WHITE PAPER

MAXIMIZING USE OF MOBILE DATA INFRASTRUCTURE: THE IMPORTANCE OF SERVICE CONTROL IN MOBILE NETWORKS

INTRODUCTION

The opportunity provided by data services has prompted mobile operators around the world to launch new architectures, marketing campaigns, and service strategies to gain market share and revenue. With the adoption of these IP-based service models, and with the introduction of “true” high-speed mobile access, operators are facing an increasing number of new challenges that threaten the success of their initiatives by turning their data networks into generic access pipelines with little service differentiation. Moreover, as service offerings mature and are supported by higher access bandwidth, subscriber quality expectations increase tremendously.

As operators capitalize on IP networks, they need to create higher-margin, higher-revenue premium services such as video streaming, push-to-talk, or interactive gaming. Mobile operators are looking for profitable ways to deliver such value-added, bundled, or personalized IP services to greater numbers of subscribers. Critical to the current strategy is the ability to understand at a granular level how subscribers are using the network, identify what applications or services are being consumed, and then intelligently apply network resources to applications and subscribers that promise the highest return on investment.

Enhancing current infrastructure with the ability to classify, manage, and control IP-based application traffic such as interactive gaming, video on demand (VoD), streaming, or even voice over IP (VoIP) would better position mobile service providers to profitably deliver higher-value offerings. With the increasing usage of applications such as peer-to-peer (P2P—for example, BitTorrent or Skype), streaming, and gaming consuming bandwidth and network resources, operators still lack the ability to optimize network capacity, or protect the quality of experience (QoE) for their valued subscribers.

Operators need to manage and control subscriber traffic. This can be accomplished by implementing service control technology, which enhances the transport network with application and subscriber awareness. Service control allows the network to identify, classify, and guarantee performance for services based on unique application content and subscriber criteria. Service control reinforces the new paradigm in which mobile service providers can define and enforce the policies for application traffic management on their network. In this way, operators can optimize network performance, overcome QoS constraints, and ensure that infrastructure is used for maximum return on investment.

Service control allows new possibilities for broadband service creation and new revenue-sharing opportunities with third-party service providers that may, in fact, be riding an operator’s network undetected.

This paper outlines the factors that illustrate the need for service control technology, and its applications and benefits in mobile data networks.

EVOLUTION OF MOBILE DATA SERVICES

Third-generation (3G) mobile networks are opening the way for access to an ever-expanding array of high-bandwidth applications and data services to mobile subscribers. Many of these will be revenue-generating services either developed or resold by the mobile operator. The availability of high-bandwidth access is typically coupled with the introduction of many general-purpose terminals, enabling numerous new network applications. These new applications may not be controlled by the mobile service providers, but may consume valuable network resources, potentially degrading the performance of the revenue-generating services without generating any financial gain. The ability to use applications such as Skype, which within a year have been downloaded more than 17 million times, on a mobile network may change all provisioning assumption used in its design.

For mobile operators, the need for service differentiation is urgent. In order to increase average revenue per user (ARPU), strengthen customer loyalty, and increase profits, mobile operators need to introduce, guarantee delivery, and protect innovative data services.

As new services proliferate, potentially beyond the mobile service provider's control, mobile operators must regain this control over their most valuable asset—their network—by equipping it with service control capabilities. These capabilities include the ability to analyze traffic usage, control bandwidth allocation between the various revenue-generating and non-revenue-generating services, and secure their network from malicious traffic.

Traffic Analysis (Data Mining)

Improvement and development of new business models requires mobile providers to accurately understand their subscribers' usage. Having such deep understanding of user behavior and data services usage allows operators to appropriately define their business policy, efficiently adapt their network dynamic traffic patterns to their existing service-delivery models, and rapidly develop new service offerings delivering new revenue-generating services over their existing networks.

Application Traffic Control

Controlling network applications traffic has many aspects. On one hand different prioritization and delivery guarantees are required for the different services, and on the other "best-effort" traffic of non-revenue-generating services should be controlled so as not to disrupt the delivery of the premium services.

