



Subscriber Control and Billing with the Cisco Content Services Gateway

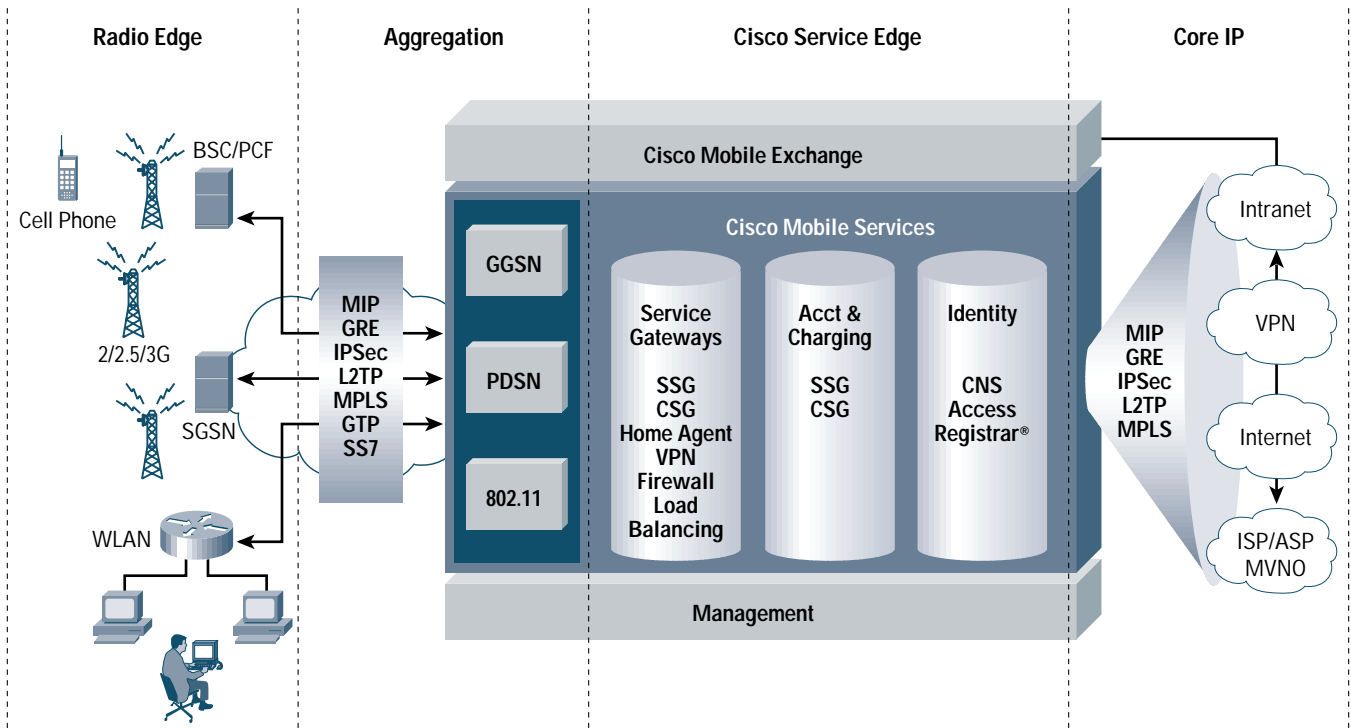
The Cisco® Content Services Gateway (CSG) is the ideal application for service providers seeking to control subscriber access to services and provide pricing capabilities that differ per service or per event. CSG enables their systems to provide advanced processing of IP flows through dynamic content examination, subscriber service access control, and subscriber account balance enforcement in a highly scalable, robust package.

The Cisco CSG is a high-speed processing module that brings subscriber awareness and control to the Service Edge. The CSG can provide a host of different service control and billing functions. Some of the more intriguing opportunities include support for content related billing of Web-enabled applications and such diverse protocols as Wireless Application Protocol (WAP). Other billing applications include support for prepaid billing, the dominant billing method for most of the world's mobile phone subscribers. The value of CSG doesn't stop with advanced billing capabilities, it can also be used for data mining and to support lawful intercept requirements in those countries where such capabilities are mandated.

CSG use in the Cisco Mobile Exchange (CMX) Framework

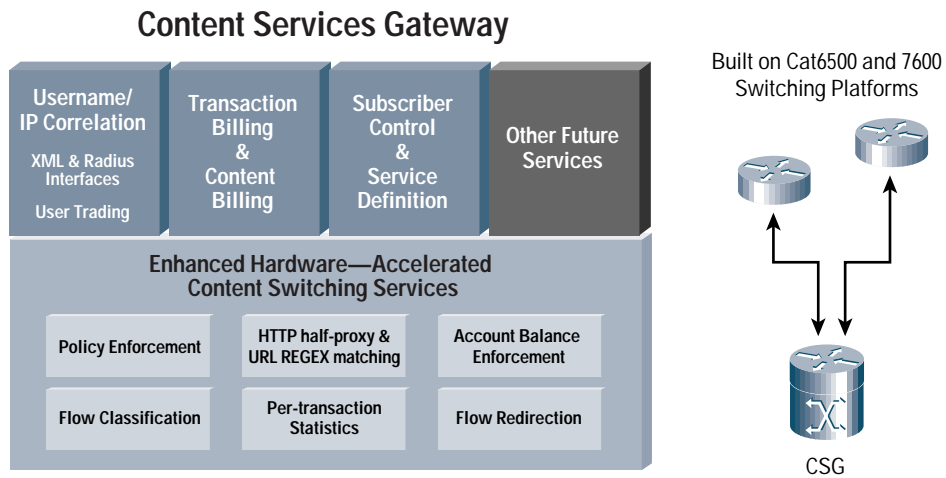
CSG is equally at home in wired and wireless networks. In wireless networks CSG provides the billing component of the Cisco Mobile Exchange (CMX). The CMX is a standards-based framework that links the radio access network (RAN) to IP networks and their value-added services. It is comprised of a number of different components (see Figure 1), including packet gateways, mobile services, load balancing, and network management services delivered on a range of Cisco platforms and application modules. Together, these components successfully address the many challenges that face mobile network operators as they seek profitability from their 2G, 2.5G, or 3G mobile packet infrastructures and their 802.11 public WLAN hotspots.

Figure 1 – CMX Framework



The CSG inserts in the Services Edge between the packet gateways (GGSNs and PDSNs) that terminate the radio access network, and the IP networks that provide the value added services. This whitepaper will review in detail some of the interesting billing and data mining capabilities of the CSG platform. For more information on the lawful intercept capabilities in the CSG please see your local Cisco account representative.

