

ContentDirector™ 2.0

Installation Guide

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

Part number 210-00072
November 2001

Copyright and trademark information

Copyright information

Copyright © 1994–2001 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. WAFL is a registered trademark of Network Appliance, Inc. in the European Union and a trademark of Network Appliance, Inc. in the United States 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. ApplianceWatch, BareMetal, ContentDirector, ContentReporter, DataFabric, SecureAdmin, Serving Data by Design, Smart SAN, SnapManager, SnapMirror, SnapRestore, 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	vii
Chapter 1	Overview of ContentDirector	1
	The ContentDirector application	2
	ContentDirector architecture	3
	About group leaders and group members	5
Chapter 2	Planning Your ContentDirector Deployment	7
	Basic planning considerations	8
	Content considerations	9
	Topology considerations	10
	Deploying ContentDirector with firewalls	13
	DNS for Streaming media	15
	Sample configurations	16
	One-level unicast	17
	Two-level unicast	18
	Unicast to multicast	20
	Multicast over satellite	21
Chapter 3	Before You Start	23
	Compatibility with previous versions	24
	System requirements	25
	Storage requirements	27
	Network topology and operation	28
	Transport port conflicts	29
Chapter 4	Installing and Uninstalling on Microsoft Windows	31
	About installing on Windows.	32
	Running the installation wizard.	33
	Uninstalling ContentDirector on Microsoft Windows	35

Chapter 5	Installing and Uninstalling on a Solaris System	37
	Installing the core application on a Solaris server	38
	Uninstalling the the core application on a Solaris server.	41
 Chapter 6	 Configuring the ContentDirector Agent Software	 43
	Planning for ContentDirector agent configuration	44
	Overview of ContentDirector agent configuration	47
	Configuring NetCache for the ContentDirector agent software	49
	Configuring advanced ContentDirector settings	51
	Configuring additional ContentDirector features.	57
 Chapter 7	 Testing Your ContentDirector Installation	 59
	Before you start.	60
	Testing distribution	61
	 Glossary	 65
	 Index	 71

Preface

Introduction

This guide describes how to configure, manage, and operate Network Appliance[™] ContentDirector 2.0.

Audience

This guide is for system administrators and others who will configure or use ContentDirector. It assumes you are familiar with your operating system, your network, and the basic concepts of how data moves over a network. If you plan to distribute streaming media content, you also need a basic understanding of streaming media protocols and service. This guide does not cover basic system or network administration topics, such as IP addressing, routing, and network topology; it emphasizes the characteristics of the ContentDirector software.

Terminology and conventions

The term “ContentDirector” refers to a complete configuration including all components of the software.

This guide uses the term “type” to mean pressing one or more keys on the keyboard. It uses the term “enter” to mean pressing one or more keys, and then pressing the Enter key.

Keyboard conventions

When describing key combinations, this guide uses the hyphen (-) to separate individual keys. For example, “Ctrl-D” means pressing the “Control” and “D” keys simultaneously. Also, this guide uses the term “Enter” to refer to the key that generates a carriage return, although the key is named “Return” on some keyboards.

Typographic conventions

The following table describes typographic conventions used in this guide.

Convention	Type of information
<i>Italic type</i>	Words or characters that require special attention. File names. Placeholders, for information you must supply. Book titles in cross-references.
Monospaced font	Command names. Information displayed on the system console or other computer monitors. The contents of files.
Bold monospaced font	Words or characters you type. What you type is always shown in lowercase letters, unless you must type it in uppercase letters.

Special messages

This guide contains special messages that are described as follows:

Note

A note contains important information that helps you install or operate the system efficiently.

Caution

A caution contains instructions that you must follow to avoid loss of data.

About this chapter This chapter contains a description of ContentDirector, its architecture, and its function.

Topics in this chapter This chapter includes the following topics:

- ◆ “[The ContentDirector application](#)” on page 2
- ◆ “[ContentDirector architecture](#)” on page 3
- ◆ “[About group leaders and group members](#)” on page 5

The ContentDirector application

About ContentDirector

ContentDirector is a distributed application that moves content over a network from centralized filers or servers to NetCache appliance destinations. The network can consist of a local area network, intranet, or internet with conventional wire and wireless links, including satellite.

Supported content types

ContentDirector distributes content for the following protocols:

Protocol	Name
http://	HTML
mms://	Microsoft Media Streaming
rtsp://	Real-Time Streaming Protocol

Note

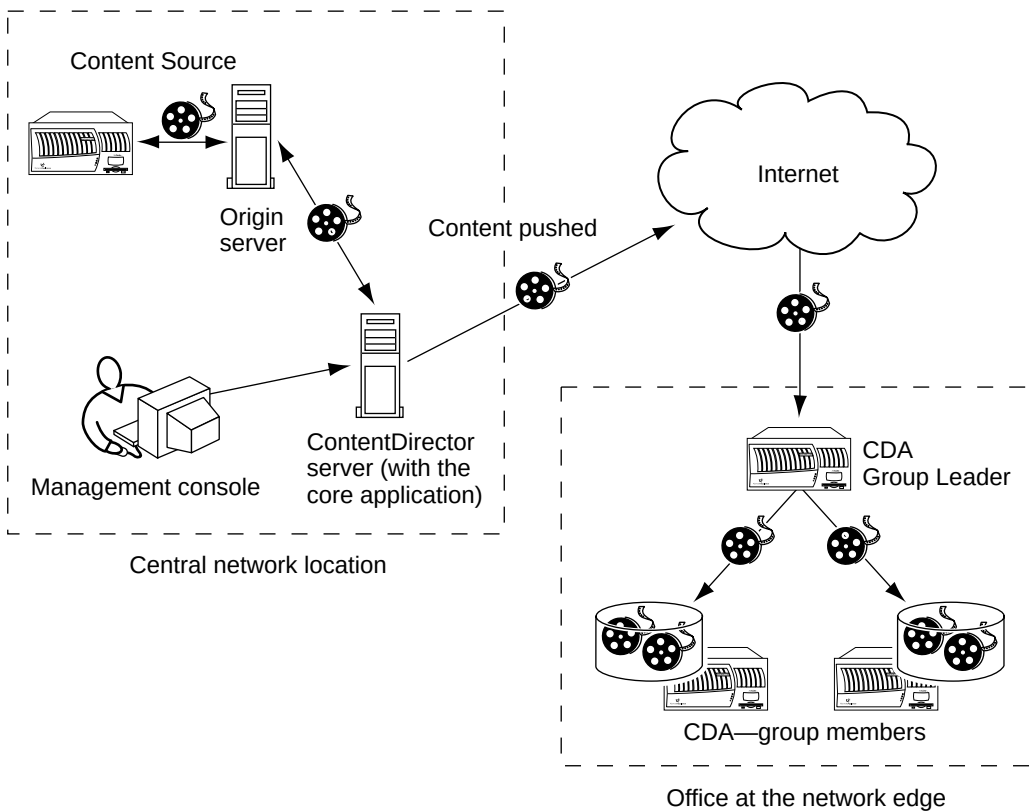
Server licenses are required to serve content under the mms:// or rtsp:// protocols. These licenses are activated on the Setup tab > System > Licenses page of the NetCache interface.

ContentDirector architecture

ContentDirector components

ContentDirector contains the following components:

- ◆ Core application, consisting of the content control manager that originates and manages content distribution tasks, scheduler, logger, and an integrated Sybase database
- ◆ ContentDirector Agents (CDAs):
 - ❖ Group members (GMs) that receive content and serve it to clients
 - ❖ Group leaders (GLs) that manage communications between the core application and group members
- ◆ Optional administrator applet to enable remote administration of the core application



Device types for installed components

Each component installs on specific device types.

Component	Device type
Core application	Windows or Solaris server
CDA	NetCache appliance Note ————— You do not need to install ContentDirector on NetCache. It is part of the NetCache kernel. See “ Configuring the ContentDirector Agent Software ” on page 43 for details. —————
Applet	Remote Java-enabled client

Master keys and security

ContentDirector components must be able to identify and authorize each other to maintain security. Each installation of the ContentDirector core application has a master key for this purpose. The core application and the CDA reference the master key to verify identity.

A default master key is created when the core application is installed. For higher security, you can create a unique master key for your ContentDirector network. See the ContentDirector Administration Guide for detailed instructions.

About group leaders and group members

Definition of group leader and group member

CDAs that receive content directly from the ContentDirector core application are called *group leaders*. Group leaders distribute content to other CDAs called *group members*. Typically, group members are located at the periphery of your network and are the ultimate recipients of the pushed content.

Note

Group leaders can be configured as assigned group leaders or candidate group leaders. See “[Properties of group leaders](#)” on page 6 for information about group leader assignments.

How group leader and group member assignments are used to distribute content

When you configure a CDA, you must specify the role it is to assume in the ContentDirector deployment. By configuring a CDA as a group leader or group member, you define the ContentDirector transport hierarchy (also called *transport groups*).

CDAs configured as group leaders communicate with their respective group members to determine the operational state of all devices in the group. After compiling this status information, the group leader sends it to the core application so that each device can be represented in the ContentDirector management console for grouping and scheduling purposes.

