



WHITEPAPER

CISCO TECHNICAL KNOWLEDGE LIBRARY

Cisco Advanced Services deliver the expert resources to address the complexity of deploying and managing the next-generation, multi-service, converged network of networks. Relationships with Cisco's experts are based on specific Advanced Services such as: Technology Extensions and Optimize Services.

Now, Cisco's Advanced Services team is signing up select customers for an additional knowledge transfer service, the second generation Cisco Technical Knowledge Library, to augment existing communications with the experts.

Select customers are being offered this service—based on Cisco's leading Content Networking technology—serving video, audio, and document content prepared by Advanced Services experts. This content can be used as self-study or in concert with other Advanced Services training activities. In addition, AS customers can elect to use the Cisco Technical Knowledge Library to archive and organize company-specific deliverables from Cisco.

The purpose of this document is to provide information on the components that are the framework of the Cisco Technical Knowledge Library, how the service is deployed to allow content to be efficiently delivered to the end user, and how it is managed. Also, this paper will briefly cover how the value of the service is increased by frequent updates and the addition of new materials, as well as the usage statistics that are provided to help the customer assess its utilization.

COMPONENTS

The Cisco Technical Knowledge Library utilizes a combination of Cisco's Enterprise Content Delivery Network suite and Media Convergence Servers to deliver content. The equipment used is a self contained system in that it is wholly owned and managed by Cisco Advanced Services, and it does not interfere with other content networking systems that the customer may already be using.

- Content Distribution Manager (CDM) – CE565 – Provides management GUI for content network
- Content Router (CR) – CE565 – Provides intelligent content request redirection
- Content Engine (CE) – CE565 / CE512– Serves content to end users
- Origin Server – Serves as the origin for content

SOFTWARE

The Cisco Technical Knowledge Library content networking devices use Cisco Application and Content Networking Software (ACNS). ACNS is a closed operating system developed for Cisco content networking devices and is not vulnerable to windows specific viruses and worms.

DEPLOYMENT

Depending on the requirements of the customer, the Cisco Technical Knowledge Library can be deployed in various scenarios in an effort to work with the customer to achieve a design that adheres to their security policy and allows for the most efficient delivery of content given their network layout. The deployment option covered by this paper is one that would be ideal for most corporate network topologies.

The only devices that are installed in the customer network are content engines placed at areas of anticipated high traffic to ensure fast and efficient delivery of content to end users. As new content is added, it is retrieved by the content engine at the main site which then replicates the content to all of the remote locations. The main site likely has the highest concentration of users and therefore should be deployed first. The main site is primarily chosen because of the number of likely users, and this may or may not be the same location as the corporate headquarters, it depends entirely on the customer's layout.

The placement of the devices when using the default scenario is shown in Figure 1.

