the match direction.

```
[edit services]
user@host# set nat rule r1 match-direction match-direction
```

In this example, the match direction is **input**.

```
[edit services]
user@host# set nat rule r1 match-direction input
```

7. Configure the term.

```
[edit services]
user@host# set nat rule r1 term term
```

In this example, the term is **t1**.

```
[edit services]
user@host# set nat rule r1 term t1
```

8. Configure the input conditions for the NAT term.

```
[edit services]
user@host# set nat rule r1 term t1 from from
```

In this example, the input conditions are **applications junos-ftp**, **applications junos-sqlnet**, **applications junos-pptp**, **applications junos-talk-udp**, **applications junos-dns-udp**, **applications junos-rtsp**, and **applications junos-sip**.

```
[edit services]
user@host# set nat rule r1 term t1 from applications junos-ftp
[edit services]
user@host# set nat rule r1 term t1 from applications junos-sqlnet
[edit services]
user@host# set nat rule r1 term t1 from applications junos-pptp
[edit services]
user@host# set nat rule r1 term t1 from applications junos-talk-udp
[edit services]
```

```
user@host# set nat rule r1 term t1 from applications junos-dns-udp
[edit services]
user@host# set nat rule r1 term t1 from applications junos-rtsp
[edit services]
user@host# set nat rule r1 term t1 from applications junos-sip
```

9. Configure the NAT term action.

```
[edit services]
user@host# set nat rule r1 term then then
```

In this example, the term action is **translated**.

```
[edit services]
user@host# set nat rule r1 term t1 then translated
```

10. Configure the properties for translated traffic.

```
[edit services]
user@host# set nat rule r1 term then translated translated
```

In this example, the property for the translated traffic is **source-pool p1**.

```
[edit services]
user@host# set nat rule r1 term t1 then translated source-pool p1
```

11. Configure the properties for translated traffic transaction type.

```
[edit services]
user@host# set nat rule r1 term then translated transaction type transaction type
```

In this example, the property for the translated traffic is **source dynamic**.

```
[edit services]
user@host# set nat rule r1 term t1 then translated translation-type source dynamic
```

12. Verify the configuration.

```
[edit services]
user@host# show
services {
        nat {
            pool p1 {
                address 20.1.1.10/32;
                port automatic
            }
            rule r1 {
                match-direction input;
                term t1 {
                    from {
         applications [ junos-ftp junos-sqlnet junos-pptp
                                        junos-talk-udp junos-dns-udp junos-rtsp
 junos-sip ];
                    }
                    then {
                        translated {
                            source-pool p1;
                            translation-type {
                                source dynamic;
                            }
                        }
                    }
                }
```

```
            }
        }
    }
```

CHAPTER 3

Example

- Examples: Configuring Application Protocols on page 39

Examples: Configuring Application Protocols

The following example shows an application protocol definition describing a special FTP application running on port 78:

```
[edit applications]
application my-ftp-app {
   application-protocol ftp;
   protocol tcp;
   destination-port 78;
   timeout 100; # inactivity timeout for FTP service
}
```

The following example shows a special ICMP protocol (**application-protocol icmp**) of type 8 (ICMP echo):

```
[edit applications]
application icmp-app {
   application-protocol icmp;
   protocol icmp;
   icmp-type icmp-echo;
}
```

The following example shows a possible application set:

```
[edit applications]
application-set basic {
   http;
   ftp;
   telnet;
   nfs;
   icmp;
}
```

The software includes a predefined set of well-known application protocols. The set includes applications for which the TCP and UDP destination ports are already recognized by stateless firewall filters.

CHAPTER 4

Configuration Statements

application

Syntax

```
application application-name {
  application-protocol protocol-name;
  destination-port port-number;
  icmp-code value;
  icmp-type value;
  inactivity-timeout value;
  learn-sip-register;
  protocol type;
  rpc-program-number number;
  sip-call-hold-timeout seconds;
  snmp-command command;
  source-port port-number;
  ttl-threshold value;
  uuid hex-value;
}
```

Hierarchy Level

[edit applications],
[edit applications application-set *application-set-name*]

Release Information

Statement introduced in Junos OS Release 10.4.

Description

Configure properties of an application and whether to include it in an application set.

Options

application-name—Identifier of the application.

The remaining statements are explained separately.

Usage Guidelines

See "Configuring Application Protocol Properties" on page 21.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

application-protocol

Syntax application-protocol *protocol-name*;

Hierarchy Level [edit applications application *application-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Identify the application protocol name. Application protocols are also called application layer gateways (ALGs).

Options ***protocol-name***—Name of the protocol. The following protocols are supported:

- **dce-rpc**
- **dce-rpc-portmap**
- **dns**
- **ftp**
- **pptp**
- **rpc**
- **rpc-portmap**
- **rtsp**
- **shell**
- **sip**
- **sqlnet**
- **talk**

Usage Guidelines See "Configuring Application Protocol Properties" on page 21.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

application-set

Syntax
```
application-set application-set-name {
    application application-name;
}
```

Hierarchy Level [edit applications]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure one or more applications to include in an application set.

Options ***application-set-name***—Identifier of an application set.

Usage Guidelines See "Configuring Application Sets" on page 30.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

