How Cisco IT Deployed Content Networking to Improve Application Performance and Security

Cisco ACNS deployment lowers costs and improves application performance and network security.

Cisco IT Case Study / Application Networking Services / Enterprise Content Networking System: This case study describes Cisco IT's internal use of Cisco ACNS Software to support Cisco Systems business. The Cisco global network is a leading-edge enterprise environment that is one of the largest and most complex in the world. Cisco customers can draw on Cisco IT's real-world experience to help support similar enterprise needs.

> "Cisco ACNS allows for virtualization of the data center at the network edge. In effect, the content engine acts as a mini data center. Providing LAN-speed access to content normally accessed over a high-latency WAN has improved productivity and user satisfaction."
>
> **– Dan Stolt, Cisco IT ACNS Global Program Manager**

CHALLENGE

Cisco Systems® regularly distributes various types of content to its more than 250 offices worldwide, ranging from live streaming video and video on demand (VoD) to desktop security and antivirus updates, software packages, and configuration policies. Cisco® IT needs its infrastructure to accomplish four functions: video distribution, software distribution, application acceleration through caching of HTTP static content, and HTTP worm and virus blocking. "Until recently, those functions were provided by separate systems," says Koen Denecker, Cisco IT engineer. For example, Cisco previously relied on a dedicated VoD system to deliver video content for product information, training, and executive presentation files, and a separate system to distribute desktop software updates. But by 2003, Cisco had developed a compelling business case for upgrading each of its four systems supporting content.

Video Distribution

Cisco distributes several forms of video content, including live, on-demand, downloadable, and pushed to the desktop. The Cisco VoD systems ran on 140 aging Windows-based servers that needed replacement and were a potential conduit into the LAN for worms and viruses. Distribution of video files devoured WAN bandwidth. Management for the servers was not centralized, contributing to higher administration costs. And replication of videos for positioning on all servers required a full-time employee to spend half of every day on the VoD system.

The rising use of the Cisco IP/TV® solution within the company added to the need for more efficient video content distribution. Cisco IT used Cisco IP/TV systems to allow employees at remote sites to view live streaming video of business meetings and financial reviews over the multicast-enabled WAN. But because the Cisco IP/TV system required its own support, Cisco IT minimized the burden by limiting its use to Windows users. Now Cisco IT wanted to extend the system to all employees, including Linux users, and to eliminate the dedicated support requirement as well.

Software Distribution

The increasing challenges of distributing business-critical software were another incentive to improve software distribution. Different teams at Cisco deliver content to employee PCs using about 20 different channels, including software downloads, desktop OS push, antivirus updates, and others. The software distribution channel, for instance, distributes laptop applications, while the desktop channel distributes the latest versions of application images such as Cisco Aironet® clients, Cisco Security Agent, and others.

A liability of the old methods of software distribution was the inability to assign priority to urgent files. "With more frequent and rapid network threats, it has become crucial for us to more quickly distribute virus update files and urgent software patches to employees around the world," says Jeroen Sourbron, IT project manager.

Application Acceleration Through Caching

To offload traffic from the WAN, Cisco IT caches intranet and Internet HTTP content. In the past, this was done using about 60 cache engines located in remote sales offices in the Americas and Asia-Pacific regions. Cisco IT estimates that these local cache engines reduced intranet and Internet WAN traffic load to local sales offices by 15 to 20 percent. Cisco wanted to retain this benefit of caching and extend it to include applications as well as content, but without the support burden associated with yet another set of dedicated servers.

Caching can also be used for application acceleration, something Cisco previously provided at the Internet edge only. "By providing application caching at bandwidth-challenged remote sites, we would improve application response times and therefore improve employee productivity," says Sourbron. For instance, rather than 60,000 users individually downloading a 400-MB file across the WAN, each site would download it just once, and then individual users could download it across the LAN.

HTTP Worm and Virus Blocking

To screen incoming HTTP traffic for known viruses and to suppress outbound propagation of HTTP-based worms, Cisco IT had deployed cache engines at Internet sites and lab sites. Although successful, this filtering function required a separate cache engine architecture and support structure—just like the other three components of content delivery.

To consolidate its approach to this complex medley of business and technical needs, Cisco IT resolved to build a content network solution that combined the four previously disparate functions: support for video content, software distribution, application acceleration, and HTTP virus and worm filtering. The solution: Cisco Application and Content Networking System (ACNS) Software.