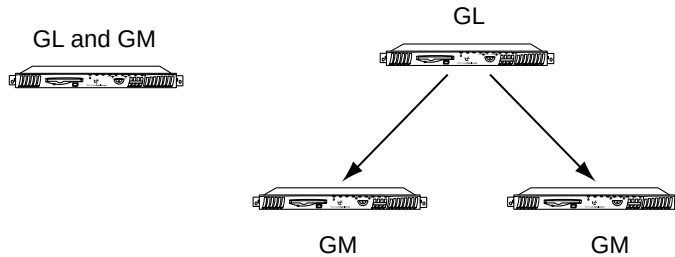
Administrators then use the ContentDirector management console to assign group leaders and group members to specific destination groups, which define the logical subset of CDAs that will receive the specified content. A destination group can consist of one or more transport groups. For example, a single content group created to distribute content to three remote branch offices could use multiple transport groups to distribute the content.

Group leader and group member configuration options

There are two configuration options for group leaders and group members:

- ◆ Group leader and group member on the same device
- ◆ Group leader and group member on separate devices

The illustration below shows both options.



Properties of group leaders

There are two types of group leaders: assigned and candidate.

- ◆ Assigned group leaders automatically become the group leader for the transport group. (A transport group is a set of CDAs on one or more subnets that can join the same multicast group.) Create only one assigned group leader per segment to avoid conflicting group leader claims.
- ◆ Candidate group leaders are on failover standby in case the assigned group leader cannot fulfil its function. If the assigned group leader fails, the candidate group leaders negotiate which machine assumes the group leader role through an election process.

For maximum reliability, designate a minimum of two group leaders whenever possible. The recommended configuration is one assigned group leader and one candidate group leader.

It is not necessary to have an assigned group leader in each transport group. If there is no assigned leader, the leader is elected from the pool of candidates. It takes less time for the core application to recognize the transport group at startup if you assign a group leader, rather than requiring elections among candidates.

About this chapter

This chapter contains basic information and generic sample configurations to help you plan your ContentDirector deployment.

Note

Deployment details vary from network to network. Please consult your Network Appliance Systems or Support Engineer for more customized deployment suggestions.

Topics in this chapter

This chapter contains the following topics:

- ◆ “[Basic planning considerations](#)” on page 8
- ◆ “[Sample configurations](#)” on page 17

Basic planning considerations

About planning considerations

There are two basic categories of considerations when planning your ContentDirector deployment:

- ◆ Content
- ◆ Topology

Your network needs to suit your content delivery needs, so get to know your content first before choosing hardware and planning topology.

For detailed information

The following sections discuss ContentDirector deployment planning considerations:

- ◆ [“Content considerations”](#) on page 9
- ◆ [“Topology considerations”](#) on page 10
- ◆ [“Deploying ContentDirector with firewalls”](#) on page 13
- ◆ [“DNS for Streaming media”](#) on page 15

Content considerations

Know your content

Before planning your content delivery network, you need to gather the following information about the content you plan to distribute:

- ◆ Frequency of jobs
- ◆ Number of destinations per job
- ◆ Size of jobs
- ◆ Job composition (HTTP, RTSP, MMS)

Interaction of content with hardware choices and topology

The factors listed above affect your topology and hardware choices:

- ◆ The frequency of jobs and number of destinations per job determine the load placed on the group leader. The load on the group leader influences three decisions:
 - ❖ On unicast networks, the optimal number of transport groups
 - ❖ Your choice of appliance for the group leader
 - ❖ Whether to enable multicasting to boost performance
- ◆ The size of jobs allows you to estimate the storage capacity required for group members.

Topology considerations

Topology factors

One goal of the planning process is to map the topology of the ContentDirector components:

- ◆ Location of the core application machine
- ◆ Location and number of group leaders and group members

Location of core application

Content sources, such as filers or conventional servers, provide the content that ContentDirector distributes to destinations. In general, locate the core application server as close as possible to these content sources for optimal performance. This means that the core application probably should reside near the center of your network.

Planning the location of group leaders

Consider the following factors when planning the location of group leaders:

- ◆ Multicast or unicast delivery channels
- ◆ Size and performance of the NetCache appliance
- ◆ Location of firewalls
- ◆ Topological location of the CDAs
- ◆ Delivery speeds between group leaders and the core application

Multicast versus unicast: ContentDirector can use either unicast or multicast transmission between transport group leaders and members, depending on whether your network is multicast-enabled. Generally, group leaders should be placed in a location where they can use a multicast channel to send content to group members. Multicasting increases performance because group leaders can distribute a single copy of the data to multiple group members simultaneously.

The default transmission mode is unicast. ContentDirector automatically switches to multicast if it detects a multicast-enabled network.

Size and performance: Consider the size and performance of the NetCache appliances. If you want a NetCache appliance to be a group leader, does it have the capacity to handle the amount of content that might need to be pushed to group members? In a unicast network for example, a C6100 can distribute content to more group members than a C1100.

Firewalls: Consider the location of firewalls. If firewalls separate the group leader from group members or the core application, additional configuration might be required to facilitate content distribution. For example, firewalls might have port restrictions that block or limit ContentDirector traffic. See “[Deploying ContentDirector with firewalls](#)” on page 13 for more information.

Topological location and delivery speeds: Typically, group leaders should be located as close to group members as possible to minimize bandwidth requirements. However, consider the topological location of the group leader in relation to the core application and other CDAs. Will the network link provide enough bandwidth for the group leader to efficiently retrieve content from the core application? Can the group leader deliver the content to group members using the least possible bandwidth?

Determining how many group leaders to assign

Consider the following factors when determining how many CDAs to assign as group leader:

- ◆ Multicast or unicast delivery channels
- ◆ Estimated workload
- ◆ Scheduling requirements
- ◆ Reliability

Multicast versus unicast: Typically, a multicast-enabled network can have more group members per group leader than a unicast network. In multicast networks, the group leader can send a single copy of the content to all group members. In contrast, in a unicast network, the group leader must deliver a separate copy of the content to each group member.

Multicast also reduces maintenance overhead. It enables ContentDirector to auto-discover group members, and allows you to configure multiple group leader candidates on a transport group.

Estimated workload and scheduling requirements: If you plan to distribute large files across a unicast network frequently, consider the size and performance of your group leader. For example, a C6100 can distribute content to multiple group members more efficiently than a C1100.

However, you can offset performance and load issues by increasing the ratio of group leaders to group members. To achieve this, make your transport groups smaller so that fewer group members are assigned to each group leader. For example, if a unicast transport group contains 11 group members and one group leader, divide the transport group into three separate transport groups—each containing three group members and a group leader.

Reliability: For maximum reliability, designate a minimum of two potential group leaders whenever possible. For example, designate one assigned group leader and one or more candidate group leaders to every network segment.

**Setting up
NetCache as
reverse proxy for
the core application**

You can set up a NetCache appliance as a reverse proxy in front of the core application server. The NetCache can serve http traffic, and cache and deliver jobs to a large number of GLs, more efficiently than the embedded web server in ContentDirector. See the *NetCache Accelerator First-Time Configuration Guide* and the *NetCache Configuration Guide* for detailed instructions.

Deploying ContentDirector with firewalls

Default ports to open in all firewalls

The default port for the ContentDirector application is 8080, and for NetCache administration, 3132. For firewalls between the core application and group leaders, these ports must be open:

- ◆ Firewall in front of the core application:
 - ❖ 8080/tcp inbound
 - ❖ 3132/tcp outbound
- ◆ Firewall in front of the group leader:
 - ❖ 3132/tcp inbound
 - ❖ 8080/tcp outbound

If you change either of these ports, the new port must be opened in both firewalls.

Configuring ports in NAT-based firewalls

For NAT-based firewalls between the core application and group leaders, you must configure the firewalls to direct inbound port traffic to the corresponding node. Below are examples with randomly chosen IP addresses:

- ◆ Firewall in front of the core application directs inbound port 8080/tcp traffic to the IP address of core application, for example:
8080 -> 10.95.100.50
- ◆ Firewall in front of the group leader directs inbound port 3132/tcp traffic to the IP address of the group leader, for example:
3132 -> 10.95.200.30

Ports to open in NAT-based firewalls on satellite networks

If the group leader is behind a NAT-based firewall and delivers data directly to a satellite without going through the firewall, open inbound port 1100/udp for MCTP backchannel traffic.

If group members on the same network are behind NAT-based firewalls and receive data directly from the satellite without going through the firewall, open outbound port 1100/udp for MCTP backchannel traffic.

Multiple group leaders behind a single NAT-based firewall

For a NAT-based firewall with multiple external addresses, you can set up one group leader behind the firewall for each external address. If you have more group leaders than external addresses in the firewall, you must reconfigure the administrative port on every group leader that does not have its own unique external firewall address.

You also must open the corresponding firewall ports:

- ◆ In the firewall in front of the group leaders, open new inbound ports and redirect traffic on them to the corresponding group leaders
- ◆ In the firewall in front of the core application, open corresponding new outbound ports

DNS for Streaming media

NetCache DNS requirement

When deploying Content Director with NetCache appliances to distribute streaming media files, it is normally necessary that the NetCache appliance have access to a DNS server.

