



**IronPort's  
scalability and  
email throttling  
help us combat  
spam and  
conserve network  
resources.**



**BOB BOSCO**

Director  
*HSD Mail, News, Web*



## IronPort Understands ISPs.

### SITUATION

Charter Communications is the 4th largest US cable company. With more than 6 million cable subscribers, Charter provides email accounts for over 1.7 million users. Email growth and the rise in spam and viruses stressed Charter's networking infrastructure and increased the management burden on the operational staff. Charter faced the challenging dilemma of combating these issues while needing to minimize capital and operating expenditures.

### TECHNICAL CHALLENGES

Spam presents several issues for ISPs like Charter. First, spam creates a nuisance for customers. Keeping customers satisfied and minimizing churn requires curtailing spam and preventing viruses from reaching their inboxes. Charter initially fought the spam problem with open-source spam filtering software. Most open-source spam filters cannot match the capture rate of commercial solutions while maintaining a low false-positive rate. In addition, open-source filters usually require substantial management overhead and constant tuning.

Another impact of spam is the increased load on the existing infrastructure. Spam comprises well over 50% of inbound email for most large ISPs.

>>>

### CHARTER COMMUNICATIONS AT A GLANCE

Revenue: >\$4 billion  
Internet Subscribers: 1.7 million  
Email Volume: >150 million/day

### THE IRONPORT ADVANTAGE

- Throughput and capacity increase
- Throttling of email volume
- Flexible policies for different email subscribers

Originally, Charter deployed a gateway solution that used an open-source MTA running on multiple general purpose servers. While this infrastructure provided a solid foundation, it could not keep up with the explosive mail volume.

Lastly, spammers represent the largest abusers of Charter's network infrastructure. The most common method for spamming entails sending illicit email via hijacked personal computers on ISP networks. In most cases, end users are not even aware the fraudulent use is occurring. Maintaining service for legitimate email senders while preventing abuse by spammers creates a challenge unique to the ISP market segment.

### THE IRONPORT™ SOLUTION

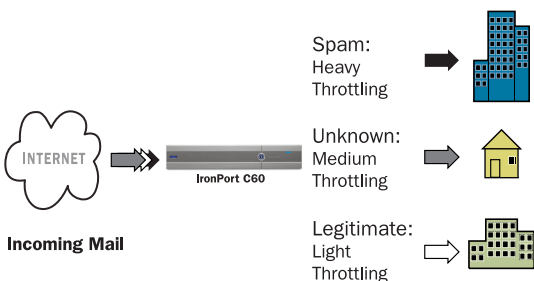
Charter uses two unique tools of the IronPort C60 email security appliance to combat these issues, throttling and Reputation Filtering.

The IronPort C60 appliance allows Charter to divide email senders into unique categories (IP address, domain name or sender reputation) and provides specific message-based rate limit thresholds for each sender.

Rate limiting acts as a highly tuned throttle for mail volume, when a throttle limit is exceeded the IronPort C60 will temporarily reject more mail from that sender.

IronPort Reputation Filtering™ also plays an important role in addressing the problems facing Charter's infrastructure. Reputation filtering allows email administrators to sort email senders based on the quality of mail they send. The poorer the reputation, the more likely the email sender is a spammer. This allows application of restrictive policies to spammers and more liberal policies to legitimate senders.

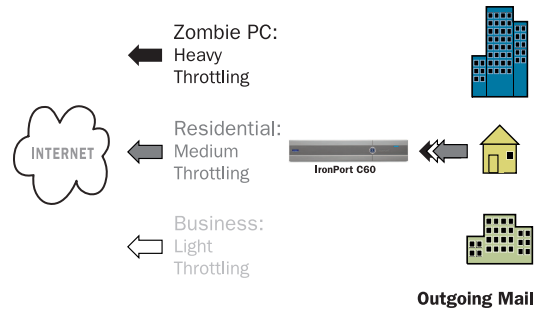
The combination of throttling and Reputation Filters helps address two major pain points for ISPs such as Charter: preventing spam from reaching customer



The IronPort C60 email security appliance allows administrators to easily manage incoming email by setting unique thresholds based on sender reputation.

inboxes and controlling spam originating from customer PCs.

To minimize the amount of spam that reaches Charter customer inboxes, known bad mail is throttled heavily and known good mail is provided more generous rate limits. With Charter's daily volume of 150 million



The IronPort C60 enables ISP administrators to throttle outbound email based on unique user groups.

messages, the IronPort C60s stop 50% at the perimeter of the network.

Throttling also minimizes the amount of spam sent from hijacked PCs in Charter's customer infrastructure. If a customer PC generates high volumes of mail that exceeds a typical customer threshold, further mail flow is temporarily blocked, thereby reducing the amount of spam traversing Charter's mail servers. