ABUSE AND FRAUD DETECTION IN HIGH-SPEED-DATA NETWORKS

Why and How can HSD Operators deal with and profit from abusers

Pat Darisme, NARUS Inc.

Abstract: *As MSOs[1] are increasing penetration of 'always on' high-speed-data (HSD) service, some zealous users are abusively taking advantage of this low-cost, high-powered flat rate service. Some MSOs are painstakingly finding users who are running small ISPs from behind their residential cable modem, using a NAT box to share a single IP between multiple systems, running residential or commercial web servers, spamming mail servers or newsgroups or performing malicious attacks on other users. These users are expensive both in terms of the network resources (network bandwidth, CPU cycles, hardware upgrades) and with the man hours consumed in identifying & dealing with these users. Most of these issues are likely to remain problems even with the advent of DOCSIS 1.1. This paper will explore various types of abuse and methods of dealing with them.*

INTRODUCTION

The Internet started as a collection of academic and research networks, but since 1994 it has become a key part of North-American life in over 149 million households[A]. The advent of high-speed residential Internet access via Cable and DSL is providing residential users with 'always on' high-speed connections to the Internet. For a large percentage of subscribers these connections bring the known benefits of broadband (more bandwidth, lower latency, always on, no busy signals etc.). These connections also open the door to new types of abuse from a small percentage of customers.

Abuse in the context of HSD can be loosely defined as any behavior by a subscriber which violates legal statutes, or service provider policies, including activities which cause the subscriber to not pay for all the services consumed or resources (network, server, CPU etc.) consumed or to impact the quality of service of other network users.

As the Cable Industry sees an increase in penetration of HSD service (some large systems have passed the 20% penetration mark) it finds itself offering Internet access to a large number of North-American Internet users: over 5 Million in 2001 and over 19.5 million expected by 2005[B]. Along with a growing piece of the revenue stream comes increased necessity to police abusers.

This paper will address three questions:

1. Why identify and deal with Abusers
2. Who are the Abusers
3. What type of Abuse exists and what solutions can be applied

1) WHY IDENTIFY AND DEAL WITH ABUSERS?

HSD service providers need to identify abusers not simply to be good corporate citizens or cybercitizens but also because abuse increases operating costs, can decrease revenue and degrade the quality of service (QOS). The diminished QOS can lead to bad press and damage to the service provider and MSO's brand.

[1] MSO – Multiple System Operator a.k.a. Cable Operator

A. Operating Costs

Operating a high-speed data network involves high capital costs (routers, servers etc.) as well as high operating costs (bandwidth, staff etc.). When a few abusers increase network usage this can lead to increased capital costs in the form of network capacity upgrades, or higher bandwidth costs, both of which lengthen the path to profitability.

In a recent example, a service provider who offers a free hosting service as part of their product offering was concerned about growing bandwidth consumption and costs. They purchased an abuse detection system relying on real-time traffic Analyzers and an Internet Business Infrastructure Platform. Using this new system, customers who were abusing the free service by distributing large files such as MP3 and 'Warez'[2] files were identified and removed. The peak bandwidth consumption of their hosting service dropped from 600Mbps to 20Mbps leading to savings estimated at $150k/month (Their bandwidth cost was approximately $250/Mb)

B. Quality of Service (QoS)

Network abuse reduces the quality of the Internet service customers are paying for. Abuse consumes resources such as limited HFC (Hybrid Fiber Coax or Cable Plant) bandwidth, costly peering bandwidth, router and server CPU cycles, storage etc. and can even cause partial or full network outages. Limiting this abuse can reduce the frequency of operational problems, limit the necessity of system upgrades and improve the overall quality of the product offered.

o Quality of Service & DOCSIS 1.1

Cable Operators sometimes mistakenly think that DOCSIS 1.1, with its ability to implement rate limiting, will resolve all QoS issues. With DOCSIS 1.1 on the HFC, service providers still need to over-subscribe the bandwidth available both on the HFC and on the back end IP network and peering links. This is done to save costs because service providers expect subscribers will not all be consuming their allocated bandwidth at the same time, or all the time, and because of the burstable nature of IP traffic. While the subscriber may be entitled to only a rate-limited 128 kbps, data models do not expect that the subscriber will use this 128 kbps 24 hrs/day 7 days/week – yet this is what some abusive subscribers do by leaving streaming audio/video services on, or running Napster or other servers, on their 'always on' connection even in their absence. With the deployment of DOCSIS 1.1, HSD providers, will still be subject to various forms of abuse.

C. Bad Press

Abuse can cause a network outage, network delays (email delays are particularly popular), or security problems all of which can lead to bad press and dilute the MSO's brand. The Press seems to enjoy articles on network outages, especially when these occur at large brand name carriers. These negative articles affect the public's perception of the quality and value of the HSD service.

D. Revenue loss

The 2-way nature of high-speed-data makes traditional theft of service practically impossible. However, in a flat rate billing environment, it is possible for paying subscribers to use more services than they are paying for. This results in a loss of potential new revenue for the operator.

[2] MP3 files are audio files (typically music) which use the MPEG 3 compression standard.
Warez is Internet jargon for pirated Software

E. Peering

Service providers (or domains) who harbor abusers or who do not take steps to limit abuse on the Internet, risk having their peering connections cancelled by upstream service providers, having services shut down (e.g. Usenet Death Penalty) or having their domain added to Blackhole lists which filter traffic. This eliminates their ability to offer Internet access[3] or services (email / news). Limiting abuse can allow the service provider to maintain the network peering relationships and service feeds (such as email & NewsGroups) which are key to offering HSD services.

F. Law Enforcement Compliance

Some jurisdictions have regulations which may require service providers to have the capability to monitor the Internet activity of selected subscribers when requested. Having proper systems in place to track these subscribers may reduce the operational burden of compliance with these law-enforcement mandates which can come on very short notice and offer very little latitude.

G. Open Access / Multiple ISP Networks

Abusers can cause problems in traditional exclusive access HSD networks where the MSO bears both the full revenue and the burden of abusers. In this environment the MSO has full control over the customer and can either charge abusers for the usage, or shut them off. In Open Access or Multiple ISP HSD deployments the MSO may be getting only a small amount of revenue from abusers who are consuming disproportionate amounts of shared HFC bandwidth or services. In this Open Access environment, the MSO may not control the customer and the ISP may not be interested in co-operating with the MSO to identify abusers. Even if contracts ensure the ISP will deal promptly with abusers, compliance is more likely if the MSO has the ability to verify abuse. In the end the burden of protecting the limited resources of a shared HFC infrastructure rests solely on the shoulders of those who have invested in it and who must protect the quality and investment already made in their brand, the MSO.

There are multiple business reasons why a service provider needs to identify network abusers. Despite the issues described above, service providers often either ignore abuse issues or have a small team of dedicated staff who struggle in a reactive mode to contain damage rather than use the right tools to proactively prevent abuse.

2) WHO ARE THE ABUSERS?

There are different types of subscribers who can abuse the network. They can be loosely categorized as follows:

A. Hackers

Hacker is a term used by some to mean "a clever programmer" and by others, (especially journalists or their editors), to mean "someone who tries to break into computer systems.” (The Internet community tends to call those who break into computer systems ‘Cracker’.) Hackers are typically power-users who have a very good understanding of computer systems, protocols and programming, and who find great joy in learning more about and using the

[3] Though the canceling of peering links because of abusive activities (attacks, spam etc.) in a domain is somewhat rare this is mostly due to the fact that dedicated network operations’ staff have spent many long hours combing through network logs to eliminate abuse before being cut-off. This reactive approach drains resources which are better suited to designing and scaling networks.

power of computers. Some would argue that the Internet, Usenet and Unix/Linux were created and are maintained by hackers, whose skills can make them desirable engineers. One of the best-known hackers/crackers is the skilled and infamous Kevin Mitnick who was jailed for over 5 years following some computer attacks in 1994.