When a client pushes content to the appliance, NetCache tries to ensure that the content will be accessible. One of the ways NetCache enforces this with streaming content is to attempt to generate a fully-qualified domain name for the streaming media server.

This provides NetCache with some measure of confidence that the cache will detect a cache hit regardless of how the client asked for the content (IP address, partially-qualified domain name, etc.) Also, because NetCache must sometimes communicate with the media server before serving cached content, doing this ensures that NetCache contacts the correct media server.

The fully qualified domain also acts as the key that is used to index the cached content.

Sample configurations

About the sample configurations

The following sample configurations are examples of how you can deploy ContentDirector. They reflect four categories of deployment, based on transmission mode and complexity of network:

Each sample contains a diagram of the network configuration and additional details you need to deploy ContentDirector in that configuration.

For detailed information

The following sections illustrate sample configurations of ContentDirector:

- ◆ [“One-level unicast”](#) on page 17
- ◆ [“Two-level unicast”](#) on page 18
- ◆ [“Unicast to multicast”](#) on page 20
- ◆ [“Multicast over satellite”](#) on page 21

Note

These are only examples and do not represent the full range of possibilities. Your exact deployment will reflect your existing network infrastructure and the needs of your organization. Please consult your Network Appliance Systems Engineer for more detailed information on deployment.

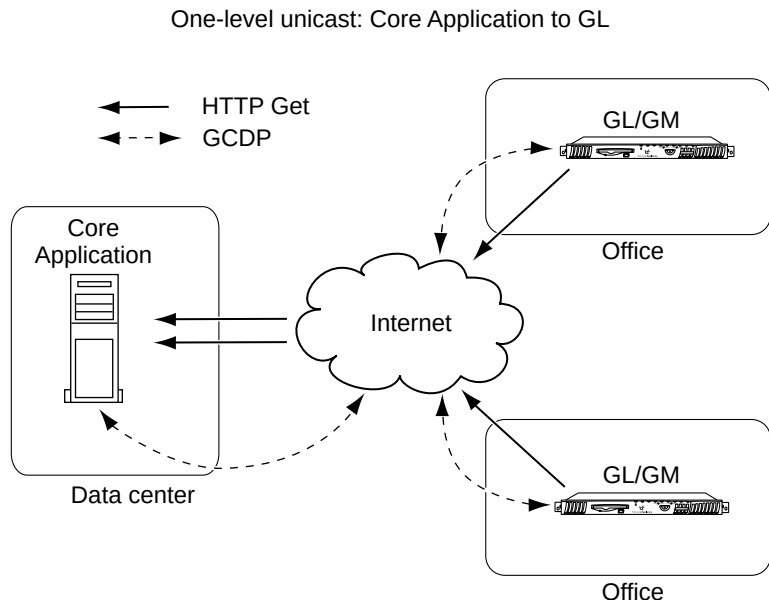
One-level unicast

About one-level unicast

This is the simplest configuration of Content Director. The core application resides in the data center, and communicates with ContentDirector Agents in remote offices. Each office has a single transport group leader/group member that fetches data directly from the core application. This deployment scenario also applies when the core application and all transport group members are on the same WAN.

Firewall requirements for one-level unicast

This configuration requires a bi-directional hole in each firewall for GCDP and an inbound hole on the core application firewall for HTTP GETs.



Two-level unicast

About two-level unicast

In this configuration, multiple branch offices in a non-multicast corporate WAN share the same ISP line.

ContentDirector conserves bandwidth by using one transport group leader for the entire WAN. Data is transmitted over the Internet only once, then distributed within the WAN via unicast from the group leader to the group members.

This configuration assumes that the core application is not resident within the corporate WAN. If the core application is within the WAN, it is probably more efficient to use one-level unicast.

Configuring transport group members for two-level unicast

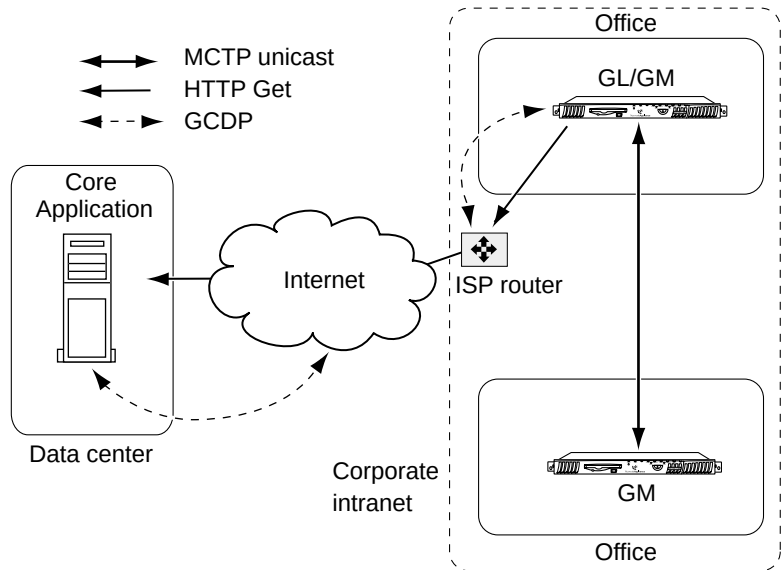
For two-level unicast, the transport group members must be configured with the unicast address of the transport group leader.

Firewall requirements for two-level unicast

This configuration requires two bi-directional holes in the firewall:

- ◆ At the core application
- ◆ In front of the transport group leader

Two-level unicast: Core Application to GL to GMs



Unicast to multicast

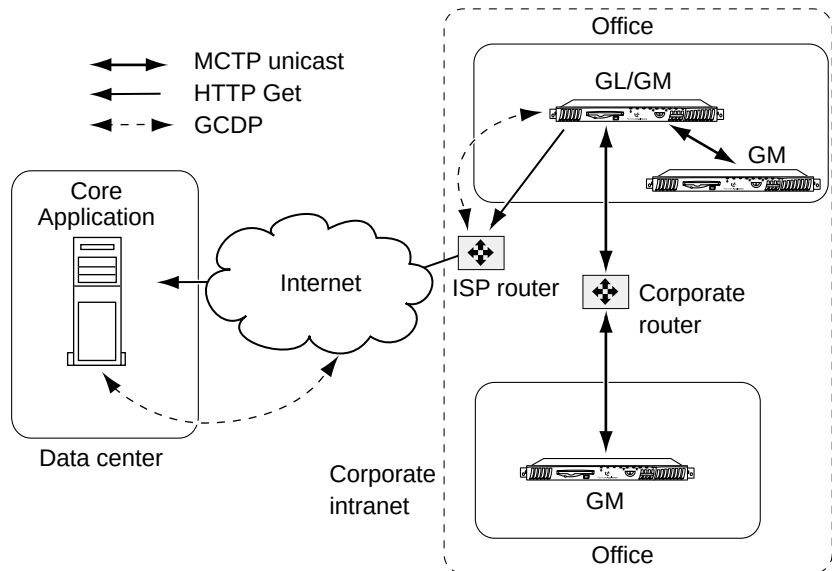
About unicast to multicast

In this configuration the core application delivers data to a transport group leader/group member on a multicast-enabled corporate WAN. This group leader/group member serves two transport group members. The group members may be either within the broadcast domain of the group leader or behind a multicast-enabled router.

Firewall requirements for unicast to multicast

Unicast to multicast requires bi-directional holes in firewalls at the core application and transport group leader.

Two-level unicast: Core Application to GL to GMs



Multicast over satellite

About multicast over satellite

The following diagram depicts a simplified layout of a satellite based content distribution network.

In the multicast over satellite configuration, the data center and uplink house the core application, content sources, and transport group leader. The transport group members are located at remote offices. They receive multicast messages and respond over a terrestrial back channel.

The group leader to group member communication is MCTP encapsulated by the satellite systems native transport (DVB). The group leader sees the satellite system as a router.

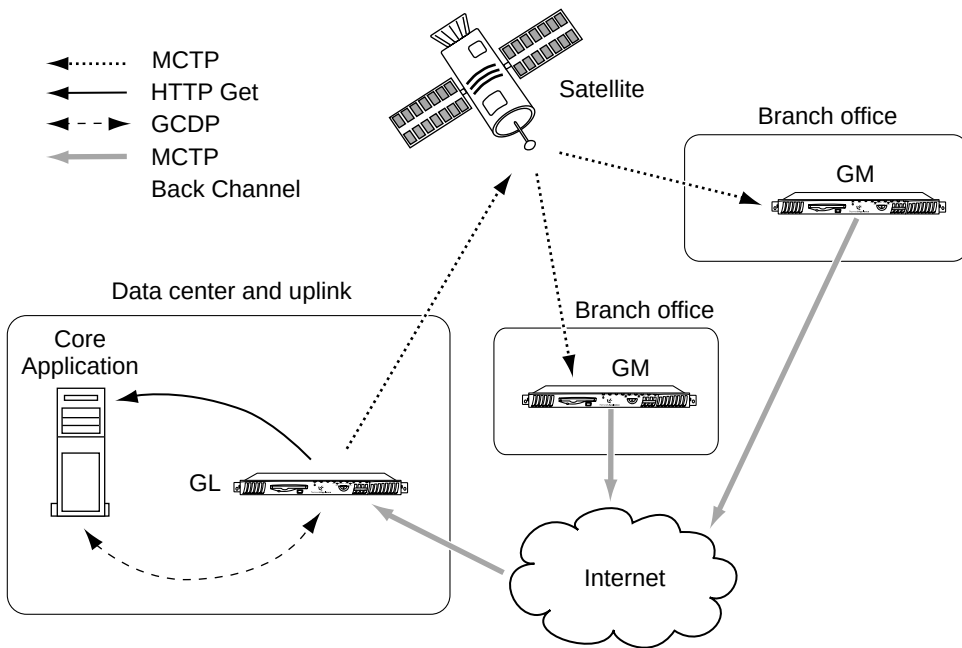
Scalability of multicast over satellite

In multicast over satellite, ContentDirector is able to produce maximum scalability, being essentially limited by the amount of feedback the transport group leader can handle. MCTP provides forward error correction (FEC) to further reduce the amount of feedback needed from the transport group members.