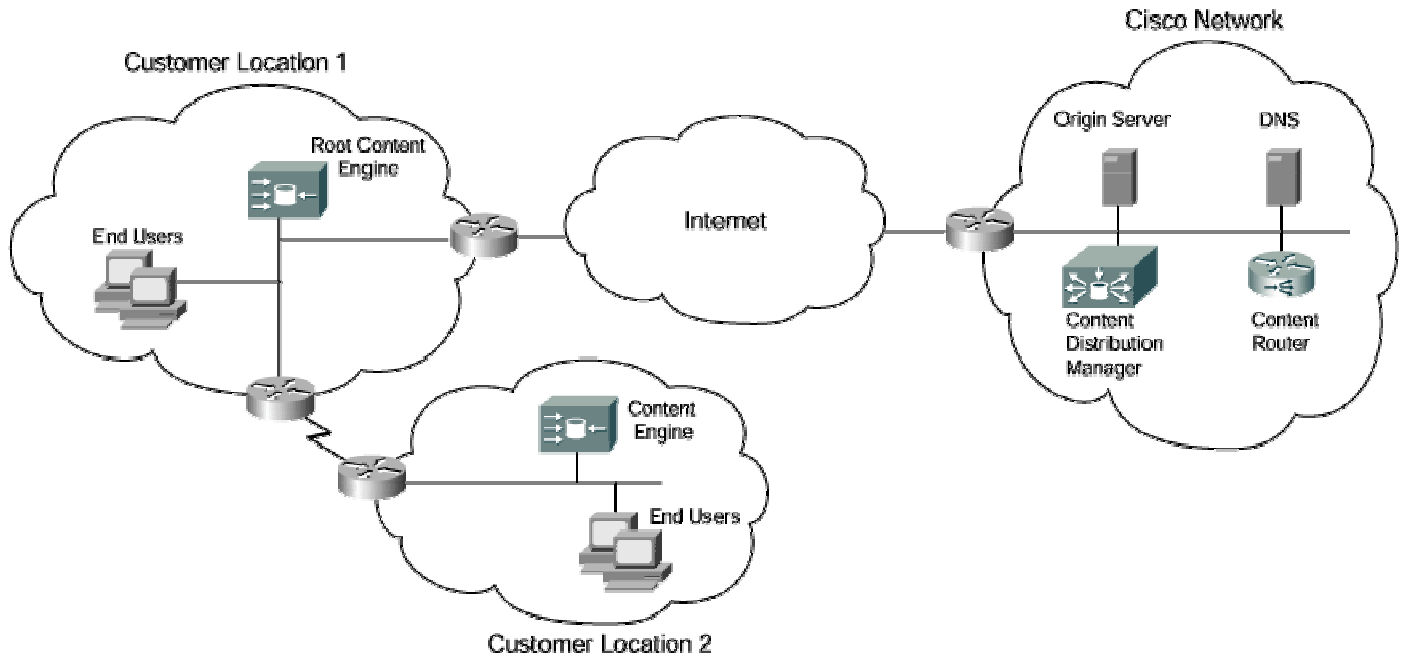


FIG. 1: CDM, CR, Origin Server, and DNS located within Cisco Network, content engines at customer site.


OPERATION AND PROVISIONING

At the main site, there is a CE designated as the “root” CE that contacts the origin server at off-peak hours designated by the customer, and acquires the content to be distributed to other content engines and served to end users. At the remote locations, there is a CE that communicates with the root CE to ensure it has the latest content. For management of the system, a CDM located on the Cisco DMZ is reachable by the customer CEs. The customer CEs contact the CDM at tunable intervals to provide status updates and to ensure synchronized configurations between the CE and CDM.

The CDM is the management platform for the system, providing a GUI based interface that allows for quick provisioning.

The CR acts as the authoritative nameserver for the domains created within the system, and then redirects end users to the closest CE depending upon the IP address of the end user and the “aliveness” or reachability of the CEs. The CE contains the high bandwidth video streams or large files that should not be propagated to end users via costly WAN links.

From the management console of the CDM, content providers, websites, and channels are created. The content provider is provisioned to designate contacts and owners for a particular website. The website is assigned to a content provider, and then within the website the administrator specifies the subdomain that end users will enter into their browser to fetch content. Lastly, channels are created and assigned to a website and contain the information about the content that should be distributed down to the CEs that are subscribed to that channel. Participating companies are each assigned a specific website and channel within the



Cisco Technical Knowledge Library to distinguish their needs and content from other participants. Within the channel, an XML file referred to as a *manifest file* is referenced that instructs the CEs which content should be downloaded and served to end users. In order to populate content onto the CEs, the CEs are assigned to the channel and the main site CE is designated as the root CE. Once a root CE is allocated to a channel, it retrieves the manifest file and then follows the instruction set within manifest and downloads the content directly from the origin server via SSL. Other non-root CEs request the content from the root CE via SSL. Simultaneously, the CR is notified that the CE has subscribed to a particular website and therefore can serve content requested from that website by end users. The website is the fully qualified domain name (FQDN) that is created to direct end users onto the system. This is possible because the website is a subdomain of `ojtfrom.cisco.com` which is served by the DNS server located on Cisco's DMZ (see Fig. 1). Upon request for the address of the newly created subdomain, the DNS server queries the CR, who returns an A record of himself, and the DNS server returns that record to the end user indicating that the website they are requesting is located on the CR. The CR then accepts the HTTP request and redirects the end user to the best CE using another XML file called a *Coverage Zone* file. This file maps end user IP addresses with CEs that are in close proximity to those users.