B. Script Kiddies

These are novice users who would like to be known as true hackers but who resort to downloading or copying simple programs posted on the Internet. 'Script Kiddies' run these scripts - often without understanding the exploit - either out of curiosity, in hopes of achieving notoriety, or to get even with someone they are unhappy with. The downloaded programs, or scripts, are automated ways of generating large amounts of traffic or other network disturbances; they affect the victims' network connectivity and potentially result in an outage. One recently well known 'Script Kiddie' is the 15 year old - identified as 'MafiaBoy' - arrested for the attacks on popular internet sites such as Yahoo, eBay and Cnn.com in the spring of 2000.

C. Unwilling victims (Trojans)

Subscribers can unknowingly generate unacceptable traffic when their computer becomes compromised either by downloading software which contains a virus or exploit, or when an intruder places such software on their computer following a break-in. This software can be set to generate or relay large amounts of data following some trigger (time, program execution, external trigger etc.).

D. Fraudulent Businesses

A subscriber can be running a fraudulent business such as a pyramid scheme or some other 'make money fast' system, such as selling cable decoder boxes or providing illegal services. They may have subscribed to high-speed data services for the sole purpose of running their business from home.

E. Criminals and Terrorists

HSD subscribers are not unlike most other segments of the population, which means that a certain percentage of subscribers are also engaging in criminal activities and using their Internet connection as a means of facilitating or perpetuating these activities.

F. Regular Subscribers

Some level of 'abuse' will simply be due to regular subscribers. These may be power-users who are ideal candidates for a premium service offering; or telecommuters who have use that is much higher than average or that violates AUP guidelines (perhaps by connecting multiple PCs to a single Cable Modem connection).

3) WHAT TYPE OF ABUSE EXISTS AND WHAT SOLUTIONS CAN BE APPLIED?

In the following sections we will explore the different types of network abuse, and for each, the type of people who cause it, its impact and different service provider solutions.

A. Spam or excessive messaging

'Spam' is Internet jargon for what is also known as Unsolicited Commercial Email

(UCE). This is loosely defined as multiple[4] messages with substantially the same content. These messages can either be email or newsgroup postings. They can be destined to one or more recipients or newsgroups[5]. Typically they have subject lines such as ‘Make Money Fast’ or ‘Free Cable TV’ or ‘Free Porn’. Recently there has been an increase in email viruses[6] which spread quickly through the Internet, congesting mail servers at service providers and corporations. These can also be considered Spam.

- Who – ‘Fraudulent businesses’ using Spam for marketing. Hackers / Script Kiddies or even regular Subscribers may also - out of malice, vengeance or desire for recognition - generate excessive messaging.

  Messaging problems can be caused by a subscriber within the Service Provider’s network or can originate on the general Internet.

- Impact – Quality of Service (QoS), Bad Press & Cost, traffic filtering
  These multiple messages congest servers (mail & news), consume precious CPU cycles, fill storage space, and consume network bandwidth. Messages are queued as the limited servers struggle to process their increasing number. Delayed or lost messages that ensue, lead subscribers to become quite vocal. On some occasions the press may even be alerted to the problem, causing potentially negative exposure to the brand and the underlying product.

  These problems generally lead the service provider to scale the messaging system by adding hardware and bandwidth to meet the ever-increasing load. This is a costly way of dealing with abusers in the HSD business where capital costs of servers are significant and flat rate pricing provides for unlimited usage.

  A Service Provider who is often a source of Spam may see their domain (it’s associated IP addresses) added to popular blackhole lists[7]. This means their email, and perhaps other Internet traffic, gets filtered and will not reach recipients in multiple domains. If an HSD provider’s domain becomes known as the source of Spam it can rapidly be added to these blackhole lists. This happened to @Home’s domain on various occasions according to Cathy Wittbrodt who was Director of Routing Engineering at @Home Network from 1996 to 2000.

  Unfortunately the damage is already done when subscribers complain, servers are filled to capacity, the domain is ‘blackholed’ or when the press calls asking for comments. A reactive approach can only attempt to contain or repair damages. For these reasons and more, it is advantageous to proactively prevent Spam.