SOLUTION

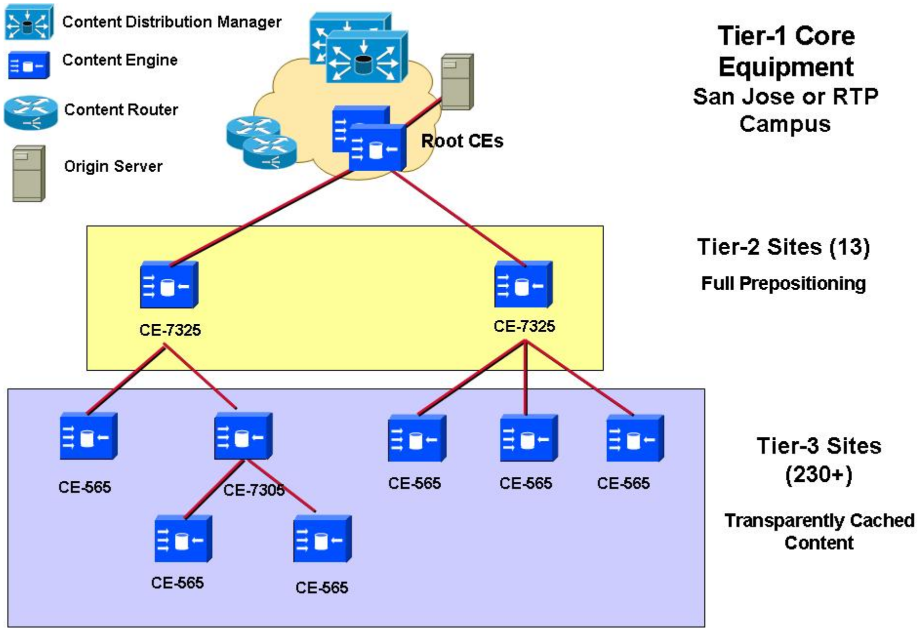
Cisco ACNS Software resides on content engines—multifunction plug-and-play appliances that eliminate the administrative burden and capital costs of deploying dedicated distributed file and application servers. "Cisco IT prefers commercial solutions when available, and Cisco ACNS met all our business and technical needs," says Sourbron. "If there were no Cisco ACNS solution, we'd need to glue together multiple commercial off-the-shelf software and homegrown solutions to acquire all the functions we wanted."

Cisco ACNS Software provides the following functions for Cisco:

- Content distribution and management for video, applications, patches, virus definition files, and more
- Content routing, or transparently redirecting end users to the best edge-delivery device based on location and content
- Edge delivery, including:
- Demand pull-caching, in which content is stored on the content engine after the first time it is requested
- Content pre-positioning, in which the content is positioned on the content engine for retrieval in anticipation of the first request

- Stream splitting for accelerated delivery of Web applications, objects, files, and real-time streaming video and audio media
- Content screening, or blocking known HTTP-based virus and worm content

Figure 1. Cisco ACNS Software Solution: Three-Tiered Architecture



Three-Tiered Architecture

Cisco IT designed its Cisco ACNS solution with a three-tiered architecture for content distribution (see Figure 1). Content is pushed from a central origin server to dedicated root content engines, where it is replicated for the 13 Tier-2 hub sites. High-priority content, such as security updates, is also pushed to more than 230 Tier-3 content engines deployed at Cisco remote sales and engineering sites.

Business groups within Cisco identify content that should be made available to all employees, such as training information, product updates, or antivirus software. This content is pushed from the origin server to content engines at the Tier-2 hub sites. When users at these sites request large files for the first time, the local content engine intercepts the request. If the content was pre-positioned, the local content engine serves it from the disk; otherwise it requests the content from Tier 2 and then serves subsequent requests from the disk.

Only one content engine is deployed at each site, a departure from the usual Cisco solution architecture. The reason is that another content engine is available at the nearest Tier-2 hub site, and this Tier 2 content engine will support any remote site until the content engine is working again.

Tables 1 and 2 summarizes the functions and composition of the three tiers.

Table 1. Content Functions by Tier

Tier	Function	Location	Content Caching	Content Distribution	Streaming Media	HTTP Worm/Virus Filtering
1	Management, routing, content acquisition	San Jose, California, with backup in Research Triangle Park, North Carolina		X		
2	Content distribution and serving	13 major sites		X	X	
3	Edge caching and limited pre-positioning	Other Cisco offices	X	X	X	X

Table 2. Equipment by Tier

Tier	Name	Equipment	Number	Capacity (2004)
1	Content Distribution Manager	CE-7305	2	N/A
1	Content Router	CE-7305 and CE-565	5	N/A
1	Root Content Engine	CE-7305 / CE-7325	4	432 GB
2	Hub Content Engine	CE-7325	16	432 GB
3A	Large Site Content Engine	CE-7305	9	432 GB
3B	Small Site Content Engine	CE-565A	230+	144 GB

Tier 1: Management, Routing, and Acquisition

Tier 1, located in San Jose, California, includes the following:

Cisco ACNS Content Distribution Manager (CDM) *software* provides centralized management and provisioning, both for pull caching and pre-positioning. Cisco IT staff, as well as the channels that provide content, use the CDM Web-based interface to configure and monitor content replication and devices. There is one CDM in San Jose California, and a backup CDM in Research Triangle Park, North Carolina.

