NetCache™ 5.4
Administration Guide

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089 USA
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Documentation comments: doccomments@netapp.com
Information Web: http://www.netapp.com

Part number 210-00317
December 2002

Copyright and trademark information

Copyright information

Copyright © 1994–2002 Network Appliance, Inc. All rights reserved. Printed in the U.S.A.

Portions copyright © 1998–2001 The OpenSSL Project. All rights reserved.

No part of this book covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Portions of this product are derived from the Berkeley Net2 release and the 4.4-Lite-2 release, which are copyrighted and publicly distributed by The Regents of the University of California.

Copyright © 1980–1995 The Regents of the University of California. All rights reserved.

Portions of this product are derived from NetBSD, which is copyrighted by Carnegie Mellon University.

Copyright © 1994, 1995 Carnegie Mellon University. All rights reserved. Author Chris G. Demetriou.

Permission to use, copy, modify, and distribute this software and its documentation is hereby granted, provided that both the copyright notice and its permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.

CARNEGIE MELLON ALLOWS FREE USE OF THIS SOFTWARE IN ITS “AS IS” CONDITION. CARNEGIE MELLON DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.

Software derived from copyrighted material of The Regents of the University of California and Carnegie Mellon University is subject to the following license and disclaimer:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notices, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS

INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of the software were created by Netscape Communications Corp.

The contents of those portions are subject to the Netscape Public License Version 1.0 (the “License”); you may not use those portions except in compliance with the License. You may obtain a copy of the License at http://www.mozilla.org/NPL/.

Software distributed under the License is distributed on an “AS IS” basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is Mozilla Communicator client code, released March 31, 1998.

The Initial Developer of the Original Code is Netscape Communications Corp. Portions created by Netscape are Copyright © 1998 Netscape Communications Corp. All rights reserved.

Software derived from copyrighted material of Network Appliance, Inc. is subject to the following license and disclaimer:

Network Appliance reserves the right to change any products described herein at any time, and without notice. Network Appliance assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Network Appliance. The use and purchase of this product do not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Network Appliance.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp and the Network Appliance design are registered trademarks of Network Appliance, Inc. in the United States, Canada, and the European Union. Network Appliance is a registered trademark of Network Appliance, Inc. in Monaco and a trademark of Network Appliance, Inc. in the United States and Canada. FAServer is a registered trademark of Network Appliance, Inc. in the United States and the European Union. NetCache is a registered trademark of Network Appliance, Inc. in the European Union and Japan, and a trademark of Network Appliance, Inc. in the United States. SnapCopy is a registered trademark of Network Appliance, Inc. in the European Union and a trademark of Network Appliance, Inc. in the United States. SnapManager is a registered trademark of Network Appliance, Inc. in the United States. WAFL is a registered trademark of Network Appliance, Inc. in the United States, the European Union, and Canada. FilerView and SecureShare are registered trademarks of Network Appliance, Inc. in the United States. Data ONTAP is a trademark of Network Appliance, Inc. in the United States and Canada. Snapshot is a trademark of Network Appliance, Inc. in the United States and the European Union. NetApp–the Network Appliance Company is a registered trademark of Network Appliance, Inc. in the United States and other countries. ApplianceWatch, BareMetal, Center-to-Edge, ContentDirector, DataFabric, MultiStore, NearStore, SecureAdmin, Serving Data by Design, Smart SAN, SnapCache, SnapDrive, SnapMirror, SnapRestore, SnapVault, Vfiler, and Web Filer are trademarks of Network Appliance, Inc. in the United States.

Apple is a registered trademark and QuickTime is a trademark of Apple Computer, Inc. in the United States and/or other countries.

Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries.

RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

Network Appliance is a licensee of the CompactFlash and CF Logo trademarks.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

Network Appliance NetCache is certified RealSystem compatible.

Table of Contents

Preface xiii

Chapter 1 **Administering Access** 1

Adding administrator accounts 2

Access control lists 5

Forming rules 7

Chapter 2 **NetCache Network Interfaces** 13

Section A: Planning summary for network interface configuration 14

Section B: About physical network interfaces 15

Section C: About virtual interfaces 17

About trunking 18

Virtual interfaces on a NetCache appliance 20

Section D: Troubleshooting network interfaces 23

Chapter 3 **Routing on the NetCache Appliance** 25

Section A: Planning summary for routing configuration 26

Section B: About routing on the NetCache appliance 29

How NetCache handles routing. 30

NetCache interaction with a firewall 32

Section C: Controls for restricting client-to-NetCache traffic 33

Section D: Controls for NetCache-to-server traffic 35

How the appliance determines outbound interfaces to use 36

About balancing server-to-NetCache traffic over interfaces 38

About restricting interfaces for connecting to servers 40

Section E: Using TCP large windows to improve performance 41

Chapter 4 **Tunneling Traffic through a NetCache Appliance** 43
About protocol tunneling 44
Configuration overviews 46

Chapter 5 **NetCache Support for DNS** 49
Section A: Planning summary for DNS configuration 50
Section B: Basic DNS configuration on a NetCache appliance 52
Section C: Optional DNS configuration 53
NetCache as a DNS proxy cache 54
Handling domain names that are not fully qualified 56
Handling DNS lookups for local servers 60
Supporting internal resolvers that cannot handle external host names 61
Using NetCache as a full-service resolver 64
Reducing the time that DNS records are cached 67

Chapter 6 **Managing Disks** 69
Section A: RAID on the NetCache appliance 70
Understanding RAID and disks. 71
Disk addresses 74
Disk space on each disk 76
Disk sizes and capabilities 77
Handling disk failure 79
Section B: RAID disk management on the NetCache appliance 82
About displaying the status and statistics of disks 83
Querying for disk health 85
About adding and removing disks 86
Section C: Reinitializing all disks 89

Chapter 7 **Using SNMP and the NetCache Appliance MIB** 91
About the SNMP implementation in NetCache 92

About the NetCache MIB 94
About user-defined traps 96

Chapter 8 **Automated Support with Autosupport** 97
Planning summary for Autosupport configuration 98
About Autosupport 100

Chapter 9 **NetCache Log Files** 107
Section A: Planning summary for log content and management 108
Section B: About NetCache log files 110
Available NetCache log files 111
File names for NetCache logs 115
About predefined and custom log file formats 117
Section C: Log management techniques 120
Available log file switching techniques 121
About log rotation 122
About log pushing 123
Section D: Location of configuration and management options 125

Chapter 10 **Error Handling** 127
Planning summary for error handling configuration 128
About customizable error messages 129
NetCache error codes 130
About hiding NetCache-generated error messages 135

Chapter 11 **Transparent Proxying** 137
Section A: Planning for transparent proxying 138
Planning information to consider as you read this chapter 139
Determining port numbers for redirected traffic 141
Section B: About using an L4 or L7 switch for transparent proxying 142

Transparent proxying requirements for an L4 or L7 switch 143
Choosing an L4 or L7 switch request distribution method 145
Planning for failover with an L4 or L7 switch 146
Preparing for switch configuration 147
Section C: About using a WCCP router for transparent proxying 148
Requirements for WCCP transparent proxying 149
Choosing a WCCP traffic redirection method 152
Choosing a WCCP transmission method 154
Choosing the optimum WCCP request distribution method 156
Distributing load based on appliance platform type 158
Determining if you need to load balance data over multiple NICs 159
Securing access to your WCCP deployment 160
Section D: WCCP service group reference information 161
WCCP service group definition guidelines 162
Listing multiple ports in a service group 165
Section E: Additional transparency features 167
When you might need to modify transparency 168
Circumventing transparent redirection of client requests 170
Retaining the client IP address as the source IP address 172
Hiding NetCache-generated error messages 175
Preventing authentication errors for forward proxy clients 176
Section F: Troubleshooting transparency 178
Troubleshooting your switch or WCCP router deployment 179

Chapter 12 **NetCache Appliance Takeover** 187
Planning summary for NetCache takeover configuration 188
Obtaining information about takeover status 190

Chapter 13 **Hierarchies** 191
Planning decisions to be made 192

About hierarchies 193
Types of hierarchies 195
Cluster hierarchies 198
Hierarchy authentication and access control 200
Standard request distribution 202
Custom rules for distributing requests 204
Hierarchy configuration example 209
Troubleshooting a hierarchy configuration 214

Chapter 14 **Bandwidth Allocation Management** 217
About bandwidth allocation 218
Creating and using virtual bandwidth buckets 220
Constructing bandwidth allocation rules 222
Bandwidth allocation rule examples 224

Chapter 15 **Administration of Multiple Appliances** 229
Section A: About managing multiple appliances 230
Section B: Working with DataFabric Manager 231
About DataFabric Manager appliance management 232
Overview of DataFabric Manager discovery methods 233
Appliance requirements for SNMP-based autodiscovery 234
Appliance requirements for HTTP-based autodiscovery 235
Appliance requirements for appliance-initiated discovery 236
Section C: Using the multiple-appliance management feature 238
Strategies for managing multiple appliances 239
About global configuration files 241
Multiple appliance management by automatic configuration 248
Scenario 1: Multiple cache administration at multiple POP sites 254
Scenario 2: Applying uniform ACL rules over multiple appliances 260
Automatic global file reading through the Appliance Manager 262

Backing up and restoring local configuration files 265
Configuring local settings that do not overwrite global settings 267
Multiple appliance management by pushed configuration files 270
Cloning appliance configurations. 274
Appliance upgrade considerations 277

Chapter 16 **Troubleshooting** 279
Section A: Determining the source of the problem 280
Verifying accessibility to the NetCache appliance 281
Determining if NetCache is the source of the problem. 284
Section B: Common NetCache troubleshooting solutions 287
Recovering from a forgotten console password 288
Rebooting a down NetCache appliance 290
Booting from the system boot media 292
Troubleshooting from the console 296
Recovering access to the Appliance Manager 299
Solving common NetCache configuration problems 301
Recovering from a system panic message 303
Section C: Diagnosing and recovering from network problems 304
Identifying and resolving network problems 305
Verifying the DNS configuration. 307
Configuring an interface using the ifconfig command 309
Downloading and deleting packet trace (pktt) files 312
Section D: Diagnosing and recovering from disk problems 314
Recovering from disk problems using boot media options. 315
Recovering from a disk failure without a hot spare disk 316
Recovering from a disk failure with a hot spare disk. 318
Section E: Diagnosing Web caching and HTTP problems 319
Determining why NetCache is not servicing any URLs 320
Determining why you cannot access a specific URL. 322

Section F: Resolving general system problems 325
Resolving file system problems 326
Resolving NVRAM problems 329
Managing core files 330
Section G: Contacting Network Appliance Technical Support 332

Glossary 333

Index 345

Preface

About this guide

This guide describes the NetCache™ 5.4 software features that you might want to configure on your NetCache appliances that are configured as Web caches, streaming media caches, news caches, streaming accelerators, and Web accelerators. It provides information for the following supported NetCache platforms: C1100, C1105, C1200, C2100, C3100, and C6100.

Information in this guide describes how specific features work and helps you plan what you need to configure to implement that feature.

Use this guide in conjunction with the *Guide to Caching Protocols and Services*, which provides protocol-specific information about deploying a NetCache appliance as a Web cache, streaming media cache, news cache, or streaming media or Web accelerator.

For information about how to upgrade or service the system hardware, see the *Field Service Guide* for your NetCache appliance model.

Audience

This guide is for system administrators who are familiar with computer networks and Web technology.

Administering Access 1

About this chapter

This chapter provides information about how to regulate administrative access to the appliance. It describes how to add and create groups of administrators. It also describes the authentication process, and how to control administrative access to the appliance using access control lists (ACLs). The appliance is permissive by default; that is, ACLs are not enabled and no requests are denied.

Topics in this chapter

This chapter provides information about the following topics:

- "Adding administrator accounts" on page 2
- "Access control lists" on page 5
- "Forming rules" on page 7

Procedures and option descriptions

See the Appliance Manager online Help for configuration procedures and option descriptions.

Location of configuration options

Options for adding users and configuring administrative access are in the following locations in the Appliance Manager:

Feature	Location
Administering users	Setup tab > Authentication
Controlling access	Setup tab > Access Control Lists

Adding administrator accounts

Accessing the Appliance Manager

The Appliance Manager is a browser-based administration tool that enables you to customize and maintain your configuration. To launch the Appliance Manager, open a Web browser and point it to

`http://hostname:port`

where *hostname* is the name of the appliance, and *port* is the Admin Port setting. The default Admin Port setting is 3132.

For example:

`http://cache1:3132/`

Default administrative user name and password: When you select an option from the Appliance Manager, you are prompted for a user name and password. By default, the user name is *admin*, and the default password is *NetCache*.

Administering access

User names, passwords, and group memberships are assigned using the authentication user and group options in the Appliance Manager. Use these options to do the following:

- Add users individually

  Authenticated users who are not members of any groups are assigned default access permissions. There is only one set of default access permissions. Permissions cannot be modified on a per-user basis.

- Manage groups of users

  Create groups, specify group memberships for users, set access permissions for the group, and edit user and group information for the local user database.

Note

A user can be a member of one group or multiple groups. Group access permissions can be set and modified on a per-group basis.

About authentication

Authentication is the process of determining a user's identity so that the user becomes known to the system. In addition to verifying a user's identity, authentication can be used in conjunction with access controls to enforce local security, allocate resources, and keep records of traffic.

The appliance authenticates a user for the first time when ACLs specifying authentication are applied, forcing authentication.

System administrators cannot access the Appliance Manager unless the user database contains at least one user name and password. The appliance provides a default administrator account and a default group called `NetCache`. The account user name is `admin` and the password is `NetCache`. All permissions assigned to the NetCache group apply to the default administrator account.

The default admin user account is configured with permissions to use all protocol services, as well as permissions to access the Appliance Manager and change the appliance configuration.

Note

The administrator user account user name and password are case-sensitive.

Using the Admin ACL option, you can create profiles with different levels of access for administrators. For example, you can apply different ACLs to different administrator accounts and allow some administrators to monitor the status of the appliance, but prevent them from making configuration changes.

When does the appliance authenticate a user?

The appliance authenticates a user for the first time when ACLs specifying authentication are applied. A user is authenticated against the local database. When authentication succeeds (that is, a match is found), any groups that a user belongs to are determined.

About the local user database

The user database contains administrator user account information that provides instructions for handling requests. Because it can contain group information, it can be used to assign access permissions based on group membership.

Groups

Grouping administrators is common practice and makes administering access less complicated than administering access by individual user. For example, the appliance can be configured to authorize access to administrative features for users in a senior administrative group, while prohibiting access to a junior group of administrators.

Where authentication server information is logged

The appliance logs general information pertaining to authentication in the Messages log file. For example, if repeated authentication failures occur, the appliance logs a simple, explicit message noting that there were many authentication failures. You can use information such as this to assess if there might be a communication problem between the appliance and the authentication server rather than a true failed attempt to authenticate the user. The appliance logs this event as a connectivity error. Notification of this event in the log may indicate that a link is down between the appliance and the server.

Access control lists

What access controls do

Access control settings prevent unauthorized access to the appliance and restrict authorized access to services. The appliance supports different types of rules that impose a variety of restrictions. Sets of rules, or access control lists (ACLs), are used to impose restrictions inside the intranet domain.

Internet setting: In an Internet setting, access controls can be used to set rules that limit access for authorized users.

Intranet setting: In an intranet setting, access controls can help enforce authentication and authorize exactly what administrators have access to.

Authorized access

When a user makes an authenticated request, the appliance checks the user against all groups in the local user database, and attempts to match ACLs that are associated with those groups. If the request is not matched by user or group ACLs, then the request is checked against all other access control rules. If access is denied, a system message displays the rule and the name of the ACL that prevented access to services.

Controlling administrative access

ACLs can be applied explicitly to authorized users, but they are also effective for administering access control to individuals as part of a group, such as administrators. ACLs can be applied to members of administrative groups that are assigned “Admin, Full” and “Admin, Read-Only” access permissions.

ACL rule checking

The appliance sequentially reads ACLs and checks for the first matching entry. When a match occurs, the action is executed. If no match occurs, no action is executed and rule checking continues.

Rule checking sequence is shown in the following table.

Stage	Description
1	Check global settings that control authentication for protocol requests.

Stage	Description
2	Check ACL permission settings for the applicable group in the local user database.
3	Check request-type (protocol specific) ACL.
4	Check Web accelerator ACL.
5	Check global ACL.
6	Check group permissions settings.
7	Allow the request.

Order of precedence

Types of rules and order of precedence are described in the following table.

Order	Type	Description
1	User and group	User and group rules explicitly allow, deny, or redirect requests. User and group ACLs have precedence over request-type, global, and group access permissions.
2	Request-type (protocol specific)	Request-type rules control specific types of traffic. Access control rules are processed only for requests of a particular type, or protocol, such as NFS. Request-type access controls have precedence over Global access controls. If a request-type rule explicitly allows, denies, or redirects a request, the appliance follows this rule regardless of any rules configured in the Global Access Control option and any content category restrictions set in the SmartFilter options.
3	Accelerator	If a request originates from a Web-accelerator (reverse-proxy), this ACL is checked.
4	Global	Global rules impose restrictions on all traffic by allowing you to specify variables, such as a user name and a URL.
5	Group access permissions	Group access permissions specify default access to services for groups, and control rewrites or redirects for blocked requests. Default rules apply to requests that have no rule matches.

Forming rules

ACLs

ACL entries allow or deny requests based on a number of variables, such as client IP addresses. ACLs are associated with specific users, and groups of users.

When ACL rules are formed, actions are combined with expressions that contain a variable-value pair. Variables and associated values form what is commonly referred to as a pattern-matching expression.

Syntax

When applying actions (for example, allow, deny, redirect, rewrite, and auth) to matching expressions, use the `action expression` syntax, as shown in the following table.

Action	Expression
`allow`	`client-ip 128.126.10.0`
`auth`	`FTP`
`deny`	`server-domain net`
`allow`	`time 9am - 5pm`
`deny`	`FTP`

Actions

Actions and expressions form rules that control requests for access to Web content and supported protocols. The following table lists supported actions and describes how they govern client requests.

This action...	Specifies...
`allow`	Allow the request to proceed and disregard all the following rules.
`auth`	Require authentication and continue the rule checking sequence if already authenticated.
`deny`	Deny the request immediately.

This action...	Specifies...
`no-log`	Selectively log and filter log file information by field. If applied as a global ACL, all logs are filtered. Entries in log files are replaced with a "-". **Note** Global authentication must be enabled.
`proxy`	Proxy session. Do not serve from cache.
`re-auth`	Force reauthentication.
`redirect` *<url>*	Redirect the request immediately.
`rewrite`	Rewrite the URL, but continue the rule checking sequence.
`try-auth`	Require authentication and continue the rule checking sequence even if authentication fails.

Variables

Variables are assigned values that form expressions, for example, *time 9am - 5pm*. The following table lists variables and provides a description and example of each.

Variable/Description	Example
`accel` Web Accelerator requests	`deny accel`
`any` Any requests	`deny any`
`auth` Authenticated request	`auth any`
`cache-ip` IP address of this NetCache	`allow cache-ip 206.80.5.0/24`

Variable/Description	Example
`cache-port` Port number on this NetCache	`deny cache-port` 8080
`client-domain` Client domain name	`deny client-domain .wisc.edu`
`client-ip` Client IP address	`deny client-ip 206.79.5.51`
`client-port` Client port number	`deny client-port 25`
`contains` Substring search operator **Note** This variable supports user, group, req-headers, server-name, client-domain, and server-domain variables.	`deny url contains bomb`
`contains-case` Case-sensitive substring search operator **Note** This variable supports user, group, server-name, client-domain, and server-domain variables.	`deny url contains-case VIOlence`
`date` Date and time	`deny group novice and date "sun nov 6 08:49:37 2002"`
`day` Day	`allow day mon - fri`

Variable/Description	Example

`group`
Multidomain support for groups.
Note
A group name with no domain name matches any group with that name, regardless of the domain.
	`auth any`
	`allow group admins`
	`deny any`
	This ACL allows access for members of group “admins” in all trusted domains

`group\`
Multidomain support for groups.
Note
Using the “\” delimiter between the domain name and group name enables domain comparison.
	`auth any`
	`allow group “ADMINS\globalgroup”`
	`deny group “NOVICE\globalgroup”`
	`deny any`
	This ACL allows access for members of ADMINS, and denies access for members of NOVICE. Globalgroup is a trusted domain.

`http` HTTP requests	`deny url “http://www.corp.com”`
`server-domain` Server domain name	`allow server-domain .mycorp.com`
`server-ip` Server IP address	`deny server-ip 206.79.5.0/24`
`server-name` Server name in URL	`allow server-name www.mine.com`
`server-port` Server port number in URL	`deny server-port 1 - 1024`
`time` Time	`allow time 9am - 5pm`
`url` URL string	`deny url http://www.mine.com/`

Variable/Description	Example
`url-prefix` Prefix of URL string	`deny url-prefix http://www.mine`
`user` User name of authenticated user	`deny user bob`

Expressions

Expressions are single predicates, variable-value pairs, range matches, or regular expressions (regex). The following table provides an example of each expression type.

Type	Definition	Example
Single predicate	<*variable*>	server-ip
Variable-value pair	<*variable*> <*value*>	client-ip 128.148.37.17
Range matching	<*variable*> <*value*> - <*value*>	server-port 1- 1024
Regular expression matching (regex)	<*variable*> matches <*regex*>	“^http://[0-9.]+/redcodeworm.asp\?X+”

Note

When you create rules, you must enclose values that contain white space or nonalphanumeric characters in double quotation marks.

Operators

Complex expressions are built using parentheses and boolean operators, such as `and` or `&&`, `or` or `||`, and `not`. For example:

- <*expr*> `and` <*expr*>
- <*expr*> `or` <*expr*>
- (<*expr*>)
- `not` <*expr*>

Caution

Using the operator `not` in combination with the action `allow` (for example, `allow not user user1`) does not result in an action to deny requests when the rule is applied.

Use caution when setting rules

The type of rule and the number of rules that the appliance must check before servicing each request can affect performance. For example, rules containing the `server-ip` variable prompt a cached DNS lookup that might be slower than using the `server-name` variable to specify server names.

In general, order your rules so that specific restrictions are listed before broad restrictions. Carefully plan the access restrictions you want to impose. Configure only the rules that are required for your environment, and where possible, collapse several rules into a single rule.

NetCache Network Interfaces 2

About this chapter

This chapter discusses the types of interfaces supported on the NetCache appliance, how the interfaces are named, and the concept of virtual interfaces.

Sections in this chapter

This chapter contains the following sections:

- Section A, "Planning summary for network interface configuration," on page 14
- Section B, "About physical network interfaces," on page 15
- Section C, "About virtual interfaces," on page 17
- Section D, "Troubleshooting network interfaces," on page 23

Procedures and option descriptions

See the Appliance Manager online Help for configuration procedures and option descriptions.

Location of configuration options

Options for configuring network interfaces are in the following location in the Appliance Manager:

Setup tab > Network > Interfaces

Section A: Planning summary for network interface configuration

Determine network interface configuration

Configuring network interfaces will be faster if you plan ahead. Use the information in the following table to determine the network interface configuration that is necessary for your organization.

Decisions to make	Your options	Considerations
Whether you need to configure additional physical network interfaces	During the setup program, configuration of at least one physical interface is required.	You can configure additional physical interfaces after setup if they are needed.
Whether to configure one or more virtual interfaces	You can configure up to eight virtual interfaces.	Advantages of using virtual interfaces are as follows: ◆ Higher throughput because of multiple interfaces working as one interface. ◆ Fault tolerance. If one interface in a virtual interface goes down, the NetCache appliance can still stay connected to the network using the other interfaces. ◆ Protection against a switch becoming a single point of failure.
Whether you need to change the state of a physical interface	The state of any interface configured during setup is up by default.	◆ You must bring down any physical interface that is to be configured as part of a virtual interface. ◆ Before performing maintenance on the link, bring the interface down. When your work is complete, bring the interface back up.

Section B: About physical network interfaces

Supported interfaces

NetCache supports the following network interfaces:

- Physical interfaces
  - FDDI
  - Ethernet
  - Gigabit Ethernet
- Virtual

  For detailed information on virtual interfaces, see Section C, "About virtual interfaces," on page 17.

Naming conventions for network interfaces

NetCache appliance uses the following interface naming conventions to refer to each network interface:

- Ethernet and Gigabit Ethernet interface names start with the letter *e* followed by the slot number (for example, *e0*) and the port number (if the adapter is a quad-port Ethernet card, for example, *e1a* and *e1b*.)

  Note
  Port numbering on quad-port cards starts from the top port.

- FDDI interface names start with the letter *f* followed by the slot number (for example, *f1* and *f2*).

NetCache appliance automatically creates host names for network interfaces by appending the slot number of the interface to the NetCache appliance's host name. For example, if the NetCache appliance is named *toaster*, the host name for *e0* is *toaster-e0*, and the host name for *e1a* is *toaster-e1a*. If the interface is an FDDI interface, the letter *f* precedes the slot number. For example, the host name for *f1* is *toaster-f1*.

When to configure a network interface

During the setup program, at least one network interface must be configured. After setup, you can do the following:

- As necessary, configure additional network interfaces, for example, if you are bringing up an additional interface on your NetCache appliance
- Edit the options previously configured for a physical interface

- Change the state of a physical interface

Note

You do not need to configure a physical interface that you want to include in a virtual interface. The only requirement is that the state of that physical interface is down. See Section C, “About virtual interfaces,” on page 17 for more information.

Section C: About virtual interfaces

About this section

This section contains information about virtual interfaces (a feature that implements trunking on the NetCache appliance), and managing various types of virtual interfaces on the NetCache appliance.

Topics in this section

This section contains the following topics:

- "About trunking" on page 18
- "Virtual interfaces on a NetCache appliance" on page 20

About trunking

About trunking

Trunking is a mechanism that groups together multiple network interfaces (links) into one logical interface (trunk). Different vendors refer to trunks by the following terms:

- Virtual aggregations
- Link aggregations
- Virtual interfaces (the term Network Appliance uses)
- EtherChannel

The NetCache implementation closely follows the IEEE 802-3ad specification.

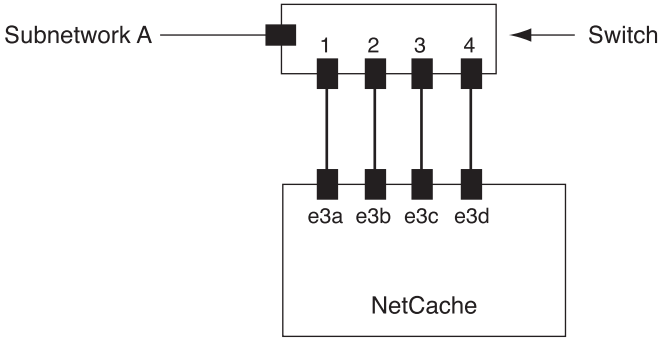
Advantages of trunking

Trunks provide several advantages over individual interfaces, such as the following:

- Higher throughput because of multiple interfaces working as one interface.
- Fault tolerance. If one interface in a trunk goes down, the NetCache appliance can still stay connected to the network using the other interfaces.
- Protection against a switch becoming a single point of failure.

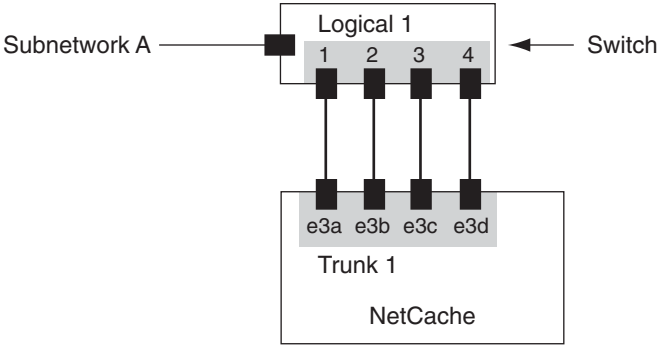
NetCache appliance interfaces before trunking

The following illustration shows four separate NetCache appliance interfaces, *e3a*, *e3b*, *e3c*, and *e3d*, before trunking.



NetCache appliance interfaces after trunking

The following illustration shows the four NetCache appliance interfaces joined after trunking into a single trunk called *Trunk1*.



Virtual interfaces on a NetCache appliance

About virtual interfaces

The feature that supports trunking on the NetCache appliance is known as a virtual interface. After being created, a virtual interface is indistinguishable from a physical network interface.

Types of virtual interfaces

There are two types of virtual interfaces:

- Single-mode
- Multi-mode

Single-mode virtual interface operation

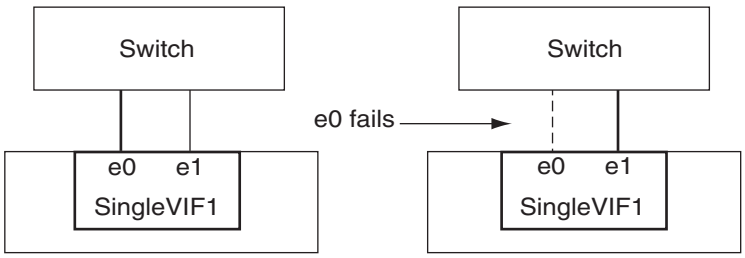
In a single-mode virtual interface, all interfaces that constitute the virtual interface share an IP address and a media access control (MAC) address. However, only one interface in the virtual interface is active. The other interfaces are on standby, ready to take over if the active interface fails. Failure means that the link status of the interface is down, which signals that the interface has lost connection with the switch.

Note

When you create a single-mode virtual interface, an interface is selected randomly to be the active interface. However, if you want to specify a certain interface to be active, you can override the random selection and specify that interface as *preferred*. For example, if you want to make a standby or a new interface active, you must make that interface the preferred interface. There can only be one preferred interface in a single-mode virtual interface.

A single-mode virtual interface can recover from a failure of up to (n-1) interfaces, where n is the total number of interfaces that form the virtual interface.

Example: In the following illustration, *e0* and *e1* are part of the SingleVIF1 single-mode virtual interface. The active interface, *e0*, fails. The *e1* interface takes over and maintains the connection to the switch.



Multi-mode virtual interface operation

In a multi-mode virtual interface, all the interfaces in the virtual interface are active at the same time. This logical aggregation of links provides higher throughput than possible if the interfaces were configured as a single-mode virtual interface.

With a multi-mode virtual interface, NetCache load balances outgoing traffic over the outgoing interfaces that are trunked. The switch automatically balances the load among the interfaces of the virtual interface if the following conditions are met:

- The switch supports trunking over multiple ports
- The switch is configured so that all ports to which links of a virtual interface are connected are part of a single logical port and share a common MAC address.

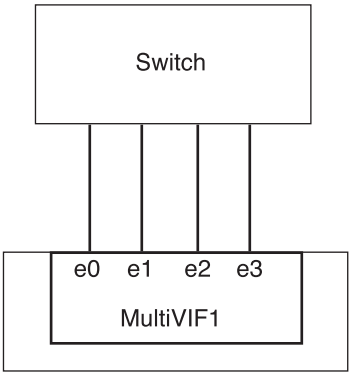
For information about configuring the switch, see your switch vendor's documentation.

Note

Some switches might not support trunking of ports configured for jumbo frames. For more information, see your switch vendor's documentation.

A multi-mode virtual interface can recover from a failure of up to (*n*-1) interfaces, where *n* is the total number of interfaces that form the virtual interface.

Example: In the following illustration, *e0*, *e1*, *e2*, and *e3* are part of the MultiVIF1 multi-mode virtual interface. All four interfaces in the MultiVIF1 multi-mode virtual interface are active.



In the preceding illustration, if any three of the interfaces were to fail one-by-one or simultaneously, the NetCache appliance still stays connected to the network.

Routing on a NetCache appliance with a multi-mode virtual interface

If this physical interface goes down or is removed from the multi-mode virtual interface, load balancing occurs over the remaining interfaces.

Prerequisites to creating a virtual interface

Before creating a virtual interface, you need to

- Identify the interfaces you want to aggregate into the virtual interface on your NetCache appliance.
- If you are creating a multi-mode virtual interface, configure a switch that supports trunking over multiple port connections according to your switch vendor's instructions.

Section D: Troubleshooting network interfaces

Use the ifconfig command for troubleshooting

When you are troubleshooting a NetCache appliance, you can use the `ifconfig` command to perform common interface configuration. See the *Command Line Reference* for more information.

Caution

Configuration changes made using the `ifconfig` command do not persist after a system reboot. To make changes persistent across a system reboot, use the `ifconfig -set` command.

Recovering from loss of connectivity to the NetCache appliance

If you bring down the administrative interface or all network interfaces, you can recover in one of the following ways:

If you have a backup configuration file: From the command line at the console, use the `config -rl` command to revert to a backup copy of the NetCache configuration.

If you do not have a backup configuration file: Use the `ifconfig` command from the command line at the console to bring up an interface. Then use the Appliance Manager to bring up and, if necessary, reconfigure the other network interfaces.

Routing on the NetCache Appliance 3

About this chapter

This chapter discusses how NetCache uses default and static routes for incoming and outgoing requests, binds traffic to interfaces, and communicates with hosts and subnets using TCP large windows.

Sections in this chapter

This chapter contains the following sections:

- Section A, "Planning summary for routing configuration," on page 26
- Section B, "About routing on the NetCache appliance," on page 29
- Section C, "Controls for restricting client-to-NetCache traffic," on page 33
- Section D, "Controls for NetCache-to-server traffic," on page 35
- Section E, "Using TCP large windows to improve performance," on page 41

Procedures and option descriptions

See the Appliance Manager online Help for configuration procedures and option descriptions.

Section A: Planning summary for routing configuration

Determine routing configuration

Configuring routing will be faster if you plan ahead. Use the information in the following table and the remainder of the chapter to determine the routing configuration that is necessary for your organization.

Decisions to make	Considerations	Option to use in the Appliance Manager
Considerations for configuring basic routing support		
Whether you need to add static routes	You need to enter static routes in the NetCache appliance routing table only if your default gateway is not aware of some addresses and you are not able to route packets to those addresses through RIP or IRDP. If you decide to use static routes, disable the Fast IP option (Setup tab > Network > General). The Fast IP option overwrites any static routes that you have specified.	Setup tab > Network > Routing > Static Routes tab
Whether you want NetCache to listen to Router Discovery messages	If your routers are configured to support IRDP, Network Appliance recommends that you enable Route Discovery. Enabling Route Discovery eliminates the need to manually configure the default gateway.	Setup tab > Network > Routing > General tab > Route Discovery Enable option This option is disabled by default.

Decisions to make	Considerations	Option to use in the Appliance Manager
Considerations when a firewall exists		
Whether you need to configure NetCache to route traffic through a firewall	If your NetCache appliance is outside a firewall, consider whether you want to use ACLs to ensure that clients and caches outside your organization cannot use this cache to resolve requests (thereby using your bandwidth). If your firewall is a nontransparent firewall acting as a proxy, you must configure the NetCache appliance as part of a hierarchy.	For ACL configuration: Setup tab > Access Control > Access Control Lists For hierarchy configuration: Setup tab > Hierarchy
Controlling interfaces over which NetCache sends out and accepts traffic		
Whether you need to restrict the NetCache interfaces through which NetCache accepts client requests	Typically, NetCache accepts client requests through any interface and IP address. You can add a level of security by using the Listen Addresses option to restrict the IP addresses, and therefore the interfaces, on which NetCache accepts client requests.	Setup tab > Network > General > Listen Addresses option Do not use this option if the appliance is configured for transparency or NetCache takeover.
Whether you need to balance traffic from servers to the NetCache appliances over NetCache interfaces	Some organizations, such as ISPs, need to balance responses from servers across multiple lines. By balancing traffic across the NetCache outbound interfaces, server-to-NetCache traffic is balanced over multiple lines.	Setup tab > Network > General > Load Balancing Interfaces option

Decisions to make	Considerations	Option to use in the Appliance Manager
Whether you want to restrict the interfaces from which NetCache can communicate with servers	Disable outgoing interfaces in the following circumstances: ◆ You want to devote an interface for administrative purposes instead of using it for regular traffic. ◆ One interface of a NetCache appliance is outside a firewall and another interface is inside the firewall. Typically, you do not want to use the interface inside the firewall for traffic to outside servers.	Setup tab > Network > General Disabled Outgoing Interfaces option
Considerations for high-bandwidth, long-haul connections		
If you have a high-bandwidth, long-haul connection, whether TCP large windows configuration would be beneficial	TCP large windows improves performance over high-bandwidth, long-haul connections by using the capacity of the pipe more effectively.	Setup tab > Network > General > TCP Large Windows Enable and TCP Large Windows List

Section B: About routing on the NetCache appliance

About this section

This section discusses how the NetCache appliance uses default and static routes for incoming and outgoing requests and how it interacts with firewalls.

Topics in this section

This section contains the following topics:

- "How NetCache handles routing" on page 30
- "NetCache interaction with a firewall" on page 32

How NetCache handles routing

The NetCache appliance does not function as a router

Although the NetCache appliance can have multiple network interfaces, it does not function as a router; that is, the NetCache appliance does not route packets between its interfaces on behalf of other network hosts.

How the NetCache appliance routes its own packets

For routing its own packets, as well as dynamic routes, the NetCache appliance relies on the default route and static routes. Normally, the NetCache appliance learns explicit routes through Internet Control Message Protocol (ICMP) redirect messages received from the default router; you do not need to enter static routes in the NetCache appliance's routing table.

Configuration consideration: You need to enter static routes in the NetCache appliance routing table only if your default gateway is not aware of some addresses and you are not able to route packets to those addresses through RIP or IRDP.

Note

If you implement static routes, disable the Fast IP option (Setup tab > Network > General). The Fast IP option overwrites any static routes that you have specified.

Management of network routing tables

NetCache uses the routed daemon to manage the network routing tables. Routed is a simple routing daemon that is enabled at boot time. Routed uses the Routing Information Protocol (RIP), which listens for packets being exchanged between routers on the network and solicits multicast router discovery Internet Control Message Protocol (ICMP) messages. NetCache uses RIP response packets to update its routing tables. The NetCache routing tables are updated with gateways that are currently recognized on the network, or with gateways that advertise a better metric than at least one of the gateways currently listed in the routing tables.

Configuration consideration: By default, RIP is enabled. Disabling RIP stops NetCache from listening for RIP response packets, and information in the routing table remains static.

About Route Discovery

The Internet Router Discovery Protocol (IRDP), which is an extension of ICMP, enables hosts attached to multicast or broadcast networks to discover the IP addresses of neighboring routers. When the Route Discovery feature on NetCache is enabled, NetCache listens to Router Discovery messages, thereby eliminating the need to manually configure the default gateway. If the default router goes down, IRDP informs NetCache about alternative routers, ensuring that NetCache maintains its connection to the Internet. Only routers that support IRDP can be discovered through the Route Discovery feature.

Configuration consideration: Route Discovery is disabled by default. If your routers are not configured to support IRDP, do not enable this option.

NetCache interaction with a firewall

If NetCache is outside a firewall

If you are deploying a NetCache appliance outside a firewall, no further configuration is required to enable NetCache to access the Internet. However, you might want to ensure that clients and caches outside your organization cannot use this cache to resolve requests, thereby using your bandwidth. See "Hierarchies" on page 191 for more information about configuring access controls to prevent access by other proxy-cache servers. See the access controls chapter in the *Security Guide* for information about how to create access controls for clients.

If NetCache is deployed inside a transparent firewall

If NetCache is deployed inside a *transparent* firewall, no explicit NetCache configuration is required. NetCache uses the default gateway to send requests to the Internet. However, the firewall must be configured to accept requests from NetCache and forward them to the Internet.

If NetCache is deployed inside a nontransparent firewall

If NetCache is deployed inside a *nontransparent* firewall, you must configure a request resolution hierarchy, with the nontransparent firewall as a member of the hierarchy. The reason is that a NetCache appliance that exists inside a nontransparent firewall has no way to send requests through the firewall to the Internet. When the firewall is configured as a hierarchy member, NetCache can route unresolved requests to the firewall for routing to the Internet.

You can specify the domains and IP addresses that are local to the NetCache appliance so that NetCache can bypass the hierarchy for requests for local origin servers. Bypassing the hierarchy for origin servers that exist physically near your NetCache appliance can speed performance and reduce the load on parent and neighbor caches.

Section C: Controls for restricting client-to-NetCache traffic

How NetCache typically accepts requests

Typically, NetCache accepts client requests through any interface and IP address, including any interface and IP address for an Internet link. You can add a level of security by restricting the IP addresses and, therefore, the interfaces through which NetCache accepts client requests.

Note

Interfaces can have more than one IP address.

Option you can use to change NetCache behavior

Using the Listen Addresses option, you can limit the NetCache appliance IP addresses on which NetCache listens for client requests. If a TCP or UDP IP address is specified in this option, NetCache listens only on that IP address. If the Listen Addresses box is left blank, NetCache listens on all of its TCP or UDP interfaces.

The Listen Addresses option is on the Network - General page (Setup tab > Network > General).

Determining whether you should use this option

Consider the following when determining whether to use this option:

- Only the IP addresses associated with the interfaces of this NetCache appliance can be listed in this option.
- You must enter a full IP address, not a network address or a subnet address.
- Each interface for an IP address listed in this option must be configured as up; otherwise, NetCache will not listen on it.
- You cannot use this option if transparency is enabled for any protocol. The reason is that the destination IP address will never be the NetCache appliance, only a destination server.
- You cannot use this option if this NetCache appliance is part of a takeover pair.

Difference between using this option and using access controls

The difference between using the Listen Addresses option and using access controls is that if you list the IP addresses of some interfaces in this option, NetCache does not accept connections through interfaces whose IP addresses are not listed. With access controls, NetCache accepts the connection but then filters out requests based on the access control that is set.

Examples of how the Listen Addresses option can be used

You can use the Listen Addresses option in the following ways:

Example 1: Allowing client traffic from your internal network but not allowing traffic from the Internet

If your NetCache appliance is inside your firewall and your firewall does not block access from all clients external to your organization, you can specify in the Listen Addresses option only the IP addresses of the interfaces to your organization's internal networks. Because the IP address for the interface to the Internet is not listed in the Listen Addresses option, NetCache will not listen on that interface. Therefore, clients on the Internet cannot access your NetCache appliance.

Example 2: Preventing random access

If your NetCache appliance is outside your firewall and you want to limit requests to your NetCache appliance to only requests from clients inside the firewall, specify in the Listen Addresses option the IP address of the interface that is connected to the firewall. NetCache will not listen on any other interfaces and, therefore, will not accept requests from hosts on the Internet.

Section D: Controls for NetCache-to-server traffic

About this section

This section describes the default behavior for the interfaces that NetCache uses to send traffic to origin servers and the circumstances for which you might want to control the outbound interfaces that the NetCache appliance uses to send traffic to origin servers.

Topics in this section

This section contains the following topics:

- "How the appliance determines outbound interfaces to use" on page 36
- "About balancing server-to-NetCache traffic over interfaces" on page 38
- "About restricting interfaces for connecting to servers" on page 40

How the appliance determines outbound interfaces to use

Default behavior for determining outbound interface use

By default, NetCache binds all types of traffic to all interfaces. You can, however, bind specific types of traffic to specific interfaces to balance the load across interfaces or to provide an additional level of security. Any time you bind traffic to a particular interface, NetCache sends or accepts that type of traffic only on that interface.

By default, if the NetCache appliance has multiple interfaces, NetCache performs a route lookup when it receives a request and selects the interface closest to the origin server. NetCache performs only one route lookup, and it selects the most efficient route to the server. Therefore, in typical circumstances, you do not need to configure NetCache to instruct NetCache how to select the outbound interfaces.

Options for controlling outbound interface use

In some circumstances, however, it is desirable to control the interfaces that NetCache selects for traffic to servers. The following two options are available to influence how NetCache selects the interfaces to use for outgoing traffic:

- Load Balancing Interfaces option

  Organizations that need to balance responses from servers across multiple lines can use this option. By specifying the interfaces over which NetCache is to balance outgoing traffic, responses from origin servers are distributed over multiple lines on their way to the NetCache appliance. See “About balancing server-to-NetCache traffic over interfaces” on page 38 for more information.

- Disabled Outgoing Interfaces option

  This option enables you to identify outgoing interfaces that you do not want NetCache to use. See “About restricting interfaces for connecting to servers” on page 40 for more information.

The following table shows how these two option settings control outbound interface selection.

Load Balancing Interfaces setting	**Disabled Outgoing Interfaces setting**	**What NetCache does**
No interfaces are listed.	No interfaces are listed.	NetCache uses the interface closest to the server.
No interfaces are listed.	An interface is listed, for example, E0.	NetCache includes all interfaces in its load balancing determination except for interfaces listed in the Disabled Outgoing Interfaces option. **Note** For the first packet and for UDP, NetCache performs a route lookup.
Specific interfaces are listed, for example, E7 and E8.	No interfaces are listed.	NetCache balances traffic only over the interfaces listed in the Load Balancing Interfaces option (in this example, only over E7 and E8 and any aliases of E7 and E8). **Note** For the first packet and for UDP, NetCache performs a route lookup and might select an interface not listed in the Load balancing Interfaces option.

About balancing server-to-NetCache traffic over interfaces

Implication of source IP address on server-to-appliance traffic

The source address of the outbound request determines which interface the origin server *replies* to and, therefore, is the IP address to which the server sends the requested object. If the NetCache appliance has multiple interfaces, you can configure their IP addresses as outbound IP addresses so that traffic can be shared across the interfaces. Because the outbound traffic is spread over multiple IP addresses, incoming packets in response to the request are directed to the appropriate interface based on the source IP address and, therefore, are balanced over the NetCache interfaces.

Option you can use for load balancing server-to appliance traffic

You can use the Load Balancing Interfaces option to specify all interfaces through which the NetCache appliance communicates when initiating outgoing connections. Each interface listed participates in the load balancing of outbound traffic by splitting traffic across outbound links. The end result is that the incoming traffic is split over NetCache interfaces.

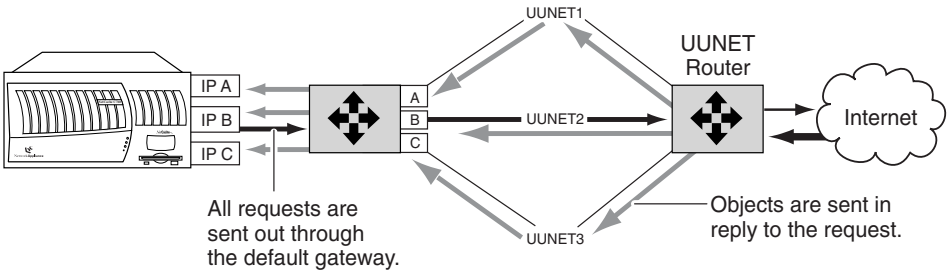
Restrictions for using this option are as follows:

- Do not list any interfaces in this option that you have listed in the Disabled Outgoing Interfaces option, which identifies interfaces that NetCache is not to use for outgoing traffic. See "About restricting interfaces for connecting to servers" on page 40 for more information about the Disabled Outgoing Interfaces option.
- You cannot use the Load Balancing Interfaces option if your NetCache appliance is part of a takeover pair.

