Cisco ACNS Software Version 5.0

Cisco Application and Content Networking System (ACNS) Software

The Cisco Enterprise Content Delivery Network, running Application and Content Networking System (ACNS) Software, enables organizations of all sizes to reduce costs, drive productivity and increase revenues by extending strategic applications from the data center to the branch including:

- Content and application acceleration
- Access management and security
- Video streaming
- Corporate communications
- E-learning
- Point-of-sale kiosks and video display
- Software and file distribution

Cisco ACNS Software combines the technologies of demand-pull caching and pre-positioning for accelerated delivery of Web applications, objects, files, and streaming media; and runs on Cisco Content Engine (Network Module and appliance), Content Distribution Manager, and Content Router hardware platforms.

Together with Cisco’s content delivery hardware platforms, intelligent Cisco ACNS Software provides the following business-critical functions:

- Content-edge delivery using the Cisco Content Engine appliance or Cisco Content Engine network module to avoid WAN congestion by storing and delivering content at the network edge
- Central management capabilities using the Cisco Content Distribution Manager (CDM) appliance
- Content routing capabilities using the Cisco Content Router appliance for HTTP routing and using the Web Cache Control Protocol (WCCP) embedded in routers and switches with Cisco IOS® Software

For turnkey “live” and on-demand streaming, customers can use the Cisco ECDN solution in conjunction with Cisco’s IP/TV® 3400 Series of appliances, which capture and deliver standards-based MPEG video with synchronized presentations, program creation, scheduling, and interactive QuestionManager features.

In the data center, Content Engines can be used with the Cisco 11500 Series Content Services Switch (CSS) and the Catalyst®
6500 Series Content Switch Module (CSM) for reverse proxy caching, which offloads expensive, backend web servers.

Figure 1. Depicts Key Applications using Cisco ACNS software

Multiple Intelligent Content Services at the Edge

Cisco Content Engines

Running ACNS Software, Cisco Content Engines (CEs) combine the benefits of demand-pull caching and pre-positioning (intelligent content push) of HTTP and streaming media in dedicated appliances or router-integrated network modules for Cisco 2600, 3600 and 3700 series routers. Cisco CEs feature unsurpassed network integration for ease of management, deployment, and access management. Cisco CEs typically reside in headquarters, branch offices, remote campuses, and international sites where WAN bandwidth is costly and scarce, as well as data centers and Service Provider points of presences (PoPs).

CE Network Modules offer the additional benefits of lower total cost of ownership, a smaller footprint, and ease of deployment and management with no performance degradation to the IP routing services. For more information on the CE Network Module:
Advanced HTTP Content Serving for Content and Application Acceleration

The Cisco Content Engine delivers content served over HTTP, whether the content was stored in the content engine via demand-pull caching or pre-positioning. A central management interface, the Cisco Content Distribution Manager (CDM), controls the policies of content expiration, user authentication, bandwidth controls, and transaction log aggregation for both demand-pulled and pre-positioned content.

Robust proxy-caching policies and rules are provided with the “rules template.” When a content request pattern match is triggered based on URL, HTTP header, port number, or IP address, a corresponding action is taken, such as “no-cache,” refresh, redirect, HTTP header-field rewrite, object freshness control, selective cache, upstream proxy and outgoing proxy selection policies, or blocking of any files that may have viruses or worms.

Extensive quality-of-service (QoS) support via type of service/differentiated services code point (ToS/DSCP) bits enables differentiated network usage for business-critical applications. Cisco ACNS Software is unique in its ability to set the DSCP bits in ToS (supported in routers with Cisco IOS Software) based upon cache hits and misses, URL, file type, and domain. Cisco ACNS Software augments network-based QoS provisioning for traffic queuing, shaping, and engineering with a high level of granularity by intelligently “coloring” packets with content-based information. For example, organizations can prioritize mission-critical applications over less productive Internet browsing.

Cisco ACNS Software enables several flexible network deployments. IP Spoofing (supported in WCCP mode) allows the client’s IP address to be passed through to the origin server to allow for easy tracking of users and authentication policies. Split DNS permits the content engine to be configured with multiple Domain Name System (DNS) servers based on domain name, such as intranet or Internet. DNS Caching allows the content engine to cache DNS entries to avoid multiple WAN accesses for DNS server resolution.

