



RSVP Local Policy Support

Feature History

Release	Modification
12.2(13)T	This feature was introduced.

This document describes the Resource Reservation Protocol (RSVP) Local Policy Support feature in Cisco IOS Release 12.2(13)T. It identifies the supported platforms, provides configuration examples, and lists related Cisco IOS command line interface (CLI) commands.

This document includes the following sections:

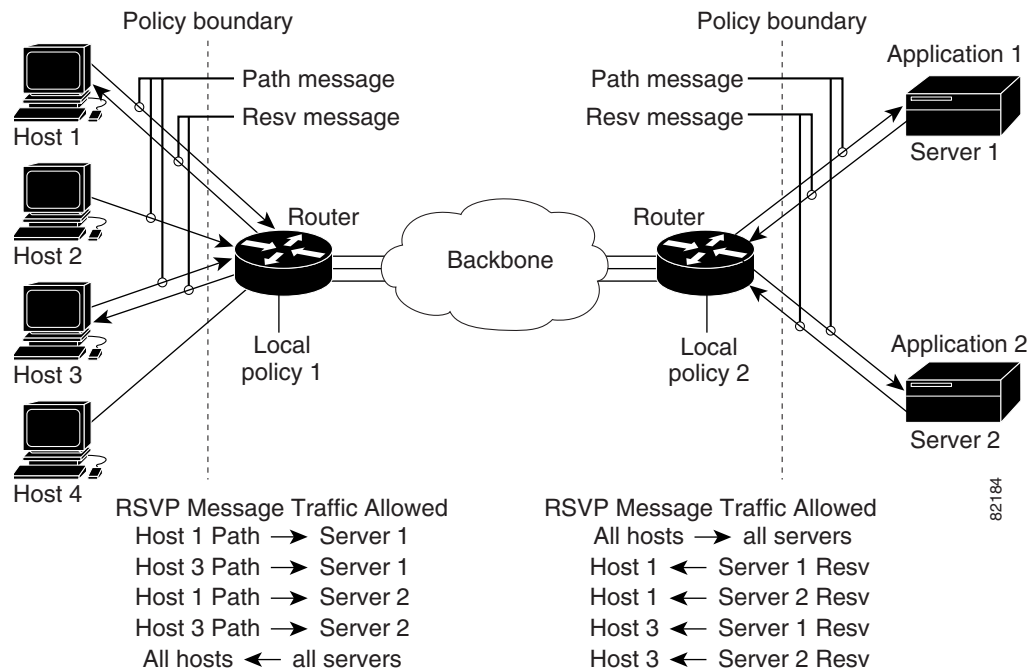
- [Feature Overview, page 1](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 3](#)
- [Prerequisites, page 4](#)
- [Configuration Tasks, page 4](#)
- [Monitoring and Maintaining RSVP Local Policy Support, page 6](#)
- [Configuration Examples, page 6](#)
- [Command Reference, page 7](#)
- [Glossary, page 17](#)

Feature Overview

Network administrators need the ability to control the resources that RSVP reservations are allowed to use. For example, they may want to restrict RSVP reservations to certain subnets or from specific network servers.

The RSVP Local Policy Support feature allows network administrators to create default and access control list (ACL)-based policies. These policies, in turn, control how RSVP filters its signalling messages to allow or deny quality of service (QoS), as shown in [Figure 1](#), to networking applications based on the IP addresses of the requesting hosts.

Figure 1 RSVP Local Policy Configuration



Benefits

RSVP Reservation Control

Network administrators can restrict the source of RSVP reservations to specific endpoints.

RSVP Reservation Preemption

High priority reservations can preempt existing reservations if there is otherwise no bandwidth available for the new, high priority reservation.

Related Features and Technologies

The RSVP Local Policy Support feature is related to QoS features such as signalling, classification, and congestion management. (See the [“Related Documents”](#) section.)

Related Documents

The following documents provide additional information:

- [Cisco IOS Quality of Service Solutions Configuration Guide](#)
- [Cisco IOS Quality of Service Solutions Command Reference](#)

Supported Platforms

For supported platforms in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

RSVP must be configured on two or more routers or on one router and one host within the network before you can use the RSVP Local Policy Support feature.

Configuration Tasks

See the following section for configuration tasks for the RSVP Local Policy Support feature. Each task in the list indicates whether the task is optional or required.