CONTENT DELIVERY

Once the channels have been created and associated with a website, and content has been placed onto the subscribing CEs, the service is ready to serve end users. The request from the end user is routed using a mechanism called *Simplified Hybrid Routing* which works in the following manner:

1. The end user's browser requests the website `http://<customer>.ojtfrom.cisco.com`
2. The end user's workstation sends a recursive DNS request to its local DNS requesting an IP address for the website.
3. The local DNS begins the address resolution process by querying nameservers. Once it is finally directed to the DNS server located in Figure 1, the DNS server responds to the query with the IP address of the CR located on Cisco's network. This record is an NS record which indicates that the CR is the authoritative nameserver for that subdomain. The user's DNS server then queries the CR, and the CR returns an A record of himself indicating that he is the desired destination. The local DNS server then replies to the original query by sending the A record of the CR to the user's workstation.
4. The workstation then originates an *HTTP GET* for the desired content to the CR.
5. The CR receives the request, and examines the requested subdomain and the source IP address of the requestor. The CR then uses the Coverage Zone file to map the requestor's IP address to a close CE. The CR then checks the aliveness of the CE, and checks to see if that CE contains the domain requested.
6. If the CE hosts the domain and is alive, then the CR sends an *HTTP 302 Temporarily Moved* to the workstation which contains the actual location of the content, the CE. The 302 indicates that the content is now at `http://<cname>.ce.<customer>.ojtfrom.cisco.com`
7. Upon receiving the 302, the workstation sends a new DNS resolution request for the CE indicated by the newly created subdomain.
8. The local DNS resolves the IP address of the content engine via the CR and replies to workstation with an A record of the CE.
9. The workstation sends a new *HTTP GET* to the CE at the address indicated.
10. The CE receives the request and delivers the content to the end user.

CONTENT

Cisco Systems, Inc. and respective content providers retain all copyrights to materials hosted by the Technical Knowledge Library. All content hosted by the Technical Knowledge Library is covered under the AS Non-disclosure agreement (NDA). Subscribing customers are responsible for compliance with the AS NDA with regards to content hosted by the Technical Knowledge Library.

The Technical Knowledge Library content and subsequent content updates are only available through the use of an installed CE managed by the AS Education team, no other method of distribution of Technical Knowledge Library content is available.

CONTENT UPDATES

To maintain the value of the Cisco Technical Knowledge Library, new content is regularly added at off-peak hours, as designated by the customer. The content that is added comes from a variety of sources within Cisco and includes white papers, Video on Demand, and Audio on Demand. These informative documents and video/audio streams cannot be found on Cisco.com.

Content is added to the Technical Knowledge Library as it is harvested or created. To aid in relevant document searches, the Cisco Technical Knowledge Library allows end users to provide feedback on the service and provides the opportunity to request more content on a particular subject. The Technical Knowledge Library team uses content requests from users to help direct and prioritize content harvesting and creation activities.

USER ACCESS

User access to TKL content can be controlled by configuring the installed CE to authenticate to an existing TACACS+ or LDAP server at the customer location. Once configured, the CE will require username and password authentication from all users attempting access TKL content and will allow or deny access based on the authentication server response.

USAGE STATISTICS

In order to assist in tracking the value of the Cisco Technical Knowledge Library, the CEs export their usage logs via SFTP to the Origin Server and the customer is provided with detailed statistics that give exhaustive information about the usage of the service in both table and graphical format. Table 1 and figure 2 show a small sample of the statistics provided.

Table 1:

Statistics		
Hits	Total Hits	168480
	Total Cached Hits	11011
	Average Hits Per Day	619
	Average Hits Per Hour	25
	Average Hits Per Visitor	79.0
	Average Data Transferred per Hit	18.4 KB
Visitors	Total Visitors	2134
	Average Visitors Per Day	7
	Average Time Spent	391 Seconds
	Average PageViews per visitor	11.21
	Average Downloads per visitor	3.87
	Average Data Transferred per Visitor	1455.0 KB
Uniq IPs	Total Uniq IPs	279
	Visitors Who Visit Once	140
	Visitors Who Visit more than Once	139
PageViews and Downloads	Total PageViews	23927
	Average PageViews Per Day	87
	Total File Downloads	8257
	Average File Downloads Per Day	30
	Total Images	110253
	Average Images Per Day	405
	Total failed requests	9047

Total Incomplete File downloads requests	1441
Number of visitors bookmarked your web site	90