A Comprehensive Security Gateway

ACNS software provides a number of robust security functions:

- **Authentication**—Authentication via Remote Authentication Dial-In User Service (RADIUS), Lightweight Directory Access Protocol (LDAP) Version 3, and Terminal Access Controller Access Control System Plus (TACACS+) provides user and administrative access control. User authentication is also supported end-to-end for Windows NT LAN Manager (NTLM) authentication to enable a single NT network logon for users to access protected Web objects within the NT domain. NTLM and LDAP group authentication are also supported to authenticate users against group membership with Active Directory compatibility. For HTTP transactions, Cisco ACNS also provides the option for the content engine to be authenticated against an authentication server local to the content engine’s network to reduce the amount of WAN traffic required to contact a remote authentication server.

- **URL filtering**—Cisco ACNS Software, in conjunction with N2H2 Internet Filtering Protocol, Secure Computing SmartFilter, or Websense Enterprise Software, enables administrators to block, monitor, and report on end users’ access to non-business and objectionable content for increased productivity, lower bandwidth usage, and reduced legal liability.

- **Antivirus Proxy and Worm Blocking**—By using proxy rules, content engines can be used to block malicious viruses and worms such as Code Red and Nimda. Rules can also be set up for the content engine to forward client requests to antivirus servers to process and for the content engine to store and serve only “clean” content.
Industry-Leading Multiformat Streaming Media Support

- Streaming media protocols supported by Cisco ACNS Software on content engines include RealNetworks Real-Time Transport Protocol/Real-Time Streaming Protocol (RTP/RTSP), Microsoft Windows Media Technologies (WMT) and Microsoft Media Server Protocol, Apple QuickTime for standards-based MPEG streaming, and HTTP-streaming delivery of MPEG, Advanced Streaming Format (ASF), and QuickTime Movie (MOV) format files.
- Live, scheduled rebroadcasts and on-demand streaming enables applications such as corporate communications, e-learning, PoS advertising, and kiosk video displays. Video-on-demand (VOD) streaming allows users to view programs when they want and have VCR-like controls such as fast-forward, rewind, pause, and more. Live and scheduled rebroadcast streaming enables real-time broadcasts using IP multicast or stream splitting, facilitating streaming across the existing network infrastructure while optimizing bandwidth usage whenever multicast is enabled.
- The integrated video decoding enables customers to use their Cisco ECDN system for distributing, controlling, and playing back MPEG files to National Television Standards Committee (NTSC) and Phase Alternating Line (PAL) analog displays. The Cisco ECDN offers a new and cost-effective way to deliver advertising to retail sites, cafeterias, lobbies, and more. Playlists are managed from the Cisco CDM Web browser interface for the integrated video-decoder card option in the content engine. Figure 2 shows the playlist functionality.

Figure 2. The playlist
IP multicast support uses Cisco IOS Software on Cisco routers to allow one stream to be tuned in by many users over the same network segment and the routers to replicate the one stream to multiple network segments. This allows live and scheduled video programs to be scaled to a wide audience with low bandwidth usage.

Stream splitting is supported for portions of the network that are not multicast enabled, where unicast streams from origin servers are sent to "splitter" CEs, which in turn resend the stream by multicast or unicast to multiple connected users. In addition, Cisco ACNS Software is also unique in its ability to receive streams by multicast into the splitter CE, which in turn resends the stream by multicast or unicast to multiple connected users.

Stream proxy mode allows CEs to cache streaming-media content and act as proxies to reduce congestion to the origin server. This mode is used if content originates from an external source such as the Internet, beyond the control of the enterprise or organization.

Stream server mode allows the CE to deliver streaming-media content as if it is an origin server. This mode is mainly used if the enterprise creates or controls its own content. Content is pre-positioned in the content engines through the CDM. In this mode, CEs can provide live stream splitting, IP multicast streaming, and VOD.

**Scalable Content Acquisition and Distribution**

A key innovation in Cisco ACNS Software v5.0 is the concept of "virtual import" using manifest files, which dramatically simplify the content acquisition and delivery process, and improve scalability.