The Load Balancing Interfaces option is on the Network - General page (Setup tab > Network > General).

Topology example

The advantage of configuring NetCache so that requests are sent out with different source interfaces is that responses from origin servers are distributed over multiple lines on their way to the NetCache appliance. In the following example, an ISP has multiple lines to the Internet and needs to balance the traffic load across those lines. Because transferring objects from the origin server generates the most traffic, the ISP needs to balance the traffic being sent to the NetCache appliance from the Internet.



In this example:

- NetCache is configured to have one interface in the Load Balancing Interfaces option for each line to the Internet. In this case, three IP addresses are required.
- NetCache sends requests to origin servers, cycling through the interfaces in the Load Balancing Interfaces list as source addresses.
- The origin servers respond by sending the requested object to the IP address where the request originated.

About restricting interfaces for connecting to servers

About the Disabled Outgoing Interfaces option

You can use the Disabled Outgoing Interfaces option to specify the interfaces that NetCache is not to use when connecting to servers.

Disable outgoing interfaces in the following circumstances:

- You want to devote an interface for administrative purposes instead of using it for regular traffic.
- One interface of a NetCache appliance is outside a firewall and another interface is inside the firewall. Typically, you do not want to use the interface inside the firewall for traffic to outside servers.
- You have more interfaces than you want to use for outbound traffic.

Restrictions for using this option are as follows:

- Do not list any interfaces in this option that you list in the Load Balancing Interfaces option.
- You cannot use the Disabled Outgoing Interfaces option if your NetCache appliance is part of a takeover pair.

The Disabled Outgoing Interfaces option is on the Network - General page (Setup tab > Network > General).

Section E: Using TCP large windows to improve performance

When using TCP large windows is beneficial

Long-haul networks have more capacity than can be used effectively with the standard TCP window size. Enabling TCP large windows dramatically improves performance over high-bandwidth, long-haul connections by using the capacity of the pipe more effectively. Using TCP large windows on local area networks, however, has no benefit.

Examples of networks that can benefit from enabling TCP large windows include the following:

- Two NetCache appliances communicating with each other over a satellite link
- Clients connecting to a NetCache appliance using DSL but with a high-capacity hop between them and the appliance

Determining which hosts or subnets to enable TCP large windows for

When the NetCache TCP Large Windows feature is configured, NetCache can communicate with specified hosts and subnets using TCP large windows. You can specify the systems or subnets with which NetCache should communicate using large windows, and also to specify the window size that NetCache should use with each.

Exercise caution when deciding which hosts or subnets NetCache should communicate with using large windows. Using large windows consumes more memory than using the standard window size; therefore, NetCache limits the number of simultaneous connections using large windows. The bigger the window size specified, the fewer simultaneous large windows connections NetCache can support.

Network Appliance recommends that you specify only a few hosts or subnets with which NetCache should communicate using large windows.

The TCP large windows options, TCP Large Windows Enable and TCP Large Windows List, are on the Setup tab > Network > General page.

Determining the window size to use

To use the capacity of the link effectively, the window size should be greater than or equal to the *bandwidth-delay product*. Calculate the bandwidth delay product by multiplying the capacity of the link (bandwidth) by the round-trip time (delay), as follows:

$$\text{window size} \geq \text{bandwidth} \times \text{delay}$$

Setting the window size precisely to optimize the usage of the link can require some experimentation, however.

Guidelines for common connection types: If you are using a T1 or T3 connection, you can use the window sizes in the following table.

Connection type	Recommended window size
T1	11264 bytes
T3	345088 bytes

The window size in the preceding table is based on a 60-millisecond delay (round-trip time). If your bandwidth is higher or the delay is higher, set a higher window size.

Tunneling Traffic through a NetCache Appliance 4

About this chapter

This chapter describes the purpose of the NetCache protocol tunneling feature and provides guidelines about when to use it.

Topics in this chapter

This chapter covers the following topics:

- "About protocol tunneling" on page 44
- "Configuration overviews" on page 46

Procedures and option descriptions

See the Appliance Manager online Help for configuration procedures and option descriptions.

Location of configuration options

Options for configuring protocol tunneling are in the following location in the Appliance Manager:

Setup tab > Network > Protocol Tunneling

About protocol tunneling

Used for servicing traffic that NetCache does not support

NetCache supports caching of HTTP, FTP, Gopher, RTSP, MMS, DNS, and NNTP traffic. You can, however, configure your NetCache appliance to service requests for protocols that NetCache does not support by tunneling the requests through the appliance. You might, for example, want NetCache to service traffic such as the following:

- Secure traffic, such as HTTPS, SSL, and SNEWS
- Traffic for protocols that do not support proxying

No browser configuration is required

When you use the protocol tunneling feature, users do not have to configure their browsers to send requests for nonstandard traffic to the NetCache appliance.

When this feature is not applicable

This feature is not for use if users configure their Web browsers or clients to access the NetCache appliance directly.

Note
The HTTP - Tunneling page of the Appliance Manager includes options to support tunneling of HTTP-based traffic to the NetCache appliance when users configure their browsers to point to the appliance.

Used for transparent or nontransparent deployments

You can use the protocol tunneling feature with either a transparent deployment (that is, you use an L4 or L7 switch or WCCP router to direct requests to the NetCache appliance) or a nontransparent deployment (no L4 or L7 switch or WCCP router).

Additional advantages of protocol tunneling

In addition to eliminating the need to configure client browsers in order to send nonstandard requests to the appliance, the protocol tunneling feature offers the following advantages:

- Your firewall can be set up to accept connections from a limited number of IP addresses.

Instead of allowing direct connections to the server from clients, you could configure the firewall to accept requests from the appliance and then route client traffic through the appliance.

- You can log client connections to the server, which is not possible if clients connect directly to the server. (Browsers configured to send traffic to the NetCache appliance issue CONNECT requests.)

  NetCache logs each connection for which it creates a tunnel.

- The NetCache appliance can provide better protection against DOS attacks than if the clients connected directly to the server.

What happens when traffic is tunneled?

With protocol tunneling, NetCache passes through specified types of nonstandard traffic without evaluating or caching it. NetCache examines only the TCP headers for the packet's source and destination and ignores the data. Because with protocol tunneling NetCache does not examine the data in a packet, NetCache does not cache objects resulting from requests serviced by this method, even if the object is cacheable. Instead, NetCache receives the request from the client and passes it through to the Internet, then receives the object from the Internet and passes it through to the client.

NetCache does not authenticate traffic that it is tunneling. Because NetCache does not examine the data in the packet, it is unaware of the protocol associated with the request.

Restrictions

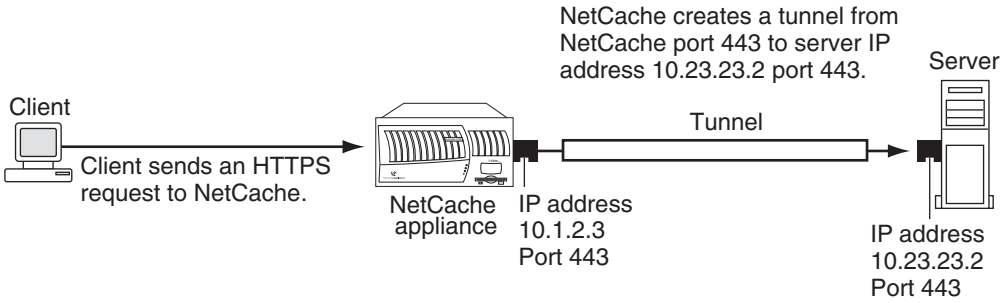
Protocol tunneling has the following restrictions:

- For port 443 traffic, you must configure either the SecureAdmin feature or protocol tunneling, but not both.
- You cannot configure protocol tunneling for any protocol that NetCache supports. If your deployment is transparent, use the NetCache transparent proxying feature to configure NetCache to handle the protocols that it supports.
- You can configure either non-transparent protocol tunneling or transparent protocol tunneling but not both.

Configuration overviews

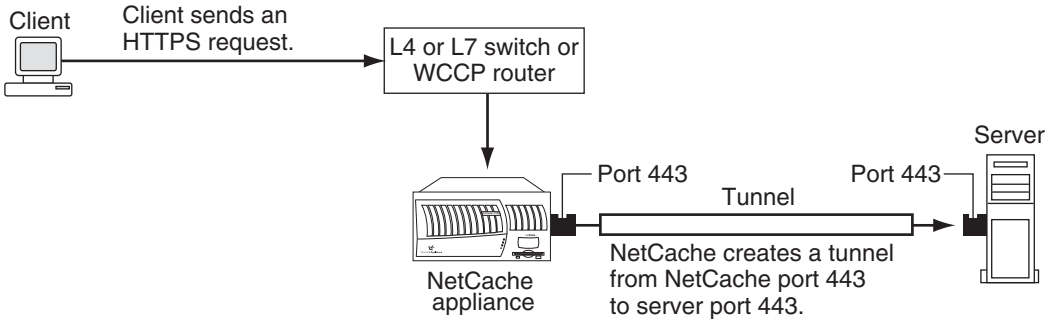
Configuration overview: nontransparent deployment

When protocol tunneling is deployed in a nontransparent environment, the NetCache protocol tunneling feature is configured to listen on a specific NetCache appliance IP address and port for a particular type of nonstandard traffic. When NetCache receives the nonstandard traffic on this IP address and port, NetCache creates a tunnel to the server IP address and server port identified in the protocol tunneling feature. For this type of deployment, you must provide a mapping of a specific NetCache IP address and port pair to a specific server IP address and port pair.



Configuration overview: transparent deployment

When protocol tunneling is deployed in a transparent environment, the L4 or L7 switch or WCCP router is configured to direct traffic for a nonstandard port to the NetCache appliance. The NetCache protocol tunneling feature is configured to listen for traffic on the nonstandard port and to create a tunnel to the server port identified in the protocol tunneling feature when it accepts the nonstandard traffic on the appliance port. For this type of deployment, you must provide a mapping of a specific NetCache port to a specific server port.



If you are deploying transparency with a WCCP router: In a transparent environment, in addition to configuring the protocol tunneling feature, you must perform the following configuration:

- Configure one or more WCCP routers to tunnel the protocols for which you are setting up protocol tunneling through this NetCache appliance.
- In the Appliance Manager, configure a WCCP service group for each protocol that you want tunneled through this NetCache appliance.

See Chapter 11, "Transparent Proxying," on page 137 for more information about setting up WCCP service groups.

If you are deploying transparency with an L4 or L7 switch: Configure the switch to send all traffic for a particular nonstandard port to the NetCache appliance.

NetCache Support for DNS 5

About this chapter

This chapter discusses setting up a NetCache appliance for host name resolution and for optional NetCache features for DNS.

Topics in this chapter

This chapter contains the following topics:

- Section A, "Planning summary for DNS configuration," on page 50
- Section B, "Basic DNS configuration on a NetCache appliance," on page 52
- Section C, "Optional DNS configuration," on page 53

Procedures and option descriptions

See the Appliance Manager online Help for configuration procedures and option descriptions.

Location of configuration options

Options for configuring the features discussed in this chapter are in the following location in the Appliance Manager:

Setup tab > DNS > General

Section A: Planning summary for DNS configuration

Determine DNS configuration

Configuring DNS will be faster if you plan ahead. Use the information in the following table to determine the DNS configuration that is necessary for your organization.

Decisions to make	Your options	Considerations
Whether you need to change basic DNS configuration	Appliance Domain DNS Nameservers	Typically organizations do not change nameservers and appliance domain. However, if the DNS nameservers that your NetCache appliance is to use changes, or the appliance is moved and, therefore, its domain name changes, you can change this information in the NetCache configuration.
Whether you need support for domain names that are not fully qualified	DNS Tree-Search Enable DNS Search Paths	System administrators of enterprises should consider configuring NetCache to handle domain names that are not fully qualified. ISPs usually do not need to configure support for domain names that are not fully qualified because their users typically enter fully qualified domain names in URLs.
Whether it is beneficial to reduce the number of DNS lookups performed by remote DNS nameservers	Hosts File	Typically, you add entries to this option only if you have a special requirement to bypass the DNS nameserver.

Decisions to make	Your options	Considerations
Whether you want clients to send DNS queries to the NetCache appliance instead of directly to DNS nameservers	DNS caching options	If the NetCache appliance is configured to function as a DNS proxy cache, the appliance can resolve a DNS query without contacting the DNS nameserver if the appliance has the host name to IP address mappings in its cache.
Whether you need to support internal resolvers that cannot handle external host names	Two methods are available: ◆ Split DNS ◆ Per Domain mapping (Domain-to-Nameserver-Mapping option)	Runtime issues and configuration requirements differ for the two methods. You must consider both issues when determining the right strategy for your organization. See “Supporting internal resolvers that cannot handle external host names” on page 61 for more information.
Whether you need to reduce the load of DNS queries on your organization’s internal resolvers	DNS iterative resolution options	When this feature is enabled, NetCache functions as a full-service resolver.
Whether you need DNS records in the NetCache DNS cache to expire before the server-assigned TTL expires	Per-Domain TTL Expiration option	In a DHCP-DDNS environment in which IP addresses are dynamically assigned, you might want to expire DNS records in the NetCache DNS cache before the server-assigned TTL expires.

Section B: Basic DNS configuration on a NetCache appliance

Required configuration to support DNS

The NetCache appliance uses DNS to resolve host names. The following information must be provided to ensure NetCache support of DNS:

- NetCache host name
- NetCache domain name
- DNS nameservers to which NetCache can send requests for name resolution

The first time the NetCache appliance boots, NetCache broadcasts a request to the network to determine whether a DHCP server is available to provide specific information about the network. If a DHCP server replies, NetCache accepts the following information from the DHCP server, if the DHCP server has been configured to provide it:

- IP address
- Default gateway
- NetCache domain name (Appliance domain name)
- DNS nameservers

NetCache provides this information as default settings during the setup program.

If a DHCP server is not available, you are prompted for this DNS information during the NetCache setup program. You can change any of these settings later, if necessary, on the DNS - General page in the Appliance Manager. To access this page, select Setup tab > DNS > General.

Failover of nameservers

Entering multiple nameservers in the NetCache DNS configuration provides failover capability if a nameserver is unavailable.

Section C: Optional DNS configuration

About this section

This section provides information to help you determine the optional DNS configuration features that you might want to use for your organization.

Topics in this section

This section contains the following topics:

- "NetCache as a DNS proxy cache" on page 54
- "Handling domain names that are not fully qualified" on page 56
- "Handling DNS lookups for local servers" on page 60
- "Supporting internal resolvers that cannot handle external host names" on page 61
- "Using NetCache as a full-service resolver" on page 64
- "Reducing the time that DNS records are cached" on page 67

NetCache as a DNS proxy cache

Problems with querying DNS nameservers

Typically, clients send DNS queries to a DNS nameserver for host name resolution. Common complaints about queries to DNS nameservers are as follows:

- DNS lookups are slow because nameservers are overloaded.
- If a DNS nameserver is not located close to a client, significant bandwidth can be consumed by sending DNS queries to remote servers.
- Nameservers are often misconfigured with incorrect entries.

How DNS caching works

You can expand the DNS capability of NetCache by configuring a NetCache appliance to function as a DNS proxy cache for use by clients. Clients send DNS queries to the NetCache appliance. If the appliance has the host name to IP addresses mapping in its cache, it can resolve the DNS query without contacting the DNS nameserver. If the appliance cannot resolve a DNS query, it contacts a DNS nameserver to resolve the query, caches the host name and IP addresses resulting from the query, and returns the host's IP addresses to the client.

Note

NetCache always caches the results of lookups that it initiated and sent to a DNS nameserver. (DNS nameservers are identified in the Nameservers option on the DNS - General page in the Appliance Manager.) NetCache then serves the host's IP address for NetCache internal processes without having to query the DNS nameserver with subsequent requests for the same host name. This type of DNS caching is not configurable.

Advantages of NetCache as a DNS cache for clients

The advantages of enabling DNS caching on a NetCache appliance are as follows:

- Reduced load on remote nameservers because the NetCache appliance can perform DNS name lookups on their behalf
- Reduced response time for DNS lookups when a NetCache appliance is deployed closer to the clients than the nameservers
- Reduced bandwidth usage

What NetCache caches

NetCache caches the results of A (answer) type and PTR (pointer) type queries, the result of which can contain the following:

- A host name to IP addresses mapping
- A CNAME record, which represents the aliases for a given host name
- An IP address to host name mapping
- A PTR record, which represents the aliases for a given host name

DNS cache is only in memory

NetCache saves the results of A type queries only in memory. When the NetCache appliance reboots, the DNS cache is cleared.

What NetCache proxies

NetCache proxies all non-A type and non-B type queries to the DNS nameserver on behalf of the client.

Requirement if the client access method is nontransparent

You can set up DNS caching regardless of the method that you have set up for clients to access the NetCache appliance. However, if your organization's client access method to this NetCache appliance is nontransparent, you must do the following in addition to enabling DNS caching:

- For UNIX, add the NetCache appliance to the list of nameservers in the *etc/resolv.conf* file on the client.
- For Windows NT, add the NetCache appliance to the Control Panel > Network > Protocols dialog box.
- For other operating systems, see your operating system documentation.

Length of time DNS lookups remain in the DNS cache

For a given response to a DNS query, NetCache saves the shortest expiry time of all the records in the response as the expiration time.

Handling domain names that are not fully qualified

Whether you need to handle domain names that are not fully qualified

If you expect that users will enter domain names that are not fully qualified, you should configure NetCache to handle such names. Users in enterprises usually know that they can enter partially qualified domain names in URLs. Therefore, system administrators of enterprises should consider configuring NetCache to handle domain names that are not fully qualified.

ISPs, as a rule, do not need to configure support for domain names that are not fully qualified because their users typically enter fully qualified domain names in URLs.

Options for handling domain names that are not fully qualified

The following options on the DNS - General page in the Appliance Manager can be configured to handle domain names that are not fully qualified:

- DNS Tree-Search Enable

  Enables and disables NetCache performing a domain tree search for DNS lookups. When this option is enabled, NetCache uses the paths specified in the DNS Search Paths option, and DNS lookups occur even if the domain name is fully qualified. Keep in mind that a domain-tree search can generate a large amount of network traffic if the servers for the listed domains are not local.

- DNS Search Paths

  Identifies the paths that NetCache should follow when trying to resolve a host name. NetCache follows the order in which the search paths are listed in this option, from the top to the bottom of the list.

Extra DNS lookups can occur with DNS tree searching

By default, when NetCache looks up a domain name in its DNS cache, NetCache first attempts to look up the domain name with the local domain name appended, even if the requested domain name is fully qualified. If the first lookup fails, the NetCache DNS resolver then performs a lookup without the local domain name appended. The result is that the resolver performs an extra lookup when the URL contains a fully qualified domain name.

Note

The concept of fully qualified differs between DNS and most application-level protocols. For DNS, a domain name is fully qualified only if a dot appears at the end of the domain name. For example, although www.books.com appears to be a fully qualified URL, it is not fully qualified according to the DNS specification because no dot appears at the end. For this reason, NetCache appends the local domain name to the domain name.

Deciding whether to enable the DNS Tree-Search Enable option

If you expect that your users will always provide fully qualified domain names, Network Appliance recommends that you do not enable the DNS Tree-Search Enable option. The reason is that when the DNS Tree-Search Enable option is enabled, a DNS lookup occurs even if the domain name is fully qualified.

Avoiding an extra DNS lookup can be beneficial for the following reasons:

- A domain tree search can be slow.
- A domain tree search generates a large amount of network traffic if the servers for the listed domains are not local.
- Queries time out if no server is available for one of the domains.

What occurs when the DNS Tree-Search Enable option is enabled

The following table describes what occurs for domain names when the DNS Tree-Search Enable option is enabled. Assume for this example that the local domain is books.com and a valid host name is web.books.com.

If the domain name in the URL is...	Then...
Unqualified (that is, it does not contain dots). For example: web	If the unqualified domain name is web, for example, and the DNS Tree-Search Enable option is enabled, the first lookup is for web.books.com, which succeeds.

If the domain name in the URL is...	Then...
Partially qualified. For example: web.books	If the partially qualified domain name is web.engr, for example, the following occurs: **1.** books.com is appended to the domain name so that the lookup is on web.books.books.com. This lookup fails. **2.** NetCache then tries web.books.com. This lookup succeeds.
Fully qualified. For example: web.books.com	If a URL contains the fully qualified domain name web.books.com, for example, the following occurs when the DNS Tree-Search Enable option is enabled: **1.** books.com is appended to the domain name so that the first lookup is for web.books.com.books.com. This lookup fails. **2.** The second lookup is for web.books.com.com. This lookup fails. **3.** The third lookup is for web.books.com. This lookup succeeds.

What occurs when the DNS Tree-Search Enable option is disabled

The following table describes what occurs for domain names when the DNS Tree-Search Enable option is disabled. Assume for this example that the local domain is books.com and a valid host name is web.books.com.

If the domain name in the URL is...	Then...
Unqualified (that is, it does not contain dots). For example: web	The local domain name is not appended to the domain name in the URL. This lookup fails.

If the domain name in the URL is...	Then...
Partially qualified. For example: web.engr	The local domain name is not appended to the domain name in the URL. The lookup of a partially qualified domain name fails right away. For example, web.engr is looked up as web.engr, and the lookup fails.
Fully qualified. For example: web.books.com	The DNS lookup succeeds the first time.

About identifying DNS search paths

By configuring the DNS Search Paths option, you increase the probability that NetCache can successfully resolve a host name if the domain name in the URL is not fully qualified. The reason is that NetCache can expand its search beyond the local domain. When the DNS Search Paths option is configured, NetCache tries to resolve the host name by searching in the following order:

1. NetCache domain name
2. Search paths in this option, from the top to the bottom of the list

Identify DNS search paths if you have enabled the DNS Tree-Search Enable option.

Note

Network Appliance recommends that you determine the most commonly looked-up host names and list those first. The reason is that NetCache does not continue searching after it makes a match (which optimizes performance).

Handling DNS lookups for local servers

About reducing DNS lookups on remote DNS nameservers

You might be able to reduce the number of DNS lookups performed by remote DNS nameservers by entering local host names and their associated IP addresses in the Hosts File option on the DNS - General page. Configuring the Hosts FIle option enables your NetCache appliance to handle DNS lookups for local servers. As a result, you do not need to configure host names and IP addresses for your local servers on remote DNS nameservers.

When to add entries to the Hosts File option

Typically, you do not need to add entries to the Hosts File option. Add entries to this option only if you have a special requirement to bypass the DNS nameserver.

For example, if you do not want to export DNS information to a DNS nameserver, you can add the host name and IP address to the Hosts File option. If you are setting up this NetCache appliance as a Web accelerator, you could, for example, add entries to this option for the Web servers that the appliance is accelerating. The DNS lookup would then be performed on the NetCache appliance, eliminating the need for a DNS lookup on a remote DNS nameserver.

Note

The DNS caching feature ignores entries input for the Hosts File option. Only DNS data actually fetched from a DNS nameserver is cached to support the DNS caching function.

What NetCache checks first for DNS host name resolution

When NetCache tries to resolve a host name, it checks the local DNS cache first, then checks the entries in the Hosts File option. NetCache sends DNS queries to the remote DNS nameserver only if it cannot resolve the host name from the DNS lookup of the entries in the Hosts File option.

Supporting internal resolvers that cannot handle external host names

Features available

If your organization's internal resolvers cannot handle external host names, you can use one of the following NetCache features to ensure that requests can be sent to DNS nameservers external to your organization:

- Split DNS

  Split DNS enables an enterprise administrator to split the DNS nameservers that the NetCache appliance queries into an internal group and an external group.

  Note
  The NetCache Split DNS feature is a customized feature for NetCache. It is not the same as the BIND Split DNS feature.

- Per Domain mapping (Domain-to-Nameserver-Mapping option)

  With this option, you configure NetCache to query a specific nameserver or set of nameservers based on the domain that is being queried.

Deciding which method is appropriate

Each organization must judge the significance of work versus runtime issues when determining the best method to use for ensuring that requests can be sent to DNS nameservers external to the organization.

Restrictions for using Split DNS: Consider using Split DNS only if all of the following are true:

- Internal nameservers can resolve *only* internal host names.
- You cannot or do not want to reconfigure your internal nameservers to resolve external host names in addition to internal host names.
- Your internal resolvers handle multiple internal domains.

Comparison of configuration and runtime issues: When making your decision about whether to use Split DNS or Per Domain mapping, you should consider the amount of work required to configure each feature and the effect of each feature at runtime. The following table compares these two features.

Split DNS	Per Domain mapping
Configuration	
Easier to configure because you do not have to list all internal domains that the internal nameservers resolve. If your internal nameservers handle a large number of domains, using Split DNS instead of Per Domain mapping can save you considerable configuration time.	More work to configure because you must list all internal domains that the internal nameservers resolve.
Runtime issues	
With Split DNS, the appliance queries the internal nameservers first. If the queries to the internal nameservers are not resolved, the appliance queries the external nameservers. Internal nameservers, therefore, will need to handle the load of queries for both internal and external host names. Each organization must judge whether the runtime penalty is significant for the organization.	Your configuration provides a mapping of domains to external nameservers. Based on your configuration, NetCache sends queries for external host names directly to the external nameservers. Therefore, no runtime penalty exists for the internal nameservers or the appliance.

Relevant options, by feature

The options applicable to each feature discussed in this section are shown in the following table. See the Appliance Manager online Help for the DNS - General page (Setup tab) for details about configuring the relevant options.

Feature	Options to use on the DNS - General page
Split DNS	Nameservers Split DNS Enable Split DNS Nameservers
Per Domain mapping	Domain-to-Nameserver-Mapping

Split DNS example

Assume that FooBar Corporation has one DNS domain named foobar.com, and that it uses the subnet 10.0.0/24 internally. They have two sets of DNS resolvers, as follows:

- Internal set of resolvers (which resolve only internal host names)

  internal-ns1.foobar.com (10.0.0.1)

  internal-ns2.foobar.com (10.0.0.2)

  internal-ns3.foobar.com (10.0.0.3)

- External set of resolvers

  external-ns1 (100.0.0.1)

  external-ns2 (100.0.0.2)

  external-ns3 (100.0.0.3)

The previous configuration enables the NetCache appliance to resolve both the internal and external names when configured with the Split DNS feature.

Using NetCache as a full-service resolver

About DNS iterative resolution

The DNS iterative resolution feature enables the NetCache full-service resolver (as specified in RFC 1123). The full-service resolver resolves DNS host names on the Internet through *iterative* queries by traversing the DNS hierarchy. That is, if the DNS server to which NetCache sends the query cannot resolve it, that DNS server takes the responsibility for forwarding the query to another DNS server. The query is forwarded "down" from the root DNS nameserver until the query is resolved.

The full-service resolver caches the results of its queries in the NetCache nameserver cache. NetCache uses cached results to speed lookups.

NetCache behavior if the full-service resolver is not enabled

If the full-service resolver is not enabled, NetCache uses its stub resolver to perform *recursive resolution*. With recursive resolution, if the DNS server to which NetCache sends a query responds that it cannot resolve the query, NetCache sends the query to a different DNS server. NetCache continues to try different DNS nameservers (one at a time) until the query is resolved.

When to enable DNS iterative resolution

Enable the full-service resolver (DNS iterative resolution) when you need to reduce the load on your company's internal resolvers. The reason is that the appliance then resolves the majority of host names for the Internet itself.

For Global Request Manager, you can reduce the query load on the back-end nameservers by enabling the DNS Iterative Resolution feature and using it in combination with the Nameserver-to-Domain Mapping option (located on the DNS - General page in the Appliance Manager).

How the full-service resolver resolves queries

When the NetCache full-service resolver is enabled, the default behavior is that the resolver resolves all queries iteratively except lookups for private IP addresses. Lookups for private IP addresses are always resolved recursively. The reason is that it is assumed that lookups for private IP addresses are local (most companies have private IP addresses). Using iterative resolution for queries outside the company helps to reduce the load on the company's internal DNS nameservers.

Relevant options for DNS iterative resolution

The following configuration options on the DNS - General page (Setup tab) in the Appliance Manager are used to configure DNS iterative resolution:

- Iterative Resolution Enable: Enables the NetCache full-service resolver (the DNS iterative resolution feature)
- Iterative Resolution Forward Query Rules
- Iterative Resolution Reverse Query Rules

Most companies do not need to configure the Iterative Resolution Forward Query Rules and Iterative Resolution Reverse Query Rules options. The reason is that the NetCache full-service resolver's default behavior alleviates the load on company internal DNS servers. See "When you must set forward or reverse query rules" on page 66 for more information.

Syntax for DNS iterative resolution query rules

The following table shows the syntax for the DNS iterative resolution query rules.

Option name	Syntax
DNS Iterative Resolution Forward Query Rules	{iterate|recurse} [!] dnsdomain.
DNS Iterative Resolution Reverse Query Rules	{iterate|recurse} [!] subnet

{iterate|recurse}
Specifies whether the query will be iterative or recursive.

[!]
Specifies that the iterative or recursive query be carried out on the following:

- DNS domains, except those specified by the dnsdomain parameter (for a forward query rule)
- Subnets, except those specified by the subnet parameter of this rule (for a reverse query rule)

dnsdomain.
(Forward query rule) Domain name suffix (for example, .org, .com, and .co.uk.) of the host name to be resolved. Network Appliance recommends terminating the domain name suffix specification with a period (.).

subnet
(Reverse query rule) Subnet IP address to be resolved.

When you must set forward or reverse query rules

You must set one or more query rules for DNS iterative resolution in the following circumstances:

- Your company has more than one internal domain.
- Your company uses globally routeable IP addresses internally.

About rule requirements if a company has more than one internal domain: If your company has more than one internal domain, you must list all internal domains in a forward query rule.

For example, if Widget Company uses the domains widget.com, widget.fr, widget.jp internally, then you would list the domains in a forward query rule as follows:

Type of rule	Setting

DNS Iterative Forward Query Rule	`recurse widget.com.`
	`recurse widget.fr.`
	`recurse widget.jp.`

About rule requirements if a company uses globally routable IP addresses internally: If your company uses globally routable IP addresses internally, you must set a reverse query rule.

The NetCache full-service resolver default behavior is to resolve all queries iteratively except queries for private IP addresses. Therefore, if you are using a globally routeable IP address internally, you must explicitly instruct NetCache that it is a local address.

For example, if Widget Company uses the IP address range 136.43.85.024 and 206.41.0.0/16 internally, you would set the rules as follows:

Type of rule	Setting
DNS Iterative Reverse Query Rule	`recurse 136.43.85.0/24` `recurse 206.41.0.0/16`

Reducing the time that DNS records are cached

Expiration of DNS records before TTL expiration

By default, NetCache honors the TTL that the server specifies and does not expire the DNS record in the NetCache DNS cache until after the server-specified TTL expires. The assumption is that the mapping between the IP address and host name in the appliance DNS cache is correct until that TTL expires. However, in some cases, the mapping might not be correct for the duration of the TTL. The Per-Domain TTL Expiration option enables you to set NetCache to expire the DNS records in its cache for the domains that you specify before the TTL expires.

For example, in environments that use DHCP (Dynamic Host Configuration Protocol) servers and DDNS (Dynamic DNS) servers to dynamically assign IP addresses, a client that was dynamically assigned an IP address might release that IP address before the server-specified TTL expires. When this event occurs, the DHCP server and the DDNS server are automatically updated, and the DHCP server can assign that released IP address to another client. The record in the appliance DNS cache is not updated until after the TTL expires.

To maintain consistency between the DDNS server and the appliance DNS cache, you must force the expiration of the DNS records in the appliance's DNS cache before the TTL expires. The Per-Domain TTL Expiration option forces expiration of DNS records for a specified domain after 15 seconds.

Examples of entries

Assume that the Widget Company's wireless laptops are managed by DHCP. The laptops are assigned addresses in the range 10.23.64.0/24, and these IP addresses are in the wireless.widget.com subdomain. You would enter domain names or in-addr.arpa format domain names rather than IP addresses in CIDR format.

The Per-Domain TTL Expiration option settings are as follows:

```
.wireless.widget.com.
.64.23.10.in-addr.arpa.
```

For the domains listed in this option, NetCache will expire the DNS records in its cache after 15 seconds.

Managing Disks 6

About this chapter

This chapter describes disk management on NetCache appliances. The information in this chapter covers disk management on NetCache appliances that support RAID (Redundant Array of Independent Disks) Level 4.

Note

NetCache appliance single-disk and internal drive systems do not support RAID Level 4 disk management.

Sections in this chapter

This chapter contains the following sections:

- Section A, "RAID on the NetCache appliance," on page 70
- Section B, "RAID disk management on the NetCache appliance," on page 82
- Section C, "Reinitializing all disks," on page 89

Procedures and option descriptions

See the Appliance Manager online Help for configuration procedures and option descriptions.

Location of configuration options

Options for configuring the features discussed in this chapter are in the following location in the Appliance Manager:

Maintenance tab > Disk > Management

Additional options related to disks are located in the following location:

Maintenance tab > Disk > Firmware

Maintenance tab > Disk > Qual Devices

Section A: RAID on the NetCache appliance

About this section

This section contains information about RAID Level 4, different types of disks used in RAID, disk addressing, usable space on disks in the RAID group, and handling disk failures on your appliance.

Topics in this section

This section contains the following topics:

- "Understanding RAID and disks" on page 71
- "Disk addresses" on page 74
- "Disk space on each disk" on page 76
- "Disk sizes and capabilities" on page 77
- "Handling disk failure" on page 79

Understanding RAID and disks

About RAID

NetCache appliances use RAID Level 4 (RAID-4) to ensure data integrity even when one of the disks fails. The file system design, together with the support for RAID, optimizes appliance performance and enables you to expand the appliance's disk storage capacity incrementally.

The RAID disk structure on your appliance is factory-installed; you do not need to configure the storage system before using the appliance. However, when planning to optimize disk space or when replacing or adding disks, you must be familiar with how the appliance uses its disk array.

Disk functions in a file system

In the RAID-4 file system, different disks have different functions. Most of the disks are *data disks*. One disk in the array is the *parity disk*, which enables the appliance to recover the data on a data disk if one fails. You can also install one or more disks to be used as *hot spares* in the event of disk failure.

Data disks: *Data disks* are those on which cached objects, logs, and other data are stored.

Parity disks: After a data disk failure, the appliance uses the *parity disk* in conjunction with the other data disks to reconstruct the failed disk's data and write it to a hot spare disk. The parity disk must be at least as large as the largest data disk. For each 28 disks added to an appliance, one drive is used for parity.

For more information about how the appliance recovers from disk failures by using the parity disk or hot spare disk, see "Handling disk failure" on page 79.

Hot spare disks: In addition to data and parity disks, you can install one or more *hot spare disks* in the appliance. A hot spare disk is not part of the RAID disk array and does not contain cached objects. After a disk failure, the appliance automatically rebuilds data onto a hot spare disk, which then replaces the failed disk in the RAID array. Using a hot spare disk avoids a system shutdown and returns the system to full performance.

A hot spare disk cannot replace a failed disk that is larger than itself. If you use only one hot spare disk in an appliance, the hot spare disk must be as large as the largest file system disk. If you have multiple hot spare disks installed, the system uses the smallest hot spare disk needed to replace the failed disk.

Hot swapping disks: Some models of the appliance allow you to *hot swap* disks. Hot swapping a disk means installing or removing it from the disk shelf while the appliance is running with minimal interruption to the appliance service. For example, you might want to hot swap a disk into an appliance to replace a disk or to add a hot spare disk.

Note

NetCache appliance single-disk and internal disk systems do not support hot swapping of disks.

Internal and external disk tray systems

An appliance with an internal disk tray is a closed system in which the disk or disks are not easily accessible. An appliance with an external disk tray or disk trays is a system in which the disk drives are exposed for easy access.

Platform support of RAID and internal disk trays

The following table describes appliance support of RAID and internal disk trays.

RAID/internal disk trays	Supported platforms
RAID-4 (multi-disk) with NVRAM ◆ Enables file systems and cache contents to survive disk failures ◆ Ensures parity ◆ Lets system run in degraded mode ◆ Enables hot swap and reconstruction of a failed drive ◆ Enables proper handling of disk media errors	C2100, C3100, and C6100
RAID-4 (multi-disk) with SVRAM ◆ Enables file systems and cache contents to survive disk failures ◆ Ensures parity ◆ Lets system run in degraded mode ◆ Enables hot swap and reconstruction of a failed drive ◆ Enables proper handling of disk media errors	C1200

RAID/internal disk trays	Supported platforms
RAID-0 (single disk)	C1100, C1105, and C1200
Internal disk trays	C1100 and C1105

RAID-4 support for C1200 NetCache appliance

The C1200 NetCache appliance is available with RAID-4 (multi-disk) or RAID-0 (single-disk) support. The C1200 RAID-4 features SVRAM, which enhances the reliability of this NetCache platform.

The C1200 RAID-4 support provides parity for error checking and correction, whereas the C1200 single-disk system uses the disk for data only.

For more information, see "Available C1200 disk roles and capabilities" on page 78.

RAID-4 degraded mode

RAID-4 support enables the appliance to continue running in certain failure situations but in a degraded mode.

For more information about the degraded mode, see "Running in degraded mode" on page 79.

Disk addresses

About disk addresses

You identify a disk by its address, which is listed in the Disk ID column of the Disk - Management page (Maintenance tab > Disk > Management) of the Appliance Manager. The Disk ID is represented in *x.y* format, where *x* refers to the host adapter and *y* refers to the disk ID number.

You use the disk address to do the following:

- Interpret system messages (for example, command output or error messages) that you see on your screen
- Locate a disk to which a system message refers

Locating a disk by its identifier

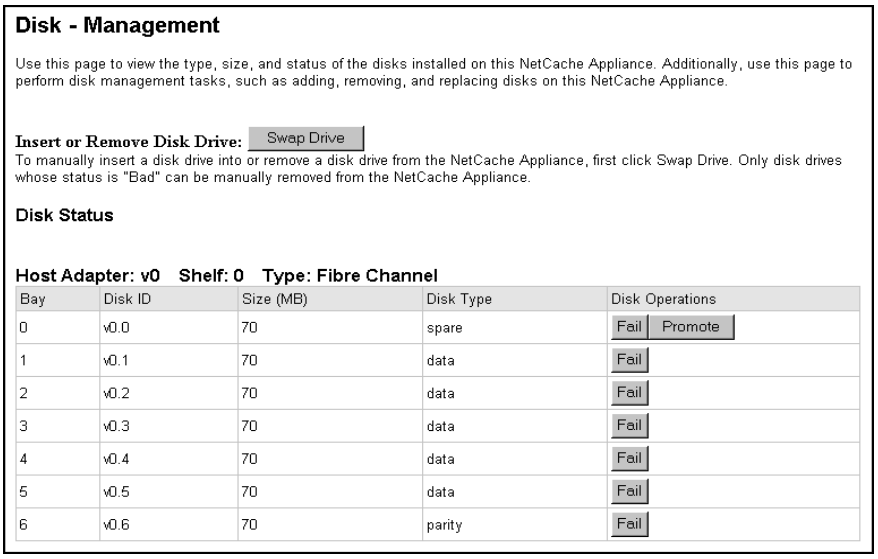
Use the Disk - Management page (Maintenance tab > Disk > Management) of the Appliance Manager to display disk information about all the disks on your appliance. This page lists the disk ID, the type (data, parity, or spare), the size, and the current status of every disk on your appliance.

Note

The Appliance Manager does not display the Disk - Management page for single disk appliances.

This information is useful when you need to locate a disk referenced by the RAID disk number in a system message.

The following is an example of the Disk - Management page output.



Disk - Management

Use this page to view the type, size, and status of the disks installed on this NetCache Appliance. Additionally, use this page to perform disk management tasks, such as adding, removing, and replacing disks on this NetCache Appliance.

Insert or Remove Disk Drive: Swap Drive

To manually insert a disk drive into or remove a disk drive from the NetCache Appliance, first click Swap Drive. Only disk drives whose status is "Bad" can be manually removed from the NetCache Appliance.

Disk Status

Host Adapter: v0 Shelf: 0 Type: Fibre Channel

Bay	Disk ID	Size (MB)	Disk Type	Disk Operations
0	v0.0	70	spare	Fail Promote
1	v0.1	70	data	Fail
2	v0.2	70	data	Fail
3	v0.3	70	data	Fail
4	v0.4	70	data	Fail
5	v0.5	70	data	Fail
6	v0.6	70	parity	Fail

SCSI disk addresses

For SCSI disks, the Disk ID is a combination of the disk's SCSI adapter number and the disk's SCSI ID number. For example, disks attached to disk adapter 0 are number 0.0 through 0.6.

Fibre channel disk addresses

For fibre channel disks, the Disk ID is a combination of the disk's adapter number and disk's fibre channel loop ID. To create the fibre channel loop ID, multiply shelf ID by eight and add it to the bay number. For example, host adapter 8, shelf 1, disk 2 has disk ID of 8.10.

Disk space on each disk

About usable disk space

A disk's *usable* space can be different from its *physical* space. Disks from different manufacturers might differ slightly in size even though they belong to the same size category. To ensure that you can replace a disk from one manufacturer with a disk from another manufacturer, the NetCache software automatically "right-sizes" its disks.

The appliance manages disk space so that objects never entirely fill the usable space. The following table shows the approximate usable disk space for each class of disk supported by the appliance.

Disk class	Usable disk space
1-GB disks	1,000 MB (2,048,000 blocks)
2-GB disks	2,000 MB (4,096,000 blocks)
4-GB disks	4,000 MB (8,192,000 blocks)
9-GB disks	8,600 MB (17,612,800 blocks)
18-GB disks	17,000 MB (36,864,000 blocks)
36-GB disks	34,500 MB (70,656,000 blocks)
72-GB disks	68,000 MB (139,264,000 blocks)

Overwriting-objects policy

The appliance uses a first-in, first-out (FIFO) replacement policy for writing cache objects. The FIFO policy operates by tracking inodes and using object ejection (truncation) to manage space. This process takes place asynchronously during the serving of requests. When a disk reaches its upper capacity, objects are ejected until there is sufficient space to record new objects.

Disk sizes and capabilities

Using disks of various sizes

Guideline for using fibre channel disks of various sizes: You can use fibre channel disks of various sizes with the same appliance, up to and including 18-GB, 36-GB, and 72-GB disks. However, unlike Network Appliance filers, the NetCache appliance does not support mixing fibre channel disks of different sizes in the same disk enclosure; they must be in separate enclosures.

The following table shows a sample configuration.

Enclosure	Data	Data	Parity	Hot Spare
Enclosure 1	Disk 0 (9-GB)	Disk 1 (9-GB)	Disk 2 (9-GB)	Disk 3 (9-GB)
Enclosure 2	Disk 0 (18-GB)	Disk 1 (18-GB)	Disk 2 (18-GB)	Disk 3 (18-GB)

Guideline for using SCSI disks of various sizes: You can use SCSI disks of various sizes with the same appliance, up to and including 18-GB, 36-GB, and 72-GB disks. Additionally, the appliance does not support mixing SCSI disks of different sizes in the same SCSI backplane.

The following table shows a sample configuration.

Backplane	Data	Data	Parity	Hot Spare
Backplane 1	Disk 0 (9-GB)	Disk 1 (36-GB)	Disk 2 (9-GB)	Disk 3 (18-GB)
Backplane 2	Disk 0 (9-GB)	Disk 1 (72-GB)	Disk 2 (18-GB)	Disk 3 (18-GB)

Available C1200 disk roles and capabilities

The following scenarios describe various disk configurations that are available on the C1200 system.

Note

On the C1200 system, 36-GB and 72-GB size disks are available. The following table shows examples for 72-GB disks.

Disks/size	Configuration	Result
Single disk — 72-GB	RAID-0: 1 data = 72-GB raw capacity	Lowest cost, no redundancy. If a disk fails, you swap the disk (or in the case of the C1100 or C1105 models, the appliance itself). **Caution** If a disk fails, a full shutdown, power off, and reinstallation of software and licenses are required. All data is lost from the disks.
Multi-disk — two disks, 72-GB	RAID-4: 1 data + 1 parity mirrored = 72-GB raw capacity	Redundancy. If a disk fails, the appliance will still run but it will run in degraded mode. For details, see “Running in degraded mode” on page 79.
Multi-disk — three disks, 72-GB	RAID-4: 1 data + 1 parity + 1 hot spare = 72-GB raw capacity	Highest reliability. If a disk fails, the appliance will still run, and the hot spare disk will be automatically promoted to the active file system, replacing the failed disk. If another disk fails after that process is complete, the appliance will enter degraded mode and behave like a two-disk system.
Multi-disk — three disks, 72-GB	RAID-4: 2 data disks + 1 parity = 144-GB raw capacity	Higher capacity with redundancy. If a disk fails, the appliance will enter degraded mode and behave like a two-disk system.

Handling disk failure

About disk failure

The effects of a disk failure on the appliance operation depend on whether or not the appliance is equipped with a hot spare. In either case, during a disk failure situation, an appliance will run in a degraded mode until the cause is remedied or shut down occurs.

Running in degraded mode

RAID-4 support enables the appliance to continue running in certain failure situations but in a degraded mode.

The appliance will enter degraded mode if either of the following conditions exist:

- Low NVRAM battery—NVRAM support fails. This condition occurs when the battery that provides power to the NVRAM card becomes low.
- Degraded RAID group—Single-disk failure. This condition occurs when a single disk, either data or parity, fails in a multi-disk system.

While running in degraded mode, the appliance will continue to run without losing data, but with the following reductions in performance:

- Reduced risk protection due to the failed component
- Calculation of parity for READS only
- Entering proxy-only mode after 24 hours
- Shutting down after 120 hours

When the appliance is rebooted, the countdown starts again. If the degraded mode condition is alleviated, the appliance will return to a fully functioning state and cease proxy-only mode (if the appliance had entered this mode).

Note

The appliance will panic if it enters double-degraded mode; that is, the appliance experiences both low-battery and degraded RAID group conditions. A double disk failure will also panic the appliance.