Figure 2 Content Services Gateway



1.0 Advanced Functions: Subscriber and Service Control

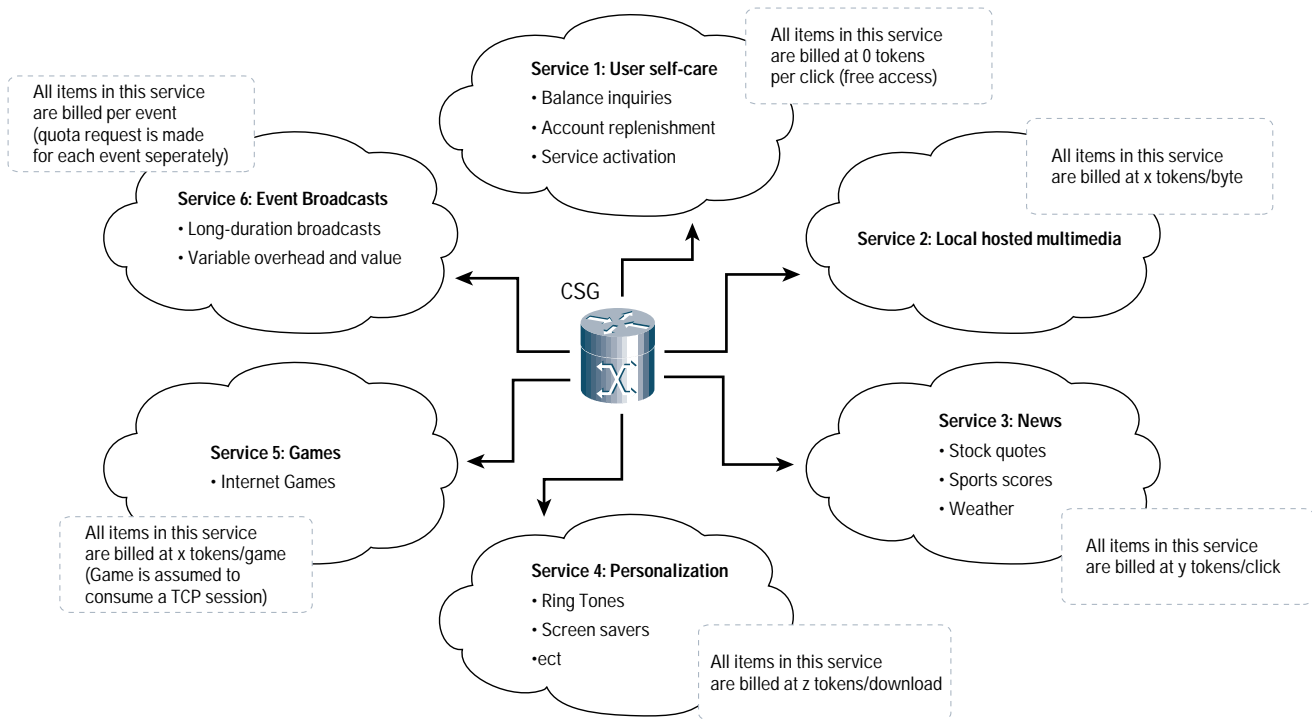
Service Definition and Access Control

For managed subscribers the Cisco CSG allows the grouping of URLs, HTTP content types, server IP addresses, server port numbers, and protocol numbers into sets called "services." A "managed" subscriber is one who must be authorized for a service before the data request is allowed to proceed, and who's per service can be blocked under the direction of the billing system. Access to a service is blocked until the subscriber is authorized to continue by the billing system. Multiple services can be used concurrently, and each is managed separately for each subscriber. Once a subscriber has been authorized, CSG reports subscriber service access attempts, usage, and enforces subscriber limits per service. CSG service definitions are very flexible in that they can contain wildcards in the form of URL regular expressions or masks for destination addresses, ports, and protocol.

Balance Management and Prepaid Billing

The Cisco CSG can be configured to meter subscriber usage such that the subscriber is not allowed to exceed the balance specified by the billing system. Each service a subscriber accesses can have a different balance and can be billed at a different rate, including provisions for free services as well as services that provide a credit. Billing per event (per click) and by volume are both supported (refer to Figure 3).

Figure 3 Billing per Service



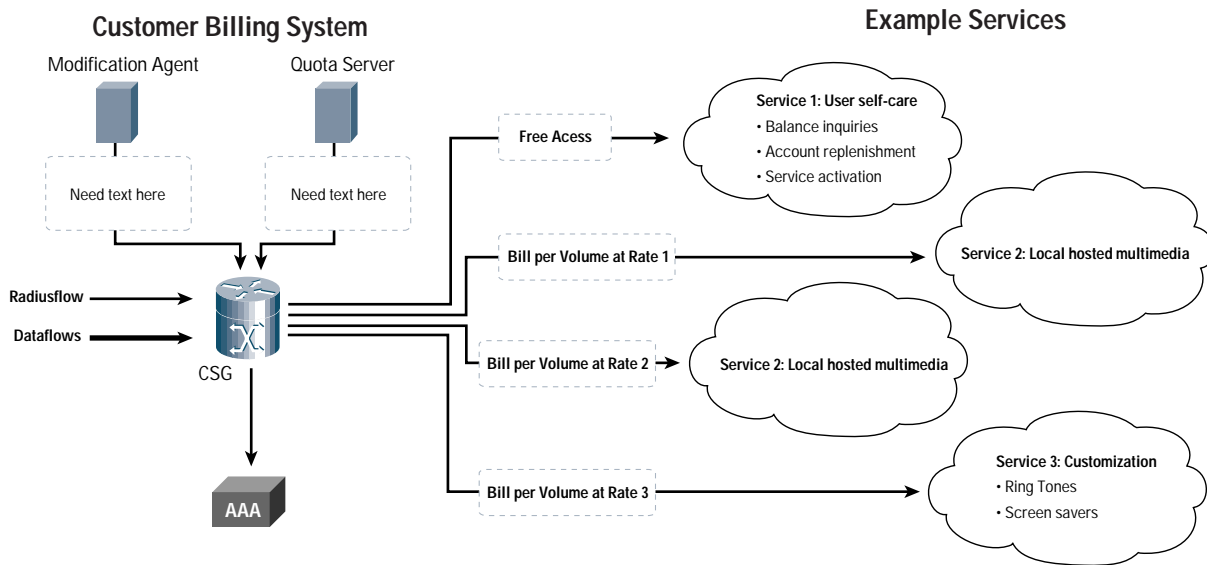
The rate at which the Cisco CSG must reauthorize a service is controlled by the billing system. A subscriber may be authorized to use a service for a specified number of transactions, a specified number of bytes, or a specified time. Also, the billing system can recall existing quota allocations when it wants to redistribute quota to other services.

When the subscriber's balance for a service is depleted, the Cisco CSG ceases to forward packets for that service. If a new session is attempted, the CSG forwards the connection to a configurable top-up server so that the billing system may offer subscribers an easy venue for replenishing their account. Ideally the billing system will have been warning the subscriber of the low balance before it is fully depleted, thus allowing an opportunity for replenishment without disrupting the data flow. If this top-up service is configured as part of a free service, the subscribers can perform the necessary actions to add money to their account and to perform

other self-care changes to their account even if access to chargeable services is denied. This allows the service provider to collect fees from subscribers affordably (without interaction with a human at the customer support center) without leakage, and it allows the subscribers to purchase new services without delay.

The Cisco CSG uses two "feeds" to communicate to the billing system: (1) a mediation agent feed for communicating charging data records (CDRs) that contain details of each subscriber transaction; and (2) a quota server feed for requesting service authorization and quota for prepaid and other balance-managed subscribers, as shown in Figure 4.

Figure 4: Communicating with the Billing System



This separation allows the customer flexibility in combining the billing system into one machine or separating it across two machines, or even across vendors. Also, the frequency of message exchange on each of the two feeds can be significantly different, thus necessitating different scaling requirements. The CDR frequency is controlled by subscriber transaction rates because one or more CDRs are created per transaction. The quota server feed frequency is controlled by the quota server itself, depending on how many transactions or how much data volume it authorizes on each request.