Configured at the CDM, the manifest file holds a list of defined origin URLs to be used for content acquisition, as well as all the acquisition and distribution policies. These include bandwidth, time-of-day and priority used for acquisition, bandwidth throttles and scheduling for distribution over the WAN and bandwidth throttles for serving content on the LAN, content freshness or "time to live," and user-authentication requirements. These policies can be set up on any Web server. For further automation, the manifest file can be set up to automatically "crawl" the origin server for additions and deletions at certain defined time periods.

Configurable "Root CEs" are assigned with the task of acquiring content from origin servers using the manifest file and HTTP, Secure HTTP (HTTPS), or File Transfer Protocol (FTP). Once the Root CEs acquire content from the origin server, they also distribute the content to its children CEs. For further scalability and load balancing, up to four levels of hierarchy, including the root content engines, can be configured for distribution. This reduces the number of content engines requiring distribution support from the root content engines, and minimizes the amount of traffic that may have to traverse across the WAN. Content engines are then grouped into "locations" that are a set of well-connected content engines. A location leader content engine and its backup content engines can be statically defined by the administrator (for example, based on the capacity of the content engine and the network link speed). If no location leader is defined, the system uses its internal algorithm to pick the location leader. If the location leader fails in this case, another content engine will be automatically selected as the new leader. This provides a fault-tolerant content-distribution system.
Superior Content and Network Management

Cisco Content Distribution Manager

The Cisco Content Distribution Manager (CDM) provides highly scalable, secure, remote management and provisioning of all supported content delivery services for both demand-pull caching and pre-positioning. The Cisco CDM provides the centralized Web-based graphical user interface (GUI) for administrators to configure and monitor content and devices for content acquisition, distribution, and serving.

Content is first grouped into channels, which are logical groupings for content distribution and consumption at the CDM. The channels are based on geography, organizational units, etc. Content engine devices are then configured to subscribe to one or more channels of content. This allows for optimal content distribution and storage. For ease of management, content engine devices can be grouped, so policies can be applied across multiple devices at the same time. The Cisco CDM GUI also provides monitoring and status of content acquisition, replication, and serving. Figure 3 shows the CDM GUI.

The Cisco CDM supports multiple customizable administrative roles, such as network manager roles or content provider roles for different business units. These roles have different administrative logins and passwords. This allows multiple administrators to access the CDM remotely from different locations, each having different levels of access rights. The GUI is protected with HTTPS for login, and administrative authentication is supported with RADIUS, TACACS+, and locally defined authentication. In addition, Cisco CDM registers all devices in the Cisco ECDN using public/private key infrastructure, and all inter-device communication and content distribution is carried over HTTPS to ensure network security. For business resilience, a redundant warm standby CDM can be configured to mirror all the configurations defined in the primary CDM. The robustness of the Cisco CDM allows service providers to provide a managed service for enterprises and organizations that want outsourced management.

Figure 3. The CDM GUI
Reliable Multicast Replication

In addition to unicast content distribution, Cisco ACNS Software supports a multicast-replication option for reliable, efficient file transfers and rich-media replications using satellite and multicast-enabled terrestrial infrastructures. Certain content engines can be configured to be multicast transmitters and the children content engines are configured to be multicast receivers. Reliable multicast transfers take advantage of the efficiency of multicast to allow one distribution to be received by many content engines simultaneously.

Rich CDM Application Programming Interfaces

For greater automation and manageability, Cisco ACNS Software v5.0 introduces a new set of XML-based application programming interfaces (APIs) to allow third-party publishing and reporting applications to interoperate with the CDM. These APIs are accessed via HTTPS and offer the same network security and access control features of the CDM GUI. APIs include:

- Management of acquisition and distribution including replication status, channel creation, deletion and modification, content engine channel assignment and removal, “add a manifest,” and “fetch manifest now”
- Configuration information for Web sites, channels, content engines, content providers, device groups
- Streaming and HTTP transaction statistics

Integrated Network Management

In addition to the CDM GUI, a command-line interface (CLI) similar to the CLI of Cisco IOS Software can also manage Cisco content engines for ease of configuration and problem diagnosis for network managers. The content engines support the robust management features that are standard in Cisco IOS Software, including Telnet, Secure Shell (SSH) Protocol, syslog, Simple Network Management Protocol (SNMP) Versions 2 and 3, TACACS+, Network Timing Protocol (NTP), and more. The local content engine GUI is also preserved to allow for local diagnosis and configuration testing.