For more information about disk failures, see Chapter 16, “Troubleshooting,” on page 279.

Disk failure with a hot spare

If the appliance has a hot spare installed, the system enters degraded mode after a single disk failure. In this state, the RAID feature enables the appliance to continue to run without losing data, although the appliance's performance is affected.

Note

NetCache appliance single-disk and internal disk systems do not support hot spare disks or the hot-swapping feature described in this section.

The appliance logs this activity in the Messages log and does not automatically shut down. If you power off the appliance while it is in degraded mode, it stops data reconstruction. After you power on the appliance again, it restarts the data reconstruction process from the beginning.

Except for a slight loss in performance while data is rebuilt on the spare disk, the failure of a single disk is transparent to the user. The appliance exits degraded mode and returns to normal operation after it finishes reconstructing data.

Network Appliance recommends that you replace the failed disk with a new hot spare after the appliance has finished reconstructing data. This way, the appliance continues to have a hot spare that can be used in case another disk fails.

The Disk - Management page (Maintenance tab > Disk > Management) in the Appliance Manager displays which disk is reserved as the hot spare.

In addition to logging disk failure and hot spare replacement activity, the Messages log on the Log Files - Messages page (Data tab > Log Files > Messages) logs any failure in the periodic check of the hot spare.

Disk failure without a hot spare

If the appliance is not equipped with a hot spare, when a disk fails, the appliance enters degraded mode. In this state, the RAID feature allows the appliance to continue to run without losing data, although the appliance's performance is affected.

Note

The disk failure process described in this section does not apply to C1100 or C1105 appliances, for which disk replacement is not an option.

In consideration that many appliance installations are in remote locations and that failures in such locations might not be easily corrected, the system continues to run in degraded mode, but shuts down every 120 hours of operation. This applies to all NetCache appliance platforms.

Caution

Replace the failed disk as soon as possible. A second disk failure will cause the entire cache of objects to be lost, and you will have to reinstall the file system.

When a disk fails, the appliance logs one of the following warning messages in the Messages log:

```
Parity disk in x, RAID group y, is broken. Halting in m hours.
```

```
Data disk in volume x, RAID group y, is broken. Halting in m hours.
```

(In the actual message, *x* is the volume number, *y* is the RAID group number, and *m* is the number of hours before the system halts.)

In addition, every hour thereafter, a message similar to the following is sent to the Messages log and the system console:

```
Wed Aug 28 16:00:00 PDT
[monitor.shutdown.brokenDisk.pending:warning]: data disk in RAID
group /vol0/plex0/rg0 is broken. Halting system in 120 hours.
```

What happens to the data on the failed disk: If no hot spare disk is available, the failed disk data will not be reconstructed but will be inaccessible until you replace the failed disk. The failed disk data is reconstructed on the new disk.

What happens with a double disk failure: If a second disk fails while the appliance is operating in degraded mode, or if two disks fail at once, the file system is damaged and cannot be repaired. You must then reinstall the appliance software and restore the configuration from a backup. For more information, see Chapter 16, "Troubleshooting," on page 279 and the topics on backing up and restoring a system configuration file in the Appliance Manager online Help.

What happens when the parity disk fails: When the parity disk fails, the appliance operates in degraded mode until you replace the failed disk. After you have installed a replacement disk, the appliance uses the information on the data disks to rebuild the parity information onto the replacement disk.

Recovering from disk failure

When the degraded mode condition is alleviated, the appliance will return to a fully functioning state and cease proxy-only mode (if the appliance entered this mode).

Section B: RAID disk management on the NetCache appliance

About this section

This section contains information required to maintain disks on RAID-enabled NetCache appliances. See the Appliance Manager online Help for the required procedures and option descriptions.

Maintenance tasks include displaying the current status of disks, and adding, removing, or replacing disks on the appliance.

Topics in this section

This section contains the following topics:

- "About displaying the status and statistics of disks" on page 83
- "Querying for disk health" on page 85
- "About adding and removing disks" on page 86

About displaying the status and statistics of disks

Management display

You can view the status of disks on your appliance using the Disk - Management page (Maintenance tab > Disk > Management) of the Appliance Manager.

Note

The Appliance Manager does not display the Disk - Management page for NetCache C1100 or C1105 appliances. It does display this page for all other NetCache appliances.

The following table describes the different columns in the Disk - Management page output.

Output heading	Description
Host Adapter	Indicates the host adapter number, which is the number of the slot in which the disk adapter is installed.
Shelf	*Shelf* is the number of the disk shelf that is connected to the disk adapter interface on the host adapter. Multiple disk shelves can be connected to a disk adapter interface if the disk adapter is a differential SCSI adapter or a fibre channel adapter. The disk shelf number starts at 0.
Type	Indicates the type of disk adapter. For example, Fibre Channel and SCSI.
Bay	*Bay* is the number of the disk slot in the disk shelf, which starts at 0.
Disk ID	Disk ID is represented in the *x.y* format, where *x* is the host adapter and *y* is the disk number. For more information, see “Disk addresses” on page 74.
Size	Size of the disk in megabytes. The disk sizes are “right-sized,” as explained in “Disk space on each disk” on page 76.

Output heading	Description
Disk Type	Indicates the current function of the disk. A disk can be a data, spare, or parity disk.
Disk Operations	The operations allowed on the disks in the appliance. The Fail operation changes the state of a disk to "Bad." The Promote operation promotes a spare disk to a file system disk, as explained in the Appliance Manager online Help.

Disk statistics

You can view the disk statistics of your appliance using the System Status - General page (Data tab > System Status > General) in the Appliance Manager. The options that display disk statistics on the System Status - General page are as follows:

- Disk Space in Use—Displays the amount of disk space consumed by objects stored on the appliance.
- Total Disk Space—Displays the total amount of data disk space available on a appliance. The disk space indicated by this option does not include the disk space of the parity disk.

Querying for disk health

Querying for disk health

The appliance can be queried to report disk health. You can use the response to this query to configure load balancers or other traffic redirection devices to redirect traffic accordingly. This functionality is especially important in acceleration deployments in which a failed disk can lead to proxied requests and increased load on the accelerated servers.

To query the appliance for disk health, send a request to the following URL:

http://cache_hostname:3132/cache_manager/disk_status

The appliance will send one of the following disk status messages in response to the preceding HTTP request:

- If the appliance is handling requests normally, it will issue the following status message:

  ```
  HTTP/1.0 200 OK

  X-Cache-Status: DISK OK
  ```

- If the appliance cannot keep up with incoming requests, it will send the following status message:

  ```
  HTTP/1.0 500 ERROR

  X-Cache-Status: DISK BUSY
  ```

Changing the disk busy threshold

The default value of the disk busy threshold is 10. The default value of 10 indicates that 10 percent of misses were proxied to back-end servers in the last five minutes because the disk could not keep up with incoming requests.

Use the `config.http.disk_busy_thr` option to change the disk busy threshold. For example:

```
set cofig.http.disk_busy_thr //

20

//
```

About adding and removing disks

Why you might add or remove disks

You might want to add disks to the appliance to increase available disk space, to add a hot spare, or to replace a failed disk. You might want to remove a disk from your appliance because you want to use it in another appliance, because it has failed, or because it is producing excessive error messages.

Note

The NetCache C1100 and C1105 appliances have no replaceable components. If a disk fails or produces an excessive amount of errors, the entire system must be replaced.

New and previously used disks

In most cases, the disk you add will be a new disk; that is, the disk has never been used.

If the disk you want to add to the appliance was previously used by another NetCache appliance or a Network Appliance filer, make sure that you *unfail* the disk before you begin. See the details in the Appliance Manager online Help.

Platforms with an internal disk tray

If you are using a appliance model with an internal tray, the number of disks you can add depends on the model you purchased. You cannot add more disks than the internal trays the appliance was shipped with can accommodate. See "Platform support of RAID and internal disk trays" on page 72 for a list of platforms with internal disk trays.

Because the disks are internal, you cannot replace a failed disk while the system is in operation. You must shut down the system first to replace a failed disk in a system with an internal disk tray.

When to add or remove disks in external disk platforms

The Appliance Manager enables you to add or remove a single disk from the system without interrupting appliance service to your users. However, during the procedure, the appliance operates in proxy-only mode. That is, the appliance proxies Web requests on behalf of users by retrieving the objects from the source Web server. No new objects are saved to the cache, and no objects in the cache

are served to users. Because users might notice slower Web performance during this time, it is a good idea to plan to add or remove disks when you expect the load on the appliance to be light.

If you are adding more than one disk or a new disk shelf to your system: If you are adding several disks or a new disk shelf to your system, the process might be faster if you shut down the system. If you shut down the system, you can add all the disks at once, then reboot the system. Otherwise, you must add the disks one at a time using the Appliance Manager, as explained in the Appliance Manager online Help.

If you must remove more than one disk from your system: If you must remove more than one disk from the appliance, Network Appliance recommends that you remove and replace each disk one at a time You must allow the data to fully reconstruct on the new disk beforeyou remove another disk.

Caution

Removing more than one disk at a time from your appliance will result in data loss. If you remove more than one disk at a time from the appliance, the appliance will not be able to rebuild the data from the remaining disks. You must reinstall both the file system and the NetCache software and licenses in that case.

If you are performing disk operations online: If you are performing disk operations online, you can perform only one operation at a time. The appliance does not allow you to begin a new disk operation if a previous disk operation is incomplete.

Using hot spares in external disk platforms

If you want to prevent loss of service time, you can add one or more hot spare disks. When a data disk on the appliance fails, a hot spare automatically replaces it without a system shutdown.

To determine whether your appliance contains a hot spare, see the Disk - Management page (Maintenance tab > Disk > Management) of the Appliance Manager. This page lists all the disks of the appliance and indicates whether a disk is a parity, data, or spare disk.

You can add more hot spare disks to the system at any time, as long as disk slots are available. However, you need to follow the procedure described in the Appliance Manager online Help.

About adding disks to your system

When you add a single disk to the appliance, the disk is initially recognized as a hot spare. If you want the disk to be used as a data disk, you must "promote" the hot spare disk to a data disk.

Procedures for installing and promoting disks are provided in the Appliance Manager online Help.

About removing disks from your system

You can remove one disk from the appliance and still have access to all data stored on that disk. However, do not remove more than one disk at a time from the appliance.

Caution

Removing more than one disk at a time from your appliance will result in data loss. If you remove more than one disk at a time from the appliance, the appliance will not be able to rebuild the data from the remaining disks. You must reinstall both the file system and the NetCache software and licenses in that case.

See the procedures in the Appliance Manager online Help.

About replacing a failed disk on your system

The procedure for replacing a failed disk differs slightly, depending on whether a hot spare is installed in the appliance. If a hot spare is installed, the appliance promotes the hot spare to a data disk and reconstructs the data from the failed disk. However, if no hot spare is available, the appliance operates in a degraded mode until you replace the failed disk.

See the Appliance Manager online Help for detailed procedures about replacing failed disks and possible errors during disk replacement.

Note

The procedures for replacing a disk apply to appliances with external disk tray systems (the disks are exposed and easily accessible). The procedures do not apply to internal disk tray systems, where the disks are not easily accessed. See "Platform support of RAID and internal disk trays" on page 72 for more information.

Section C: Reinitializing all disks

When you need to reinitialize disks

You might need to initialize all disks in the following circumstances:

- You decide to redeploy an existing appliance and you need to completely reconfigure it.
- You have a C2100 model appliance that you want to upgrade from a version earlier than 5.3.1.
- You have a C1200 model appliance that you want to upgrade from a single-disk to a multi-disk system.
- You have a C1200 or C2100 model appliance that you want to boot from a compact flash PC-card.
- Network Appliance Technical Support advises you that the only way to recover from an error is to reinitialize all disks.

Caution

Initializing all disks causes all existing data to be lost.

Reinitializing all disks

To initialize all disks, complete the following steps.

Step	Action	
1	If the console is...	Then...
	Displaying the appliance prompt, for example, **netcache1>**	Place the system boot diskette into the diskette drive of the appliance and enter **`reboot`**.
	Not displaying the appliance prompt	Reboot from diskette. ◆ If the console is showing the ok prompt, enter **`boot`**. ◆ If the console is unresponsive, enter **`boot floppy`**. If the console is still unresponsive, reset the appliance by turning it off, leaving it off for 30 seconds, and then turning it back on.
2	When the boot menu appears, enter **`4`** to choose Initialize all disks. After the initialization process finishes, the setup script runs. You will be prompted for the appliance IP address and other information.	
3	Upload the new software image through the Appliance Manager. See the Appliance Manager online Help for instructions. Until you upload the new software image, no operating system exists on the disks. Therefore, do not reboot the appliance until after you have uploaded the new operating system and have been prompted to reboot.	

Using SNMP and the NetCache Appliance MIB 7

About this chapter

This chapter describes how SNMP (Simple Network Management Protocol) works on the NetCache appliance.

Topics in this chapter

This chapter contains the following topics:

- "About the SNMP implementation in NetCache" on page 92
- "About the NetCache MIB" on page 94
- "About user-defined traps" on page 96

Procedures and option descriptions

See the Appliance Manager online Help for configuration procedures and option descriptions.

Location of configuration options

Options for configuring the features discussed in this chapter are in the following location in the Appliance Manager:

Setup tab > Administration > SNMP

About the SNMP implementation in NetCache

What the SNMP process does

If SNMP is enabled in NetCache, NetCache will respond to SNMP requests and SNMP traps whenever specific events occur, and sends these traps to the SNMP managers. (A trap monitors a specific occurrence on the NetCache appliance; for example, a trap can monitor the disks on a NetCache appliance.) The SNMP managers might then carry out actions based on information received in the trap notifications.

SNMP agent and MIB groups supported

For diagnostic and other network management services, NetCache supports an SNMP version 1 compatible agent. This agent provides support for the MIB-II specification and a Network Appliance custom MIB. The following MIB-II groups are supported:

- System
- Interfaces
- Address translation
- IP
- ICMP
- TCP
- UDP
- SNMP

Note

Transmission and EGP MIB-II groups are not supported.

The Network Appliance custom MIB is discussed in "Groups and objects in the custom MIB" on page 94.

About traps

You set traps to inspect the value of MIB variables periodically. Whenever the value of a MIB variable meets the conditions you specify, a trap is sent to the network management stations on the trap host list in the NetCache SNMP configuration. The trap host list identifies the network management stations that receive the trap information.

You can set traps on any numeric variable in the MIB. For example, you can set a trap to monitor the disks on a NetCache appliance and have the SNMP application on your network management station display a flashing message on your console that informs you that a disk has failed.

Types of traps in NetCache

There are two types of traps in NetCache:

- Built-in—Built-in traps are predefined in NetCache and are automatically sent to the network management stations on the trap host list if an event occurs. These traps are based on
  - RFC 1213, such as coldStart, linkDown, linkUp, and authenticationFailure
  - Specific traps defined in the Network Appliance custom MIB, such as diskFailedShutdown, cpuTooBusy, and overTempShutdown

  Because the built-in traps track environmental conditions, they can vary between NetCache models.
- User-defined—User-defined traps exist only after you create them using the Appliance Manager or the command line interface.

  See "About user-defined traps" on page 96 for more information.

SNMP limits in NetCache

The NetCache appliance supports the following SNMP limits:

- Specification of up to eight communities. A community is a name that is used as a password by the SNMP manager to communicate with the NetCache SNMP agent.
- Trap notifications for up to eight management stations (trap hosts).

Where to get more information

See the following RFCs (Requests For Comments) for more information:

- RFC 1157—Defines and describes SNMP.
- RFC 1213—Defines and describes the SNMP MIB-II specification.

About the NetCache MIB

Information contained in the MIB

The NetApp custom MIB provides detailed information about many aspects of NetCache appliance operation.

Where to obtain the MIB

You can obtain the custom MIB from the NetCache CD-ROM or from the NOW Web page at http://now.netapp.com/ (perform a search for *MIB*). To locate the MIB on the CD-ROM, read the index.htm file in the top-level directory of the CD-ROM. You will need to install the MIB file on your network management station.

Ensuring that your workstation can obtain information about MIB objects

When you configure the basic SNMP options in the Appliance Manager, you provide the IP addresses or host names of up to eight trap hosts (network management workstations). You must install the NetCache MIB file on each of those trap hosts to ensure that each host can obtain information from the NetCache appliance about the objects that are part of the MIB. Follow the installation procedure included in your workstation documentation.

Groups and objects in the custom MIB

Objects in the custom MIB fall into the groups listed in the following table.

Group	Description
product	Includes product information, such as software version and system ID
systat	Includes system-level statistics
NetCache options	Includes information about appliance options, for example, whether particular protocol services are enabled and licensed
NetCache information	Includes information about some NetCache configuration settings, for example, the NetCache version, the admin port, and the IP address of a server that NetCache is accelerating

Group	Description
Various groups related to protocol statistics	Includes general NetCache statistics and various statistics for HTTP, NNTP, FTP, DNS, and streaming

Note

For information about the specific objects that are available, click the Show MIB Browser button at the bottom of the SNMP page in the Appliance Manager (Setup tab > Administration > SNMP).

About user-defined traps

About user-defined traps

You can create custom SNMP traps to send specific types of information to your network management station. To create a trap, you need to determine the information you want the trap to report on, and then determine the MIB variable that tracks that information.

Identifying a MIB variable to be used with a new trap

The NetApp MIB lists available variables with short descriptions. You can locate the MIB variable from the MIB on the NetCache CD-ROM or from the NOW Web page. However, it is easier to use the SNMP MIB browser in the Appliance Manager to select a variable and the object identifier (OID) associated with it.

Using the MIB browser in the Appliance Manager provides the following benefits:

- It presents the MIB variable information in an orderly, readable manner.
- When you click on the object name, the trap OID for the selected variable is imported directly into the New SNMP Traps page. You do not have to type the trap parameters into the page yourself, which is required if you look for this information in the MIB on the CD-ROM or on the NOW site.

To access the SNMP MIB browser, select Setup tab > Administration > SNMP in the Appliance Manager. Then click Show MIB Browser at the bottom of the page.

Automated Support with Autosupport 8

About this chapter

This chapter describes the NetCache Autosupport feature, which you can use to prevent potential problems from becoming problems.

Topics in this chapter

This chapter provides information about the following topics:

- "Planning summary for Autosupport configuration" on page 98
- "About Autosupport" on page 100

Procedures and option descriptions

See the Appliance Manager online Help for configuration procedures and option descriptions.

Location of configuration options

Options for configuring Autosupport are in the following location in the Appliance Manager:

Setup tab > Administration > Autosupport

Planning summary for Autosupport configuration

Determine Autosupport configuration

Configuring Autosupport will be faster if you plan ahead. Use the information in the following table to determine the Autosupport features that are appropriate for your organization.

Decisions to make	Your options	Considerations
Use Autosupport	By default, Autosupport sends messages to Network Appliance over HTTPS, with minimal detail (no private data). You can change the default settings.	◆ You can be alerted to potential problems before they become actual problems. ◆ Support for Autosupport is included as part of your basic warranty service.
Recipients of Autosupport messages	One or both of the following: ◆ Network Appliance Technical Support. ◆ Non-Network Appliance recipients. You can specify up to five e-mail addresses for event alerts and up to five addresses to receive both event messages and weekly reports.	Network Appliance looks for potential problems and has the experience to help you solve problems quickly.
Message types you want Autosupport to send	◆ If Network Appliance Technical Support is a recipient, event messages and weekly reports are sent. ◆ For non-Network Appliance recipients, you can separately identify recipients to receive event alerts and recipients to receive both event messages and weekly reports.	Sending event alerts to employees with pagers enables them to respond more quickly to problems when they are out of the office.

Decisions to make	Your options	Considerations
Level of detail in Autosupport messages (for messages to Network Appliance only)	◆ Include private information, such as IP addresses, in Autosupport messages. ◆ Do not include private information in Autosupport messages. ◆ Include the host name or system ID in the subject line of Autosupport messages.	If you are concerned about revealing data that you consider to be sensitive external to your company, specify that the messages include a minimal level of detail. By default, the system ID is included in the subject line of Autosupport messages. You can have the host name of the appliance in the subject line instead.
How Autosupport messages can be sent	◆ For messages to Network Appliance, the transport can be HTTP Post, HTTPS Post, or SMTP e-mail. ◆ For non-Network Appliance recipients, the transport must be SMTP e-mail.	◆ HTTPS Post provides the highest level of security. Firewalls might block transport, however. ◆ Typically, messages sent by HTTP Post can bypass firewalls. ◆ SMTP e-mail requires a mail server. If a firewall blocks the mail server, use HTTP Post.
If SMTP e-mail is the transport for Autosupport messages	◆ You can choose the transport for messages to Network Appliance. ◆ The transport for non-Network Appliance recipients is always SMTP e-mail.	You must have at least one host at your site that listens on the SMTP port (25) to send mail—an SMTP server or a mail forwarder, such as the sendmail program or Microsoft Exchange server. This host must be reachable by the NetCache appliance. You can specify up to five e-mail hosts.

About Autosupport

Autosupport described

The Autosupport feature sends messages automatically to Network Appliance™ Technical Support, members of your organization, or both, depending on how you configure Autosupport. Autosupport messages alert recipients about problems and potential problems with the NetCache appliance. Network Appliance strongly encourages you to use the Autosupport feature.

Reasons for using Autosupport: Network Appliance recommends that you include Network Appliance Technical Support as a recipient of your Autosupport messages for the following reasons:

- Network Appliance has programmed scripts to automatically look for particular data in Autosupport weekly reports that might indicate a potential problem. Some Network Appliance customers have been surprised when they were alerted by Network Appliance Technical Support about potential system problems—before the customers were aware that their appliances were not functioning optimally.
- Network Appliance will help you solve problems that Autosupport detects. Network Appliance provides a range of support, including automated parts replacement, e-mail contact, and contact by a Technical Support engineer, depending on the type of problem. For example, if Network Appliance receives a message that a disk failure occurred on your NetCache appliance, a replacement disk is automatically sent to you.

Protection of private data: Revealing private data outside your company does not need to be a concern. You can set up Autosupport so that private data is not included in the messages sent to Network Appliance. Additionally, you have a choice of transports, including HTTPS, over which Autosupport messages to Network Appliance can be sent.

Types of Autosupport messages

Autosupport generates the types of messages shown in the following table. Details about the contents of Autosupport messages appear later in the chapter.

Type	Description
Event alert	A brief one-line message that Autosupport sends to recipients you have identified when an event tracked by Autosupport occurs. Event alerts are commonly sent to personnel with devices such as pagers who want to be notified of problems when they are in the field. Event alerts and event messages are sent at the same time.
Event message	A message that Autosupport sends to recipients you have identified when an event tracked by Autosupport occurs. The subject line is the same one-line description that is sent as an event alert. The message contains information to help you diagnose and troubleshoot the problem. Event alerts and event messages are sent at the same time.
Weekly report	A message that Autosupport sends automatically each week to recipients you have identified. Unlike event alerts and event messages, weekly reports are not triggered by a particular event.

Events that trigger Autosupport messages

If Autosupport is enabled, Autosupport generates an event alert and an event message when an event in the following table occurs.

Event	Subject line of the message
Low NVRAM lithium battery	BATTERY_LOW!!!
Disk failure	DISK_FAIL!!!
Disk failed reconstruction	DISK RECONSTRUCTION FAILED!!!
Out-of-date disk Messages log detected	DISK_FIRMWARE_NEEDED_UPDATE!!!

Event	Subject line of the message
Fan failure	FAN_FAIL!!!
Shutdown because of overheating	OVER_TEMPERATURE_SHUTDOWN!!!
Partial RPS failure (One of the two power supplies on a NetCache appliance using a redundant power supply (RPS) has ceased functioning.)	POWER_SUPPLY_DEGRADED!!!
System reboot	REBOOT
System reboot using the `reboot` command	REBOOT (reboot command)
System reboot using the `halt` command	REBOOT (halt command)
System reboot caused by an internal halt	REBOOT (internal halt)
System reboot caused by an internal reboot	REBOOT (internal reboot)
System reboot caused by a watchdog timer reset	REBOOT (watchdog reset)
System reboot caused by turning on power	REBOOT (power on)
System reboot following a panic	REBOOT (panic)
System reboot after loading firmware	REBOOT (after entering firmware)
System reboot after running a WAFL™ check	REBOOT (after WAFL_check)
System reboot for an unknown reason	REBOOT (unknown reason)

Event	Subject line of the message
System reboot caused by a power glitch, for example, a power interruption	REBOOT (power glitch)
`wack` command was run	WAFL_check!!!
Fibre channel arbitrated loop is unreliable	FC-AL UNRELIABLE!!!
Fibre channel arbitrated loop has link failures	FC-AL LINK_FAILURE!!!
Storage health monitor detected degraded disk I/O	DISK_IO_DEGRADED!!!
Storage health monitor detected a SCSI sense error	DISK_RECOVERED_ERRORS!!!
Storage health monitor detected low disk throughput	DISK_LOW_THRUPUT!!!
Storage health monitor detected an impending disk failure	DISK_FAILURE_PREDICTED!!!
Incorrect system hardware configuration detected (PCI card only)	SYSTEM_CONFIGURATION_ERROR
Fibre channel disk shelf configuration error	CONFIGURATION_ERROR!!!
Disk shelf error	SHELF_FAULT!!!
Spare disk failure	SPARE FAIL!!!
Weekly backup of /etc/messages	WEEKLY_LOG
`option autosupport.doit` command	USER_TRIGGERED (user supplied subject)
Log file push failure	LOG_PUSHING_FAILED

Event	Subject line of the message
SmartFilter one week from expiring	SmartFilter on NetCache
WebWasher license expiration	WebWasher on NetCache
Minicore sent to Network Appliance	Subject determined by Autosupport

Content of Autosupport event messages and weekly reports

The following table shows the type of content that can be included in event messages and weekly reports. The content that is actually included depends on whether you specify Complete or Minimal as the detail level for event messages and weekly reports.

"Filtered" in the Minimal column means that sensitive data is removed. For example, only nonsensitive content from the Messages log is sent if the level of detail is specified as Minimal. If the level of detail is specified as Minimal, regardless of content type, IP addresses and MAC addresses are removed. Either the system ID (the default) or host name is included in the subject line of the message when the level of detail is Minimal. You control whether the system ID or host name is included by using the Identifier to use in subject line of minimal Autosupport messages option.

Content	Complete detail	Minimal detail
Date and time stamp of the message	X	X
Software licenses enabled on the NetCache appliance	X	X
Service usage (availability statistics)	X	X
System serial number (if available)	X	X
NetCache software version	X	X
NetCache appliance system ID	X	X
NetCache appliance host name	X	Configurable

Content	Complete detail	Minimal detail
SNMP contact name and location (if specified in the SNMP page)	X	—
Messages log contents	X	Filtered
ECC memory scrubber statistics	X	X
Registry statistics	X	X
NetCache statistics	X	—
Cumulative HTTP/FTP/NNTP/streaming statistics	X	—
NetCache configuration changes from default	X	—
Volume status	X	X
Checksum status	X	X
Parity Inconsistency (PI) information	X	X
WAFL check logs	X	Filtered
Hit rates	X	—
Utilization statistics	X	Filtered
WAFL statistics	X	X
Output from the following console commands:		
sysconfig -a sysconfig -c sysconfig -d sysconfig -r	X	X (-a filtered)
options	X	Filtered
ifconfig -a	X	—
ifstat -a	X	Filtered

Content	Complete detail	Minimal detail
df df -i	X	X
vol status vol status -v vol status -c	X	X
fcstat fcal_stats fcstat device_map fcstat link_stats	X	X
/etc/messages	X	Filtered
perf report -t	X	X

NetCache Log Files 9

About this chapter

This chapter describes the available NetCache log files, how they are named, and the formats available for each type of log. This chapter also describes the ways that you can set up log file management.

The *Guide to Messages and Log File Entries* describes specific headers that are available in the various logs. The information about log headers will help you determine the headers that you want to include in your logs and analyze your logs. This online guide is available from within the Appliance Manager online Help, on the NOW Web site (http://now.netapp.com), and on the product CD.

Topics in this chapter

This chapter includes information about the following topics:

- Section A, "Planning summary for log content and management," on page 108
- Section B, "About NetCache log files," on page 110
- Section C, "Log management techniques," on page 120
- Section D, "Location of configuration and management options," on page 125

Procedures and option descriptions

See the Appliance Manager online Help for configuration procedures and option descriptions.

Section A: Planning summary for log content and management

Determine log configuration

Configuring logs will be faster if you plan ahead. Use the information in the following table to determine the log configuration that is necessary for your organization.

Decisions to make	Your options	Considerations
Planning for log management configuration		
Log switching technique and schedule	NetCache provides the following log switching techniques, which apply to all logs but the Messages log: ◆ (Default) Rotating logs on the NetCache appliance With this technique, up to 10 logs of each log type can be stored. When a new log is created, the oldest log is deleted. ◆ Pushing logs to an FTP server or a Web server By default, logs are rotated when the log file size reaches 10 MB. You can change the maximum log file size and schedule log rotation or log pushing at specific intervals. **Note** The log switching technique is a global setting that applies to all log files except the Messages log. Messages log handling is not configurable.	◆ If log rotation when logs reach a maximum file size of 10 MB is acceptable for your organization, you do not need to reconfigure the global log settings (on the Setup tab > System > Log Files page). ◆ Pushing logs to an FTP server or a Web server is particularly useful for organizations that need to archive logs or need postprocessing log analysis. ◆ If your disk usage chart in the Appliance Manager shows a considerable amount of space being used by log files, consider taking the following actions: ❖ Reduce the size of your log files. ❖ Push log files to an HTTP or FTP server.

Decisions to make	Your options	Considerations
Whether you want system (syslog) messages that appear on the NetCache console to be sent immediately to a remote server's syslog daemon that is listening on port 514	Enable the Send NetCache Messages to a Remote Server option, if appropriate.	◆ You could, for example, monitor unauthorized use of this NetCache appliance in real time because the remote server would receive immediate notification if someone logged in to the NetCache appliance through the console.
Planning for log content configuration		
Whether the default log format is acceptable for each log	By default, the logs are generated in a default log format specific to each log. You can select other predefined formats or customize the log file format to meet your requirements. The predefined log formats and available log headers vary according to log type.	◆ If you are using a log analyzer tool, what type of format is required? For example, do you require Netscape extended format or Common log format for HTTP data? ◆ For data about some features, for example, SmartFilter or DynaBLocator WebWasher, to be logged, you must configure a custom log and include headers specific to the feature in the log. See the *Guide to Messages and Log File Entries* for available formats for each log file.

Section B: About NetCache log files

About this section

This section helps you to understand the logs that NetCache provides and introduces you to the log file formats that are available. See the *Guide to Messages and Log File Entries* for details about the headers that are available in the various logs.

Topics in this section

This section includes information about the following topics:

- "Available NetCache log files" on page 111
- "File names for NetCache logs" on page 115
- "About predefined and custom log file formats" on page 117

Available NetCache log files

Summary of available log files

The log files in the following table are available to help you monitor your NetCache appliance.

Log type	Type of information logged	Customizable?
ContentDirector log	Reports diagnostic information about the ContentDirector agent software.	No
CMS log	Reports details of the appliance processing of the the table of contents (TOC) file generated by the DataFabric Manager (DFM computer). This log is available only if the CMS (Content Management System) agent is enabled on the appliance through DFM or a third-party product.	No
DNS log	Reports information about the DNS lookups that were initiated by the NetCache resolvers.	No
FTP transfer access log	Records the details of FTP transactions on the NetCache appliance.	No
GRM server access log	If the GRM server is configured as a DNS server, the GRM server access log provides DNS query information from interactions between DNS nameservers and the GRM server. If the GRM server is configured as an L7 server, the log reports the URL redirection information between the client and the GRM server (client IP address, the requested URL, and the agents to be returned).	Yes
GRM server details log	The GRM server details log records information about agents and IP addresses and the proximity data they send to the GRM server.	Yes
ICAP log	Reports information about ICAP server transactions. The default ICAP log file format captures common errors, such as unavailable services or ACL configuration problems.	Yes

Log type	Type of information logged	Customizable?
Messages log	Reports NetCache events, such as reboots, device failures, and errors. Critical system events are also reported to the console. Use this log when you are looking for NetCache configuration or runtime errors. **Note** The syslog daemon automatically sends messages to the Messages log and the system console. Optionally, you can configure the Send the Appliance Messages to a Remote Server option on the System - Logging page in the Appliance Manager to immediately send syslog messages to a remote server's syslog daemon that is listening on port 514.	No
—	**Messages log file management:** The Messages log is always enabled and cannot be disabled. The Messages log normally uses only a small amount of memory and generating it should not affect normal NetCache operations. The Messages log is never pushed or rotated like other NetCache logs. Regardless of the log file switching technique you select, a new Messages log is started every Sunday at midnight. At that time, the recently replaced *messages* file is copied to *messages.0*, the *messages.0* file is copied to *messages.1*, and so on. The oldest Messages log is deleted.	
NNTP access log	The NNTP access log records information about client transactions conducted through the appliance for news services.	Yes
Streaming access log	Reports information about client connections, including the client IP address and port number, the server host name and port number, the number of bytes sent, and the total connection time.	Yes
Streaming details log	Reports information about the internal transactions that occur during streaming connections, including object hit and miss information and bit-rate switching data.	Yes

Log type	Type of information logged	Customizable?
Web server acceleration log	Reports transactions between the NetCache appliance configured as an accelerator and one or more Web servers that it accelerates, depending on how you have configured your Web (HTTP) accelerator rules. You can log Web server acceleration transactions in the Web access log or in one or more Web server acceleration logs. Some organizations, such as CDNs, log Web server transactions separately for each customer for which they provide acceleration services. **Note** Log header settings for HTTP logging apply to the Web access log and the Web server acceleration logs.	Yes
Web access log	Reports client transactions received by NetCache, whether requests are serviced or denied, and cache hits and misses. This log is used only for Web-based requests (such as HTTP and Gopher). The Web access log is helpful for tracking the types of objects that are cache hits and misses. The Web access log is also helpful for evaluating the load on the NetCache appliance (for example, peak performance and the content requested at peak times).	Yes

See the *Guide to Messages and Log File Entries* for more details about the content of the log files in the preceding table and examples of the log files.

Logs are enabled by default

NetCache appliance log files are enabled by default except for the Web server acceleration logs. The Messages log is always enabled and cannot be disabled. However, you can manually enable and disable the other NetCache logs from the Appliance Manager.

Note

For features that require a license, for example, NNTP, MMS, RTSP, and GRM, you cannot generate log data unless you have purchased and installed the license and configured your NetCache appliance for that service. Contact your Network Appliance sales engineer or the Installed Base Group (ibg@netapp.com) to obtain software licenses.

File names for NetCache logs

Log file names

When log files are pushed or rotated, the oldest of each type of enabled logs is discarded, and the file that was the active log file is renamed and saved. NetCache saves the active log file plus from zero to nine of the last logs of each log type.

The following table shows the names that NetCache assigns to each log type.

Log type	Active log name	Saved log file name
CMS log	CMS_log	*log_name*.0 through *log_name*.9 For example: messages.0 through messages.9
ContentDirector log	CDLog	
DNS log	dns_log	
FTP transfer access log	ftpxf_log	
GRM server access log	grm_log	
GRM server details log	grm_details_log	
ICAP 1.0 log	icap_log	
Messages log	messages	
NNTP access log	nntp_log	
Streaming access log	streaming_log	
Streaming details log	streaming_details_log	
Web access log	http_log	
Web server acceleration log	http_accel_<log id>	*log_name*_<*log.id*>.0 through *log_name*_<*log.id*>.255

When NetCache saves the active file, the name takes the following form:

log_name.cache_hostname.timestamp

For example:

http_log.your_cache.2002.12.30.14.45

In the preceding example, your_cache is the name of your NetCache appliance, and 2002.12.30.14.45 is the date and time when the log was pushed to the server. The time stamp is written with a four-digit year, two-digit month, two-digit day, two-digit hour, and two-digit minute.

About predefined and custom log file formats

Types of log file formats that are available

When you first install your NetCache appliance, the logs are generated in a default log format specific to each log. You can select other predefined formats or customize the log file format to meet your requirements. Most NetCache appliance log files adhere to the Extended Log File Format conventions described by the World Wide Web Consortium (www.w3.org). The Extended Log File Format enables you to add or delete log file headers so you can create customized log files that can be read by generic log analyzers.

In general, you can select two types of log file formats for your log files, predefined formats and custom formats.

- Predefined formats

  When you select a predefined format, you cannot alter the field set of the log (the list of log file headers) to change the information that is reported.

  Because each log reports a specific type of information, the predefined formats differ from log to log. However, all of the log formats adhere to the Extended Log File Format conventions described by the World Wide Web Consortium.

- Custom log format

  When you select a custom format, you modify the field set of a predefined format or create a new format. Because the list of headers is specific to each log, some headers that can be used in the Web access log, for example, cannot be used in the other logs. When you generate the log file, the log headers appear in the order that you entered them.

  Note

  You cannot customize the Messages log, ContentDirector log, DNS, and FTP transfer access log.

Available log file formats

The formats available for each NetCache log file are shown in the following table.

Log	Formats available
CMS log	The CMS log cannot be customized. For more information, contact Network Appliance technical support.
ContentDirector log	The ContentDirector log cannot be customized. For more information, contact Network Appliance technical support.
FTP transfer access log	◆ Default format only
GRM server access log	◆ GRM Server Access Log Default Format ◆ Custom
GRM server details log	◆ GRM Server Details Log Default Format ◆ Custom
ICAP 1.0 log	◆ ICAP Default Log Format ◆ Custom
NNTP access log	◆ NNTP Access Log Default Format ◆ Custom Format
Streaming access log	◆ Streaming Access Log Default Format ◆ Custom
Streaming details log	◆ Streaming Details Log Default Format ◆ Custom
Web access log Web server acceleration log	◆ Web Access Log Default Format ◆ Common Log Format ◆ Netscape Extended Format ◆ Squid Native Format ◆ Custom Format

See the *Guide to Messages and Log File Entries* for details about the headers that are available in the various logs.

Section C: Log management techniques

About this section

This section provides details about the methods that NetCache provides for handling NetCache logs—log rotation and log pushing. Read this section to determine whether to use the default log switching technique of log rotation when a log reaches the maximum file size of 10 MB.

Topics in this section

This section includes information about the following topics:

- "Available log file switching techniques" on page 121
- "About log rotation" on page 122
- "About log pushing" on page 123

Available log file switching techniques

Available techniques

You can choose one of the following log switching techniques:

- Log pushing—Pushes the log to a specified Web or FTP server.
- Log rotation (the default)—Rotates the log at a specified interval.

You can use only one log switching technique at a time, but you can alternate between them. Log pushing, log rotation, and the parameters that control when the logs are pushed or rotated are global settings. That is, the settings apply to all enabled NetCache logs except the Messages log.

The Messages log is not configurable. NetCache always rotates the Messages log. A new Messages log is started every Sunday at midnight. At this time, the recently replaced *messages* file is copied to *messages.0*, the *messages.0* file is copied to *messages.1*, and so on. The oldest Messages log is deleted.

Parameters for controlling log handling

You can specify that logs are to be rotated or pushed when they reach a maximum file size or according to a schedule that you set. However, NetCache always rotates or pushes a log when it reaches the maximum size if the maximum size is reached before the scheduled rotation or push time. You can set a minimum log file size of 1 MB or a maximum size of 1999 MB. The default value is 10 MB.

Typically organizations set the maximum file size to 100 MB or several hundred MB per day. For a normally busy C6100, for example, log files can reach 10 GB or more per day. Setting a small maximum file size value in such a case would result in too many log files to realistically be able to manage.

If you are pushing logs to a Web server or an FTP server according to a schedule, schedule log pushing for off-peak hours. In addition, avoid setting a large log file size. The reason is that if a network failure occurs during a log push, NetCache restarts the log push from the beginning of the file. If the log files are smaller, a greater chance exists that a complete log file might have been pushed before the network failure occurred.

About log rotation

Log rotation defined

When log rotation is the log file switching technique (the default), logs remain on the NetCache appliance until they are rotated out. The NetCache appliance keeps the current log file and up to 10 previous log files on disk for each protocol.

Rotated logs remain in the NetCache appliance logs directory and are viewable from the Appliance Manager.

Note

Configuration of the log rotation switching technique does not affect the Messages log. The Messages log files are rotated automatically.

What happens when logs rotate

When the NetCache appliance rotates the logs, it deletes the oldest log file and saves the active log file to disk. The NetCache appliance keeps the current log file and up to 10 previous log files on disk.

Changing from log rotation to log pushing

When you change the log file management technique from log rotation to log pushing, the NetCache appliance schedules all the old logs to be pushed to the FTP or Web server. If you do not want the old logs to be pushed to the FTP or Web server, delete the logs before committing the configuration change.

About log pushing

Log pushing defined

When log pushing is the log switching technique, the NetCache appliance pushes logs to an FTP or a Web server at a specific interval, at preset times, or when a log file reaches a specified file size. You configure the criteria that determine when the logs are pushed. You cannot set the file size larger than 1,999 MB.

Note
Messages log files are never pushed.

The NetCache appliance keeps the current log file and up to 10 previous log files on disk. After the NetCache appliance successfully pushes a log file to the FTP or Web server, the NetCache appliance deletes the log from storage.

Why choose log pushing?

You might choose to set up log pushing for archival purposes or if your organization needs postprocessing log analysis.

Server requirements for log pushing

The server to which you want to push logs must be running an FTP or a Web server and must allow the NetCache appliance to rename and delete files in the directory you specify as the log repository. Network Appliance recommends that you set up a user account for the NetCache appliance logging on the FTP or Web server and push the logs to that location.

What happens if a log push is not successful

If a regularly scheduled log push is not successful, the NetCache appliance attempts every five minutes to push the logs to the FTP or Web server. The log push interval is not configurable. The NetCache appliance continues to attempt to push the logs every five minutes until it succeeds.

During this time, the log file that was not pushed is saved to disk and is not accessible. If another scheduled push time occurs and NetCache still cannot push the log files successfully, NetCache saves these log files to disk.

If the log push continues to be unsuccessful, NetCache sends an Autosupport message every hour stating that the log push failed. NetCache continues to try pushing the log files indefinitely or until you change the log management technique to log rotation.

When the problem that caused the push to fail is resolved, NetCache continuously pushes the first 10 files from the spool. Five minutes later, NetCache pushes the next 10 log files from the spool. NetCache continues pushing 10 log files from the spool every five minutes until all log files have been pushed.

Note

The behavior described in this section does not apply to the data logged through the Streaming on-demand monitoring feature and sent to servers.

File renaming when logs are pushed

When the NetCache appliance pushes the logs, it renames the active log files by appending the host name and a timestamp to the name of the log file.

What happens if you turn off log pushing

If you disable log pushing and do not reenable it within five minutes, NetCache deletes all log files that have not yet been pushed to the FTP or Web server.

Section D: Location of configuration and management options

Location of configuration options

The following table shows the location of the log file options in the Appliance Manager.

What to configure	Location
Global log management setup	
Log management technique and parameters	Setup tab > System > Logging
Log file setup and customization options for specific logs	
CMS log	This log is always enabled when automatic DFM Discovery is enabled on the appliance. No customization is possible for which fields can be included. However, the schedule and retry values are configurable through DataFabric Manager, the appliance CLI, and through the zephr API.
ContentDirector log	The log is always enabled when the ContentDirector Agent is enabled and no customization is possible.
DNS log	Setup tab > DNS > DNS - General
FTP transfer access log	Setup tab > FTP > FTP - General
GRM server access log	Setup tab > GRM Server > Logging
GRM server details log	Setup tab > GRM Server > Logging
ICAP log	Setup tab > ICAP > ICAP 1.0
Messages log	The log is always enabled and no customization is possible.
NNTP access log	Setup tab > NNTP > Logging
Streaming access log	Setup tab > Streaming Media > Logging

What to configure	Location
Streaming details log	Setup tab > Streaming Media > Logging
Web access log	Setup tab > HTTP > Logging
Web server acceleration log	To enable the accelerator log for a specific acceleration rule: Setup tab > HTTP > Web server acceleration > Rules tab > New Rule > Log Number option To configure log headers: Setup tab > HTTP > Logging

Location of log file management options

Select Data tab > Log Files > *logfilename* in the Appliance Manager to access the log maintenance pages. From these pages, you can

- View an entire log file or the last lines of a log file
- Copy log files to your computer
- Delete one or more log files
- Send log files to a remote FTP server or HTTP Web server
- Send a log to NetApp Technical Support

Error Handling 10

About this chapter

This chapter explains how to customize HTTP error messages. It also explains how to hide NetCache error messages from users.

Topics in this chapter

This chapter covers the following topics:

- "Planning summary for error handling configuration" on page 128
- "About customizable error messages" on page 129
- "NetCache error codes" on page 130
- "About hiding NetCache-generated error messages" on page 135

Procedures and option descriptions

See the Appliance Manager online Help for configuration procedures and option descriptions.

Location of configuration options

Options for configuring the features discussed in this chapter are in the following locations in the Appliance Manager:

Feature	Option location
Customized HTTP error messages	Maintenance tab > Software > Error Pages
Stealth mode	Setup tab > HTTP > General > Stealth Mode option

Planning summary for error handling configuration

Determine error handling configuration

Configuring error handling will be faster if you plan ahead. Use the information in the following table to determine the error handling configuration that is necessary for your organization.

Decisions to make	Considerations
Whether to customize error messages	When an error message is displayed, do you want the message to include specific information that would not be available with HTTP 1.1 error codes? For example, if you are using WebWasher DynaBLocator content filtering, do you want to display the blocked category name in the message? Do you want your error messages to include contact information for a person in your organization?
Whether to hide references to NetCache in NetCache error messages	If you do not want your users to be aware that a NetCache appliance exists on the network, you can use “stealth mode” to display generic error messages instead of NetCache-specific messages.

About customizable error messages

Overview of NetCache customizable error messages

NetCache provides several error messages, derived from HTTP 1.1 error codes, that you can customize for your organization. For example, default error message text that NetCache supplies instructs the user to contact the administrator. You might want to modify the error text to include the name and telephone number of the administrator.

Applicable protocols

Customizable error messages apply to HTTP and to FTP over HTTP.

Where the error messages are displayed

The error messages described in this chapter appear in the following locations:

- Web browser
- Web access log

Most error messages appear in the Web browser. Under certain circumstances (when proxy authentication is required, for example) the error message is written to the Web access log, and an on-screen dialog box prompts the user for a valid user name and password.

NetCache error codes

About NetCache error codes

NetCache supports one proprietary error code (510), plus 11 additional codes that build on standard HTTP 1.1 error codes (200, 201, 302, 400, 401, 403, 407, 412, 500, 502, and 504).