2.0 Core Functions: Basic and Content-level Accounting

Transaction (Event) Billing

The Cisco CSG provides detailed charging records for each transaction. A transaction is most easily thought of as a TCP connection, but it can be any of the following:

- An HTTP method (for example, GET, POST) within a HTTP 1.1 persistent connection—If multiple methods are presented within a persistent connection, then these will be multiple "transactions." Note that this is true only if the CSG policy is configured for "type http" processing; otherwise this is just treated as a simple TCP connection.
- A TCP connection, starting with SYN, and ending with FIN or RST or a timeout
- A pair of User Datagram Protocol (UDP) flows (one in each direction), starting with a new pair of source and destination addresses and ports, and ending with a configurable period of idle
- A pair of IP flows (one in each direction), starting with a new pair of source and destination addresses, and ending with a configurable period of idle

For TCP connections, the Cisco CSG reports connection-termination information so that the billing system may apply business logic to determine if the subscriber should be charged for the event. For example, the business logic may contain a provision to not charge for failed transactions. This could be applied to the CSG reporting of FIN, RST, timeout, or authorization failure to determine if

the connection was likely to have failed in error. Careful consideration is needed when applying such logic because some clients tend to terminate connections using RST even when the operation was successful. Robust business-class servers, on the other hand, tend to use RST only in the event of an error.

Another benefit of the Cisco CSG for TCP connections is that it allows the billing system to exclude network overhead when reporting payloads. That is, in addition to reporting the full IP byte counts in each direction, the CSG also reports just the transferred payload size (that is, no IP or TCP headers) in each direction and excludes any byte counts for network retransmits. Similarly for prepaid, the CSG can deduct volume-based quota using either full IP byte counts or payload-only counts. As a result, it is possible to charge the subscriber only for the size of the information that was requested and, therefore, not overcharge because of network issues that would cause retransmits.

The Cisco CSG reports the flow statistics (byte and packet counts), start time, and duration. In addition, if the billing system indicates that this is a balance-managed subscriber, the CSG includes the service ID, session ID, and quota used for each transaction.

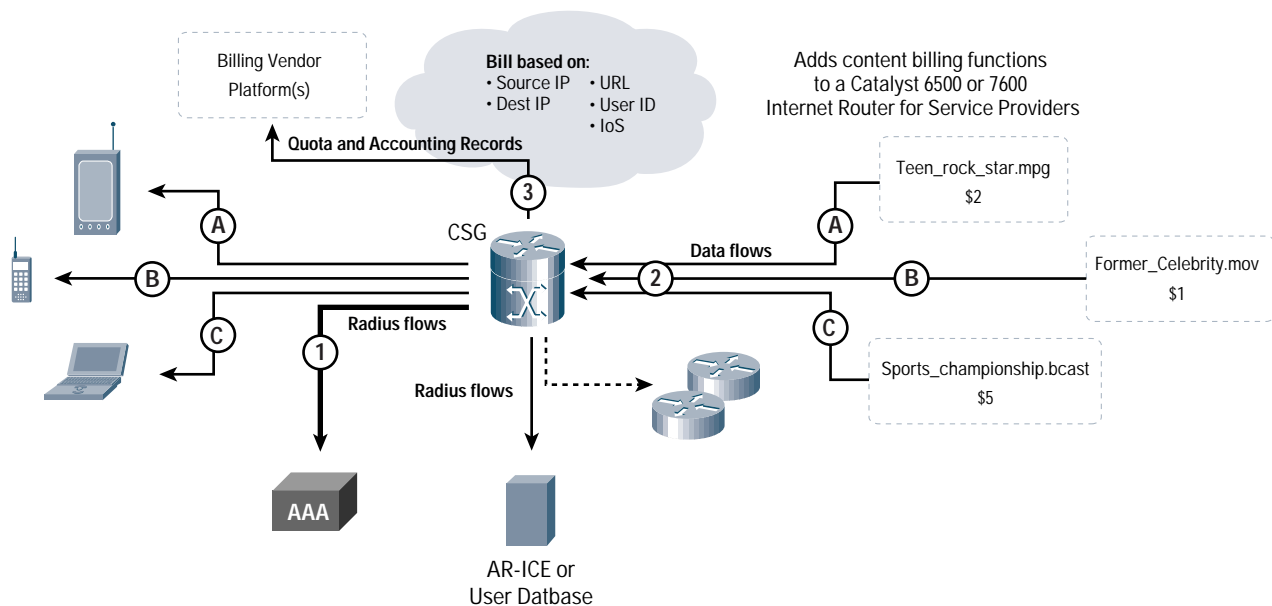
Content Billing

The content-billing support provided in the Cisco CSG is a marked improvement over other accounting protocols. Offering more than standard IP flow accounting, the Cisco CSG examines HTTP requests to gather URLs and other HTTP header information for accounting purposes. For File Transfer Protocol (FTP), the CSG examines the flows to extract filenames and directory paths for each GET or PUT operation, and, in addition, reports the directory name for each NLIST operation. By reporting this in addition to the transaction information discussed earlier (for example, usage statistics) and user identity, the CSG enables differentiated billing based on content type, host name, directory accessed, or even on individual files.

The ability to apply differentiated billing has several practical applications. For example, in some cases it may be more appropriate, or more lucrative, to reverse-bill some content transfers back to the content provider. Although chargeable events occur when consumers download information of value from a Web site, the general browsing of a Web site is usually assumed to be cost-free by the person browsing the page.

As Figure 5 shows, for chargeable events, content can carry different consumer value, regardless of network statistics (for example, volume and duration) that were used for traditional charging. A news brief of a major sporting event, for example, can carry a significantly higher consumer value than other content that is not date-sensitive.