- [Creating an RSVP Local Policy](#) (required)
- [Specifying Command Line Interface \(CLI\) Submodes](#) (required)

Creating an RSVP Local Policy

To create an RSVP local policy, use the following command beginning in global configuration mode:

Command	Purpose
Router(config)# ip rsvp policy local {default acl acl [acl1...acl8]}	Creates a local policy to determine how RSVP resources are used in a network.

Specifying Command Line Interface (CLI) Submodes

To specify CLI submodes, use the following command beginning in local policy mode:

Command	Purpose
Router(config-rsvp-policy-local)# {accept forward} {all path path-error rsvp rsvp-error}	Defines the properties of the default or ACL-based local policy that you are creating.

See the [ip rsvp policy local](#) command for more detailed information on submodes.

Verifying RSVP Local Policy Configuration

To verify RSVP local policy configuration, use this procedure:

- Step 1** Enter the **show ip rsvp policy** command to display policy-related information including local and default policies configured, Common Open Policy Service (COPS) servers configured, and the preemption parameter configured—enabled or disabled.



Note There are no COPS servers configured in the following output.

```
Router# show ip rsvp policy

Local policy:

    A=Accept    F=Forward

    Path:-- Resv:-- PathErr:-- ResvErr:-- ACL:104
    Path:-- Resv:-- PathErr:-- ResvErr:-- ACL:None [Default policy]

COPS:

Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

- Step 2** Enter the **show ip rsvp policy local detail** command to display information about the (selected) local policies currently configured.

```
Router# show ip rsvp policy local detail

Local policy for ACL(s): 104
    Preemption Priority: Start at 0, Hold at 0.
    Local Override: Disabled.

        Accept    Forward
    Path:         No      No
    Resv:         No      No
    PathError:   No      No
    ResvError:   No      No

Default local policy:
    Preemption Priority: Start at 0, Hold at 0.
    Local Override: Disabled.

        Accept    Forward
    Path:         No      No
    Resv:         No      No
    PathError:   No      No
    ResvError:   No      No

Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

Monitoring and Maintaining RSVP Local Policy Support

To monitor and maintain the RSVP Local Policy Support feature, use the following commands in EXEC mode:

Command	Purpose
Router# show ip rsvp policy	Displays either the configured COPS servers or the local policies.
Router# show ip rsvp policy local	Displays selected local policies that have been configured.
Router# show ip rsvp reservation detail	Displays detailed RSVP-related receiver information currently in the database.
Router# show ip rsvp sender detail	Displays detailed RSVP-related sender information currently in the database.

Configuration Examples

This section provides a configuration example for the RSVP Local Policy Support feature.

RSVP Local Policy Support Example

In the following example, any RSVP nodes in the 192.168.101.0 subnet can initiate or respond to reservation requests, but all other nodes can respond only to reservation requests. This means that any 192.168.101.x node can send and receive Path, PathError, Resv, or ResvError messages. All other nodes can send only Resv or ResvError messages.

In the following example, ACL 104 is configured for a local policy:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# access-list 104 permit ip 192.168.101.0 0.0.0.255 any

Router(config)# ip rsvp policy local acl 104

Router(config-rsvp-policy-local)# forward all

Router(config-rsvp-policy-local)# end
```

In the following example, a default local policy is configured:

```
Router(config)# ip rsvp policy local default

Router(config-rsvp-policy-local)# forward resv

Router(config-rsvp-policy-local)# forward resverror

Router(config-rsvp-policy-local)# end
```

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

New Commands

- [ip rsvp policy local](#)
- [ip rsvp policy preempt](#)
- [show ip rsvp policy local](#)

Modified Commands

- [show ip rsvp policy](#)

ip rsvp policy local

To create a local procedure that determines the use of Resource Reservation Protocol (RSVP) resources in a network, use the **ip rsvp policy local** command in global configuration mode. To disable this feature, use the **no** form of this command.