Error message text files

The text for each error code is stored in a file that begins with the number of the error code and ends with the extension ".htm." For example, the error message text for code 501 resides in 501.htm.

The following table shows the default error message text for the 12 error codes that NetCache supports. Each message can be modified by editing the HTML file associated with its error code. See "<!--NETCACHE ERROR--> error tag" on page 132 for a definition of <! --NETCACHE ERROR-->.

Error code	Default error message text (user editable)	Explanation
200	OK	The request was successful.
201	Success	The request was successful.
302	Move Temporarily You are being redirected to a new location because *<!--NETCACHE ERROR-->*	The requested URL, image file, or text form was moved to a new location.
400	Bad Request The following error occurred: *<!--NETCACHE ERROR-->* Please contact the administrator.	This general error message indicates that the origin server did not understand the request. Improper URL syntax, among other issues, can trigger this error.
401	Unauthorized Authentication is required because *<!--NETCACHE ERROR-->*	The user is not authorized to access the origin server. **Note** When HTTP transparent authentication is enabled, NetCache (instead of the server) sends this error.

Error code	Default error message text (user editable)	Explanation
403	Forbidden You were denied access because *<!--NETCACHE ERROR-->*	The origin server refused to allow the user to access it.
407	Proxy Authentication Required Authentication is required because *<!--NETCACHE ERROR-->*	The NetCache appliance requires user authentication. This error appears in the Web access log, but it does not appear on screen. Instead, the Web browser displays a dialog box, which requires the user to enter a user name and password.
412	NetCache error Error: *<!--NETCACHE ERROR-->*	The object was in the cache but the `If-Match` condition specified by the client failed (did not match).
500	Server Error The following error occurred: *<!--NETCACHE ERROR-->* Please contact the administrator.	This generic message indicates that a problem occurred on the origin server.
502	Bad Gateway The following error occurred: *<!--NETCACHE ERROR-->* Please contact the administrator.	The gateway tried to obtain a response from an origin server or another gateway, but the other device sent a negative response.
504	Gateway Timeout The following error occurred: *<!--NETCACHE ERROR-->* Please contact the administrator.	The gateway did not send a response within the timeout period.
510	Content Fill Error The following error occurred: *<!--NETCACHE ERROR-->* Please contact the administrator.	NetCache was unable to place an object into (or retrieve an object from) the object cache. This is a proprietary NetCache error code.

<!--NETCACHE ERROR--> error tag

The <!--NETCACHE ERROR--> error tag, which appears in most of the default error messages, is a proprietary variable that responds to the current error code by displaying the specific text string stored for that error code in the errors.desc file. For example, code 400 returns “Bad URL,” whereas code 504 returns “Server unreachable.”

You can change the output strings that the <!--NETCACHE ERROR--> error tag returns by editing errors.desc. The errors.desc file is a plain ASCII file similar to the numbered HTML files that store error message text for HTTP 1.1 error codes. The errors.desc file is listed in the Current Error Files list on the Data tab > Software > Error Pages page in the Appliance Manager. Message text in the errors.desc file overrides the default message text that NetCache provides.

Note

Everything between (and including) the angle brackets in the <!--NETCACHE ERROR--> error tag must be inserted into the appropriate error message text file intact and unchanged. Those strings will be converted to instance-specific text output when the error message is displayed.

Additional NetCache error tags

You can insert one or more of the error tags shown in the following table into your error messages to supply instance-specific information when an error message is displayed.

For example, you can have NetCache respond to a failed page request by displaying the name of the blocked URL, the IP address of the client that made the request, and the date the failure occurred.

Variable	Description
<!--NETCACHE:URL-->	This string identifies the URL that was blocked.
<!--NETCACHE:USERNAME-->	This string identifies the user whose request failed.
<!--NETCACHE:CLIENT_IP-->	This string provides the IP address of the client that made the failed request.
<!--NETCACHE:DATE-->	This string specifies when the failed request was made.

Variable	Description
<!--NETCACHE:HOST_NAME-->	This string provides the host name of the NetCache appliance that is processing the error.
<!--NETCACHE:CATEGORY-->	This string indicates the SmartFilter or WebWasher DynaBLocator category that applies to the current error code.

When the error message is displayed, each string is replaced with the current value of the variable. For example, the message "Your request for *<!--NETCACHE:URL-->* has been denied." might be displayed as "Your request for http://www.anysite.com has been denied."

Note

Everything between (and including) the angle brackets in the error tags must be inserted into the appropriate error message text file intact and unchanged. Those strings will be converted to instance-specific text output when the error message is displayed. The only error tag for which you can edit the output strings is the *<!--NETCACHE ERROR-->* error tag.

Error tag syntax

The following example illustrates the proper use of error tags in an error message text file.

```
<HTML>
<HEAD><TITLE>403 Forbidden</TITLE></HEAD>
<BODY>
<H1>Forbidden</H1>
<H4>
You were denied access because:<P>
<!--NETCACHE ERROR--><P>
DATE:<!--NETCACHE:DATE--><P>
URL:<!--NETCACHE:URL--><P>
USERNAME:<!--NETCACHE:USERNAME--><P>
CLIENT_IP:<!--NETCACHE:CLIENT_IP--><P>
```

```
CATEGORY:<!--NETCACHE:CATEGORY--><P>
<H4>
<HR>
</BODY>
</HTML>
```

Error message file output

Viewed within a Web browser, the preceding HTML file produces the following output.



Forbidden

You were denied access because:

OLD_TAG: Access denied by SmartFilter content category. The requested URL belongs to the following category: Sports.

DATE: Fri, 16 Mar 2001 04:31:22 GMT

URL: http://www.nfl.com/

USERNAME:

CLIENT_IP: 10.53.50.65

SF_CATEGORY: Sports

About hiding NetCache-generated error messages

Hiding NetCache-generated messages

NetCache provides detailed messages about errors it detects and information about how to resolve the problem that caused the error to occur. If you do not want end users to be aware that a Web cache is being used, you can suppress NetCache messages and instead display more generic, less detailed Web browser messages. Hiding the existence of a Web cache is sometimes referred to as running in *stealth mode*.

Restrictions for stealth mode

Stealth mode is applicable only to transparent and nontransparent HTTP.

Messages displayed by browsers when stealth mode is on

Different browsers sometimes display different messages in response to the same error condition. However, the user of a particular browser will always see the same message, regardless of the error condition. For example, if the user of a Netscape browser sends NetCache a request that ultimately fails, that user might receive a return message indicating that the connection has been reset.

Transparent Proxying 11

About this chapter

This chapter discusses the NetCache transparent proxy feature. When transparent proxying is deployed, a switch or router redirects client requests to a proxy-cache server (such as a appliance). This chapter provides information to aid you in planning for transparent proxying. For a conceptual overview of transparent proxying, see the *Deployment Guide*.

Clarification of terms

This chapter uses the terms *client-side traffic* and *server-side traffic*. Client-side traffic flows from the client to NetCache and from NetCache to the client. Server-side traffic flows from NetCache to the origin server and from the origin server to NetCache.

Topics in this chapter

This chapter contains the following sections:

- Section A, "Planning for transparent proxying," on page 138
- Section B, "About using an L4 or L7 switch for transparent proxying," on page 142
- Section C, "About using a WCCP router for transparent proxying," on page 148
- Section D, "WCCP service group reference information," on page 161
- Section E, "Additional transparency features," on page 167
- Section F, "Troubleshooting transparency," on page 178

Procedures and option descriptions

See the Appliance Manager online Help for configuration procedures and option descriptions related to transparency.

Location of configuration options

To access the transparent proxying options in the Appliance Manager, select:

Setup tab > Transparency

Section A: Planning for transparent proxying

About this section

This section describes the decisions that you should be considering as you read this chapter. It also explains the type of information that you must gather before you begin configuring your appliance for transparent proxying.

Topics in this section

This section provides information about the following topics:

- "Planning information to consider as you read this chapter" on page 139
- "Determining port numbers for redirected traffic" on page 141

Planning information to consider as you read this chapter

Decisions to be made

In this chapter, you will determine the following:

- How the appliance fits into your current L4 or L7 switch or WCCP router deployment
- The implications of using third-party proxy-cache servers in your deployment
- How to achieve failover with the transparency method you choose
- If you are deploying transparency with a WCCP router, the type and number of required WCCP service groups
- Whether you want to redirect traffic using the default ports
- Whether you need to set up transparent proxy authentication for HTTP
- What type of security measures (if any) you want to use with your redirection device
- Whether you need to modify transparent redirection to meet a specific need, such as client-server authentication

Information to gather before continuing

Before continuing with the NetCache configuration, ensure that you have the following information:

- Protocols that you want to transparently proxy
- If you are deploying transparent proxying with an L4 or L7 switch, the L4 or L7 switch configuration documentation
- If you are deploying transparency with WCCP routers
  - The number, type, and properties of the WCCP service groups that you need to create, including the WCCP password for each service group, if desired
  - Cisco IOS specifications for configuring your WCCP routers
  - If you are using unicast transmission, the IP addresses of the WCCP routers
  - If you are using multicast transmission, one or more multicast IP addresses to be used when configuring your service groups.

    Multicast IP addresses do not need to be unique among service groups. The same multicast IP address can be used for all service groups.

- If you plan to use load balancing over the appliance interfaces, record the IP addresses of the interfaces over which this appliance will deliver data to clients

  Network Appliance recommends using the WCCP Appliance IP Addresses for Load Balancing option for MMS and RTSP streaming media.

When to use the optional transparency features

The following table provides reasons that you might want to modify transparency and describes the NetCache feature you can use to accomplish your goal.

If you want to...	You can use these features...
Enable your users to have direct contact with Web servers that have a large amount of uncacheable data	IP forwarding
Ensure that client requests arrive at the origin server with the client IP address as the source address (for example, because the server requires IP-based authentication)	IP forwarding URL forwarding IP spoofing Dynamic forwarding
Allow streaming media content providers to measure how many distinct users are viewing their content	IP spoofing for MMS, RTSP, or both
Ensure that the term *proxy-cache server* does not appear in NetCache error messages	Stealth mode

To learn more about these features, see Section E, "Additional transparency features," on page 167.

Determining port numbers for redirected traffic

Descriptions of port settings

The following table shows, for each protocol supported for transparent proxying, the recommended port numbers to use for transparent redirection. You must open these ports on the switch or router and on the appliance.

Protocol	Required port setting	Comments	Default setting
DNS	53	This port number is not configurable.	53
FTP	21	This port number is not configurable.	21
HTTP	80	You can set multiple HTTP proxy ports. Therefore, you can set a proxy port to 80 for transparency, even if you are already running the NetCache service on port 3128.	3128
NNTP	119	None.	119
MMS	1755	This port number is not configurable.	1755
RTSP	554	If you use WCCP for transparent proxying and redirect RTSP traffic to a port number greater than 1024, random non-RTSP traffic is sent to that port. This random traffic can cause network problems.	554
RTCP	2001 (recommended)	You must set an RTCP port if you are using QuickTime for streaming. RTCP allows quality-of-service feedback information to be exchanged between QuickTime clients and the streaming media cache through UDP. This port must be an odd number.	2001

Section B: About using an L4 or L7 switch for transparent proxying

About this section

This section describes using an L4 or L7 switch for transparent proxying. It provides failover and deployment information and describes the suggested ports to set for transparent proxying.

Topics in this section

This section provides information about the following topics:

- "Transparent proxying requirements for an L4 or L7 switch" on page 143
- "Choosing an L4 or L7 switch request distribution method" on page 145
- "Planning for failover with an L4 or L7 switch" on page 146
- "Preparing for switch configuration" on page 147

Transparent proxying requirements for an L4 or L7 switch

About using a switch for transparent proxying

You can use an L4 or L7 switch to pass DNS, FTP, HTTP, NNTP, MMS, and RTSP requests to the appliances. To learn more about the differences between L4 and L7 switches, see the *Deployment Guide*.

L4 and L7 switch deployment requirements

To deploy appliances with an L4 or L7 switch, you need to

- Place the switch in an optimal network location

  For more information, see "Switch location recommendations" on page 144.
- Configure the switch so that it can pass requests to the appliance

  See the switch vendor's documentation and "Choosing an L4 or L7 switch request distribution method" on page 145.
- Configure transparent proxying options in the Appliance Manager (or CLI) for the protocols you want to redirect

  For configuration procedures, see the Appliance Manager online Help.

Requirements for transparent proxying with a switch

To deploy transparent proxying with an L4 or L7 switch, you must meet the requirements listed in the following table. Network Appliance also recommends that you comply with the "best practice" recommendations that are listed in the table. Items listed in the table are requirements unless otherwise noted.

Category	Requirements and recommendations
Appliance	◆ A network interface is required for each switch attached. ◆ The appliance should be directly connected to the switch (best practice).
Network layout	◆ The switch must be in a location to detect all traffic for the clients it is expected to serve.

Category	Requirements and recommendations
L4 or L7 switch configuration	Switch configuration involves the following high-level steps: ◆ Identify traffic to be redirected to the appliances and the request distribution method to be used. ◆ Identify the appliances to which traffic is to be redirected. Contact your switch vendor for specific switch configuration settings.
NetCache configuration	For each protocol for which you want to set up transparent proxying, enable the transparency feature. See the Appliance Manager online Help for configuration details.

Switch location recommendations

The following table provides recommendations for locating your switch.

Switch location in relation to...	Comments
Appliances	L4 and L7 switches use MAC address rewriting as the method for redirecting packets. Therefore, your L4 and L7 switches must be on the same subnet as the appliances to which the switch is to redirect packets. For maximum efficiency, Network Appliance recommends directly connecting the switch to each appliance.
Clients	The switch must be located so that it can view all network traffic for the clients that it is expected to serve.

Choosing an L4 or L7 switch request distribution method

Influencing how requests are distributed over proxy-cache servers

The hashing function on a switch can be set up to distribute requests over appliances based on either of the following:

- IP address (the most commonly used method)
- URL (L7 switches only)

Typically, you want to achieve an even distribution of requests across your appliances.

IP address-based request distribution recommendations

If you want to use the switch to use IP addresses as the basis for request distribution, see the recommendations in the following table. These recommendations provide the most balanced distribution of requests across your appliances.

For a appliance running as a...	Recommended request distribution method
Forward proxy	Destination IP address (default)
Reverse proxy	Source IP address

L7 URL-based request distribution recommendation

Some L7 switches allow for request distribution based on URL. The L7 switch examines the request and determines whether the object is cacheable. This capability enables you to set up your switch so that requests for obviously uncacheable objects, such as URLs for CGI, bypass the appliance. Noncacheable objects are then obtained directly from an origin server. You should use URL-based request distribution in forward proxy deployments only.

Planning for failover with an L4 or L7 switch

Failover with an L4 or L7 switch

If you deploy transparent proxying with an L4 or L7 switch, NetCache does not need any active failover mechanism. The switch monitors the appliances that it is aware of. The following table shows the failover behavior of a switch for each protocol that NetCache supports for transparent proxying.

Protocol	Type of failover the switch provides
DNS (port 53) FTP (port 21) HTTP (port 80) MMS (port 1755) RTSP (port 554)	Redirects the requests to other appliances or, if all the appliances fail, to the Internet or an internal origin server.
NNTP (port 119)	Redirects requests to other appliances. The switch does not fail over NNTP requests to the Internet. You can, however, configure the switch to fail over to the news server. Before doing so, make sure that your news server can handle the traffic load. News servers generally cannot handle the volume of news requests that appliances can handle. Therefore, failing over to a news server is often not possible.

Preparing for switch configuration

Strategy for initial configuration

Strategies for initial configuration of transparent proxying are as follows:

- Set up the appliances offline.

  Setting up the appliances offline before passing all your network traffic to the L4 or L7 switch will have the least impact on your users. If you deploy transparent proxying during planned network downtime, you might be able to work directly on the network without affecting your users.

  The procedure described in the online Help assumes that you will configure the appliance offline, test the configuration, then pass your network traffic to the switch.

- Set up transparent proxying on an installed appliance.

  You can set up transparent proxying on an installed appliance if a spare network interface is available. A separate network interface card enables the existing NetCache service to continue during the conversion process.

  If you choose to use this method, ensure that for HTTP transparent proxying you do the following:

  - Leave the HTTP Proxy Ports setting as it is so that users can still proxy Web requests through the existing NetCache configuration.
  - Add an additional HTTP Proxy Ports setting of 80 for HTTP transparent proxying.

Avoiding traffic loops

If you have more than one network interface and you are deploying transparent proxying with an L4 or L7 switch, make sure that the port through which outgoing NetCache traffic is sent is not configured as a transparent port. If outgoing NetCache traffic is sent back through an incoming cache port on the switch, the switch passes the traffic back to the appliance, creating a traffic loop. If a traffic loop occurs, no requests are serviced. For HTTP, MMS, and RTSP transparent proxying, this event is recorded in the Messages log file. For NNTP transparent proxying, the NNTP trace log file can help you trace the path that the request has taken. The NNTP trace log is available only through the CLI.

Section C: About using a WCCP router for transparent proxying

About this section

This section describes what you need to plan for when implementing transparent proxying with WCCP. This section also provides planning information for defining service groups and discusses the available traffic distribution strategies.

Topics in this section

This section provides information about the following topics:

- "Requirements for WCCP transparent proxying" on page 149
- "Choosing a WCCP traffic redirection method" on page 152
- "Choosing a WCCP transmission method" on page 154
- "Choosing the optimum WCCP request distribution method" on page 156
- "Distributing load based on appliance platform type" on page 158
- "Determining if you need to load balance data over multiple NICs" on page 159
- "Securing access to your WCCP deployment" on page 160

Requirements for WCCP transparent proxying

About WCCP

The Web Cache Communication Protocol (WCCP) provides a way for routers to redirect and distribute traffic among one or more proxy-cache servers (such as an appliance). WCCP has a built in load-balancing mechanism and provides redundancy.

WCCP can be used for both forward-proxy and reverse-proxy deployments. A WCCP router can redirect and distribute DNS, FTP, HTTP, NNTP, MMS, and RTSP requests across multiple appliances.

Note

You can also use a policy-based router to redirect traffic to the appliance. Contact your Network Appliance representative for more information.

Requirements for transparent proxying with a WCCP 2.0 router

To deploy transparent proxying with a WCCP router, you must meet the requirements listed in the following table.

Category	Requirements and recommendations
Appliance	◆ A network interface is required for each router attached.
Network layout	◆ The router must be in a location to detect all traffic for the clients it is expected to serve. See “Router location” on page 150 for more information. ◆ If a firewall is between the WCCP router and the appliance, you must allow UDP port 2048. WCCP runs over UDP using port 2048.
Router configuration	◆ You must meet the software requirements described in “WCCP 2.0 software requirements” on page 150. ◆ Configure WCCP service group information to correspond to service group configuration on the appliances. See Cisco documentation for information about setting up WCCP 2.0.

Category	Requirements and recommendations
NetCache configuration	◆ For each protocol for which you want to set up transparent proxying, enable the transparency feature. ◆ Configure service group information, which includes identifying traffic to be redirected to the appliances and the request distribution method to be used. NetCache can then send information to the router that the router can use to configure itself.

WCCP 2.0 software requirements

To implement transparent proxying with WCCP, your router or switch must meet the software requirements listed in the following table. See the Cisco Web site for more information about WCCP 2.0 requirements.

Hardware	Required software version
WCCP router	IOS 12.0(4) T images and later versions
WCCP switch	IOS 12.1(4) T images and later versions

Router location

The following table provides information about WCCP router location.

Router location in relation to...	Comments
NetCache appliances	When you have multiple subnets, the router and appliances can be on different subnets. However, Network Appliance recommends that, for efficiency, the router and appliances be on the same subnet. You can directly connect a WCCP router to an appliance. However, a direct connection is not a requirement or a best practice recommendation.

Router location in relation to...	Comments
Clients	The router must be located so that it can view all network traffic for the clients that it is expected to serve.
Firewalls	◆ Do not place the WCCP router in a location where a firewall that uses Network Address Translation (NAT) is located between it and the appliance. ◆ Firewall configuration for WCCP traffic can be difficult. Consult your Network Appliance service engineer for configuration help and deployment recommendations.

Choosing a WCCP traffic redirection method

Types of WCCP traffic redirection

You can configure a WCCP router to redirect client or server traffic to NetCache using the following methods:

- IP-GRE encapsulation

  In IP-GRE encapsulation, the original IP packet is encapsulated in another IP packet containing the appliance's IP address. IP-GRE encapsulation is the default traffic redirection method.

  Note

  IP-GRE packets that pass through a transparent firewall to the appliance are not reencapsulated when NetCache sends them to clients.

- MAC address rewriting

  In MAC address rewriting (sometimes referred to as L2 rewriting), the router replaces the original MAC address with the address of the target proxy-cache server. This method can be used only when the WCCP router and appliance are on the same subnet.

To configure the client traffic redirection method, use the Redirection Method option. To configure the server traffic redirection method, use the Return Method option. You can access both options by selecting Setup tab > Transparency > WCCP Global Settings.

How to choose a traffic redirection method

When deciding whether to modify the WCCP traffic redirection method, consider the information in the following table.

If...	Use this redirection method...	Comments
You are concerned about redirection efficiency	MAC address rewriting	MAC address rewriting redirects traffic more quickly than does IP-GRE encapsulation. However, MAC address rewriting can be used only when the WCCP router and appliance are on the same subnet.

If...	Use this redirection method...	Comments
The router and appliance are on different subnets	IP-GRE encapsulation	IP-GRE can be used when the router and appliance are on the same subnet or on different subnets.
You need to use IP spoofing	IP-GRE encapsulation	MAC address rewriting cannot be used in IP spoofing deployments. See "Retaining the client IP address as the source IP address" on page 172 for more information.

WCCP traffic redirection requirements for request forwarding

If you have enabled one or more of the request forwarding options, you can use MAC address rewriting only if the appliances are connected to the server-side router interface. If you use IP-GRE encapsulation, you can use any interface on the router to redirect traffic to the appliances. See "Circumventing transparent redirection of client requests" on page 170 for more information about request forwarding.

See the Cisco documentation for information about additional limitations of MAC address rewriting.

Choosing a WCCP transmission method

Transmission methods between WCCP routers and appliances

NetCache supports both unicast and multicast transmission between WCCP routers and appliances. If your WCCP routers are configured for WCCP multicast, you can configure WCCP service groups for multicast transmission between WCCP routers and appliances. Unicast and multicast are defined as follows:

- With unicast transmission, communication occurs between one host and another, in this case, between a WCCP router and an appliance.
- With multicast transmission, multiple hosts can listen for transmission from one host. For example, all transmissions from a appliance for a service group configured for multicast are detected by all devices listening to the multicast address for that service group.

The advantages of using multicast transmission between members of a service group are as follows:

- Use of multicast significantly reduces network traffic.
- Less configuration is required in NetCache.

  With unicast transmission, you must explicitly identify WCCP routers with which the appliance interacts. If a router is later removed from the network, you must remove the router's IP address from the NetCache configuration.

  Network Appliance recommends that you select one transmission scheme for your WCCP transparency deployment—either unicast or multicast—to simplify configuration and management.

Configuration requirements for multicast

Configuration requirements for multicast transmission are as follows:

- If you want a WCCP router to handle multicast service groups, you must enable the router for multicast. (Most WCCP routers support multicast. See your Cisco documentation for information about how to configure routers for multicast.)
- Parameters for each service group, including the transmission method, must match in the service group configuration on all routers and appliances that will handle that service group.
- For each WCCP service group that you configure in NetCache, provide a multicast IP address. A multicast IP address does not have to be unique among service groups.

If you are using WCCP multicast transmission, Network Appliance recommends that you deploy the appliance on the same subnet as the WCCP router.. Thus, you can limit multicast transmissions to one subnet. Otherwise, you must enable general multicast transmission on all the routers between the appliance and the WCCP router.

Note

A WCCP router configured for multicast transmission can handle both multicast service groups and unicast service groups.

Choosing the optimum WCCP request distribution method

Influencing the number of requests redirected to each proxy-cache server

Part of a WCCP service group definition is defining the method the router will use to distribute requests across proxy-cache servers in the same service group that the router belongs to. (The request distribution method is also referred to as the *hashing* method.)

The WCCP request distribution method is designed to minimize duplication of objects between proxy-cache servers. Requests for objects from the same origin server are sent to the same proxy-cache server. When a proxy-cache server that was unavailable becomes available again, it takes over responsibility for handling requests for the same origin servers it handled previously.

Typically, you want to achieve an even distribution of requests across your appliances.

The following table shows the basic criteria available for request distribution and how they apply to the modes in which you can run an appliance.

For a NetCache running as...	Recommended distribution method (hashing)
A forward proxy	Destination IP address
An accelerator (also referred to as a reverse proxy)	One or both: ◆ Source IP address ◆ Source port

Forward proxy recommendations

When users send requests to arbitrary Internet servers (that is, when users send requests to many destinations), distribution on destination IP address provides the most equal distribution over multiple appliances that are running as forward proxies.

Accelerator recommendations

If you are deploying the appliance as an accelerator, distributing requests based on source IP address provides the best distribution. If your appliance is accelerating a single Web server and you set the distribution method to destination IP address, most (or all) requests will be sent to one appliance

because the destination IP address is the same for all requests. Even if your appliance is accelerating a few origin servers, the variation in destination IP addresses is limited.

For an accelerator, adding the criterion of hashing on source port, as well as source IP address, results in requests from the same client being distributed over multiple appliances. This distribution is created because the source port numbers are dynamically assigned by the operating system on the client and are in effect only for the duration of the connection.

Distributing load based on appliance platform type

Adjusting request distribution based on weighting

The WCCP Assignment Weighting Factor option (Setup tab > Transparency > WCCP > Global Settings) enables you to influence the amount of traffic sent to the appliance. The WCCP router uses this weighting factor, in conjunction with other basic request distribution criteria that you have provided, to determine the amount of traffic sent to this appliance. For example, if your deployment includes a C1100 and a C6100, you might want to specify weighting criteria so that the C6100, which can handle more requests, receives a greater portion of requests than the C1100. (You can set a weighting factor only for the appliance you are currently configuring. To set weighting factors for multiple appliances, you must configure each appliance separately.)

Each appliance can be assigned a weighting number between 0 and 255. For example, assume you set the following weights:

NetCache A: 255

NetCache B: 110

NetCache C: 75

The WCCP router adds the weights together to find a total and divides the traffic appropriately. In the preceding example, NetCache A receives 58 percent of the redirected traffic, NetCache B receives 25 percent of the redirected traffic, and NetCache C receives 17 percent of the redirected traffic.

The WCCP Assignment Weighting Factor setting works only with appliances. If your WCCP deployment contains appliances running releases earlier than 5.1 or third-party proxy-cache servers, you should set the weighting value to 0 (zero).

Determining if you need to load balance data over multiple NICs

Sending data over one network interface can limit throughput

Typically, in a transparent deployment with a WCCP router, NetCache chooses one network interface over which to deliver data to clients. However, delivery of data over a single network interface might not be optimal for some types of transparent proxy deployments.

For example, a streaming media cache can deliver streaming data to clients very quickly over multiple network interfaces. However, if the proxy is able to deliver streaming data over only a single network interface, the proxy is likely to become limited in its network throughput by the bandwidth of this single network interface.

How to deliver data over multiple network interfaces

By using the "WCCP NetCache IP Addresses for Load Balancing" option on the WCCP Global Settings page (Setup tab > Transparency > WCCP Global Options), you can enable NetCache to deliver data over multiple network interfaces; you list the NetCache network interfaces over which you want NetCache to deliver data to clients. If you leave the list blank, NetCache sends and receives data to clients over a single interface (per router), which NetCache chooses.

Usage guidelines for sending data over multiple network interfaces

Use the following guidelines to determine which, if any, NetCache network interfaces to list in the "WCCP NetCache IP Addresses for Load Balancing" option:

- You must include the interface used for the default route in your interface list. Otherwise, a traffic loop might occur.
- List only IP addresses for network interfaces through which this appliance communicates with clients. You would not, for example, list a network interface through which this appliance communicates with another appliance.
- Distribute traffic over multiple interfaces only when necessary. Typically, NetCache can deliver DNS, FTP, HTTP, and NNTP data over a single network interface without adversely affecting performance.

Securing access to your WCCP deployment

If you want to restrict WCCP group access

Network Appliance recommends that you use the WCCP service group password feature to restrict unauthorized users from joining a WCCP service group. The service group password, which you set by protocol, is for authentication between the appliance and all routers in the WCCP Routers list. You have the option to set a service group password when you create a new service group.

You can assign a different password to each service group or you can assign the same password to all service groups.

Note

You must configure the same password on all WCCP routers and proxy-cache servers that belong to a service group.

The WCCP password can consist of up to eight characters (no spaces are allowed).

Section D: WCCP service group reference information

About this section

This section provides guidelines for creating WCCP service groups and describes how to list multiple services in a service group.

Topics in this section

This section provides information about the following topics:

- "WCCP service group definition guidelines" on page 162
- "Listing multiple ports in a service group" on page 165

WCCP service group definition guidelines

WCCP service groups control communication

Communication between WCCP routers, appliances, and third-party proxy-cache servers is controlled by the *WCCP service group* to which the device belongs. Service groups comprise one or more proxy-cache servers and one or more WCCP routers. Service groups specify the type (or types) of traffic the router should redirect and the identity of all target proxy-cache servers.

About WCCP quick fill templates

Most basic service group definition tasks can be accomplished using the *quick fill template*s provided in the Appliance Manager and CLI. Quick fill templates provide service group details for the default traffic settings configured on the appliance. (These default settings correspond to the RFC-specified port settings for the specified traffic.) The quick fill templates should meet most of your service group requirements. You can alter entries provided by NetCache as necessary.

The Quick Fill Templates option is located on the New WCCP Service Group page. To access the New WCCP Service Group page, select Setup tab > Transparency > WCCP Service Groups, and then click New Group.

Note

IP spoofing requires additional service group configuration. See "IP spoofing deployment requirements for WCCP" on page 173 for more information about IP spoofing for WCCP.

Service group definition guidelines

The following table provides a brief summary of service group definition guidelines.

Recommendation	Reason
Attempt to define service groups using a quick fill template first.	The quick fill templates automatically provide defaults for most of the required service group information.

Recommendation	Reason
Define and enable the same service group on all proxy-cache servers and routers that you want to include in the service group.	Proxy-cache servers and routers that do not have a particular service group defined and enabled will not receive or redirect the specified traffic.
Assign a unique ID to each service group.	Different service groups cannot share the same ID. You can use any number between 0 and 255, but the number cannot already be assigned to another service group. This service group ID restriction applies only to enabled service groups.
Enable the protocol and associated ports for the traffic you are redirecting before defining a service group.	Disabled protocols and ports cannot be listed in a service group.
List client-side and server-side port numbers in separate service groups.	Client-side and server-side port numbers cannot be listed in the same service group.
List each type of port traffic in only one service group.	A specific type of port traffic must be handled by only one service group. For example, you cannot create one service group to handle HTTP TCP port 80 and another service group to handle HTTP TCP port 80 and TCP port 8080.
Create no more than eight service groups.	Currently, a WCCP router can be configured for only eight service groups. If you need to redirect more than eight types of traffic, you must list multiple services in a service group. Services that use the same transport protocols can be listed in the same service group.
Set a WCCP service group password.	The WCCP service group password restricts unauthorized users from joining a WCCP service group.
Define a client-side and a server-side service group if you are implementing IP spoofing.	For IP spoofing, you must define both client-side and server-side service groups so that server responses will be directed back to the appliances. For more information, see “IP spoofing deployment requirements for WCCP” on page 173.

Recommendation	Reason
Define and enable two client-side service groups for Apple QuickTime streaming: one for the control connection and one for the feedback connection. Network Appliance recommends that you enable two service groups for the control and feedback connections for all streaming media, including RealNetworks and Windows Media.	Apple QuickTime streaming requires the UDP feedback channel.

Defining service groups for streaming media

When streaming media is delivered to clients, separate connections typically exist for the control and feedback information. Although you can force streaming clients to use the control connection (TCP) only, you must allow both the control and feedback connections to ensure optimum streaming media quality. (Apple QuickTime streaming requires both the control and feedback channels.)

To redirect the streaming media control and feedback channels, you must define one service group for the control connection and another service group for the feedback connection.

MMS: For MMS streaming traffic, use the Dynamic Client MMS Control and Dynamic Client MMS Feedback quick fill templates to create the control and feedback service groups.

RTSP: For RTSP streaming traffic, use the Dynamic Client RTSP Control and Dynamic Client RTSP Feedback quick fill templates to create the control and feedback service groups.

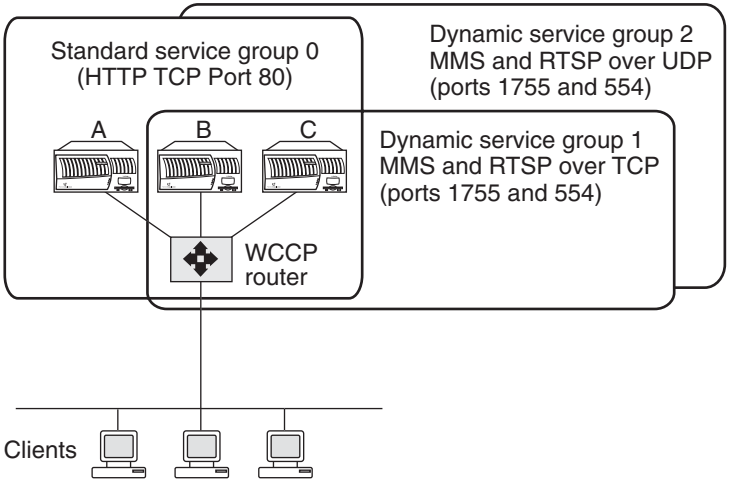
Listing multiple ports in a service group

A service group can be defined for multiple protocols

Although most service groups can be defined for a single protocol (such as FTP), you can define a service group for multiple protocols as long as the ports use the same transport protocol (such as TCP). You can list up to eight ports in each service group. Listing multiple ports is useful for instances when two protocols always accompany one another. For example, UDP ports 554 and 2001 must both be redirected if you want to redirect both RealNetworks and QuickTime streaming traffic.

Example of multiple service group configuration

The following illustration shows one router, multiple appliances, and multiple service groups.



Appliance A is configured to handle only HTTP requests. Appliance A belongs to standard service group 0.Appliances B and C are configured to handle HTTP requests and MMS and RTSP requests over both TCP and UDP. Therefore, appliances B and C are each configured to belong to three service groups—standard service group 0, dynamic service group 1 for MMS and RTSP over TCP, and dynamic service group 2 for MMS and RTSP over UDP.

The router in this example must handle HTTP, MMS, and RTSP requests. Therefore, the router belongs to standard service group 0 (HTTP), dynamic service group 1 (MMS and RTSP over TCP), and dynamic service group 2 (MMS and RTSP over UDP).

Section E: Additional transparency features

About this section

This section describes additional NetCache features that you can use to modify transparent proxying to meet your individual requirements.

Topics in this section

This section provides information about the following topics:

- "When you might need to modify transparency" on page 168
- "Circumventing transparent redirection of client requests" on page 170
- "Retaining the client IP address as the source IP address" on page 172
- "Hiding NetCache-generated error messages" on page 175
- "Preventing authentication errors for forward proxy clients" on page 176

When you might need to modify transparency

Why you might need to modify transparency

Because a proxy-cache server intercepts client requests, the server becomes part of the request-response chain. Most proxy-cache servers routinely replace the client IP address with the proxy-cache server IP address. In some circumstances, however, this behavior is not desirable. For example, servers that require IP-based authentication require the client IP address to be the source IP address on a request.

This section discusses the reasons you might want to modify transparency and how you can use NetCache to accomplish your goals.

Information to gather for optional features

The following table shows the information that you should gather about optional transparency features before you start transparent proxy configuration.

If you want to set up...	Gather this information...
Transparent HTTP authentication	Do you want to enable this feature for transparent FTP requests?
Stealth mode	If you want to hide NetCache-generated error messages from your users, see "About NetCache-generated errors" on page 175 for details.
IP forwarding	◆ IP addresses of servers for which you want this appliance to forward requests directly to the origin server ◆ IP addresses of origin servers that require client authentication
URL forwarding	◆ (HTTP and QuickTime RTSP only) URLs for which you want this appliance to forward requests directly to the origin server ◆ URLs of origin servers that require client authentication
Dynamic forwarding	HTTP status codes that you want to trigger dynamic forwarding

If you want to set up...	Gather this information...
IP spoofing	Protocols for which you want to set up IP spoofing **Note** IP spoofing is not available for QuickTime RTSP, DNS, FTP, and NNTP.

Circumventing transparent redirection of client requests

Options you can use to bypass transparent redirection

If you want certain types of client requests to bypass the appliance, you must configure one or more of the *request forwarding* options provided by NetCache. The request forwarding options are described in the following table.

Request forward method	Behavior
IP forwarding	Forwards requests for specified IP addresses directly to the origin server
URL forwarding	Forwards requests for specified URLs directly to the origin server
Dynamic forwarding	Redirects clients to the origin server after an initial request results in a specified HTTP response code

To access the request forwarding options in the Appliance Manager, select Setup tab > Transparency > Request Forwarding.

How to use the request forwarding options

The following table describes how to use the request forwarding options.

If you want to...	Use these features	Gather this information
Enable direct routing for servers that require authentication	IP forwarding URL forwarding	Record all IP addresses or URLs that require authentication
Enable direct routing for servers that require client logging data	IP forwarding URL forwarding	Record the IP addresses or URLs of servers that require client logging information
Enable direct routing for requests that cannot be satisfied by the appliance	Dynamic forwarding	Identify the HTTP status codes that you want to result in direct routing

IP and URL forwarding restrictions

The following restrictions apply to the request forwarding options:

- IP forwarding is a global option that applies to all protocols that have been enabled for transparency.
- URL forwarding is applicable only to HTTP and RTSP.
- You cannot enable IP spoofing and the request forwarding options for the same protocol.

Note

If you have IP spoofing enabled and want to bypass specific IP addresses, you can use the "Enable tunneling of server IP addresses" option to bypass them (Setup tab > HTTP > Tunneling).

- NetCache does not cache objects associated with the requests that are being forwarded as a result of IP or URL forwarding. Objects are not cached because the origin server returns the objects directly to the client, not through the appliance.

How request forwarding works

When you enable a request forwarding method, NetCache returns client requests to the network for direct routing to the client. Therefore, requests arrive at the destination server with the client's IP address intact. The origin server then responds directly to the client.

Retaining the client IP address as the source IP address

About IP spoofing

You can use the appliance IP spoofing feature to configure NetCache to use the client IP address as the source address when communicating with servers. Requests originating from a client retain the client's source address even if requests are passed through a chain of proxy-cache servers. The requests, therefore, appear to originate from the client rather than from the appliance.

Note

Even when IP spoofing is enabled, the appliance can continue to send one of its IP addresses to the origin server, instead of using the client's. For example, if a DNS lookup results in an IP address that is different than the one the client requested, the appliance uses one of its IP addresses to ensure that content is redirected back to it. You can force the appliance to always send the client IP address by enabling the "Force HTTP IP spoofing for certain servers" option (Setup tab > Transparency > Transparency and IP Spoofing Enable).

Unlike request forwarding, NetCache intercepts the responses from origin servers and caches objects fetched on behalf of the spoofed client. The symmetric routing allows you to gather more accurate client statistics in origin server logs than would be possible if the appliance IP address were used to initiate the connection to the server.

To access the IP spoofing options, select Setup tab > Transparency > Transparency and IP Spoofing Enable.

IP spoofing restrictions

The following restrictions apply to IP spoofing:

- IP spoofing must be set by protocol. It is not applicable to DNS, FTP, NNTP, and QuickTime RTSP transparent proxying.
- Routing between the client and the origin server must be symmetric so that server responses are redirected to the same appliance that the client traffic was sent through.
- If a hierarchy is configured on your appliance and parent caches are identified, the appliance must be in a location on the network where it can intercept the traffic between the requesting client and the parent caches.
- To enable IP spoofing for streaming media, you should enable IP spoofing for HTTP, in addition to RTSP or MMS, so that server-side HTTP-encapsulated streaming media is also redirected to the appliance.

- IP spoofing is incompatible with the request forwarding options (Setup tab > Transparency > Request Forwarding). If you have IP spoofing enabled and want to bypass specific IP addresses, you should use the "Enable tunneling of server IP addresses" option to bypass them.

IP spoofing deployment requirements for WCCP

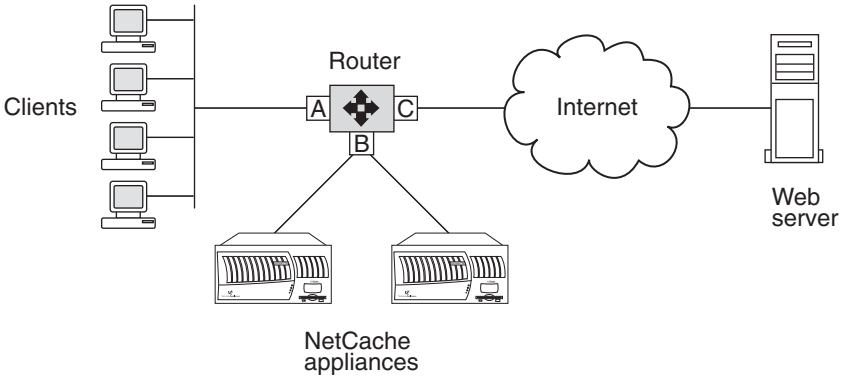
IP spoofing deployments require symmetric routing so that server responses are redirected to the same appliance that received the client request. To implement IP spoofing for WCCP, the following conditions must be met:

- The WCCP router must support an inbound redirection feature.
- Separate router interfaces must be assigned to appliances, clients, and servers.
- Inbound redirection filters must be set on the WCCP router for both client-side and server-side traffic.

The following sections describe these conditions.

WCCP router inbound redirection feature support: Before implementing IP spoofing, contact your Cisco representative to ensure that your WCCP router supports inbound redirection. At the time of this writing, Cisco routers that support the MAC address rewriting feature do not support the inbound redirection feature. Therefore, you cannot deploy IP spoofing with routers that support MAC address rewriting.

Assignment of separate router interfaces: In addition to dedicating one interface on the router to clients and another interface to origin servers, you must dedicate a router interface for the appliances, as shown in the following illustration (A, B, and C represent the separate interfaces).



Inbound redirection filters: In the router configuration, an inbound redirection filter based on the client-side WCCP service group must be applied on the client-side interface of the router in order to route client-to-server traffic to the appliances. Similarly, an inbound redirection filter based on the server-side WCCP service group must be applied on the server-side interface of the router to route server-to-client traffic to the appliances.

Hiding NetCache-generated error messages

About NetCache-generated errors

NetCache provides detailed messages about errors it detects and information about how to resolve the problem that caused the error to occur. If you do not want end users to be aware that a Web cache is being used, you can suppress NetCache messages and instead display more generic, less detailed Web browser messages. Hiding the existence of a Web cache is sometimes referred to as running in *stealth mode*.

Use stealth mode to hide NetCache error messages

If you want to hide NetCache error messages, you can configure NetCache for stealth mode. If stealth mode is enabled, the browser provides the error message. The error message that is displayed is browser-specific. Users of a particular browser will always see the same message, no matter what the error condition.

Stealth mode is enabled by the "Do Not Report Errors to Selected Clients" option on the HTTP - General page. To access this page, select Setup tab > HTTP > General. See the Appliance Manager online Help for stealth mode configuration information.

Note

Stealth mode can be used for both transparent and nontransparent proxying of HTTP requests.

Preventing authentication errors for forward proxy clients

Why proxy authentication errors occur

When a proxy-cache server is operating in transparent mode, Web browsers and media players do not normally have the host name of that proxy-cache server in their proxy settings configuration. When a Web browser or media player is not aware of the existence of a proxy-cache server and it receives a proxy authentication request, it displays an error message and does not prompt the user for a password.

NetCache solution for authentication and transparent proxying

Network Appliance has designed an authentication scheme for HTTP transparent proxying. This authentication scheme does not conform to the HTTP 1.1 specification. If you enable this feature, NetCache violates the HTTP specification because it inserts and strips 401 authentication requests.

To access the NetCache HTTP Transparent-Mode Authentication option, select Setup tab > Authentication > General.

Important considerations for determining whether to use HTTP authentication with transparency

Consider the following when determining whether to use authentication for transparent proxying:

- If IP addresses do not form a one-to-one association with users or computers

  If you expect access to occur through an address translation device or through multiple Web browsers on a compute server, users trying to authenticate simultaneously might obtain shared privileges, might never be prompted, or both.
- When the IP address in the cache expires (for a previously authenticated client) and a user requests 401 (unauthorized) protected content from an origin server, an end user might be prompted for multiple credentials consecutively, if the request is for a site that also requires HTTP-based authentication.

How the NetCache authentication scheme works

NetCache inserts 401 (unauthorized) requests into transparent proxy requests to obtain an authentication credential from a Web browser. The Web browser sends the credential until the user accesses another site. NetCache caches the IP addresses of clients so that it can determine which clients have been

authenticated to use the appliance and determine the credentials that the clients used. IP addresses in the cache expire after a period of time that you can configure.

Note

For Web accelerators, the appliance does not need to cache client IP addresses. When the appliance is deployed as a Web accelerator, it represents the Web site to be authenticated.

Section F: Troubleshooting transparency

About this section

This section contains information to help you troubleshoot your switch or WCCP router transparency setup. Choose the troubleshooting actions that are applicable to the protocols that you are deploying transparently.

Topic in this section

This section provides information about the following topic:

- "Troubleshooting your switch or WCCP router deployment" on page 179

Troubleshooting your switch or WCCP router deployment

Troubleshooting tips for both switch and router deployments

The following table shows several items to check if you encounter problems while testing transparency settings in the Appliance Manager. Select the troubleshooting actions based on the protocols for which you are setting up transparent proxying.

Action	Applicable protocols	Details
Check that the devices in your transparency deployment are accessible.	DNS FTP HTTP NNTP MMS RTSP	At a client computer, complete the following steps from the command line: **1.** Ping the IP address of the router. **2.** Ping the IP address of the appliance.
Confirm that the request is being sent through the switch or WCCP router.	DNS FTP HTTP NNTP MMS RTSP	Trace the route of a client request to the target server to ensure that the requests are being sent through the switch or WCCP router. A tool such as `traceroute` for UNIX can help you trace the route of requests.
Check whether the client is connected to the streaming media cache.	MMS RTSP	Complete the following steps: **1.** At a client computer that is excluded from transparent proxying, request the media stream that the user reported was not working. **2.** Check the Streaming access log to determine if the client connected to the streaming media cache. If the stream is not delivered or if it is not playing as you expect, a problem with the MMS or RTSP transparent proxying configuration on the appliance might exist.