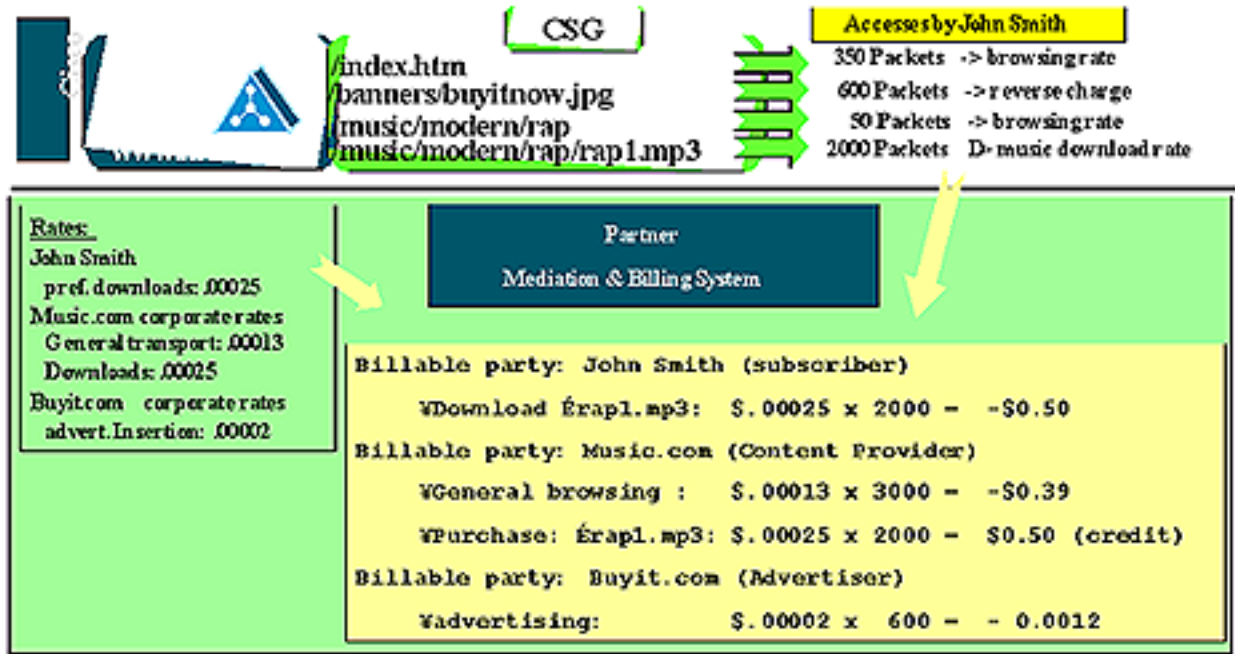
Figure 5: Differing Values of Content



The content provider already compensates the service provider for hosting the site, but a frequently accessed Web page may be more costly for a service provider. Because the Cisco CSG provides detailed information on how a site is accessed, service providers can use information to back-bill access to the content provider. Similarly, user access to advertising banners can be charged back to the advertiser.

Figure 6 illustrates how the Cisco CSG processing of user access information enables the billing system to provide differentiated billing.

Figure 6: Using URLs to Differentiate Content



When configured to generate accounting records for all traffic, the Cisco CSG identifies and measures all flows, regardless of protocol. No predefinition is needed for individual services being accessed. The resulting accounting records describe each flow. Through a service provider's chosen billing mediation system, billing policies can be applied to distinguish the billable parties and rates, as shown in Figure 6.

These examples highlight the e-commerce applications of content billing, but the Cisco CSG also provides benefits for corporate enterprise customers. A service provider can offer corporate contracts that differentiate business access from personal access. Because billing can be differentiated by content request, a service provider can bill work-related content requests (or virtual-private-network [VPN] access) to its enterprise customer, and bill other content requests as personal use. This also could be used by companies to support partners coming in on SSL based extranet connects. An example here would be a pharmaceutical company that wants doctors to have "free" access to selected drug related information on their web site via a mobile device.

Furthermore, the enterprise customer can value the detailed enterprise access reports that are possible by data mining of accounting records provided by the Cisco CSG. Even for encrypted enterprise flows, the high-speed monitoring provided by the Cisco CSG will identify the destination and the accessing user.

Figure 7 Differentiating Content

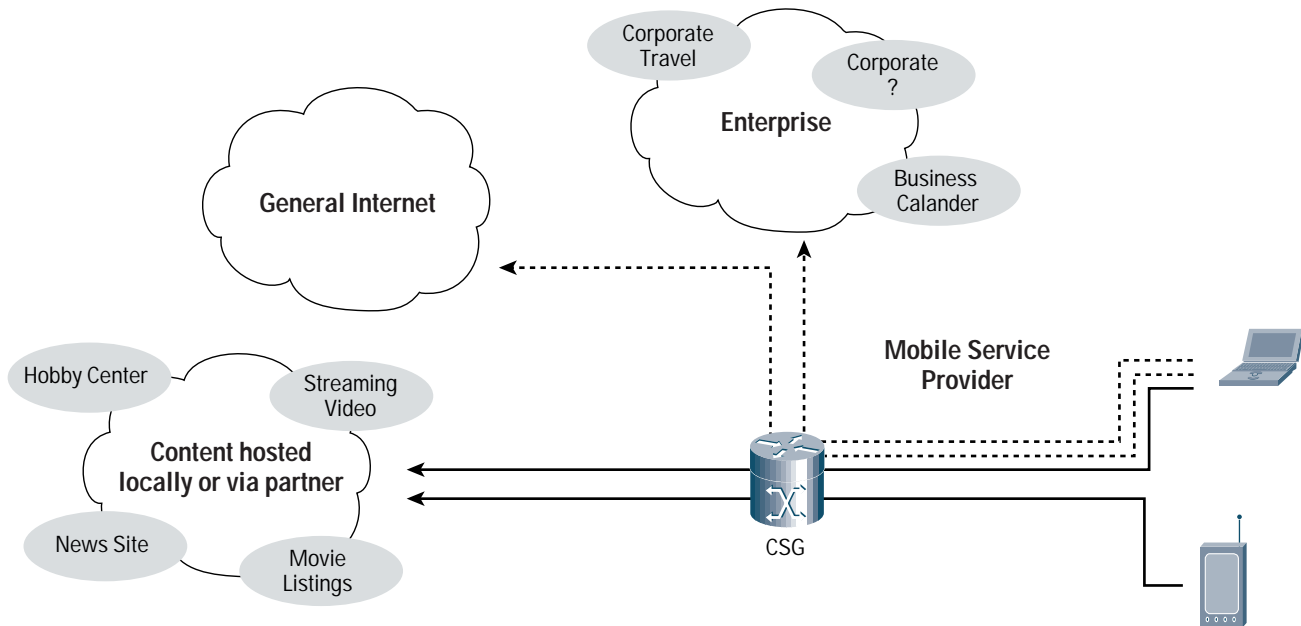


Figure 7 illustrates how differentiated usage is identified by the Cisco CSG. Although the laptop user is connected via the corporate access account, the content requests to systems not defined for approved business use can be charged to the subscriber rather than to the enterprise. The subscriber benefits by having a single access account authorized for both business and personal access. The enterprise benefits from business-only charging and detailed usage reports.

Subscriber Awareness

In today's dynamic environments, IP addresses are no longer reliable for use in identifying users. IP addresses can be dynamically assigned via Dynamic Host Configuration Protocol (DHCP), or users can connect from multiple devices with multiple IP addresses. In such networks it is desirable to correlate the subscriber identity to the IP address being used for data flows as early as possible. This avoids possible issues with quick reuse of IP addresses that result in incorrect billing. Cisco CSG identifies users in two ways:

- It can receive Remote Access Dial-In User Service (RADIUS) accounting start messages from which it examines username (attribute 1) and caller ID (attribute 31).
- It can query any customer-supplied Extensible Markup Language (XML) database that can return information for a given IP address. Note that the XML interface is intended as a backup. The RADIUS accounting stop is still needed to remove Cisco CSG user correlation entries before they can possibly be reassigned by DHCP.

Cisco CSG examines RADIUS accounting flows between the network access server (for example, in mobile wireless networks this would be the Gateway GPRS Support Node [GGSN] or home agent, depending on the access technology that is deployed) and the authentication, authorization, and accounting (AAA) system in order to correlate subscribers to their IP addresses and to track their entry and exit from the provider network. Cisco CSG combines this information with the information on transaction activity that it gathers, thus providing the billing system with a detailed view of the subscriber's use of the network. Each Cisco CSG accounting record contains the user identity if the system administrator has enabled this feature.

