Managing Costly Customers

October 2000

The HTRC Group

P.O. Box 2087
San Andreas, CA 95249
www.htrcgroup.com

About The HTRC Group, LLC

The High-tech Resource Consulting Group, LLC focuses on service provider networking, providing consulting,custom market research, and market research studies to service providers and product manufacturers.

Table of Contents

Introduction

Network service providers (NSPs) continue to witness an explosion in data traffic. Yet generating high-margin revenue and creating unique customer value from selling pure bandwidth remains a challenge. Competitive pressures have long since chiseled away the high margins on data access. Although NSPs are filling their networks with bandwidth, the revenue margins produced from that bandwidth are relatively small. One major reason is churn, and the costs associated with churn. One of the significant factors that contribute to churn is fraudulent behavior.

This white paper identifies the affects of costly customers and examines intelligent business infrastructure as a possible solution. Managing costly customers through an intelligent business infrastructure increases operational efficiencies and reduces costs.

The Business Environment

Not long ago, the only IP services offered were dial-up Internet access and email. As recently as 1995, most Internet users employed cutting-edge 14.4Kbps modems to connect to less than 200,000 Web sites. For the most part, Web sites were a novelty, constructed in fundamental HTML (HyperText Markup Language) with simple static graphics. Businesses were just beginning to understand the value of business-to-business communications using email, the first universal IP-based business service.

All service providers have a different view of the market, some being more cost conscious than others. Ongoing costs are largely influenced by how efficient networks are operated. The cost of network operations is a significant differentiation, and customer activity, such as fraudulent behavior has a dramatic effect on costs.

The Market

There are many ways to segment the service provider market, and for the purpose of this paper, we segmented service provider types into wholesale providers, retail providers, and free service providers. These segments may include ISPs, CLECs, ILECs, and IXCs. NSPs may offer multiple connection types to their customers, including dial-up, ISDN, DSL, T1 speeds and greater.

Wholesale providers provide their service provider customers with dial up infrastructure. These providers maintain large networks, often consisting of thousands of remote access ports deployed both nationally and internationally.

Retail providers sell Internet connectivity directly to end-users. They may or may not be facilities based. Most retail providers "rent" dial-up ports from wholesale providers. For example, AOL and Earthlink outsource dial-up infrastructure from wholesale providers. Retail providers own the end-user customer relationship.

Free service providers offer Internet connectivity to end-users at no cost. Most customers of free service providers are required to wade through banner advertisements in exchange for free Internet access. Most free providers rely on wholesale providers for dial-up Internet access customers. The revenue model for providing free Internet access continues to be uncertain, and thus is a model not suitable to every provider. Another free service provider, Freei Networks, has recently announced they are filing chapter 11, and selling their subscriber base to Netzero. Free providers have begun to examine alternative IP services as a new revenue source from their existing customer base.

Each of these service provider types capitalize on their core competency, wholesale providers who provide the infrastructure to downstream providers. Retail providers target end-users directly and are generally experts in marketing. Free providers operate on alternative revenue models, with some subsidizing Internet access with advanced IP services, such as applications rental. Although these providers have different revenue models, all have a need for an intelligent business infrastructure that can track customer IP behavior and identify fraudulent customers in real time.

Service Creation

IP service flexibility is critical in order to move forward in the market, as NSPs introduce new IP services in the network. There are two basic types of new services, proactive and reactive. Both are important strategies that address a competitive market. Proactive services are those services that are truly first to market, while reactive services are those that are replications of successful proactive services. For example, Exodus demonstrated a viable market for collocation services. Colocation facilities and services have since been replicated and are offered by many.

The value in being first to market with a successful IP service is short-lived, as other providers will quickly replicate any successful service. But time remains an essential factor, and the IP provider who can decrease the time it takes to develop, deploy, and deliver new IP services has an important competitive advantage. NSPs must have the capability of being first to market with a new service, as well as the capacity to resolve competitive threats. Business infrastructure is paramount in bringing usage-based IP services to market in an increasingly competitive market. NSPs require a business infrastructure that gives them the ability to increase operational efficiencies, detect fraudulent customer behavior, and deliver on the changing value proposition of IP services.

Customer Focus

Historically, NSPs have been limited in the services they could offer. IP services, with the rare exceptions of those providers who built their own equipment, were generally dependent on the functionality of networking products. The Internet access market has been fairly elastic

with mild competition. Access, however, has become increasingly commoditized, resulting in more competition and narrow margins.

In offering services to the customer, most NSPs have used an approach that focused on network and technology. Increased competition and new IP service-enabling technologies, such as a more intelligent business infrastructure, are facilitating a shift in service focus from the network to the customer.