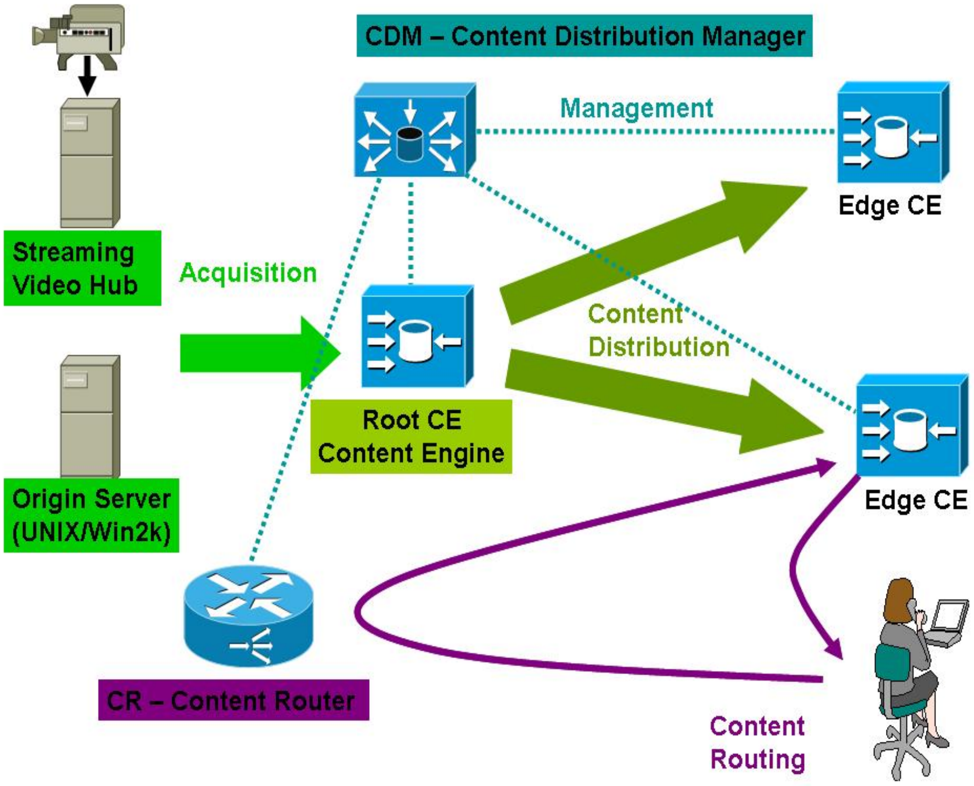
Cisco ACNS content routers redirect users to the closest Tier-2 content engine by simplified hybrid routing, which uses a combination of domain name server (DNS) resolution and HTTP 302 redirects. There are five content routers in the Cisco ACNS network.

Origin servers are owned and maintained by content owners. Cisco root content engines acquire content from origin servers. The origin server can use any operating system that is accessible by FTP, HTTP, HTTPS, Trivial File Transfer Protocol (TFTP), or common Internet file system (CIFS), including operating systems such as Microsoft

Windows, Linux, and Sun Solaris. For ease of administration, content can be assigned to virtual groups called channels.

A streaming video hub generates a digital video from an analog signal. “Live streams originate from a studio encoder, stream to the Tier-1 content engines, and then are split into multicast or unicast streams over the network to users,” says Daniel Stolt, Cisco IT’s global program manager for the Cisco ACNS system. “VoD streams originate at an origin server, then are acquired and distributed to the Tier-2 content engines by several channels.”

Figure 2. Tier 1 Equipment and Functions within the ACNS Network



After discussing acquisition and distribution policies with the content owner, Cisco IT specifies policies such as distribution schedules using the CDM interface. For certain content, Cisco IT has configured the system to periodically check with the origin server to look for content additions and deletions. Policies define the following:

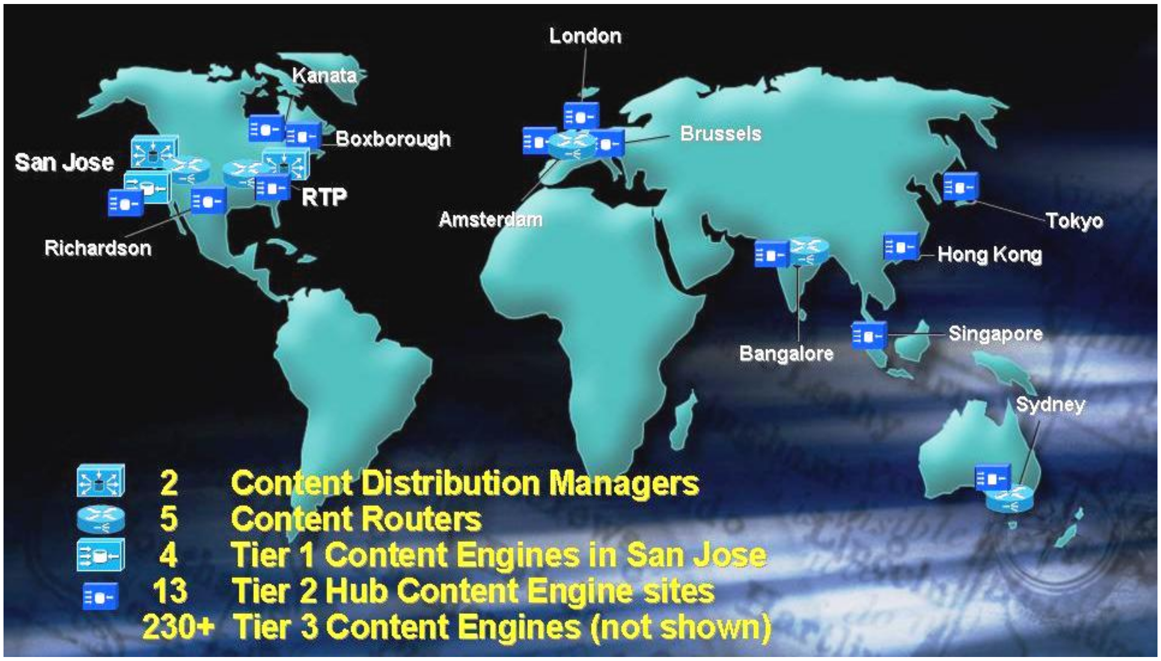
The bandwidth that the Cisco ACNS network is allocated on the WAN. Live streaming media content is allowed at any time of the day, and more content—and larger files—can be pushed over the WAN at night.