applications

Syntax
```
applications { ... }
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 10.4.

Description Define the applications used in services.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

destination-port

Syntax destination-port *port-value*;

Hierarchy Level [edit applications application *application-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) destination port number.

Options ***port-value***—Identifier for the port. For a complete list, see "Configuring Source and Destination Ports" on page 26.

Usage Guidelines See "Configuring Source and Destination Ports" on page 26.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

icmp-code

Syntax icmp-code *value*;

Hierarchy Level [edit applications application *application-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Internet Control Message Protocol (ICMP) code value.

Options ***value***—The ICMP code value. For a complete list, see "Configuring the ICMP Code and Type" on page 24.

Usage Guidelines See "Configuring the ICMP Code and Type" on page 24.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

icmp-type

Syntax icmp-type *value*;

Hierarchy Level [edit applications application *application-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description ICMP packet type value.

Options *value*—The ICMP type value, such as **echo** or **echo-reply**. For a complete list, see "Configuring the ICMP Code and Type" on page 24.

Usage Guidelines See "Configuring the ICMP Code and Type" on page 24.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

inactivity-timeout

Syntax inactivity-timeout *seconds*;

Hierarchy Level [edit applications application *application-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Inactivity timeout period, in seconds.

Options *seconds*—Length of time the application is inactive before it times out.
Default: 30 seconds

Usage Guidelines See "Configuring the Inactivity Timeout Period" on page 29.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

learn-sip-register

Syntax learn-sip-register;

Hierarchy Level [edit applications application *application-name*]

Release Information Statement introduced in Junos OS Release 11.4.

Description Activate SIP register to accept potential incoming SIP calls.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

protocol

Syntax protocol *type*;

Hierarchy Level [edit applications application *application-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Networking protocol type or number.

Options *type*—Networking protocol type. The following text values are supported:

- **ah**
- **egp**
- **esp**
- **gre**
- **icmp**
- **igmp**
- **ipip**
- **ospf**
- **pim**
- **rsvp**
- **tcp**
- **udp**
- **vrrp**

NOTE: IP version 6 (IPv6) is not supported as a network protocol in application definitions.

Usage Guidelines See "Configuring the Network Protocol" on page 23.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

rpc-program-number

Syntax rpc-program-number *number*;

Hierarchy Level [edit applications application *application-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Remote procedure call (RPC) or Distributed Computing Environment (DCE) value.

Options *number*—RPC or DCE program value.
Range: 100,000 through 400,000

Usage Guidelines See "Configuring an RPC Program Number" on page 29.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

sip-call-hold-timeout

Syntax sip-call-hold-timeout *seconds*;

Hierarchy Level [edit applications application *application-name*]

Release Information Statement introduced in Junos OS Release 11.4.

Description Timeout period for SIP calls placed on hold, in seconds.

Options *seconds*—Length of time the application holds a SIP call open before it times out.
Default: 7200 seconds
Range: 0 through 36,000 seconds (10 hours)

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

snmp-command

Syntax snmp-command *command*;

Hierarchy Level [edit applications application *application-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description SNMP command format.

Options ***command***—Supported commands are SNMP **get**, **get-next**, **set**, and **trap**.

Usage Guidelines See "Configuring an SNMP Command for Packet Matching" on page 29.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

source-port (Applications)

Syntax source-port *port-number*;

Hierarchy Level [edit applications application *application-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Source port identifier.

Options ***port-value***—Identifier for the port. For a complete list, see "Configuring Source and Destination Ports" on page 26.

Usage Guidelines See "Configuring Source and Destination Ports" on page 26.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

ttl-threshold

Syntax ttl-threshold *number*;

Hierarchy Level [edit applications application *application-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Specify the traceroute time-to-live (TTL) threshold value. This value sets the acceptable level of network penetration for trace routing.

Options ***number***—TTL threshold value.

Usage Guidelines See "Configuring the TTL Threshold" on page 29.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

uuid

Syntax uuid *hex-value*;

Hierarchy Level [edit applications application *application-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Specify the Universal Unique Identifier (UUID) for DCE RPC objects.

Options ***hex-value***—Hexadecimal value.

Usage Guidelines See "Configuring a Universal Unique Identifier" on page 30.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

PART 3

Administration

- ALG Operational Mode Commands on page 53

CHAPTER 5

ALG Operational Mode Commands

clear services alg statistics

Syntax clear services alg statistics
<application-protocol *protocol*>
<interface *interface-name*>

Release Information Command introduced in Junos OS Release 10.4.

Description Clear ALG statistics.

Options **none**—Clear all statistics.

application-protocol—(Optional) Clear statistics for one of the following application protocols:

- **dce-rpc**—Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—Domain Name System protocol
- **ftp**—File Transfer Protocol
- **pptp**—Point-to-Point Tunneling Protocol
- **rpc**—Remote Procedure Call protocol
- **rpc-portmap**—Remote Procedure Call protocol portmap service
- **rtsp**—Real-Time Streaming Protocol
- **rsh**—Remote Shell
- **sip**—Session Initiation Protocol
- **sql**—SQLNet
- **talk**—Talk Program

interface *interface-name*—(Optional) Clear statistics for a particular interface.

Required Privilege Level clear

List of Sample Output clear services alg statistics on page 54

Output Fields When you enter this command, the ALG statistics are cleared. There is no specific output.

Sample Output

clear services alg statistics

```
user@host> clear services alg statistics
```

show services alg conversations

Syntax show services alg conversations
<brief >
<application-protocol *protocol*>
<interface *interface-name*>

Release Information Command introduced in Junos OS Release 10.4.

Description Display ALG information for JSF.

Options **none**—Display standard information about all JSF ALG sessions.

brief —(Optional) Display the specified level of output.

application-protocol—(Optional) Display information about one of the following application protocols:

- **dce-rpc**—Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—Domain Name System protocol
- **ftp**—File Transfer Protocol
- **pptp**—Point-to-Point Tunneling Protocol
- **rpc**—Remote Procedure Call protocol
- **rpc-portmap**—Remote Procedure Call protocol portmap service
- **rtsp**—Real-Time Streaming Protocol
- **rsh**—Remote Shell
- **sip**—Session Initiation Protocol
- **sql**—SQLNet
- **talk**—Talk Program

interface *interface-name*—(Optional) Display information about a particular interface.

Required Privilege Level view

List of Sample Output
show services alg conversations on page 56
show services alg conversations brief on page 56
show services alg conversations application-protocol on page 57
show services alg conversations interface on page 58

Output Fields Table 9 on page 56 lists the output fields for the **show services alg conversations** command. Output fields are listed in the approximate order in which they appear.

Table 9: show services alg conversations Output Fields

Field Name	Field Description
Interface	Name of the interface.
ALG	Name of the ALG in use.
Number of conversations	Number of ALG conversations open. A conversation is a group of parent and child sessions.
Group ID	Numeric identifier for the session.
Parent session status	Status of the parent session: • **Active** • **Closed**
Parent session ID	Numeric identifier for the parent session.
Protocol	Protocol used for the parent session.
Forward Flow	The source and destination prefixes for forward flow.
Reverse Flow	The source and destination prefixes for reverse flow.
Child session status	Status of the child session: • **Active** • **Closed**
Child session ID	Numeric identifier for the child session.
Protocol	Protocol used for the child session.

Sample Output

show services alg conversations

```
user@host> show services alg conversations
Interface name: ms-2/1/0
ALG : SQLV2 ALG, State : active
Number of conversations: 1
Parent session status: closed
Child session : 1, protocol: TCP
Forward Flow : {10.50.50.2:37244 -> 10.40.40.10:4334}
Reverse Flow : {10.40.40.10:4334 -> 10.11.11.10:37244}
```

show services alg conversations brief

The output for the **show services alg conversations brief** command is identical to that for the **show services alg conversations** command. For sample output, see show services alg conversations on page 56.

show services alg conversations application-protocol

This command has the same output for the rpc, dce-rpc, rpc-portmap and dce-rpc-portmap ALGs.