```
ip rsvp policy local { default | acl acl [acl1...acl8]}
```

```
no ip rsvp policy local
```

Syntax Description

default	Used when an RSVP message does not match any access control list (ACL).
acl <i>acl</i> [<i>acl1...acl8</i>]	Used when an ACL is specified. Values for each ACL are 1–199.
Note	You must associate at least one ACL with an ACL-based policy. However, you can associate as many as eight.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp policy local** command to create a local procedure that determines the use of RSVP resources in a network.

There are two types of local policies—one default local policy and one or more ACL-based local policies. The default policy is used when an RSVP message does not match any ACL-based policies. You can use local policies in the following combinations:

- A default policy and no ACL-based policies. All RSVP messages, regardless of reservation (data flow) source or destination, are subject to whatever is defined in this one policy.
- ACL-based policies and no default policy. If an RSVP message does not match the ACLs of any of these local policies, RSVP sees if there are any remote policies in place that allow the router to pass the RSVP message to a COPS server for an accept/reject decision. If there are no COPS servers, the RSVP message is accepted. This final decision can be changed to a reject decision with the **ip rsvp policy default-reject** command.
- A default policy and ACL-based policies. If an RSVP message does not match the ACLs of any of these local policies, RSVP will carry out whatever decisions are in the default local policy.

An ACL-based policy must have at least one ACL associated with it, but it can optionally have up to eight ACLs. The ACLs can be standard or extended IP ACLs. They are matched against source/destination addresses/ports based on RSVP objects inside RSVP signalling messages, not on the IP headers of the RSVP messages.

CLI Submodes

Once you type the **ip rsvp policy local default** or the **ip rsvp policy local acl** command, you enter local policy CLI submode where you define the properties of the default or ACL-based local policy that you are creating.



Note

The local policy that you create automatically rejects all RSVP messages unless you enter a submode command that instructs RSVP on the types of messages to accept.

The submode commands are as follows:

accept—Accepts, but does not forward RSVP messages.

accept {all | path | path-error | resv | resv-error }

- **all**—Accepts all RSVP messages.
- **path**—Accepts incoming Path messages that match the ACL(s) of this policy. If you omit this command, incoming Path messages that match the ACL(s) are rejected and a PathError message is sent in reply. However, the PathError reply is also subject to local policy.
- **path-error**—Accepts incoming PathError messages that match the ACL(s) of this policy. If you omit this command, incoming PathError messages that match the ACL(s) are rejected.
- **resv**—Accepts incoming Resv messages that match the ACL(s) of this policy and performs any required admission control. If you omit this command, incoming Resv messages that match the ACL(s) are rejected and a ResvError message is sent in reply. However, the ResvError reply is also subject to local policy.
- **resv-error**—Accepts incoming ResvError messages that match the ACL(s) of this policy. If you omit this command, the incoming ResvError messages matching the ACL(s) are rejected.
- **default**—Sets a command to its defaults.
- **exit**—Exits local policy configuration mode.
- **forward**—Accepts and forwards RSVP messages.

forward {all | path | path-error | resv | resv-error }

- **all**—Accepts and forwards all RSVP messages.
- **path**—Accepts and forwards Path messages that match the ACL(s) of this policy. If you omit this command, Path messages matching the ACL(s) are not forwarded to the next (downstream) hop.
- **path-error**—Accepts and forwards PathError messages that match the ACL(s) of this policy. If you omit this command, the PathError message matching the ACL(s) are not forwarded to the previous (upstream) hop. You may want to reject outbound PathError messages if you are receiving Path messages from an untrusted node because someone could be trying to port-scan for RSVP. If you reply with a PathError message, then the untrusted node knows you support RSVP and your IP address. Such information could be used to attempt RSVP-based attacks.
- **resv**—Accepts and forwards Resv messages that match the ACL(s) of this policy. If you omit this command, Resv messages matching the ACL(s) are not forwarded to the previous (upstream) hop.
- **resv-error**—Accepts and forwards ResvError messages that match the ACL(s) of this policy. If you omit this command, the ResvError message matching the ACL(s) is not forwarded to the next (downstream) hop. You may want to reject outbound ResvError messages if you are receiving Resv messages from an untrusted node because it could be someone trying to port-scan for RSVP. If you reply with a ResvError message, then the untrusted node knows you support RSVP and your IP address. Such information could be used to attempt RSVP-based attacks.

- **local-override**—Overrides any remote (COPS) policy by enforcing the local policy in effect. Finalizes any decisions by this policy. If local-override is omitted, RSVP holds on to the local policy decision to see if a remote (COPS) policy exists that will make a decision on the RSVP message, and only if there is no remote policy decision will the local policy decision be enforced.
- **no**—Negates a command or sets its defaults.
- **preempt-priority** <start-priority> [<hold-priority>]—Indicates the priorities for resource requests contained in Resv messages that match the ACL(s) of this policy. The range of priority values is 0 to 65,535.

The *start-priority* argument indicates the priority of the reservation when it is initially installed. The *hold-priority* argument indicates the priority of the reservation after it has been installed. When the *start-priority* argument is higher than the *hold-priority* argument, new reservations can steal bandwidth from longer-lived reservations; however, the start and hold priorities are often configured to be the same value. In order for reservations to be preempted in favor of reservations with higher priorities, there must be no RSVP bandwidth remaining on the interface the Resv message was received on, and a global **ip rsvp policy preempt** command must be issued. RSVP will preempt the first so many lower-priority reservations whose combined bandwidth meets (or exceeds) the amount of bandwidth required by a new, incoming, higher-priority reservation.

Label switched path (LSP) sessions are ignored when you select reservations to be preempted, because LSP sessions have their own preemption priority scheme that is configured with the **tunnel mpls traffic-eng priority** command.

In non-LSP sessions, RSVP reservations that are installed on a particular interface are searched in the following order to determine if they are eligible for preemption at a specific preemption priority:

- Destination address
- IP protocol type
- Destination port
- Source address (fixed-filter (FF) style reservations only)
- Source port (FF style reservations only)
- Downstream hop address (for shared media only; for example, Ethernet)

The above fields are searched from lower to higher values. The source address and source port fields are not checked for shared-explicit (SE) or wildcard-filter (WF) style reservations.

**Note**

If you exit local policy submode without entering any submode commands, the policy you have created will reject *all* RSVP messages.

Examples

In the following example, any RSVP nodes in the 192.168.101.0 subnet can initiate or respond to reservation requests, but all other nodes can respond only to reservation requests. This means that any 192.168.101.x node can send and receive Path, PathError, Resv, or ResvError messages. All other nodes can send only Resv or ResvError messages.

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)# access-list 104 permit ip 192.168.101.0 0.0.0.255 any
```

```
Router(config)# ip rsvp policy local acl 104
```

```
Router(config-rsvp-policy-local)# forward all
Router(config-rsvp-policy-local)# exit
Router(config)# ip rsvp policy local default
Router(config-rsvp-policy-local)# forward resv
Router(config-rsvp-policy-local)# forward resverror
Router(config-rsvp-policy-local)# end
```