Group member and firewall requirements for multicast over satellite

If the group leader and group members are behind a firewall, you must configure an outbound hole on the group member side of the firewall, and an inbound NAT hole on the group leader side. Configure the group members with the external NAT'ed address for the group leader.

Multicast over satellite



Preliminary information

This chapter discusses the information that you need before you install ContentDirector. Once you have planned your ContentDirector deployment, you need to verify the following items:

- ◆ The system has adequate resources
- ◆ The network topology is appropriate to the ContentDirector configuration that you defined
- ◆ The network is on-line and the connections are working properly
- ◆ There are no conflicts between the ports that are used by ContentDirector and those of other applications or services

Chapter topics

The chapter discusses the following topics

- ◆ [“Compatibility with previous versions”](#) on page 24
- ◆ [“Network topology and operation”](#) on page 28
- ◆ [“Transport port conflicts”](#) on page 29

Compatibility with previous versions

ContentDirector 1.0 ContentDirector 2.0 is not compatible with, or upgradable from, ContentDirector version 1.0. If you plan to install version 2.0 on a machine where version 1.0 is currently installed, you need to uninstall 1.0 first.

System requirements

System requirements for core application machines

OS: The core application runs on Windows NT and 2000 and Solaris UNIX systems.

Processor and RAM: The processor speed and RAM on the core application machine can be fairly modest, however, performance is improved if you increase the speed and memory of the system. If you intend to push jobs that are quite large or to run multiple jobs at any given time, you should consider increasing the processor speed and RAM of the core application machine beyond the minimal requirements.

Video: The installation utility and the user interface require that the video system be capable of displaying at least 256 colors. If the video system does not meet this requirement, the installation cannot complete, and the user interface cannot display correctly.

Table of system requirements

The following table provides system requirement details.

	Windows NT	Windows 2000	Solaris	NetCache (GL and GM only)
OS	Service Pack 4 and above	Server, Advanced Server, and Professional (all versions)	Version 2.7 and above	Version 5.2 and above
Processor	500 MHz	500 MHz	400 MHz	NA
RAM	Core application: 256 Mb (512 Mb-1Gb preferred) CDA: 256 Mb	Core application: 256 Mb (512 Mb-1Gb preferred) CDA: 256 Mb	512 Mb	256 Mb

Note

ContentDirector does not support Windows Terminal Server as an operating environment.

Storage requirements

Storage requirements for the ContentDirector components

The storage requirements for the core application, the transport group leaders, and the transport group members differ.

- ◆ The core application requires space for the software, logs, the database, and directories related to processing jobs.
- ◆ The group leaders require only the space required by the CDA software.
- ◆ The group members require space for the CDA software and the content that is pushed to them.

Storage requirements for the core application

Storage requirements for the core application include the program, database, and log files.

ContentDirector software including the embedded database requires 50 MB at installation.

The database increases in size over time in proportion to the number and size of jobs it holds.

The space required for log files is determined by the following factors:

- ◆ Level of logging (default: debug, which is the most verbose)
- ◆ Maximum number of log files to be kept on the system (default: 5)
- ◆ Maximum log size (default: 2000 KB)

Storage requirements for CDAs

The size of the CDA software for both group leaders and group members is less than 50 MB. The group leader does not store the job assignment, so it does not need further storage capacity. The group member must store the size of the largest job assignment pushed, plus the sum of all content previously pushed to the group member that it still stores.

Network topology and operation

Network topology

ContentDirector uses network connectivity to distribute content. The connections can be on VPNs on intranets and the Internet. The core application machine communicates with the ContentDirector agents using a TCP connection and HTTP.

Each ContentDirector agent is a member of a transport group. The subset of the overall network topology that contains the transport group is call the network segment (netseg).

Network operation and links

Before you begin to deploy ContentDirector, you should determine the following:

- ◆ Verify that the network is running and stable
- ◆ Verify that you have the correct IP address for the core application machine.

Note

If you have a NAT based firewall, the NATed IP address must be used.

- ◆ If you have not done so in the planning phase, determine which routers in a given network segment are multicast enabled. Multicast enabled routers are necessary for multicast transport (group leader to group member) across routers. This is essential for transport via satellite. If routers are not multicast enabled, only unicast transport can be used across routers.
- ◆ If you want a transport group to include devices on both sides of a unicast router, you can only designate devices on one side of the router as group leaders (assigned or candidate). If CDAs on both sides of the unicast router are designated as group leaders, two active group leaders will be elected. In effect, this creates two transport groups.

Caution

Do not remove the primary network interface card from a NetCache appliance and use it as the primary network interface card in another NetCache appliance. Doing so can cause the CDA to malfunction.

Transport port conflicts

About the transport port

The ports used for transport between the core application and the transport group leaders are assigned to 8080 by default. Other applications might also bind to port 8080, causing port conflicts. RealNetworks' RealPlayer is one example of this.

To reconfigure the transport port, you need to change it at the core application and at each CDA.

Reconfiguring the transport port on the core application

Two scripts are available for reconfiguring the transport port.

- ◆ `chgports` allows you to specify the port to use for transport.
- ◆ `chgtom` automatically changes the port to the next available port and displays the new port number

The location of these scripts depends on the operating system of the core application machine:

- ◆ Under Windows, the `ContentDirector\Ccm` directory
- ◆ Under Solaris, the `/opt/NTAPccm/bin` directory

To reconfigure the transport port, complete the following steps.

Step	Action
1	Stop the ContentDirector service.
2	Navigate to <code>ContentDirector\Ccm</code> (for Windows) or <code>/opt/NTAPccm/bin</code> (for Solaris).
3	At the prompt, run either <code>chgports</code> or <code>chgtom</code> : To run <code>chgports</code> , type: <code>chgports -tn <port number></code> where <code><port number></code> is the new port, then press Enter. To run <code>chgtom</code> , type: <code>chgtom</code> then press Enter.

Step	Action
4	Start the ContentDirector service.
5	Change the ContentDirector port on each CDA to match the new port. See “Reconfiguring the transport port on the CDA” .

Reconfiguring the transport port on the CDA

When you change the transport port at the core application, you must also change it at each CDA to match the new port. To change the port at the CDA, complete the following steps.

Step	Action
1	From the NetCache Manager utility, select Setup > ContentDirector > Advanced.
2	Under Core Application Port, enter the new port number you configured at the core application.
3	Click Commit Changes.

About this chapter

This chapter provides background information and instructions for installing and uninstalling ContentDirector on Microsoft Windows.

Topics in this chapter

This chapter includes the following topics:

- ◆ [“About installing on Windows”](#) on page 32
- ◆ [“Running the installation wizard”](#) on page 33
- ◆ [“Uninstalling ContentDirector on Microsoft Windows”](#) on page 35

About installing on Windows

The installation wizard

The ContentDirector core application installs onto Microsoft Windows through a graphical installation wizard. The procedures in this chapter apply to both Windows 2000 server and Windows NT.

Note

You do not need to install the CDA because it is included with the Netcache kernel. For instructions on enabling and configuring the CDA on NetCache, see [“Configuring the ContentDirector Agent Software”](#) on page 43.

Information you need before you start

Before starting the installation, you need to gather the following information:

- ◆ The IP addresses of all machines that will run the core application
- ◆ Your ContentDirector license number from the media box that contains the software.

Running the installation wizard

Procedure

To run the ContentDirector installation wizard, complete the following steps.

Note

You need administrative privileges to install ContentDirector under Windows NT and Windows 2000.

Step	Action
1	Insert the ContentDirector CD into the CD drive.
2	Navigate to the root directory of the CD and double-click setup.exe to begin the installation.
3	At the Welcome screen, click Next.
4	In the License Agreement screen, please read the license agreement carefully. Click Yes to accept the license agreement and continue with the installation.
5	In the Choose Destination screen, accept the default location of C:\Program Files\Network Appliance Inc\ContentDirector, or click the Browse button to select another location. Click Next.
6	In the Select Program Folder screen, select a program folder for the ContentDirector program icons. Choose one of the following actions: ◆ Click Next to accept the default program folder ◆ Select a different folder from the list under Existing Folders ◆ Type in the name of a new folder under Program Folders
7	In the Edit Data screen enter your license number or click the Evaluation checkbox. Your license number is included with in the product shipment. The Evaluation expires after a sixty-day period. At that time you will need to purchase ContentDirector and obtain a license to continue running it. Click Next.