```
user@router> show services alg conversations application-protocol rpc
Interface name: ms-1/1/0
ALG : SUNRPC ALG, State : active
  Number of conversations: 2
    Parent session status: closed
      Child session : 1, protocol: UDP
        Forward Flow : {192.168.203.198:1019 -> 192.168.203.194:2049}
        Reverse Flow : {192.168.203.194:2049 -> 192.168.203.198:1019}
      Child session : 2, protocol: UDP
        Forward Flow : {192.168.203.198:36595 -> 192.168.203.194:2049}
        Reverse Flow : {192.168.203.194:2049 -> 192.168.203.198:36595}
    Parent session status: closed
      Child session : 1, protocol: UDP
        Forward Flow : {192.168.203.198:954 -> 192.168.203.194:613}
        Reverse Flow : {192.168.203.194:613 -> 192.168.203.198:954}
      Child session : 2, protocol: UDP
        Forward Flow : {192.168.203.198:53836 -> 192.168.203.194:613}
        Reverse Flow : {192.168.203.194:613 -> 192.168.203.198:53836}

user@router> show services alg conversations application-protocol dns
Interface name: ms-1/1/0
ALG : DNS ALG, State : active
  Number of conversations: 1
    Parent session status: closed
      Child session : 1, protocol: UDP
        Forward Flow : {192.168.203.198:1019 -> 192.168.203.194:2049}
        Reverse Flow : {192.168.203.194:2049 -> 192.168.203.198:1019}


user@router> show services alg conversations application-protocol ftp
Interface name: ms-1/1/0
ALG : DNS ALG, State : active
  Number of conversations: 1
    Parent session status: closed
      Child session : 1, protocol: UDP
        Forward Flow : {192.168.203.198:53836 -> 192.168.203.194:613}
        Reverse Flow : {192.168.203.194:613 -> 192.168.203.198:53836}

user@router> show services alg conversations application-protocol pptp
Interface name: ms-2/0/0
ALG : PPTP ALG, State : active
  Number of conversations: 1
    Parent session status: active
    Parent session : 1, protocol : TCP
      Forward Flow : {15.15.15.10:1511 -> 40.40.40.10:1723}
      Reverse Flow : {40.40.40.10:1723 -> 15.15.15.10:1511}
      Child session : 1, protocol: GRE
        Forward Flow : {15.15.15.10:0 -> 40.40.40.10:49913}
        Reverse Flow : {40.40.40.10:49913 -> 15.15.15.10:65001}
      Child session : 2, protocol: GRE
        Forward Flow : {40.40.40.10:0 -> 15.15.15.10:0}
        Reverse Flow : {15.15.15.10:0 -> 40.40.40.10:65000}

user@router> show services alg conversations application-protocol rtsp
Interface name: ms-0/1/0
ALG : RTSP ALG, State : active
  Number of conversations: 1
    Parent session : 1, protocol : TCP
      Forward Flow : {9.0.0.2:3985 -> 3.1.2.1:554}
```

```
      Reverse Flow : {9.1.0.2:554 -> 9.0.0.2:3985}
    Child session : 1, protocol: UDP
      Forward Flow : {9.1.0.2:35859 -> 9.0.0.2:38159}
      Reverse Flow : {9.0.0.2:38159 -> 3.1.2.1:35859}
    Child session : 2, protocol: UDP
      Forward Flow : {9.1.0.2:35859 -> 9.0.0.2:37391}
      Reverse Flow : {9.0.0.2:37391 -> 3.1.2.1:35859}

user@router> show services alg conversations application-protocol rsh
Interface name: ms-0/1/0
ALG : RSH ALG, State : active
  Number of conversations: 1
    Parent session : 1, protocol : TCP
      Forward Flow : {9.0.0.2:3985 -> 3.1.2.1:554}
      Reverse Flow : {9.1.0.2:554 -> 9.0.0.2:3985}
    Child session : 1, protocol: UDP
      Forward Flow : {9.1.0.2:35859 -> 9.0.0.2:38159}
      Reverse Flow : {9.0.0.2:38159 -> 3.1.2.1:35859}

user@router> show services alg conversations application-protocol sip
Interface name: ms-1/1/0
ALG : SIP ALG, State : active
  Number of conversations: 1
    Parent session status: active
    Parent session : 1, protocol : UDP
      Forward Flow : {20.1.1.2:5060 -> 30.1.1.2:5060}
      Reverse Flow : {30.1.1.2:5060 -> 70.1.1.2:5060}
    Child session : 1, protocol: UDP
        Forward Flow : {20.1.1.2:6000 -> 30.1.1.2:12442}
        Reverse Flow : {30.1.1.2:12442 -> 70.1.1.2:6000}

user@router> show services alg conversations application-protocol sql
Interface name: ms-2/0/0
ALG : SQLV2 ALG, State : active
  Number of conversations: 1
    Parent session : 1, protocol : 0
      Forward Flow : {0.0.0.0:0 -> 0.0.0.0:0}
      Reverse Flow : {0.0.0.0:0 -> 0.0.0.0:0}
    Child session : 1, protocol: TCP
      Forward Flow : {50.50.50.2:19099 -> 40.40.40.10:32773}
      Reverse Flow : {40.40.40.10:32773 -> 1.1.1.1:19099}

user@router> show services alg conversations application-protocol talk
Interface name: ms-0/1/0
ALG : TALK ALG, State : active
  Number of conversations: 1
    Parent session : 1, protocol : TCP
      Forward Flow : {9.0.0.2:3985 -> 3.1.2.1:554}
      Reverse Flow : {9.1.0.2:554 -> 9.0.0.2:3985}
    Child session : 1, protocol: UDP
      Forward Flow : {9.1.0.2:35859 -> 9.0.0.2:38159}
      Reverse Flow : {9.0.0.2:38159 -> 3.1.2.1:35859}
```

show services alg conversations interface