Content that is pushed to specific Tier-2 content engines, often based on the global region. Some content is location-specific, such as content written in different languages.

Content freshness, or “time to live,” which directs content engines to delete content that has passed its expiration date.

Content priority. Certain channels have higher-frequency acquisition and distribution schedules, and receive higher priority for content replication. For instance, antivirus updates, which can change every 15 minutes, have higher priority than desktop images, which change only once per quarter.

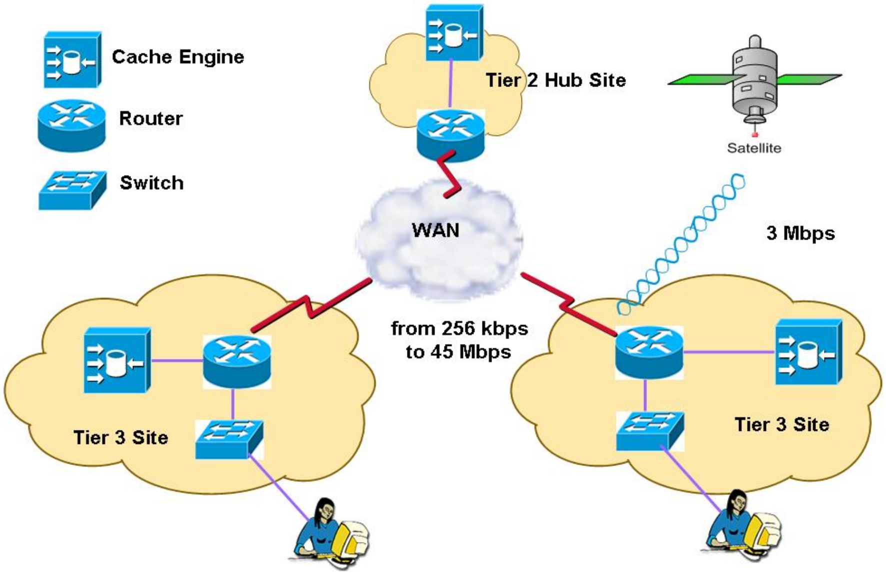
Figure 3. Tier 2 Network Topology


London
Kanata
Boxborough
Brussels
San Jose
RTP
Amsterdam
Richardson
Tokyo
Hong Kong
Bangalore
Singapore
Sydney
2 Content Distribution Managers
5 Content Routers
4 Tier 1 Content Engines in San Jose
13 Tier 2 Hub Content Engine sites
230+ Tier 3 Content Engines (not shown)

Tier 2: Content Distribution and Serving

Cisco maintains too many video files to provide them all at every Cisco site. Instead, Cisco maintains them only at the 13 Tier-2 sites in large offices worldwide (see Figure 3). Tier-2 sites are equipped with high-end Cisco 7325 content engines because they provide the performance and disk space to generate and store large volumes of video content.

Figure 4. Tier 3 Network Topology at Edge Offices



Tier 3: Edge Caching and Limited Pre-positioning

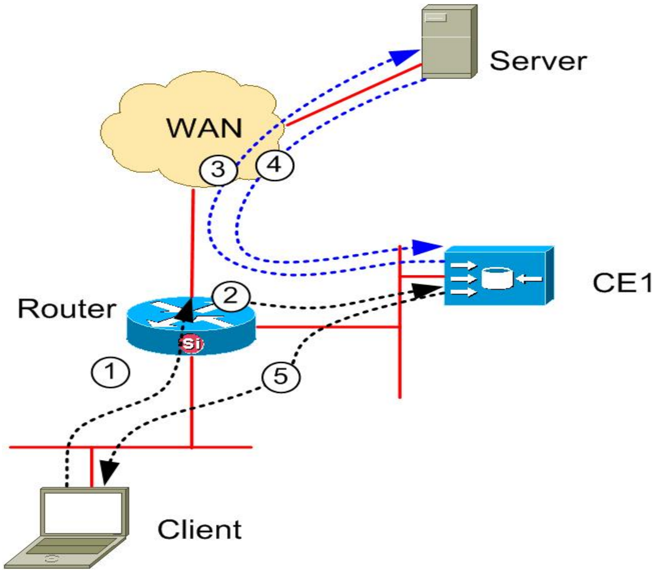
Tier 3 includes most remaining Cisco sites, approximately 230 (see Figure 4). Sites with more than 400 employees use the Cisco 7305 Content Engine, which redirects employees' content requests with Web Cache Communication Protocol (WCCP) and accepts pre-positioning of content from local channels. The smaller offices use the Cisco 565A Content Engine, which also redirects using WCCP but accepts pre-positioning only for desktop software. The majority of the content that Tier-3 sites serve to local users is cached: when the first user requests the content, it is downloaded across the WAN, and subsequent requests are served from the local disk. All Tier-3 content engines support streaming video connections for both Windows and Linux clients, overcoming a limitation of Cisco's previous video solution.