Step	Action
8	ContentDirector installs. The status window displays a progress bar showing the percentage complete.
9	The installed ContentDirector services start.
10	Click Finish to dismiss the installation wizard.

Test your installation

After installing, it is highly recommended that you test your installation by running one small content distribution task to all destinations. For more information, see [“Testing Your ContentDirector Installation”](#) on page 59 .

Uninstalling ContentDirector on Microsoft Windows

About uninstalling Uninstalling ContentDirector is performed where the core application resides. No folders, files, services, or registry settings for ContentDirector remain after it is uninstalled.

Procedure To uninstall ContentDirector on Microsoft Windows, complete the following steps:

Step	Action
1	Stop the ContentDirector service.
2	At the Windows desktop, click Start > Settings > Control Panel.
3	Double-click Add/Remove Programs.
4	In the Add/Remove Programs Properties screen, click ContentDirector.
5	Click Add/Remove.
6	In the InstallShield Wizard Welcome screen, select Remove.
7	Click Next.
8	In the Confirm File Deletion screen, click OK to continue uninstalling.
9	If the wizard displays a ReadOnly File Detected screen, click the checkbox for Don't display this message again, then click Yes.
10	In the Maintenance Complete screen, click Finish to dismiss the InstallShield wizard.
11	Click OK in the Add/Remove Programs Properties screen to return to the Windows desktop.

About this chapter This chapter discusses the procedure for installing ContentDirector on a Solaris system.

Chapter topics This chapter discusses the following topics.

- ◆ [“Installing the core application on a Solaris server”](#) on page 38
- ◆ [“Uninstalling the the core application on a Solaris server”](#) on page 41

Installing the core application on a Solaris server

About installing the core application

The installation of ContentDirector on a Solaris system requires that you execute the `pkgadd` (package add) command for the NTAPccm package. This runs the scripts that install the program. You are prompted to provide information and make decisions as the installation program runs.

- Before you start
- The ContentDirector installation requires the following.
- ◆ You need the license number that came with the ContentDirector media box to perform the installation.
 - ◆ You must be logged in as root, which provides super user privileges.
 - ◆ The ContentDirector CDROM must be mounted on to the system on which you are installing the software. If this is not possible, the contents of the CDROM must be copied to a location that is accessible to the system.

Installing the NTAPccm package

To install the NTAPccm package on the core application server complete the following steps

Step	Action
1	From any prompt, enter: <code>pkgadd -d <cdrom mount point>/solaris/NTAPccm.</code> Result: The following information is displayed. ◆ The available package ◆ The build number You receive the following prompt. Select package(s) you wish to process (or 'all' to process all packages). (default: all) [?,??,q]

Step	Action
2	Press Enter to select the default. Result: processing begins and the license is displayed. The following prompt appears. <pre>Do you agree to this license (y/n)?</pre>
3	Press Y to agree to the license and continue the installation. Result: The following prompt appears. <pre>Enter product license key (press enter for evaluation):</pre>
4	Enter the license key or press Enter. Result: The following prompt appears. <pre>The selected base directory </opt/NTAPccm> must exist before installation is attempted. Do you want this directory created now [y,n,?,q]</pre>
5	Press Y to create the directory and continue the installation. Result: The following prompt appears. <pre>This package contains scripts which will be executed with super-user permission during the process of installing this package. Do youwant to continue with the installation of <NTAPccm> [y,n,?]</pre>
6	Press y. Result: the following text is displayed. <pre>Installing Content Control Manager as <NTAPccm> ## Installing part 1 of 1.</pre> The directories and files that are being copied scroll past, after which information about the final installation processes is displayed. If the installation completes successfully, the last line of screen output is the following. <pre>Installation of <NTAPccm> was successful.</pre>

Note

To start the core application, enter the following:
`/etc/init.d/ccm start`

Uninstalling the the core application on a Solaris server

About uninstalling ContentDirector on a Solaris system

The uninstall process uses the `pkgrm` (package remove) command to uninstall ContentDirector. The program stops the ContentDirector services and removes all of the files and directories and updates the system information.

Uninstalling the NTAPccm package on the core application server

To uninstall the NTAPccm package on the core application server complete the following steps.

Step	Action
1	Stop the core application with the command: <code>/etc/init.d/ccm stop</code>
2	From any prompt, enter: <code>pkgrm NTAPccm</code> Result: Information about the package than build number are displayed, and you receive the following prompt. <code>Do you want to remove this package?</code>
3	Enter <code>y</code> Result: The following information and prompt appear. <code>## Removing installed package instance <NTAPccm></code> <code>This package contains scripts which will be executed</code> <code>with super-user</code> <code>permission during the process of removing this</code> <code>package.</code> <code>Do you want to continue with the removal of this</code> <code>package [y,n,?,q]</code>

Step	Action
4	Enter y Result: The following informational text is displayed. <pre data-bbox="534 388 1126 840">## Verifying package dependencies. ## Processing package information. ## Executing preremove script. Warning: doesn't look like NTAPccm is running. CCManager is not running DbServer is not running Scheduler is not running DbLogger is not running CCMTomcat is not running CCMRegistry is not running ## Removing pathnames in class <none></pre> The files and directories that are being removed drift by. If the removal of the package is successful, the following text is displayed. <pre data-bbox="534 992 995 1020">Removal of <NTAPccm> was successful.</pre>

About this chapter

This chapter introduces the ContentDirector™ agent (CDA) software, describes how the agent software is used in a ContentDirector distribution network, and provides procedures for configuring the NetCache appliance as a ContentDirector group leader or group member.

ContentDirector is a Java-based application that moves content over a network from centralized filers or servers to cache or server destinations. The network can be a local area network, intranet, or Internet with conventional wire and wireless links, including satellite.

In this chapter, NetCache appliances running the ContentDirector agent software are referred to as *CDAs*.

Topics in this chapter

This chapter contains the following topics:

- ◆ [“Planning for ContentDirector agent configuration”](#) on page 44
- ◆ [“Overview of ContentDirector agent configuration”](#) on page 47
- ◆ [“Configuring NetCache for the ContentDirector agent software”](#) on page 49
- ◆ [“Configuring advanced ContentDirector settings”](#) on page 51
- ◆ [“Configuring additional ContentDirector features”](#) on page 57

About ContentDirector configuration using the CLI

This chapter describes using ContentDirector options in the NetCache Manager utility to configure the NetCache appliance as a ContentDirector agent. For descriptions of CLI configuration commands, see the *NetCache Command Line Reference*.

To get information about ContentDirector commands from the CLI, enter the following command:

```
set config.cd.?
```

The preceding command lists the available ContentDirector options.

To get help for a specific ContentDirector option, enter the following command:

```
help config.cd.optionname
```

Planning for ContentDirector agent configuration

Information to gather for CDA configuration

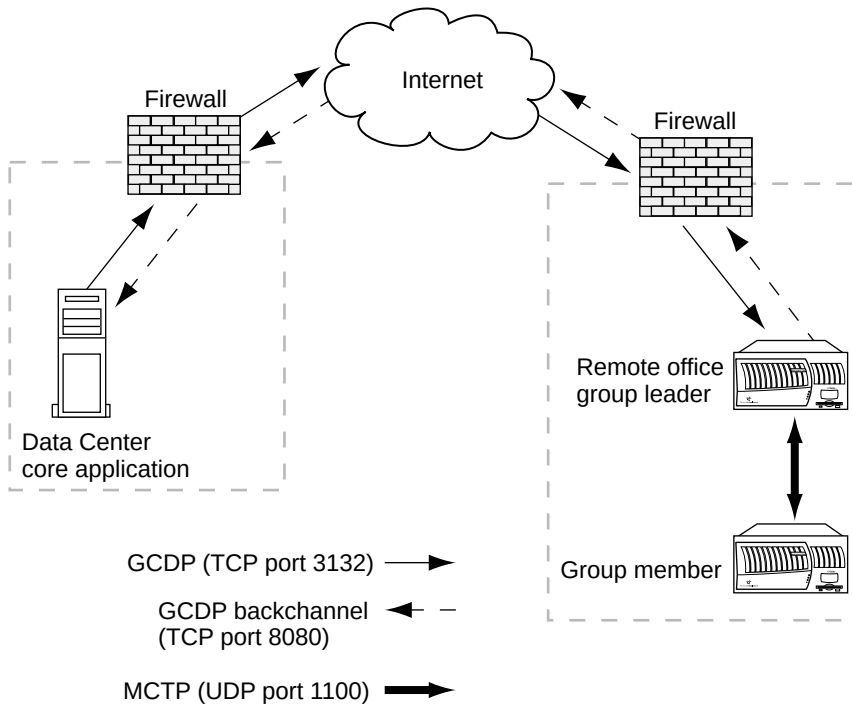
ContentDirector agent configuration will require less time if you make some decisions and gather some information before you start configuring the CDA. Determine the following:

- ◆ Whether you want to configure the CDA as a group leader or group member
- ◆ The IP address of the core application, if you are configuring a group leader
- ◆ The IP address of the group leader, if you are using a unicast network and are configuring a group member
- ◆ The IP addresses of any firewalls between the CDA and other ContentDirector devices (for example, the core application, group leaders, and group members)
- ◆ The port number to use for core application, if you are configuring a group leader and do not want to use the default port number (8080)

You might need to change the port number if an application uses the same port, for example, RealProxy™ Server, which uses port 8080 for HTTP encapsulation. See “[Transport port conflicts](#)” on page 29 for more information on reconfiguring the default port.