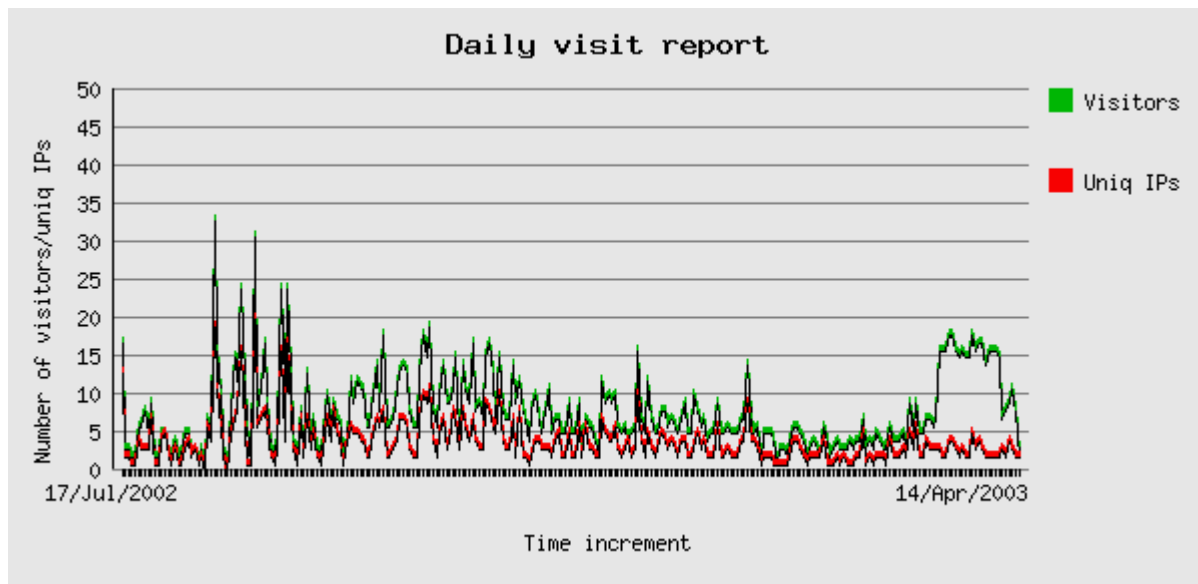


Figure 2: Graphical report of visitors over several months

LOGISTICS

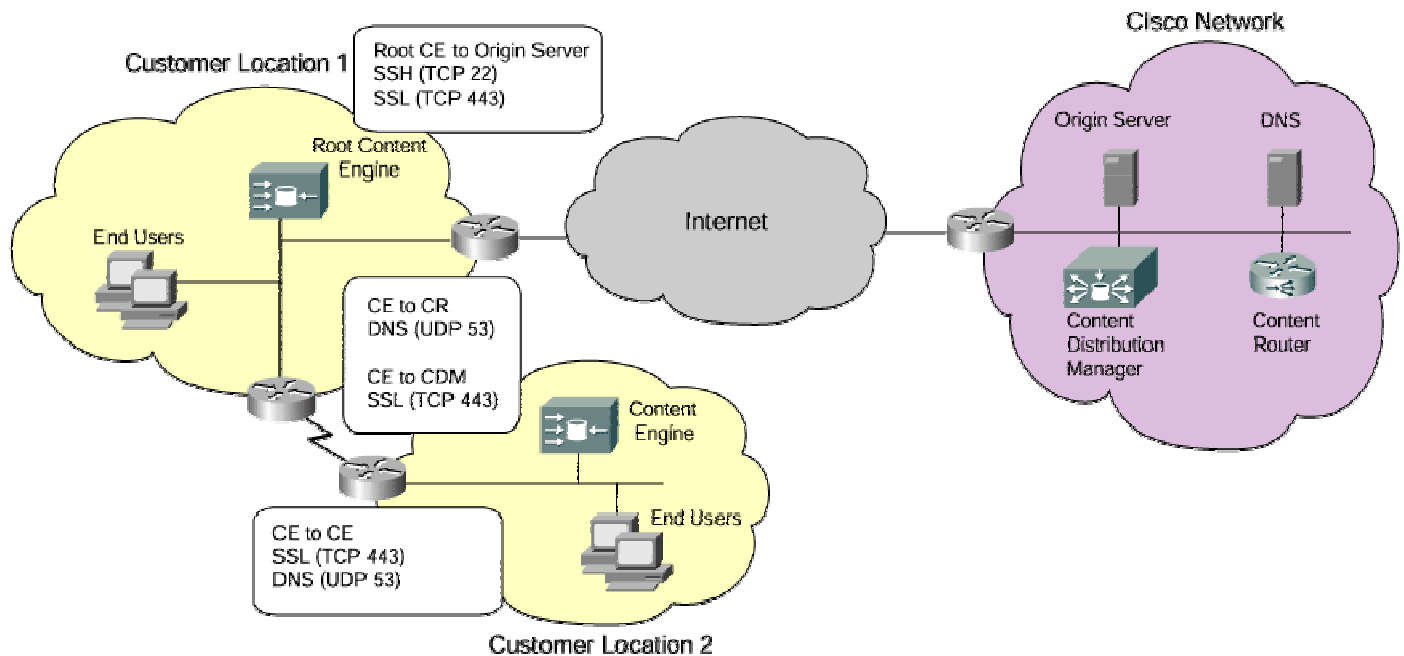
For the main site, the customer needs to supply 1 RU of 19" rack space with 110v AC for the CE565/CE512 root CE. The same rack and power provisions are needed for CEs located at any remote customer sites.