  Service Provider Solutions

- To defend from Spam originating on the general Internet, Service Providers can purchase a third party mail service[8] which filters out known Spam domains. These third party services do help to limit Spam from the Internet but do not address Spam generated by

[4] Though the exact amount of “multiple’ or ‘n’ hasn’t been clearly defined, partly because violators would then simply send ‘n-1’ unsolicited messages, an generally accepted number is 20.

[5] Cross-postings or a same message posted to multiple newsgroups are typically called ‘ECP’ or Excessive Cross Postings and are a form of Spam.

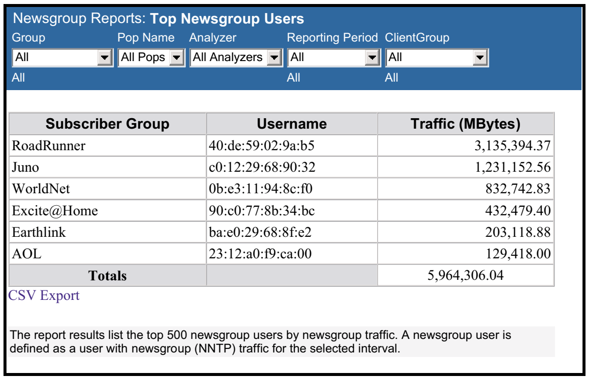
[6] ‘I Love You’ and ‘Naked Wife’ are the most recent email virus subject lines

[7] MAPS - Mail Abuse Prevention System LLC (MAPS) [www.mail-abuse.org] is the maintainer of one such mail list that approximately 40% of all Internet Addresses use to filter out known Spam domains.

[8] BrightMail [www.brightmail.com] provides one such service.

internal subscribers, which requires prompt internal response to prevent it from congesting the network.

If the ‘Spam’ originates on the HSD provider’s network there is more flexibility and need to deal with the problem. Once the abuser is identified, if the source is on the Service Provider’s network, the subscriber can either be eliminated or moved to a more appropriate billing plan.



Newsgroup Reports: **Top Newsgroup Users**

Group	Pop Name	Analyzer	Reporting Period	ClientGroup
All	All Pops	All Analyzers	All	All
All			All	All

Subscriber Group	Username	Traffic (MBytes)
RoadRunner	40:de:59:02:9a:b5	3,135,394.37
Juno	c0:12:29:68:90:32	1,231,152.56
WorldNet	0b:e3:11:94:8c:f0	832,742.83
Excite@Home	90:c0:77:8b:34:bc	432,479.40
Earthlink	ba:e0:29:68:8f:e2	203,118.88
AOL	23:12:a0:f9:ca:00	129,418.00
Totals		5,964,306.04

The report results list the top 500 newsgroup users by newsgroup traffic. A newsgroup user is defined as a user with newsgroup (NNTP) traffic for the selected interval.

Figure 1: Abuse Detection Report showing users generating over 3 GigaBytes of NewsGroup traffic over a 7 day period.

Real-Time Analysis

Communications software can monitor the number or recipients of messages (email/news) sent by subscribers, while ignoring the content in order to maintain privacy. Real-time software can generate an alert when a threshold is met allowing the service provider to act immediately once the nth email is detected, rather than waiting for an outage to be created when excessive damage is done.

Mediation software

Mediation can also be used to threshold the number of messages, such that messages beyond a threshold can be billed (e.g. 50 free emails/week, $1 each additional email) effectively turning the abuse into revenue. This approach acts as a deterrent to excessive messaging, while potentially increasing revenue.

B. Reselling of bandwidth

Bandwidth resale involves the use of a single subscriber connection (single IP address, flat fee service ~$44.95) for more than one PC. Examples of this are offering ISP services to neighbors or sharing the connection between multiple PCs, typically using a NAT server[9].

- Who – ‘Hackers’, ‘Script Kiddies’, Home based businesses, college students and corporate telecommuters are the types of subscribers who will purchase an unlimited bandwidth single connection and share it amongst multiple PCs. With the decrease in PC prices and the availability of home networking equipment, typical home users are also beginning to connect multiple PCs behind a single cable modem.