Operations

Internet products and services are developed and deployed so quickly that NSPs reference product cycles in Internet yearsærather than normal calendar years. In the near future, service providers may quickly lose market share to faster, nimbler providers who capitalize on bringing differentiated advanced IP services to market first.

Some early Internet access market strategies have included gaining early market share through price differentiation by offering dial-up access at cost in order to gain market share. These providers were literally banking on their ability to increase operational efficiencies over time. Operational efficiencies are one of the most significant competitive advantages providers have today. Service providers need the technical as well as the business infrastructure to effectively compete in today's market.

For every provider, the cost of the network varies, largely depending on the degree of automation implemented in network operations. For example, most have automated customer registration; however, many smaller providers still have cumbersome static account registration. Bandwidth and network operational costs are also heavily influenced by how a provider interconnects with the Internet with public peering, private peering, and transport connections.

Fraudulent use of the network is a significant recurring operational cost that can be avoided. Automating fraud detection as well as a course of action to correct it will increase operational differentiation, and ultimately reduce the cost of providing services.

This flexible business infrastructure is critical, as competition has become a function of the value propositions of competing business models, not of the quality of network performance or the uniqueness of the latest technology. Competitive strategies based on business models are changing almost daily. Creating a robust business infrastructure gives NSPs the strategic agility necessary to react to these fast-changing market conditions and to refine the arsenal of IP services that reduce costs and bring value to customers.

Homegrown Solutions

The expertise of the network professionals who work for service provider organizations has a great influence on success. One challenge that service providers face today is obtaining and retaining qualified people. There are two ways to gain expertise, either develop it in-

house or acquire it. The churn rate of network professionals at a service provider organization will have a direct impact on the operational functionality and efficiency of the network. The churning of expertise creates significant problems in maintaining homegrown solutions, for problems arise when the people who created custom applications leave the organization. Providers are then challenged with attempting to modify custom homegrown solutions in order to address changing market demands.

For example, when a service provider employs a key person to build an important custom fraud detection solution, and that key person leaves, the provider is left with few people, if any, familiar with the custom solution and able to make changes needed to keep pace with business demands.

Building an intelligent business and network infrastructure can be costly. Every provider has had to make a decision regarding buying an off the shelf solution or developing a custom solution in house. Two key factors to remember when making build vs. buy decisions are: which solution is going to yield the greatest flexibility while scaling with success, and how quickly can new services and functionality be incorporated into the solution.

Fraudulent customer behavior

The business and network infrastructure that tracks service usage should also track fraudulent behavior. Real time coverage is required in order to take immediate action to stop fraudulent behavior and reduce costs. The services likely to be abused are simultaneous dial-up account use and abuse of "unlimited" Internet access. From our interviews with service providers, anywhere from 3% to 10% of dial-up customers will attempt fraudulent simulations of dial-up account use by sharing account information with co-workers, friends, and family.

When fraudulent customers are successful, they can cost providers in terms of occupying a port on remote access equipment, leeching bandwidth, and creating inaccurate information for network and bandwidth capacity planning. Many providers address fraudulent behavior by blindly provisioning additional remote access ports and upstream bandwidth capacity. As we mentioned before, customers that leave their dial-up connection on as long as they can are truly abusing access privileges. This problem can be remedied with manual time-out setting on remote access gear, however individual account information may not be tied into existing business infrastructure and this solution may not scale across thousands of ports.

Internet access is the most frequently abused service. However, Web site hosting is another service that can be abused. Dial-up access customers are generally offered a personal Web site with their account. Fraudulent behavior occurs when a customer posts adult content, driving usage well above allotted bandwidth usage. Advanced IP services offered by providers are also susceptible to fraud, and providers must track usage in real time in order to maintain good customer usage. Because the IP service market is difficult to predict, providers need the infrastructure which will enable them to track customer behavior for services not yet thought of.

Hacking and SPAMMING are two additional types of fraudulent customer behavior. In most cases, SPAMMING violates most customer agreements, and will cost in terms of email server resources, outbound bandwidth for outbound email, as well as inbound bandwidth for undeliverable email.

Hacking is mainly an annoyance to most service providers, as most are well versed in the latest security threats. However, when a teenage script kitty successfully gains control of a router, it can cost significantly in terms of the time it takes to reconfigure and refortify network equipment, not to mention being embarrassing.

Armed with fraudulent customer information, service providers can take action toward maintaining profitable customers. For example, costly customers who abuse unlimited access can be targeted with more suitable and profitable services, such as DSL or ISDN. Knowing customer behavior in real time enables providers to take action, either by targeting abusive customers with more suitable and profitable services or by terminating unprofitable user accounts.

The Cost of Owning Fraudulent Customers

Many providers are beginning to examine the total cost of owning fraudulent customers. The cost of fraudulent customer behavior varies significantly among providers, and will depend on services offered, existing fraud detection systems, and how fast fraudulent customers are dealt with. Based on our interviews, roughly one out of every ten dial-up customers gets a free ride with no return for the service provider.