The Cisco content engine and Cisco CDM are also supported by CiscoWorks. CiscoWorks is complementary to the Cisco CDM and is a common tool to manage content engines together with Cisco routers, switches, and other networking devices for device CLI configuration, configuration inventory, syslog analysis, and device troubleshooting.

The Cisco content engines also support SNMP v2 and v3 Management Information Bases (MIBs) for HTTP and streaming media statistics, hardware resources, and events with customizable traps. This allows content engines to work with standard SNMP management packages to provide comprehensive management support.
Logging and Reporting

Cisco ACNS Software provides comprehensive, industry-standard system, audit, and transaction logs. HTTP transactions are logged via Squid log and W3C-compliant Apache common log formats. Streaming-media logs are also generated with W3C-compliant logs for Windows Media and Real format logs for Real Media. These logs provide Web usage information that can be turned into customizable performance and activity reports via commercial reporting tools. Figure 4 shows sample reports.
Flexible Client Request Redirection Choices

Cisco ACNS Software v5.0 offers multiple methods for client requests to be intelligently directed to the most appropriate content engine. Customers can choose one or all of the following methods depending on their network infrastructure and preference:

- Transparent Edge Intercept using Web Cache Communication Protocol (WCCP)
- Nontransparent Edge Intercept using a browser proxy configuration
- Content routing using HTTP redirect

Transparent Edge Intercept with WCCP

Cisco pioneered WCCP, the industry’s first content-routing technology. With WCCP, a router with Cisco IOS Software transparently redirects specified traffic to local content engines, reducing WAN bandwidth usage for maximized content-serving performance and availability. WCCP is an open protocol that is supported within Cisco IOS Software in Cisco routers, and within Cisco ACNS Software in the content engine. This technology enables the content engines to store and deliver content locally to users without requiring changes to the existing network architecture, URLs, client browsers, or end servers. Cisco ACNS Software offers the most advanced implementation of WCCP Version 2:

- Scalable clustering—Enables each content engine cache member to work in parallel, greatly improving scalability, redundancy, and availability. Up to 32 content engine cache members can be clustered to scale for the desired capacity. "WCCP flow protection" prevents breaking of existing flows when the WCCP cluster load distribution changes because of the addition or subtraction of a content engine. "WCCP slow start" prevents cluster destabilization when a new content engine is added to a heavily loaded content engine cluster.
- Fault tolerance—Enables dynamic failover to other content engine cluster members if a content engine fails. If all content engines in a cluster fail, the WCCP-enabled router dynamically turns off WCCP and forwards content traffic directly to the origin server. In addition, content engines support "WCCP multi-homing," which allows a WCCP-enabled, multigroup Hot Standby Router Protocol router pair to share a content engine cluster, creating a fully redundant caching system. If a router fails, existing Cisco IOS Software fault-tolerant and fail-safe mechanisms are applied. For example, a hot standby router could dynamically take over operations, redirecting Web requests to the cache cluster.
- Fault prevention—Content engines can achieve fault prevention for network-or application-level problems. "Overload bypass" prevents a content engine from becoming a bottleneck when traffic loads exceed the capacity of a content engine. "Dynamic client bypass" prevents source-IP authentication problems by selectively allowing clients to directly connect to origin servers.
**Non-Transparent Edge Intercept Using Browser Proxy Configurations**

Non-transparent Edge Intercept uses either a Proxy Automatic Configuration (PAC) file or is set on an individual basis on the client Web browsers to use the specified content engine (local content engine) as an outgoing proxy for content (such as port 80 and others). Cisco ACNS Software v5.0 supports Non-Transparent Edge Intercept both for demand-pull caching and pre-positioned content.