The Cisco CSG can process RADIUS messages in two modes: either as a RADIUS accounting endpoint in which Cisco CSG is the final destination for the messages; or as a RADIUS accounting proxy whereby Cisco CSG forwards the RADIUS messages to a further destination. Note that in proxy mode the Cisco CSG does not forward non-accounting (that is, access) messages. Proxy mode simplifies network configuration when the messages need to be forwarded also to a AAA server or other RADIUS-aware node.

The Cisco CSG also can request subscriber correlation from an outside source using XML requests. The XML database is key to Cisco CSG for rediscovering user IDs that may have been lost because of inactivity or CSG failure; for example, if CSGs were not deployed as a stateful pair. Support for such XML requests is, for example, provided by the Cisco Access Registrar® Identity Cache Engine (ICE). When using an XML-enabled username server, it is still desirable to provide Cisco CSG with RADIUS accounting messages for the additional benefits that they provide:

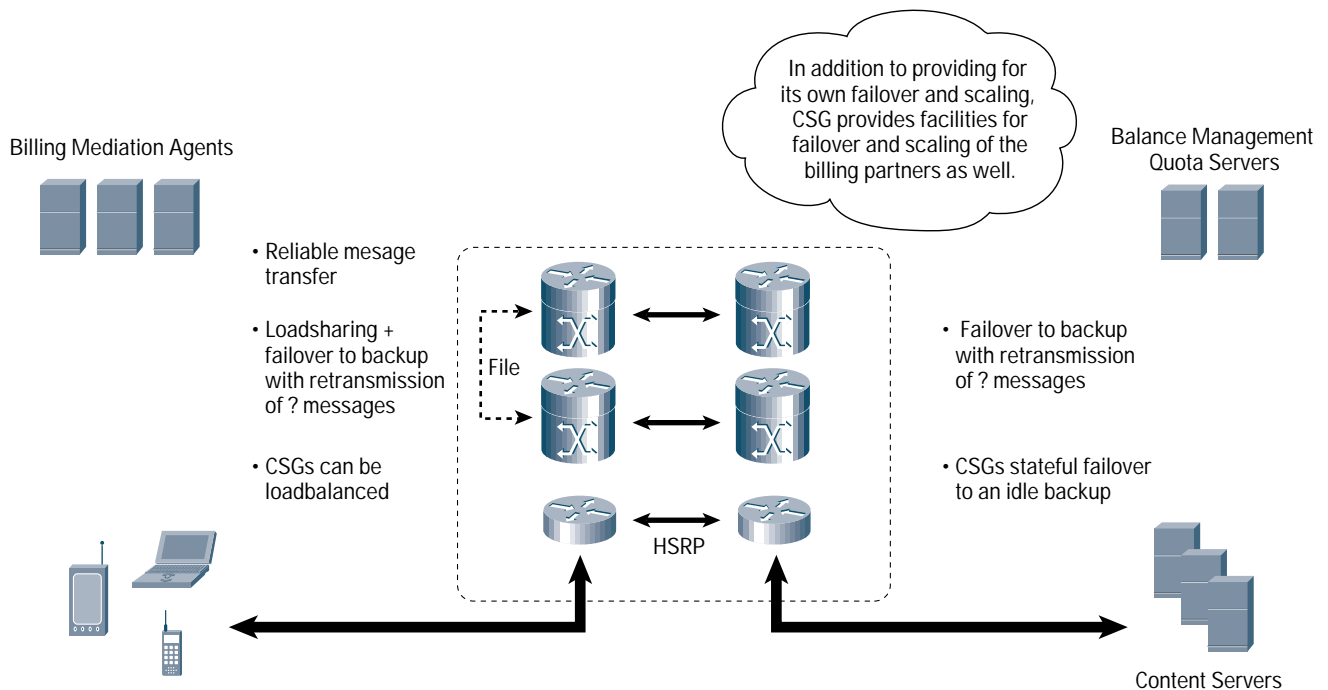
- The processing of accounting start messages is a performance optimization designed to avoid the overhead of database accesses for every new user.
- RADIUS messages are also key to Cisco CSG for maintaining synchronization with the IP address space: accounting stops are checked for IP addresses that should no longer be associated with a particular user ID, thus allowing Cisco CSG to remove its internal representation for these users. Further, accounting on and off messages are used to automatically determine when the internal User table should be cleared.

3.0 Cisco CSG Reliability and Failover

Cisco CSG offers leading-edge reliability and scalability. Cisco CSG reliability features allow for continued operation if either the CSG or the billing system fails. As Figure 8 shows, Cisco CSG offers:

- Reliable transfer of charging records—the records are sequenced, acknowledged or retransmitted, and timestamped. Network Timing Protocol (NTP)-based time adjustments are supported.
- Automatic failover to back up the billing system with retransmit of unacknowledged CDRs
- Load sharing of billing-system CDR collectors (mediation agents) for increased capacity
- Stateful failover of Cisco CSGs; continuation of user sessions, continuation of billing statistics collection, and preservation of username identity correlation
- Load balancing of Cisco CSGs (with or without stateful failover) using Cisco IOS® Server Load Balancing (SLB)
- Chassis reliability features such as Route Processor redundancy, Hot Standby Router Protocol (HSRP), and dual power supplies

Figure 8: Scaling and Failover



Efficient and Reliable Message Exchange with Billing Systems

Delivering accounting records for each content request necessitated the need for an efficient accounting protocol. Because Cisco CSG delivers critical billing information, reliable delivery is very important. Cisco CSG chose to use the GPRS Tunneling Protocol (GTP' V0), as defined in 3GPP TS 32.015 V3.4.0 plus the portions of 3GPP TS 32.015 V3.9.0 that apply to GTP' V0, as a transport for its accounting records. The protocol is based on UDP, but builds in a reliability layer on top, with acknowledgements, retransmissions, and support for backup mediation agents. The records are easily parsed, further contributing to its efficiency.

Cisco CSG Stateful Failover

Cisco CSG Stateful Failover provides for user session continuation, continuation of billing statistics collection, and preservation of subscriber-identity information. For stateful failover, Cisco CSGs are deployed in pairs, with one being active while the other is a backup. The backup is idle except for processing the fault-tolerant messages from the active primary. The primary and backup communicate over a configured fault-tolerant virtual LAN (VLAN). The primary and the backup can share the same chassis, though additional reliability is achieved by placing them in separate chassis.