Related Commands

Command	Description
show ip rsvp policy	Displays the configured local policies.
show ip rsvp policy cops	Displays the policy server address(es), ACL IDs, and current state of the router server connection.
show ip rsvp policy local	Displays selected local policies that have been configured.

ip rsvp policy preempt

To have Resource Reservation Protocol (RSVP) take bandwidth from lower-priority reservations and give it to new, higher-priority reservations, use the **ip rsvp policy preempt** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip rsvp policy preempt

no ip rsvp policy preempt

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled by default.

Command Modes Global configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines Use the **ip rsvp policy preempt** command to enable or disable the preemption parameter for all configured local and remote policies without setting the preemption parameter for each policy individually. This command allows you to give preferential quality of service (QoS) treatment to one group of RSVP hosts or applications over another.

Examples The following example enables preemption:

```
Router(config)# ip rsvp policy preempt
```

The following example disables preemption:

```
Router(config)# no ip rsvp policy preempt
```

Related Commands	Command	Description
	show ip rsvp policy	Displays the configured local policies.

show ip rsvp policy

To display the policies currently configured, use the **show ip rsvp policy** command in EXEC mode.

```
show ip rsvp policy [cops | local [acl] ]
```

Syntax Description		
cops local	(Optional) Displays either the configured Common Open Policy Service (COPS) servers or the local policies.	
<i>acl</i>	(Optional) Displays the access control lists (ACLs) whose sessions are governed by COPS servers or the local policies.	

Defaults This command has no default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced as show ip rsvp policy cops .
	12.2(13)T	This command was modified to include the local keyword.

Usage Guidelines Use the **show ip rsvp policy** command to display current local policies, configured COPS servers, default policies, and the preemption parameter (disabled or enabled).

Examples The following is sample output from the **show ip rsvp policy** command:

```
Router# show ip rsvp policy

Local policy:

    A=Accept    F=Forward

    Path:-- Resv:-- PathErr:-- ResvErr:-- ACL:104
    Path:-- Resv:-- PathErr:-- ResvErr:-- ACL:None [Default policy]

COPS:

Generic policy settings:
    Default policy: Accept all
    Preemption:      Disabled
```

[Table 1](#) describes the fields shown in the display.

Table 1 *show ip rsvp policy Command Field Descriptions*

Field	Description
Local policy	The local policy currently configured. A = Accept the message. F = Forward the message. Blank (--) means messages of the specified type are neither accepted or forwarded.
COPS	The Common Open Policy Service (COPS) servers currently in effect.
Generic policy settings	Policy settings that are not specific to COPS or the local policy. Default policy: Accept all means all RSVP messages are accepted and forwarded. Reject all means all RSVP messages are rejected. Preemption: Disabled means that RSVP should not implement any preemption decisions required by a particular local or remote policy. Enabled means that RSVP should implement any preemption decisions required by a particular local or remote policy.