- Impact – Quality of Service, Cost, Revenue When a residential connection is shared by multiple systems it typically leads to higher data-consumption than is anticipated in the traffic and data modeling assumptions that go into capacity planning of the network. The Quality of Service drops as limited bandwidth (either HFC or peering) is consumed by this higher than expected usage. Costs can also increase as additional capacity is purchased either in the form of additional spectrum allocated to the HSD service, or additional bandwidth purchased from the upstream ISP. Since premium service offerings (offering multiple IP addresses) are not purchased, revenue also suffers.

[9] NAT [Network Address Translation] servers use a single IP address (provided by the Service Provider) to allow an unlimited number (typically up to 253) of additional IP Clients with individual IP addresses to share that single IP address and it’s bandwidth. NAT servers can be a Linux or Windows server running special software, or be included in firewall / router systems which connect behind the Cable Modem. NAT servers are sometimes called ‘proxy’ servers.

- Service Provider Solutions

Since NAT servers mask the multiple IP addresses of their clients they are very difficult to detect. NAT servers leave no traces on servers rendering log file parsing pointless. There are only two options for service providers to deal with NAT servers:

Usage based billing - Sharing a network connection is only profitable to customers because of flat rate billing models. Usage based billing models immediately defeat this type of abuse, or more properly align network expense to revenue generated. Much like people would never consider sharing their Cell phone or long-distance service which are billed on usage, an HSD bill based on the bandwidth or services consumed is less likely to be shared.

Real-Time Analysis – Analyzers monitoring the patterns of IP streams can potentially identify certain signatures of IP streams which are carrying IP content destined for different PCs'. Prototype NAT detection systems relying on these signatures have been designed. Though expectations are positive, these have yet to be tested.

C. Residential Server Hosting

Subscribers can use a residential HSD connection to run servers of any kind. The most frequent type of server encountered is an HTTP server, however many other servers including FTP, Mail, Telnet, news, streaming video, Peer-to-Peer (Napster) and others can generate upstream bandwidth. Home DHCP servers can serve the wrong IP addresses to other subscriber PCs causing isolated outages.

- Impact – Quality of Service, Bandwidth, Revenue, Outage

QoS & Bandwidth - HSD systems are deployed with the assumption that bandwidth consumption is asymmetrical with much heavier downstream usage, as such downstream capacity on the HFC portion of these HSD systems far exceeds upstream capacity. Servers violate this assumption congesting the upstream bandwidth leading to degradation in the quality of service. Even with QoS policies like DOCSIS 1.1's rate-limiting, home based servers can still generate large consistent usage (albeit with reduced throughput) as the servers are accessed at all hours from the always active Internet population, rather than following the usage patterns of a more 'typical' subscriber.

According to an @Home abuse manager, an MSO used active polling to check every connection in a 20,000 subscriber system for the presence of home servers. "Out of 20,000 subscribers they found 969 servers consuming 34% of the system's bandwidth".

Revenue - Some HSD providers offer a more expensive or premium product for server hosting; unfortunately subscribers are unlikely to sign up for the pricier version when the entry-level product provides the same functionality. Even with DOCSIS 1.1 rate limiting, many subscribers are likely to settle for the expected 128k rate-limit for their home-based servers.

Outages - Home DHCP servers cause isolated outages for neighboring subscribers who may receive the wrong IP address and thus not be allowed on the network.

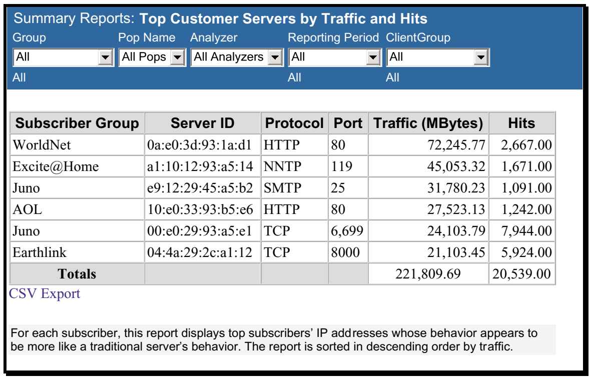
- Service Provider Solutions

As home based servers do not leave any log file trails on service provider servers they can be difficult to detect but there are 3 options to deal with them.