```
user@router> show services alg conversations interface ms-1/1/0

ALG : FTP ALG, State : active
Number of conversations: 1
Parent session status: active
Parent session : 1, protocol : TCP
Forward Flow : {10.20.20.10:47164 -> 10.30.30.30:21}
```

show services alg statistics

Syntax show services alg statistics
<application-protocol *protocol*>
<interface *interface-name*>

Release Information Command introduced in Junos OS Release 10.4.

Description Display ALG statistics for JSF.

Options **application-protocol**—(Optional) Display statistics for one of the following application protocols:

- **dce-rpc**—Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—Domain Name System protocol
- **ftp**—File Transfer Protocol
- **pptp**—Point-to-Point Tunneling Protocol
- **rpc**—Remote Procedure Call protocol
- **rpc-portmap**—Remote Procedure Call protocol portmap service
- **rtsp**—Real-Time Streaming Protocol
- **rsh**—Remote Shell
- **sip**—Session Initiation Protocol
- **sql**—SQLNet
- **talk**—Talk Program

interface *interface-name*—(Optional) Display information about a particular interface.

Required Privilege Level view

List of Sample Output show services alg statistics application-protocol on page 65
show services alg statistics interface on page 67

Output Fields Table 10 on page 59 lists the output fields for the **show services alg statistics** command. Output fields are listed in the approximate order in which they appear.

Table 10: show services alg statistics Output Fields

Field Name	Field Description
Interface	Name of the interface.
ALG statistics	Name of the ALG for which the statistics are displayed.

Table 10: show services alg statistics Output Fields *(continued)*

Field Name	Field Description
Packets with wrong header	Number of packets with wrong header.
Non epm 3.0 packets	Number of non epm 3.0 packets.
Packets with type mismatch	Number of packets with type mismatch.
Packets with id mismatch	Number of packets with id mismatch.
Packets with call mismatch	Number of packets with call mismatch.
Packets fragmented	Number of packets fragmented.
Packets queued	Number of packets queued.
Packets dropped	Number of packets dropped.
Packets released	Number of packets released.
Invalid packets received	Number of invalid packets received.
Reply packets received	Number of reply packets received.
Oversized packets received	Number of oversized packets received.
ALG parser errors	Number of parsing failed errors.
Packets translated	Number of packets translated.
PPTP Objects Active	Number of PPTP objects active.
PPTP Objects Total	Number of PPTP objects in total.
PPTP Objects Error	Number of PPTP objects having errors.
PPTP ASL Group Active	Number of PPTP groups active.
PPTP ASL Group Total	Number of PPTP groups in total.

Table 10: show services alg statistics Output Fields *(continued)*

Field Name	Field Description
PPTP ASL Group Error	Number of PPTP groups having errors.
PPTP Packets received	Number of PPTP packets received.
PPTP Packets Discarded	Number of PPTP packets discarded.
PPTP Packets Free	Number of PPTP packets freed.
PPTP OCRQ Received	Number of Outgoing Call Requests received.
PPTP OCRQ Discarded	Number of Outgoing Call Requests discarded.
PPTP OCRP Received	Number of Outgoing Call Packets received.
PPTP OCRP Discarded	Number of Outgoing Call Packets discarded.
PPTP WEN(SLI) Received	Number of WEN (SLI) packets received.
PPTP WEN(SLI) Discarded	Number of WEN (SLI) packets discarded.
PPTP CCRQ-CDSN Received	Number of Call Clear Requests received.
PPTP CDSN Received	Number of Call Disconnection Notifications received.
PPTP CCRQ-CDSN Discarded	Number of Call Clear Requests discarded.
PPTP Session Create	Number of PPTP sessions created.
PPTP Session Destroy	Number of PPTP sessions destroyed.
PPTP Gate Create	Number of PPTP gates created.
PPTP Gate Hit	Number of PPTP gates hit.
PPTP Gate Timeout	Number of PPTP gates timed out.

Table 10: show services alg statistics Output Fields *(continued)*

Field Name	Field Description
PPTP NAT Events	Number of NAT events.
PPTP DO-NAT Total	Number of DO NATs in total.
PPTP DO-NAT Ok	Number of DO NATs okay.
PPTP DO-NAT Pending	Number of DO NATs pending.
PPTP DO-NAT Fail	Number of DO NATs failed.
PPTP DO-RM Total	Number of DO RMs in total.
PPTP DO-RM Ok	Number of DO RMs okay.
PPTP DO-RM Pending	Number of DO RMs pending.
PPTP DO-RM Fail	Number of DO RMs failed.
PPTP NAT-ASYNC Total	Number of NAT-ASYNCs in total.
PPTP NAT-ASYNC Invalid	Number of NAT-ASYNCs invalid.
PPTP NAT-ASYNC Error1	Number of NAT-ASYNCs error1.
PPTP NAT-ASYNC Error2	Number of NAT-ASYNCs error2.
PPTP ASL Hole Ok	Number of ASYNC holes okay.
PPTP ASL Hole Error	Number of ASYNC hole errors.
PPTP ASL First Hit	Number of ASYNC holes first hit.
PPTP ASL Hole Timeout	Number of ASYNC holes timed out.
PPTP ASL Invalid	Number of ASYNC holes invalid.
PPTP NAT Ctx Free	Number of NAT Ctxs free.

Table 10: show services alg statistics Output Fields *(continued)*

Field Name	Field Description
PPTP Create Resource Error	Number of create resource errors.
PPTP set S2C hole error	Number of server-to-client hole errors.
PPTP set C2S hole error	Number of client-to-server hole errors.
PPTP lnbrk error	Number of PPTP lnbrk errors.
PPTP Mpool Create Error	Number of Mpool create errors.
PPTP RM register client Error	Number of client registration errors.
Call packet with rpcbind2	Number of call packets with rpcbind2.
Call packet with rpcbind3	Number of call packets with rpcbind3.
Call packet with rpcbind4	Number of call packets with rpcbind4.
Invalid rpcbind call	Number of invalid rpcbind calls.
Reply packet with rpcbind2	Number of reply packets with rpcbind2.
Reply packet with rpcbind3	Number of reply packets with rpcbind3.
Reply packet with rpcbind4	Number of reply packets with rpcbind4.
Invalid rpcbind reply	Number of invalid rpcbind replies.
Packets exceeded maximum length	Number of packets exceeding maximum length.
Packets dropped by ALG	Number of packets dropped by the ALG.
Number of describe messages received	Number of describe messages received.

Table 10: show services alg statistics Output Fields *(continued)*

Field Name	Field Description
Number of setup messages received	Number of setup messages received.
Number of teardown messages received	Number of teardown messages received.
Total packets dropped	Total number of SIP packets dropped.
Unexpected requests dropped	Number of unexpected requests dropped.
Unexpected responses dropped	Number of unexpected responses dropped.
Packets DSCP marked	Number of Differentiated Services code point (DSCP) packets marked.
Packets DSCP marked error	Number of Differentiated Services code point (DSCP) packets marked as error.
NAT errors	Number of Network Address Translation errors.
RR headers exceeded maximum limits	Number of RR headers exceeded maximum limits.
Contact headers exceeded maximum limits	Number of contact headers exceeded maximum limits.
Invite dropped due to call limit	Number of invites dropped due to call limit.
Messages not processed by sip stack	Number of messages not processed by sip stack.
Unknown packets dropped	Number of unknown packets dropped.
Decoding Errors	Number of decoding errors.
Packets received in out of state	Number of packets received in out of state.
Packets received	Number of packets received.

Table 10: show services alg statistics Output Fields *(continued)*

Field Name	Field Description
Packets freed by ALG	Number of packets freed by ALG.
Gate fail errors	Number of gate fail errors.
Lookup packets	Number of lookup packets.
Announce packets	Number of announce packets.
Delete packets	Number of delete packets.

Sample Output

show services alg statistics application-protocol

While the statistics are the same for dce-rpc and dce-rpc-portmap, both rpc and rpc-portmap have the same output too.

