



Security Threat Response Manager

STRM Application Configuration Guide

Release 2008.3

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-028822-01, Revision 1

Copyright Notice

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense. The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Reorient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Consult the dealer or an experienced radio/TV technician for help. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

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

Configuring DSMs
Release 2008.3

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

January 2009—Revision 1

The information in this document is current as of the date listed in the revision history.

CONTENTS

ABOUT THIS GUIDE

Conventions	1
Technical Documentation	1
Contacting Customer Support	2

1 DEFINING APPLICATION MAPPINGS

About the STRM Applications View	1
Defining Application Mappings	2
Example of a Mapping File	4
Defining Application Signatures	4
About the Application Signatures File	4
Defining New Applications	5
Example of a Signatures.xml File	6

2 DEFAULT APPLICATIONS

3 ICMP TYPE AND CODE IDS

Identifying Default ICMP Types	27
Identifying Default ICMP Codes	28

4 PROTOCOL IDS

5 PORT IDS




ABOUT THIS GUIDE

The *STRM Application Configuration Guide* provides you with information about how to configure the Applications feature. The Applications feature enables STRM to classify applications used in a flow and is useful when you investigate various types of security threats using the Offense Manager, Event Viewer, or the Flow Viewer.

Conventions

The following table lists conventions that are used throughout this guide:

Table 1 Icons

Icon	Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, device, or network.
	Warning	Information that alerts you to potential personal injury.

Technical Documentation

You can access technical documentation, technical notes, and release notes directly from the Juniper Customer Support web site at <https://www.juniper.net/support>. Once you access the Technical support web site, locate the product and software release for which you require documentation.

Your comments are important to us. Please send your e-mail comments about this guide or any of the Juniper Networks documentation to:

techpubs-comments@juniper.net.

Include the following information with your comments:

- Document title
- Page number

**Contacting
Customer Support**

To help you resolve any issues that you may encounter when installing or maintaining STRM, you can contact Customer Support as follows:

- Open a support case using the Case Management link at <http://www.juniper.net/support>
- Call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

1

DEFINING APPLICATION MAPPINGS

By default, STRM classifies many known applications. However, you can also define new or custom application mappings.

To create new or customized application mappings:

- Step 1 Define applications** - Update the Application Views to define new applications in the STRM Administration interface. For more information about updating the Applications Views, see the *STRM Administration Guide*.
- Step 2 Map traffic to the applications** - In [Step 1](#), you specify a name and ID for the application; however, you must also map traffic to the applications. You can map traffic to the applications using one, or both, of the following methods.
 - **Define application mappings** - Update the application mapping file, which maps applications to STRM's Application Views based on IP address and port number. For more information, see [Defining Application Mappings](#).
 - **Define application signatures** - Define application signatures to apply to flows that STRM's default application mapping could not determine the correct application. This method involves creating rules, based on IP address, port, and content, to assign application IDs to flows. For more information, see [Defining Application Signatures](#).
- Step 3 Deploy the changes** - Deploy the changes to other systems in your STRM deployment using the Administration Console. For more information, see the *STRM Administration Guide*.











This chapter provides information about defining application mappings including:

- [About the STRM Applications View](#)
- [Defining Application Mappings](#)
- [Defining Application Signatures](#)

About the STRM Applications View

When STRM detects a flow, it assigns an application ID to the flow. The mappings in the mapping file overrides the assigned values. The application ID assignment is based on the content of the flow, the protocol used for the flow, and the port. The mapping file also maps the application ID to values defined in the Application View of your STRM interface.

The mapping allows STRM to store the classified data in the database and display color-coded data on STRM graphs, based on the defined application ID. The following figure shows an example of the Chat Application View in the STRM interface, which shows the associated ID in the Values column.

Manage Group: Chat				
Name	Value(s)	Weight	Color	Actions
AOL	3001	60	#4F3B4B	 
ICQ	3002	90	#FF0000	 
IRC	5782...	80	#DDBBBB	 
MSN	5847...	60	#0000FF	 
Misc_IM	3005...	60	#FFFF00	 

You can edit the application mapping file to ensure traffic is appropriately classified in the STRM interface. However, STRM also includes default application IDs, which you can view in the Applications View of the STRM interface. For example, in the previous figure, the Chat group includes the default AOL group, which is defined in the default application mapping file to ensure all AOL traffic is assigned a value of 3001. For more information about default values, see [Chapter 2 Default Applications](#).



Note: For more information about enabling or disabling application detection, see the *STRM Administration Guide*.

Defining Application Mappings

Using the application mapping file, you can create user-defined application mappings based on IP address and port number.

To define application mappings:

- Step 1** Using Secure Shell (SSH), log in to STRM.
- Step 2** Open the following file:

```
/store/configservices/staging/globalconfig/user_application_mapping.conf
```



Note: To edit the name of the `user_application_mapping.conf` file, you can edit the `User Application Mapping` parameter in the `Flow Processor` configuration window. For more information, see the *STRM Administration Guide*. If the `user_application_mapping.conf` does not exist in your system, create the file and place the empty file in the following directory:

```
/store/configservices/staging/globalconfig/user_application_mapping.conf
```

- Step 3** Update the file, as necessary.

When updating the file, note the following:

- Each line in the file indicates a mapped application. You can specify multiple mappings (each on a separate line) for the same application.

- You can specify a wildcard character * for any field. Use the wildcard character alone, and not part of a comma-separated list. The wildcard character indicates that the field applies to all flows.
- A flow can be associated with multiple mappings; therefore, a flow is mapped to an application ID based on the mapping order in the file. The first mapping that applies in the file is assigned to the flow.
- When you add new application ID numbers, we recommend that you apply numbers that range between 15,000 to 20,000. Contact Customer Support for further information.
- The format of the entry must resemble the following:

```
<New ID> <Old ID> <Source IP Address>:<Source Port> <Dest IP Address>:<Dest Port> <Name>
```

Where:

- **<New ID>** specifies the application ID you want to assign to the flow. A value of 1 indicates an unknown application. If the ID you want to assign does not exist, you must create the ID using the Application View in the STRM interface. For more information, see the *STRM Administration Guide*.
- **<Old ID>** specifies the default application ID of the flow, as assigned by STRM. A value of * indicates a wildcard character. For more information about default values, see [Chapter 2 Default Applications](#).
- **<Source IP Address>** specifies the source IP address of the flow. This field can contain either a comma-separated list of addresses or (Classless Inter-Domain Routing) CIDR values. A value of * indicates a wildcard character, which means that this field applies to all flows.
- **<Source Port>** specifies the associated port. This field can contain a comma-separated list of values or ranges specified in the format: <lower port number>-<upper port number>. A value of * indicates a wildcard character, which means that this field applies to all flows.
- **<Dest IP Address>** specifies the destination IP address of the flow. This field can contain either a comma-separated list of addresses or CIDR values. A value of * indicates a wildcard character, which means that this field applies to all flows.
- **<Dest Port>** specifies the associated destination port. This field can contain a comma-separated list of values or ranges specified in the format: <lower port number>-<upper port number>. A value of * indicates a wildcard character, which means that this field applies to all flows.
- **<Name>** specifies a name you want to assign to this mapping. This field is optional.

For example, the following example maps all flows that match the IP addresses and ports for which the Flow Collector has assigned to the Old ID of 1010 and assign the new ID of 15000:

```
15000 1010 10.100.100/24,10.100.50.10:* 172.14.33.33:80,443
```

Step 4 Save and exit the file.

Step 5 Log in to STRM.

Step 6 Click **Config** to access the Administration Console.

Step 7 If necessary, edit your Application View.



Note: For information about creating or editing views, see the *STRM Administration Guide*.

Step 8 From the menu, select **Configurations > Deploy configuration changes**.

The Deploy configuration changes window appears:

Step 9 Click **Close**.

You have successfully deployed your changes.

Example of a Mapping File

```
15000 1010 10.100.100/24,10.100.50.10:* 172.14.33.33:80,443
AllowedWebTypeA
15000 1010 10.100.30/24:* 172.14.33.20:80 AllowedWebTypeA
15100 * *:33333
64.35.20/24,64.33/16,64.77.34.12:33333,33350-33400 GameX
15100 1,34803,34809 *:33333 *:33333,33350-33400 GameX
```

Defining Application Signatures

Using the application signatures file, you create IP address, port, and content-based rules to assign application IDs to flows that STRM does not automatically detect.

This section includes:

- [About the Application Signatures File](#)
- [Defining New Applications](#)
- [Example of a Signatures.xml File](#)

About the Application Signatures File

The application signatures file is a definition file distributed to all Flow Collectors by the primary Console. The file includes source and destination ports and ranges.

Characteristics of the application signatures file include:

- Hex content is delimited with the pipe character “|”. For example:
`<dstcontent offset="0" depth="4">|45 54|</dstcontent>` or,
`<dstcontent offset="0" depth="4">GET</dstcontent>`
- A flow can be associated with multiple signatures; therefore, a flow is mapped to an application ID based on the signature order in the file. The first signature that applies in the file is assigned to the flow.
- Port Only definitions allow for a single Application View instead of Ports and Application Views. Port Only definitions extract and read the port number from the TCP header. This saves processing power on large structured separate networks. Port Only application profiles are evaluated after content-based application profiles.



Note: For a list of STRM 6.2 default application identification numbers, see [Chapter 2 Default Applications](#).

Defining New Applications

To define new applications, you must edit the `signatures.xml` file and the Applications View, and then deploy the changes from the Administration Console.



Note: When editing the `signatures.xml` file, the data inserted between the XML tags is case-sensitive. For example, when specifying TCP within the XML tags, you must enter this using all capital letters.

To edit your application signatures file:

Step 10 Using SSH, log in to STRM.

Step 11 Enter the following:

```
cd /store/configservices/staging/globalconfig
```

Step 12 Open the following file:

```
signatures.xml
```

Step 13 Make the necessary changes using the following parameters:

Table 1-1 Application Signatures Default Parameters

Parameter	Description
appid	Specify a unique ID for each application that you wish to define. We recommend that you apply numbers that range between 15,000 to 20,000 for custom applications. Contact Customer Support for further information.
appname	Specify the name of the application. The application name is used in the Flow Viewer and Offense Manager interfaces.
groupname	Specify the group name for the application. Note: This parameter is currently not used with the exception of the automatic generation script.
description	Specify the long description of the application and any required notes for the particular signature.
revision	Specify a revision for version control.
protocol	Specify the protocol. If the same signature is required for more than one protocol, define the second signature.
srcip	Specify the specific source IP address for the signature to execute. Note: Use multiple application identifications if more than one source IP address is required.
srcport	Specify the specific source port for the signature to execute. Note: Use multiple application identifications if more than one source port is required.

Table 1-1 Application Signatures Default Parameters

Parameter	Description
dstip	Specify the specific destination IP address for the signature to execute. Note: Use multiple application identifications if more destination IP addresses are required.
dstport	Specify the specific destination port for the signature to execute. Note: Use multiple application identifications if more than one destination port is required.
commondstport	Specify the destination port most commonly associated with the application.
commonsrcport	Specify the source port most commonly associated with the application.
srccontent offset	Specify the source content and offset value.
dstcontent offset	Specify the destination content and offset value.



Note: When you create a Port Only application profile, you must use `commondstport` or `commonsrcport` fields. The `srcport`, `dstport`, `srccontent`, and `dstcontent` fields are not applicable with Port Only application profiles.

Step 14 Save and exit the file.

Step 15 Log in to STRM.

Step 16 Create, edit, or reconfigure your application changes.



Note: For information about creating or editing views, see the *STRM Administration Guide*.

Step 17 From the menu, select **Configurations > Deploy configuration changes**.

The Deploy configuration changes window appears:

Step 18 Click **Close**.

You have successfully deployed your changes.

Example of a Signatures.xml File

```
<signatures>
<signature>
  <appid>1009</appid>
  <appname>IMAP</appname>
  <groupname>Mail</groupname>
  <colour>#ff0000</colour>
  <description>IMAP traffic</description>
  <revision>1</revision>
  <protocol>TCP</protocol>
</signature>
</signatures>
```

```
<srcip>any</srcip>
<srcport>any</srcport>
<dstip>any</dstip>
<dstport>any</dstport>
<commondstport>143</commondstport>
<srccontent offset="0" depth="128"
ignorecase="true">LOGIN</srccontent>
<dstcontent offset="0" depth="5">* OK</dstcontent>
<weight>30</weight>
</signature>
</signatures>
```

8 DEFINING APPLICATION MAPPINGS

2

DEFAULT APPLICATIONS

STRM includes default application IDs, which you can view in the Applications View of the STRM interface. This chapter provides the default application values as they appear in the Applications View. The default application values apply to all source and destination flows; however, the destination port is specific to the application.

For more information about the Application View, see the *STRM Administration Guide*.

The following table provides the default Application values for STRM:

Table 2-1 Default Applications

Application View Group	Sub-Component	Value	Description
Chat	AOL-ICQ	3001	AOL Instant Messenger (AIM) traffic
Chat	CUSeeMe	60016	CUSeeMe traffic
Chat	Google	3006	Google IM traffic
Chat	ICQ	3002	ICQ traffic
Chat	Jabber	3004	Jabber protocol traffic
Chat	Lotus-IM	60162	Lotus IM traffic
Chat	MSN	3000	MSN traffic
Chat	Misc_IM	3005	Misc IM traffic
Chat	Windows-POPUP	60170	Windows Messenger Service Pop-up
Chat	Yahoo	1033	Yahoo traffic
Chat	iChat	3008	iChat traffic
Chat	IRC	3003	IRC traffic
Chat	IRC	5668	IRC traffic
Chat	IRC	5669	IRC traffic
Chat	IRC	5782	IRC traffic
Chat	MSN	5672	MSN Traffic
Chat	MSN	5685	MSN Traffic

Table 2-1 Default Applications (continued)

Application View Group	Sub-Component	Value	Description
Chat	MSN	5695	MSN Traffic
Chat	MSN	5831	MSN Traffic
Chat	MSN	5832	MSN Traffic
Chat	MSN	5847	MSN Traffic
ClientServer	CVSpsserver	60150	CVS traffic
ClientServer	CVSup	60129	CVS traffic
ClientServer	CitrixIMA	60115	Citrix IMA traffic
ClientServer	FIX	60057	FIX traffic
ClientServer	FoldingAtHome	60121	FoldingAtHome traffic
ClientServer	INFOC-RTMS	60102	RTMS information traffic
ClientServer	INT-1	60111	INT-1 server traffic
ClientServer	MATIP	60101	MATIP traffic
ClientServer	MeetingMaker	60108	Meeting maker traffic
ClientServer	NetIQ	60127	NetIQ traffic
ClientServer	PEPGate	60104	PEPGate traffic
ClientServer	Unisys-TCPA	60105	Unisys TCPA traffic
ContentDelivery	Ariel-419	60166	Ariel content delivery
ContentDelivery	Ariel-422	60167	Ariel content delivery
ContentDelivery	BackWeb	60024	BackWeb traffic
ContentDelivery	Chaincast	60156	Chaincast traffic
ContentDelivery	EntryPoint	60000	EntryPoint traffic
ContentDelivery	Kontiki	60148	Kontiki traffic
ContentDelivery	NewsStand	60146	New strand traffic
ContentDelivery	Webshots	60147	Webshots Desktop traffic
DataTransfer	AFS	60126	AFS file system traffic
DataTransfer	Apple-iTunes	60163	iTunes traffic
DataTransfer	BITS	60178	Background intelligent transfer service (Windows Updates)
DataTransfer	CU-Dev	60070	CU-dev traffic
DataTransfer	DLS	60002	DLS traffic
DataTransfer	FNAonTCP	60069	FNA traffic
DataTransfer	FTP	1002	File Transfer Protocol (FTP) on common port
DataTransfer	MSMQ	34806	MSMQ traffic

Table 2-1 Default Applications (continued)

Application View Group	Sub-Component	Value	Description
DataTransfer	Microsoft-ds	60142	Microsoft directory server traffic
DataTransfer	Misc-Transfer-Ports	21878	Misc common data traffic ports
DataTransfer	NFS	1007	Network File System (NFS) traffic
DataTransfer	NNTPNews	1013	NNTP traffic
DataTransfer	NW5-CMD	60078	Netware traffic
DataTransfer	NW5-NCP	60076	Netware traffic
DataTransfer	NetBIOS-IP	60013	Windows/Netbios networking
DataTransfer	NortonGhost	60194	Norton Ghost traffic
DataTransfer	SHARESUDP	60106	UDP sharing traffic
DataTransfer	SunND	60173	Sun ND traffic
DataTransfer	TFTP	1003	TFTP traffic
DataTransfer	UUCP	60012	UUCP traffic
DataTransfer	WindowsFileSharing	1014	Windows file sharing
DataTransfer	WindowNetworkPorts	51336	NETBIOS. Windows networking
DataTransfer	WindowsNetworkPorts	51337	NETBIOS. Windows networking
DataTransfer	WindowsNetworkPorts	51338	NETBIOS. Windows networking
DataTransfer	WindowsNetworkPorts	51339	NETBIOS. Windows networking
DataTransfer	WindowsNetworkPorts	51340	NETBIOS. Windows networking
DataTransfer	XFER	21984	XFER traffic
DataTransfer	lockd	60068	lockd traffic
DataTransfer	FTP	27719	FTP traffic
DataTransfer	FTP	27720	FTP traffic
DataTransfer	FTP	5787	FTP traffic
DataTransfer	FTP	5788	FTP traffic
DataTransfer	FTP	5789	FTP traffic
DataTransfer	FTP	5820	FTP traffic
DataTransfer	FTP	5821	FTP traffic
DataTransfer	FTP	5833	FTP traffic
DataTransfer	FTP	5844	FTP traffic

Table 2-1 Default Applications (continued)

Application View Group	Sub-Component	Value	Description
DataTransfer	FTP	5845	FTP traffic
DataTransfer	Misc-Transfer-Ports	21879	Miscellaneous data traffic ports
DataTransfer	Misc-Transfer-Ports	21910	Miscellaneous data traffic ports
DataTransfer	Misc-Transfer-Ports	21919	Miscellaneous data traffic ports
DataTransfer	Misc-Transfer-Ports	22012	Miscellaneous data traffic ports
DataTransfer	NNTPNews	51335	NNTP traffic
DataTransfer	TFTP	21930	TFTP traffic
DataTransfer	WindowsFileSharing	1021	Windows file sharing
DataWarehousing	ARCserverBackup	34730	ARC server backup
DataWarehousing	BAAN	60082	BAAN traffic
DataWarehousing	FileMaker	60112	FileMaker traffic
DataWarehousing	Filenet	34800	Filenet traffic
DataWarehousing	GuptaSQLBase	34841	GuptaSQLBase traffic
DataWarehousing	JDENet	60099	JDENet traffic
DataWarehousing	MS-SQL	10002	Database MS SQL Server
DataWarehousing	Misc-DB	37309	Oracle list service
DataWarehousing	Misc-DB	35298	Oracle list service
DataWarehousing	Misc-DB	39044	Oracle list service
DataWarehousing	Misc-DB	39045	Oracle list service
DataWarehousing	Misc-DB	51249	Oracle list service
DataWarehousing	MySQL	37291	MySQL traffic
DataWarehousing	ORA	37302	ORA traffic
DataWarehousing	ORA	37299	ORA traffic
DataWarehousing	Oracle	42069	Oracle traffic
DataWarehousing	Oracle	37289	Oracle traffic
DataWarehousing	Oracle	37290	Oracle traffic
DataWarehousing	Oracle	37394	Oracle traffic
DataWarehousing	Oracle	37401	Oracle traffic
DataWarehousing	Oracle	37512	Oracle traffic
DataWarehousing	Oracle	37751	Oracle traffic
DataWarehousing	Oracle	37762	Oracle traffic
DataWarehousing	Oracle	37870	Oracle traffic

Table 2-1 Default Applications (continued)

Application View Group	Sub-Component	Value	Description
DataWarehousing	Oracle	37871	Oracle traffic
DataWarehousing	Oracle	37914	Oracle traffic
DataWarehousing	Oracle	38292	Oracle traffic
DataWarehousing	Oracle	42060	Oracle traffic
DataWarehousing	OracleClient	60086	OracleClient traffic
DataWarehousing	PostgreSQL	37292	PostgreSQL traffic
DataWarehousing	Progress	60110	Progress traffic
DataWarehousing	SAP	40380	SAP R/3 application server
DataWarehousing	SAP	40456	SAP R/3 application server
DataWarehousing	SAP	40695	SAP R/3 application server
DataWarehousing	SQL-NET	35159	SQL-NET
DataWarehousing	SQL-NET	34923	SQL-NET
DataWarehousing	giop-ssl	39043	giop-ssl traffic
DirectoryServices	CRS	60060	CRS traffic
DirectoryServices	Ident	60059	Ident traffic
DirectoryServices	LDAP	34801	LDAP traffic
DirectoryServices	RRP	60133	RRP traffic
DirectoryServices	SSDP	60158	SSDP traffic
DirectoryServices	WINS	60088	WINS traffic
DirectoryServices	mDNS	60183	mDNS traffic
FilePrint	IPP	60097	IPP traffic
FilePrint	MDQS	60195	MDQS traffic
FilePrint	Printer	60051	Printer traffic
FilePrint	tn3287	60062	tn3287 traffic
FilePrint	tn5250p	60064	tn5250p traffic
Games	AshéronsCall	60122	AshéronsCall traffic
Games	Battle.net	60116	Battle.net traffic
Games	Doom	60039	Doom traffic
Games	Half-Life	60119	Half-life traffic
Games	Kali	60042	Kali traffic
Games	LucasArts	60157	LucasArts traffic
Games	MSN-Zone	60123	MSN-Zone traffic
Games	Mythic	60149	Mythic traffic
Games	Quake	60040	Quake traffic
Games	SonyOnline	60138	SonyOnline traffic

Table 2-1 Default Applications (continued)

Application View Group	Sub-Component	Value	Description
Games	Tribes	60124	Tribes traffic
Games	Unreal	60117	Unreal traffic
Games	YahooGames	60120	YahooGames traffic
Healthcare	DICOM	60143	DICOM traffic
Healthcare	HL7	60154	HL7 traffic
InnerSystem	Flowgen	1023	Flow Collector and Flow Processor traffic
InnerSystem	Common-Ports	51332	Flow Processor
InnerSystem	UpdateDaemon	1024	Update Daemon traffic
InnerSystem	Common-Ports	51333	Common ports traffic
InnerSystem	Common-Ports	51334	Common ports traffic
InternetProtocol	ActiveX	60056	ActiveX traffic
InternetProtocol	IPHeaderCompression	34843	IPHeaderCompression traffic
InternetProtocol	SOAP-HTTP	60179	SOAP-HTTP traffic
Known_to_client_or_server	known	-1	Known traffic
Legacy	AFP	60058	AFT traffic
Legacy	FNA	60008	FNA traffic
Legacy	IPX	34837	IPX traffic
Legacy	LAT	60030	LAT traffic
Legacy	MOP-DL	60130	MOP-DL traffic
Legacy	MOP-RC	60131	MOP-RC traffic
Legacy	NETBEUI	60006	NETBEUI traffic
Legacy	PPP	34846	PPP traffic
Legacy	PPPoE	60137	PPPoE traffic
Legacy	SLP	60077	SLP traffic
Legacy	SNA	60007	SNA traffic
Mail	ESMTP	5673	ESMTP traffic
Mail	Groupwise	60084	Groupwise traffic
Mail	IMAP	1009	IMAP traffic
Mail	IMAP	5689	IMAP traffic
Mail	IMAP	5690	IMAP traffic
Mail	IMAP	5794	IMAP traffic
Mail	IMAP	5808	IMAP traffic
Mail	MSExchange	34817	MSExchange traffic
Mail	MSSQ	60048	MSSQ traffic

Table 2-1 Default Applications (continued)

Application View Group	Sub-Component	Value	Description
Mail	Misc-Mail-Port	27668	Misc-Mail-Port traffic
Mail	Misc-Mail-Port	22079	Misc-Mail-Port traffic
Mail	Misc-Mail-Port	22158	Misc-Mail-Port traffic
Mail	Misc-Mail-Port	22177	Misc-Mail-Port traffic
Mail	Misc-Mail-Port	22178	Misc-Mail-Port traffic
Mail	Misc-Mail-Port	22184	Misc-Mail-Port traffic
Mail	Misc-Mail-Port	22314	Misc-Mail-Port traffic
Mail	Misc-Mail-Port	22550	Misc-Mail-Port traffic
Mail	Misc-Mail-Port	22551	Misc-Mail-Port traffic
Mail	OSI	60071	OSI traffic
Mail	POP	1008	Mail POP3 traffic
Mail	POP	5687	Mail POP3 traffic
Mail	POP-port	22315	POP-port traffic
Mail	SMTP	1004	Mail SMTP request
Mail	SMTP	5686	Mail SMTP request
Mail	SMTP	5688	Mail SMTP request
Mail	SMTP	5691	Mail SMTP request
Mail	SMTP	5812	Mail SMTP request
Mail	SMTP	5850	Mail SMTP request
Mail	SMTP	5851	Mail SMTP request
Mail	SMTP-port	22080	SMTP-port traffic
Mail	biff	60083	biff traffic
Misc	Anet	34812	Anet traffic
Misc	AppleOUI	34819	AppleOUI traffic
Misc	Appletalk-IP	51326	Appletalk-IP traffic
Misc	Appletalk-IP	51324	Appletalk-IP traffic
Misc	Appletalk-IP	51325	Appletalk-IP traffic
Misc	Appletalk-IP	51327	Appletalk-IP traffic
Misc	Appletalk-IP	51328	Appletalk-IP traffic
Misc	Appletalk-IP	51329	Appletalk-IP traffic
Misc	Appletalk-IP	51330	Appletalk-IP traffic
Misc	Appletalk-IP	51331	Appletalk-IP traffic
Misc	Authentication	21122	Authentication traffic
Misc	Authentication	21028	Authentication traffic
Misc	Authentication	21061	Authentication traffic

Table 2-1 Default Applications (continued)

Application View Group	Sub-Component	Value	Description
Misc	Authentication	21140	Authentication traffic
Misc	Authentication	21624	Authentication traffic
Misc	Authentication	51341	Authentication traffic
Misc	Authentication	51342	Authentication traffic
Misc	Authentication	51343	Authentication traffic
Misc	Authentication	51344	Authentication traffic
Misc	Authentication	51345	Authentication traffic
Misc	Authentication	51346	Authentication traffic
Misc	Authentication	51347	Authentication traffic
Misc	Authentication	51348	Authentication traffic
Misc	CHAOSnet	34822	CHAOSnet traffic
Misc	DHCP	21065	DHCP traffic
Misc	DHCP	21064	DHCP traffic
Misc	DNS	1017	DNS traffic
Misc	DNS-Port	21125	DNS-Port traffic
Misc	DNS-Port	21036	DNS-Port traffic
Misc	Daynachip	34815	Daynachip traffic
Misc	GSM	34830	GSM traffic
Misc	GSS-SPNEGO	5861	GSS-SPNEGO traffic
Misc	Hosts2-Ns	36804	Hosts2-Ns traffic
Misc	Hosts2-Ns	34804	Hosts2-Ns traffic
Misc	IPIX	34826	IPIX traffic
Misc	IPv4	34844	IPv4 traffic
Misc	IPv6	34845	IPv6 traffic
Misc	Ingres	34805	Ingres traffic
Misc	JPEG	34840	JPEG traffic
Misc	Kerberos	34810	Kerberos traffic
Misc	LotusNotes	34732	LotusNotes traffic
Misc	ManagementServices	34054	ManagementServices traffic
Misc	ManagementServices	34057	ManagementServices traffic
Misc	ManagementServices	34205	ManagementServices traffic
Misc	ManagementServices	34208	ManagementServices traffic
Misc	ManagementServices	34209	ManagementServices traffic
Misc	ManagementServices	34213	ManagementServices traffic
Misc	ManagementServices	34216	ManagementServices traffic

Table 2-1 Default Applications (continued)

Application View Group	Sub-Component	Value	Description
Misc	ManagementServices	34221	ManagementServices traffic
Misc	ManagementServices	34556	ManagementServices traffic
Misc	ManagementServices	34557	ManagementServices traffic
Misc	ManagementServices	34560	ManagementServices traffic
Misc	ManagementServices	34563	ManagementServices traffic
Misc	ManagementServices	34564	ManagementServices traffic
Misc	ManagementServices	34636	ManagementServices traffic
Misc	ManagementServices	34661	ManagementServices traffic
Misc	ManagementServices	34727	ManagementServices traffic
Misc	ManagementServices	34728	ManagementServices traffic
Misc	ManagementServices	34735	ManagementServices traffic
Misc	Marimba	60015	Marimba traffic
Misc	Misc-Ports	21302	Misc-Ports traffic
Misc	Misc-Ports	20908	Misc-Ports traffic
Misc	Misc-Ports	20909	Misc-Ports traffic
Misc	Misc-Ports	20915	Misc-Ports traffic
Misc	Misc-Ports	20916	Misc-Ports traffic
Misc	Misc-Ports	20996	Misc-Ports traffic
Misc	Misc-Ports	20998	Misc-Ports traffic
Misc	Misc-Ports	21003	Misc-Ports traffic
Misc	Misc-Ports	21007	Misc-Ports traffic
Misc	Misc-Ports	21008	Misc-Ports traffic
Misc	Misc-Ports	21015	Misc-Ports traffic
Misc	Misc-Ports	21016	Misc-Ports traffic
Misc	Misc-Ports	21020	Misc-Ports traffic
Misc	Misc-Ports	21021	Misc-Ports traffic
Misc	Misc-Ports	21035	Misc-Ports traffic
Misc	Misc-Ports	21039	Misc-Ports traffic
Misc	Misc-Ports	21042	Misc-Ports traffic
Misc	Misc-Ports	21043	Misc-Ports traffic
Misc	Misc-Ports	21056	Misc-Ports traffic
Misc	Misc-Ports	21069	Misc-Ports traffic
Misc	Misc-Ports	21070	Misc-Ports traffic
Misc	Misc-Ports	21071	Misc-Ports traffic
Misc	Misc-Ports	21072	Misc-Ports traffic

Table 2-1 Default Applications (continued)

Application View Group	Sub-Component	Value	Description
Misc	Misc-Ports	21073	Misc-Ports traffic
Misc	Misc-Ports	21074	Misc-Ports traffic
Misc	Misc-Ports	21081	Misc-Ports traffic
Misc	Misc-Ports	21109	Misc-Ports traffic
Misc	Misc-Ports	21116	Misc-Ports traffic
Misc	Misc-Ports	21121	Misc-Ports traffic
Misc	Misc-Ports	21130	Misc-Ports traffic
Misc	Misc-Ports	21141	Misc-Ports traffic
Misc	Misc-Ports	21147	Misc-Ports traffic
Misc	Misc-Ports	21148	Misc-Ports traffic
Misc	Misc-Ports	21160	Misc-Ports traffic
Misc	Misc-Ports	21301	Misc-Ports traffic
Misc	Misc-Ports	21303	Misc-Ports traffic
Misc	Misc-Ports	37305	Misc-Ports traffic
Misc	Misc-Ports	39042	Misc-Ports traffic
Misc	Misc-Ports	42372	Misc-Ports traffic
Misc	Misc-Ports	50643	Misc-Ports traffic
Misc	Misc-Ports	50795	Misc-Ports traffic
Misc	MiscApp	1016	MiscApp traffic
Misc	MiscApp	1018	MiscApp traffic
Misc	MiscApp	1019	MiscApp traffic
Misc	MiscApp	1022	MiscApp traffic
Misc	MiscApplication	34847	MiscApplication traffic
Misc	MiscProtocol	34848	MiscProtocol traffic
Misc	NFS	51349	NFS traffic
Misc	NSP	34842	NSP traffic
Misc	NTP	34811	NTP traffic
Misc	Nessus	34731	Nessus traffic
Misc	Network-Config-Ports	21470	Network-Config-Ports traffic
Misc	Network-Config-Ports	5700	Network-Config-Ports traffic
Misc	Network-Config-Ports	20912	Network-Config-Ports traffic
Misc	Network-Config-Ports	20913	Network-Config-Ports traffic
Misc	Network-Config-Ports	21139	Network-Config-Ports traffic
Misc	RPC	21167	RPC traffic
Misc	SNMP-Ports	21299	SNMP-Ports traffic

Table 2-1 Default Applications (continued)

Application View Group	Sub-Component	Value	Description
Misc	SNMP-Ports	21300	SNMP-Ports traffic
Misc	SymantecGhost	34729	Symantec Ghost traffic
Misc	Syslog	1015	Syslog traffic
Misc	Time	21200	Time traffic
Misc	Time	21006	Time traffic
Misc	Unknown_TCP	34803	Unknown TCP traffic
Misc	Unknown_UDP	34809	Unknown UDP traffic
Misc	VMTP	34813	VMTP traffic
Misc	at-nbp	34813	at-nbp traffic
Misc	dsp3270	34816	dsp3270 traffic
Multimedia	Intellex	6000	Intellex traffic
Multimedia	VideoFrame	60091	VideoFrame traffic
Multimedia	WebEx	60139	WebEx traffic
Network Management	CiscoDiscovery	60055	CiscoDiscovery traffic
Network Management	FlowRecords	60176	Flow records traffic
Network Management	ICMP	60009	ICMP traffic
Network Management	IPComp	60161	IPComp traffic
Network Management	NetFlowV5	60175	NetFlow v5 traffic
Network Management	RSVP	60096	RSVP traffic
Network Management	SMS	60087	SMS traffic
Network Management	TimeServer	60125	TimeServer traffic
Network Management	VIPC	34802	VIPC traffic
No_Detect_Attempt	nodetectattempt	0	nodetectattempt traffic
P2P	Aimster	60132	Aimster traffic
P2P	Audiogalaxy	60118	Audiogalaxy traffic
P2P	BitTorrent	2006	BitTorrent traffic
P2P	Blubster	2003	Blubster traffic
P2P	Common-P2P-Port	33954	Common P2P port traffic

Table 2-1 Default Applications (continued)

Application View Group	Sub-Component	Value	Description
P2P	Common-P2P-Port	33955	Common P2P port traffic
P2P	Common-P2P-Port	33956	Common P2P port traffic
P2P	DirectConnect	5863	DirectConnect traffic
P2P	DirectConnect	5864	DirectConnect traffic
P2P	DirectConnect	5865	DirectConnect traffic
P2P	DirectConnect	5866	DirectConnect traffic
P2P	DirectConnect	5867	DirectConnect traffic
P2P	EarthStationV	60182	EarthStationV traffic
P2P	FileRogue	60145	FileRogue traffic
P2P	Filetopia	60168	Filetopia traffic
P2P	Furthurnet	60160	Furthurnet traffic
P2P	GnuCleusLan	2009	GnuCleusLan traffic
P2P	Gnutella	2000	Gnutella traffic
P2P	Groove	60134	Groove traffic
P2P	Hotline	60136	Hotline traffic
P2P	Kazaa	2001	Fastrack (Kazaa) traffic
P2P	LimeWire	2008	LimeWire traffic
P2P	Morpheus	2010	Morpheus traffic
P2P	Napster	2011	Napster traffic
P2P	Napster2	60181	Napster2 traffic
P2P	OpenNap	2007	OpenNap traffic
P2P	PeerEnabler	2204	P2P PeerEnabler traffic
P2P	PeerEnabler	2004	P2P PeerEnabler traffic
P2P	Piolet	2005	Piolet traffic
P2P	ScourExchange	60113	ScourExchange traffic
P2P	Soulseek	60184	Soulseek traffic
P2P	Tripnosis	60135	Tripnosis traffic
P2P	eDonkey	2002	eDonkey traffic
P2P	iMesh	60114	iMesh traffic
RemoteAccess	ATSTCP	60107	ATSTCP traffic
RemoteAccess	Attachmate-GW	60100	Attachmate-GW traffic
RemoteAccess	CORBA	60043	COBRA traffic
RemoteAccess	Citrix	34814	Citrix traffic
RemoteAccess	CitrixICA	5670	Remote Access Citrix ICA Traffic

Table 2-1 Default Applications (continued)

Application View Group	Sub-Component	Value	Description
RemoteAccess	CitrixICA	5671	Remote Access Citrix ICA Traffic
RemoteAccess	GoToMyPC	60164	GoToMyPC traffic
RemoteAccess	JavaRMI	60109	JavaRMI traffic
RemoteAccess	MSTerminalServices	6001	MS terminal services
RemoteAccess	OpenConnect-JCP	60085	OpenConnect-JCP traffic
RemoteAccess	OpenWindows	34807	OpenWindows traffic
RemoteAccess	PCanywhere	20948	PCanywhere application
RemoteAccess	PCanywhere	50528	PCanywhere application
RemoteAccess	Persona	60093	Persona traffic
RemoteAccess	RDP	60052	RDP traffic
RemoteAccess	RemotelyAnywhere	60188	RemotelyAnywhere traffic
RemoteAccess	SMTBF	60103	SMTBF traffic
RemoteAccess	SSH	1005	SSH traffic
RemoteAccess	SSH-Ports	20947	SSH-Ports traffic
RemoteAccess	SSH-Ports	20949	SSH-Ports traffic
RemoteAccess	SSL	60001	SSL traffic
RemoteAccess	SSL-Shell	60092	SSL-Shell traffic
RemoteAccess	SmartSockets	60169	SmartSockets traffic
RemoteAccess	SunRPC	60027	SunRPC traffic
RemoteAccess	Tacacs	34808	Tacacs traffic
RemoteAccess	Telnet	1000	Telnet traffic
RemoteAccess	Telnet-Port	20950	Telnet-Port traffic
RemoteAccess	Timbuktu	60017	Timbuktu traffic
RemoteAccess	VNC	1006	VNC traffic
RemoteAccess	XWindows	60050	XWindows traffic
RemoteAccess	radmin	60177	radmin traffic
RemoteAccess	rexec	60081	rexec traffic
RemoteAccess	rlogin	60089	rlogin traffic
RemoteAccess	rsh	60128	rsh traffic
RemoteAccess	rsynch	60159	rsynch traffic
RemoteAccess	rwho	60090	rwho traffic
RemoteAccess	tn3270	60010	tn3270
RemoteAccess	tn5250	60063	tn5250 traffic
RoutingProtocols	ARP	34820	ARP traffic

Table 2-1 Default Applications (continued)

Application View Group	Sub-Component	Value	Description
RoutingProtocols	AURP	60011	AURP traffic
RoutingProtocols	BGP	60029	BGP traffic
RoutingProtocols	BPDU	34821	BPDU traffic
RoutingProtocols	Banyan-VINES	34838	Banyan-VINES traffic
RoutingProtocols	CBT	60045	CBT traffic
RoutingProtocols	CiscoOUI	34823	CiscoOUI traffic
RoutingProtocols	DRP	60038	DRP traffic
RoutingProtocols	DTP	60192	DTP traffic
RoutingProtocols	EGP	60032	EGP traffic
RoutingProtocols	EIGRP	60065	EIGRP traffic
RoutingProtocols	GatewayRouting	34836	Gateway Routing traffic
RoutingProtocols	IDP	34825	IDP traffic
RoutingProtocols	IGMP	60041	IGMP traffic
RoutingProtocols	IGP	60098	IGP traffic
RoutingProtocols	IanaProtocol-IP	34835	IanaProtocol-IP traffic
RoutingProtocols	OSPF	60031	OSPF traffic
RoutingProtocols	PAgP	60190	PAgP traffic
RoutingProtocols	PIM	60044	PIM traffic
RoutingProtocols	PVSTP	60189	PVSTP traffic
RoutingProtocols	RARP	60047	RARP traffic
RoutingProtocols	RIP	60028	RIP traffic
RoutingProtocols	SpanningTree	60046	Spanning tree traffic
RoutingProtocols	VLAN-Bridge	60191	VLAN-Bridge traffic
RoutingProtocols	VTP	60193	VTP traffic
SecurityProtocols	DPA	60061	DPA traffic
SecurityProtocols	GRE	60033	GRE traffic
SecurityProtocols	IPMobility	60172	IPMobility traffic
SecurityProtocols	IPSec	60037	IPSec traffic
SecurityProtocols	ISAKMP	60080	ISAKMP traffic
SecurityProtocols	L2TP	60026	L2TP traffic
SecurityProtocols	PPTP	60036	PPTP traffic
SecurityProtocols	RC5DES	60067	RC5DES traffic
SecurityProtocols	SOCKS	60079	SOCKS traffic
SecurityProtocols	SWIPE	60171	SWIPE traffic
SecurityProtocols	SoftEther	60186	SoftEther traffic

Table 2-1 Default Applications (continued)

Application View Group	Sub-Component	Value	Description
Streaming	Abacast	60174	Abacast traffic
Streaming	H.261	34829	H.261 traffic
Streaming	H.262	34828	H.262 traffic
Streaming	H.263	34827	H.263 traffic
Streaming	MPEG-Audio	60053	MPEG-Audio traffic
Streaming	MPEG-Video	60054	MPEG-Video traffic
Streaming	MicrosoftMediaServer	4002	Streaming Microsoft Media Server Protocol (MMS)
Streaming	Motion	60185	Motion traffic
Streaming	RTP-Skinny	34834	RTP-Skinny traffic
Streaming	RTSP	5071	RTSP traffic
Streaming	RadioNetscape	60180	RadioNetscape traffic
Streaming	Real	60003	Real traffic
Streaming	ST2	60034	ST2 traffic
Streaming	StreamWorks	60014	StreamWorks traffic
Streaming	StreamingAudio	4000	Shoutcast MP3 stream
Streaming	StreamingAudio	4001	Shoutcast MP3 stream
Streaming	WinMedia	60025	WinMedia traffic
Streaming	WinampStream	60165	WinampStream traffic
Streaming	WindowsMediaPlayer	5005	WindowsMediaPlayer traffic
Streaming	WindowsMediaPlayer	5006	WindowsMediaPlayer traffic
Uncommon Protocol	DEC	34824	DEC traffic
Uncommon Protocol	UncommonProtocol	34850	UncommonProtocol traffic
Unknown_apps	Unknown	1	Unknown traffic
VoIP	CiscoCTI	60144	CiscoCTI traffic
VoIP	Clarent-CC	60075	Clarent-CC traffic
VoIP	Clarent-Complex	60074	Clarent-Complex traffic
VoIP	Clarent-Mgmt	60072	Clarent-Mgmt traffic
VoIP	Clarent-Voice-S	60073	Clarent-Voice-S traffic
VoIP	Dialpad	60140	Dialpad traffic
VoIP	G711	34833	G711 traffic
VoIP	G722	34832	G722 traffic
VoIP	G729	34831	G729 traffic
VoIP	H.323	60018	H.323 traffic

Table 2-1 Default Applications (continued)

Application View Group	Sub-Component	Value	Description
VoIP	I-Phone	60066	I-Phone traffic
VoIP	MCK-Signaling	60094	MCK-Signaling traffic
VoIP	MCK-Voice	60095	MCK-Voice traffic
VoIP	MGCP	60152	MGCP traffic
VoIP	Megaco	60155	Megaco traffic
VoIP	Micom-VIP	60035	Micom-VIP traffic
VoIP	Net2Phone	60153	Net2Phone traffic
VoIP	RTCP-B	60022	RTCP-B traffic
VoIP	RTCP-I	60020	RTCP-I traffic
VoIP	RTP-B	60021	RTP-B traffic
VoIP	RTP-I	60019	RTP-I traffic
VoIP	SIP	60151	SIP traffic
VoIP	Skype	3007	Skype traffic
VoIP	T.120	60023	T.120 traffic
VoIP	VDOPhone	60004	VDOPhone traffic
VoIP	Vonage	60187	Vonage traffic
Web	HTTPImageTransfer	1034	HTTPImage transfer traffic
Web	HTTPWeb	1010	HTTPWeb traffic
Web	HTTPWeb	1012	HTTPWeb traffic
Web	HTTPWeb	1020	HTTPWeb traffic
Web	JAVA	5050	Java traffic
Web	NortonAntiVirus	1025	Norton AntiVirus traffic
Web	SecureWeb	1011	Web HTTPS traffic
Web	SiteMinder	1026	SiteMinder traffic
Web	Squid	5070	Squid traffic
Web	Web-Port	21085	World Wide Web HTTP
Web	Web-Port	21739	World Wide Web HTTP
Web	Web-Port	21085	World Wide Web HTTP
Web	Webdocument	5013	WebDocument traffic
Web	WebFileTransfer	5000	WebFileTransfer traffic
Web	WebFileTransfer	5060	WebFileTransfer traffic
Web	WebFileTransfer	5061	WebFileTransfer traffic
Web	WebFileTransfer	5062	WebFileTransfer traffic
Web	WebGraphic	5014	WebGraphic traffic
Web	WebMediaAudio	5001	WebMediaAudio traffic

Table 2-1 Default Applications (continued)

Application View Group	Sub-Component	Value	Description
Web	WebMediaAudio	5003	WebMediaAudio traffic
Web	WebMediaAudio	5004	WebMediaAudio traffic
Web	WebMediaAudio	5021	WebMediaAudio traffic
Web	WebMediaAudio	5031	WebMediaAudio traffic
Web	WebMediaDocuments	5010	WebMediaDocuments traffic
Web	WebMediaDocuments	5011	WebMediaDocuments traffic
Web	WebMediaDocuments	5012	WebMediaDocuments traffic
Web	WebMediaDocuments	5030	WebMediaDocuments traffic
Web	WebMediaDocuments	5040	WebMediaDocuments traffic
Web	WebMediaVideo	5002	WebMediaVideo traffic
Web	WebMediaVideo	5007	WebMediaVideo traffic
Web	WebMediaVideo	5008	WebMediaVideo traffic
Web	WebMediaVideo	5020	WebMediaVideo traffic
Web	Webmin	51350	Web-based system administration interface

3

ICMP TYPE AND CODE IDs

This chapter provides information about default ICMP type and Code IDs including:

- [Identifying Default ICMP Types](#)
- [Identifying Default ICMP Codes](#)

Identifying Default ICMP Types

The following table lists the default ICMP Codes:

Table 3-1 ICMP Types

ICMP Type	Description
0	EchoReply
3	DestinationUnreachable
4	SourceQuench
5	Redirect
8	Echo
9	RouterAdvertisement
10	RouterSelection
11	TimeExceeded
12	ParameterProblem
13	Timestamp
14	TimestampReply
15	InformationRequest
16	InformationReply
17	AddressMaskRequest
18	AddressMaskReply
30	Traceroute

Identifying Default ICMP Codes

The following table lists the default ICMP codes:

Table 3-2 ICMP Codes

ICMP Code	Description
3	Destination Unreachable Codes
0	Net Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation Needed and Don't Fragment was Set
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown
3	Destination Unreachable Codes
8	Source Host Isolated
9	Communication with Destination Network is Administratively Prohibited
10	Communication with Destination host is Administratively Prohibited
11	Destination Network Unreachable for Type of Service
12	Destination Host Unreachable for Type of Service
13	Communication Administratively Prohibited
14	Host Precedence Violation
15	Precedence cutoff in effect
5	Redirect Codes
0	Redirect Datagram for the Network (or subnet)
1	Redirect Datagram for the Host
2	Redirect Datagram for the Type of Service and Network
3	Redirect Datagram for the Type of Service and Host
11	Time Exceeded Codes
0	Time to Live exceeded in Transit
1	Fragment Reassembly Time Exceeded
12	Parameter Problem Codes
0	Pointer indicates the error

Table 3-2 ICMP Codes (continued)

ICMP Code	Description
1	Missing a Required Option
2	Bad Length

41

0.5

PROTOCOL IDS

This chapter provides information about default protocols IDs used in STRM.

The following table lists the default common protocols:

Table 4-1 Protocol ID

Protocol ID	Protocol Port	Description
6	TCP	
17	UDP	
1	ICMP	
2	IGMP	
38	IDPR-CMTP	
40	IPv6	
46	RSVP	
47	GRE	
50	ESP	
51	AH	
54	NARP	
99	ANY	
89	OSPFGRP	
94	IPIP	
132	SCTP	

5

PORT IDs

This chapter provides information about default port IDs used by STRM.

The following table lists the default common ports:

Table 5-1 Port ID

Port	Protocol	Protocol Description
20	FTP	File Transfer Protocol
21	FTP	File Transfer Protocol
22	SSH	Secure Shell
23	Telnet	
25	SMTP	Send Mail Transfer Protocol
53	DNS	Domain Name Service
68	DHCP	Dynamic Host Control Protocol
80	HTTP	HyperText Transfer Protocol
81	HTTP	HyperText Transfer Protocol
110	POP3	Post Office Protocol - version 3
115	SFTP	Secure File Transfer Protocol
119	NNTP	Network New Transfer Protocol
123	NTP	Network Time Protocol
137	NetBIOS-ns	Network Basic Input/Output System Name Service
138	NetBIOS-dgm	Network Basic Input/Output System Datagram Service
139	NetBIOS	Network Basic Input/Output System
143	IMAP	Internet Message Access Protocol
161	SNMP	Simple Network Management Protocol
194	IRC	Internet Relay Chat
220	IMAP3	Internet Message Access Protocol 3
389	LDAP	Lightweight Directory Access Protocol
443	SSL	Secure Socket Layer

Table 5-1 Port ID (continued)

Port	Protocol	Protocol Description
445	SMB	NetBIOS over TCP
995	SPOP	Secure Post Office Protocol
1243		SubSeven and other trojans
1433		Microsoft SQL Server
1521	Oracle SQL	
2049	NFS	Network File System
3306	mySQL	
4000	ICQ	
6000		X Windowing System
6699	Napster	
6667	IRC	
6776		SubSeven and other trojans
8080	HTTP	
31337		ackOrifice and other Trojans spells Elite