Action	Applicable protocols	Details
Check whether the client is connected to the streaming server.	MMS RTSP	In the Appliance Manager, select Data tab > Streaming > Detailed Statistics. View the detailed statistics to determine whether the client is connected to the streaming server. Transparent proxying of MMS or RTSP service is working if you see an entry with the IP address of the client from which you made the media request and the name of the media file that you requested. Transparent proxying of MMS or RTSP is not working if no entry exists.
Check whether the streaming media configuration options are configured correctly.	MMS RTSP	In the Appliance Manager, select Setup tab > Streaming Media > RTSP and MMS. Verify the following on the pages: ◆ MMS, RTSP, or both (as applicable) are enabled. ◆ All relevant streaming media options are configured. All options relevant to the streaming protocol that you are deploying are required. See the online Help for information about configuring these settings.

Action	Applicable protocols	Details
Check whether the transparency settings are configured correctly.	DNS FTP HTTP NNTP MMS RTSP	Check the Transparency and IP Spoofing Enable page to see if transparent proxying is enabled for all the protocols you are deploying transparently. **For WCCP router deployments only:** If you configure the WCCP options in the Transparency pages for a particular protocol but forget to enable transparency for that protocol, the IP address of the appliance appears in the router configuration in the list of Web caches, news caches, and streaming media caches that the router is aware of. However, the appliance does not service any requests. Check the Transparency - WCCP Service groups page to see if WCCP is enabled for the protocols you are deploying transparently. Compare the WCCP service group information you set on the appliance to the service group information configured on the WCCP router to see if: ◆ The service group numbers match the service groups configured on the WCCP router. ◆ If you configured a WCCP password, it matches the password you configured on the router for the same service group. Also check whether you set the port settings correctly, as described in “Determining port numbers for redirected traffic” on page 141.

Action	Applicable protocols	Details
Check the WCCP statistics on the appliance.	DNS FTP HTTP NNTP MMS RTSP	The WCCP statistics on the WCCP - General page in the Appliance Manager are useful for debugging problems with your transparent proxy deployment with a WCCP router. These statistics show totals for all service groups to which this appliance belongs. However, by enabling and disabling some settings on the Transparency and IP Spoofing Enable page, you can determine whether WCCP is working for specific service groups. You can view statistics for only one service group by doing the following: **1.** Select Setup tab > Transparency > Transparency and IP Spoofing Enable. Disable WCCP for all but one protocol. Commit your changes. **2.** Select Data tab > WCCP > General. Record the numbers shown in the WCCP statistics. **3.** Send a request of the type of protocol for which WCCP is enabled. **4.** Check the WCCP statistics on the WCCP - General page again to determine if the numbers increased. If they have, you know that WCCP is working for the service group (protocol) for which WCCP is enabled. **Note** It is not necessary to start with the statistics showing 0. For this test, you are trying to determine if the WCCP router and the appliance are communicating, rather than looking at the actual numbers. **5.** Repeat Steps 1 through 4 for each of the protocols for which you are configuring transparent proxying with a WCCP router.

Action	Applicable protocols	Details
Check whether the switch is configured correctly.	DNS FTP HTTP NNTP MMS RTSP	Check the switch to confirm that the switch is configured to pass to the appliance requests of the protocols for which you are deploying transparent proxying. If the switch is configured incorrectly, your appliance might not receive any traffic. If your switch is configured correctly and you can confirm that the appliance is receiving traffic, verify that your routing scheme is configured so that NetCache can send requests to the WAN. For MMS and RTSP, ensure that the switch is configured to pass requests for both TCP and UDP to the streaming media cache. If your deployment includes RTSP for QuickTime, ensure that you have specified the RTCP port and that you have configured the switch to pass traffic for the RTCP port to the appliance. For FTP, ensure that the switch is set to redirect port 21 requests to this appliance and no other. **Note** Do not set `proto any` on Alteon switches.

Action	Applicable protocols	Details
Check whether the router is configured correctly.	DNS FTP HTTP NNTP MMS RTSP	On the router, use WCCP commands described in your WCCP documentation to troubleshoot your WCCP router configuration. Check the following: ◆ Ensure that the router is configured to pass requests for all protocols for which you are deploying transparent proxying to the appliance. ◆ Ensure that the service group for each protocol in your transparent proxy deployment is enabled on the router. ◆ For each service group, ensure that you have entered the following command to apply a filter to the router's outbound (or inbound for IP spoofing) interface. Otherwise, the router cannot redirect the appropriate packets to a appliance. For HTTP (Standard Service Group 0), enter the following at the command line: **`ip wccp web-cache redirect out`** For NNTP, MMS, or RTSP, enter the following at the command line: **`ip wccp n redirect out`** In the preceding example, *out* represents the router's outbound interface. If you want to redirect inbound traffic, specify the following: **`ip wccp n redirect in`** ◆ Determine whether the router is aware of all appliances that belong to the same service group as the router. For HTTP, enter the following at the command line: **`show ip wccp web-cache detail`** For NNTP, MMS, or RTSP, enter the following at the command line: **`show ip wccp n detail`** where *n* is the number of the service group for which you want to list members.

Action	Applicable protocols	Details
Check whether the router is configured correctly (continued).	DNS FTP HTTP NNTP MMS RTSP	◆ Determine if the optional WCCP password that you configured on the router for the service group matches the WCCP password that you configured on the Create a WCCP Service page for the same service group. ◆ Turn on the `wccp debug` mode, as necessary, to obtain more debug information on the router. ◆ For MMS and RTSP, ensure that the router is configured to pass requests for both TCP and UDP to the streaming media cache. ◆ For FTP, ensure that the router is set to redirect port 21 requests to this appliance and no other.
Check the WCCP statistics on the router.	DNS FTP HTTP NNTP MMS RTSP	Check the statistics on the router. **1.** For HTTP, enter the following command: **`show ip wccp web-cache`** **2.** For FTP, NNTP, MMS, and RTSP, enter the following command: **`show ip wccp n`** where *n* is the service group number of the protocol for which you are testing. **3.** Record the Number of Cache Engines and Total Packets Redirected values. **4.** Submit a request. **5.** Check the router statistics again, comparing the number shown in the Total Packets Redirected statistic to the number you recorded previously for this statistic.

NetCache Appliance Takeover 12

About this chapter

This chapter helps you plan NetCache takeover configuration and monitor the status of NetCache appliances configured as takeover partners.

The NetCache takeover feature provides a way of setting up automatic failover between two NetCache appliances. This feature is useful if you are not using an L4 or L7 switch or a WCCP router with transparency to enable client access to NetCache appliances. (With an L4 or L7 switch or a WCCP router and transparency, if a NetCache appliance becomes unavailable, the switch or router automatically fails over to another NetCache appliance or the Internet.) With NetCache takeover, you configure two NetCache appliances as a takeover pair, thereby setting them up to monitor each other's status and take over for each other in case of failure.

Note

See the *Deployment Guide* for details about how the NetCache takeover feature works, the services it supports, and deployment considerations.

Topics in this chapter

This chapter provides information about the following topics:

- "Planning summary for NetCache takeover configuration" on page 188
- "Obtaining information about takeover status" on page 190

Procedures and option descriptions

See the Appliance Manager online Help for configuration procedures and option descriptions.

Location of configuration options

Options for configuring NetCache takeover are in the following location in the Appliance Manager:

Setup tab > Takeover > All Settings

Planning summary for NetCache takeover configuration

Determine NetCache takeover configuration

Configuring NetCache takeover will be faster if you plan ahead. Use the information in the following table to determine the configuration that is necessary for your organization.

Decisions to make	Considerations
Which IP address of the network interface on this NetCache appliance is to be dedicated to receive heartbeat messages from the takeover partner.	◆ Do not send proxy traffic to this interface. ◆ This interface must be on the same LAN as the takeover interface of this NetCache appliance. ◆ You cannot configure the Listen Addresses option on the Setup tab > Network > General page and takeover.
Which IP address of the network interface on the other NetCache appliance is to be dedicated to receive heartbeat messages from this NetCache appliance.	
Whether to configure a single mode virtual interface (VIF) with NetCache takeover.	Configuring a single mode VIF (virtual interface) with NetCache takeover enables you to achieve a higher fault tolerance than can be achieved with NetCache takeover alone. For an illustration of the use of a single mode VIF with takeover, see the *Deployment Guide*. For more information about virtual interfaces, see Chapter 2, "NetCache Network Interfaces," on page 13.

Decisions to make	Considerations
Whether to enable protocol and user authentication.	If you enable protocol and user authentication, do one of the following so that takeover works correctly: ◆ Configure the same user names and passwords on both partners. ◆ Run an LDAP server or RADIUS server and have both NetCache appliances point to it.
Whether to set access controls.	Users are allowed or denied access to NetCache services and content based on which NetCache services they request. You must configure access control parameters the same on both takeover partners. Otherwise, if a takeover occurs, some users might not be able to access content that they could access before the takeover.
Whether to set URL restrictions.	Users are allowed or denied access to content based on which NetCache appliance services they request. You must configure URL restrictions identically on both takeover partners. Otherwise, if a takeover occurs, users might not be able to access content that they could access before the takeover occurred. Conversely, users might be able to access content that they were restricted from accessing.

Obtaining information about takeover status

Takeover event messages in the Messages log

When one partner takes over for the other partner, the following message is logged in the Messages log, indicating that takeover occurred:

```
Took over addresses of partner.
```

When one partner gives back responsibility to the other partner, the following message is logged in the Messages log:

```
Gave back addresses of partner.
```

You can view the Messages log on the Log Files - Messages page (Data tab > Log Files > Messages) in the Appliance Manager.

Status page messages

The Takeover - Status page (Data tab > Takeover > Status) in the Appliance Manager also shows the current state of the partner of the NetCache appliance.

Hierarchies 13

About this chapter

This chapter discusses the NetCache hierarchy feature and how the NetCache appliance handles requests it cannot resolve. The hierarchy feature allows you to configure NetCache appliances, third-party proxy-cache servers, and firewalls to work together to load balance requests, distribute content, or provide backup and failover capability for your network. The hierarchy feature is flexible, and it enables you to create simple to complex schemes.

Topics in this chapter

This chapter contains the following topics:

- "Planning decisions to be made" on page 192
- "About hierarchies" on page 193
- "Types of hierarchies" on page 195
- "Cluster hierarchies" on page 198
- "Hierarchy authentication and access control" on page 200
- "Standard request distribution" on page 202
- "Custom rules for distributing requests" on page 204
- "Hierarchy configuration example" on page 209
- "Troubleshooting a hierarchy configuration" on page 214

Procedures and option descriptions

See the Appliance Manager online Help for configuration procedures and option descriptions.

Location of configuration options

To access the hierarchies options in the Appliance Manager, select:

Setup tab > Hierarchies

Planning decisions to be made

Deployment decisions to be made

This chapter will help you make the following deployment decisions:

- Whether a hierarchy would be beneficial to your NetCache deployment
- Type of hierarchy that best fits the needs of your NetCache deployment

Decisions you should make before configuring your hierarchy

Before you begin to set up a hierarchy, it is a good idea to consider membership roles and gather information specific to each member (proxy-cache server or firewall) of your hierarchy. Consider the following:

- If a firewall exists in the NetCache environment, whether special NetCache configuration is required.
- If you want an authentication scheme, and where in the hierarchy to implement the scheme.
- Whether you need to customize how requests are distributed among hierarchy members.
- How you want each NetCache appliance to interact with other proxy-cache servers and firewalls in your organization.
- Distribution modes and protocols that the hierarchy feature supports.
- Whether you need to identify each hierarchy member to your NetCache appliance as a logical parent, a logical neighbor, or a firewall.
- Whether you need to create custom hierarchy rules or whether hierarchy rules supplied by NetCache are sufficient for your organization. For example, consider whether you want to designate a specific NetCache appliance in your hierarchy to service a specific protocol or request type.

Information to gather before you continue

Before continuing with NetCache configuration, ensure that you have the following information:

- Host name of all caches to be configured in the hierarchy
- HTTP ports used by each cache in the hierarchy

About hierarchies

What is a hierarchy?

The NetCache hierarchy feature imposes a logical structure on top of a physical network. This structure enables a NetCache appliance to forward requests it cannot resolve to other NetCache appliances, third-party proxy-cache servers, and firewalls. Hierarchies are commonly used for Web cache and streaming media cache configurations, and are typically configured to

- Distribute content over multiple caches
- Provide load balancing and failover capability
- Provide backup for single hosts

Note
The NetCache hierarchy feature does not apply to news cache configurations.

Purpose of a hierarchy

Hierarchy configurations affect traffic *outbound* from the NetCache appliance on which you configure the hierarchy. Hierarchies enable you to define what occurs when the NetCache appliance you are configuring cannot resolve a request, that is, what happens when a *cache miss* occurs. A cache miss occurs in the following situations:

- A NetCache appliance does not have the requested cacheable object in its cache.
- The requested object is noncacheable. For example, the requested object contains secure data, personal Web pages, or any HTTP objects (URL substrings, MIME types, and object extensions) that you do not want the NetCache appliance to cache.

With no hierarchy configured, the NetCache appliance forwards the request to the Internet and attempts to retrieve the requested object from the origin server.

With a hierarchy configured, the NetCache appliance forwards the request to the next level up in the hierarchy, to its *parent* cache. If the parent cache has the object, it returns the object to the NetCache appliance, the *child* cache. If the parent cache does not have the object, it retrieves the object from the Internet on behalf of the child cache.

Logical roles

Each member of a hierarchy is assigned a logical role, and each member is configured according to protocol, port, and any requirements for authentication. A hierarchy member can be logically identified as a parent, child, or neighbor.

Logical role	Description
Parent	NetCache appliances, third-party proxy-cache servers, and firewalls can be identified as a parent. Parents can fetch objects directly from the Internet on behalf of the NetCache appliance you are configuring.
Child	When you identify a parent or firewall as a member of the hierarchy, the NetCache appliance you are configuring is the *child* of that parent or firewall.
Neighbor	NetCache appliances and third-party proxy-cache servers can be identified as a neighbor. Neighbors can accept a query for a requested object from another NetCache appliance or from a third-party proxy-cache server. Neighbors cannot fetch objects directly from the Internet on behalf of another cache. **Note** Neighbors cannot be assigned in streaming media cache configurations.

Firewalls as hierarchy members

Firewalls filter client requests and prevent a company's network devices from sending traffic directly to the Internet; they are responsible for connecting to origin servers. Because some requests must be sent to origin servers on the Internet, a firewall must be explicitly identified as a hierarchy member.

Note

Transparent firewalls give the appearance that users are connecting directly to origin servers. You do not need to identify transparent firewalls in NetCache appliance hierarchies because requests are routed to the Internet through the NetCache appliance default gateway.

Types of hierarchies

Common configurations

Hierarchies control how NetCache forwards unresolved requests. They are configured on an appliance-by-appliance basis; that is, a hierarchy configuration provides instructions *only* for the appliance on which the hierarchy is configured. No other NetCache appliance, third-party proxy-cache server, origin server, or firewall is aware of any hierarchy that is configured on another NetCache appliance. Common hierarchy configurations include

- Single host (a single parent cache or a single firewall)
- Parent cluster or firewall cluster
- Neighbor

Hierarchies that contain a single parent or firewall

The simplest type of hierarchy has one member in addition to the NetCache appliance being configured, that is, one proxy-cache server or one firewall. You would configure a single-member hierarchy if

- Your NetCache appliance does not have direct connectivity to the Internet.
- You want another proxy-cache server to provide content control for your NetCache appliance.

Cluster hierarchies

A cluster is a group of proxy-cache servers (parents) or firewalls over which the NetCache appliance distributes requests. Clusters do the following:

- Load balance requests over multiple proxy-cache servers or firewalls that handle the same protocol
- Fail over to maintain connectivity if any member of the cluster goes down

For more information see, “Cluster hierarchies” on page 198.

Neighbors

A neighbor is a logical role that can be assigned to hierarchy members on a Web cache. Neighbors cannot fetch objects directly from the Internet on behalf of another cache; however, they can accept a query for a requested object from another NetCache appliance or from a third-party proxy-cache server.

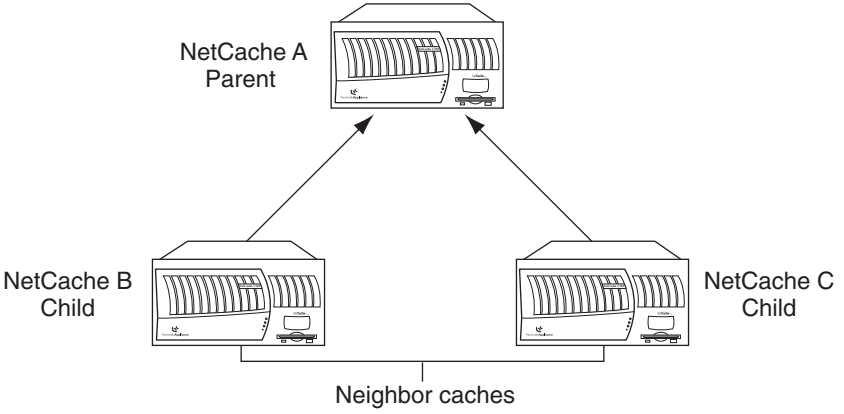
The communication protocol used to contact neighbors is always ICP (Internet Cache Protocol). ICP is a query-based communication that increases traffic without significantly increasing hit rate. ICP overhead can introduce network latency.

Note

Streaming media configurations do not support neighbors.

Neighbors as hierarchy members

The following illustration shows a hierarchy that includes a neighbor. In this case, one of the hierarchy members is identified as a parent and the other is identified as a neighbor. If your hierarchy includes a neighbor, ICP is used to query each hierarchy member to resolve a request.



About ICP

ICP is a method of distributing requests within a cache hierarchy. A derivative of the User Datagram Protocol (UDP), ICP enables NetCache to query other caches for individual Web pages. If ICP is configured as a distribution method, the only UDP packets that NetCache sends or receives are ICP packets. NetCache accepts all UDP packets and then drops any UDP packets that are not ICP.

Note

ICP is used for querying for availability of objects only, not for the actual fetching of objects. Fetching of objects is done using the protocol specified in the URL.

ICP can be configured to support multiple parent caches, a parent and a neighbor, or multiple firewalls. Before you enable ICP as a distribution method, consider the following:

- ICP is a query-based communication.

  When ICP is enabled, the child cache queries each hierarchy member to determine if a member of the hierarchy has the requested object. This method increases traffic without significantly increasing hit rate; that is, ICP can introduce latency.

- Load balancing and failover are not supported.

  Unlike a cluster configuration, if the hierarchy consists of multiple parents, the child cannot balance requests over the two parent caches.

Note

Network Appliance recommends using ICP only for backward compatibility with squid-based caches.

Cluster hierarchies

About clusters

A cluster is a group of two or more proxy-cache servers (parents) or firewalls over which the NetCache appliance distributes requests. You can specify multiple proxy-cache servers or multiple firewalls to be members of a logical *cluster*. The cluster acts as a parent to the NetCache appliance you are configuring. Cluster hierarchies load balance by distributing requests across multiple parents and provide failover if any member of the cluster goes down.

Cluster load balancing

Load balanced requests are distributed from a child cache across multiple parents. Load balancing is advantageous for networks in which the volume of requests for service is difficult to predict.

For load balancing to occur, at least two cluster members must handle the same protocol. The NetCache appliance on which you are configuring the hierarchy uses a proxy-selection algorithm to determine which hierarchy member in the cluster can best handle the request. The appliance then sends the request only to that hierarchy member.

Note

Load balancing requests among NetCache appliances that vary in capacity can overwhelm a smaller cluster member. Load balancing is most effective among members of like capacity.

Cluster failover

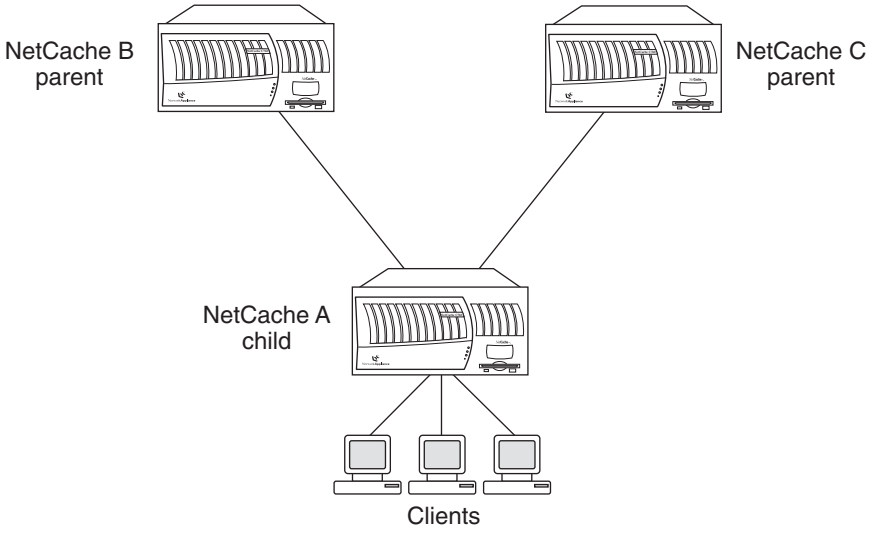
Failover provides a mechanism for two NetCache appliances, third-party proxy-cache servers, or firewalls to serve the same functionality. If one member of the cluster goes down, the NetCache appliance you are configuring sends the request to another cluster member.

The NetCache hierarchy feature can be set up to monitor direct connectivity and provide failover to another cache if an Internet connection goes down.

For more information, see "Custom rules for distributing requests" on page 204.

Cluster hierarchy configuration

The following illustration shows a cluster hierarchy configuration. Load balancing and failover occur automatically between cluster members.



Note

Proxy-cache servers or firewalls that handle multiple protocols can be configured as members of more than one cluster in a hierarchy.

Hierarchy authentication and access control

Types of authentication

Members of a hierarchy can be configured to authenticate users, or they can be configured to authenticate to each other.

User authentication can be enabled on proxy-cache servers that receive user requests.

Hierarchy authentication can be enabled at higher levels, where requests are sent from proxy-cache servers at lower levels in the hierarchy. Multiple NetCache appliances can use the same user name and password to log in to a parent that requires hierarchy authentication. For example, you could require a child to authenticate to a parent cache. Similarly, you could require authentication between a child and cluster members.

Planning hierarchy authentication

When creating a plan for hierarchies, you need to determine whether you want to require lower-level NetCache appliances to authenticate to other members of their hierarchy. If you decide to require authentication, consider

- The level at which to enable authentication, and whether you should require user authentication or hierarchy authentication
- How you want request records shown in log files

  You must decide what kind of request records you want in the log files at each level in the hierarchy. Whether the log files on parents and cluster members show the child NetCache appliance or the client depends on how you set up your hierarchy authentication scheme.

  For information about log file entries, see the log file information in the online Help.

Child authentication schemes

When making decisions about how the NetCache appliance you are configuring (the child) authenticates to other members of the hierarchy, consider that a child can be configured to authenticate to a parent or pass client authentication to a parent.

Parent authenticates child: If you enable user authentication on the parent, then the parent database (NetCache, LDAP, or RADIUS) must contain the child's user name and password information. The child must be configured to send its user name and password to the parent. In the NetCache log file entries, the child proxy-cache server is identified as the sender of the request.

Parent authenticates clients (passthrough): If you enable passthrough for authentication, the child passes client authentication to a parent. User authentication must be enabled on the cache that is authenticating the user. It is not necessary to enable authentication on both the parent and the child. In the NetCache log file entries, the client is identified as the sender of the request.

Content filtering within the hierarchy

Content filtering is most effective when performed by the child cache. If access restrictions are imposed on the child, then restricted content that can be accessed from the parent cannot be cached on the child. For example, if a user authenticates to a parent that allows access to restricted content, that user can make the content available to all users who have access to the child.

Consider an international ISP (NetCache Canada) that wants to prevent access to specific Web content in the United States (NetCache USA). An effective scheme to control access to content could be set up as follows:

- NetCache Canada identifies NetCache USA as a parent, and is configured to forward all requests for origin servers in the United States to NetCache USA.
- NetCache Canada is configured to authenticate users. Access controls are set to prevent access to specific content from U.S. Web sites.
- NetCache USA is configured to authenticate NetCache Canada. The database on NetCache USA must contain a user name and password to authenticate NetCache Canada.

Note

Access control settings on higher-level proxy-cache servers are effective if all child caches have exactly the same access restrictions.

Where to find more information

For information about setting up authentication and access control for hierarchy members, see the *Security Guide*.

Standard request distribution

About default forwarding

NetCache forwards unresolved outbound requests based on the information entered when the hierarchy is configured. Default settings can be enabled on the Hierarchies - General page in the Appliance Manager (Setup tab > Hierarchies > General). The NetCache default settings for distributing outbound requests are highly efficient, and most organizations do not require custom settings. For example, you can enable default hierarchy forwarding rules to send

- Requests for local servers or the local domain directly to local servers
- Requests for noncacheable objects directly to origin servers
- Protocol-specific requests to hierarchy members that support the same protocol

  The NetCache hierarchy feature supports default forwarding rules for handling HTTP, FTP, FTP over HTTP, Gopher, Tunnel (HTTPS), MMS, and RTSP protocol requests.

Note

If you are configuring a hierarchy for a Web cache, all hierarchy members handling transparent FTP must be NetCache appliances.

Distribution methods

Distribution methods are settings that control how NetCache forwards unresolved requests. You define the distribution method when you create a forwarding rule on the Hierarchies - Forwarding Rules page (Setup tab > Hierarchies > Forwarding Rules).

NetCache can be configured to distribute unresolved requests in one of the following ways:

- Direct—Send requests directly to the origin server, a local domain, or an origin server on the Internet. The NetCache appliance does not send a request through another proxy-cache server or firewall. This method of distribution requires the NetCache appliance to have direct connectivity to the Internet.
- Single host—Send requests to a specified proxy-cache server or firewall.
- Parent cluster or firewall cluster—Load balance requests over multiple parents or multiple firewalls that handle the same protocol.

- ICP (Internet Cache Protocol)—Query other cache hosts within the hierarchy for individual Web pages. ICP is always used for communicating with neighbors.

Direct monitor

Direct monitor is a basic hierarchy setting on the Setup > Hierarchy > General page that enables NetCache to monitor Internet connectivity by establishing TCP connections with each host specified. When attempts to connect to all hosts fail, the Internet connection is considered down and NetCache fails over to the next forwarding rule for directing requests. Failover can be enabled or disabled on a per-rule basis. See "Custom settings to support failover" on page 206 for more information.

Note

To designate a direct path to the Internet that supersedes host defined connections, you must create a hierarchy forwarding rule to identify and set the distribution method for a particular host to "direct."

Custom rules for distributing requests

Using custom settings to direct requests

NetCache default settings for distributing outbound requests are highly efficient, and most organizations do not require custom settings. However, custom rules can be created to direct requests to hierarchy members or to origin servers that are local or remote to the NetCache appliance you are configuring. For example, custom rules can be set to

- Direct requests of a specific type to a specific hierarchy member
- Specify a backup host for failover

You define custom rules by creating forwarding rules on the Hierarchies - Forwarding Rules page (Setup tab > Hierarchies > Forwarding Rules).

Note
Logical roles must be assigned before custom rules are created.

Custom settings disable default forwarding

If you create a rule to handle a protocol-specific request, default forwarding for all related protocols is disabled. This means that in addition to creating a rule to direct a protocol to a specific member of the hierarchy, you must also create a rule to manage the remainder of HTTP, FTP, FTP over HTTP, Gopher, and Tunnel requests and all other supported protocols to other members of the hierarchy.

Ordering rules

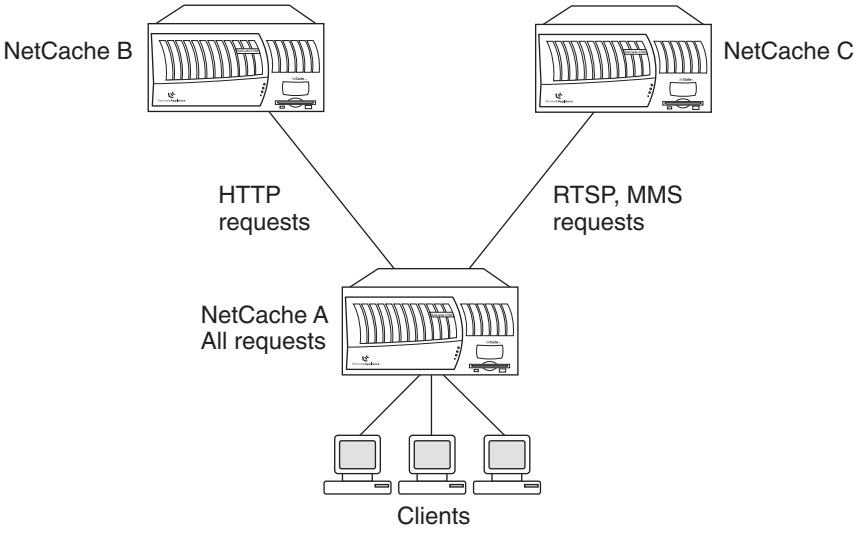
NetCache executes rules in the order in which they are listed. If you create custom rules for directing requests, consider whether you need to modify the order of those rules to ensure that specific rules are executed before general rules. For example, if you create a custom rule to designate a backup host or a backup cluster, order the rule lower in the rules list than a primary host rule or cluster rule. This way, the backup rule is executed only if the primary rule fails

In another example, assume that you want all HTTPS requests to be tunneled to a specific host. List the custom rule that directs tunnel requests to a specific host before the more general noncacheable rule.

Custom settings for directing requests

Custom rule settings can be used to forward requests of a specific type to a specific hierarchy member.

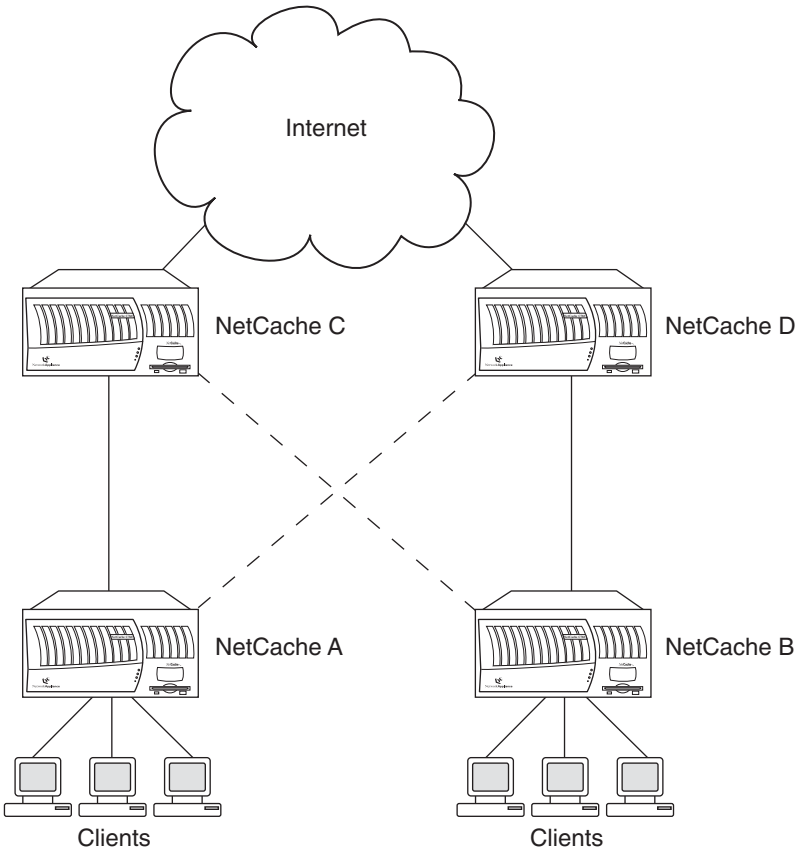
In the following example, custom settings on NetCache A forward all HTTP requests to NetCache B and forward all requests for streaming media to NetCache C. Custom rule settings for HTTP, MMS, and RTSP disable automatic distribution for all protocols. This means that NetCache A must also be configured with a custom rule that specifies forwarding for FTP, Tunnel, and Gopher requests.



Custom settings for specifying primary host backup

Custom rule settings can be used to specify a backup host to support continuous connectivity if a primary host fails.

In the following example, NetCache B identifies NetCache D as a primary parent, and NetCache C as a secondary parent. NetCache A identifies NetCache C as a primary parent, and NetCache D as a secondary parent. If C goes down, D provides backup for C and handles requests for A. If D goes down, C provides backup for D and handles requests for B.



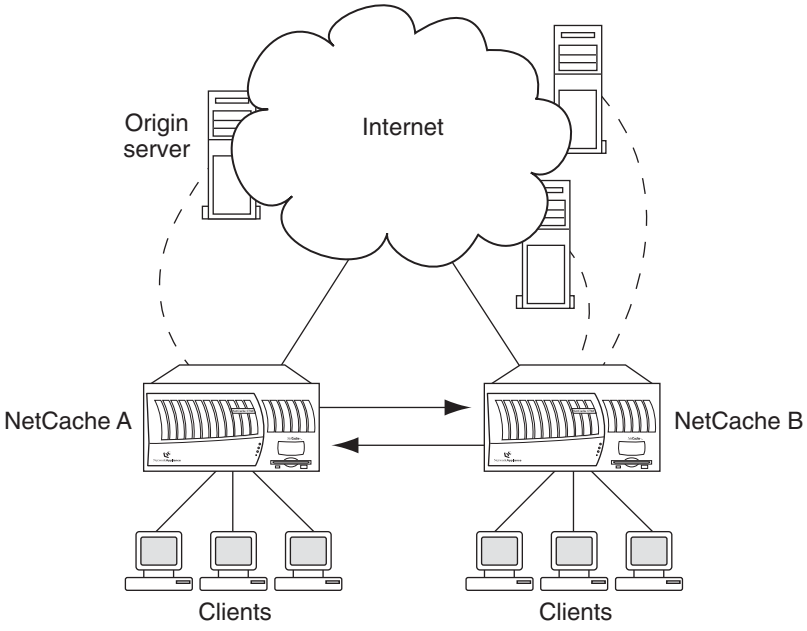
Custom settings to support failover

Custom rule settings can be used to provide failover if a connection to the Internet fails.

Direct monitor is a NetCache hierarchy feature that can be set up to monitor Internet connectivity using direct connections. Monitoring direct connections enables NetCache to detect and route around connectivity problems. NetCache uses TCP to establish connections to hosts specified in the NetCache configuration. When connection attempts to all hosts fail, the Internet connection is considered down, and NetCache fails over to the next forwarding rule for directing requests.

If NetCache fails to connect to a destination specified in a hierarchy forwarding rule, the next user-defined rule is evaluated. If NetCache is unable to connect using any of the forwarding rules, NetCache bypasses the hierarchy and retrieves the content directly from the Internet (known as the “direct” distribution method). You can disable failover on a per-rule basis to control traffic that should not fail over and ultimately be forwarded directly to the Internet.

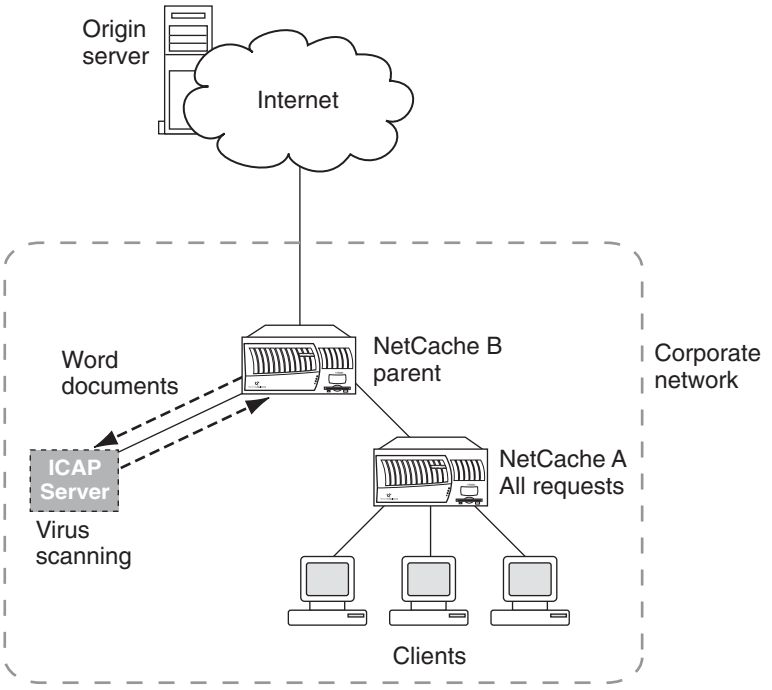
In the following example, NetCache A and NetCache B are set up to monitor direct connections to the Internet. Each member of the hierarchy provides failover if one member loses connectivity.



Custom settings to support services

Custom rule settings can be used to define conditions for handling requests of a specific type.

In the following example, the parent resolves requests for Word documents, and then sends the files to an ICAP server where the content is scanned for virus contamination before being returned to the client. The ICAP server is configured separately on the parent cache and is not part of the hierarchy.


Origin
server
Internet
Word
documents
NetCache B
parent
Corporate
network
ICAP
Server
Virus
scanning
NetCache A
All requests
Clients

Hierarchy configuration example

About the hierarchy

In this example, the ABC Corporation hierarchy is set up to direct requests of a specific type to a specific hierarchy member. ABC has three NetCache appliances, NetCache A, NetCache B, and MP3 Cache. All caches are inside a corporate firewall.

ABC hierarchy members are identified as follows:

- In the hierarchy configuration of NetCache A, MP3 Cache and NetCache B are identified as parents.
- In the hierarchy configuration of NetCache B and MP3 Cache, Firewall 1 is identified as a hierarchy member (firewall).

Using a hierarchy to direct requests

ABC Corporation wants to achieve the following goals:

- NetCache A sends all its unresolved requests to NetCache B, which would then pass requests it could not resolve to the firewall.
- All MP3 traffic is directed to one NetCache appliance, and other types of traffic are directed to a different NetCache appliance.

Configuration settings for NetCache A

This section describes how options are configured on the hierarchy configuration pages of NetCache A.

Hierarchies > General page: The following table shows the configuration on the General page.

Options on the General page	Configuration settings on NetCache A
Hierarchy Enable	Check box is selected.
Bypass Hierarchy for Noncacheable Objects	Check box is *not* selected.
This Domain Is Local to This NetCache Appliance	Check box is selected and the local domain is identified as *abc.com*.

Because “Bypass Hierarchy for Noncacheable Objects” is not selected, the NetCache predefined rule for sending requests for noncacheable objects directly to the origin server is disabled.

Hierarchies > Parents page: The following table shows how each parent is identified in the hierarchy configuration on NetCache A.

Options on the Parents page	Configuration settings for identifying MP3 Cache	Configuration settings for identifying NetCache B
Host Name	MP3 Cache	NetCache B
Ports Used by This Host	HTTP (Port 80), MMS (Port 1755), RTSP (port 554), ICP (Port 7)	HTTP (Port 80), MMS (Port 1755), RTSP (554), ICP (Port 7)
Host Supports	HTTP	HTTP
Cache Objects from This Host	Check box is selected.	Check box is selected.
Monitor Status through	HTTP	HTTP
Hierarchy Authentication	None	None

Hierarchies > Forwarding Rules page: The following tables show the hierarchy rules configured on NetCache A for forwarding MP3 requests to one NetCache appliance and forwarding all other types of requests to a different NetCache appliance.

Rule Number	Rule description
1	Send all requests for domain *abc.com* directly to local servers.
2	Send MP3 requests to MP3 Cache.
3	Send all other types of requests to NetCache B.

Rule 1: NetCache creates this local domain rule automatically when you select the Local Domain Enable check box on the Hierarchies - General page.

Rule 2: Rule 2 was created on the Forwarding Rules page, as shown in the following table.

Rule element	Setting on NetCache A
Rule Name (user-defined)	MP3
Rule Enable	Enabled
Protocols	None selected (rule applies to all protocols)
Conditions	Phrase: URL equals '*.mp3' **Note** It is not necessary to enter the beginning and ending single quotation marks when creating the rule in the Appliance Manager. You must enter beginning and ending quotation marks when you configure conditions from the CLI, however.
Distribution Method	Single Host: MP3 Cache

Rule 3: Rule 3 was created on the Forwarding Rules page, as shown in the following table.

Rule element	Setting on NetCache A
Rule name (user-defined)	Non-MP3
Rule Enable	Enabled
Protocols	None selected (This rule applies to all protocols.)
Conditions	None
Distribution Method	Single Host: NetCache B

Rule 3 is placed after the MP3 rule in the rule list so that the MP3 traffic is sent to MP3 Cache before NetCache executes the more general rule.

Configuration settings on MP3 Cache and NetCache B

The hierarchy configuration settings on both MP3 Cache and NetCache B are the same, as shown in the following tables.

Hierarchies > General page: The following table shows the configuration on the General page.

Options on the General page	Configuration settings on MP3 Cache and NetCache B
Hierarchy Enable	Check box is selected.
Bypass Hierarchy for Noncacheable Objects	Check box is not selected.
This Domain Is Local to This NetCache Appliance	Check box is selected and the local domain is identified as *abc.com*.

Hierarchies > Firewalls page: The following table shows the hierarchy configuration for NetCache appliances MP3 Cache and NetCache B. Neither NetCache appliance is configured to be aware of the other. The reason is that it is more efficient for MP3 Cache and NetCache B to fetch objects they do not have cached from the Internet, by way of the firewall, rather than querying the other appliance for the object.

Options on the Firewalls page	Configuration settings on MP3 Cache and NetCache B
Host Name	Firewall 1
Ports Used When Contacting This Host	HTTP (Port 80), MMS (Port 1755), RTSP (port 554), ICP (Port 7)
Host Supports	HTTP, MMS, RTSP
Cache Objects from This Host	Check box is selected.
Monitor Status through	HTTP
Hierarchy Authentication	None

Hierarchies > Forwarding Rules page: The following table describes hierarchy rules for forwarding MP3 requests to one NetCache appliance and forwarding all other types of requests to a different NetCache appliance.

Rule Number	Rule description
1	Send all requests for domain *abc.com* directly to the local servers.
2	Send all requests for noncacheable objects directly to the Internet.
3	Send all unresolved requests to Firewall 1.

You do not need to create custom rules on MP3 and NetCache B because NetCache enables and orders the rules in this example for you.

Rule 1: NetCache enables its local domain rule automatically because you have enabled the Local Domain Enable option on the Hierarchies - General page.

Rule 2: NetCache enables its noncacheable rule automatically because you have selected the "Bypass Hierarchy for Noncacheable Objects" option on the Hierarchies - General page.

Rule 3: NetCache automatically creates protocol-specific rules to handle requests for origin servers on the Internet.

Troubleshooting a hierarchy configuration

Requests are not distributed as expected

The most likely causes of improper distribution of requests by your NetCache appliance are as follows:

- You created a protocol-specific custom hierarchy rule but did not create a rule to handle the remainder of the traffic for that protocol.

  NetCache provides protocol-specific hierarchy rules that are enabled according to the protocols you have specified that your hierarchy members handle. If you create a custom rule for a particular protocol, you must create a custom rule to handle the remainder of the requests for that protocol.

- Hierarchy forwarding rules are not in the correct order.

  The order of the rules is important because NetCache executes rules in the order in which they are listed in the hierarchy rules list, from top to bottom.

Requests for the local domain are not sent to local servers

The Local Domain rule controls whether requests for local servers are sent to the local servers. This rule is enabled when you select the Local Domain Enable check box on the Hierarchy - General page, which is associated with the "This Domain Is Local to This NetCache Appliance" option. Ensure that you have selected the Local Domain check box and that the local domain name is correct.

An exception to this guideline is if your local domain resides both inside and outside your firewall. You must create custom rules to handle this situation.

Requests for noncacheable objects are not handled

The NetCache default behavior is to send requests for noncacheable objects directly to origin servers. This cannot occur, however, unless your NetCache appliance has direct connectivity to the Internet. If your NetCache appliance does not have direct connectivity to the Internet, modify the noncacheable rule supplied by NetCache to send noncacheable object requests to another proxy-cache server that you have identified as a parent.

HTTP requests are not load balanced

If your log entries indicate that ICP is being used, the distribution method in the associated hierarchy forwarding rule is ICP rather than *cluster*. Load balancing occurs only if a hierarchy rule includes cluster as the distribution method.

If you have identified as neighbors any hierarchy members that handle HTTP, the distribution method in the HTTP-to-all rule supplied by NetCache was set to ICP. The reason is that NetCache always uses ICP to query neighbors.

Do not include neighbors as hierarchy members: Network Appliance recommends that you do not include neighbors as hierarchy members because of the overhead required by ICP communication. If no firewall exists and connectivity allows the specified neighbor to reach the Internet, you should identify that neighbor as a parent instead. If the neighbor does not have connectivity to the Internet, you should remove the neighbor from the hierarchy configuration and rely, instead, on parents to resolve requests.

Bandwidth Allocation Management 14

About this chapter

This chapter describes the appliance bandwidth allocation feature. The bandwidth allocation feature enables you to control bandwidth usage for specific types of traffic. You can also use the rules described in this chapter to completely deny or allow the flow of specific traffic types through the appliance.

Topics in this chapter

This chapter provides information about the following topics:

- "About bandwidth allocation" on page 218
- "Creating and using virtual bandwidth buckets" on page 220
- "Constructing bandwidth allocation rules" on page 222
- "Bandwidth allocation rule examples" on page 224

Note

This chapter describes bandwidth allocation management using the Appliance Manager. For descriptions of CLI commands for bandwidth allocation management, see the descriptions for the `config.ipfw` options in the CLI (`show config.ipfw.*`).

Procedures and option descriptions

See the Appliance Manager online Help for configuration procedures and option descriptions related to bandwidth management.

Location of configuration options

To access the bandwidth allocation options in the Appliance Manager, select:

Setup tab > Network > Bandwidth Allocation

About bandwidth allocation

What is bandwidth allocation?

The NetCache bandwidth allocation feature enables you to control the total bandwidth capacity that specified categories of connections can collectively consume on the NetCache appliance.

Using the NetCache Manager fields associated with bandwidth allocation, you can:

- Set aside portions of your total NetCache bandwidth capacity into various-size capacity *bandwidth buckets*.