```
user@router> show services alg statistics application-protocol dce-rpc
Interface name: ms-1/1/0
  DCE-RPC ALG statistics:
    Packets with wrong header : 0
    Non epm 3.0 packets       : 0
    Packets with type mismatch: 0
    Packets with id mismatch  : 0
    Packets with call mismatch: 0
    Packets fragmented        : 0
    Packets queued            : 0
    Packets dropped           : 0
    Packets released          : 0
```

```
user@router> show services alg statistics application-protocol dns
Interface name: ms-2/0/0
  DNS ALG statistics:
    Invalid packets received   : 0
    Reply packets received     : 3509
    Oversized packets received : 0
```

```
user@router> show services alg statistics application-protocol ftp
Interface name: ms-1/1/0
FTP ALG statistics:
Packets dropped           : 0
ALG parser errors         : 0
Packets translated        : 0
```

```
user@router> show services alg statistics application-protocol pptp
Interface name: ms-2/0/0
  PPTP ALG statistics:
    PPTP Objects Active  : 1
    PPTP Objects Total   : 1
    PPTP Objects Error   : 0
    PPTP ASL Group Active  : 1
    PPTP ASL Group Total   : 1
    PPTP ASL Group Error   : 0
    PPTP Packets received  : 11
    PPTP Packets Discarded  : 0
```

```
    PPTP Packets Free  : 0
    PPTP OCRQ Received  : 1
    PPTP OCRQ Discarded  : 0
    PPTP OCRP Received  : 1
    PPTP OCRP Discarded  : 0
    PPTP WEN(SLI) Received  : 3
    PPTP WEN(SLI) Discarded  : 0
    PPTP CCRQ-CDSN Received  : 0
    PPTP CDSN Received  : 0
    PPTP CCRQ-CDSN Discarded  : 0
    PPTP Session Create  : 3
    PPTP Session Destroy  : 0
    PPTP Gate Create  : 0
    PPTP Gate Hit  : 2
    PPTP Gate Timeout  : 0
    PPTP NAT Events  : 0
    PPTP DO-NAT Total  : 1
    PPTP DO-NAT Ok  : 1
    PPTP DO-NAT Pending  : 0
    PPTP DO-NAT Fail  : 0
    PPTP DO-RM Total  : 1
    PPTP DO-RM Ok  : 2
    PPTP DO-RM Pending  : 0
    PPTP DO-RM Fail  : 0
    PPTP NAT-ASYNC Total  : 0
    PPTP NAT-ASYNC Invalid  : 0
    PPTP NAT-ASYNC Error1  : 0
    PPTP NAT-ASYNC Error2  : 0
    PPTP ASL Hole Ok  : 2
    PPTP ASL Hole Error  : 0
    PPTP ASL First Hit  : 2
    PPTP ASL Hole Timeout  : 0
    PPTP ASL Invalid  : 0
    PPTP NAT Ctx Free  : 0
    PPTP Create Resource Error  : 0
    PPTP set S2C hole error  : 0
    PPTP set C2S hole error  : 0
    PPTP lnbrk error  : 0
    PPTP Mpool Create Error  : 0
    PPTP RM register client Error  : 0
```

```
user@router> show services alg statistics application-protocol rpc
Interface name: ms-1/1/0
  RPC ALG statistics:
    Call packet with rpcbind2 : 2
    Call packet with rpcbind3 : 0
    Call packet with rpcbind4 : 0
    Invalid rpcbind call      : 0
    Reply packet with rpcbind2: 2
    Reply packet with rpcbind3: 0
    Reply packet with rpcbind4: 0
    Invalid rpcbind reply     : 0
    Packets fragmented        : 0
    Packets dropped           : 0
    Packets released          : 0
```

```
user@router> show services alg statistics application-protocol rtsp
Interface name: ms-0/1/0
  RTSP ALG statistics:
    Packets exceeded maximum length : 0
    Packets dropped by ALG : 0
    Number of describe messages received : 8
```

```
    Number of setup messages received : 30
    Number of teardown messages received : 7
```

```
user@router> show services alg statistics application-protocol rsh
Interface name: ms-2/0/0
  RSH ALG statistics:
    Invalid packets received   : 0
    Packets dropped by ALG   : 0
    ALG parser errors  : 0
    Packets freed by ALG     : 0
```

```
user@router> show services alg statistics application-protocol sip
Interface name: ms-2/0/0
  SIP ALG statistics:
    Total packets dropped  : 0
    Unexpected requests dropped : 0
    Unexpected responses dropped : 0
    Packets DSCP marked  : 0
    Packets DSCP marked error  : 0
    NAT errors : 0
    RR headers exceeded maximum limits : 0
    Contact headers exceeded maximum limits  : 0
    Invite dropped due to call limit : 0
    Messages not processed by sip stack : 0
    Unknown packets dropped  : 0
    Decoding Errors : 0
    Packets received in out of state  : 0
```