This section provides information to help you determine the types of information required for your deployment.

The following illustration shows the traffic flow in a typical ContentDirector deployment. See “[ContentDirector port requirements](#)” on page 46 for more information about ContentDirector port traffic.



ContentDirector port requirements

The following table describes the protocols and ports required for ContentDirector communication.

Protocol	Transport	Traffic description	Explanation
GCDP	TCP	Sent from the core application to port 3132 on the group leader Sent from the group leader to port 8080 on the core application	The Global Content Distribution Protocol (GCDP) is used to deliver core application commands and data to group leaders.
MCTP	UDP	Sent from the group leader to port 1100 on the group member	The Multicast Content Transfer Protocol (MCTP) is used to distribute data from group leaders to group members.

Overview of ContentDirector agent configuration

Prerequisite tasks

Before you begin configuring the CDA, you must have already done the following:

- ◆ Run the setup program from the NetCache appliance console.
The setup program prompts you for the information required to identify the NetCache appliance to the network, including its IP address, host name, DNS domain, and default gateway. If you have not already run the setup program, see the *NetCache Quick Setup* document.
- ◆ Read and become familiar with the planning information for the ContentDirector agent software contained in the *NetCache Deployment Planning Guide*.
The procedures in this chapter assume that you understand this information.
- ◆ Plan your ContentDirector distribution network, including the location of all group leaders and group members, before beginning the ContentDirector agent configuration.
- ◆ Install and configure the ContentDirector 2.0 core application software on a dedicated central server.

How the agent software fits into the overall ContentDirector configuration

The procedures described in this chapter assume that you will configure the ContentDirector software and the ContentDirector agent software as follows.

Step	Action
1	Install and start the ContentDirector core application on the distribution server.
2	Configure the ContentDirector agent software on all group leaders and group members, as described in this chapter.
3	Start up all CDAs, network segment by network segment. As each group leader comes up, the group leader sends a report to the core application listing all active group members. This report is called a network segment report.

Step	Action
4	Check to see if group leaders and group members are communicating properly by refreshing the network segments on the ContentDirector management console. The newly added destinations should be displayed in the Network view.

Overview of CDA configuration

The following table provides an overview of the steps required to configure a CDA.

Step	Action	See...
1	Plan your CDA deployment.	“Planning for ContentDirector agent configuration” on page 44
2	Configure the CDA General options.	“Configuring NetCache for the ContentDirector agent software” on page 49
3	Configure any required CDA advanced options.	“Configuring advanced ContentDirector settings” on page 51
4	Configure additional CDA options required for your deployment.	“Configuring additional ContentDirector features” on page 57

Other configuration that might be required

NetCache appliances configured as group leaders and group members are typically configured for Web or streaming media caching and run the ContentDirector agent software in addition to one or both of these modes. For more information about configuring the CDA for Web caching and for streaming media caching, see the NetCache documentation..

Configuring NetCache for the ContentDirector agent software

Before reading further

The following procedures assume that you have read and are familiar with the ContentDirector planning information contained in the *ContentDirector Installation Guide*. You should have also read [“Planning for ContentDirector agent configuration”](#) on page 44.

Decide the role of the CDA prior to configuration

Before configuring the ContentDirector agent software on the NetCache appliance, determine whether you are configuring the CDA as a group leader or group member.

To configure the CDA as a group leader, see [“Configuring the CDA as a group leader”](#) on page 49.”

To configure the CDA as a group member, see [“Configuring the CDA as a group member”](#) on page 50.

Configuring the CDA as a group leader

To configure the CDA as a group leader, complete the following steps.

Step	Action
1	From the NetCache Manager utility, select Setup tab > ContentDirector > General.
2	Select the ContentDirector Agent Enable check box.
3	In the ContentDirector Agent Operating Mode option, select Group Leader and choose the group leader state. Group leaders can have two states: ◆ Assigned ◆ Candidate See “Properties of group leaders” on page 6 and “Planning for ContentDirector agent configuration” on page 44 for explanations of these group leader states.

Step	Action
4	Enter the IP address of the core application in the Core Application IP Address option.
5	Click Commit Changes at the bottom of the page.
6	Configure any required group leader advanced settings. See “Configuring advanced ContentDirector settings” on page 51 for information about these advanced settings.
7	Configure any additional features required for your deployment. See “Configuring additional ContentDirector features” on page 57 for more information.

Configuring the CDA as a group member

To configure the CDA as a group member, complete the following steps.

Step	Action
1	From the NetCache Manager utility, select Setup tab > ContentDirector > General.
2	If you have not already done so, select the ContentDirector Agent Enable check box.
3	In the ContentDirector Agent Operating Mode option, select Group Member.
4	Click Commit Changes at the bottom of the page.
5	Configure any required group member advanced settings. See “Configuring advanced ContentDirector settings” on page 51 for information about these advanced settings.
6	Configure any additional features required for your deployment. See “Configuring additional ContentDirector features” on page 57 for more information.

Configuring advanced ContentDirector settings

About the ContentDirector optional settings

The ContentDirector advanced settings enable you to modify the firewall and transport settings of your ContentDirector agent. The ContentDirector advanced settings are located on the ContentDirector - Advanced page.

This section includes the following topics about advanced features that can be configured for group members:

- ◆ [“Identifying a CDA located behind a NAT-based firewall”](#) on page 52
- ◆ [“Specifying the group leader IP address”](#) on page 53

This section includes the following topics about advanced features that can be configured for group leaders:

- ◆ [“Identifying a CDA located behind a NAT-based firewall”](#) on page 52
- ◆ [“Disabling UDP fragmentation”](#) on page 54
- ◆ [“Modifying the multicast IP addressing mode”](#) on page 54
- ◆ [“Changing the core application port”](#) on page 55

Recommendations for configuring the ContentDirector advanced settings

Use the following recommendations to determine if you need to configure any of the ContentDirector advanced settings.

Situation	Recommendation	See...
Group member recommendations		
If the group member is behind a firewall and is unable to communicate with other ContentDirector devices	Configure the “If this ContentDirector Agent Is behind a NAT-Based Firewall” option.	“Identifying a CDA located behind a NAT-based firewall” on page 52
If the group member is unable to communicate with the group leader	Verify that the group leader IP address is specified in the Group Leader IP Address option.	“Specifying the group leader IP address” on page 53

Situation	Recommendation	See...
Group leader recommendations		
If the group leader is behind a firewall and is unable to communicate with other ContentDirector devices	Configure the “If this ContentDirector Agent Is behind a NAT-Based Firewall” option.	“Identifying a CDA located behind a NAT-based firewall” on page 52
If the group leader uses a satellite or wireless network to distribute ContentDirector data to group members	Disable the UDP Fragmentation option to ensure that lost packets will not impact performance.	“Disabling UDP fragmentation” on page 54
If you want the group leader to send data to some group members but not others	Select the “Use Multiple Multicast IP Addresses for Better Performance” field in the Enable Single Multicast IP Address option.	“Modifying the multicast IP addressing mode” on page 54
If you want to change the port number of the core application server	Enter the desired port number in the Core Application Port option.	“Changing the core application port” on page 55
Additional configuration recommendations		
If you want to enable ContentDirector logging	ContentDirector logging is enabled by default. However, you can view and manage ContentDirector logs.	“About ContentDirector logging” on page 57 and “Managing the ContentDirector log” on page 57
If you want to limit ContentDirector bandwidth	Specify a ContentDirector bandwidth limit using the NetCache bandwidth allocation management feature.	“Setting ContentDirector connection bandwidth limits” on page 57

Identifying a CDA located behind a NAT-based firewall

If this CDA is behind a firewall that uses Network Address Translation (NAT) to obscure internal IP addresses, you must specify the IP address of the CDA so that it can communicate with the external ContentDirector devices.

Note

Firewalls configured for dynamic NAT addressing are not supported. The CDA communicating with the core application or group members outside the firewall must have a static NAT address.

To specify the static NAT IP address of the CDA, complete the following steps.

Step	Action
1	From the NetCache Manager utility, select Setup tab > ContentDirector > Advanced.
2	Answer the questions in the “If this ContentDirector Agent Is behind a NAT-Based Firewall” option. If you answer No to one or both of the questions, you must enter the public NAT IP address that translates to the internal IP address assigned to the CDA.
3	Click Commit Changes at the bottom of the page.

Specifying the group leader IP address

Typically, the group leader IP address is automatically discovered during the ContentDirector agent configuration. However, if you are not using a multicast-enabled network, for unicast group members you can manually enter a comma- or space-delimited list of group leader candidate host names or IP addresses.

To specify the list of group leader candidates, complete the following steps.