SNMP – standard SNMP MIB (DOCSIS & MIB II) data collected from the modem can give a count of the number of packets sent and received by the modem (since the last modem reboot[10]). Although a high amount of sent packets (some call this a 'top talkers report') may be a hint of a home server, it could also simply be someone sending large email messages (perhaps containing pictures of their new-born) or uploading files to their hosted service someplace on the Internet (i.e. Homestead or GeoCities community web pages). Also, a 'top talkers report' gives no indication as to the port or service on which this potential home based server is running. SNMP data collection also places additional bandwidth on the network, potentially increasing congestion.

Active Polling – A system can be dedicated to actively poll successive ports from every subscriber IP address on the network in search for a server. Given that a server can run on any TCP port between 1 and 65,535[11], many successive polls (over 65 thousand polls per subscriber) are required on a typical system to identify servers. Using active polling generates traffic on the network and may well return a false negative if the polling packet receives no response for various reasons which can include a dropped packet, a server which is periodically shut-down or a server which is configured to be unresponsive to certain IP addresses or request formats.

Real-Time Analyzer – A real-time Analyzer that can see all IP sessions can easily identify the top home servers both by bandwidth and by hits, while also identifying the port on which these are running. This gives the Service Provider a clear list of the top residential servers, as well as the necessary information to go after them and either up-sell them to a higher service, or insist the subscribers shut down the servers.



Summary Reports: **Top Customer Servers by Traffic and Hits**

Group: All
Pop Name: All Pops
Analyzer: All Analyzers
Reporting Period: All
ClientGroup: All

All
All
All

Subscriber Group	Server ID	Protocol	Port	Traffic (MBytes)	Hits
WorldNet	0a:e0:3d:93:1a:d1	HTTP	80	72,245.77	2,667.00
Excite@Home	a1:10:12:93:a5:14	NNTP	119	45,053.32	1,671.00
Juno	e9:12:29:45:a5:b2	SMTP	25	31,780.23	1,091.00
AOL	10:e0:33:93:b5:e6	HTTP	80	27,523.13	1,242.00
Juno	00:e0:29:93:a5:e1	TCP	6,699	24,103.79	7,944.00
Earthlink	04:4a:29:2c:a1:12	TCP	8000	21,103.45	5,924.00
Totals				221,809.69	20,539.00

CSV Export

For each subscriber, this report displays top subscribers' IP addresses whose behavior appears to be more like a traditional server's behavior. The report is sorted in descending order by traffic.

Figure 2: Sample Customer Server Detection Report listing top customer servers with related ISP (Open Access environment) CM MAC address, port and traffic.

Usage based billing – Home-based servers increase the amount of bandwidth (mostly upstream) used by a residential connection. A Billing model based on the bandwidth consumption will simultaneously deter customers from using the connection to host a web site or share Napster files, while increasing the revenue collected from those users who persist. Flexible mediation systems can allow service providers to offer free or low-cost usage up to a low threshold, while increasing the price for those users who host home servers. This turns the abusive and costly subscribers into lucrative customers.

D. Excessive Bandwidth use – High Traffic subscribers.

Data collected in production HSD networks has shown that a small percentage (<1%) of subscribers account for over 20% of the total bandwidth consumed. This is typically due to these select few subscribers taking advantage of the flat rate billing to download huge amounts of content from Internet File Servers,

[10] Some subscribers are rebooting the Cable Modem at frequent intervals in order to destroy the MIB Interface counters which are stored in volatile memory.

[11] TCP Ports are typically implemented as a 16 bit counter ~ $2^{16} = 65,536$

or leaving streaming audio (NetRadio) service on for hours, even in their absence. More sophisticated users run 'bots' against newsgroups in order to fill their hard-drive with all of their favorite pictures and software which are automatically downloaded throughout the day and night.