  For example, you can limit all in-bound streaming traffic to a given maximum bandwidth or limit the bandwidth usage on an interface.
- Assign connections matching a specified set of properties, such as protocol, source or destination IP addresses, and in-bound (server-side) or out-bound (client-side) communication to a bandwidth bucket.

  For example, you can restrict aggregate bandwidth by single protocol (IP, TCP, UDP, MMS, RTSP, HTTP), by a streaming protocol set (both RTSP and MMS), or by an application (ContentDirector).
- Deny NetCache service to a category of connections completely, or allow NetCache service to the same category of connections with no bandwidth restriction whatsoever.

  For example, you can deny all FTP traffic to a specified server.

How does bandwidth allocation work?

All connections assigned to a specific bandwidth bucket share the total bandwidth space allocated for that bandwidth bucket. The NetCache appliance enforces the bandwidth limit, if necessary, by using buffers to space out both incoming and outgoing packets.

As a result, TCP connections, as well as protocol connections based on UDP, gracefully use the specified bandwidth bucket with a minimum of burstiness, allowing NetCache to enforce the bandwidth allocation rules efficiently.

Note

As a partial alternative to bandwidth allocation, NetCache supports streaming bandwidth management rules that simply allow or deny categories of streaming connections on the basis of their *requested* bandwidth. For more information, see the streaming information in the online Help.

Elements of bandwidth management

To implement bandwidth management, you must create bandwidth allocation buckets and bandwidth allocation rules. Bandwidth allocation buckets define the bandwidth, admission control, and dynamic creation properties that control how packets are throttled on the network. Bandwidth allocation rules define the conditions under which a packet is sent to a specific bucket.

Creating and using virtual bandwidth buckets

About bandwidth allocation buckets

Bandwidth buckets define the virtual "space" that is to be set aside for a particular type of traffic. When you create a new bandwidth bucket, you specify the bandwidth, admission control, and dynamic creation properties of the bucket. Dynamic bucket properties enable you to write masking schemes that use properties in the IP packet to determine whether a bandwidth bucket should be created.

Creating new bandwidth buckets

To create new bandwidth buckets, use the New Bucket button in the Buckets tab on the Network Bandwidth Allocation page (Setup tab > Bandwidth Allocation > Buckets tab).

Viewing existing bandwidth buckets

If you have existing bandwidth buckets, you can view them in the Current Bandwidth Allocation Buckets table (Setup tab > Bandwidth Allocation > Buckets tab).

Dynamic buckets defined

Dynamic buckets are unique bandwidth allocation buckets that are created at the time they are required. By masking the bits in the IP header field, you can create multiple, unique bandwidth buckets that share a single bucket definition.

The appliance examines the rules set for the bucket and the properties specified in the Dynamic Bucket Properties field on the New Bandwidth Bucket page (Setup tab > Network > Bandwidth Allocation > Buckets tab) to determine if a new bandwidth bucket must be created.

How dynamic buckets are generated

The bandwidth management feature uses the IP header masking scheme to help identify packets that should be sent to a dynamic bucket. The bitmask indicates the number of bits that should be set to one. For example:

```
mask dst-ip 0xffffffff
```

In the preceding example, all 32 bits of the destination IP address are set to one. Packets with the same identifier after masking fall into the same queue.

Masking schemes for dynamic buckets

As shown in the following table, you can use several different masking schemes to classify packets for redirection to dynamic buckets.

Mask	Used to identify packets based on	Example
`proto`	Protocol	`mask proto`
`dst-ip`	Destination IP address	`mask dst-ip 0xffffffff`
`src-ip`	Source IP address	`mask src-ip 0xffffffff`
`dst-port`	Destination port	`mask dst-port 0xffff`
`src-port`	Source port	`mask src-port 0xffff`
`all`	All identifiers: `proto`, `dst-ip`, `src-ip`,`dst-port`, `src-port`	`mask all` (All bits in all fields are used to identify packets.)

You can specify multiple masking properties for the bucket. For example:

```
mask dst-ip 0xffffffff dst-port 0xffff
```

The preceding masking properties classify packets based on their destination IP address and port number. For more examples of dynamic bucket masking, see "Example 5: Limiting inbound and outbound connections" on page 226 and "Example 6: Limiting client-side connections" on page 226.

Constructing bandwidth allocation rules

About bandwidth allocation rules

Traffic cannot be directed to bandwidth buckets until you create bandwidth allocation rules. Bandwidth allocation rules allow, deny or assign categories of connections to bandwidth buckets, which can have various capacities. For example, using the bandwidth allocation rules, you can limit traffic to

- Protocols
- Traffic flows (client or server or both)
- Times of day
- Interfaces

As packets arrive, the bandwidth allocation rules are scanned until a match is found. When a match is found, the packets are directed to the appropriate bandwidth bucket.

Creating new bandwidth rules

To create new bandwidth rules, use the New Rule button in the Rules tab on the Network Bandwidth Allocation page (Setup tab > Bandwidth Allocation).

Viewing existing bandwidth allocation rules

If you have existing bandwidth allocation rules, you can view these rules in the Current Bandwidth Allocation Rules table.

The cumulative AND logic of multiple filtering options

If multiple parameters are shown in the filtering options column in the Current Bandwidth Allocation Rules table, their application follows AND logic. To be included in a listed bandwidth management rule, a connection must match *all* the parameters specified in the rule filtering options, not just one parameter. Therefore, the filtering options in the following example indicate that Rule 1 applies only to streaming (RTSP and MMS) connections that are to and from upstream servers or parent appliances *and* are active from 7:30 a.m. to 7:30 p.m. *and* are received or transmitted through interface ns0 on this appliance.

Rule #	Protocol	Bandwidth	Filtering Options
1	Streaming	Pipe 1, 100 Mbits/sec	server traffic, 7:30am-7:30pm, via ns0

Rule 1 does *not* apply to streaming server traffic connections that are active from 7:30 a.m. to 7:30 p.m. but received or transmitted through the *ns1* interface.

First-numbered rules take precedence

If multiple bandwidth allocation rules are configured for one NetCache appliance, the rules are applied in the order in which they are numbered in the Current Bandwidth Allocation Rules table. If a category of connections is included in two bandwidth allocation rules that assign it to two different bandwidth buckets, the earliest numbered rule determines the bandwidth bucket to which this category of connections is assigned.

Well-ordered rules example: In the following bandwidth allocation rules example, although both Rule 1 and Rule 2 could apply to RTSP connections received or transmitted through NetCache appliance interface ns0, Rule 1, which is the first rule applied, effectively assigns those connections to bandwidth Pipe Number 1. Rule 2 applies only to those streaming (RTSP and MMS) connections not received or transmitted through interface ns0 and assigns these connections to bandwidth Pipe 2.

Rule #	Protocol	Bandwidth	Filtering Options
1	Streaming	Pipe 1, 100 Mbits/sec	via ns0
2	Streaming	Pipe 2, 50 Mbits/sec	—

Misordered rules example: If, by accident, the rules are reversed, as in the following example, then the new Rule 1 would apply to all streaming connections and assign these connections to bandwidth Pipe 1. No streaming connections, not even those received and transmitted through interface ns0, would be passed to Rule 2 and be assigned to bandwidth Pipe 2.

Rule #	Protocol	Bandwidth	Filtering Options
1	Streaming	Mmbits/sec	—
2	Streaming	Mmbits/sec	via ns0

Note

If necessary, you can change the order in which your bandwidth allocation rules are applied. For more information, see the Appliance Manager online Help.

Bandwidth allocation rule examples

Example 1: Limiting bandwidth for the streaming servers

The following bandwidth settings allocate a maximum aggregate bandwidth capacity of 100 Mbps, for all server-side streaming connections to share during daylight hours.

Rule properties:

Rule #	Protocol	Action	Filtering Options
1	Streaming	Use bucket 1	server traffic, time 7:00am-7:00pm

Bucket properties:

Bucket #	Bandwidth	Admission Control	Dynamic Bucket Properties
1	100 Mbits/sec	Disabled	—

Example 2: Limiting bandwidth for a specific server

The following bandwidth settings allocate a maximum aggregate bandwidth capacity of 10 Mbps, for all Web traffic directed at the server with destination IP address 128.10.10.0 port 80.

Rule properties:

Rule #	Protocol	Action	Filtering Options
2	HTTP	Use bucket 2	to 128.10.10.0 80, 7:00am-7:00pm

Bucket properties:

Bucket #	Bandwidth	Admission Control	Dynamic Bucket Properties
2	10 Mbits/sec	Disabled	—

Example 3: Limiting bandwidth for a specific interface

The following bandwidth settings allocate a maximum aggregate bandwidth capacity of 100 Kbps, for all Web traffic received at appliance interface ns0.

Rule #	Protocol	Action	Filtering Options
3	HTTP	Use bucket 3	in, via ns0

Bucket properties:

Bucket#	Bandwidth	Admission Control	Dynamic Bucket Properties
3	100 kbytes/sec	Disabled	–

Example 4: Limiting bandwidth by protocol

The following bandwidth rules provide

- A bandwidth pipe of 100 Mbps for all streaming protocol traffic
- Another bandwidth pipe of 100 Mbps to be shared by all other protocols

Rule properties:

Rule #	Protocol	Action	Filtering Options
1	Streaming	Use bucket 1	–
2	IP	Use bucket 2	–

Bucket properties:

Bucket #	Bandwidth	Admission Control	Dynamic Bucket Properties
1	100 Mbits/sec	Disabled	–
2	100 Mbits/sec	Disabled	–

Example 5: Limiting inbound and outbound connections

The following bandwidth settings use dynamic bucket properties to limit clients to 64 Kbps (for NNTP connections, both inbound and outbound).

Note

In the following example, the IP address 172.30.200.60 represents the appliance and 119 represents the port number for NNTP traffic.

Rule properties:

Rule #	Protocol	Action	Filtering Options
1	TCP	Use bucket 1	from any to 172.30.200.60 119
2	TCP	Use bucket 1	from 172.30.200.60 119 to any

Bucket properties:

Bucket #	Bandwidth	Admission Control	Dynamic Bucket Properties
1	64 Kbits/sec	Disabled	mask src-ip 0xffffffff dst-ip 0xffffffff

Example 6: Limiting client-side connections

The following bandwidth allocation settings use dynamic bucket properties to limit each client to 50 Kbps (for NNTP connections to clients only).

Note

In the following example, the IP address 172.30.200.60 represents the appliance and 119 represents the port number for NNTP traffic.

Rule properties:

Rule #	Protocol	Action	Filtering Options
1	TCP	Use bucket 1	from 172.30.200.60 119 to any

Bucket properties:

Bucket #	Bandwidth	Admission Control	Dynamic Bucket Properties
1	50 Kbits/sec	Disabled	mask dst-ip 0xffffffff dst-port 0xffff

Administration of Multiple Appliances 15

About this chapter

This chapter describes procedures and scenarios for configuring and administering multiple appliances using the DataFabric Manager™ software or the appliance Automatic Configuration feature.

Topics in this chapter

This chapter provides information about the following topics:

- Section A, "About managing multiple appliances," on page 230
- Section B, "Working with DataFabric Manager," on page 231
- Section C, "Using the multiple-appliance management feature," on page 238

Section A: About managing multiple appliances

What is multiple appliance management?

As companies expand their data storage networks, the IT costs associated with managing the new data storage devices typically increase as well because of the effort required to individually monitor and maintain the storage devices.

Network Appliance provides two appliance-management tools designed to reduce administrative overhead, the DataFabric Manager software and the on-board multiple-appliance management feature. These appliance management tools are useful in the following situations:

- You need to set up multiple appliances. Rather than manually configuring each appliance through the Appliance Manager, you can copy settings from a source appliance in their entirety to the other appliances.
- You have a large network of appliances and a set of configurations, such as ACL rules or group memberships, that you must frequently update and apply to more than one appliance uniformly.

DataFabric Manager is a robust appliance management product with many other monitoring capabilities. For more information about DataFabric Manager, see the *DataFabric Manager Administration Guide* and Section B, "Working with DataFabric Manager," on page 231.

For more information about the on-board multiple-appliance management feature, see Section C, "Using the multiple-appliance management feature," on page 238.

Section B: Working with DataFabric Manager

About this section

This section describes the DataFabric Manager software and how you can use it to monitor and manage your NetCache appliances. Before reading this section, you should familiarize yourself with the information in the *DataFabric Manager Administration Guid*e.

The *DataFabric Manager Administration Guide* provides extensive information to help you use DataFabric Manager to manage your appliances, including:

- Conceptual information
- Autodiscovery details and process tables
- Implementation recommendations
- Troubleshooting information

Topics in this section

This section provides information about the following topics:

- "About DataFabric Manager appliance management" on page 232
- "Overview of DataFabric Manager discovery methods" on page 233
- "Appliance requirements for SNMP-based autodiscovery" on page 234
- "Appliance requirements for HTTP-based autodiscovery" on page 235
- "Appliance requirements for appliance-initiated discovery" on page 236

About DataFabric Manager appliance management

About DataFabric Manager

DataFabric Manager is a standalone Network Appliance software product designed to simplify management of all Network Appliance storage devices. DataFabric Manager provides remote, centralized management of Network Appliance data storage infrastructures, including global enterprise, storage network, and CDN deployments. DataFabric Manager's integrated appliance management system enables IT staff to centrally monitor and remotely configure both filers and NetCache appliances.

Essentially, DataFabric Manager is a suite of tools that runs on a management server and consolidates tasks that would otherwise require separate operations. DataFabric Manager can be managed using the comprehensive user interface or the CLI.

How you can use DataFabric Manager

In addition to using DataFabric Manager to configure multiple, remote NetCache appliances, you can also use it to

- Alert you when an appliance reaches a certain threshold or state
- Monitor appliance statistics and health
- Track discovery of new hosts and notify users through an event
- Group objects so that you can monitor and administer objects as a group or only a specific object, as appropriate
- Track data over time to help you troubleshoot problems and anticipate future needs by providing
  - Graphs that contain historical data and trends
  - Reports that show that if usage of a specific volume increases at the current rate, it will be full in a certain number of days
- Send a command to one or more appliances
- Remotely update NetCache software (but not add-on software, such as SecureAdmin™ software) on one or more NetCache appliances

How to obtain DataFabric Manager

To obtain DataFabric Manager, contact your Network Appliance sales representative.

Overview of DataFabric Manager discovery methods

SNMP requirement for monitoring appliances

You must have SNMP enabled on your appliances and routers to ensure that DataFabric Manager can monitor and manage appliances.

Note

By default, SNMP is disabled on NetCache appliances, and enabled on filers.

As soon as DataFabric Manager is installed, the discovery process begins. To ensure that DataFabric Manager can discover NetCache appliances, you must enable SNMP on those appliances. You can also wait until after installing DataFabric Manager to enable SNMP on NetCache appliances, but this will cause a delay before DataFabric Manager can discover appliances.

DataFabric Manager discovery methods

DataFabric Manager can discover appliances using any of the following methods:

- SNMP-based autodiscovery—Default DataFabric Manager discovery method. For more information about SNMP-based discovery, see “Appliance requirements for SNMP-based autodiscovery” on page 234.
- HTTP-based autodiscovery—Secondary DataFabric Manager discovery method. This method is used when an SNMP request to an appliance times out. For more information about HTTP-based discovery, see “Appliance requirements for HTTP-based autodiscovery” on page 235.
- Appliance-initiated discovery—This method is useful if youSS think that DataFabric Manager discovery might take too long, for example when appliances are deployed over multiple geographic areas. For more information about appliance-initiated discovery, see “Appliance requirements for appliance-initiated discovery” on page 236.

Appliance requirements for SNMP-based autodiscovery

Appliance options you need to configure for this method

To permit SNMP-based autodiscovery, you must enable SNMP on the appliance by selecting the SNMP Enable option (Setup tab > Administration > SNMP). By default, SNMP is disabled.

Related DataFabric Manager options

The Host Discovery option in DataFabric Manager (Options link) must be enabled to support this feature. Host Discovery (SNMP-based autodiscovery) is enabled by default.

SNMP-based autodiscovery is the primary method for discovery

SNMP-based autodiscovery is the primary DataFabric Manager discovery method. When you install DataFabric Manager, it uses SNMP-based host discovery to automatically locate and identify appliances and networks. If an SNMP request times out, DataFabric Manager tries the HTTP-based autodiscovery mechanism discussed in the following section.

Appliance requirements for HTTP-based autodiscovery

Appliance options you need to configure for this method

You do not need to configure anything on the appliance to permit HTTP-based autodiscovery. However, when HTTP-based autodiscovery is used, DataFabric Manager cannot receive monitoring information unless SNMP is enabled.

When DataFabric Manager discovers an appliance using HTTP-based autodiscovery, it tries to enable SNMP, using the built-in XML interface. This method works only for appliances running NetCache 5.3 and later. If you are running a release prior to NetCache 5.3, you must manually enable SNMP.

Related DataFabric Manager options

The HTTP-based Discovery Enabled, HTTP-based Discovery Port, and Automatic SNMP Enabled options in DataFabric Manager (Main window > Options link) must be enabled to support this feature. The HTTP-based Discovery Enabled and HTTP-based Discovery Port options are enabled by default. You must manually enable the Automatic SNMP Enabled option (or manually enable SNMP on the appliance using the Appliance Manager or CLI).

When HTTP-based autodiscovery is used

HTTP-based discovery acts as a backup discovery method for the SNMP auto discovery mechanism. DataFabric Manager (version 2.2 and later only) uses HTTP-based discovery if an SNMP request to the same address times out. The SNMP and HTTP connection attempts have the same total time-out value, but SNMP is tried two times, with each attempt having half the time-out value of HTTP. HTTP-based autodiscovery is tried once.

Mechanism of HTTP autodiscovery

DataFabric Manager sends a special HTTP ping message to the NetCache administration port to discover NetCache appliances. The NetCache appliance requires no user authentication for this special message, and responds automatically with a list of its active interfaces.

Appliance requirements for appliance-initiated discovery

Appliance options you need to configure for this method

The following options on the DataFabric Discovery - All Settings page (Setup tab > DataFabric Discovery) must be configured for this method:

- Enable DFM Discovery
- DFM Service

The preceding settings are correctly configured for the default DataFabric Manager host name `datafabricmanager`. You do not need to change these settings unless you have previously disabled DataFabric Manager discovery or want to specify a different host name or IP address and port for the DataFabric Manager management station.

Additionally, you must enable SNMP (Setup tab > SNMP > General) to configure the appliance to send monitoring information to DataFabric Manager.

Note

The following CLI options apply to this feature: `config.admin.dfm.enable` and `config.admin.dfm.service`. See the CLI help for more information about these options.

Related DataFabric Manager options

The Appliance Initiated Discovery Enabled option in DataFabric Manager (Main window > Options link) must be enabled to support this feature. The Appliance Initiated Discovery Enabled option is disabled by default.

Restrictions

The following restrictions apply to appliance-initiated discovery:

- Appliance-initiated discovery can occur only when a NetCache appliance joins a network after DataFabric Manager has been started.
- Appliance-initiated discovery is available only on NetCache appliances that are running NetCache 5.4 and later. (NetCache versions prior to NetCache 5.4 cannot use DNS to obtain DataFabric Manager's IP address and port.)

Sequence of events in appliance-initiated discovery

When a NetCache appliance boots, it opens a connection to the DataFabric Manager management station identified in the NetCache configuration settings (Setup tab > DataFabric Discovery). The appliance then sends an initial HTTP

`GET` discovery message to the management station and waits for a response. If the appliance cannot contact the management station, it waits an hour and tries again, repeating this cycle until the management station is contacted. Before each connection attempt, the appliance checks DNS to identify the IP address and port of the DataFabric Manager management station.

Note

NetCache 5.4 and later versions have support for DNS lookups for DataFabric Manager. DNS lookups are performed only when the DFM Service option (Setup tab > DataFabric Discovery) is set to a host name instead of an IP address and port.

Section C: Using the multiple-appliance management feature

About this section

This section describes the CLI-based multiple appliance management feature. It describes configuration files, their use in multiple-appliance management, and provides information about cloning existing configurations.

Topics in this section

This section provides information about the following topics:

- "Strategies for managing multiple appliances" on page 239
- "About global configuration files" on page 241
- "Multiple appliance management by automatic configuration" on page 248
- "Scenario 1: Multiple cache administration at multiple POP sites" on page 254
- "Scenario 2: Applying uniform ACL rules over multiple appliances" on page 260
- "Automatic global file reading through the Appliance Manager" on page 262
- "Backing up and restoring local configuration files" on page 265
- "Configuring local settings that do not overwrite global settings" on page 267
- "Multiple appliance management by pushed configuration files" on page 270
- "Cloning appliance configurations" on page 274
- "Appliance upgrade considerations" on page 277

Strategies for managing multiple appliances

About the multiple-appliance management feature

The multiple-appliance management feature is a CLI-based tool that enables administrators to remotely configure one or more appliances. The multiple-appliance management CLI options enable the administrator to apply a common set of configuration settings to multiple appliances on the network. You enter these common settings in text files called global configuration files.

Automatic configuration strategies

The appliance administrator can use one of several automatic configuration strategies, as shown in the following table.

Strategy	Description
Global automatic configuration file strategy	This strategy is the most automated. The administrator can create and maintain one or more global configuration text files whose settings will be periodically read and downloaded by target appliances configured to do so. For details, see the following sections: ◆ "About global configuration files" on page 241 ◆ "Multiple appliance management by automatic configuration" on page 248
Global pushed configuration file strategy	The administrator can create and maintain one or more global configuration text files and manually push those files to directories on target appliances configured to use those files. For details, see the following sections: ◆ "About global configuration files" on page 241 ◆ "Multiple appliance management by pushed configuration files" on page 270

Strategy	Description
Appliance configuration cloning strategy	The administrator can choose not to create a global configuration file, but instead copy the active configuration of a source appliance to a target appliance. For details, see “Cloning appliance configurations” on page 274.

About global configuration files

What are global configuration files?

The appliance command line interface (CLI) enables the administrator to apply a common set of configuration settings contained in one or more centrally located global configuration text files to multiple appliances on the network.

Later, by manually editing or reconfiguring one or more configuration settings in the global configuration files, the administrator effectively reconfigures those settings for all appliances using these files.

Default configuration files

Every configuration setting that you view or make through the Setup tab pages in the Appliance Manager is recorded as one or more parameters in configuration files on the appliance.

Two configuration files exist by default or are automatically generated by the appliance software as you install the appliance and configure it through the Appliance Manager Web pages or the CLI:

- default.cfg—Contains all the default appliance settings. This file is supplied automatically by the system when the appliance is installed. This file must never be edited.
- local.cfg—Contains all the configuration changes to the default settings that you made to the local appliance while installing the appliance or configuring it through the Appliance Manager or the CLI. This file must never be modified directly, only indirectly, through the Appliance Manager or through the CLI.

When the appliance software boots up, the local appliance determines its active configuration by reading default.cfg settings first and local.cfg settings last. Settings in the last read file, local.cfg, overwrite any conflicting settings in any previously read files, in this case, default.cfg.

Viewing local.cfg values

To view local changes made by administrators to the appliance, enter the following CLI command:

```
show $local.cfg:config.*
```

User-generated global configuration files

The administrator can create customized global configuration text files containing appliance settings to be stored on a source server or a source appliance and applied uniformly to a set of target appliances. The administrator can then configure those target appliances to periodically read the settings in the global configuration files and incorporate the global configuration file settings into each target appliance's active configuration.

When global configuration files are applied: Global configuration file settings are meant to be applied by each appliance after the default.cfg settings, but before its local.cfg settings. If the settings in the global configuration file conflict with the local.cfg settings, local.cfg settings are applied. Settings in the last-applied configuration file overwrite any conflicting settings in previously applied configuration files.

How global settings are propagated: The following table describes how centrally configured settings in global configuration files can be applied to all appliances in a network.

Global configuration file propagation process	Global configuration file source server or appliance		Global configuration file target appliances	
	ServerA .cfg files	**ApplianceA .cfg files**	**ApplianceB .cfg files**	**ApplianceC .cfg files**
1. All appliances have default configuration files.	—	default.cfg local.cfg	default.cfg local.cfg	default.cfg local.cfg
2. The administrator creates, configures, and saves to ServerA or source ApplianceA one or more global configuration files containing settings to be applied uniformly to all appliances.	globlac.cfg globlbw.cfg	N/A	default.cfg local.cfg	default.cfg local.cfg
	N/A	default.cfg globlacl.cfg globlbw.cfg local.cfg	default.cfg local.cfg	default.cfg local.cfg

Global configuration file propagation process	Global configuration file source server or appliance		Global configuration file target appliances	
	ServerA .cfg files	**ApplianceA .cfg files**	**ApplianceB .cfg files**	**ApplianceC .cfg files**
3. The administrator then configures the target appliances to periodically read the global configuration files from the source server or appliance and incorporate the global settings in their active configuration. Alternatively, the administrator manually pushes configuration files to local drives on target appliances and configures the target appliances to read those files.	globlac.cfg globlbw.cfg	N/A	default.cfg globlacl.cfg globlbw.cfg local.cfg	default.cfg globlacl.cfg globlbw.cfg local.cfg
	N/A	default.cfg globlacl.cfg globlbw.cfg local.cfg	default.cfg globlacl.cfg globlbw.cfg local.cfg	default.cfg globlacl.cfg globlbw.cfg local.cfg
4. Any subsequent changes that the administrator makes to a global configuration file on ServerA or source ApplianceA are periodically propagated to target ApplianceB and ApplianceC. Alternatively, the administrator manually pushes the modified configuration file to local drives on the target appliances.	globlacl.cfg globlbw.cfg	N/A	default.cfg globlacl.cfg globlbw.cfg local.cfg	default.cfg globlacl.cfg globlbw.cfg local.cfg
	N/A	default.cfg globlacl.cfg globlbw.cfg local.cfg	default.cfg globlacl.cfg globlbw.cfg local.cfg	default.cfg globlacl.cfg globlbw.cfg local.cfg

What do global configuration files contain?

The settings in global configuration files consist of a version number and a list of configuration option strings and values specifying the appliance settings that the administrator wants to apply globally.

Version line: The first line of the file specifies the version of the appliance with which the option strings that follow are compliant. The syntax of the version line is:

`#!Config V`*`x.xxx`*

where *x.xxx* is the appliance version number.

Option strings: The option strings are the same strings used with the `set` command when configuring an appliance through the CLI, the same option strings that appear if you enter show `config.*` in the CLI console.

The syntax for each setting is:

`config.`*`option_string =valid_appliance_value`*

For example, a global configuration file named *globlbw.cfg* might contain the following streaming settings, which the administrator might want to apply uniformly to all the appliances in the network:

```
config.streaming.rulelist.bandwidth = //
allow group ourgroup and bitrate 0k - 140k
allow group theirgroup and bitrate 0k - 56k
allow time 7am - 7pm and bitrate 0k - 56k
deny any
//
config.streaming.rulelist.cacheability = //
no-cache server-name www.mine.com
no-cache not group finance
no-cache bitrate 1Mbps
//
```

For a complete listing of CLI `config.*` option strings, see the configuration option reference table in the *Command Line Reference*.

Ways to create a global configuration file

Global configuration files are text files. They can be created either manually or by redirecting the output of the CLI `show` command.

Manually creating a configuration file: Using a text editor on a server where you want to locate your global configuration files, you can manually create a global configuration file and its entries if you are familiar with the CLI option strings.

Cloning the configuration of an existing appliance: Using the CLI `show -clone` command, redirect the `show -clone` command output of an existing appliance configuration to a configuration file on an FTP or HTTP server. For example:

```
show -clone > ftp://srvrz:cfg/multicache1.cfg
```

Then edit that file to contain only the settings that you want to apply globally over multiple appliances.

Note

If you manually create a global configuration file, begin the file with the following version line string: *#!Config Vx.xxx* where *x.xxx* is the appliance version number that your option strings are complaint with.

Generating a configuration file using show config.*: Using the settings of a source appliance that has already been configured through the Appliance Manager, you can generate a configuration file by completing the following steps.

Step	Action
1	Using the Appliance Manager, configure a local appliance with the settings that you want to include in the global configuration file. As each page is configured, click Commit Changes at the bottom of that page.

Step	Action

2	In the CLI console, enter the **show** command and redirect its output to a text file either on a server with HTTP or FTP connectivity or on the source appliance itself.
	◆ If you want to redirect to an HTTP or FTP server, enter
	show config.*partial_option_string > {ftp|http}://[usr:pw@]srvr/path/file***
	partial_option_string is a partially complete CLI configuration option string that, in combination with an asterisk, specifies the subset of configuration settings that you want directed to a global configuration file.
	usr:*pw* is the login name and password, if any, necessary to write to the source server where the global configuration file will be written.
	srvr/*path*/*sfile* is the server, directory, and file name where the global configuration will be located.
	path/*file* is the directory location and file name on the server where you want the global configuration file written.
	For example:
	`show config.acl* >ftp://admn:secrt @serverC//configz/globacl.cfg`
	◆ If redirecting to a location on the source appliance, enter
	show config.*partial_option_string > path/file***
	Example:
	`show config.acl* > /temp/globacl.cfg`

3	If you redirected the global configuration file to a server, you can use a text editor to make any necessary edits to the file. If you redirected the global configuration file to a location on the source appliance, you cannot edit the file directly. **Note** In either case, the appliance automatically includes the required appliance version line at the start of the resulting file.

Editing the configuration file settings to append rather than overwrite

To append to rather than overwrite values for matching settings specified in earlier configurations, edit your later configuration file settings, replacing the **=** character with the **+=** character combination.

In the following table, Example 1 shows the `config.auth.users` setting in global configuration file A *overwritten* by the matching setting in global configuration file B. Example 2 shows the `config.auth.users` setting in global configuration file A *appended to* by the matching setting in global configuration file B.

Examples	Setting in global configuration file A	Setting in global configuration file B	Resulting active setting in Appliance10
Example 1: overwritten settings	`config.auth.` `users = jack@abc.com`	`config.auth.` `users = jill@abc.com`	`config.auth.` `users = jill@abc.com`

Example 2: appended settings	`config.auth.`
	`users = jack@abc.com`
		`config.auth.`
		`users +=`
		`jill@abc.com`
			`config.auth.`
			`users=\\`
			`jack@abc.com`
			`jill@abc.com`
			`\\`

Inserting comment lines in global configuration files

If you manually edit your configuration files, you can use the `#` character to set off comment lines. For example:

```
# The following section sets bandwidth allocation
# Do not change!
```

Note

Comment lines starting with the `#` character in the source global configuration file will be stripped out of the active configuration that is pulled or cloned to target appliances. Restore operations from target appliances to global configuration source files will overwrite all comment lines.

Multiple appliance management by automatic configuration

About automatic configuration

The appliance automatic configuration setup, in which centralized global configuration file settings are periodically pulled into the active configurations of target appliances, is the most automated means of multiple appliance management.

For information about...	See...
Configuring automatic configuration	This section, "Multiple appliance management by automatic configuration"
A scenario in which automatic configuration is employed	"Scenario 1: Multiple cache administration at multiple POP sites" on page 254
The Appliance Manager page that supports automatic configuration	"Scenario 2: Applying uniform ACL rules over multiple appliances" on page 260
Backing up and restoring automatic configuration files	"Backing up and restoring local configuration files" on page 265
Supporting local configurations that append to, rather than overwrite, global configuration file settings	"Configuring local settings that do not overwrite global settings" on page 267

Create or generate the global configuration files

On one centrally located and accessible appliance, create your global configuration files by doing one of the following:

- Manually create a text file with the CLI commands you want to apply over multiple-appliances.
- Redirect `show` command output of an existing appliance configuration to a configuration file. For example:

```
show config.* > ftp://serverA//cfg/globalcfg1.cfg
```

For details about creating global configuration files, see "Ways to create a global configuration file" on page 244.

Configure the appliances to use the global configuration files

In the CLI console of each target appliance on which you want to carry out global multiple-cache management, use the `set config.admin.config.list` command to specify the global file or files to read.

Setting to read global configuration files from a source server: The following sample entry specifies that after it reads the default.cfg file, the target appliance reads global configuration files located on ServerA:

```
set config.admin.config.list \\
default.cfg
ftp://serverA//cfg/globalcfg1.cfg
ftp://serverA//cfg/globalcfg2.cfg
local.cfg
\\
```

Note

The default.cfg and local.cfg files are existing files that must not be directly edited. In the `set config.admin.config.list` command line, always list default.cfg first and local.cfg last.

The preceding command line example applies the settings in the configuration files in the order in which they are listed.

- The settings in `globalcfg2.cfg` will overwrite any *conflicting* settings in `default.cfg` and `globalcfg1.cfg`.
- The settings in local.cfg overwrite any conflicting settings in any of the other three files.

Setting to read global configuration files from a source appliance:

The following sample entry specifies that after reading the default.cfg file, the target appliance reads, global configuration files located on the source appliance:

```
set config.admin.config.list \\
default.cfg
http://admin:appliance@applianceA.mycorp.com:3132/tmp/globalcfg1.c
fg
local.cfg
\\
```

Note

You can also specify global configuration files to read through the Automatic Configuration page of the Appliance Manager on each appliance. See “Scenario 2: Applying uniform ACL rules over multiple appliances” on page 260.

Schedule the appliances to refresh their configurations

In the CLI of each appliance on which you want to carry out multiple-cache management, set up either *periodic* or *scheduled* refresh.

Periodic refresh: A periodic configuration refresh ensures that the appliance configuration is refreshed with the global configuration file settings at a simple time interval specified in minutes.

To set up a *periodic* configuration refresh, enter commands similar to the following:

```
set config.admin.config.refresh.trigger periodic
set config.admin.config.refresh.rate 3600
```

Scheduled refresh: A scheduled configuration refresh refreshes each appliance configuration at a specified time following a daily, weekly, or monthly schedule.

To set up a *daily* configuration refresh schedule, enter commands similar to the following:

```
set config.admin.config.refresh.trigger scheduled
set config.admin.config.refresh.sched_type daily
set config.admin.config.refresh.schedule 23
```

To set up a *weekly* configuration refresh schedule, enter commands similar to the following:

```
set config.admin.config.refresh.trigger scheduled
set config.admin.config.refresh.sched_type weekly
set config.admin.config.refresh.wdays 2 4 6
set config.admin.config.refresh.schedule 23
```

To set up a *monthly* configuration refresh schedule, enter commands similar to the following:

```
set config.admin.config.refresh.trigger scheduled
set config.admin.config.refresh.sched_type monthly
set config.admin.config.refresh.mdays 1 7 14 21
set config.admin.config.refresh.schedule 23
```

Note

You can also schedule configuration refreshes through the Automatic Configuration page of the Appliance Manager on each appliance. See "Scenario 2: Applying uniform ACL rules over multiple appliances" on page 260.

Modify the global configuration files as required

Modifications that you make to your global configuration files on a source server or a source appliance are periodically propagated to the target appliances configured to read them.

Modifying configuration files located on a server: If the global configuration file is located on a source server, you can modify the global configuration file by opening the configuration file directly in a text editor and edit the setting you want to change.

Your changes to the target global configuration file will take effect on each appliance configured to read that file when the next automated refresh takes place.

If you want to display global configuration file settings through the CLI

Using the `show` command, you can display global configuration file settings directly from the command line by prepending the `show` command with the full network and directory pathname to the file whose settings you want to display. Use the following syntax:

`show ${ftp|http}://[`*`usr`*`:`*`pw`*`@]`*`path`*`/`*`file`*`:config.`*`opt_str`*

usr:*pw* is the login name and password, if any, required to access the server on which the configuration file is located.

path is the FTP URL or HTTP URL path to the global configuration file, including the server host name and any directory path.

file is the name of the global configuration file.

`config.`*opt_str* is the configuration option string you want to display.

For example:

```
show $ftp://serverA//cfg/globalcfg2.cfg:
config.http.ports
```

If you want to clear most nondefault settings from the local.cfg file

If you want to clear most local.cfg file nondefault configuration settings on each appliance, use the CLI config -z command. The config -z command resets the configuration values on the appliance to their default settings (except as noted in the following table). All configuration values specified in configuration files are also reset. Note that all references to global configuration files (configuration files pulled from remote locations) are also cleared from the configuration file list.

The following table lists the configuration values that are not reset when you click Reset Configuration.

Option	CLI equivalent
All the Setup tab > Network > Interfaces options	config.system.vinterface.* config.system.interface.*
Nameservers option (Setup tab > DNS > General page)	config.system.dns.nameservers
Default Gateway (Setup tab > Network > Routing)	config.system.gateways.ip
Route Discovery Enable option (Setup tab > Network > Routing)	config.system.routed.rdisc
Appliance Host Name option (Setup tab > System > Host Name)	config.system.hostname

If you want to refresh global configurations immediately

If you want to refresh the global configuration on a managed appliance immediately, before the time that you scheduled through the `set config.admin.config.refresh.*` command lines, you can force the refresh by entering **`config -n`** in the CLI console.

Avoiding local.cfg file overwrite

On each target appliance, the settings in the system local configuration file, local.cfg overwrite the values of any matching configurations in global configuration files applied previously.

The local.cfg file contains any settings you have made on the local appliance through either the Appliance Manager or the CLI.

If you want local configurations that merely append to, not overwrite, settings in global configuration files, see “Configuring local settings that do not overwrite global settings” on page 267.

Persistency of the running configuration

On each appliance, the running configuration is the combination of the default.cfg, local.cfg, and global configuration file settings. The running configuration is persistent. If you are forced to reboot the appliance, it will restart using the configuration that was running when it was last shut down.

Consequently, you can include in your global configuration files many settings normally associated with startup, such as the DNS server settings or gateway settings.

Scenario 1: Multiple cache administration at multiple POP sites

Implementation requirements

In this scenario, a telecommunications company, Company XYZ, uses global configuration files to administer 55 appliances installed to service Web and streaming requests at multiple POP sites over a geographic area that spans multiple time zones.

Advantages of multiple-cache configuration

The primary reasons for implementing multiple-cache management at Company XYZ are

- To minimize the task of administering individual appliances locality
- To avoid conflicting configuration settings among multiple appliances
- To simplify the task of appliance vendor support

The configurations for all appliances run by Company XYZ are stored and accessible at a single location.

Multiple cache architecture

The multiple-cache configuration of Company XYZ is designed to minimize the number of settings that are made to each appliance's local.cfg file.

Running configuration versus local configuration: appliances always store the running configuration and, after a reboot, load the last running configuration, rather just using the settings specified in the local.cfg file.

Therefore, a configuration scheme that specifies the default gateway, DNS server, and time-zone configuration in a global configuration file rather than the in local.cfg file presents no problem even though default gateway, DNS server, and time-zone configuration are necessary to local appliance reboot operations.

Global configuration file types: At the central administration site, the administrator creates and maintains the global configuration files shown in the following table on a centralized FTP server.

Sample global configuration file	Contents
common.cfg	Settings common to all appliances.

Sample global configuration file	Contents
pop_name.cfg	Settings specific to each POP (one file for each POP site).
http.cfg	Settings to configure HTTP. This file is used by most appliances in the company.
streaming.cfg	Settings to configure RTSP- and MMS- based streaming. Only select appliances at each POP use this file.

Global configuration file assignment

One of the Company XYZ appliances at the POP BBB has the following `config.admin.config.list` option setting entered into its local.cfg file:

```
config.admin.config.list = \\
default.cfg
ftp://30.30.30.30//nc/5.0.1/common.cfg
ftp://30.30.30.30//nc/5.0.1/pop_bbb.cfg
ftp://30.30.30.30//nc/5.0.1/http.cfg
ftp://30.30.30.30//nc/5.0.1/streaming.cfg
local.cfg
\\
```

Contents of the common.cfg file

The common.cfg file contains settings common to all appliances at Company XYZ. Comment lines are prepended by #.

```
#!Config V5.300

# Allow scrolling after pressing <RETURN>
config.cli.show_chunk = 15
# IP Forwarding for troublesome sites
config.transparency.bypass_ip.addrs = \\
1.1.1.1
2.2.2.2
3.3.3.3
4.4.4.4
5.5.5.5
\\
config.transparency.bypass_ip.enable = on

# SNMP
config.snmp.auth_traps.hosts = \\
```

```
200.1.1.1
204.2.2.2
\\
config.snmp.enable = on
# Autosupport
config.autosupport.from = netcache@someone.net.mx
config.autosupport.recipients.note = \\
netcache@someone.net.mx
autosupport@netapp.com
\\
config.autosupport.recipients.full = \\
autosupport@netapp.com
netcache@someone.net.mx
\\
config.autosupport.mailhosts = 1.2.3.4
config.autosupport.enable = on
# Messages Log File
config.system.logs.period = 360
config.system.logs.trigger = size
config.system.logs.max_size = 1999
config.system.logs.technique = rotate
# Time Server
config.system.timed.servers = 2.3.4.5
config.system.timed.proto = rdate
config.system.timed.max_skew = 1h
config.system.timed.enable = on
# DNS
config.system.dns.domain_tree_search_enable = off
config.system.dns.domainname = someone.net.mx
# AdminList Refresh Activity
# Refresh every day at midnight
config.admin.config.refresh.sched_type = daily
config.admin.config.refresh.schedule = 0
config.admin.config.refresh.trigger = scheduled
# Avoid to CONNECT through appliances on
Port 25
!25
\\
# Change GUI password to <something>
config.auth.users = admin:!@#$%^&*()
```

Configuration refresh settings : To more easily control the time of configuration refreshes, the administrator moves the configuration refresh schedule settings to the common.cfg file.

Contents of the *POPname*.cfg file

Each POP-specific configuration file at Company XYZ contains the following information:

- WCCP router list
- Default gateway
- DNS name servers
- Time zone

```
#!Config V5.300

config.wccp.routers = \\
10.1.1.1
20.2.2.2
\\
config.system.timezone = America/Mexico_City
config.system.gateways.ip = 10.1.1.2.2
config.system.dns.nameservers = \\
10.11.11.11
10.12.12.12
10.13.13.13
\\
#
#config.transparency.bypass_ip.addrs += \\
#10.11.12.13
#\\
```

WCCP router configuration: WCCP routers are specified in the POP-specific configuration files. Because the POP-specific files are listed after the common file, the WCCP features are not enabled in the common file.

Note

If you want to enable DNS caching service on the appliance, a better strategy might be to list the POP-specific configuration file first, or to provide a *pre* and *post* version. By providing a *pre* and *post* version, you can specify WCCP routers early in the *pre* file and then specify local "additions" to common configurations in the *post* file.

Contents of the http.cfg file

The http.cfg file contains settings specific to Company XYZ's Web appliances.

```
#!Config V5.300

config.http.ports = 80
config.http.transparency = on
config.wccp.http.enable = on
config.http.default_max_age = 2592000
config.http.req_lastmod = on
```

```
config.http.logs.access.format = \\
x-localtime time-taken c-ip x-transaction bytes cs-method cs-uri x-
username x-hiercode rs(Content-Type) x-note
\\
```

Contents of the streaming.cfg file

The streaming.cfg file contains settings specific to Company XYZ's streaming appliances.

```
#!Config V5.300

config.rtsp.transparency = on
config.rtsp.enable = on
config.mms.transparency = on
config.mms.enable = on
config.wccp.rtsp.service_number_udp = 5
config.wccp.rtsp.service_number_tcp = 4
config.wccp.rtsp.enable = on
config.wccp.mms.service_number_udp = 3
config.wccp.mms.service_number_tcp = 2
config.wccp.mms.enable = on
```

Cache installation procedure

The administrators install each new appliance at Company XYZ with the following steps:

1. Physically install each appliance on its rack.
2. Boot the appliance.
3. Carry out the setup and installation procedures, which include installing license codes.
4. Clear most local configuration settings on each appliance with the CLI `config -z` command.
5. Set the global configuration file sources for each appliance using the `set config.admin.config.list` command and option at the CLI console for that appliance.
6. Clear the default gateway and DNS name server settings from the local.cfg file of each appliance by using the following `clear` commands in the CLI console for that appliance:

   ```
   clear config.system.gateways.ip

   clear config.system.dns.nameservers
   ```

Multiple-cache change control

To ensure smooth application of the global configuration changes to the appliances at Company XYZ, the following precautions are taken:

- Modifications to the local.cfg file at each appliance are forbidden.
- An appliance in a lab environment is normally used for testing new configurations.
- If it is necessary to test a modification on a production system, the administrator carries out the following actions:
  - The administrator adds the modification to one of the POP configuration files and then loads the configuration on one of the appliances at that POP.
  - If the results are acceptable after an observation period (minutes or hours, depending on the situation), the administrator introduces the modification into the common.cfg file.

Modification example modification: The administrator at Company XYZ wanted to add a particular IP address to the forwarding list that was specified in the common.cfg file.

1. The following setting was added to the configuration file for POP BBB:

```
config.transparency.bypass_ip.addrs += \\
132.55.55.10
\\
```

2. The administrator executed the `config -n` command on one of the appliances in POP bbb.

After the administrator verified that this setting solved a particular issue, this change was removed from the pop_bbb.cfg file and the IP address was added to the common.cfg file.

Scenario 2: Applying uniform ACL rules over multiple appliances

Applying global ACL rules through multiple-cache management

The sample global multiple-cache configuration described in this section implements an ACL rule that enables, on a network-wide scale, some users to bypass the usual appliance authentication requirements because they are not in the database or because they are administrators.

Stage	Process

1	At ServerA the administrator creates a global configuration file, bypassauth.cfg, containing the following ACL command line:
	`config.acl.global = \\`
	`allow client-ip 1.2.3.4`
	`allow client-ip 1.7.12.123`
	`allow client-ip 1.8.123.32`
	`allow client-ip 1.9.132.38`
	`allow client-ip 1.10.132.39`
	`allow server-name 'intranet.company.com'`
	`try-auth any`
	`deny user paul`
	`allow auth`
	`deny any`
	`\\`
	This ACL command line setting enables some users, accessing the appliance from secured terminals, to bypass the usual appliance authentication requirements because they are not in the database or they are administrators. All others must authenticate unless they are accessing a few well-defined pages.

Stage	Process

2	In the CLI console of ApplianceA, ApplianceB, ApplianceC, and ApplianceD, the administrator enters command lines to
	◆ Specify the global configuration file to read:
	`set config.admin.config.list \\`
	`default.cfg`
	`ftp://serverA//cfg/bypassauth.cfg`
	`local.cfg`
	`\\`
	◆ Set up a periodic configuration refresh:
	`set config.admin.config.refresh.trigger periodic`
	`set config.admin.config.refresh.rate 1440`

3	As they have been configured in Stage 2, ApplianceA, ApplianceB, ApplianceC, and ApplianceD read the bypassauth.cfg file on ServerA every 24 hours (1440 minutes) and incorporate its settings into their active configurations.