Step	Action
1	From the NetCache Manager utility, select Setup tab > ContentDirector > Advanced.
2	Enter the list of group leader candidate host names or IP addresses in the Group Leader IP Address option. Use commas or spaces as separators between entries.
3	Click Commit Changes at the bottom of the page.

Note

If you have multiple group members and do not want to manually enter the group leader IP address on each group member, you can set up a host name in DNS called `group_leader` or `group_leader.domain.com` that corresponds to the elected group leader IP address.

Disabling UDP fragmentation

By default, the UDP Fragmentation option allows UDP packets to be fragmented when the network supports a maximum MTU size that is smaller than the size of a packet. However, UDP fragmentation is not recommended for high-bandwidth lossy networks, such as satellite or wireless networks, where many dropped packets can impact performance. Although this kind of packet loss is rare in conventional networks, it is common on satellite connections or other forms of wireless communication.

To disable UDP fragmentation, complete the following steps.

Step	Action
1	From the NetCache Manager utility, select Setup tab > ContentDirector > Advanced.
2	Clear the UDP Fragmentation check box.
3	Click Commit Changes at the bottom of the page.

Modifying the multicast IP addressing mode

The Multicast IP Addressing Mode option enables single or multiple multicast IP addressing for group members. By default single multicast IP addressing is enabled.

About single multicast IP addressing: When you enable single multicast IP addressing, all group members in a content group receive data, even if you do not want a particular group member to receive content. This method can be inefficient because processing power is expended to determine whether the data is needed.

If you want all group members on the network to receive data, there is no performance difference between single and multiple multicast IP addressing.

You might also want to enable single multicast IP addressing if your organization imposes a limitation on the number of multicasting addresses that can be used on your network.

By default, single multicast IP addressing uses two multicast addresses:

- ◆ Multicast address 239.100.1.1 is used for the data, global, and control channels.
- ◆ Multicast address 239.100.1.2 is used for the group leader election channel. Only potential group leaders use this additional multicast address.

About multiple multicast IP addressing: In contrast to single multicast IP addressing, in which all group members receive data whether they need it or not, multiple multicast IP addressing enables you to send data to only those group members that require it. When you enable multiple multicast IP addressing, group members that are to receive data subscribe to a different multicast IP address from within the multicast IP address range 239.100.1.1 - 239.100.1.8.

When you use the multiple multicast IP addressing method, only group members that will receive data will expend CPU time to process the multicast data. All other group members will simply ignore data sent to multicast IP addresses that they are not listening for.

Enabling single multicast IP addressing: To enable single multicast IP addressing, complete the following steps.

Step	Action
1	From the NetCache Manager utility, select Setup tab > ContentDirector > Advanced.
2	In the Multicast IP Addressing Mode option, select “Use Single Multicast IP Address.”
3	Click Commit Changes at the bottom of the page.

Changing the core application port

The Core Application Port option specifies the port for the core application. The core application uses HTTP for transport. The default port is 8080. See [“ContentDirector port requirements”](#) on page 46 for more information.

You can specify another HTTP port, but you must ensure that you include the core application port in the HTTP Proxy Ports option on the HTTP - General page.

To change the core application port number, complete the following steps.

Step	Action
1	From the NetCache Manager utility, select Setup tab > ContentDirector > Advanced.
2	Enter the desired core application port number in the Core Application Port option.
3	Click Commit Changes at the bottom of the page.

Where to find more information

See the NetCache Manager online Help for more information about the ContentDirector options.

Configuring additional ContentDirector features

About ContentDirector logging

The ContentDirector log provides diagnostic information for fatal errors and is enabled by default. For more information about the ContentDirector log, contact your Network Appliance technical support representative.

Managing the ContentDirector log

You can use the NetCache Manager log management features to manage your ContentDirector log. Using the log management features you can view, copy, delete, and compress ContentDirector log files. You can also upload the ContentDirector log files to an FTP or Web server.

To access the ContentDirector log management options in the NetCache Manager utility, select Data Tab > Log Files > ContentDirector. The ContentDirector logging online Help provides additional log management information.

Setting ContentDirector connection bandwidth limits

You can use the NetCache bandwidth allocation management feature to limit the bandwidth for content distribution connections between group leaders and group members.

You might want to modify the bandwidth limit if you are running other applications or devices on the same network and need them to receive more bandwidth. You might also want to limit bandwidth if you are charged for exceeding specific bandwidth levels on your network.

You can create bandwidth allocation rules for ContentDirector traffic to

- ◆ Reserve a portion of your total NetCache bandwidth capacity for ContentDirector traffic
- ◆ Allow, deny, or assign connections to group leaders based on time and interface

See the *NetCache Routine Administration Guide* for more information about using the bandwidth allocation management feature.

Generating a unique master key

A master key is used at two ends of data transfers to ensure the security or integrity of the transaction. Each installation of the ContentDirector core application has a master key for this purpose. When ContentDirector is installed, it contains matching default master keys at the core application and each CDA. It

is ready to use without any further modifications to the master key. For a higher level of security, you can generate a unique master key for your ContentDirector network through the management console of the core application. See the *ContentDirector 2.0 Administration Guide* for detailed instructions.

About this chapter

This chapter contains instructions on how to perform a basic test of your ContentDirector installation. The test instructions describe how to distributing content to a selected destination and verify its presence at the destination.

Topics in this chapter

This chapter contains the following topics:

- ◆ [“Before you start”](#) on page 60
- ◆ [“Testing distribution”](#) on page 61

Before you start

Checking connectivity in ContentDirector

Before you test your installation, check the Network View in ContentDirector to confirm that the core application detects the CDA.

To check the network view, complete the following steps:

Step	Action
1	At the left side of the ContentDirector main screen, click Network.
2	On the left panel, click the plus + sign next to the NetSeg number to expand the view.
3	ContentDirector displays information about the CDA: ◆ On the left panel, beneath the NetSeg number, ContentDirector displays the group leader icon and the name of the machine on which the group leader is installed. ◆ On the right panel, the type of the CDA lists as Transport Group Leader, Transport Group Member, or both. The type should match the type you configured. The correct status is: online, responding, host site(s), and license. Any other statuses indicate a problem.

Testing distribution

About testing distribution to NetCache appliance

These instructions describe how to set up and run a simple job to test HTML or media file distribution to a single NetCache appliance.

These instructions assume that you have the following resources available:

- ◆ Network with proven connectivity
- ◆ Files you wish to distribute (content sources) on a file server or Network Appliance filer
- ◆ ContentDirector core application installed and running, and agent configured and running on NetCache appliance

Resources for content distribution

ContentDirector requires four types of user-defined resources to distribute content:

- ◆ Content source - identifies your source content on your local storage by URL
- ◆ Policy - regulates how content is handled during distribution
- ◆ Job - defines sources, destinations, and schedule
- ◆ Destination group - specifies a group of destinations that all receive content from the same source

For maximum simplicity and minimal preparation:

- ◆ You can use the default policy that comes with ContentDirector . You only need to change the default policy if your network includes a satellite link.
- ◆ When you create a job, ContentDirector prompts you to create a destination group, so a separate procedure is not necessary.

Creating a content source

Only system administrators can create content sources. For test purposes, the recommended source is a single .html or .txt file in its own directory. To create a content source, complete the following steps.

Step	Action
1	Log in as a system administrator.

Step	Action
2	On the top menu bar of the ContentDirector main screen, click Sources.
3	Click New.
4	Next to Scheme, click the dropdown arrow and select the protocol.
5	In the Host name field, enter a unique name for this source. The host name must have at minimum a domain, for example: http://oursite. It may contain a full domain name such as http://oursite.com. It may not end with a slash /.
6	Click Browse and select the source folder for the source content, then OK to select the location. The source folder must be on a local or mapped drive.
7	Click OK to save the new source.
8	Click Close to return to the main screen. Result: The new content source appears in the Sources view of the main screen.

Using the default policy

The quickest way to run your test is to use the default policy supplied with ContentDirector. You do not need to make any changes to the default policy for your test, unless you are testing distribution via a satellite link.

To view or change the default policy, complete the following steps:

Step	Action
1	At the left side of the ContentDirector main screen, click Policies.
2	Double-click the default policy to open it.
3	If you are testing via satellite, continue to the next step. If you are not, click Close to return to the main screen.
4	To change the policy for satellite link, click the Network tab.
5	Click Save to save your changes and return to the main screen.

Creating a job

To create a job, complete the following steps:

Step	Action
1	At the top of the ContentDirector main screen, click Jobs.
2	Click New.
3	In the Job Name field, enter a descriptive name for this job.
4	Leave the default entries in the other fields. Import job and Description can be left blank.
5	Click the Content tab.
6	In the Hosted site field, click the dropdown arrow and select the source you created for this test.
7	Click Add to select the source directory from a local Solaris or Windows file server. In the Browse screen, select the source location for the content on the local file system.
8	Click the Destination tab.
9	For simplicity in testing, select an individual destination. Click the destination name on the Available Servers panel, then click Add.
10	Leave the Filters and Schedule tabs at the default values. This test job is not scheduled, and must be run manually.
11	Click OK to save the job.
12	The new job displays in the Jobs view of the main screen.