Non-Revenue-Generating Traffic Control

As witnessed by broadband wireline service providers for the past several years, high-speed access and general-purpose terminals are the main factors that influence many of the emerging bandwidth-consuming applications. The most notable applications in this category are the file-sharing P2P applications used by subscribers to swap video, audio, and data files. In addition to consuming high volume for long time periods, these applications are typically symmetric in their bandwidth requirements, not matching the asymmetric provisioning of most access networks. It is very important to control such traffic in a way that protects the network resource without alienating the subscribers who use these applications.

Revenue-Generating Traffic Prioritization

Developing new revenue streams requires the delivery of new premium services over a common network pipeline. Streaming, gaming, and other latency-sensitive premium services could be vastly improved by dynamically enforcing the appropriate control policies. Such policies could be based on specific subscriber or application parameters, adding real value, offering performance guarantees, and optimizing the availability of network resources. Such capabilities would benefit both the operator and the subscribers who use these services. From the subscriber point of view, services are no longer delivered on a "best-effort" basis, but rather at an accepted quality and reliability, justifying the payment of a premium price. For the providers expecting to build a critical-mass business around value-added services such as video, music, and gaming, this directly translates into revenue increase and subscriber churn decrease.

P2P: Skype, Skinny, and File Sharing

As more general-purpose terminals get on the mobile network, evidence of P2P traffic on mobile networks becomes evident. Although some of these applications simply burden the network with the increasing bandwidth they consume, other P2P applications such as BitTorrent or Skype and Skinny may subtract from voice revenue if not addressed properly. It is important for the mobile service provider to learn the usage patterns of these applications, and to develop appropriate offerings to address this revenue loss.

Traffic patterns for P2P applications vary dramatically from their client-server counterparts, causing a significant change in upstream data requirements, time-of-day activity, and use of expensive international transit links. Left unmanaged, P2P can become a financial burden—network resources are consumed, forcing constant investment in network capacity without any additional revenue. Failure to accurately manage P2P traffic can lead to customer support load and subscriber turnover as network congestion degrades the performance of other applications. Technology solutions must be able to not only deal with existing protocols but quickly adapt to new and emerging protocols to overcome the P2P challenge.

Security Threats to Network Integrity

"Always-on" connections, as made possible by mobile data access networks such as General Packet Radio Service (GPRS), Code Division Multiple Access (CDMA), wireless LAN (WLAN), and 3G, expose subscribers to a growing number of malicious threats such as the upcoming mobile viruses or even traditional broadband viruses and worms, degrading the overall user experience. Meanwhile, operators are impacted by support and network-management concerns that can result from denial-of-service (DoS) or other network attacks.

SERVICE CONTROL SOLUTION

Today's access networks are first designed to give IP connectivity to users rather than controlling the traffic for optimizing specific flows such as P2P, or layering a variety of QoS policies to support the performance requirements of value-added services. When these access networks are augmented with inline traffic intelligence, such as the service control solution, allowing operators to identify subscribers, classify applications and traffic behavior, guarantee performance of latency-sensitive applications, and provide information on individual services (data mining), then new business models, including enhanced profitable service delivery and cost reduction, become possible.