"Every Cisco office has a content engine with Cisco ACNS Software because every office needs to download software upgrades, and making them available locally spares the WAN," says Denecker. For Tier-3 sites, Cisco IT had also considered deploying content engine network modules for Cisco 2600, 3600, and 3700 series routers, but ultimately decided to use the Cisco 565A Content Engine because it had greater disk capacity at the time. "Entry-level ACNS content engines mitigate the bandwidth challenges that our smaller sites face," says Sourbron. "It makes more sense for us to push software upgrades and video files to these offices just once, rather than risk having inadequate disk space on the network module."

User Experience

Content can be proactively pre-positioned (placed on the Tier 2 or occasionally the Tier 3 content engine by the administrator, in preparation for an expected large demand. This is done for commonly downloaded items like virus .DAT updates. Content can also be reactively cached at the Tier 3 content engine, after the first user requests static content from an origin server and has it delivered to their location. When a Cisco user requests content already present on the local Tier-3 content engine, the content is delivered at LAN speeds. When a user requests content that is not present on the local content engine, the request is routed over the WAN to a Tier-2 content engine or another remote origin server. The user's experience is the same whether the content is served locally or remotely. If the content has not been cached, the following steps occur in the background (see Figure 5):

Figure 5. Steps for Delivering Non-Local Content to the End User



The router intercepts the request sent by any of the following protocols: HTTP, FTP over HTTP, Domain Name System (DNS), Microsoft Media Server (MMS), and Real Time Streaming Protocol (RTSP).

The router redirects appropriate traffic to the content engine through WCCP.

The content engine requests the content from the origin server.

The origin server serves the content directly to the content engine, where it is cached to disk.

When enough data has been received to begin serving, the employee begins receiving it through the content engine cache. Subsequent requests for the same content, from any user in the same facility, are also served from the cache.

Cisco sometimes pushes high-demand content, such as software, to the Tier-3 content engines to relieve WAN congestion during business hours. Stolt says, “WCCP can access this content even though it wasn’t acquired through the caching process.”

Configuration

To simplify configuration, Cisco IT established device groups for all content engines in the same tier. Changes to the device group apply to all content engines in the group. To enable caching in Tier-3 devices, for instance, Cisco IT uses the CDM interface to select the device group, selects the caching options just once, and then pushes the configuration to all devices with one command.

Table 3. Content Channels and Example Characteristics

Channel	Owner	Quota	Priority	Refresh Rate
desktop	Desktop team	20 GB	Medium	24 hours
patches	Desktop team	100 MB	High	6 hours
antivirus	Security team	20 MB	High	15 minutes
images	Desktop team	10 GB	Low	1 week
vod	Communications Media team	200 GB	Medium	24 hours

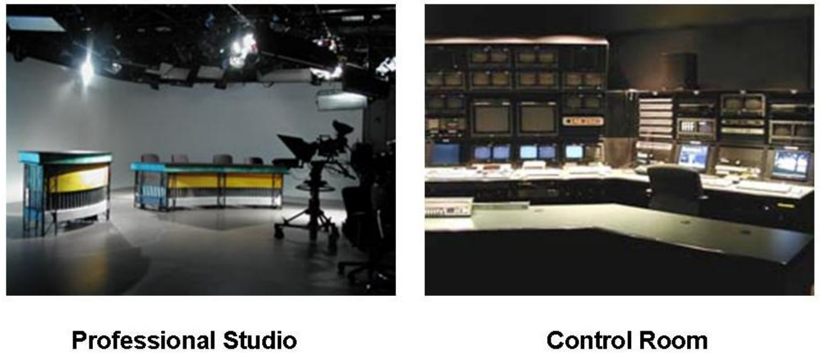
Content Priorities

Cisco assigns priorities to the different channels (see Table 3), reserving top priority for the antivirus channel. The priority affects how soon the new file is distributed to desktops. For example, new desktop application files are made available for downloads on the next business day, while new antivirus update files are available in just 20 to 30 minutes. “We don’t want nonurgent jobs to fill bandwidth,” says Sourbron. “Sending a multigigabit video file to Beirut over its 256-Kb link might take days. We’ve set it up so that if a virus update file becomes available during that time, it receives priority.”