Network connectivity required at each site includes 1 10/100/1000 RJ-45 Ethernet port with 1 internally and Internet reachable IP address. This means that the address provided should allow internal corporate users to originate requests to the CE and the CE itself should be able to originate traffic and therefore establish TCP connectivity out to Cisco's network through the Internet, but external users should not have the ability to originate traffic to the CE.

Connectivity must be in the form of direct access to the internet through firewalls or other gateway devices. **Proxy connections from the CE to the Technical Knowledge Infrastructure are not supported.** Proxy connections, for users to access content from the CE, is supported.

To increase security of the installed CE, it is strongly suggested that access is limited to only the inbound and outbound ports required by the content engine, via the use of firewalls and access lists.

For multiple location installations, the CEs at the main and remote site must have connectivity to each other, as well as connectivity from the CEs to the CDM, CR, and the origin server. The CEs need to have reachability to each other via SSL (TCP 443) and DNS (UDP 53). All CEs need the ability to reach the CDM via SSL, and the CR via DNS (UDP 53) and DNS, while the root CE also needs connectivity to the Origin Server via SSH (TCP 22), and SSL (TCP 443).



Device	Originated	Inbound
Root CE	TCP 22, 443 to 64.102.241.26 TCP 443 to 64.102.241.27 UDP 53 to 64.102.241.22 and .28 TCP 80 to 64.102.241.25	TCP 80 from internal sites UDP 53 from non-root CE
Non-root CE	TCP 443 to root CE UDP 53 to root CE	TCP 80 from internal sites

PROTOCOL REQUIREMENTS

CE outbound to Origin Server

HTTPS / SSL (TCP 443)

TCP port 443 is used for acquisition of content by the CE to the Origin Server.

SSH (TCP 22)

TCP port 22 is used by the CE to upload usage logs to the Origin Server. The transfer is done via SFTP.


CE outbound to Content Distribution Manager (CDM)

HTTPS / SSL (TCP 443)

TCP Port 443 is used for all communications between the CE and CDM. Registration and system updates from the CDM to the CE will use Port 443 which is initiated by the CE.

CE outbound to OS upgrade server (CDM)

HTTP (TCP 80)



TCP Port 80 is used to download the latest ACNS software. Upgrades are invoked by the CDM. The CE then downloads the latest version from the upgrade server and updates itself to the latest version.

CE to Content Router (CR – Multiple Location Installation)

DNS (UDP 53)

UDP port 53 is used by the CE to send keep-alive messages to the CR.

Root CE to CE (Multiple Location installations)

DNS (UDP 53)

In a multiple location installation of the Cisco Technical Knowledge Library, the root CE will act as the origin server and CR for the other CEs within the same channel. In order for request to be routed to non-root CEs at customer locations, UDP Port 53 must be open from the non-root CEs to the root CE for transmission and receipt keep-alives.

HTTPS / SSL (TCP 443)

TCP port 443 will be used for content acquisition by the non-root CE

FOR MORE INFORMATION

For additional information, a copy of the Technical Knowledge Library presentation, a service demonstration, or help with an opportunity, please send an email message to tkl-info@cisco.com.

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International
BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland •
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2007 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Printed in the USA