```
user@router> show services alg statistics application-protocol sql
Interface name: ms-2/0/0
  SQLNET ALG statistics:
    Packets received  : 5
    ALG parser errors  : 0
    Packets freed by ALG : 0
    Gate fail errors  : 0
```

```
user@router> show services alg statistics application-protocol talk
Interface name: ms-2/0/0
  TALK ALG statistics:
    Lookup packets  : 5
    Announce packets  : 0
    Delete packets : 0
```

show services alg statistics interface

```
user@router> show services alg statistics interface ms-1/1/0
Interface name: ms-1/1/0
FTP ALG statistics:
Packets dropped           : 0
ALG parser errors         : 0
Packets translated        : 0
```

show services sessions

Syntax show services sessions
<brief | extensive | terse>
<application-protocol *protocol*>
<count>
<destination-port *destination-port*>
<destination-prefix *destination-prefix*>
<interface *interface-name*>
<limit *number*>
<protocol *protocol*>
<service-set *service-set*>
<source-port *source-port*>
<source-prefix *source-prefix*>

Release Information Command introduced in Junos OS Release 10.4.

Description Display session information.

Options **none**—Display standard information about all sessions.

brief | extensive | terse—(Optional) Display the specified level of output.

application-protocol—(Optional) Display information about one of the following application protocols:

- **dce-rpc**—Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—Domain Name System protocol
- **ftp**—File Transfer Protocol
- **pptp**—Point-to-Point Tunneling Protocol
- **rpc**—Remote Procedure Call protocol
- **rpc-portmap**—Remote Procedure Call protocol portmap service
- **rtsp**—Real-Time Streaming Protocol
- **rsh**—Remote Shell
- **sip**—Session Initiation Protocol
- **sql**—SQLNet
- **talk**—Talk Program

count—(Optional) Display a count of the matching entries.

destination-port *destination-port*—(Optional) Display information for a particular destination port. The range of values is from 0 to 65535.

destination-prefix *destination-prefix*—(Optional) Display information for a particular destination prefix.

interface *interface-name*—(Optional) Display information about a particular interface. On M Series and T Series routers, ***interface-name*** can be **ms-*fpc/pic/port*** or **rsp*number***. On J Series routers, ***interface-name*** is **ms-*pim*/0/*port***.

limit *number*—(Optional) Maximum number of entries to display.

protocol *protocol*—(Optional) Display information about one of the following IP types:

- ***number***—Numeric protocol value from 0 to 255
- **ah**—IPsec Authentication Header protocol
- **egp**—An exterior gateway protocol
- **esp**—IPsec Encapsulating Security Payload protocol
- **gre**—A generic routing encapsulation protocol
- **icmp**—Internet Control Message Protocol
- **icmp6**—Internet Control Message Protocol version 6
- **igmp**—Internet Group Management Protocol
- **ipip**—IP-within-IP Encapsulation Protocol
- **ospf**—Open Shortest Path First protocol
- **pim**—Protocol Independent Multicast protocol
- **rsvp**—Resource Reservation Protocol
- **sctp**—Stream Control Transmission Protocol
- **tcp**—Transmission Control Protocol
- **udp**—User Datagram Protocol

service-set *service-set*—(Optional) Display information for a particular service set.

source-port *source-port*—(Optional) Display information for a particular source port. The range of values is from 0 to 65535.

source-prefix *source-prefix*—(Optional) Display information for a particular source prefix.

Required Privilege Level view

List of Sample Output

show services sessions on page 71
show services sessions brief on page 71
show services sessions extensive on page 71
show services sessions terse on page 71
show services sessions application-protocol on page 71
show services sessions count on page 73
show services sessions destination port on page 73

show services sessions destination prefix on page 73
show services sessions interface on page 73
show services sessions protocol on page 74
show services sessions service-set on page 74
show services sessions source port on page 74
show services sessions source prefix on page 74

Output Fields Table 11 on page 70 lists the output fields for the **show services sessions** command. Output fields are listed in the approximate order in which they appear.

Table 11: show services sessions Output Fields

Field Name	Field Description
Interface	Name of the interface.
Session ID	Session ID that uniquely identifies the session.
ALG	Name of the application.
Flags	Session flag for the ALG: • **0x1**—Found an existing session. • **0x2**—Reached session or flow limit. • **0x3**—No memory available for new sessions. • **0x4**—No free session ID available.
IP Action	Flag indicating whether IP action has been set for the session..
Offload	Flag indicating whether the session has been offloaded to the Packet Forwarding Engine.
Asymmetric	Flag indicating whether the session is uni-directional.
Service set	Name of a service set. Individual empty service sets are not displayed.
Sessions Count	Number of sessions.
Flow or Flow Prot	Protocol used for this session.
Source	Source prefix of the flow in the format ***source-prefix:port***. For ICMP flows, port information is not displayed.
Dest	Destination prefix of the flow. For ICMP flows, port information is not displayed.
State	Status of the flow: • **Drop**—Drop all packets in the flow without response. • **Forward**—Forward the packet in the flow without looking at it. • **Reject**—Drop all packets in the flow with response. • **Watch**—Inspect packets in the flow. • **Bypass**—Bypass packets in the flow. • **Unknown**—Unknown flow status.

Table 11: show services sessions Output Fields *(continued)*

Field Name	Field Description
Packet Direction	Direction of the flow: ingress **(I)**, egress **(O)** or unknown.
Frm count	Number of frames in the flow.

Sample Output

show services sessions

```
user@host> show services sessions
ms-2/0/0
Session: 293, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     10.10.10.2:43677 ->    10.20.20.1:53    Forward  I        1
UDP    10.20.20.1:53    ->        1.1.1.1:43677 Forward  O        1
Session: 53, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     10.10.10.2:37494 ->    10.20.20.1:53    Forward  I        1
UDP    10.20.20.1:53    ->        10.11.11.11:37494 Forward  O        1
Session: 66, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     10.10.10.2:48161 ->    10.20.20.1:53    Forward  I        1
UDP    10.20.20.1:53    ->        10.11.11.11:48161 Forward  O        1
Session: 17, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     10.10.10.2:38908 ->    10.20.20.1:53    Forward  I        1
UDP    10.20.20.1:53    ->        10.11.11.11:38908 Forward  O        1
Session: 42, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     10.10.10.2:58189 ->    10.20.20.1:53    Forward  I        1
UDP    10.20.20.1:53    ->        10.11.11.11:58189 Forward  O        1
```

show services sessions brief

The output for the **show services flows brief** command is identical to that for the **show services sessions** command. For sample output, see show services sessions on page 71.

show services sessions extensive