Cisco CSG Scaling

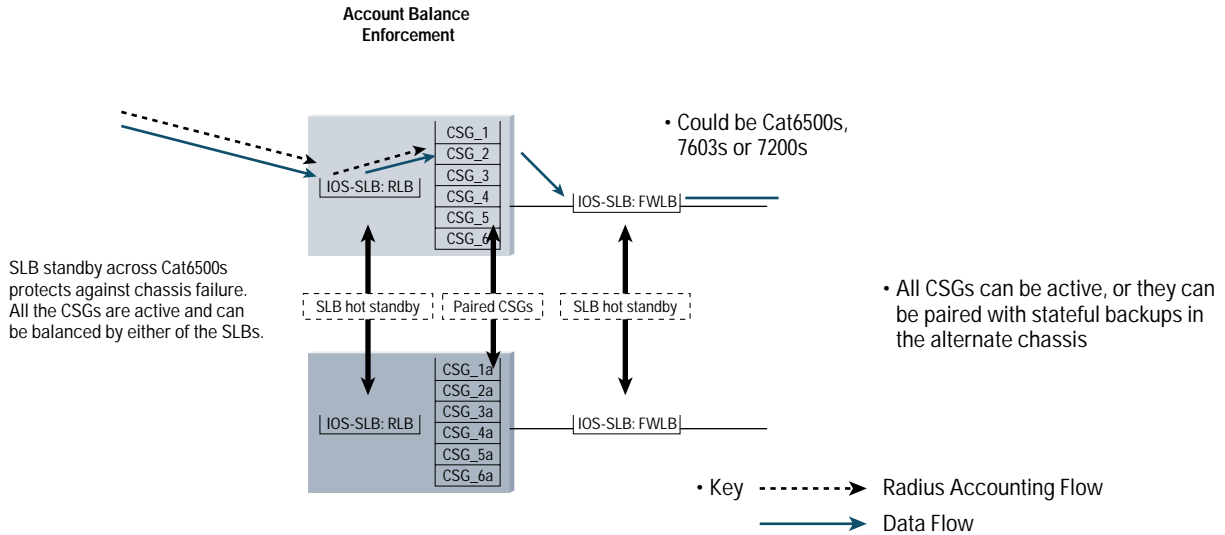
Each Cisco CSG can maintain user ID correlations for 300,000 subscribers, and can process several thousand connections per second and multiple gigabits per second of bandwidth. Using multiple units, the Cisco CSG can scale to accommodate very large environments supporting millions of users. Together with Cisco IOS SLB, a redundant Cisco CSG environment needs very little excess capacity. The load of a single failed Cisco CSG is spread across all remaining Cisco CSGs, so each Cisco CSG needs to have excess capacity for only a fraction of the failed system, equal to $1/n$, where n is the number of systems left after the failure. Where capacity is needed to sustain failure of multiple Cisco CSGs, more excess capacity should be planned. Also, spreading the Cisco CSGs across multiple chassis minimizes the number of Cisco CSGs that fail when an entire chassis fails.

Cisco CSGs, whether they reside in one or multiple chassis, are load balanced as a single farm. The Cisco IOS SLB RADIUS Load-Balancing (RLB) feature, with its ability to associate RADIUS flows and related data flows for the same user, ties all of a subscriber's flows to the same Cisco CSG. On the return side, the Cisco IOS SLB Firewall Load-Balancing (FWLB) feature is needed to pass the return data flow back to the correct Cisco CSG. The load balancers themselves can be fully redundant and support stateful failover.

When deployed as a simple farm of load-balanced Cisco CSGs, an XML-enabled user-identity repository such as the Cisco Access Registrar ICE is needed so that the user-identity correlation remains available as subscribers that were previously assigned to a failed CSG are redistributed to the remaining CSGs. Note that if user-identity correlation is not needed, the Cisco CSG can be deployed without the Cisco Access Registrar ICE (or equivalents). In either case, user TCP connections will fail when the CSG fails, user-identity information is lost and must be relearned (via the Cisco Access Registrar ICE, etc.), but UDP flows will continue (albeit without billing information). As discussed in the following paragraph, these drawbacks can be eliminated by combining Cisco CSG Stateful Failover with Cisco CSG Load Balancing.

Cisco CSG Load Balancing can be combined with Cisco CSG Stateful Failover so that stateful pairs of CSGs can be load balanced for increased scaling without loss of user connections or billing capability. TCP connections are preserved, generation of billing information is resumed, and user identity is preserved without the need for an outside cache. Such a configuration is shown in Figure 9.

Figure 9: Scaling + Stateful Failover

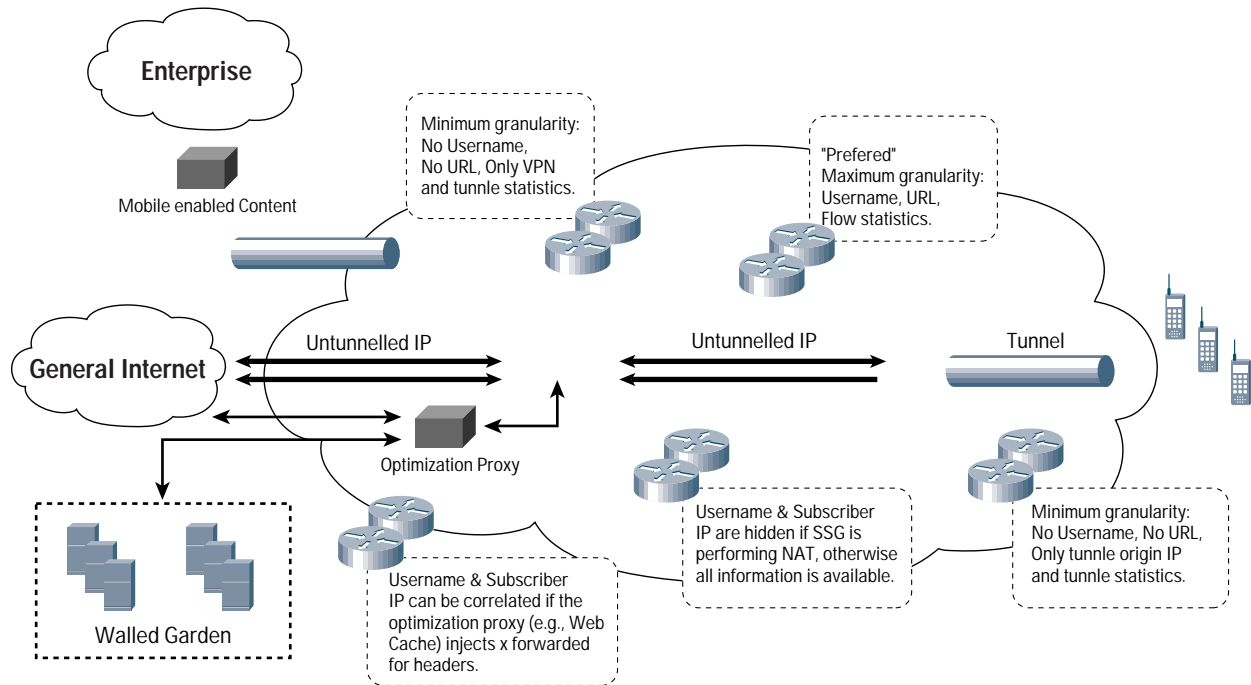


Although Figure 9 illustrates only single-site Cisco CGS failover capability, support for multisite failover is also available. In multisite failover designs, traffic is sent to one of the other data centers owned by the service provider. Traffic should be diverted to the alternate only if the primary site is completely unavailable, either because of failure or because its capacity has been exceeded. The Cisco IOS SLB Backup ServerFarm feature provides the support necessary to achieve this.

4.0 Cisco CSG Placement

In order to provide unique charging per protocol, the Cisco CSG must be in the path of untunneled traffic. When the traffic is tunneled, CSG charges for the tunnel. This is very useful for VPN traffic direct from the end station as VPN tunnels are typically charged on a volume or time basis. When traffic is not tunneled, CSG can inspect the protocol flows to provide application-level information that is used for differentiated charging per content as described earlier in the Content Billing section of this whitepaper. For subscriber-identity correlation, CSG must also reside in the data flow before any IP Network Address Translation (NAT) or proxy occurs. Figure 10 shows the various placement choices, using a General Packet Radio Service (GPRS) network as an example and considering Layer 2 encapsulation such as PPP over GRE (PPPoGRE), tunnel management devices such as the Cisco Service Selection Gateway (SSG), and Web caches.