Use with Streaming Video

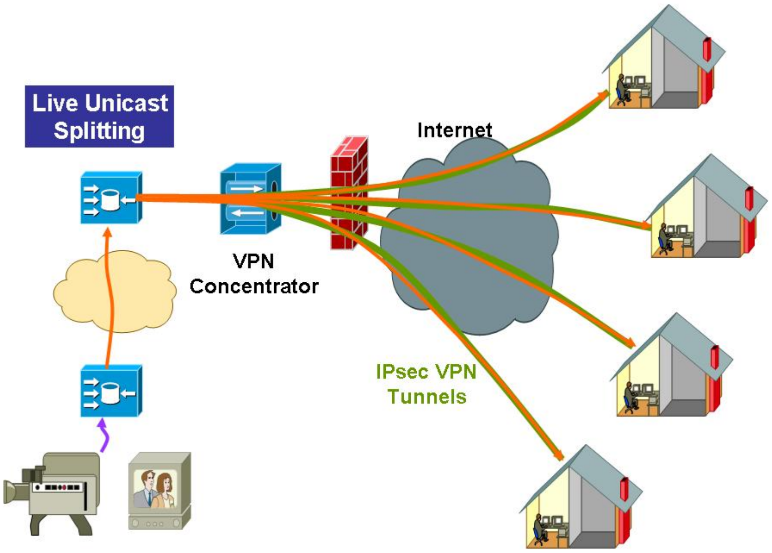
Cisco ACNS Software supports MPEG, Windows Media Technologies, RealVideo, and QuickTime streaming video for employee training, real-time corporate communications, and customer relations. Many organizations within Cisco use Cisco ACNS in conjunction with the Cisco IP/TV solution, which provides live MPEG streaming. The Cisco IP/TV solution captures the live event and Cisco ACNS distributes it as a VoD to the remote site for later viewing.

Figure 6. Streaming Video Studios



Cisco supports 40-50 live streaming video events every month, with about 250 people watching (see Figure 7). Cisco broadcasts Cisco-wide quarterly events, and various business groups broadcast quarterly or annual meetings to communicate updates in corporate vision and direction. Live video events like this are essential to keeping a global organization working together smoothly. Cisco maintains professional studios and a professional video crew to support events like this. Live events are multicast across the LAN and WAN to avoid overloading the origin server and WAN links.

Figure 7. Unicast Traffic Splitting for Remote Access



Remote access VPN links (see Figure 7) cannot support multicast, however, and the VPN concentrator splits the multicast traffic into live unicast streams sent along each individual secure VPN tunnel across the Internet.

Figure 8. Video On Demand (VoD) Studios

Group VOD Studio

Individual VOD Studio

Cisco creates 400 – 500 Videos on Demand every month (see Figure 7). Some of the VoDs are created in studios with professional crews; and others are self-serve VoDs created by individual subject matter experts in single-person video booths. Over 70,000 VoD viewers are used by Cisco employees and contractors to learn new material and keep up to date with the vast technical knowledge required in their jobs. Over 27,000 VoD files have been accumulated over three years, equaling over 250 Gigabytes of content. A good deal has also been “aged” and removed from circulation. These VoDs are prepositioned at each Tier 2 hub content engine, and cached at Tier 3 content engines when they are requested by users at the Tier 3 site.

Deployment Process

Implementation began in early 2003, when Cisco IT staff built the Tier-1 content engines and the Tier-2 sites. In the Europe, Middle East, and Africa (EMEA) region, Cisco outsourced implementation. “When Cisco deploys something new for the first time, we use our own resources and proceed slowly so that we can learn and document best practices,” says Denecker. “After that we involve outsourced engineers and hand over the documentation to them. This has been a best practice in EMEA for years.”

In EMEA, the team first pre-staged the 55 Cisco ACNS content engines for the Tier-3 sites, loading and configuring the basic software in Brussels and then shipping the boxes to Cisco offices throughout the region, from South Africa to Dubai to Sweden. At their destinations, the outsourcing partner rack-mounted the boxes and provided basic network connectivity. Then the engineers in Brussels downloaded the remaining software through the CDM. Sourbron says, “This step-by-step process allowed us to save on travel costs for the skilled engineers, use local resources from the outsourcing partner for rack-mounting and network connectivity, and still maintain a high level of quality through central verification.” The caching functionality became available immediately when each device went live, whereas other functions, such as streaming video and VoD distribution, became available for all sites after the global rollout was completed.

In May 2004, a mere three weeks after the devices arrived in Brussels, all 55 sites in EMEA were operational. The deployment was equally rapid for 35 sites in the Asia-Pacific region and 150 sites in the Americas. “We attribute the rapid deployment to preplanning, including logistical details like having the right people to escort the boxes through customs,” says Denecker. “The centralized management of the Cisco CDM allows for global deployment by centralizing device configurations and licensing, which is normally difficult to maintain in a distributed environment.”

RESULTS

Return on Investment

Cisco IT in EMEA alone expects a return of $511,000 in year one, $517,000 in year two, and $657,000 in year three. Factors contributing to rapid return on investment include:

- **Reduced support costs—** Decommissioning the VoD servers eliminated the $61,300 spent annually on outside support contracts.
- **Reduced storage requirements —** Cisco IT eliminated more than 30 terabytes of storage space dedicated to VoD by replacing it with Cisco ACNS video caching, reducing Cisco IT storage costs by about $3 Million..
- **Server replacement cost avoidance —** By eliminating the need to replace 140 aging servers over two years, Cisco saved a one-time cost of approximately $1.4 million.
- **Reduced content replication costs —** Content replication required one-half of a full-time employee annually. That cost has been entirely eliminated because the management is automated and integrated into the global support process.
- **Delayed bandwidth upgrade —** By caching HTTP traffic over the WAN, the Cisco ACNS system postponed the need to upgrade Cisco's WAN in EMEA. Similar savings are expected in South and Central America and parts of the Asia-Pacific region. "We reduced HTTP traffic by about 10 to 15 percent, and HTTP traffic accounts for 10 to 20 percent of bandwidth usage," says Denecker. Because the bandwidth upgrade cycle is once every two or three years, Cisco IT EMEA expects to achieve cost reduction in year three, with savings between $250,000 and $750,000.
- **Reduced costs for virus and worm remediation —** By replacing Windows-based servers with Cisco content engines, Cisco IT anticipates savings of $100,000 to $350,000 per outbreak, for global savings of $500,000, according to Stolt's estimate.
- **Increased availability —** After the last major Priority 1 (P1) outage related to slide downloads, Cisco IT was asked to evaluate the use of Cisco ACNS for offloading central Web servers. "IT implemented ACNS in less than a week, and subsequently there have been no more P1 outages caused by slide downloads," says Stolt. "We estimate the cost savings at $150,000."