Related Commands

Command	Description
ip rsvp policy local	Creates a local procedure that determines the use of RSVP resources in a network.

show ip rsvp policy local

To display the local policies currently configured, use the **show ip rsvp policy local** command in EXEC mode.

```
show ip rsvp policy local [detail] [default | acl acl]
```

Syntax Description	detail	(Optional) Additional information about the configured local policies including preempt-priority and local-override.
	default	(Optional) Information about the default policy.
	acl <i>acl</i>	(Optional) Used when an ACL is specified. Values are 1–199.

Defaults This command has no default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines Use the **show ip rsvp policy local** command to display information about the (selected) local policies currently configured.

If you use the ACL option, you can specify only one ACL. However, that parameter can be any ACL of any local policy that you have created. If you have multiple local policies with a common ACL, then using the ACL option displays all local policies with that ACL. On the other hand, if you have created local policies each with multiple ACLs, you cannot use the ACL option to show only a specific policy. You must omit the ACL option and show all the local policies.

Examples The following is sample output from the **show ip rsvp policy local detail** command after you enter the **ip rsvp policy local acl 104** command:

```
Router# show ip rsvp policy local detail

Local policy for ACL(s): 104
  Preemption Priority: Start at 0, Hold at 0.
  Local Override: Disabled.

          Accept  Forward
Path:      No      No
Resv:      No      No
PathError: No      No
ResvError: No      No

Default local policy:
  Preemption Priority: Start at 0, Hold at 0.
  Local Override: Disabled.
```

■ **show ip rsvp policy local**

```

                Accept  Forward
Path:          No      No
Resv:          No      No
PathError:    No      No
ResvError:    No      No

```

```

Generic policy settings:
  Default policy: Accept all
  Preemption:     Disabled

```

Table 2 describes the fields shown in the display.

Table 2 *show ip rsvp policy local detail Command Field Descriptions*

Field	Description
Local policy for ACL(s)	The local policy currently configured for a specified ACL.
Preemption Priority	Start at 0, Hold at 0 indicates the priorities for resource requests contained in Resv messages that match the ACL(s) of this policy. Values are 0 to 65,535. Start at 0 indicates the priority of the reservation when it was installed. Hold at 0 indicates the priority of the reservation after it was installed.
Local Override	Overrides any remote (COPS) policy by enforcing the local policy in effect. Disabled = not active; enabled = active.
Path, Resv, PathError, ResvError	Types of RSVP messages being accepted and forwarded. No = message not being accepted or forwarded; yes = message being accepted and forwarded.
Default local policy	The default local policy currently configured.
Preemption Priority	Start at 0, Hold at 0 indicates the priorities for resource requests contained in Resv messages that match the ACL(s) of this policy. Values are 0 to 65,535. Start at 0 indicates the priority of the reservation when it was installed. Hold at 0 indicates the priority of the reservation after it was installed.
Local Override	Overrides any remote (COPS) policy by enforcing the local policy in effect. Disabled = not active; enabled = active.

Related Commands

Command	Description
ip rsvp policy local	Creates a local procedure that determines the use of RSVP resources in a network.

Glossary

access control list—See ACL.

ACL—access control list. An ACL consists of individual filtering rules grouped together in a single list. It is generally used to provide security filtering, though it may be used to provide a generic packet classification facility.

flow—A stream of data traveling between two endpoints across a network (for example, from one LAN station to another). Multiple flows can be transmitted on a single circuit.

latency—The delay between the time a device receives a packet and the time that packet is forwarded out the destination port.

packet—A logical grouping of information that includes a header containing control information and (usually) user data. Packets most often refer to network layer units of data.

policy—Any defined rule that determines the use of resources within the network. A policy can be based on a user, a device, a subnetwork, a network, or an application.

port scanning—The act of systematically checking a computer's ports to find an access point.

Resource Reservation Protocol—See RSVP.

RSVP—Resource Reservation Protocol. A protocol for reserving network resources to provide quality of service guarantees to application flows.

router—A network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

tunnel—A secure communications path between two peers, such as routers.

Voice over IP—See VoIP.

VoIP—Voice over IP. The ability to carry normal telephony-style voice over an IP-based Internet maintaining telephone-like functionality, reliability, and voice quality.