**Content Routing Using HTTP Redirect**

Organizations or even specific locations that do not support Edge Intercept mechanisms can use powerful Cisco content-routing technology to intelligently redirect client requests for pre-positioned content using the source-IP address of the client desktops. Each Cisco ECDN system can support up to eight geographically dispersed Cisco Content Routers for scalability and redundancy. At the CDM, the administrator configures the location of the coverage zone file, which specifies the client source-IP addresses. The CDM then sends the coverage zone, content engine, and channel-subscription information to the content router, which uses its algorithm to construct the routing table. The CR is assigned as the authoritative DNS for a predefined, ECDN-specific, fully qualified domain name. The content router then uses DNS to intercept the request, consults the coverage-zone routing tables and determines which CE is closest and available to the client’s IP address. The CR then responds to the client with an HTTP redirect to request content from the specified content engine. Redirection works through firewalls and Network Address Translations (NATs), preserving network security.

The important benefit of this system is that the redirections are precise so that CEs can be provisioned with different channels of content and the right content to serve their communities of users. This in turn optimizes local bandwidth, storage, and throughput capacity that the CEs serve.
## Table 1  Key Features of Cisco ACNS Software v5.0

### HTTP Serving
- Demand-pull caching features:
  - Forward and reverse proxy caching
  - Transparent (WCCP v2), nontransparent (browser proxy configuration), and Layer 4 redirection
  - HTTP 1.0 and 1.1 Web caching, File Transfer Protocol (FTP) over HTTP proxy, HTTPS tunneling, Internet Cache Protocol (ICP), proxy mode
  - Rules template for cache policies and rules
  - IP spoofing that present clients’ IP addresses for easy tracking of users
  - Split DNS that allows a content engine to be configured with multiple DNS servers based on domain name, such as intranet and Internet
  - DNS caching allows the content engine to cache DNS entries to avoid multiple WAN accesses for DNS server resolution
- Web content preloading via CLI or local Web GUI:
  - Preload HTTP, FTP, and Multimedia Messaging Service (MMS) files with URL list for a small number of content engines
  - Bandwidth and type of service/differentiated services code point ToS/DSCP controls for preload, day-of-week and time-of-day scheduling, replication status, authentication support
  - ToS/DSCP set by cache hit or miss, URL, file type, domain to classify traffic using cache rules template
  - Pre-positioned content: HTTP delivery of static files for any file format, including PDF, Flash, Shockwave, etc.

### Streaming-Media Support
- Concurrent streaming of Real, Windows Media Technologies (WMT), Darwin, and HTTP
- Live splitting (auto setup with tree structure), IP Multicast, and VOD can all be delivered in both Proxy and Server for Real and WMT
- Rule-based filtering for MMS and Real-Time Streaming Protocol (RTSP)
- Streaming bandwidth throttles and time-of-day for all streaming protocols
- VOD server for standards-based MPEG-4, MPEG-2, MPEG-1, and QuickTime video over RTP/RTSP to Apple QuickTime players (no additional license fee)
- RealSystem 8 Proxy and Server Subscriber: (additional license fee)
  - Certified by RealNetworks, certified RealSystem-powered
  - RealNetworks RTP/RTSP delivery
  - Live-stream pull splitting (unicast in, multicast or unicast out) and push splitting (multicast or unicast in)
  - Encoder failover
  - Content pre-positioning for VOD streaming in Server Subscriber mode
- Microsoft WMT v4.0 Server and Proxy: (additional license fee)
  - Windows Media MMS delivery over TCP, UDP, or HTTP
  - Content pre-positioning for VOD streaming
  - Variable bit-rate support
  - Multicast sourcing
  - Supports live-stream pull splitting, including multicast or unicast into the content engine and multicast or unicast out of content engine to connected clients
  - Certified by Microsoft
- HTTP streaming delivery of MPEG, ASF, and QuickTime Movie format files
- MPEG video display for retail kiosks:
  - Predefined play lists with multiple video clips and time-of-day setting, centrally managed by CDM, multiple playlists per content engine
  - One video stream per AV-decoder card option or content engine-507/560-AV (integrated MPEG-1 and -2 decoders, National Television Standards Committee [NTSC] and Phase Alternating Line [PAL] TV output)
  - Set Top Box interoperability
Table 1  Key Features of Cisco ACNS Software v5.0 (Continued)