```
user@host> show services sessions extensive
ms-0/1/0
Session: 2, ALG: 0, Flags: 0x0080, IP Action: no, Offload: no
NAT PLugin Data:
  NAT Action:   Translation Type - DYNAMIC NAT44
    NAT source         3.1.1.2         ->    10.10.10.127
TCP           3.1.1.2:52145 ->        4.1.1.2:23    Forward  I             22
  Byte count: 1483
  Flow role: Unknown, Timeout: 0
TCP           4.1.1.2:23    ->   10.10.10.127:52145 Forward  O             18
  Byte count: 2712
  Flow role: Unknown, Timeout: 0
```

show services sessions terse

```
user@router> show services sessions terse
ms-1/1/0
Session: 1, ALG: ftp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
TCP          10.2.2.2:52138 ->       10.1.1.2:21    Forward  I             33
TCP          10.1.1.2:21    ->       10.2.2.2:52138 Forward  O             31
```

show services sessions application-protocol

This command has the same output for the rpc, dce-rpc, rpc-portmap and dce-rpc-portmap ALGs.

```
user@router> show services sessions application-protocol dce-rpc
```

```
Interface name: ms-1/1/0
Session: 8, ALG: portmapper, Flags: 0x1800, IP Action: no, Offload: no
UDP    192.168.203.198:1019  ->192.168.203.194:2049  Forward  I              4
UDP    192.168.203.194:2049  ->192.168.203.198:1019  Forward  O              4
Session: 7, ALG: portmapper, Flags: 0x1800, IP Action: no, Offload: no
UDP    192.168.203.198:954   ->192.168.203.194:613   Forward  I              1
UDP    192.168.203.194:613   ->192.168.203.198:954   Forward  O              1
Session: 6, ALG: portmapper, Flags: 0x1800, IP Action: no, Offload: no
UDP    192.168.203.198:53836 ->192.168.203.194:613   Forward  I              1
UDP    192.168.203.194:613   ->192.168.203.198:53836 Forward  O              1
Session: 5, ALG: portmapper, Flags: 0x1000, IP Action: no, Offload: no
UDP    192.168.203.198:59813 ->192.168.203.194:111   Forward  I              1
UDP    192.168.203.194:111   ->192.168.203.198:59813 Forward  O              1
Session: 4, ALG: portmapper, Flags: 0x1800, IP Action: no, Offload: no
UDP    192.168.203.198:36595 ->192.168.203.194:2049  Forward  I              1
UDP    192.168.203.194:2049  ->192.168.203.198:36595 Forward  O              1
Session: 3, ALG: portmapper, Flags: 0x1000, IP Action: no, Offload: no
UDP    192.168.203.198:56050 ->192.168.203.194:111   Forward  I              1
UDP    192.168.203.194:111   ->192.168.203.198:56050 Forward  O              1
```

```
user@router> show services sessions application-protocol dns
Interface name: ms-2/0/0
Session: 293, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     50.50.50.2:43677 ->    60.60.60.10:53    Forward  I        1
UDP    60.60.60.10:53    ->        1.1.1.1:43677 Forward  O        1
Session: 53, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     50.50.50.2:37494 ->    60.60.60.10:53    Forward  I        1
UDP    60.60.60.10:53    ->        1.1.1.1:37494 Forward  O        1
Session: 66, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     50.50.50.2:48161 ->    60.60.60.10:53    Forward  I        1
UDP    60.60.60.10:53    ->        1.1.1.1:48161 Forward  O        1
Session: 17, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     50.50.50.2:38908 ->    60.60.60.10:53    Forward  I        1
UDP    60.60.60.10:53    ->        1.1.1.1:38908 Forward  O        1
Session: 42, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     50.50.50.2:58189 ->    60.60.60.10:53    Forward  I        1
UDP    60.60.60.10:53    ->        1.1.1.1:58189 Forward  O        1
```

```
user@router> show services sessions application-protocol ftp
Interface name: ms-4/1/0
Session: 1, ALG: 1, Flags: 0x0040, IP Action: no, Offload: no
TCP       30.1.1.1:32843 ->       20.1.1.1:21    Forward  I       26
TCP       20.1.1.1:21    ->        1.1.1.0:32843 Forward  O       30
```

```
user@router> show services sessions application-protocol pptp
Interface name: ms-2/0/0
Session: 3, ALG: pptp, Flags: 0x2800, IP Action: no, Offload: no, Asymmetric: no
GRE        40.40.40.10:0     ->    15.15.15.10:0     Forward  O              21
GRE        15.15.15.10:0     ->    40.40.40.10:65000 Forward  I               0
Session: 2, ALG: pptp, Flags: 0x2800, IP Action: no, Offload: no, Asymmetric: no
GRE        15.15.15.10:0     ->    40.40.40.10:49913 Forward  I              88
GRE        40.40.40.10:49913 ->    15.15.15.10:65001 Forward  O               0
Session: 1, ALG: pptp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
TCP        15.15.15.10:1511  ->    40.40.40.10:1723  Forward  I              13
TCP        40.40.40.10:1723  ->    15.15.15.10:1511  Forward  O              12
```

```
user@router> show services sessions application-protocol rtsp
Interface name: ms-0/1/0
Session: 13, ALG: rtsp, Flags: 0x0800, IP Action: no, Offload: no
UDP        9.1.0.2:5004  ->        9.0.0.2:3989  Forward  O      152
UDP        9.0.0.2:3989  ->        3.1.2.1:5004  Forward  I        0
Session: 9, ALG: rtsp, Flags: 0x0800, IP Action: no, Offload: no
```

```
UDP        9.1.0.2:5004  ->        9.0.0.2:3986  Forward  O        3
UDP        9.0.0.2:3986  ->        3.1.2.1:5004  Forward  I        0

user@router> show services sessions application-protocol rsh
Interface name: ms-2/0/0
Session: 3, ALG: 2, Flags: 0x0840, IP Action: no, Offload: no
TCP    60.60.60.10:1023  ->     50.50.50.2:1020  Forward  O        4
TCP     50.50.50.2:1020  ->    60.60.60.10:1023  Forward  I        3
Session: 1, ALG: 2, Flags: 0x0040, IP Action: no, Offload: no
TCP     50.50.50.2:1021  ->    60.60.60.10:514   Forward  I     1331
TCP    60.60.60.10:514   ->     50.50.50.2:1021  Forward  O     2485

user@router> show services sessions application-protocol sip
Interface name: ms-2/0/0
Session: 4, ALG: sip, Flags: 0x0800, IP Action: no, Offload: no
UDP           20.1.1.2:6000  ->       30.1.1.2:12682 Forward  I             246
UDP           30.1.1.2:12682 ->       70.1.1.2:6000  Forward  O               0
Session: 1, ALG: sip, Flags: 0x0000, IP Action: no, Offload: no
UDP           20.1.1.2:5060  ->       30.1.1.2:5060  Forward  I              10
UDP           30.1.1.2:5060  ->       70.1.1.2:5060  Forward  O               9

user@router> show services sessions application-protocol sql
Interface name: ms-2/0/0
Session: 3934, ALG: sqlnet, Flags: 0x0800, IP Action: no, Offload: no
TCP     50.50.50.2:39754 ->    40.40.40.10:1408  Forward  I       26
TCP    40.40.40.10:1408  ->        1.1.1.1:39754 Forward  O       23

user@router> show services sessions application-protocol talk
Interface name: ms-0/2/0
Session: 4, ALG: 65, Flags: 0x0800, IP Action: no, Offload: no
TCP            2.2.2.2:36888 ->        1.1.1.2:33294 Forward  O               4
TCP            1.1.1.2:33294 ->        2.2.2.2:36888 Forward  I               3
Session: 7, ALG: 65, Flags: 0x0800, IP Action: no, Offload: no
UDP            2.2.2.2:1165  ->        1.1.1.2:518   Forward  O               1
UDP            1.1.1.2:518   ->        2.2.2.2:1165  Forward  I               1
Session: 8, ALG: 65, Flags: 0x0000, IP Action: no, Offload: no
UDP            1.1.1.2:1509  ->        2.2.2.2:518   Forward  I               3
UDP            2.2.2.2:518   ->        1.1.1.2:1509  Forward  O               3
Session: 6, ALG: 0, Flags: 0x0000, IP Action: no, Offload: no
UDP            1.1.1.1:123   ->        1.1.1.2:123   Forward  O               4
```

show services sessions count

```
user@host> show services sessions count
Interface   Service set                                        Sessions count
ms-1/1/0    ss                                                              2
```

show services sessions destination port

```
user@router> show services sessions destination-port 21
ms-1/1/0
Session: 1, ALG: ftp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
TCP           10.2.2.2:52138 ->       10.1.1.2:21    Forward  I              25
TCP           10.1.1.2:21    ->       10.2.2.2:52138 Forward  O              24
```

show services sessions destination prefix

```
user@router> show services sessions destination-prefix 10.1.1.2
ms-1/1/0
Session: 1, ALG: ftp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
TCP           10.2.2.2:52138 ->       10.1.1.2:21    Forward  I              25
TCP           10.1.1.2:21    ->       10.2.2.2:52138 Forward  O              24
```

show services sessions interface

```
user@router> show services sessions interface ms-1/1/0
ms-1/1/0
Session: 1, ALG: ftp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
```

```
TCP           10.2.2.2:52138 ->       10.1.1.2:21    Forward  I              30
TCP           10.1.1.2:21    ->       10.2.2.2:52138 Forward  O              29
```

show services sessions protocol

```
user@router> show services sessions protocol tcp
ms-1/1/0
Session: 1, ALG: ftp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
TCP           10.2.2.2:52138 ->       10.1.1.2:21    Forward  I              30
TCP           10.1.1.2:21    ->       10.2.2.2:52138 Forward  O              29
```

show services sessions service-set

```
user@router> show services sessions service-set sample
ms-1/1/0
Session: 1, ALG: ftp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
TCP           10.2.2.2:52138 ->       10.1.1.2:21    Forward  I              33
TCP           10.1.1.2:21    ->       10.2.2.2:52138 Forward  O              31
```

show services sessions source port

```
user@router> show services sessions source-port 21
ms-1/1/0
Session: 1, ALG: ftp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
TCP           10.2.2.2:52138 ->       10.1.1.2:21    Forward  I              33
TCP           10.1.1.2:21    ->       10.2.2.2:52138 Forward  O              31
```

show services sessions source prefix

```
user@router> show services sessions source-prefix 10.2.2.2
ms-1/1/0
Session: 1, ALG: ftp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
TCP           10.2.2.2:52138 ->       10.1.1.2:21    Forward  I              33
TCP           10.1.1.2:21    ->       10.2.2.2:52138 Forward  O              31
```

PART 4

Index

- Index on page 77

Index

Symbols

#, comments in configuration statements....xii
( ), in syntax descriptions....xii
< >, in syntax descriptions....xii
[ ], in configuration statements....xii
{ }, in configuration statements....xii
| (pipe), in syntax descriptions....xii

A

ALGs
  configuring....22
application statement....41
  usage guidelines....21
application-protocol statement....42
  usage guidelines....22
application-set statement....43
  usage guidelines....30
applications
  example configuration....39
applications statement
  applications hierarchy....43

B

braces, in configuration statements....xii
brackets
  angle, in syntax descriptions....xii
  square, in configuration statements....xii

C

clear services alg statistics command....54
comments, in configuration statements....xii
conventions
  text and syntax....xi
curly braces, in configuration statements....xii
customer support....xiii
  contacting JTAC....xiii

D

destination-port statement
  applications....43
  RPM....44
    usage guidelines....26
documentation
  comments on....xiii

F

font conventions....xi

I

icmp-code statement....44
  usage guidelines....24
icmp-type statement....45
  usage guidelines....24
inactivity-timeout statement....45
  usage guidelines....29

L

learn-sip-register statement....45

M

manuals
  comments on....xiii

P

parentheses, in syntax descriptions....xii
protocol statement
  applications....46
    usage guidelines....23

R

rpc-program-number statement....47
  usage guidelines....29

S

show services alg conversations command....55
show services alg statistics command....59
show services sessions command....68
sip-call-hold-timeout statement....47
snmp-command statement....48
  usage guidelines....29
source-port statement
  RPM....48
    usage guidelines....26
support, technical *See* technical support
syntax conventions....xi

T

technical support
    contacting JTAC....xiii
time-to-live threshold....29
ttl-threshold statement....49
    usage guidelines....29

U

Universal Unique Identifier....30
uuid statement....49
    usage guidelines....30