The Business Case for SoftSwitch/Session Border Controller

Executive Summary

There are a number of reasons why service providers should consider adding IP based voice and multimedia services to their current offerings. Local exchange carriers are struggling to retain their current customers, ISPs are trying to generate incremental revenues, long distance carriers are striving to reduce interconnection costs and wholesale carriers are trying to offer enhanced services to their service provider customers as well as to reduce their interconnection costs. Through enabling service providers to generate incremental revenues, reduce interconnection costs and customer churn, IP based voice and multimedia services offer an attractive solution.

Unfortunately, IP networks have been traditionally viewed as poor revenue generators due to the multiple technical problems that prevent the consistent delivery of high-quality, real-time interactive voice and multimedia services. Common problems associated with IP networks include secure connection to customers behind Network Address Translation (NAT) devices and firewalls, Quality of Service (QoS) and Service Level Agreement (SLA) assurance and secure IP-IP peering between service provider networks.

SoftSwitches/Session Border Controllers (SS/SBC) are a new generation of networking devices that are designed to overcome the technical problems to delivering profitable voice, video and other real-time interactive services across IP network borders. This white paper describes the role SS/SBCs play in enabling the problem-free delivery of interactive IP services and how SysMaster's SM 7000 Universal SoftSwitch/Session Border Controller (SS/SBC) can help service providers resolve IP network integration problems.

Introduction

Faced with increased competition many service providers are striving to reduce customer churn, lower operating costs and improve profitability. Local exchange carriers are struggling to retain their current customers, ISPs are trying to generate incremental revenues, long distance carriers are striving to reduce interconnection costs and wholesale carriers are trying to offer enhanced services to their service provider customers as well as to reduce their interconnection costs.

IP based voice and multimedia services offer attractive alternative for generating incremental revenues, reducing interconnection costs and increasing customer loyalty. Many service providers have already realized those benefits but as they started building IP infrastructure they faced an entirely new set of security, service assurance, and convergence problems. As a result today most VoIP networks are relatively isolated from existing communication infrastructure and thus provide limited revenue opportunities. The only viable way to make IP services profitable is to ensure good integration with both traditional and IP communication infrastructure.

SoftSwitches/Session Border Controllers

SS/SBCs reside at the service provider's network edge where they complement existing routers. They serve as both source and destination for all signaling messages and media stream entering or exiting the provider's network. SS/SBCs perform a number of functions, including:

- IP-to-IP peering
- Protocols conversion and codecs transcoding
- NAT/Firewall traversal
- Quality of Service enforcement
- Network security enforcement

The Yankee Group predicts that the Session Border Controller's market will take off in 2004 as adoption of VoIP VPNS, managed IP PBX, and IP Centrex services drive Tier 1 and smaller carriers to take advantage of the lower costs and operational efficiencies of native IP peering. The Yankee Group estimates that by 2007, the market will grow to $624 million, a CAGR of 124%[1] between 2003 and 2007.

[1] Session Controllers: A New Breed of Intelligence Edge Devices, Yankee Group, Sep. 2002

IP-to-IP Peering

From service provider's point of view, interconnecting with other providers allows IP based services to be extended to a broader range of customers, which could increase revenues for all participating parties. The traditional method of connecting with peers is based on using PSTN gateways and multiple TDM circuits. While that arrangement works for voice traffic and provides the security and accounting information required, it introduces unnecessary codec conversion which reduces voice quality and increases service provider's costs. Additionally, that approach is not flexible enough to support value-added services such as unified messaging.

SysMaster's SM 7000 SS/SBC offers flexible and cost effective alternative for reliable and secure IP-to-IP peering. SM 7000 intercepts all incoming signaling messages and media streams, converts (if necessary) and routes them based on preset rules and algorithms. The solution seamlessly integrates with other SIP/H.323 devices and offers low total cost of ownership.