- Who – regular subscribers who fail to realize that NetRadio services consume bandwidth and power users who love newsgroups , etc.

- Impact – Cost, Revenue, QoS
When the HSD system reaches its maximum capacity, subscriber growth is impacted by the limited HFC or peering bandwidth. Dealing with those few (<1%) high traffic subscribers can allow the system to reclaim bandwidth and add as much as 20% more subscribers before upgrading peering links or dedicating more spectrum to HSD services.

- Service Provider Solutions - High traffic subscribers can be addressed in 3 ways

  SNMP – collecting MIB information from the CMTS & CM provides the number of packets in / out of a modem since the last modem reboot[12]. Collecting this MIB data allows the service provider to identify the top users, but SNMP polls also contribute to the bandwidth congesting the network.

  Real-Time Analyzers – Real-time analyzers on the IP infrastructure can produce reports of the top subscribers by total traffic, upstream and downstream traffic. This allows the Service Provider to quickly identify the top users as well as the protocol or services they are using, without adding bandwidth to the network and regardless of modem reboots.

  Usage based billing – Much like how residential long distance and cell phone use is not abused, subscribers are less likely to leave NetRadio services on when they leave the house if they are being charged for the amount of bandwidth or services used.

E. <u>Mis-configured systems – IP theft</u>

Subscribers can mis-configure their client PC either deliberately or erroneously. This usually involves 'IP Theft' where the main PC or a second PC is statically[13] configured with the wrong IP address. In some systems DHCP servers run in promiscuous[14] mode offering an IP address to every PC the subscriber connects.

- Who – Both Hackers and regular subscribers can decide they want to connect a second or third PC behind the Cable Modem without paying for the additional IP address.

- Impact – Quality of Service
When a subscriber uses the IP address that is assigned to another subscriber, the latter will either experience heavy packet loss or a service outage. Operations staff and CSRs must then spend many hours tracking down the source of the problem if they do not have the proper tools.

- Service Provider Solutions – It is very difficult to identify the subscriber who uses the wrong IP address. In some cases SNMP[15] can be used

[12] The DOCSIS specifications do not require the CMTS to maintain bits in/out counters; these are kept in Volatile memory the CM and are reset to zero following a CM reboot.

[13] Static configuration is where a subscriber hard-codes the system IP address. This is different from dynamic configuration where the IP address is assigned by a Service Provider maintained DHCP server.

[14] In promiscuous mode a DHCP server does not require a system identifier (such as a host name or MAC address) before it provides an IP address.

[15] This depends on the granularity of the Cable Modem MIB.

to successively check each modem looking to see if its Client PC is configured with the stolen IP address.

F. Attacks

There are a number of IP based attacks for which subscribers can be either the originator or the target. Intrusions (user breaks into an other users system), denial of service^C (TCP synflooding, ICMP attacks, smurfing[16] etc.), virus distribution, portscans[17], forgery campaigns, censorship attempts, etc. are some of the attacks that are seen in IP networks.

- Who – Script Kiddies and Hackers are, by definition, the subscribers who use the Internet to attack other subscribers. These can be random attacks, to learn or test the effects of an exploit, or attacks to gain notoriety in the online community.

- Impact – Quality of Service, Bandwidth, Bad Press
When an HSD network is the recipient, these attacks can consume huge amounts of bandwidth and even generate an outage (such as those which crippled eBay, CNN and other leading web sites in the Spring of 2000).

When an HSD network is the source of an attack, other providers will expect the originating Service Providers operations staff to quickly stop the attack and may not hesitate to shut down peering interfaces in an effort to protect their networks from the attack. When peering links are shut down quality of service is directly affected as traffic either cannot reach its destination, or must be re-routed over a longer path.

A victim whose computer is attacked may expect the service provider to offer reasonable protection. Even if the service provider doesn't offer a 'managed or firewalled' connection, it may be reasonable to expect that the service provider would identify and block some attack traffic such as preventing the subscriber's entire 512 kbps rate-limited connection from being saturated with attack traffic.

Attack reports are common topics for press articles on 'CyberCrime' or network outages and can damage the brand and the public perception of the HSD service offering.