**Management**

- Content acquisition and distribution:
  - Content acquisition via Virtual Import from origin servers by root content engines for HTTP, HTTPS, and FTP
  - Channel-based acquisition and distribution control with bandwidth-shaping, priority, scheduling, content expiration, and authentication policies specified in the Manifest File. Content distribution is done by HTTPS
  - Enhanced tree distribution hierarchy for scalability and optimal performance
  - Multicast replication option available (additional license fee)
- Client request redirections:
  - Transparent Edge Intercept with advanced WCCP Version 2: includes scalable clustering (WCCP flow protection, WCCP slow start), fault tolerance (WCCP multihome router support), fault prevention (overload bypass, dynamic client bypass), TCP tuning knobs, and WCCP standby mode for easy maintenance
  - Non-Transparent Edge Intercept with browser proxy configuration
  - Content routing with DNS Intercept and HTTP redirect
- CLI similar to Cisco IOS Software for individual content-engine and CDM-configuration management
- Extended SNMP Version 2 and Version 3 MIBs
- Local content engine Web GUI, SSH Version 1, and Telnet access
- CiscoWorks2000 Resource Management Essentials (RME) Version 3.4 support of content engines and CDM: CLI editor, inventory, netconfig, syslog analyzer, device availability
- Transaction logging and log pushing via FTP
- HTTP cache transaction logs, Squid logs, W3C-compliant Apache common logs
- W3C-compliant common logs for WMT streaming
- Real streaming logs

**Content Access Management and Network Security Policies**

- Authentication
  - RADIUS, TACACS+, and LDAP Version 3 client support
  - Full NT LAN Manager (NTLM) authentication: NTLM object caching, NTLM pass-through, and user authentication for WMT streaming
  - NTLM and Lightweight Directory Access Protocol (LDAP) group-authentication support
- URL filtering
  - Websense Enterprise Version 4.3 client content-filtering support on content engine—Requires separate server from Websense
  - Secure Computing SmartFilter Version 3.1 server and client content-filtering support (additional license fee)—On-box content-engine solution that does not require separate SmartFilter server. Admin Console Version 3.1 is enhanced for central device policies and LDAP group-authentication support
  - N2H2 Internet Filtering Protocol Version 1.0 client content-filtering support on content engine—Requires separate N2H2 Sentinel server from N2H2
Ordering Information

Table 2 lists the major system and value added software options available. Note all the software options must be ordered in with their corresponding hardware platforms identified in the Content Engine Datasheet at: [http://www.cisco.com/en/US/products/hw/contnetw/ps761/products_data_sheets_list.html](http://www.cisco.com/en/US/products/hw/contnetw/ps761/products_data_sheets_list.html).

### Table 2  Cisco ACNS Software v5.0 Part Numbers

<table>
<thead>
<tr>
<th>Software Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF-ACNS-5.0-K9</td>
<td>Cisco Application and Content Networking Software v5.0</td>
</tr>
</tbody>
</table>