Lower Infrastructure Management Costs

Cisco ACNS Software has greatly simplified management at remote Cisco offices, avoiding incremental costs for installation and changes. "Say we have a content engine in a remote site like South Africa," says Denecker. "The local office only needs to connect the box to a console, make a few simple configuration changes to make the engine talk to a local browser, and from then on it's part of the Cisco global configuration network. All subsequent changes are made centrally, from the CDM."

For Cisco IT staff worldwide, changes have become a simple matter of logging in to the CDM GUI and selecting the new configuration, which is pushed automatically to the selected group of content engines. For example, suppose Cisco decides to no longer cache a particular application, or needs to specify which content engines should receive content from a new channel. "With a single click of a button we can upgrade 250 ACNS devices overnight," says Sourbron. "With other platforms, we'd be looking at many hours, if not days, spent logging in to each device individually. It's a powerful way to manage."

The Cisco ACNS team in Brussels can even delegate certain configuration and control to channels such as e-learning or security. Cisco business groups can load their content on the origin server and then log in to the CDM themselves to monitor distribution. "Internal business channels no longer have to ask IT about the progress of their content distribution," says Denecker. "And if distribution is not proceeding as planned and the problem is in their area, they can more quickly take action."

Enhanced Software Distribution

Before Cisco deployed Cisco ACNS Software, providing fast software updates was hindered by manual content replication. That is, Cisco IT had to create one copy of each software image file, patch, video file, or other type of content. The task consumed half of a full-time employee's time. Now Cisco ACNS Software automates the replication process, freeing that person to focus on other tasks.

The Cisco ACNS solution also mitigates the bandwidth drain of distributing large files. For instance, Cisco EMEA recently migrated its user base to Microsoft Office 2003, a 300+ MB file, and the other regions are in the process of migration. Distributing a 300-MB file individually to 40,000 employees at more than 230 sites would have consumed 12 terabytes, bringing the WAN to a crawl in many areas. Instead, Cisco sent the file once to each site, consuming just 70 gigabytes of bandwidth. "Content distribution on a large scale like ours requires a content distribution network," says Denecker.

"Central management and transparent replication of content with ACNS makes it just as easy to distribute software to 60,000 desktops as to 60," says Dave Stafford, IT analyst for desktop engineering "What's more, by making software content available at LAN speed, the ACNS solution dramatically decreases the time needed to completely reinstall all software on a laptop or desktop PC. Laptop rebuilds at local LAN speed take 90 minutes, compared to 8 hours over the WAN."

The Cisco ACNS network also supports automatic virus definition file updates. Cisco employees' PCs automatically check for virus updates during boot and once a day, with about 40,000 hits on the virus definition file servers globally. Whenever virus definition file updates (average size 180 Kilobytes) or new virus detection engine updates (average size 1.9 Megabytes) are available, users' antivirus client automatic requests are redirected via content routing to the regional Tier 2 content engine. If the user is at a Tier 3 site, WCCP intercepts the update request and the update is served directly from the Tier 3 content engine. This redirection spares the virus definition file servers, and spares the WAN from having to transport 32 Gigabytes of duplicate file updates, as well as significantly hastening the virus update process. Whenever new viruses appear and spread with amazing speed across the Internet, Cisco Information Security pushes out new virus updates directly to each laptop, using the ACNS network. Within minutes each PC is alerted to download and install the new virus definition files from the local Content Engine (again sparing the virus definition files, the WAN, and the users' time). The new virus definition files immediately begin screening all emails for the new viruses, repairing or deleting the infected files. This ability to respond immediately to proactively block virus infections before they sweep through an enterprise network can save millions of dollars in damages and remediation efforts.

HTTP Worm and Virus Filtering

When Cisco identifies a new HTTP worm or virus, a Cisco IT staffer simply logs into the CDM and stipulates that requests containing the virus signature be dropped. "If someone in, say, New York is infected, we can effectively stop the virus from crossing the WAN and going to Toronto or South America," says Denecker. The Cisco content engine with Cisco ACNS Software is a component of the SAFE Blueprint for enterprise architecture from Cisco for mitigating network and application security threats.

Integrated Streaming Architecture for Video

Video distribution is far simpler and more flexible with the Cisco ACNS solution than in the past. Cisco uses real-time streaming video for corporate communications, e-learning, live events such as executive presentations, and marketing updates. The company typically also produces video files and makes them available on demand after the event. In addition, for short videos such as important 2-minute messages from executives, Cisco pushes these 200-MB video files to the desktop, where they pop up automatically. All types of video content are made available on all

Tier-2 content engines. Tier-3 engines push video as well as select VoD content. Cisco developed an early VoD distribution system, and estimated that Cisco averages $115M in savings based on productivity and travel avoidance per year by using online learning and communications tools.