A Service Provider can discover an attack after being notified by either another service provider, an attacked customer, or multiple subscribers complaining of an outage or poor service or even the press. Once people are complaining about the attack, the service provider is caught in a reactive mode and much of the damage is already done.

- Service Provider Solutions:
Real-Time Analyzer – A real-time analyzer can monitor IP traffic on the Service Provider‘s network and alert them to increases in traffic, or certain patterns of traffic such as portscans.

G. Illegal activities

Some behavior is not only against the AUP but is simply illegal. Gambling, child porn, fraud, theft of information, software piracy, copyright infringement etc. are all illegal activities which can be perpetrated with the assistance of a HSD service.

[16] Smurfing - Denial-of-service attack consists largely of the use of forged ICMP echo request packets and the direction of packets to IP broadcast addresses rapidly congesting the network and quickly leading to an outage.

[17] In a portscan a user looks at all IP ports to find a vulnerability to exploit perhaps to gain access to, or simply crash the system

- Who – Fraudulent businesses engage in activities such as gambling, software piracy and fraud. Hackers typically believe software should be free and are known to perform software piracy.

- Impact – While these activities may not affect the HSD Service Provider's network or business model, authorities may require, with proper warrants, the service provider to co-operate in selected investigations by providing data on involved parties who are subscribers. This can consume operational resources as staff parse logs in search of the requested data.

- Service provider Solutions
  There is little a service provider can do to prevent or quickly identify this type of illegal activity. The best option is to use a real-time Analyzer system which can track certain activities and store these in a database for later retrieval. However, knowing that service providers did not have the proper tools to track illegal activities the FBI has come up with software called 'Carnivore[18]' which tracks Internet access for law-enforcement.

CONCLUSION

Various forms of abuse in service provider networks can be costly whether in terms of lost revenue, deterioration in quality of service, premature system upgrades, bad press or network downtime. As the subscriber base grows in High-Speed-Data systems, Service Providers are continuously faced with the cost of upgrading capacity. In some cases it may be more economical to reclaim bandwidth lost to abuse than to purchase and upgrade capacity. Since reactive approaches can only attempt to contain damage, reclaiming lost bandwidth is best done with a proactive monitoring approach.

Network equipment such as routers, switches and modems can provide some network information (e.g. SNMP or RMON data) but are fundamentally built to forward packets and provide reliable IP services, and are not designed for the granular real-time data collection required for abuse detection or mediation. Dedicated hardware appliances are the only tools with the flexibility to provide systematic real-time identification of Spammers, home servers, bandwidth 'hogs', IP address theft and some forms of attacks, while operating at wire speeds up to Gigabit Ethernet or OC-12 (both of which are ubiquitous in today's HSD networks).

In addition to identifying various forms of abuse, a scalable software infrastructure (Internet Business Infrastructure) relying on real-time analyzers can help the service provider implement usage based or tiered billing services, which deter from abuse, both across DOCSIS 1.1 services and over the existing legacy subscriber base. Though there are different ways of dealing abusive customers, usage based billing models with granular measurements will both deter abuse and turn those persistent abusers into some of the most lucrative subscribers.

[18] http://www.fbi.gov/programs/carnivore/carnivore.htm

ABOUT THE AUTHOR

Pat Darisme is a Broadband Strategist and Principal Systems Engineer with NARUS Inc., the leader in Internet Business Infrastructure Solutions. During his time at NARUS he has helped design a decision support and abuse detection system for HSD Service Providers and open access environments. Prior to joining NARUS he was at Excite@Home Network where he worked in Operations and Engineering. He holds a B. Sc. in Electrical Engineering from Universite Laval in Quebec city, Canada. He can be reached at patd@narus.com.

[A] Source: Nielsen//NetRatings Global Internet Trends, Q2 2000, http://www.eratings.com/news/20000907.htm

[B] Source Forward Concepts, Broadband in the local loop '00, 2000 http://www.forwardconcepts.com/press26.htm

[C] CERT® Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks http://www.cert.org/advisories/CA-1998-01.html