Distributing content

To distribute your selected content, run the job you created by completing the following steps.

Step	Action
1	In the Jobs view table, select the job.
2	Click Run on the lower menu bar. Result: the following prompt appears: Are you sure you want to run the selected job(s)?
3	Click Yes. Result: After a few moments, the values in the Status field of the Jobs table changes as the event progresses through the various stages. Note_____ If the job is a small one, some of the stages may flash on and off the screen too quickly to be seen. _____ New output scrolls through the Status window. When the Job is finished running the status Completed or Failed appears in the Status field. ASSIGNMENT FINISH appears in the Status window.

Verifying the presence of pushed content at the destination

To verify that the pushed content is present at the destination, set up the NetCache as a proxy server in a client web browser, then request one of the files pushed.

Glossary

appliance	A device that performs a single, well-defined function and is simple to install and operate, for example, a NetCache appliance or NetApp filer.
assignment	Temporary files containing content and header data about to be distributed by ContentDirector.
authentication	The process of verifying the identity of a user who is logging in to a computer system.
cache	<i>Verb.</i> To store data temporarily for expedited access. <i>Noun.</i> The location in which data is stored temporarily. There are a variety of types of caches, including disk cache, memory cache, and Web cache.
client	A workstation or PC in a client-server architecture; that is, a computer system or process that requests services from and accepts the responses of another computer system or process.
console	A physical or virtual terminal that is used to monitor and control a NetApp appliance.
ContentDirector	A Network Appliance scalable software solution that automates the distribution of content from the center to the edge of networks.
ContentDirector agent (CDA)	A component of ContentDirector that acts as distribution or destination point at the edge of the network, for content pushed from the center of the network.

content provider	Any company in the business of aggregating or producing content for delivery via the Internet.
core application	The controlling component of ContentDirector at the center of the network that schedules, selects content, and creates policies for the distribution of content to the edge.
Data ONTAP	A software product designed exclusively for NetApp appliances that optimizes file service by combining patented file-system technology and a microkernel design dedicated to network data access. Developed by Network Appliance.
destination	A node at the edge of the network that receives content through ContentDirector and serves it to clients.
destination group	A group of network edge nodes that are targeted to receive content from the same source in ContentDirector. Destination groups are purely logical and do not need to map to physical groups of nodes.
distribution event	One instance of distributing content from ContentDirector.
domain	A subset of ContentDirector resources, associated with specific groups of users and visible only to them and administrators.
Domain Name System (DNS)	An Internet service for finding computers on an IP network.
domain administrator	A ContentDirector user with administrative rights to a specific subset of program resources.
edge device	Any device, for example a NetCache appliance, that is deployed at the periphery of a LAN and WAN environment to interface traffic from the edge of one network to the other.

file server	A computer that provides file-handing and storage functions for multiple users.
filer	An appliance that attaches to a computer network and is used for data storage. NetApp filers operate using Data ONTAP software.
firewall	A server or device deployed between a LAN and the external WAN to control all inbound and outbound traffic, thus the enhancing security of the network behind the firewall.
fully qualified domain name (FQDN)	The complete name of a specific computer on the Internet, consisting of the computer's host name and its domain name.
group leader	A network node that acts as a ContentDirector distribution point, or passthrough, for content near the edge of a network. Group leaders transmit content to group members.
group member	A network node that acts as a ContentDirector destination point for content at the edge of a network. Group members receive content from group leaders.
IP address	The unique numerical address of a computer that is attached to a TCP/IP network, for example, 198.95.226.66.
job	A re-usable set of parameters in ContentDirector that specify the content and schedule for distributing content.
MIME	Multipurpose Internet Mail Extensions. A specification that defines the mechanisms for specifying and describing the format of Internet message bodies. An HTTP response containing the MIME Content-Type header allows the HTTP client to invoke the application that is appropriate for the data received.

MMS	Microsoft Media Streaming. The streaming media control protocol used in Windows Media Technologies 3 and 4 streams.
mount	To make the file system on a particular device accessible by attaching it to the file hierarchy.
NetCache	The proprietary software that runs on NetCache appliances. Developed by Network Appliance.
NetCache appliance	An appliance designed specifically to serve Internet and intranet content quickly and reliably. Developed by Network Appliance.
NetCache Manager	The browser interface through which a NetCache appliance is managed.
network interface card (NIC)	A printed circuit board that connects a computer or other node to a network. Also known as a “network adapter.”
network segment	A set of ContentDirector agents on one or more subnets that can join the same multicast group.
NOW	NetApp On the Web. The secure customer service Web site for Network Appliance.
NTFS permissions	The permissions used in NTFS-style security to control access to files and directories.
policy	A re-usable set of rules in ContentDirector governing how content is handled during distribution events, criteria for success, and email notifications of job status.

quorum	Threshold criteria for the success of a content push in ContentDirector.
regular user	A non-administrative ContentDirector user. Regular users have only the rights granted by membership in a group of users, defined by an administrator.
Remote Shell	A program that enables a user on one system to execute a program on another system. Remote Shells are usually established with the <code>rsh</code> command and are not interactive.
resource	An object in ContentDirector that is necessary for using the program. Users can create, modify, use and delete resources. Resources include: jobs, policies, destination groups, destinations, sources, contacts, users, and user groups.
rsh	The command used to establish a Remote Shell connection.
RTSP	Real Time Streaming Protocol. An open standard for delivery of real-time media over the Internet.
shadow	Copy of content most recently distributed by ContentDirector for a specific job.
Snapshot	A Data ONTAP feature that creates an online, read-only copy of the entire file system—called a “snapshot”—that protects against accidental deletions or modifications of files without duplicating file contents.
source	Directory on a local disk drive at the center of the network, containing content to be distributed through ContentDirector to NetCache appliances at the edge .
stream	A media file that is transmitted in a continuous flow over a network. Streams are of two types, live and on-demand.

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.
streaming server	A server configured to serve streaming media to clients.
system administrator	A ContentDirector user with administrative rights to all program resources.
user group	A list of non-administrative ContentDirector users, and the rights that they share.
Time To Live (TTL)	The time limit on how long a copy of an object remains in the cache before NetCache verifies the object with the originating Web server.
volume	An independent file system with its own RAID groups.
workspace	Directory used by ContentDirector for temporary and backup copies of distributed content and command buffers.

Index

C

CDA. *See* ContentDirector

content types

- supported 2

ContentDirector

- advanced configuration options

 - Group Leader IP Address 53

 - Multicast IP Addressing Mode 54

 - NAT-based firewall 52

 - UDP fragmentation 54

- agent

 - advanced configuration 51

 - advanced configuration options

 - Core Application Port 55

 - bandwidth limits 57

 - CLI commands 43

 - communication 5

 - configuration 47

 - configuration overview 48

 - configuration planning 44

 - core application port 44

 - firewall planning 11

 - log 57

 - logging 57

 - MCTP ports 46

 - multicast IP addressing 55

 - multicast networks and 11

 - multiple multicast IP addressing 55

 - network recommendations 11

 - planning for configuration 44

 - protocol service for 48

 - recommendations for advanced configuration 51

 - single multicast IP addressing 54

 - size and performance planning 10, 11

 - UDP fragmentation and 54

 - unicast networks and 11

- bandwidth limits 57

- bandwidth planning 11

- CLI configuration commands 43

- communication 5

- components 3

- configuration

 - additional features 57

 - advanced options 51

 - CLI commands 43

 - information to gather 44

 - overview 48

 - planning for 44

 - prerequisites 47, 49

 - protocol service for 48

 - recommendations for advanced options 51

 - verifying 48

- configuration overview 47

- content groups 5

- core application port 44, 56

- defined 43

- firewalls and 52

 - NAT addressing 52

 - planning 11

- GCDP ports 46

- group leaders 5

 - configuring 49

 - definition of 5

 - how used 5

 - planning for 11

 - reliability planning 12

 - specifying IP address for 53

- group members

 - configuration 50

 - how used 5

- log 57

- management console 5

- minimum system requirements for 25

- multicast IP addressing 54

 - enabling 55

 - multiple multicast IP addressing 55

 - single multicast IP addressing 54

- multicast networks and 10

- NAT addressing restrictions 52

- network recommendations 10, 11

- network segment report 47

- ports required 46

- satellite communication and 54

- size and performance planning 10, 11
- status messages 47
- transport groups 5, 11
- UDP fragmentation and 54
- unicast networks and 10
- verifying configuration 48
- version 1.0 24

- ContentDirector Agent Operating Mode option 49
- ContentDirector Enable option 49
- Core Application IP Address option 50
- Core Application Port option 55

F

- firewalls
 - in networks with satellite links 21
 - NAT-based
 - configuring ports in 13
 - multiple group members behind 14
 - ports on satellite networks 13
 - opening default ports in 13

G

- GCDP
 - ports 46
- Global Content Distribution Protocol. *See* GCDP
- group leaders
 - assigned versus candidate 6
 - minimum configuration 6

M

- MCTP
 - ports 46
- Multicast Content Transport Protocol. *See* MCTP
- Multicast IP addressing Mode option 54

P

- protocols
 - supported 2

U

- UDP fragmentation 54