4	Later, to modify the global ACL bypass authentication rules, the administrator logs into ServerA and modifies the `config.acl.global` option in the bypassauth.cfg file.:
	`config.acl.global= \\`
	`allow client-ip 1.2.3.4`
	`allow client-ip 1.7.12.123`
	`allow client-ip 1.8.123.32`
	`allow client-ip 1.9.132.38`
	`allow client-ip 1.10.132.39`
	`allow client-ip 1.10.132.40`
	`allow client-ip 1.10.132.50`
	`allow server-name 'intranet.company.com'`
	`try-auth any`
	`deny user paul`
	`deny user bmay`
	`allow auth`
	`deny any`
	`\\`

5	As they have been configured in Stage 2, ApplianceA, ApplianceB, ApplianceC, and ApplianceD read the bypassauth.cfg file on ServerA every 24 hours (1440 minutes) and incorporate its modified settings into their active configurations.

Automatic global file reading through the Appliance Manager

Using the Appliance Manager Automatic Configuration page

On each managed appliance, the administrator has a GUI-based alternative method for setting up that appliance to read part of its configuration from one or more global configuration files.

You can create and configure your global configuration files as described in "Ways to create a global configuration file" on page 244. Then, for each appliance that you want to include in your multiple-cache management network, you can start the Appliance Manager and open the System - Automatic Configuration page. To access this page, select the Setup tab > System > Automatic Configuration.

The following options can be configured:

- Automatic Configuration Files
- Automatic Configuration Update Interval

Automatic Configuration Files

In this option, specify the global configuration files that this appliance uses in addition to its default and local settings to determine its own configuration. You can specify the files by FTP URL or HTTP URL. Acceptable inputs include:

```
ftp://[user:password@]server//path/configfilename
http://[user:password@]server/path/configfilename
http://[user:password@]cache:adminport/
configfilename
```

Conflicting settings are resolved as follows:

- The settings contained in the global configuration files overwrite any conflicting default settings contained in the default configuration file.
- The settings contained in the local configuration file overwrite any conflicting settings in a global configuration file.
- If more than one global configuration file is listed, settings in a file listed later overwrite any conflicting settings in a file listed previously.

By setting this option on a group of appliances to point them to a common global configuration file, the administrator can implement configuration changes on multiple appliances by manually editing a single file.

Examples of entries are as follows:

```
ftp://nc1:mypw@cfgsrvr//cfg/acls.cfg
ftp://nc1:mypw@cfgsrvr//cfg/ports.cfg
```

Automatic Configuration Update Interval

In this option, specify the interval at which this appliance reads the configuration settings in the files specified in the Automatic Configuration Files list. The following options are available:

- Periodically at the Following Intervals

  The appliance reads the automatic configuration files after the specified number of hours has elapsed.

- Daily

  The appliance reads the automatic configuration files every day at the time specified in the Scheduled Times option.

- Weekly, on the Following Days

  The appliance reads the automatic configuration files on the specified days at the time of day specified in the Scheduled Times option.

- Monthly, on the Following Dates

  The appliance reads the automatic configuration files every month on the specified date (or dates) at the time of day specified in the Scheduled Times option.

  To set monthly read dates, enter the dates separated by spaces. For example:

  ```
  1 8 15 22 29
  ```

  The preceding example indicates that the automatic configuration files will be read and will refresh this appliance configuration on the 1st, 8th, 15th, 22nd, and 29th day of every month.

If you set the Automatic Configuration Update Interval option to Daily, Weekly, on the Following Days, or Monthly, on the Following Dates, the Scheduled Times option specifies the time (or times) of the specified days that the appliance reads the automatic configuration files. The format for your entry is

```
hr:min{am|pm}
```

For example, if you select Mon (Monday) in the Weekly setting of the Automatic Configuration Update Interval option, and enter **`1:00am`** in the Scheduled Times option, the appliance reads the automatic configuration files every Monday at 1:00 a.m.

When you want to specify multiple scheduled times, enter each scheduled time on a new line. For example:

```
1:00am
3:00pm
8:00pm
```

Get Configuration Files Now option

Click Manual Update under this option if you want this appliance to update its configuration immediately with the files specified in the Automatic Configuration Files list.

Backing up and restoring local configuration files

GUI or command line methods to back up and restore

Appliance configuration backup and restoration can be carried out through the Appliance Manager or through the CLI `config`, `config_backup`, or `config_restore` command.

Using Appliance Manager Backup and Restoration

On each managed appliance, use the Back Up / Restore page of the Appliance Manager to back up and, if necessary, restore its local.cfg and global configuration files. To access this page, select Maintenance tab > Configuration Files > Back Up / Restore.

Backing up configuration files: Use the "Back Up Current Configuration File as" option to back up all current configuration files on the appliance to a single backup file.

Enter a backup file name and click Back Up Configuration.

Restoring a previously backed up configuration: If necessary, use the Current Backup Files option to restore a previous backup configuration to an appliance.

From the Current Backup Files list, select the backup configuration that you want to restore to your appliance. Select one of following two restoration options and click Submit:

- Restore the Configuration Locally—Restores the local configuration and any global configuration files to the local appliance.
- Restore the Configuration in Detached Mode—Restores the local configuration file locally and writes all the settings contained in any global configuration file into the local configuration file so that all global settings are now part of the local configuration and cannot be overwritten by global configuration file changes. This operation effectively detaches the local appliance from future global configuration file updates.

Using the CLI config command to carry out backup and restoration

On each managed appliance, you can also use the `config`, `config_backup`, or `config_restore` command from the CLI console to carry out backup and configuration operations.

See the information about maintenance commands in the *Command Line Reference* for more information.

Configuring local settings that do not overwrite global settings

The overwriting property of local.cfg

The non-editable system default local configuration file, local.cfg, is the last-applied file on your appliances. Its settings consist of any settings you have made on the local appliance through either the Appliance Manager or the CLI. The configuration values in the local.cfg file overwrite the values of any matching configurations in global configuration files applied previously. This presents a problem to administrators who want to implement local settings that merely append to, not overwrite, settings in global configuration files.

Creating a local configuration file with appendable settings

You can configure an appliance with local settings that do not overwrite matching settings in previously applied global configuration files. Avoid making those settings on the local appliance through the Appliance Manager or CLI. Instead create an appendable local configuration file consisting of local settings that append to, not overwrite, previous global settings.

To create a local configuration file with appendable settings, complete the following steps.

Step	Action
1	At the appliance where you want to apply local settings that append to, rather than overwrite, global settings, make sure that no local values have been configured for those settings through the Appliance Manager or the CLI. If local settings have been set, use the `clear` command to reset that configuration to default. For example: `clear config.autosupport.recipients.note`

Step	Action

2	At a source server, create an appendable local configuration file containing appendable settings that you want to apply to that local appliance only. For example:
	`config.autosupport.recipients.note += barry@xyz.com`
	`config.global.acl += allow client ip 10.10.22.3`
	Note
	The `+=` characters in the preceding example indicate that the values that follow will be appended to, rather than overwrite, any existing values for those settings. For details, see "Editing the configuration file settings to append rather than overwrite" on page 247.

3	Use the `cp` command to save each appendable local configuration file to a local directory on the target appliance. Use the following syntax:
	`cp {ftp|http}://[usr:`*`pw`*`@]/`*`srvr/path/sfile`*
	`/nc_path/nc_file`
	Note
	Enter the preceding syntax on one line with a space separating the */sfile* and */nc_path* variables.
	usr:*pw* is the login name and password, if any, necessary to access the source server where the appendable local configuration file was created.
	srvr/*path*/*sfile* is the host name, directory, and file name of the configuration file on the source server.
	nc_path/*nc_file* is the target directory location and file name on the appliance where you want the local appendable configuration file copied.
	For example:
	`cp ftp://usrA:pw@srvrA//cfg/localappends.cfg`
	`/tmp/localappends.cfg`

Step	Action

4	At the CLI console of the target appliance, use the `config.admin.config.list` setting to add this file to the local appliance's active configuration. Remember to do the following:
	◆ Include a local directory path.
	◆ List the appendable local configuration file just before the local.cfg file.
	For example, the following command line directs the local appliance to apply the settings in the localappends.cfg file just before the local.cfg settings:
	`set config.admin.config.list \\`
	`default.cfg`
	`ftp://serverA//cfg/bypassauth.cfg`
	`/tmp/localappends.cfg`
	`local.cfg`
	`\\`

5	To apply your configuration immediately, enter **`config -n`**

Modifying local appendable configuration settings

If you need to modify local appliance settings specified in an appendable local configuration file, you can do so by editing the text of that file directly.

Caution

Never use the Appliance Manager or the CLI to modify your local appliance settings specified by the appendable local configuration file. Doing so enters those settings into the local.cfg file and consequently will cause the appliance to apply the modified settings in overwrite rather than appendable mode.

Multiple appliance management by pushed configuration files

Pushing configuration files versus automatic configuration

An alternative to multiple appliance management by automatic configuration is to manually push an updated global configuration to target appliances.

From a source server, you can use the CLI `cp` command to manually push a configuration file to a location on a target appliance. The target appliance can be configured to use the settings in the copied configuration file.

Note

This operation is not automated. Subsequent modifications to the global configuration file on the source server must be manually copied to the target appliance.

For information about...	See...
Procedures for setting up and carrying out a global configuration push	This section, "Multiple appliance management by pushed configuration files"
Procedures for backing up and restoring appliances using pushed global configuration files	"Backing up and restoring pushed configuration files" on page 273
Supporting local appliance configurations that append to, rather than overwrite, global configuration file settings	"Configuring local settings that do not overwrite global settings" on page 267

Setting up a pushable configuration file

To set up a source server to target appliance configuration file pushing, complete the following steps.

Step	Action
1	At the source server, generate or create a configuration text file containing the configurations that you want to push to target appliances. Use the procedures described in "Create or generate the global configuration files" on page 248.
2	Accessing the CLI console of each target appliance where you want to push a configuration file, make sure that no local values have been configured for those settings through the Appliance Manager or the CLI. If local settings have been set, use the `clear` command to reset that configuration to default. For example: `clear config.autosupport.recipients.note`
3	Accessing the CLI console of each target appliance, use the `cp` command to copy the configuration file to the local directory on the appliance. Use the following syntax: `cp {ftp|http}://[`*usr*`:`*pw*`@]`*/srvr/path/sfile /nc_path/nc_file* **Note** Enter the preceding syntax on one line with a space separating the */sfile* and */nc_path* variables. *usr*:*pw* is the login name and password, if any, necessary to access the source server where the configuration file was created. *srvr*/*path*/*sfile* is the host name, directory, and file name of the configuration file on the source server. *nc_path*/*nc_file* is the target directory location and file name on the appliance where you want the configuration file copied. For example: `cp ftp://usrA:pw@srvrA//cfg/pushedfile.cfg /tmp/pushedfile.cfg`

Step	Action

4	Accessing the CLI console of each target appliance, use the `config.admin.config.list` setting to add this file to the local appliance's active configuration. Remember to do the following:
	◆ Include a local directory path.
	◆ List the configuration file just before the local.cfg file.
	For example, the following command line directs the local appliance to apply the settings in the pushedfile.cfg file just before the local.cfg settings.
	`set config.admin.config.list \\`
	`default.cfg`
	`/tmp/pushedfile.cfg`
	`local.cfg`
	`\\`

5	Accessing the CLI console of each target appliance, use the CLI `set config.admin.config.refresh*` commands to schedule times at which the target appliance will refresh its active settings with any new settings in the pushed configuration file. Follow the procedure described in "Schedule the appliances to refresh their configurations" on page 250.
6	To apply your configuration immediately, enter the following at the CLI console of the target appliance: **`config -n`**
7	Push any subsequent changes to the configuration file to the target appliance, following the procedure in Step 3. **Note** At each target appliance, never use the Appliance Manager or the CLI to modify the local appliance settings specified by the copied configuration file.

Backing up and restoring pushed configuration files

Restoration of pushed configuration files can only be performed locally, to the appliance being restored. The CLI commands to carry out backup and restoration are described in the following paragraphs.

Backing up configuration files: To back up the local.cfg file and the pushed global configuration file on an appliance, use one of the following CLI command lines:

- `config -c backup_file`
- `config_backup backup_file`

Restoring configuration files: To restore a backed-up local.cfg file and a pushed global configuration file to an appliance, use one of the following CLI command lines:

- `config -r backup_file`
- `config_restore backup_file`

If your appliances are not picking up all pushed values

On each target appliance, the settings in the system default local configuration file, local.cfg (which contains any settings you have made on the local appliance through either the Appliance Manager or the CLI), overwrite the values of any matching configurations in global configuration files applied previously. This means that conflicting option values will be set to the value defined in local.cfg.

To view local changes that were made by administrators to the appliance through the Appliance Manager or CLI, enter the following command from the local appliance CLI:

```
show $local.cfg:config.*
```

If you want local configurations that merely append to, not overwrite, settings in global configuration files, see the procedure in “Configuring local settings that do not overwrite global settings” on page 267.

Cloning appliance configurations

Copying a configuration to another appliance

If you do not want to create and maintain a global configuration file, but you want to reuse settings configured on one appliance on other appliances, you can use the `config -clone` command/parameter combination to quickly copy, or "clone," the configuration of one appliance to another appliance.

With the following procedure, local appliance settings that were specified during appliance setup (such as the host name) are preserved on the local target appliance, even after the copy is completed.

Note

This operation is not automated. Subsequent modifications to the source appliance configuration are not automatically copied to the target appliance.

To clone one appliance configuration to other appliances, complete the following steps.

Step	Action
1	Using the CLI or Appliance Manager, set up the source appliance with the configuration that you want to copy to any target appliance.
2	At the CLI console of the target appliance, enter the `config -clone` command using the following syntax: `config -clone` *`admn`*`:`*`pw`*`@`*`src_nc_name`*`:`*`src_admn_port`* *admin* is the name of the administrator of the source appliance. *pw* is the administrator's password. *src_nc_name* is the FQDN of the source appliance. *src_admn_port* is the administration port on the source appliance. For example, the following command line in the ApplianceB CLI console copies the configuration of ApplianceA: `config -clone admin:passwrdz@Appliancea.yurcorp.com:133`

Step	Action
3	To confirm that the copy operation is complete, in the CLI console of the target appliance, enter the following command and view the resulting configuration display: **`show config.*`**
4	Use the CLI commands or the Appliance Manager to edit any configuration settings that need to be edited on the target appliance. **Note** Settings specific to the local appliance (such as the host name) that you specified during appliance setup are preserved on the target appliance, even after the copy is completed.

Note

Any comment lines (prefaced with the `#` character) that are inserted in the source configuration file will not be included in the configuration that is cloned to the target appliance.

Copying a configuration to a global configuration file

You can use the `show -clone` command/parameter combination to quickly copy, or "clone," the configuration of one appliance to a configuration file that is suitable for use as a global configuration file.

With the following procedure, local appliance settings that were specified during appliance setup (such as the host name) are not copied to the configuration file.

Note

This operation is not automated. Subsequent modifications to the source appliance configuration are not automatically copied to the target appliance.

To clone one appliance configuration to other appliances, complete the following steps.

Step	Action
1	Using the CLI or Appliance Manager, set up the source appliance with the configuration that you want to copy to the configuration file.

Step	Action
2	At the CLI console of the target appliance, enter the `show -clone` command using the following syntax: `show -clone ftp://`*`ftp.server.com`*`/`*`cache`*`.cfg` where *ftp.server.com* is the name of the FTP server. *cache.cfg* is the name of the configuration file.
3	If you do not want to propagate all of the cloned configuration settings, edit the file to contain only the settings that you want to apply to your appliances.
4	On each appliance that you want to use the global configuration file, specify the following on the Setup tab > System > Automatic Configuration page in the Appliance Manager: ◆ The location of each global configuration file in the Automatic Configuration Files list ◆ The interval at which you want the appliance to read the listed multiple-cache configuration files

Appliance upgrade considerations

Version upgrade of local configuration files

Starting with NetCache 5.0.*x*, when you upgrade from one version of NetCache to the next, any configuration file on the local appliance that you are upgrading is updated to be compliant with the version that you are upgrading to.

Global configuration file version string requirements

All global configuration files that are read by appliances undergoing upgrade to NetCache 5.3.1 require an initial version string line of the following syntax:

```
#!Config Vx.xxx
```

In the preceding string, *x.xxx* is the number of the NetCache version with which the option settings contained in this configuration file are compliant.

Note

All the configuration options specified in the configuration file must be compliant with the version specified in this line.

Automatic local version conversion: When reading configurations from a remote global configuration file, the local appliance reads the version line of that global configuration file.

If the NetCache version of the remote global configuration file is *earlier* than the version of NetCache installed on the local appliance, the local appliance locally converts any outdated configuration options from the global configuration file to be compliant with its own installed version of NetCache.

Before upgrading a local appliance version

Before you upgrade the NetCache version of a local appliance, verify that the global configuration files that it references all contain an initial version string line.

If a global configuration file contains no version string, the local appliance does not read the global configuration file and displays an error message.

Before upgrading a global configuration file version

Before you modify a global configuration file to support a later version of NetCache, verify that every appliance that reads that global configuration file is running either the version of NetCache that you are modifying to or a later version.

If the NetCache version of a remote global configuration file is *later* than the version of NetCache installed on a local appliance, the local appliance does not read that global configuration file and displays an error message.

Troubleshooting 16

About this chapter

This chapter discusses the most common problems with the NetCache appliance, how to troubleshoot those problems, and how to get technical assistance from your service provider or Network Appliance Technical Support if you cannot troubleshoot or resolve those problems.

Topics in this chapter

This chapter contains the following topics:

- Section A, "Determining the source of the problem," on page 280
- Section B, "Common NetCache troubleshooting solutions," on page 287
- Section C, "Diagnosing and recovering from network problems," on page 304
- Section D, "Diagnosing and recovering from disk problems," on page 314
- Section E, "Diagnosing Web caching and HTTP problems," on page 319
- Section F, "Resolving general system problems," on page 325
- Section G, "Contacting Network Appliance Technical Support," on page 332

Related information

Hardware problems are described in the hardware guides. See the hardware guide for your NetCache appliance model for information about system LEDs, LCD error messages, and system start-up messages.

Section A: Determining the source of the problem

Troubleshooting approach

If the Web cache service is not working, determine whether the source of the problem is the NetCache appliance or the network. Problems on the network can obstruct the Web cache service.

Topics in this section

This section includes information about the following topics:

- "Verifying accessibility to the NetCache appliance" on page 281
- "Determining if NetCache is the source of the problem" on page 284

Verifying accessibility to the NetCache appliance

Determine if the NetCache appliance is accessible

To determine whether the NetCache appliance is running, complete the following steps.

Step	Action	
1	Try to access the Appliance Manager. If you are unable to access the Appliance Manager, see "Recovering access to the Appliance Manager" on page 299.	
2	**If...**	**Then...**
	You can access the Appliance Manager	NetCache is running.
	You cannot access the Appliance Manager	Check the NetCache appliance's network interfaces to make sure that the management workstation can access the appliance. See "Configuring an interface using the ifconfig command" on page 309 for more information.
3	If you still have not found the source of the problem, try to access the console using the `telnet` command.	
4	**If...**	**Then...**
	You can access the console through `telnet`	The NetCache appliance is turned on.

Step	Action	
	You cannot access the console through `telnet`.	The system might have halted during a boot process. Go to the console and press Enter. ◆ If you get an OK prompt, the system is running. ◆ If the system prompts "whether you want to attempt a floppy boot," someone left a system boot diskette in the diskette drive. Remove the diskette and cycle power on the NetCache appliance.
5	Check the LED indicators on the NetCache appliance. See the hardware guide for your NetCache appliance model for more information about the LED indicators.	
6	If you are using a terminal server and the NetCache appliance seems to be up but you cannot enter commands from the console, check all connections between the NetCache appliance and the system where you are entering commands. For example, if the terminal server is in a failure mode, it does not take your input. In this case, reboot the terminal server.	
7	If it still appears that the NetCache appliance is down, follow the procedure described in "How to reboot a down NetCache appliance" on page 290.	
8	If you still are not successful finding the problem, use the `telnet` command to access `hostname` *`admin_port`* or `hostname` *`proxy_port`*	

Step	Action	
9	**If...**	**Then...**
	The connection is accepted	Press Enter a couple of times. If you see an error message, NetCache is up.
	The connection is refused	NetCache is probably not running; a network problem might exist that is causing the problem, or the cache may not be accepting requests from your IP address.

Determining if NetCache is the source of the problem

Determining the source of the problem

To determine whether the problem is due to the NetCache appliance, complete the following steps.

Note

If your NetCache appliance is configured for transparent proxying, you must perform this procedure at a computer that does not receive traffic filtered by an L4 or L7 switch.

Step	Action
1	Record the proxy configuration information from your browser or from the browser of the user reporting the problem.
2	Remove the proxy configuration from the browser.
3	Enter a URL into the browser's location field. You are requesting the URL directly from the Internet.

Step	Action	
4	**If...**	**Then...**
	The URL is returned	Configuration errors are with either of the following: ◆ The proxy configuration in the browser ◆ The NetCache appliance See "Determining configuration errors" on page 285 for further troubleshooting.
	The URL is not returned	The problem is with any of the following: ◆ The browser, possibly a bug ◆ The network ◆ The service provider ◆ The host machine The most common problem is that the network connection is not firmly attached to the host machine. However, problems with the machine itself can occur. See "Determining other problems" on page 286 for further troubleshooting.

Determining configuration errors

To determine whether the problem is caused by errors in the proxy configuration of the browser or on the NetCache appliance, complete the following steps.

Step	Action
1	Check the browser's proxy configuration to ensure that the browser is set up correctly.

Step	Action
2	If you are using an automatic proxy configuration file, ensure that it is set up correctly and that the file name and location that are in the browser are correct. The *Deployment Guide* contains detailed information about using an automatic proxy configuration file.
3	If there is no problem with the browser configuration, see "Verifying accessibility to the NetCache appliance" on page 281.

Determining other problems

To determine if the problem is caused by any other reason, such as a bug in the browser, network, service provider, or the host machine configuration, complete the following steps.

Step	Action
1	Look for problems on your network. See "Identifying and resolving network problems" on page 305 for more information about troubleshooting network problems.
2	Contact your service provider.
3	Contact the administrator of the target host.

Section B: Common NetCache troubleshooting solutions

About this section

This section describes troubleshooting procedures for diagnosing and resolving some of the common errors that cause disruptions in NetCache service, such as recovering from a forgotten password and regaining access to the Appliance Manager.

Topics in this section

This section includes information about the following topics:

- "Recovering from a forgotten console password" on page 288
- "Rebooting a down NetCache appliance" on page 290
- "Booting from the system boot media" on page 292
- "Troubleshooting from the console" on page 296
- "Recovering access to the Appliance Manager" on page 299
- "Solving common NetCache configuration problems" on page 301
- "Recovering from a system panic message" on page 303

Recovering from a forgotten console password

Resetting the console password

To reset the NetCache appliance's console password, complete the following steps.

Step	Action	
1	Insert the system boot diskette into the disk drive.	
2	Reboot the system using one of these methods. **Note** Booting from the diskette takes longer than booting from the hard disk	
3	**If the console is...**	**Then do this...**
	Showing the NetCache appliance prompt (for example, `toaster>`)	Enter **`reboot`**.
	Showing the `ok` or `mon>` prompt	Enter **`b`**.
	Not responding	If you have an appliance model other than C1100 or C1105, enter **`boot floppy`**.
	Still unresponsive	Reset the NetCache appliance by turning it off, leaving it off for 30 seconds, and turning it back on.

	Result: After the NetCache appliance boots, the console will display the following menu:
	`1) Normal Boot`
	`2) Boot without starting system devices`
	`3) Change Password`
	`4) Initialize all disks`
	`5) Maintenance mode boot`
	`Selection (1-5)?`	

Step	Action
4	Type `3` and press Enter.

5	When the NetCache appliance prompts you for a new password, enter it at the prompt.
	The system prints the following message:
	`Password Changed`
	`Hit Return to reboot:`

6	Remove the diskette from the disk drive and reboot the NetCache appliance by pressing Enter.

Rebooting a down NetCache appliance

Normal NetCache appliance behavior

The NetCache appliance normally restarts itself after an unexpected shutdown. However, configuration errors or a disk failure can result in the NetCache appliance not rebooting automatically.

How to reboot a down NetCache appliance

To reboot the NetCache appliance if it does not automatically restart itself, complete the following steps.

Step	Action	
1	Write down the messages displayed on the console and the message on the LCD.	
2	Do one of the following, depending on your console display.	
3	**If the console is...**	**Do this...**
	Showing the `ok` or `mon>` prompt	Enter **`b`**.
	Unresponsive	Reset the NetCache appliance by turning it off, leaving it off for 30 seconds, and turning it back on.
4	If the NetCache appliance does not boot, insert the system boot diskette in the disk drive.	
5	**If the console is...**	**Do this...**
	Showing the `ok` prompt	Enter **`boot`**.
	Unresponsive	Reset the NetCache appliance by turning it off, leaving it off for 30 seconds, and turning it back on.

Step	Action

	Result: After the NetCache appliance boots, the console displays the following menu:
	`1) Normal Boot`
	`2) Boot without starting system devices`
	`3) Change Password`
	`4) Initialize all disks`
	`5) Maintenance mode boot`
	`Selection (1-5)?`

6	Type **`1`** and press Enter.
7	If you cannot boot the NetCache appliance from the system boot diskette, call Network Appliance Technical Support. See Section G, “Contacting Network Appliance Technical Support,” on page 332.

Booting from the system boot media

Appliance models that this section applies to

The information in this section applies to all NetCache appliance models.

Boot media to use

The following table shows the media used for booting the various appliance models.

Note
For an unresponsive appliance, reset the appliance by turning it off, leaving it off for 30 seconds, and turning it back on again. If the appliance is still unresponsive, proceed with rebooting.

For this model...	Use this boot media...
C1200 and C2100	System boot compact flash PC-card **Note** The C2100 appliance boots from a resident compact flash PC-card.
C1100, C1105, C3100, and C6100	System floppy boot diskettes

When to boot from the system boot media

You might need to reboot the NetCache appliance from the system boot diskettes or compact flash PC-card to correct configuration problems, recover from a forgotten password, or correct certain disk configuration problems.

Where to find new system boot images

Occasionally, Network Appliance makes new system boot images available when releasing upgrades to the NetCache software. Check the NOW site (http://now.netapp.com/) to see whether you need to create new system boot diskettes or compact flash PC-card for a software upgrade.

Secure system boot media

To avoid security problems, limit access to the system boot diskettes and compact flash PC-cards.

Booting from system diskettes to bypass the current configuration

You can bypass the current configuration on the NetCache appliance by booting the appliance from the system boot diskettes.

To boot the NetCache appliance from the system boot diskettes, complete the following steps.

Step	Action	
1	Insert the first system boot diskette into the disk drive.	
2	**If the console is...**	**Then...**
	Showing the `ok` prompt	Enter **`boot`**.
	Unresponsive	Enter **`boot floppy`**. If the console is still unresponsive, reset the NetCache appliance by turning it off, leaving it off for 30 seconds, and turning it back on again.
	Note Booting from the diskette takes longer than booting from the hard disk.	

Step	Action

3	Insert all other system boot diskettes into the disk drive when prompted by the console.
	
	Result: After the NetCache appliance boots, the console displays the following menu:
	
	`1) Normal Boot`
	`2) Boot without starting system devices`
	`3) Change Password`
	`4) Initialize all disks`
	`5) Maintenance mode boot`
	
	`Selection (1-5)?`

4	Type **`2`** and press Enter. You are bypassing the configuration.
5	Run the `setup` command to set the main configuration options. For more information about the `setup` parameters, see the NetCache *Quick Setup* document.
6	Remove any diskettes from the disk drive.
7	Go to the Appliance Manager and restore a backup configuration file. See the topics on backing up and restoring a system configuration file in the Appliance Manager online Help for more information.
8	Reboot the NetCache appliance to apply the backup configuration.

Booting from a compact flash PC-card

The C1200 and C2100 model appliances use a compact flash PC-card as the primary boot device. On the C1200, the flash card is normally never removed from the appliance. The flash card on the C2100 is always resident.

Hot swapping of the flash card is not supported; that is, the appliance must be halted and powered down prior to removal or installation of the flash card.

The rules for when you would boot and where to obtain boot files are the same as those stated for booting from diskettes.

To boot the appliance from the compact flash PC-card, complete the following steps.

Step	Action	
1	Halt the appliance.	
2	**If the console is...**	**Then...**
	Showing the `ok` prompt	Enter **`bye`**.
	Unresponsive	Enter **`bye`**. If the console is still unresponsive, reset the appliance by turning it off, leaving it off for 30 seconds, and turning it back on again.
	After the appliance boots, the NetCache prompt will display.	
3	Run the `setup` command to set the main configuration options. For more information about the `setup` parameters, see the *NetCache Quick Setup* document.	
4	Go to the Appliance Manager and restore a backup configuration file. See the topics on backing up and restoring a system configuration file in the Appliance Manager online Help for more information.	
5	Reboot the appliance to apply the backup configuration.	

Troubleshooting from the console

Using the NetCache appliance command line

To access the Appliance Manager, the NetCache appliance must first be accessible from a host running a Web browser. If you cannot access the Appliance Manager, you might need to use the NetCache appliance command line.

You can use the NetCache appliance command line directly at the console or by establishing a Telnet session to the NetCache appliance. You can also access the console through a Telnet session if you have a terminal server setup.

Note

Making configuration changes from the console puts the NetCache appliance configuration out of synchronization with the Appliance Manager. The Appliance Manager reapplies its configuration at the next system boot.

Both the console and a Telnet session to the console provide access to a single console session. That is, everything entered through the Telnet session is echoed at the console, and vice versa. Only one Telnet session can be open at a time.

If you are using the `telnet` command to log out from the NetCache appliance, press **`Ctrl-]`**, then press **`Ctrl-D`** to log out of the Telnet session.

About the console password

Although Telnet and the console share the same session, each prompts you for a password. Both console and Telnet connections use the same password. This password is referred to as the console password.

During initial system setup, the console password required to log in to the console or establish a Telnet connection with the NetCache appliance is created. You can change this password only through the console command line by using the `passwd` command. The `passwd` command prompts for the old password, if any, then requests the new password twice.

Using the sysstat command to get the system status

Entering the `sysstat` command at the NetCache appliance's console or the command line provides the following information:

- CPU usage
- Number of URLs being served

- Network traffic
- Disk activity
- Bandwidth savings

An example of `sysstat` output for a system is as follows:

```
cache2> sysstat 2
 CPU    URLs/s   Net kB/s    Disk kB/s       BW savings/s
        tot   hit  miss  in    out    read   write
  2%     0     0    0   0      0     16     24   0%
  0%     0     0    0   0      0      6      7   0%
  1%     0     0    0   0      0     10     16   0%
  0%     0     0    0   0      0      5      8   0%
```

The following table shows the action to take when you identify problems examining the `sysstat` output.

Problem	Action to take
No network traffic	Check the NetCache appliance's interface configuration using the `ifconfig` command. See "Configuring an interface using the ifconfig command" on page 309 for more information.
No disk activity	Call Network Appliance Technical Support.

Using the config command to manipulate the NetCache configuration

In case of disaster, you can use the `config` command to manipulate the NetCache appliance configuration from the console command line. By using the `config` command, you can create a backup configuration, revert to a previous configuration, delete an old configuration, clear the current configuration, and clone a configuration file from another NetCache appliance.

Use the `config` command options as follows, where *config_file* is the name of the backup configuration file:

Syntax 1: `config -n`

Syntax 2: `config [-z | -Z]`

Syntax 3: `config [-c | -d | -v] config_file`

Syntax 4: `config -r [-global | -detach] [-skip] config_file`

Syntax 5: `config -clone` *`user:password@cache:port`*

Option	Description
`-n`	Downloads and recompiles the configuration files listed in the `config.admin.config.list` option.
`-z`	Restores the configuration to default values
`-Z`	Clears the current configuration. No configuration will exist upon a reboot.
`-c`	Backs up the current configuration to a named file. You can also use the `config_backup` command.
`-d`	Deletes the named configuration file.
`-v`	Displays the named configuration file.
`-r`	Restores the named configuration file locally. You can also use the `config_restore` command.
`-r` `-global`	Restores the named configuration file to all sources.
`-r` `-detach`	Detaches the cache from remote servers.
`-r` `-skip`	Skips invalid values in the backup file.
`-clone`	Clones the configuration of another NetCache appliance to this NetCache appliance.

Recovering access to the Appliance Manager

Reasons why the Appliance Manager might be unavailable

Two possible reasons why you cannot access the Appliance Manager are as follows:

- You might be entering the incorrect Admin Port number in the URL for the Appliance Manager.
- The network interface might be down.

What to check

If the NetCache appliance appears to be running but the Appliance Manager is unavailable, complete the following steps.

Step	Action
1	Try entering the URL for the Appliance Manager again. You might be using the incorrect Admin Port number in the URL for the Appliance Manager. The default value for the Admin Port is 3132. If you changed the default value of the Admin Port option and forgot the number, you must restore a previous configuration backup file. See the topics on backing up and restoring a system configuration file in the Appliance Manager online Help for more information. Also, see "Using the config command to manipulate the NetCache configuration" on page 297 for information about how you can create configuration backup files from the command line.
2	Check the NetCache appliance's interface configuration. Use the `ifconfig` command at the console to check the interface configuration. See "Configuring an interface using the ifconfig command" on page 309 for more information.
3	If the interface configuration is correct, use the `telnet` command to try to access the console from a workstation to determine whether the console is available.

Step	Action
4	If the console is available and there are no visible error messages, reboot the NetCache appliance. See "Rebooting a down NetCache appliance" on page 290 for instructions.
5	If rebooting the NetCache appliance does not work, call Network Appliance Technical Support. See Section G, "Contacting Network Appliance Technical Support," on page 332 for information about how to contact Technical Support.

Solving common NetCache configuration problems

Most common configuration problems

The most common configuration problems that can affect Web cache service are

- A damaged configuration file
- A misconfigured network interface
- A misconfigured IP address

Configuration file issues

Booting when the configuration file is damaged: If you cannot boot the NetCache appliance and you suspect the cause is a configuration error, try booting from the system boot diskette. For more information, see "Booting from the system boot media" on page 292.

Recovering from a damaged configuration file: If a NetCache configuration was damaged, replace the file with a backup copy.

You can restore a saved version of the configuration through the Appliance Manager or replace it from the console using the command line. See the topics on backing up and restoring a system configuration file in the Appliance Manager online Help for more information.

Multiple cache administration: If you restore a configuration file that other NetCache appliances read for configuration updates, you can instruct those appliances to refresh their configurations immediately to avoid further configuration problems.

Network interface issues

Run the `ifconfig` command from the console to reconfigure an interface. See "Configuring an interface using the ifconfig command" on page 309 for more information.

IP address misconfiguration issues

If you can access the NetCache appliance from the console, but not from an administration workstation, the NetCache appliance might have an IP address that is unreachable.

To fix the IP address misconfiguration problem, complete the following steps.

Step	Action
1	Log in to the NetCache appliance from the system console.
2	At the NetCache appliance prompt, enter the following command: `ifconfig` *`interface_name IP_address netmask netmask`* where *interface_name* is the name of the interface for which you are configuring the IP address and netmask is the subnet mask of the network to which this NetCache appliance is connected. **Note** Changing the configuration from the command line makes temporary changes. It does *not* affect the saved NetCache configuration. The saved NetCache configuration is reapplied the next time the system is booted. You can, however, use the `ifconfig -set` *options* command to make the change permanent.
3	From an administration workstation, start a browser and point it to the Appliance Manager.
4	Check the Network - Interfaces page (Setup tab > Network > Interfaces) to make sure that the network interfaces are configured correctly. Specifically, check the IP address and netmask.
5	If the “Only from These Hosts and Networks” option on the Administrative Access page (Setup tab > Administration > Administrative Access) is selected, make sure that the host you are working from is included in the list of hosts allowed.

Recovering from a system panic message

Example of a system panic message

If your NetCache appliance experiences a serious problem, it issues a system panic message similar to the following message:

```
PANIC: system hung (NS0)!
```

Meaning of a system panic message

This message indicates that either a problem with the hardware exists or a bug in the system software exists.

What to do if you receive a system panic message

If you receive a system panic message, call Network Appliance Technical Support immediately.

Note

The panic class of this message is significant; the actual text of the message varies with circumstances. Be sure to write down the actual panic message and send it to Network Appliance Technical Support when reporting a NetCache appliance problem.

Section C: Diagnosing and recovering from network problems

About this section

This section describes how to isolate the source of common network problems that can disrupt NetCache appliance services.

Topics in this section

This section includes information about the following topics:

- "Identifying and resolving network problems" on page 305
- "Verifying the DNS configuration" on page 307
- "Configuring an interface using the ifconfig command" on page 309
- "Downloading and deleting packet trace (pktt) files" on page 312

Identifying and resolving network problems

Detecting network problems

You can detect network problems by going to the NetCache appliance console and using the `ping` command. The `ping` command verifies whether the NetCache appliance can communicate with other hosts on the network and whether other hosts can communicate with the NetCache appliance.

How to troubleshoot network problems

If you expect that the NetCache appliance should be able to connect with a host but `ping` does not respond with a message indicating that the host is alive, complete the following steps to troubleshoot the problem.

Step	Action
1	Check that the network cable is tightly connected to the proper interface connector.
2	Use the `ifconfig -a` command at the console to verify that the IP address and netmask are set correctly, and the up and running flags are displayed.
3	Use the `arp -a` command at the console to confirm that the NetCache appliance has the correct IP-to-Ethernet address map for the host you are trying to reach.
4	Use the `netstat -i` command at the console to check for excessive errors on the interfaces. If you see excessive input errors (ierrs) or output errors (oerrs), check the network connections on both ends of the connection. Bad transceivers or network hubs can sometimes introduce errors into the network. Collisions reported by the `netstat` command are a concern only if the NetCache appliance detects a substantial percentage of collisions, as compared to the total packet throughput. The goal is to keep collisions below 5 percent, but a network can operate properly (but slowly) with collision rates as high as 30 percent.
5	Run the `netstat -r` command to examine the routing tables.

Step	Action
6	Run the `route -s` command to find out the status of the default router.
7	Run the `ifstat -a` command to display statistics for all of the network interfaces on this NetCache appliance, including the virtual host and the loopback address.
8	Run the `traceroute` command to display the route that packets take to a network host.

Note

An improperly set up network router can also cause network problems. If a router is not working correctly or is not configured with the NetCache appliance's IP address, clients or hosts on the other side of the router cannot access the NetCache appliance through that router.

Contact technical support about other network problems

If you encounter other network problems, contact Network Appliance Technical Support for help, as described in Section G, "Contacting Network Appliance Technical Support," on page 332.

Verifying the DNS configuration

About verifying the DNS configuration

Troubleshoot the DNS configuration as you would on any network. The only difference is the location where the DNS values are configured on the NetCache appliance.

Determining whether a DNS problem prevents reaching a host

NetCache error messages distinguish between a problem with a connection (the connection or the host is down) and a failure when an attempt is made to translate the host name to an IP address. If you receive an error message that indicates the latter, it is likely that a DNS problem exists. A DNS problem might be limited to only some hosts or it might be global.

Network Appliance recommends that you confirm that NetCache is not causing the problem before you investigate a potential DNS problem. You can do so by using the `ping` command or `nslookup` from a non-NetCache computer to request name resolution for the host for which you are receiving error messages. If you experience the same problem, then the problem is on the server side. If the problem is gone, continue your NetCache troubleshooting by checking the DNS configuration items in the next section.

Configuration items to check for DNS

Check the following DNS items:

- The nameservers and the appliance domain name
  - In the Appliance Manager, this information is configured on the DNS - General page (Setup tab > DNS > General).
  - In the NetCache CLI, use the `show status.dns.*` command.
- The DNS configuration on your nameserver

  Make sure that your nameserver is still able to service the DNS queries.

What else to check

While troubleshooting DNS configuration, also check the items in the following table.

If...	Then...
URLs outside the firewall cannot be accessed	Make sure that the DNS server that the NetCache appliance is configured with can resolve the Internet names (external URLs).
URLs inside the firewall cannot be accessed	Make sure that the DNS server is able to resolve the URLs that you are trying to access.

Configuring an interface using the ifconfig command

About using the ifconfig command

The NetCache appliance configuration contains the information required to configure network interfaces at system boot. If you cannot access the Appliance Manager, you can use the `ifconfig` command at the console to configure an interface.

The changes you make using the `ifconfig` command at the console are persistent only if made using the -set option.

ifconfig command syntax

The `ifconfig` command syntax is as follows:

```
ifconfig [ -a | [ [-set] <interface>
[ [ alias | -alias ] <address> ] [ up | down ]
[ netmask <mask> ] [ broadcast <address> ]
[ mtusize <size> ]
[ mediatype { tp | tp-fd | 100tx | 100tx-fd | 1000fx | auto } ]
[ flowcontrol { none | receive | send | full } ]
[ trusted | untrusted ]
] ]
```

When to use the ifconfig command

Usually, you use the `ifconfig` command for the discussed purposes in the following paragraphs:

Changing the interface's IP address, network mask, or broadcast address: The following are examples of `ifconfig` commands that can be used to configure an Ethernet interface on a NetCache appliance:

```
ifconfig e1 192.9.200.6
ifconfig e1 netmask 255.255.255.0
ifconfig e1 broadcast 192.9.200.255
```

The interface names on your system might be different, depending on your NetCache appliance model. See "Naming conventions for network interfaces" on page 15 for more information about interface naming conventions.

Setting the media type on an Ethernet interface: The following are examples of `ifconfig` commands that can be used to configure an Ethernet interface on a NetCache appliance:

```
ifconfig e1 mediatype 100tx-fd
ifconfig e2 mediatype 1000fx
ifconfig e3 mediatype 100tx
```

The media types you can use depend on the type of Ethernet card. The possible types you can enter in the `ifconfig` command are the same as those you can select when running the setup program.

The media types are described in the following table.

Media type	Description
tp	10Base-T
tp-fd	10Base-T, full-duplex
100tx	100Base-T
100tx-fd	100Base-T, full-duplex
1000fx	Gigabit Ethernet
auto	10Base-T/100Base-TX Ethernet using autonegotiation

Setting the maximum transmission unit (MTU): Generally, you will not need to set the mtusize option for the interfaces on your NetCache appliance. However, you can use this option to set the jumbo frame size on a Gigabit Ethernet interface. This option can also be used to set the frame size on an FDDI interface when the network infrastructure does not support the default FDDI frame size.

The following is an example of an `ifconfig` command that can be used to set the MTU (jumbo frame size) for a Gigabit Ethernet interface on a NetCache appliance.

```
ifconfig e8 mtusize 9000
```

To view the current setting of the MTU size, use the command

```
netstat -i
```

Bringing an interface up or down: The following are examples of `ifconfig` commands that can be used to bring an interface up and bring an interface down.

```
ifconfig e1a up

ifconfig f1 down
```

Showing the current configuration of all interfaces: To show the current configurations of all network interfaces, enter the following:

```
ifconfig -a
```

Showing the configuration of a single interface: To show the current configuration of a specific network interface, for example *e0*, enter the following:

```
ifconfig e0
```

Downloading and deleting packet trace (pktt) files

About pktt files

If you encounter certain kinds of networking problems, Network Appliance Technical Support might instruct you to run a packet trace. NetCache provides a way to download these files to Network Appliance Technical Support for analysis.

How to download a pktt file

To download a `pktt` file, complete the following steps.

Step	Action
1	In the Appliance Manager, select Utilities tab > Diagnostics > Packet Trace.
2	In the "Select a Packet Trace File" list, select the file that you want to download.
3	To download the file, select "Send the File to the Following FTP or Web Server," then enter the FTP server or the Web server URL in the box. If the FTP server or the Web server requires a user name, password, port, or path, use the following format: *protocol*`://user:`*password@server:port/path/file* where *protocol* can be `ftp`, `http`, or `https`.
4	Click Submit.

How to delete a pktt file

To delete a `pktt` file, complete the following steps.

Step	Action
1	In the Appliance Manager, select Utilities tab > Diagnostics > Packet Trace.
2	In the “Select a Packet Trace File” list, select the file that you want to delete.
3	To delete the file, select “Delete the file.”
4	Click Submit.

Section D: Diagnosing and recovering from disk problems

About this section

This section describes how to troubleshoot and recover from disk problems on the NetCache appliance.

Topics in this section

This section contains information about the following topics:

- "Recovering from disk problems using boot media options" on page 315
- "Recovering from a disk failure without a hot spare disk" on page 316
- "Recovering from a disk failure with a hot spare disk" on page 318

Recovering from disk problems using boot media options

About this section

This section provides information about options on the system boot diskette or compact flash PC-card that are useful for resolving disk problems. See “Booting from the system boot media” on page 292 for information about the media.

Using various disk maintenance options on the system boot media

You can use Option 5, “Maintenance mode boot,” on the system boot diskette or compact flash PC-card for troubleshooting hardware or configuration problems related to disks. For a list of all commands available with Option 5 and their descriptions, enter the following at the CLI prompt:

```
*> disk ?
```

The following output is displayed on your screen:

```
usage: disk <options>
Options are:
    fail   <disk_name> - fail a file system disk
    remove <disk_name> - remove a spare disk
    swap - prepare (quiet) bus for swap
    unswap - undo disk swap and resume service
    scrub  { start | stop } - start or stop disk scrubbing
    unfail <disk_name> - make a failed disk a spare again
    unbypass <disk_name> - unbypass a bypassed disk
    bypass <disk_name> - bypass an unbypassed disk
    rescan - rescan the disks
    suspend <disk_name> - suspend I/O to a disk
    resume <disk_name> - resume I/O to a disk
```

Note

Before booting the NetCache appliance in maintenance mode, call Network Appliance Technical Support for instructions.

Exiting maintenance mode

You must power cycle the NetCache appliance to exit maintenance mode.

Recovering from a disk failure without a hot spare disk

About this section

How disk failures affect the NetCache appliance depends on whether a hot spare disk is installed. This section describes how the NetCache appliance reacts to a disk failure when a hot spare disk is not available.

What happens with a single disk failure

For all models except the C1100, C1105, and single-disk C1200, if a single disk fails and a hot spare disk is not installed, the appliance continues to run without losing any data, but with a degraded performance.