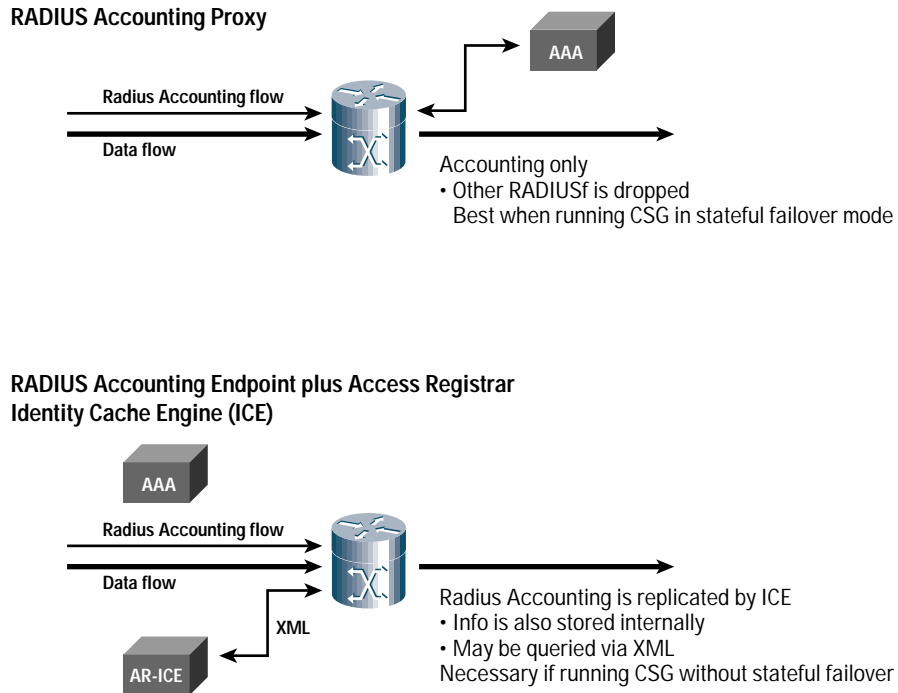
Figure 10: CSG Placement; GPRS example



Considerable information can be lost, depending on where the Cisco CSG is placed (refer to Figure 10). The Cisco CSG attempts to provide as much information as it can gather. Some Wireless Application Protocol (WAP) gateways, Web caches, and optimization devices are capable of inserting an x-forwarded-for header into the HTTP traffic. The Cisco CSG can parse this header and use the imbedded IP address for correlating the subscriber identity.

Data-path placement is only part of the puzzle. Cisco CSG works best when a RADIUS accounting feed is directed to the system. If RADIUS accounting is not already being targeted to another device in the service provider's network, providing this for Cisco CSG should not pose a problem. If RADIUS accounting is already in use for other receivers, the RADIUS flow can be proxied through the Cisco CSG or replicated by outside devices to provide copies for the CSG. One possible way to accomplish the replication is with Cisco Access Registrar software (AR). Figure 11 shows the two RADIUS routing options.

Figure 11: Discovering the Subscriber Identity



Operation in WAP Environments

As noted earlier, to provide full application-level accounting granularity, Cisco CSG must receive traffic that is untunneled. Full user identification is available when the subscriber IP address has not been lost through NAT or some other translation. As such, placement on the binary-encoded side of a WAP gateway results in only bulk flow statistics for the WAP data flow. Also, some WAP gateways source the HTTP connections from their own IP addresses rather than retaining the user's IP address in the IP header. This simplifies the implementation of the WAP gateway, so there are good reasons why a vendor might design its product this way. If the subscriber IP address is communicated in an x-forwarded-for header, a configurable option in some WAP gateways, the Cisco CSG can parse for the header and correlate the user identity. Proxy WAP gateways that do not use x-forwarded-for are incompatible with Cisco CSG transaction-level billing. Note that WAP gateways that operate in router mode and do not hide user addresses from the IP header do not need x-forwarded-for support to interoperate with CSG because the subscriber address is not hidden.

5.0 Cisco CSG Content Accounting Records

Cisco CSG content accounting records contain several pieces of information and provide separate formats for HTTP, FTP, TCP, UDP, and IP, with the most detailed being the HTTP and FTP reporting. The Cisco CSG can be configured to provide general TCP, UDP, and IP statistics, or to present granular application-level (that is, content level) information in addition to the general statistics.

Cisco CSG accounting records attempt to address the following needs:

- Accurately identify the user, even in environments with dynamic IP address assignment
- Obtain the URL for an HTTP content request or path or filename for a FTP transfer
- Obtain the type of device (that is, the browser) that generated the HTTP request
- Obtain the type of service (ToS) from the first packet of this connection
- Obtain transaction-termination information so that the billing system can decide transaction success or failure

Note that defining "successful" connection termination is sometimes difficult. The Cisco CSG is able to apply content-level processing to provide HTTP and FTP application level completion codes that augment the information derived from just the standard TCP termination sequence (RST versus FIN). Unfortunately, the Cisco CSG has no standard termination information to report for UDP or other protocol types, except for detection of idle timeout. Even for TCP, some client browsers terminate a connection with a RST even if no error is encountered on the transfer. It is generally advisable to focus on server-initiated RSTs and

to ignore client-initiated RSTs as failure indications. The Cisco CSG provides the details of the termination, such as which end of the connection initiated the termination; termination type (RST, FIN, or a timeout); and, for HTTP 1.1, whether or not the connection is still open. The billing system can combine the information provided to decide success or failure, and charge or refund accordingly. Application level completion codes provided by the CSG are important because it is quite common for the application to return an error and to follow by closing the TCP connection with a FIN, which indicates a non-error connection closure. An example of this is an HTTP download for a stale hyperlink, which the server presents as a "not-found" Web page. Even though the TCP connection closed with FIN, the subscriber did not receive the chargeable content that the subscriber was hoping to download.

HTTP requests are actually represented with two records per request:

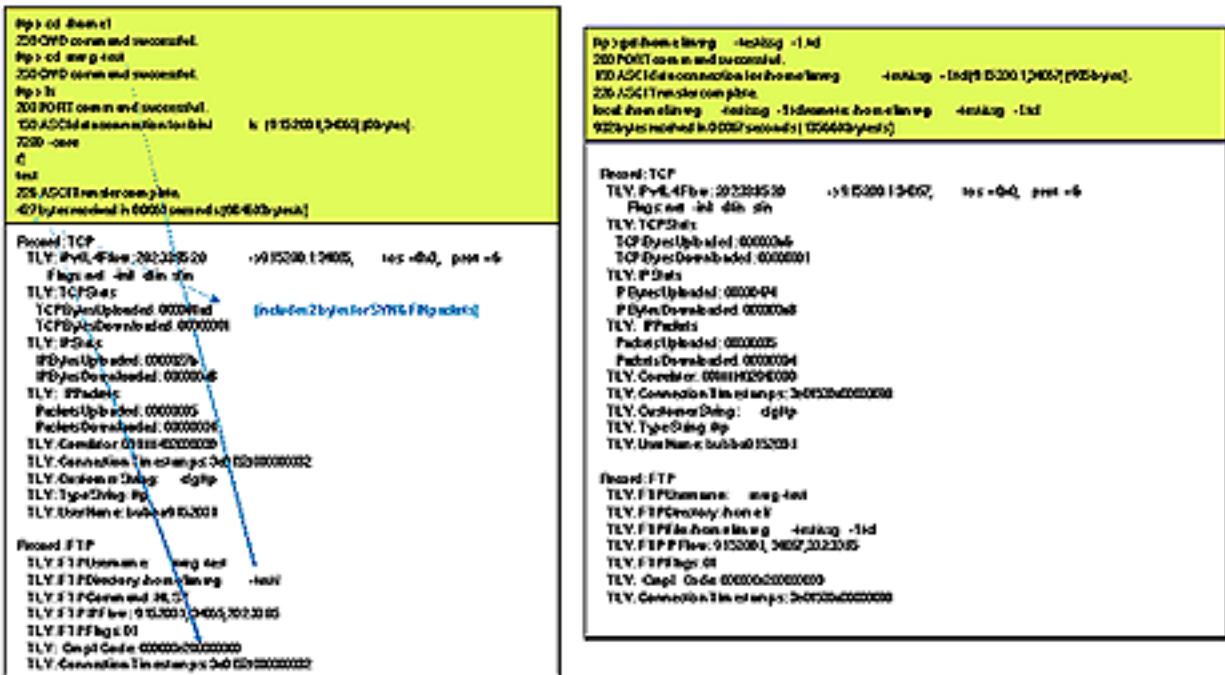
- An HTTP header record, which carries the user ID and select HTTP header fields for the URL, the browser type, and a correlator for matching this record to the subsequent statistics record
- An HTTP statistics record, which carries information about the size of the transfer, from both an overall IP perspective and a payload (TCP) perspective—The TCP byte counts are exclusive of any retransmits, so the billing application can charge for the content received by the user and avoid charging for any network problems that the transfer may have experienced. Because these TCP byte counts are based on the TCP sequence numbers, they exclude both the IP and TCP headers except for the flag bytes from the SYN and FIN packets.

For HTTP 1.1 persistent connections, each HTTP GET request has a pair of these records; the connection-termination flags are valid only for the HTTP statistics record representing the last request.

Similarly, as shown in Figure 12, FTP transfers are represented with two records per event:

- A FTP record, which carries the path, filename, and completion code—Note from the example that the Cisco CSG can reconstruct the directory path even though multiple change directory requests were entered in the user session.
- A TCP statistics record, which carries information about the size of the transfer, from both an overall IP perspective and a payload (TCP) perspective—As with the other TCP statistics records generated by the Cisco CSG, the TCP byte counts are exclusive of any retransmits, so the billing application can charge for the content received by the user and avoid charging for any network problems that the transfer may have experienced. Because these TCP byte counts are based on the TCP sequence numbers, they exclude both the IP and TCP headers except for the flag bytes from the SYN and FIN packets.

Figure 12: FTP Transaction Reporting



6.0 What Is Next

- Further content processing for other applications—the most detailed billing for the Cisco CSG is currently focused on HTTP and FTP. Consider how one might apply similar detail to other applications. Even though Cisco CSG produces billing records for all IP applications today, the level of detail diminishes depending on the underlying protocol. Customer requirements will undoubtedly drive additional detail for other applications.
- Additional actions to be taken using content—clearly billing is not the only possible use for content classification. Other uses will arise, including restricted access, quality of service, and additional features that will more tightly integrate the content transfers with the network operation. The desired results are further improvements in end-user satisfaction, increased value of the Internet, and increased business for providers of access or content.

7.0 Glossary

CDR—Charging Data Record.

Cluster—Set of computer systems that are connected through multisystem hardware or software to supply services traditionally provided by a single system. This arrangement provides higher availability and better scalability of the system.

FIN—Finish flag, TCP header

Firewall—Router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.

Firewall farm—Group of firewalls.

Firewall load balancing—Load-balancing scheme in which the network administrator configures a group of firewalls into a firewall farm. When a client initiates a connection, IOS SLB chooses a firewall for the connection based on a hash algorithm.

FTP—File Transfer Protocol.

GGSN—Gateway GPRS Support Node.

GRPS—General Radio Packet Service. A wireless communications protocol.

Home Agent—In Mobile Internet Protocol (Mobile IP), a home agent is a router on a mobile node's home network that maintains information about the device's current location, as identified in its care-of address. The home agent uses tunneling mechanisms to forward Internet traffic so that the device's IP address doesn't have to be changed each time it connects from a different location. A home agent may work in conjunction with a foreign agent, which is a router on the visited network.

HSRP—Hot Standby Router Protocol. Provides high network availability and transparent network topology changes. HSRP creates a Hot Standby router group with a lead router that services all packets sent to the Hot Standby address. The lead router is monitored by other routers in the group, and if it fails, one of these standby routers inherits the lead position and the Hot Standby group address. See also redundancy, stateful backup, stateless backup.

HTTP—Hypertext Transport Protocol

IOS SLB—IOS Server Load Balancing. Load-balancing product in which the network administrator defines a virtual server that represents a group of real servers in a cluster of network servers known as a server farm. When a client connection is intercepted because of the virtual server, IOS SLB chooses a real server for the connection based on a configured load-balancing algorithm.

IP—Internet Protocol.

Load balancing—Spreading user requests among available servers within a cluster of servers, based on a variety of algorithms.

Message Digest Algorithm Version 5—See MD5.

NAS—Network Access Server. A Network Access Server (NAS) is a network device that enables an independent service provider (ISP) to provide connected customers with Internet access. A network access server has interfaces to both the local telecommunication service provider such as the phone company and to the data network. The server authenticates users requesting

login. It receives a network connection request (e.g., a dial up call) from each user host that wants to access the network, performs the necessary steps to authenticate and authorize each user, usually by verifying a user name and password, and then allows requests to begin to flow between the user host and hosts (computers) elsewhere on the network.

NAT—Network Address Translation. Modification of one or more of the following fields in an IP packet: source IP address, destination IP address, source TCP/UDP port, destination TCP/UDP port.

Network Address Translation—See NAT.

NTP—Network Time Protocol. Network Time Protocol (NTP) is a standard protocol that is used to synchronize computer clock times in a network of computers.

QOS—Quality of Service

Real server—The specification of a physical server associated with a virtual server. The specification includes the real server's IP address and an optional weight to be used by the virtual server predictor.

Redundancy—The duplication of devices, services, or connections so that, in the event of a failure, the redundant devices, services, or connections can perform the work of those that failed. See also stateful backup, stateless backup.

RST—Reset flag, TCP header.

Server farm—Group of real servers that provide various applications and services.

SGSN—Serving GPRS Support Node.

SLB—See IOS SLB.

Stateful backup—Redundancy scheme that enables the active node to incrementally backup its decisions, or "keep state," to a backup node.

Stateless backup—Redundancy scheme that allows new user connections to be routed to an alternate system upon failure of the primary, but does not preserve information between systems.

SYN—Synchronize Sequence Numbers flag, TCP header.

TCP—Transmission Control Protocol.

ToS—Type of Service

URL—Universal Record Locator.

WAP—Wireless Application Protocol. Suite of protocols used to deliver services to wireless devices.

Wireless Application Protocol—See WAP.



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 Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 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
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