**Value-added Software Options**

<table>
<thead>
<tr>
<th>Value-added Software Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF-CE510-RCPS-8.0 (=)</td>
<td>RealSystem 8 combined proxy/server for Cisco CE-510</td>
</tr>
<tr>
<td>SF-CE565-RCPS-8.0 (=)</td>
<td>RealSystem 8 combined proxy/server for Cisco CE-565</td>
</tr>
<tr>
<td>SF-CE7305-RCPS-8.0 (=)</td>
<td>RealSystem 8 combined proxy/server for Cisco CE-7305</td>
</tr>
<tr>
<td>SF-CE7320-RCPS-8.0 (=)</td>
<td>RealSystem 8 combined proxy/server for Cisco CE-7320</td>
</tr>
<tr>
<td>SF-NM-RCPS-8.0 (=)</td>
<td>Combined RealSystem 8 Proxy and Subscriber for Cisco NM-CE-BP-20G-K9, NM-CE-BP-40G-K9, and NM-CE-BP-SCSI-K9</td>
</tr>
<tr>
<td>SF-CE507-RCPS-8.0 (=)</td>
<td>RealSystem 8 combined proxy/server for Cisco CE-507</td>
</tr>
<tr>
<td>SF-CE560-RCPS-8.0 (=)</td>
<td>RealSystem 8 combined proxy/server for Cisco CE-560</td>
</tr>
<tr>
<td>SF-CE590-RCPS-8.0 (=)</td>
<td>RealSystem 8 combined proxy/server for Cisco CE-590</td>
</tr>
<tr>
<td>SF-CE7320-RCPS-8 (=)</td>
<td>RealSystem 8 combined proxy/server for Cisco CE-7320</td>
</tr>
<tr>
<td>SF-WMS-56 (=)</td>
<td>Windows Media software 56 Mbps</td>
</tr>
<tr>
<td>SF-WMS-84 (=)</td>
<td>Windows Media software 84 Mbps</td>
</tr>
<tr>
<td>SF-WMS-168 (=)</td>
<td>Windows Media software 168 Mbps</td>
</tr>
<tr>
<td>SF-WMS-224 (=)</td>
<td>Windows Media software 224 Mbps</td>
</tr>
<tr>
<td>SF-WMS-560 (=)</td>
<td>Windows Media software 560 Mbps</td>
</tr>
<tr>
<td>SF-WMS-1008 (=)</td>
<td>Windows Media software 1008 Mbps</td>
</tr>
<tr>
<td>SF-CE-510-TL-5.0 (=)</td>
<td>Multicast Client Replication software for Cisco CE-510</td>
</tr>
<tr>
<td>SF-CE-565-TL-5.0 (=)</td>
<td>Multicast Client Replication software for Cisco CE-565</td>
</tr>
<tr>
<td>SF-CE-7305-TL-5.0 (=)</td>
<td>Multicast Client Replication software for Cisco CE-7305</td>
</tr>
<tr>
<td>SF-CE-7325-TL-5.0 (=)</td>
<td>Multicast Client Replication software for Cisco CE-7325</td>
</tr>
<tr>
<td>SF-CE-507-TL-5.0 (=)</td>
<td>Multicast Client Replication software for Cisco CE-507</td>
</tr>
<tr>
<td>SF-CE-560-TL-5.0 (=)</td>
<td>Multicast Client Replication software for Cisco CE-560</td>
</tr>
<tr>
<td>SF-CE-590-TL-5.0 (=)</td>
<td>Multicast Client Replication software for Cisco CE-590</td>
</tr>
<tr>
<td>SF-CE7320-TL-5.0=</td>
<td>Multicast Client Replication software for Cisco CE-7320</td>
</tr>
<tr>
<td>SF-SMF12</td>
<td>Secure Computing SmartFilter 12-month subscription (pricing option by number of users)</td>
</tr>
<tr>
<td>SF-SMF24</td>
<td>Secure Computing SmartFilter 24-month subscription (pricing option by number of users)</td>
</tr>
</tbody>
</table>
For further details on hardware options, spares and orderability information refer to the Content Engine Datasheet at:
or

Web Cache Communication Protocol Support

The Web Cache Communication Protocol (WCCP) is a free software feature in Cisco IOS Software that runs on the following Cisco platforms: Cisco 7x00 series routers, uBR 72xx Universal Broadband Router, Cisco 6400 Node Route Processor (NRP), Cisco Catalyst 6x00 Multilayer Switch Feature Card (M SFC), Cisco Catalyst 5x00 Route Switch Module (RSM), Cisco AS5800 Access Server, Cisco AS5300, Cisco 4x00/M, Cisco M C3810 Multi-Point Controller, and Cisco 3600, 2600, 2500, 1700, and 1600.

WCCP v2 is available in the following and later Cisco IOS Software releases: 12.2, 12.2(x)T, 12.1, 12.0(3+)T, 12.0(11+)S, 12.1(13)E. WCCP v1 is available in the following Cisco IOS Software releases: 12.2, 12.2(x)T, 12.1, 12.0, 12.0T, 12.0S, 11.1(18+)CC/CA, 11.2(13+)P.

Cisco Systems Service and Support Solutions

Cisco support solutions are designed for one purpose—to ensure customer success through the delivery of a suite of proactive solutions. Cisco services and support include planning, design, implementation, operational, and optimization solutions. By including services and support with Cisco equipment purchases, customers instantly gain access to a wealth of resources. Cisco service and support solutions enhance the customer’s network investment, reducing the cost of doing business, among other benefits.

Additional Resources

Ordering: For more information, visit:

Cisco ECDN Hardware—Cisco Content Engines:

Cisco Content Engine Network Module:

Cisco Content Switches:
http://www.cisco.com/go/contentswitch
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 • 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 © 2003, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. 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. (0301R)