Bandwidth

Aggregate fraudulent customer behavior can cost 1% to 5% of the monthly bandwidth bill. Premium bandwidth is not cheap, especially when bandwidth is not overly provisioned. The cost of bandwidth includes both the equipment that must be provisioned to account for fraudulent simultaneous dial-up and abuse of unlimited Internet access.

Churn

Battling customer churn rates continues to be difficult across the board. The reduction of Churn rates will have a positive impact directly on the bottom line. Costly customers can also increase monthly churn rates an additional 1% to 5%.

Operations

As we had previously mentions, the cost of network operations varies greatly among providers, and fraudulent customers may cost 1% to 3% of network operations. For this analysis, operational costs primarily include the salaries of people operating the network.

Fraudulent behavior can dramatically affect the cost of network operations and support. The costs associated with managing and maintaining fraudulent customers are generally estimated by providers to be a small percentage of their overall operational costs. While the operational percentage may be low, the total cost of network operations is significant.

Additional Considerations

Additional cost considerations include factors difficult to quantify, such as reputation damage and lost opportunity. Fraudulent use can tie up dial-up ports, effectively increasing the dial-up port to customer ratio. Busy modem banks and slow Internet access can quickly tarnish a provider's reputation. Lost opportunity is the most difficult factor to quantify; however, being hacked and encountering busy modem ports may drive away customers. These factors contribute to customer churn, effectively increasing the overall cost of sales.

The Bottom Line

Costly customers can dramatically impact the bottom line. In a market where access margins continue to thin, effectively reducing costly customers will have a positive impact on network costs. Profitability is becoming more of a priority with the financial community, and any initiatives focused on controlling costs and increasing operational efficiencies are strongly encouraged.

For most NSPs, growth is defined by the increase of paying subscribers, with the value of a service provider's subscribers roughly determined by a factor (generally influenced by the amount of subscribers) times annual revenue. The goal has been to increase the number of subscribers as fast as possible, thus increasing the value of the provider. There has been no economic way to identify the value of individual subscribers.

With an intelligent business infrastructure, NSPs can eliminate costly customers and determine the value of individual customers by identifying usage details. Not all customers are created equal. Some cost more than others, depending on network resources used, such as the small percentage of dial-up users who consistently tie up modem ports for lengthy periods of time. With an intelligent business infrastructure, NSPs can identify profitable customers and focus on retaining them.

Solution Criteria

Service providers are dependent on technological innovation for service creation and differentiation. There are both business and technical considerations to account for when evaluating new technology. Business considerations should include how a technology increases the capacity to bring a service or services to market, as well how flexible that technology is in accommodating changes. Technical considerations should include what network integration is required and how network operations will be affected. Following are some criteria to keep in mind when evaluating intelligent business infrastructure.

Performance

Performance is the largest differentiation for Internet-based services today, and it is also the hardest to accomplish. Performance can be defined in many different ways; for Internet access, performance is defined by reliably delivering fast connectivity. Service providers place great emphasis on extremely high availability, and strive to maintain good dial-up port ratios.

Extensibility

Intelligent business infrastructure should include an extensible framework that supports the creation and deployment of integrated operational and business support applications. The development of standards based "interface compatible" components that comprise the building blocks of IP services will enable NSPs to integrate everything from simple to very complex services quickly.

Support

Customers of service providers generally rate service and support as one of the most important criteria when choosing a provider. NSPs should choose a solution that can be integrated into existing customer care and support systems. Operational and emergency procedures should be well documented by both NSP and vendor in order to eliminate uncertainty if and when trouble arises. Solution vendors should provide 24x7 support including live and online information resources in order to solve problems that arise.

Security

The Internet is an eclectic environment that includes varying security requirements. The information from an intelligent business infrastructure solution must be secured to protect data integrity. Solutions should include a range of security parameters for providers to use, such as encryption algorithms (DES, triple-DES, Blowfish), key-exchange algorithms (Diffie-Hellman) and authentication mechanisms.

Reliability & Scalability

Expectations of reliability online continue to increase with time. Broadband deployments are changing users' expectations of Internet access performance. Because data networking is a magnet for Murphy's Law, business infrastructure should be tested for reliability and resiliency. Business and network infrastructure solutions should scale well beyond projected growth.

Conclusion

NSPs urgently require a flexible business infrastructure that can identify and manage costly customers, facilitates real-time billing, and resides on a modular framework in order to deploy IP services effectively in a rapidly changing market. Deploying an intelligent business infrastructure that detects costly customers will have an immediate return and a positive impact on the bottom line. Managing costly customers through a flexible business infrastructure that collects detailed IP information results in tremendous gain for NSPs.