Enhanced Productivity Through Application Acceleration

The Cisco ACNS solution has increased sales productivity by reducing the time that sales personnel spend connected to the sales portal from an average of 3 hours per week to 2 hours, a reduction of 33 percent. “In the past, running e-sales from South Africa might take 1 to 2 minutes for each click because application components had to be downloaded,” Sourbron says. “Now, with caching, that time is reduced to 10 to 20 seconds.”

NEXT STEPS

Next steps for the company’s Cisco ACNS solution include the following:

- Standardizing device management to the point where it can be outsourced
- Extending the Cisco ACNS network to partner sites, such as outsourced support engineers who staff the Cisco Technical Assistance Center (TAC)
- Extending the network to Executive Briefing Centers (EBCs) so that the presenter can schedule a video using the CDM interface
- Distributing new software being developed in support of Cisco IT’s new Oracle 11i ERP upgrade
- Using satellite rather than terrestrial links for distribution of content to Tier-2 sites—“Satellite will be used for both live multicast media broadcasts and multicast replication during off hours,” says Stolt
- Publishing all VoD files in both Windows Media and RealVideo formats to support Linux as well as Windows clients
- Offering more Data Center services like file services at the network edge.

“Cisco ACNS allows for virtualization of the data center at the network edge,” says Stolt. “This allows centralized management and resources. In effect, the content engine acts as a mini data center. Providing LAN-speed access to content normally accessed over a high-latency WAN has improved productivity and user satisfaction.”

LESSONS LEARNED

“In the past, a clear division separated the networking and hosting teams,” says Denecker. “ACNS blurs the distinction, so it is essential to identify people with both types of skills who can resolve different types of problems.”

From its thousands of applications, Cisco identified a few that are incompatible with caching. “Try to do testing before you enable caching everywhere in the network,” says Sourbron.

Stolt offers the business perspective: “Make collaborative decisions with content providers about which content to pre-position, where, and for how long. Building good relationships with content providers helps avoid any issues about content presence or quotas.”

“As we continue to collapse more replication architectures into a single ACNS network,” Stolt says, “we’re distributing content using less WAN bandwidth, making it available more quickly, cutting management costs, and providing better protection against network threats. ACNS is the Swiss Army knife for IT, providing a collection of tools that span networking, security, hosting, data centers, and the desktop. In this way it brings the experience of being at the data center to Cisco employees around the world.”

Table 4. Glossary

Term	Definition
ACNS	Application and Content Networking System
CDM	Content Distribution Manager – provides a centralized management system for both content acquisition and distribution, managing Content Engine policy settings and configurations, and monitoring network nodes.
CE	Content Engine -- serves client requests for content.
Content Channels	Logical set of content based on information given for that content's acquisition and distribution, like the "antivirus" channel with Antivirus DAT files, the "desktop" channel with software packages, or the "vod" channel with Video on Demand files
CMS	Configuration Management System
Content	A file or media stream which may be requested, and may be on-demand, pre-loaded, pre-positioned, or live
Content Provider	Information identifying the provider of the content, including contact information
Coverage Zone	Defined in an XML file, information identifying which CEs will service which clients
CR	Content Router -- redirects client requests for content to the closest Content Engine containing that content.
Device group	Grouping of devices sharing some common configuration(s)
Edge	Located near the requesting client
Forwarder	The CE in each location responsible for distribution to downstream CE's
Fully Qualified Domain Name (FQDN)	The full name of a system: its local hostname followed by its domain name, e.g. videohost1.cisco.com, as given by the local Domain Name System (DNS).
Live content	A content stream (typically streaming media) being broadcast from an origin server, like IP/TV or Real content
Location	A logical grouping of CEs
Manifest file	An XML file providing information and rules for acquiring and serving content
Multicast cloud	A CE that multicasts the content, and a list of CEs that will receive that multicast
On-demand content	Content that is acquired, cached, and delivered by the local CE because of a user request
Playlist	Definition of content to be played out a video-out equipped CE
Pre-loaded content	Content retrieved to an individual CE because the administrator scheduled a retrieval in anticipation of user requests
Pre-positioned content	Content that is delivered through a network of CEs because the administrator has configured acquisition and distribution in anticipation of user requests.
Replication	Distribution of content from one CE to another
Request	Communication from a device to retrieve content
Root CE	The CE that acquires the content from the source, and begins distribution
Simplified Hybrid Routing (SHR)	A content routing technology used to route content requests to the nearest Tier2 CE; SHR uses the Domain Name System (DNS) to ensure that the Content Router receives all requests for content from the Tier 2 CE. Once the Content Router receives these requests, it can redirect the end user to the content.
Sprayer	A source of streaming content, such as HTTP, Real, WMT, and RTSP/RTP services
Web Cache Communication Protocol (WCCP)	The Tier 3 enterprise router uses WCCP to detect and intercept client requests for content and route these requests to a Content Engine within the same network.
Website	Information identifying the origin server, and the FQDN clients will use to request content through ACNS

FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**