Full Protocols Conversion and Codecs Transcoding

It could be challenging or impossible to connect directly several IP networks due to the existence of several signaling protocols and voice codecs. The problem typically arises when service provider with H.323 infrastructure decides to interconnect with counterparty with SIP infrastructure. The problem is further complicated if the origination networks use voice codecs which the termination network does not support. In such cases service providers need to use equipment that transparently converts signaling and media streams to ensure seamless interworking of the connected networks.

SysMaster's SM 7000 SS/SBC supports full protocol conversion between H.323, SIP, SS7, MGCP, MEGACO, PSTN, ISDN, and CAS. That feature makes SysMaster's equipment very easy to integrate with any existing communications infrastructure. SM 7000 also supports multiple codecs transcoding including G723.1, G729A/B/AB, G726, and GSM. The equipment allows multiple codecs to operate concurrently on different ports.

NAT/Firewall Traversal

Service delivery to subscribers behind Network Address Translation (NAT) devices and firewalls is often complicated as associated media and signaling protocols are often broken down. Most businesses today have NAT/Firewalls installed at their network edge; most residential DSL subscribers also have NAT/Firewalls bundled with their service package so the problem calls for a universal solution. While today's firewalls are able to dynamically open and close multiple ports as required by VoIP signaling protocols such as SIP and H.323, they remain ineffective at securely supporting both incoming and outgoing end-to-end media flows. NAT devices, on the other hand, prevent two-way voice and multimedia communication because the private IP addresses and ports used by IP devices (e.g. VoIP phones) are not routable in public networks.

SysMaster's SM 7000 offers NAT/Firewall friendly SIP implementation allowing seamless integration with existing NAT devices and firewalls. All devices communicate through outbound connections using protocols and ports that can transparently transit most business and home firewalls. The proxy-based solution architecture also ensures seamless work with NAT devices.

Quality of Service (QoS) enforcement

IP based services are notoriously associated with increased customer dissatisfaction and churn as service quality degrades. Typically as the number of users and their individual bandwidth consumption increases the overall Quality of Service decreases. This problem makes it difficult to manage differentiated service levels. A typical network device such as a router does not provide differentiated QoS based on session layer information such as user identity, media coding etc. Extracting such information from the signaling protocols, however enables service providers to implement sophisticated admission control and traffic management policies that allows them to offer per session chargeable SLAs typically demanded by business customers. Such information also enables carriers to enforce IP-IP interconnect agreements to deliver 'end-to-end' SLAs.

SysMaster's SM 7000 SS/SBC solution features real-time VoIP traffic prioritization, bandwidth utilization control and collection of detailed statistics. The solution enables VoIP traffic prioritization to minimize the impact of over-subscription on service quality. It enables service providers to offer managed IP services with guaranteed service levels that meet the needs of their customers while maximizing the utilization of the available network resources.

Network Security Enforcement

As IP networks are inherently insecure and susceptible to attacks, fraud and misuse, network security is one of the biggest concerns of service providers and enterprises. To address security issues, service providers need equipment that can restrict network access to only authorized users while hiding network infrastructure. A particular problem with IP voice networks is the need to conceal route sensitive information from third parties. For example, if a service provider A uses service provider B's termination services, and service provider C, who uses A's infrastructure finds out about B, then C would try to bypass A.

SysMaster's SM 7000 SS/SBC addresses security issues through its proxy mode of operation, which ensures traffic anonimization. The that mode the solution allows full RAS and RTP data transfer for gateways behind NAT or gateways that want to keep their identity. This bandwidth intensive mode fully controls the RAS and Q.932 data streams and also supports number translation and dynamic call control.

Conclusion

Service providers should seriously consider offering IP based voice and multimedia services as an attractive alternative for generating incremental revenues, reducing interconnection costs and increasing customer loyalty. To realize the full benefits of IP based services, however, they need to build IP infrastructures capable of delivering consistent quality of service to the end user. SoftSwitches/Session Border Controllers could help service providers solve most technical problems with IP networks integration and should therefore be considered as an integral element in any modern IP infrastructure.

About SM7000 Universal SoftSwitch/Session Border Controller Solution

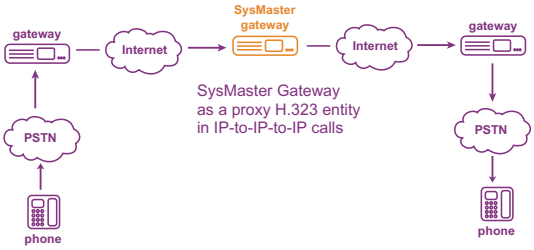
SysMaster's SM 7000 SS/SBC is designed to meet the service providers' needs for scalability, performance and high throughput. SM 7000 acts as a proxy H.323/SIP server redirecting H.323/SIP traffic as it enters and exits the service provider's network. Functionally the solution is comprised of H.323/SIP compliant gateway that handles voice codecs and protocols conversions and H.323/SIP gatekeeper that resolves call routing.

Gateway

The H.323/SIP compliant Gateway allows implementing flexible H.323 setups, hiding the source IP address of the origination party (traffic anonimization), SIP/H.323 packet conversion, and full codec conversion. Some of the key functionalities of the gateway include:

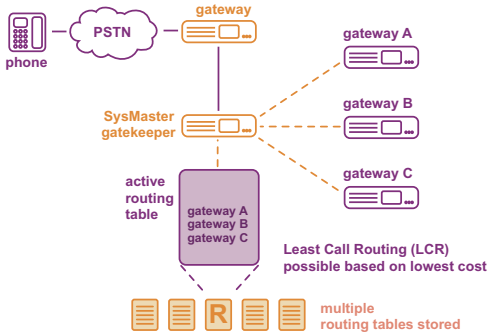
Traffic Anonimization

The gateway supports IP-to-IP-to-IP services in proxy mode or callback server mode. In this mode the gateway intelligently seeks to establish communications using the codecs that both end-gateways support. This way the throughput of the gateway increases significantly as the need for decoding/encoding the packages is eliminated. If a common encoding format cannot be found, the gateway translates the voice packets in format suitable for each end-gateway. The unique implementation offers flexibility for inbound calls to come via IP and go out via IP or PSTN based on the selected dialing plan/routing table. This gateway solution supports up to 1920 one-way VoIP channels and 480 PSTN/SS7 channels.



Custom Routes

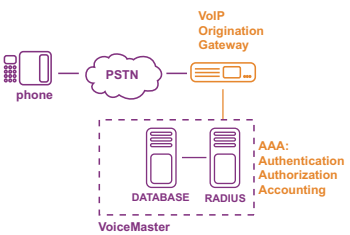
The gateway can use custom routes per termination gateway. Each route has "price" coefficient attached via predefined providers. In case a call route is serviced by multiple providers, the gateway in proxy mode can pick the least expensive route.



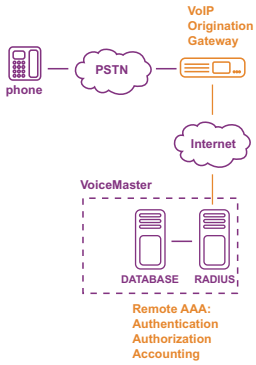
RADIUS Billing

The gateway can send to a RADIUS server call details record for all calls going through it. The CDR records can be later exported and viewed for billing purposes. In addition, the gateway can optionally play IVR messages over IP networks if this is required.

Local gateway/RADIUS communication setup



Remote gateway/RADIUS communication setup

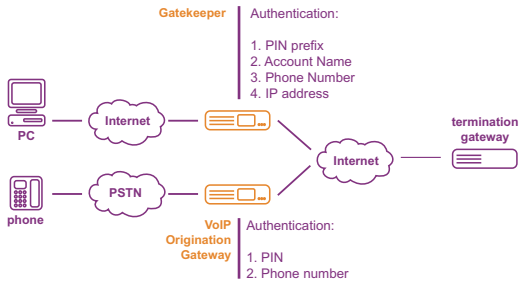


Gatekeeper

The H.323/SIP compliant Gatekeeper is the only gatekeeper in the industry that allows dynamic call control through a proprietary calling time authorization mechanismSome of the key functionalities of the Gatekeeper include:

Authentication

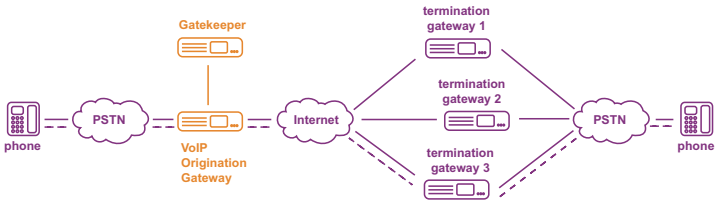
The gatekeeper supports the following methods of calling station authentication: IP address, Username (H323ID),PIN Number/Tech-Prefix, Caller ID (ANI), and any combination of the previous methods. The authentication is flexible enough to allow dynamic call authentication in environments where the clients change dynamically their IP addresses (such as IP Phone and Microsoft NetMeeting (TM) clients). The easiest way to implement dynamic client authentication is PIN Number/Tech-Prefix based. Simply use the standard PIN numbers to pre-pend to the phone number.



PC and Phone users are processed. The Gatekeeper allows for real time PC-to-Gateway and Gateway-to-Gateway billing and real time connection control is supported.

Optimized Routing Call Management

Optimized Routing call management is used when the company wants to optimize the call termination costs in real time. The algorithm allows dynamic call handling and call routing to select the most cost efficient termination point or provider. It requires the dialing plan management and gatekeeper functionality to be highly integrated to allow all dialing plan changes to be propagated to the underlying gatekeeper in real-time.



Actual call is dynamically routed through Gateway 3 because it offers the least cost per call

Authorization

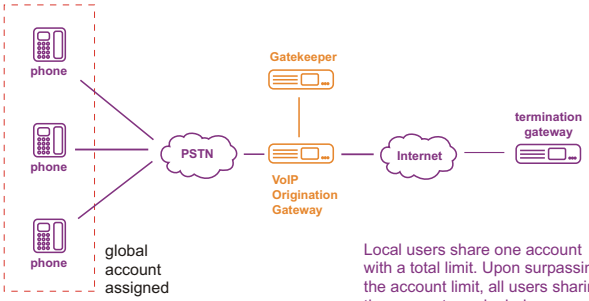
The gatekeeper supports dynamic authorization to provide a single point of entry to the routing system. By inserting new rates the service provider can change the billing and routing of each call. The gatekeeper supports the following routing mechanisms - Optimized Routing (including LCR), Preferred Provider Routing, Average Success Rate (ASR) Routing and Route Fail Over.

Modes of Operation

SM 7000 Gatekeeper/Session Border Controller supports several modes of operation. Direct/Static Mode allows call resolution without RAS message control. This mode will allow number translation and dynamic call control given that the participating gateways support canMapAlias attribute. Routed Mode allows direct control of RAS messages with very low level of bandwidth utilization. This mode allows number translation and dynamic call control for gateways that do not support canMapAlias attribute. Proxy Mode allows full RAS and RTP data transfer for gateways behind NAT or gateways that want to keep their identity. This bandwidth intensive mode fully controls the RAS and Q.932 data streams and supports number translation and dynamic call control.

Dynamic Call Management

SysMaster offers the only gatekeeper in the industry that will disconnect a call after its predefined time has elapsed . This unique dynamic call management functionality quarantines that all wholesale and user accounts are billed dynamically against calls in progress. Other features of the gatekeeper include dynamic call timing for single calls, support for wholesale multiple call timing, and support for concurrent calls.



Local users share one account with a total limit. Upon surpassing the account limit, all users sharing the account are denied access.

SysMaster
2700 Ygnacio Valley Rd, Suite 210
Walnut Creek, CA 94598
United States of America

Email: sales@sysmaster.com
Web site: www.sysmaster.com