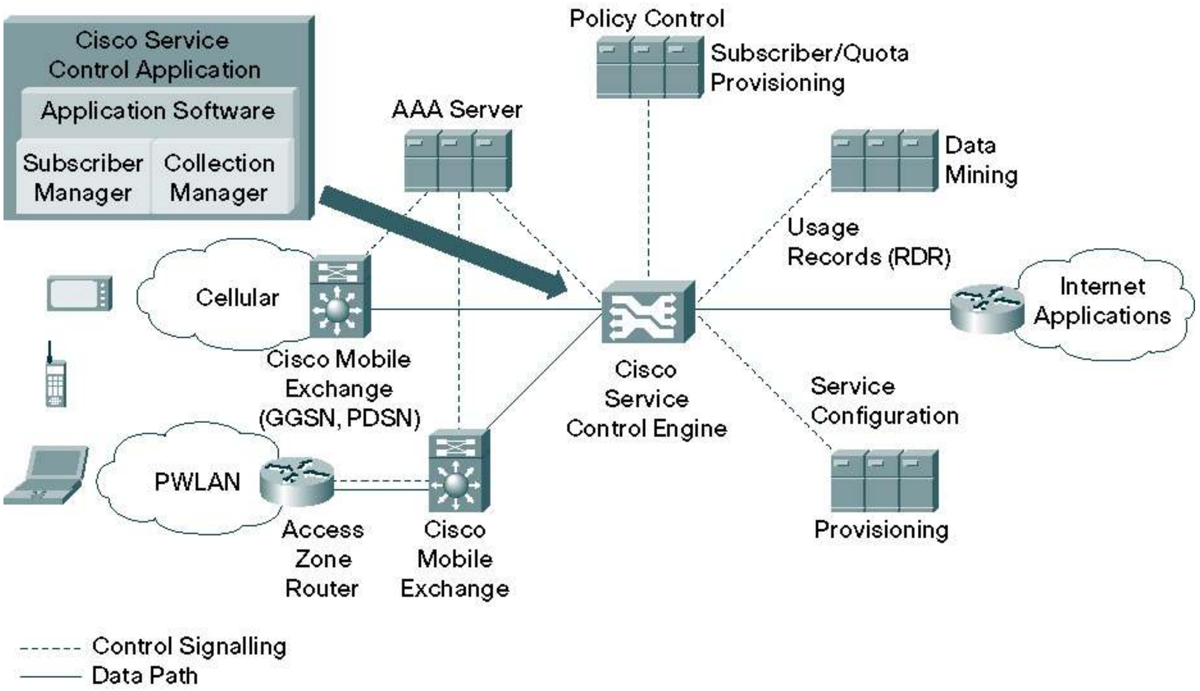
For instance, using a service control solution, service providers can differentiate performance of their own branded services, or of services provided by their chosen partners, from any other "best-effort," "uncontrolled" service. Networks enabled with service control can provide operators with new ways to manage network capacity according to their business priorities, and increase the value of their network assets to better partner with content providers.

Service control, both a software and hardware solution, is an IP network element built specifically to address the challenges and provide the benefits highlighted previously. Situated "in line" on the IP data stream, the platform performs hardware-accelerated, application-layer, stateful deep-packet inspection to accurately classify and control traffic by content, application, and subscribers.

The customized hardware of the platform is built to combine extremely efficient stateful processing of traffic into a fully programmable framework, which balances between performance and flexibility needs. This allows the platform to process gigabits of traffic while ensuring it is adaptable enough to address traffic-analysis requirements resulting from changing or emerging applications and protocols.

Typically installed at the edge of the mobile data network, upstream of the mobile aggregation device (gateway GPRS support node [GGSN] or packet data serving node [PDSN]), the platform interoperates with subscriber-authentication and -management components as well as data-collection and policy-provisioning systems to transparently deliver dynamic, customized, and application-differentiated broadband services to subscribers (Figure 1).

Figure 1
Cisco® Service Control Application for Mobile Networks



A service control platform provides mobile operators with a rich set of tools to manage network traffic and address performance, as well as service security concerns. The solution offers providers ways to create new paradigms for the definition and delivery of data services. Operators can tailor the experience of each subscriber in accordance with any defined policy, and truly differentiate service offerings.

Service control applications are specifically designed to assist operators by improving network analysis and reporting as well as establishing more granular control for the deployment of new services. The following section outlines the potential applications of service control technology in mobile data networks and potential areas of direct impact upon an operator's business.

Usage Analysis

Improving and developing new business models requires that broadband service providers accurately understand their subscribers' usage. Service control technology is intended to dramatically improve data service usage analysis. Obtaining meaningful usage data from IP networks is a particularly difficult task, especially when dealing with nonstandard applications such as Skype or Skinny.