The C1100, C1105, and single-disk C1200 models enter a system panic when a single disk failure occurs. The appliance must be halted and powered down before having the disk removed and replaced. Additionally, for the C1200 model, see "What happens with cold swap devices" on page 317.

The disk failure causes automatic shutdown after 120 hours. You can restart the appliance without fixing the disk, but the appliance continues to shut itself off every 120 hours until you repair or replace the disk.

The appliance sends a warning message to the Messages log and the system console every hour after a disk has failed.

Caution

Replace the disk as soon as possible because a second disk failure can cause the NetCache appliance to lose the entire file system.

What happens with a double disk failure

If a second disk fails while the NetCache appliance is operating in degraded mode, or if two disks fail at the same time, the file system is damaged and cannot be repaired. You must reinstall both the file system and the NetCache software in that case. See the topics on backing up and restoring a system configuration file in the Appliance Manager online Help for more information.

Caution

Removing more than one disk at a time from your appliance will result in data loss. If you remove more than one disk at a time from the appliance, the appliance will not be able to rebuild the data from the remaining disks.

What happens after you replace a disk drive

After you replace a disk drive, when the NetCache appliance boots, it detects the new drive, starts file service, and rebuilds the missing data in the background with minimum interruption to service. For a single-disk C1200 model, you must reinstall the NetCache appliance software and licenses after replacing a disk drive.

What happens with cold swap devices

The C1200 appliance disk drives are cold swap drives, which means the appliance must be halted and powered off before you remove or install a drive. The C1200 uses a compact flash PC-card as its primary boot device (default). The PC-card resides on the C1200 and is normally never removed.

Recovering from a disk failure with a hot spare disk

About this section

How disk failures affect the NetCache appliance depends on whether a hot spare disk is installed. This section describes how the NetCache appliance reacts to a disk failure when a hot spare disk is available.

What happens if a hot spare disk is available

If a hot spare disk is available when a disk failure is detected, the hot spare disk automatically comes online as a replacement. The missing data is rebuilt on the hot spare disk in the background so that the interruption to file service is minimized.

The Messages log file records information about the disk failure and hot spare disk replacement activity. The Messages log also logs any failures detected in the periodic checks of the hot spare disk.

Automatic shutdown does not occur if a single disk drive fails and a hot spare disk is available. After the appliance is finished rebuilding data on the hot spare disk, replace the failed disk with a new hot spare disk as soon as possible to ensure that a hot spare disk is always available in the system.

If you do not replace the hot spare disk and another disk fails, a warning message is displayed every hour to remind you to replace the disk. The appliance gracefully shuts down every 120 hours until a replacement disk is installed.

Viewing the hot spare disk in the GUI

You can view the hot spare disks available on your NetCache appliance on the Disk - Management page (Maintenance tab > Disk > Management). The disks are labeled *spare* in the Disk Type column.

Section E: Diagnosing Web caching and HTTP problems

About this section

This section describes how to isolate the source of common problems related to the ability of the NetCache appliance to cache Web objects, process URL requests, and handle basic HTTP proxy tasks.

Topics in this section

This section includes information about the following topics:

- "Determining why NetCache is not servicing any URLs" on page 320
- "Determining why you cannot access a specific URL" on page 322

Determining why NetCache is not servicing any URLs

About this section

This section lists the configuration items to check if NetCache cannot service any Web requests. Several configuration errors can cause NetCache to not service Web requests for users.

Note

For problems related to media player URLs, see the troubleshooting sections in the streaming media chapter in the *Guide to Caching Protocols and Services*.

The log files can provide clues

Check the Messages log and the Web access log for clues as to the source of the problem. Often you can quickly determine whether an obvious configuration problem exists.

If you see error codes, check an HTTP reference for descriptions of the return values.

Configuration items to check

If you cannot determine the source of the problem from the log files, check the following items:

- If you have enabled protocol authentication on the Authentication - General page (Setup tab > Authentication > General) and Authentication - LDAP page (Setup tab > Authentication > LDAP) in the Appliance Manager, but you have not pointed NetCache to an LDAP server or RADIUS server, or you have not added users to the NetCache user database, the NetCache appliance cannot service requests.

  Try turning off protocol authentication and then requesting a URL to confirm that this is the source of the problem.
- If you have configured any access controls, check the access control configuration for a setting that might stop all requests. Check also for incorrect regular expressions.

  For more information about creating access controls, see the chapter about access controls in the *Security Guide*.
- Use the `show status.http.*` command to display HTTP statistics.
- Verify the DNS configuration.

  See “Verifying the DNS configuration” on page 307 for details.

- Try running the `sysstat` command at the console. This command reports the number of URLs being served, disk activity, and network traffic.

  See "Using the sysstat command to get the system status" on page 296 for more information.
- If you are using an automatic proxy configuration file (*proxy.pac*), check its configuration. See the *Deployment Guide* for an annotated example of this file.

Determining why you cannot access a specific URL

What to check

If NetCache is servicing requests for URLs, but you are experiencing problems accessing a specific URL, try requesting the URL either directly from the Web server or through the NetCache appliance using the `telnet` command.

Note

You can request a URL directly from a Web server only if your network is set up to allow direct access to the Web server. If your network is set up so that all HTTP requests must pass through your NetCache appliance, requesting a URL directly from the Web server will not work because NetCache will intercept the request.

Requesting a URL directly from a Web server

To request a URL directly from a Web server, complete the following steps.

Step	Action
1	From a workstation, use the `telnet` command to access a Web server. For example: `telnet www.netapp.com 80` where `80` is the port number on the Web server. If your network is set up so that you can request a URL directly from a Web server, access to Web server *www.netapp.com* should be successful.
2	Use the `GET` command to request the HTML source at the root of the Web server. For example: `GET / HTTP/1.0`
3	Press Enter twice.

Step	Action	
4	**If...**	**Then...**
	The HTML source information begins scrolling up the screen	The Web server is up. The source of the problem is either NetCache or the network. If you see an HTTP return error code, check an HTTP reference for descriptions of these return values.
	The HTML source information is not returned	The source of the problem is the Web server.

Requesting a URL through the NetCache appliance

To request a URL through the NetCache appliance, complete the following steps.

Step	Action	
1	From a workstation, use the `telnet` command to access the NetCache appliance. For example: `telnet hostname` *`proxy_port`* where *hostname* is the name of the NetCache appliance and *proxy_port* is the HTTP Proxy Ports option setting in the HTTP - General page (Setup tab > HTTP > General). The default is `3128`.	
2	After you access the NetCache using Telnet, enter the `GET` command to request a URL that you know exists. For example: `GET http://www.netapp.com/ HTTP/1.0`	
3	Press Enter.	
4	**If...**	**Then...**
	The HTML source information begins scrolling up the screen	The NetCache appliance is operating normally. If you see an HTTP return error code, check an HTTP reference for descriptions of these return values.

Step	Action	
	The HTML source information is not returned	Make sure that the NetCache appliance can send requests outside the firewall.

Section F: Resolving general system problems

About this section

This section describes how to resolve system-related problems, such as file system and NVRAM problems. This section also describes how to manage core files if a system crash occurs.

Topics in this section

This section includes information about the following topics:

- "Resolving file system problems" on page 326
- "Resolving NVRAM problems" on page 329
- "Managing core files" on page 330

Resolving file system problems

About this section

This section describes problems you might encounter with the file system and explains how to correct these problems.

When the file system is inconsistent

The file system rarely becomes inconsistent. However, an inconsistent file system can be a result of combined disk and NVRAM failure, or a problem with a newly installed kernel.

If your file system becomes inconsistent, the NetCache appliance displays a message about the problem. Contact Network Appliance Technical Support for assistance, as described in Section G, "Contacting Network Appliance Technical Support," on page 332.

When a file system must be reinstalled

You might need to install a new file system after a fatal error or if two disks fail at or close to the same time.

Note

After you install a new file system, you must also reinstall the NetCache software. The NetCache software is shipped with your system on CD-ROM. If an upgrade is available, you can download it from the Network Appliance NOW site (*http://now.netapp.com/*).

How to install a new file system

To install a new file system on the NetCache appliance, complete the following steps.

Step	Action

1	Insert the first system boot diskette followed by the remaining diskettes into the disk drive as the system prompts you.
	After the NetCache appliance boots, the console will display the following menu:
	`1) Normal Boot`
	`2) Boot without starting system devices`
	`3) Change Password`
	`4) Initialize all disks`
	`5) Maintenance mode boot`
	`Selection (1-5)?`

2	Type **4** and press Enter.
	The following prompts are displayed on the console:
	`WARNING: there appear to be valid labels on the disks!`
	`Zero disks and install a new file system?`

3	Type **y** and press Enter. The following prompt is displayed on the console: `This will erase all the data on the disks, are you sure?`

4	Type **y** and press Enter.
	The following message is displayed on the console:
	`Zeroing disks: takes approximately xx minutes.`
	where xx is the number of minutes displayed depending on your system.
	`A disk can be reserved and designated as a "hot spare" which will be used to automatically replace another disk should a disk fail in your configuration. Note that the spare disk will be reserved and will not be used for your file system.`
	`Reserve a disk for use as a "hot spare"?`

Step	Action
5	(Optional) Type **`y`** and press Enter. The following message is displayed on the console: `"Hot spare" disk 0 reserved.`

Resolving NVRAM problems

NVRAM battery failure

If the NetCache appliance detects low batteries on the NVRAM card, it gives advance warning and automatically shuts down every 24 hours.

If the NetCache appliance is in RAID degraded mode and the NVRAM batteries are low, it fails to boot. You must replace the NVRAM batteries immediately.

NVRAM battery failures generally do not cause data loss. When the NetCache appliance executes the `halt` command, it flushes the contents of NVRAM to disk, then turns off the NVRAM so that no battery power is used.

Inconsistent NVRAM contents

This kind of data error can occur only when you boot a system after a failure or after you turn off a NetCache appliance without using the `halt` command.

The NetCache appliance performs a number of checks to ensure that the NVRAM contents are consistent. If the contents are inconsistent, it discards the inconsistent contents and dumps core.

The file requests received during the last few seconds before the NetCache appliance shuts down are lost. This does not cause the file system to become inconsistent, but files written during the last 10 seconds before shutdown might contain old or incorrect data. Also, because the parity of some recently written stripes might be incorrect, the NetCache appliance must perform a parity check on the entire RAID array. The parity check (and any correction) is performed online, in the background, while continuing otherwise normal operation.

Managing core files

What core files are created

If a hardware or software failure occurs, the NetCache appliance might crash. If a system crash occurs, the NetCache appliance displays a message on the system console, logs a message in the Messages log, and creates a core file named *core.n* (the *n* in the file name is a number).

Core files include information that might be essential for determining the cause of the crash and are often necessary for investigating problems involving the file system.

How many core files are kept

The NetCache appliance saves a maximum of two core files on disk. These core files, named `core.0` and `core.1`, are the files that were created for the previous two system crashes.

What to do with core files

By default, the NetCache appliance automatically sends Autosupport e-mail to Network Appliance Technical Support each time the system is rebooted. However, if you have disabled Autosupport or if you removed the Network Appliance entry from the Autosupport e-mail list, contact Network Appliance Technical Support when your system creates a core file.

The Appliance Manager provides a way to download core files to a client if you need to send a core file to Network Appliance Technical Support. You can also choose to delete a core file to reclaim disk space for proxying.

Downloading a core file

To download a core file in the Appliance Manager, complete the following steps.

Step	Action
1	In the Appliance Manager, select Maintenance tab > Core Files > Current Core Files.
2	In the “Select a Core File” list, select the file that you want to download.
3	Select “Copy the File to Your Computer.”

Step	Action
4	Click Submit.

To download a core file using the NetCache CLI, enter the following command:

```
CacheName> nccore -ul core_file
```

Deleting a core file

To delete a core file in the Appliance Manager, complete the following steps.

Step	Action
1	In the Appliance Manager, select Maintenance tab > Core Files > Current Core Files.
2	In the “Select a Core File” list, select the file that you want to delete.
3	Select “Delete the File.”
4	Click Submit.

To delete a core file using the NetCache CLI, enter the following command:

CacheName> nccore -d *core_file*

Section G: Contacting Network Appliance Technical Support

Information to note before calling for support

Before contacting your service provider or Network Appliance Technical Support, make sure that you have the following information available:

- The system serial number (from the Autosupport message)
- The system configuration as reported in the System Configuration - General page (Data tab > System Configuration > General) in the Appliance Manager
- Any diagnostic messages as reported in the Messages log on the Logging - Messages page (Data tab > Logging > Messages).

How to contact Network Appliance

The telephone numbers and Web address for contacting Network Appliance Technical Support are as follows:

- Telephone

  For U.S. customers:

  (888) 4-NETAPP (US and Canada)

  (1-888-463-8277)

  (408) 822-4700

  For European customers:

  00-800-44-638277 Europe

  31-23-567-9605 Europe

  For all other international customers:

  +1 408 822-4700 (Ask for Technical Support.)
- Web address

  http://www.netapp.com/support

  http://now.netapp.com

When you request technical support through the Web, be sure to include the following in your message:

- Your contact information
- A complete description of the problem
- Listings or printouts of the Messages log, if applicable

Glossary

adapter card

A SCSI card, network card, hot-swap adapter card, serial adapter card, or VGA adapter that plugs into an appliance expansion slot.

appliance

A device that performs a well-defined function and is easy to install and operate.

authentication

A security step performed by NetCache. If protocol authentication is enabled, NetCache requires users to provide a user name and password before servicing any Web requests.

Autosupport

Mechanism that triggers e-mail messages from the customer site to Network Appliance Technical Support or another specified e-mail recipient when a problem or potential problem occurs with the NetCache appliance.

CIDR

See **Classless Inter-Domain Routing**.

Classless Inter-Domain Routing (CIDR)

A type of network routing that uses the network mask instead of the address class to determine the destination network. NetCache access controls can be specified in CIDR format.

console

A terminal that is attached to a NetCache appliance's serial port and is used to monitor and manage the operation of the NetCache appliance.

cookie

A small file sent by a Web server containing information about a particular Web page. This information is generally used to maintain user-specific information and to adjust the appearance of a particular page accordingly, allowing for more personalized content. However, a Web page with a cookie attached to it requires special attention by NetCache, and might be uncacheable.

degraded mode RAID degraded mode is the operating mode of a NetCache appliance when a disk is missing from the RAID array or the batteries on the NVRAM card are low. The missing disk or batteries should be replaced as soon as possible.

DES (Data Encryption Standard) Public key encryption algorithm that uses 56-bit keys. DES is widely used for data encryption to secure communication over the Internet.

disk ID number A number assigned by the NetCache appliance to each disk when it probes the disks at boot time.

disk shelf A shelf that contains disk drives and is attached to the NetCache appliance.

Domain Name Service (DNS) A method by which computers connected to a TCP/IP network can identify each other, using known DNS servers as telephone books in which to look up other machines.

Ethernet adapter An Ethernet interface card.

expansion card A SCSI card, NVRAM card, network card, hot-swap card, or console card that plugs into a NetCache appliance expansion slot.

expansion slot Slots on the system board in which you insert expansion cards.

external disk tray system Asystem in which the disk drives are exposed for easy access.

See also **internal disk tray system**.

FDDI adapter An FDDI interface card.

FDDI-fiber An FDDI adapter that supports a fiber-optic cable.

FDDI-tp An FDDI adapter that supports a twisted-pair cable.

Feeder server The component of a news server that accepts news feeds from other news servers. The Feeder server might be on the same computer as other news server software components or it might be on a different computer.

Fully Qualified Domain Name (FQDN) A host's FQDN consists of its host name and its domain name, separated by a period. For example, the host euler, located in the domain *netapp.com*, has an FQDN of *euler.netapp.com*.

hot spare disk A disk installed in the NetCache appliance that can be used to substitute for a failed disk. Before the disk failure, the hot spare disk is not part of the RAID disk array.

hot swap Adding, removing, or replacing a disk while the NetCache appliance is running.

If-Modified-Since (IMS) A query the NetCache appliance sends to a Web server in order to verify the consistency of an object, that is, to determine whether the object has been modified.

internal disk tray system A closed system in which the disks are not easily accessible.

See also **external disk tray system**.

Internet Cache Protocol (ICP) The method by which a hierarchy of NetCache appliances communicate with each other. A derivative of the User Datagram Protocol, ICP enables NetCache to query other caches for individual Web pages.

LDAP server Lightweight Directory Access Protocol server. LDAP is a client-server protocol for accessing a directory service. NetCache can be configured to point to an LDAP server for authentication of user requests.

live stream

A live stream is a streaming media presentation occurring in real time, like the news program that you watch on your television set. Some organizations record a live media stream and then broadcast the media stream to their employees or customers at a specified time. All users who have requested the media stream see the same media stream at the same time. Users are not able to rewind or fast-forward a live media stream.

See also **stream**, **on-demand stream**, **streaming media**, and **streaming media presentation**.

mail host

Client host responsible for sending automatic e-mail to Network Appliance Technical Support when certain NetCache appliance events occur.

Maintenance Mode

An option when booting a NetCache appliance from the system boot diskette. Maintenance Mode provides special commands for troubleshooting the hardware and system configuration.

Message Digest 5 (MD5)

The MD5 algorithm, created by RSA Data Security, Inc., is a checksum generation for use in security applications. Common uses include verifying the integrity of system files and password checking.

MIB

ASCII files that describe the information that the SNMP agent sends to network management stations.

Microsoft Media Streaming (MMS) protocol

The streaming media control protocol used in Windows Media Technologies (WMT) 3 & 4 streams. MMS is a proprietary protocol owned by Microsoft.

See also **streaming media**.

MIME

See **Multipurpose Internet Mail Extensions**.

MMS

See **Microsoft Media Streaming protocol**.

Multipurpose Internet Mail Extensions (MIME)

A set of definitions and specifications describing the various kinds of information that can be sent across the Internet (video, audio, and so on) and the methods used in their transmission. Every Web browser sends a block of information, called a MIME header, to a server when requesting a Web page. The server, in turn, sends back a MIME response header, as well as the page. Many types of information can be passed in these MIME headers, such as the type of browser used and the last time the Web page requested was modified.

network adapter

An Ethernet, FDDI, or ATM adapter.

network management station

Client workstation on a network that uses a third-party application to process information.

news cache

A NetCache appliance that was configured to accept news requests from clients and to be able to fetch requested news data from a news server or another NetCache appliance that connects to a news server.

NNTP

Network News Transfer Protocol. A news transmission protocol for the Internet. NNTP can be used to transport news from one host to another. Also, newsreader software can use NNTP to access the news database on a server host. One great advantage that NNTP has over UUCP, which preceded NNTP for news transport, is that an NNTP host receiving multiple newsfeeds generally receives only one copy of each article.

NVRAM

Nonvolatile random access memory. Static random access memory that is made into non-volatile storage by having a battery permanently connected.

See also **SVRAM**.

on-demand stream

A previously recorded media stream that users can request at a time most convenient to them. Users can rewind and fast-forward on-demand media streams. Also called video on demand (VOD).

See also **stream**, **live stream**, and **streaming media**.

NVRAM card Adapter card that contains the NetCache appliance's NVRAM cache.

parity disk Disk on which parity information is stored for the RAID-4 disk drive array. Used to reconstruct data in failed disk blocks or on a failed disk.

POST Power-on self-tests run by the NetCache appliance right after the power is turned on.

Pragma:no-cache Request issued by a browser specifying that the proxy agent fetch the original object from the source and not a cached copy.

Proxy mode The default mode of operation for NetCache. In this mode, the cache serves all users who set up their browsers to use NetCache as their proxy. While acting as a proxy, NetCache also caches Web pages requested by users, greatly decreasing response time for subsequent requests for the same Web page, as well as greatly decreasing total network bandwidth usage.

See also **Web accelerator**, **streaming accelerator**.

RAID Redundant Array of Independent Disks. A technique that protects against disk failure by computing parity information based on the contents of all the disks in the array. The NetCache appliance uses RAID Level 4, which stores all parity information on a single disk.

RADIUS server Remote Authentication Dial-In User Service. RADIUS is a client-server protocol for accessing a directory service. NetCache can be configured to point to an RADIUS server for authentication of user requests.

Reader server The component of a news server that obtains the data that the news cache requests from the news storage device such as a NetApp filer. When the news cache does not have requested news in its cache, it connects to the Reader server component of the news server, through NNTP. The Reader server might be on the same computer as other news server software components or it might be on a different computer.

Real Time Streaming Protocol (RTSP)

RTSP is the streaming media control protocol used in RealNetworks G2 and Apple QuickTime 4 streams. RTSP is an open protocol.

See also **streaming media**.

Real-Time Transport Control Protocol (RTCP)

A feedback protocol that provides quality of service information to the streaming server. The RTCP feedback mechanism periodically describes the state of the network so the streaming server and client can negotiate the optimum bit rate for current network conditions. By default, RTCP uses UDP for transport.

RSA (Rivest, Shamir, and Adleman)

Public key encryption algorithm that uses 2048-bit keys. RSA is widely used in public key cryptography to create matched public and private key pairs for data encryption. Data encrypted with the public key can be decrypted only with the private key, and data encrypted with the private key can be decrypted only with the public key.

RTCP

See **Real-Time Transport Control Protocol**.

RTSP

See **Real Time Streaming Protocol**.

SCSI adapter

Expansion card that supports the SCSI disk drives.

SCSI ID

The number of a disk drive on the SCSI chain (0 to 6).

SCSI address

The full address of a disk, consisting of the disk's SCSI adapter number and SCSI ID (for example, 9a.1).

SecureAdmin

SecureAdmin is a NetCache security feature that enables you to administer NetCache in a nontrusted environment using an encrypted exchange of information between NetCache and a client. SecureAdmin supports the Secure Sockets Layer (SSL), and the Secure Shell (SSH) protocol options. SSL can be enabled to secure HTTP transmissions, or SSH can be enabled to replace Telnet and RSH clients and provide confidential NetCache administration.

Secure Shell (SSH) Protocol that is a standard method for replacing Telnet and RSH sessions to secure encrypted communication over the Internet.

Secure Sockets Layer (SSL) Protocol that is a standard method for secure, encrypted communication over the Internet. By encrypting the data on the sending end before it is sent out over the Internet, users can be reasonably assured that unauthorized parties intercepting their information cannot read it. Secure forms of the Network News Transport Protocol (NNTP) and Secure HTTP (HTTPS) can be proxied by NetCache.

serial adapter An expansion card for attaching a terminal as the console on the NetCache appliance.

serial console An ASCII or ANSI terminal attached to a NetCache appliance's serial port. Used to monitor and manage NetCache appliance operations.

SNMP agent NetCache process that gathers status and diagnostic information and forwards it to network management stations.

SNMP community Name that is used as a password by the SNMP manager to communicate with the NetCache SNMP agent.

SNMP trap User-defined process that monitors a specific occurrence on the NetCache appliance, for example, a trap that monitors the disks on a NetCache appliance.

splitting The process of delivering a unique stream to multiple clients simultaneously. Splitting reduces the number of requests sent across the network to the streaming server.

See also **stream** and **streaming media**.

stream

A streaming media file being transmitted over a network. Streams are of two types, live and on-demand.

See also **live stream**, **on-demand stream**, **streaming media**, and **unique stream**.

streaming accelerator

A NetCache appliance that caches content from one or more streaming servers that you identify. A streaming accelerator provides that content to clients that request it. To the outside world, the streaming accelerator is the streaming server. In contrast, when NetCache runs as a streaming media cache, it acts as an agent for the media player.

streaming media

A term used to describe media files that begin playing while they are being transmitted over the network to the media player on the client computer. In contrast, conventional Web files must be downloaded entirely before the user can view them. Commonly requested types of streaming media are video and audio. Streaming media also includes interactive media, cartoon-like animations, panoramic data, and more.

streaming media cache

A specially configured NetCache appliance that intercepts client requests for streaming media. When a streaming media cache is deployed between clients and a streaming media server, streaming requests that would otherwise have been sent directly to the streaming server are sent to the cache. NetCache satisfies client requests by delivering cached or split streaming media content directly to users.

See also **splitting**, **stream**, **streaming media**.

streaming media presentation

A general term used to describe the delivery of live or on-demand streaming media. A streaming media presentation can consist of multiple *unique streams*.

See also **stream**.

SVRAM

Semi-volatile random access memory. SVRAM uses a part of main memory as if it is NVRAM.

See also **NVRAM**.

Time To Live (TTL)

A Web object's Time To Live (TTL) is the time limit on how long a copy of that Web object remains in the cache before NetCache verifies the object with the originating Web server. An object's TTL is often determined by an explicit expiration time included in the MIME header of the object itself. If the object does not include an expiration time, NetCache calculates a default TTL for the object.

thinning

In streaming media, the streaming server's process of dropping a consistent number of video or audio frames to try to make the data being delivered to the client stream more efficiently during playback.

See also **streaming media**.

unique stream

A stream is *unique* if the connection speed, media type, or thinning parameters are different from another stream that is part of the same streaming media presentation.

See also **stream** and **streaming media**.

User Datagram Protocol (UDP)

A means of transferring information over a network, such as the Internet. It forms the backbone of the InterCache Protocol (ICP) used by NetCache to communicate with other caches in a hierarchy.

WAFL

Write Anywhere File Layout. The file system designed for NetApp appliances to optimize write performance.

WCCP 2.0-based router

A Cisco router running WCCP 2.0 software.

Web accelerator

A NetCache appliance that caches content from one or more *Web servers* that you identify. A Web accelerator provides that content to clients that request it. To the outside world, the Web accelerator *is* the Web server. In contrast, when NetCache runs as a Web cache, it acts as an agent for the browser.

Web cache

An intermediary server that accepts requests from clients and forwards them to a Web server or services the request from its own cache. A Web cache acts as an agent for the client browser.

Index

A

access controls, hierarchies and 201
access to the appliance
  access control lists 1
  adding administrative accounts 1
  administering 1
ACLs
  actions 7
  described 7
  expressions 11
  operators 11
  syntax 7
  variables 8
adding disks 86
admin account, default 2
Append Domain option
  DNS, appending the domain name 56
Appliance Manager
  cannot access
    ifconfig command 309
    possible reasons for 299
  loss of connectivity to 23
Appliance Manager, accessing 2
arp command 305
authentication
  HTTP transparent proxying 176
  in hierarchies 200
  protocol tunneling feature and 45
authentication, defined 3
automatic configuration file
  strategy for multiple cache management 239
Automatic Configuration page
  supporting multiple cache management 262
Automatic Configuration Update Interval option 263
automatic e-mail support to NetApp. *See* Autosupport
automatic proxy configuration file, troubleshooting 321
automatic rebooting of appliance 290
Autosupport
  configuration planning 98
  defined 100
  events that trigger 101
  protection of private data 100
  reasons for using 100
  types of messages generated 100

B

backup files, configuration
  reverting to 23
balancing traffic
  server to appliance 38
  TCP traffic 38
bandwidth allocation
  description of 218
  displaying rules 220, 222
  rules
    AND logic of filtering options 222
    precedence and order of listing 223
    viewing 220, 222
binding traffic to outbound interfaces 36
boot diskette
  creating 89, 292, 293
  using for rebooting 290
booting
  from system boot diskette 292, 293, 301
  into maintenance mode 315
broadcast address, setting using ifconfig 309

C

caching DNS data
  CNAME record 55
  lookups 54
    how long cached 55
  what is cached 55
  what is proxied 55
cloning a NetCache configuration 274
CMS log
  log formats available 118
  name of 115
  type of data logged 111
CNAME record, cached on appliance 55

cold swap drives 317
collisions, when to be concerned 305
command line, using 296
commands
    arp 305
    config 297
    config -rl 23
    for networking problems 305
    halt 329
    ifconfig 299, 305, 309
        bringing up network interface 23
    netstat 305
    routed status 306
community (SNMP), defined 93
compact flash PC-card 294, 317
config command, using 297
configuration backup files, damaged 301
configuration cloning
    cloning from one appliance to another 274
    strategy for multiple cache management 240
configuration errors, URL requests not serviced 320
configuration files
    default.cfg 241
    default.cfg and local.cfg 241
    global 242
    local.cfg 241
CONNECT requests, defined 45
console
    accessing 296
    cannot enter commands through 282
    obtaining system status 296
    password
        changing 296
        for console and Telnet 296
    session 296
ContentDirector log
    log formats available 118
    name of 115
    type of data logged 111
core files
    description of 330
    naming 330
    number saved 330
    sending to Network Appliance 330
cp command 271
crash of appliance
    information provided about 330
    troubleshooting 330
creating a boot diskette 89, 292, 293
custom log formats
    how you can use them 117
    types available, by log type 117
customizable error messages
    error codes in 130
    error tag syntax 133
    planning for 128
    tags you can add 132
customizing logs
    Extended Log File Format and 117
    log formats for 117
        ordering log headers 117

D

data disk
    definition of 71
    See also disks
data rebuild, on the hot spare 318
database, local user 3
DataFabric Manager
    appliance as agent
        log for 111, 115
    defined 230
DDNS servers, IP address assignment with 67
default route in routing table 30
degraded mode 79
DHCP
    how IP addresses are assigned 67
    release of IP addresses 67
DHCP server and appliance interaction
    at appliance startup 52
    data the appliance obtains from the server 52
    dynamic assignment of IP addresses 67
    IP address expiration in the DNS cache 67
Disabled Outgoing Interfaces option 40
    purpose 36
    restrictions for using 40
    versus Load Balancing Interfaces option 37
    when to use 40

disk failures
automatic recovery from 71
automatic shutdown 316, 318
degraded mode 80
effects of 79
hot spare exists 80, 318
messages about 81, 316, 318
multiple disks 81, 316
parity disks 81
removing a disk 88
single disk 316
two disks 316
using a hot spare disk 71
when to replace a disk 80
disks
adding 86
internal disk tray 86
multiple disks or a new disk shelf 87
reasons for adding 86
when to add 86
addressing, use of 74
cold swapping 317
degraded mode 80
hot spare 71
hot swapping, description of 72
internal disk trays 72
managing 71
parity disks 71
problems 316, 318
recovering from 315
reinitializing 89
removing 88
internal disk trays 86
multiple disks 87
reasons for removing 86
when to remove 86
replacing 88
SCSI ID number 74
sizes 77
statistics, understanding 84
types in RAID 71
types on appliance 71
usable space 76
See also disk failures
DNS
appliance support for 49
internal resolvers, evaluating support needed 61
port for 141
querying nameservers, problems 54
See also DNS features on the appliance
DNS configuration, checking 307
DNS features on the appliance
appliance as a nameserver 53
basic configuration for 52
DNS cache
forcing expiration of IP addresses in 67
how records are cached 67
DNS iterative resolution
described 64
how queries are resolved 64
options for 65
when query rules are required 66
when to enable 64
with GRM 64
DNS proxy caching
nontransparent, requirements 55
setting up 54
troubleshooting 178
DNS search paths
identifying 59
use of 59
domain tree search 56
problems with 57
Domain Tree Search option 56
example set to Off 58
example set to On 57
full-service resolver 64
name resolution 52
Split DNS feature, described 61
DNS log
name of 115
type of data logged 111
DNS lookups 56
avoiding extra 56, 57
caching on appliance 55
for remote servers 50, 60
what the appliance caches 55
DNS nameservers
appliance as 53

bypassing remote 60
failover of 52
requirement to bypass 60
domain name
appliance 52
not fully qualified 56
double disk failures 81, 316
dynamic forwarding
defined 170
examples 140

E

error codes in customizable error messages 130
error messages
customizable, planning for 128
displayed by netstat 305
hiding with transparent proxying 175
stealth mode 135, 175
supressing appliance messages 135
transparent proxying 135
EtherChannel, in multi-mode VIFs 21
Ethernet
interface names and numbers 15
setting the media type 310
supported interfaces for 15
event alert (Autosupport)
described 101
events that trigger 101
event messages (Autosupport)
content of 104
described 101
events that trigger 101
Extended Log File Format 117

F

failover
DNS nameservers 52
hierarchies for 198
with an L4 switch 146
with an L7 switch 146
See also NetCache takeover
failure, disks 71
mutiple disks 81, 316
parity disks 81
single disk 316
when to replace 80
FDDI
interface names and numbers 15
setting the MTU 310
supported interfaces for 15
Feeder server definition 335
file system
inconsistent 326
installing a new one 326
firewalls
appliance inside nontransparent 32
appliance inside transparent 32
appliance outside of 32
hierarchies and 194
forward proxy, request distribution with
switch 145
FTP transfer access log
log formats available 118
name of 115
type of data logged 111
FTP, port number for 141, 146

G

Gigabit Ethernet, supported interfaces for 15
global configuration file
appending local settings 267
backing up and restoring 265
using the Appliance Manager 265
using the CLI 266
configuring NetCache to use 249, 250
contents of 244
generating or creating 242, 244
propagation 242
pushing to target NetCache appliances 270
specifying refresh times through the Appliance
Manager 263
GRM server access log
log formats available 118
name of 115
type of data logged 111
GRM server details log
log formats available 118
name of 115

type of data logged 111
GRM, DNS iterative resolver with 64
grouping administrators 3
groups 3

H

halt command
use with VRAM battery failures 329
using to avoid inconsistent NVRAM 329
hierarchies
access control with 201
authentication for 200
child 200
clusters 195, 198
common configurations 195
custom rules 204
defined 193
disabling default forwarding 204
failover 198, 206
firewalls as members 194
ICP for 196
information to gather 192
load balancing requests 198
member roles 194
methods for distributing requests 202
neighbors 195
planning for 191, 192, 200
purpose of 193
troubleshooting 214
with single firewall 195
host name, appliance 52
hot spare disk
adding 87
and disk failures 80, 318
checking for 87
definition of 71
See also disks 71
hot swapping a disk 72
HTTP port numbers with transparency 141
HTTP Proxy Ports option
setting for transparent proxying 147
HTTP 1.1 error codes
customizing messages 129
HTTP 1.1 error codes, customizing messages 130
HTTP-based traffic versus protocol tunneling 44
HTTPS, tunneling traffic 44

I

ICAP log
formats available 118
name of 115
type of data logged 111
ICMP redirect messages
appliance learning routes through 30
defined 30
ICP
defined 196
drawbacks 197
used with neighbors 196
IERRS (input errors) displayed by netstat 305
ifconfig command 305
bringing up network interface 23
checking interface configuration 299, 301
syntax 309
use in troubleshooting 299, 309
interfaces. *See* network interfaces
internal disk tray
adding and removing disks 86
supported platforms 72
Internet Cache Protocol. *See* ICP 196
IP addresses
using ifconfig 309
with DHCP servers 67
IP forwarding
data needed to configure 168
defined 170
examples 140
IP spoofing
benefits 172
data needed to configure 169
defined 172
examples 140
restrictions 172
symmetric routing and 173
IP takeover. *See* NetCache takeover
IP-GRE encapsulation 152
IRDP, described 31
iterative queries with full-service resolver 64

L

Listen Addresses option
- compared with access controls 34
- determining whether to use 33
- examples 34
- purpose 33
- versus ACLs 34

load balancing
- in hierarchies 198
- over appliance network interfaces 159

Load Balancing Interfaces option
- balancing server to appliance traffic 38
- purpose 36, 38
- restrictions 38
- topology example 38
- versus Disabled Outgoing Interfaces option 37

local.cfg
- configuration settings precedence 241
- description of 241
- the overwriting property of local.cfg settings 267

log files
- about custom headers 117
- configuration planning for 108
- custom log formats 117
- default settings for 113
- disabling 113
- enabling 113
- Extended Log File Format and 117
- file names for 115
- formats for 117
- FTP transfer access log 111
- management techniques 120, 121
  - log pushing 121
  - log pushing requirements 123
  - log rotation 121, 122
  - parameters for 121
  - switching between 122
- maximum file size, controlling 121
- Messages log, description of 112
- NNTP access log, description of 112
- NNTP trace log, looking for traffic loops in 147
- predefined formats 117
- pushing to an FTP or Web server 123
- schedules, controlling 121
- Streaming access log, description of 112
- Streaming details log, description of 112
- types available 111
- use with troubleshooting 320
- Web access log, description of 113

log headers
- Extended Log File Format 117
- log formats 117
- where to find details about 119

log pushing
- described 121, 123
- file renaming during 124
- reasons for using 123
- requirements 123
- server requirements for 123
- unsuccessful push 123

log rotation
- changing to log pushing 122
- described 121
- number of logs kept 122
- when logs rotate 122

logging 4

logging into the appliance 296

logging out from the appliance 296

long-haul networks, TCP large windows with 41

L4 or L7 switch
- deployment requirements 143
- failover with 146
- location in relation to clients 144
- location in relation to NetCache 144
- location recommendations 144
- requirements for transparent proxying 143
- setting up transparent proxying with 147
- troubleshooting transparent proxying 183

L7 switch, request distribution by URL 145

M

MAC address rewriting 152

media type
- description of 310
- for an Ethernet interface 310

messages
- error

customizing 127
panic 303
supressing appliance messages 135
generated by Autosupport 100
Messages log
description of 111, 112
disk failure reported 316, 318
name of 115
pushing to FTP or Web server 123
when it is rotated 121
MIB
NetCache custom
described 94
groups and objects in 94
what is included 96
where to obtain 94
MTU, setting 310
multi-mode virtual interface, described 21
multiple cache management
backing up and restoring global configuration file 265
cloning NetCache configurations 274
configuration files 241
configuring NetCache to use a global configuration file 249
global configuration 242
global configuration file contents 244
global configuration files 242
scenario applying uniform set of ACL rules to caches 260
scheduling NetCache to use global configuration files 250
use of pushed global configuration files 270
use of the Appliance Manager 262

N

name resolution on appliance, DNS 52
nameservers. *See* DNS nameservers
naming
core files 330
log files 115
network interfaces 15
NetCache appliance
cannot boot 292, 301
console 296
login 296
logout 296
password forgotten 288
down 290
not accessible 301
not servicing URL requests 299, 320
RAID level support 71
rebooting, automatic 290
requesting URLs through 323
software, where to obtain 326
troubleshooting 280
configuration to check 320
determining if the software is running 281
not servicing URL requests 281
NetCache console. *See* console
NetCache takeover 187
description of 187
obtaining status 190
pairs 187
planning for 188
netmasks, configuring using ifconfig 309
netstat command
excessive errors on interfaces 305
IERRS (input errors) 305
Network Appliance Technical Support
contacting 332
network cards. *See* network interfaces
network connection not attached 285
network interfaces
accepting client requests through
default 33
limiting 33
balancing server-to-NetCache traffic over 38
binding outbound traffic to 36
bringing down 311
bringing up 311
configuring 15, 309
down, reconfiguring 309
errors on 305
if all interfaces are down 23
planning for configuration 14
reconfiguring with ifconfig command 309
showing current configuration

of all network interfaces 311
of one network interface 311
supported interfaces 15
troubleshooting 23
using ifconfig to configure 309
virtual
described 17, 18
multi-mode 20, 21
prerequisites 22
types 20
network mask
configuring using ifconfig 309
See also netmasks
networks
connections, checking 305
problems with 305
statistics 305
news server components 338
NNTP access log 112
log formats available 118
name of 115
NNTP port, default 141
NNTP trace log, looking for traffic loops in 147
noncacheable objects, L7 switch with 145
nontransparent firewalls, appliance inside 32
Non-Volatile RAM (NVRAM). *See* NVRAM
NVRAM
failures in 329
inconsistent NVRAM contents 329
problems, troubleshooting 329
replacing batteries 329

P

packet trace files, how created 312
panic message 303
parity disks
description of 71
See also disks
passwd command
changing console password 296
password, console 296
forgotten password 288
resetting 288
physical interfaces
naming conventions for 15
supported 15
policy-based routers, directing traffic to the appliance 149
ports
DNS port number 141, 146
FTP port number 141, 146
HTTP port number 141, 146
MMS port number 141, 146
NNTP port number 141, 146
RTCP port number 141
RTSP port number 141, 146
protocol tunneling feature
advantages 44
configuration overview
nontransparent deployment 46
transparent deployment 46
how it works 45
restrictions 45
traffic used for 44
when not applicable 44
proxy-cache server, definition of 343
proxy.pac file, troubleshooting 321
pushed configuration, for multiple cache management 239
pushing core files 330
pushing logs
described 121

Q

queries, DNS 54
QuickTime
RTCP port required 141

R

RADIUS server, definition of 338
RAID
disk status, displaying 74
disks 71
file system, description of 71
level used by NetCache appliance 71
Reader server description 338
rebooting NetCache appliance
automatic e-mail to NetApp 330

from diskette 292
instructions 290
reinitializing disks 89
removing a disk 88
request distribution
hierarchies 202
switches
hashing function 145
methods available 145
on URL 145
request forwarding 170
hierarchies for 202
process 171
restrictions 171
request resolution, appliance as a DNS proxy cache 54
requesting URLs
from Web servers 322
through an appliance 323
resetting passwords 288
resolvers
appliance as full service resolver 64
appliance supporting internal DNS resolution 61
reverse proxy, request distribution with 145
Route Discovery, described 31
routed status command 306
routing
default route in routing table 30
how the appliance routes packets 30
ICMP redirect messages 30
Internet Router Discovery Protocol 31
routing tables on the appliance 30
RTSP Ports option
setting for transparent proxying 141
rules, types of 6

S

SCSI ID, identifying disks 74
secure traffic, tunneling of 44
security, appliance console password 296
server-to-appliance traffic, balancing over interfaces 38
service groups. *See* WCCP service groups
shutdown
unexpected 290
single-mode virtual interface, described 20
SNEWS, tunneling traffic 44
SNMP
agent and groups supported 92
appliance implementation, description of 92
implementation, description of 92
MIB specifications implemented 92
NetCache custom MIB 94
traps
defined 92
obtaining an OID 96
types of 93
user-defined, planning for 96
Split DNS
described 61
options for 62
restrictions for 61
SSL, tunneling traffic 44
status, determining for system 296
stealth mode
description of 135
with transparent proxying 135
streaming accelerator
described 341
Streaming access log
description of 112
log formats available 118
name of 115
Streaming details log
description of 112
log formats available 118
name of 115
streaming media
load balancing over appliance interfaces 159
port settings for 141
troubleshooting 179
support (technical), how to contact 332
switch. *See* L4 switch or L7 switch
syslog daemon 112
syslog messages
defined 109, 112
sending to remote server 109, 112
sysstat command 296

obtaining system status 296
use in troubleshooting 321
system boot diskette 290
creating 292
maintenance mode 315
where images are available 292
system crash
information provided about 330
troubleshooting 330
system panic (crash) 303
system password 296
system status at console 296

T

takeover. *See* NetCache takeover
TCP large windows
advantage 41
determining hosts or subnets to use with 41
determining window size 42
common connection type 42
when to use 41
Technical Support, Network Appliance, contacting 332
telnet command
accessing the appliance console with 281
accessing the NetCache console with 323
accessing Web servers with 322
connection password 296
logging out from the appliance 296
traceroute tool 179
traffic loops, avoiding with transparent proxying 147
transparent firewalls, appliance inside 32
transparent proxying 137, 140
authentication with 176
avoiding traffic loops 147
bypassing 170
client-side and server-side traffic 137
dynamic forwarding 140
error messages, hiding 135
failover
L4 or L7 switch 146
failover with L4 or L7 switch 146
hiding error messages with 175
information to gather 139
IP forwarding
data needed to configure 168
examples 140
restrictions 171
IP spoofing
benefits 172
data needed to configure 169
examples 140
restrictions 172
load balancing
over appliance network interfaces 159
L4 switch with 143, 147
L7 switch with 143, 147
modifying 168
optional features 168
planning summary 139
port settings for 141
streaming media 141
protocols supported 146
request forwarding for 170
stealth mode, purpose 135
streaming media port settings 141
URL forwarding 168
URL forwarding restrictions 171
WCCP and 148, 159
trap hosts, defined 93
traps
description of 92
obtaining an OID 96
SNMP 96
types of 93
user-defined
described 96
planning for 96
troubleshooting 182, 323
appliance not accessible 301
automatic proxy configuration file 321
booting, from system boot diskette 290, 292, 301
cannot access a specific URL 322
cannot access Appliance Manager 299
cannot boot appliance 292, 293, 301
checking connections 305
configuration to check 320

core files, use with 330
data in log files 320
determining if appliance is the problem 280
disk problems 316, 318
automatic shutdown 316, 318
failures 71
DNS configuration 307
down appliance 290
rebooting 290
inconsistent file system 326
interfaces, showing current configuration
of all network interfaces 311
of one network interface 311
network connection not attached 285
network interfaces 23
network problems 305
NVRAM problems 329
obtaining help 332
packet trace files 312
password, forgotten console password 288
removing a disk 88
requesting URLs
from Web servers 322
through a NetCache appliance 323
reverting to configuration backup file 23
software problems 303
sysstat command 321
system crash (appliance) 330
system panic message 303
transparent proxying
DNS caching 178
streaming media 179
using WCCP statistics 182
WCCP router with 178
WCCP settings in NetCache 181
URL requests not serviced 281, 299, 320
using Autosupport for problem alerts 100
using the config command 297
trunking
advantages of 18
description of 18
multi-mode 21
tunneling
protocol, traffic used for 44
secure traffic 44

U

URL forwarding
data needed to configure 168
examples 140
URLs
cannot access specific URL 322
requesting from Web servers 322
requesting through an appliance 323
requests not serviced 281, 299, 320

V

virtual interfaces
advantages 18
described 17
multi-mode 21
single-mode 20
supported interfaces 15
trunking described 18
types 20

W

WCCP
cache weighting 158
client-side and server-side traffic 137
definition of 149
IOS images running with 150
IP spoofing for 173
load balancing 159
multicast requirements 154
password 139, 160
quick fill templates for 162
service groups
configuring for multiple protocols 165
configuring for streaming media 164
definition of 162
guidelines 162
limitations 163
password 139
planning 160
port restrictions 165
restricting access to 160
restrictions for traffic type 163
streaming media and 164

software requirements 150
traffic distribution
accelerator case 156
forward proxy case 156
hashing 156
methods 156, 159
traffic redirection
methods 152
requirements for request forwarding 153
transmission methods
multicast 154
multicast requirements 154
unicast 154
transparent proxying
requirements 149
troubleshooting 178
version NetCache supports 149
WCCP routers
appliance interface load balancing with 159
connection to the appliance 150
location in relation to clients 151
redirection method 152
WCCP statistics, viewing 182
Web access log
description of 113
log formats available 118
name of 115
pushing to FTP or Web server 123
Web Cache Control Protocol. *See* WCCP
Web server acceleration log
log formats available 118
name of 115
type of data logged 113
Web server, requesting URLs from 322
weekly reports (Autosupport)
content of 104
described 101
windows, large TCP 41