Service control technology provides high-performance application and subscriber-aware traffic classification, offering operators unrivaled visibility into network activity. By tracking all IP traffic flows and performing stateful deep-packet inspection, the solution collects statistics about the applications and services used by individual subscribers. Taking the guesswork out of capacity planning and detailing the subscriber demographics helps operators uncover the new revenue potential and hidden operational costs associated with IP service delivery in mobile networks.

Traffic Optimization

The growing number of subscribers with data-capable mobile devices and the growing success of mobile data applications (such as browsing, streaming, or downloading) associated with constrained radio resources, lead mobile service providers to deploy a service control solution to optimize the traffic and the bandwidth on a per-service and per-subscriber basis. All network traffic is identified and each network conversation over every protocol is assigned with the appropriate quality of service (QoS) to meet the mobile provider's business policy.

Using state-of-the-art capacity and throughput management applied to network traffic on a global, subscriber, or individual flow-level hierarchy allows operators to dictate how network resources are distributed. The result is improved subscriber experience and overall satisfaction with mobile data network performance, thus lowering subscriber churn while fuelling the growth of mobile data services.

Service Network Security

The lack of security-conscious users and the open nature of the Internet create a breeding ground for network security threats impacting both service providers and subscribers. Subscribers are under a constant threat of DoS attacks and worm and virus infection, or even common port scan. Recent threats have created "security storms" over the Internet resulting from popular viruses such as Sasser, Slammer, and Blaster. Additionally, as more "IP-enabled" handsets and personal digital assistants (PDAs) become a target for hackers, service security becomes a paramount concern for operators on all fronts.

Increased network traffic caused by the multiplicative effect of infected terminals results in increased administrative costs and technical support calls as operators seek to track, disable, and block the spread of a virus attack. Infected terminals can generate network congestion as they attempt to propagate a viral infection, resulting in performance degradation for all users. Port scans can cause handsets to get in and out of hibernation mode, increasing loads on network equipment and shortening the battery life of mobile handsets. Service control-enabled networks stop and proactively mediate security threats that increase providers' costs by creating unwanted traffic and network congestion.

Tiering and Access Control

As content proliferates and content suppliers begin to partner with network operators, mobile service providers will need to protect copyrights, which may be based upon subscription, and prevent unauthorized access to content.

A service control platform helps operators enforce different policies on the user access to a variety of applications or services. This dynamic, subscriber-centric enforcement model allows for the creation of access and throughput-on-demand services that can improve overall subscriber satisfaction by allowing subscribers to select or gain access to chosen content and resources. Providers can now initiate truly customized products and services and enforce service parameters directly correlated to the needs of individual users.

Premium Service Enablement

The ability for mobile service providers to offer differentiated service bundles on a per-service or per-user basis is essential to satisfy their customers and increase ARPU. A corporate customer may be willing to pay premium prices for a service package if higher quality is guaranteed.

Integrating into existing QoS frameworks and communicating with policy servers and network transport elements, service control solutions help enable dynamic, real-time provisioning of network QoS based on application activity, greatly simplifying integration and delivery costs associated with multiple services delivery.

MAXIMIZING THE MOBILE DATA INFRASTRUCTURE

With the growing penetration of mobile data services, operators must increase their visibility and improve their control over network and user activity. Enabling IP networks to differentiate between services such as Web browsing, music downloads, video streaming, VoIP, or P2P traffic makes it possible to control the quality of individual services or charge for them effectively. Cisco Service Control helps mobile service providers maximize the revenue they generate out of their mobile data infrastructure.

A service control network element adds a programmable service layer to mobile data networks, helping providers identify subscribers, classify applications, guarantee service performance, and provide information about IP services without costly infrastructure upgrades.

Specifically built to be deployed at the network edge, the Cisco Service Control solution offers operators unparalleled control over network traffic and subscriber usage. Now an operator’s transport network can be augmented with vital functions. For a small incremental investment, operators can quickly deploy new IP services, reduce overall costs, amortize massive investments in network access across multiple services, establish new partnerships with third parties, and test new business models. The capability to profitably deliver premium IP services has arrived.

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

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

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

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

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

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

LG/LW8568 06/05

Printed in USA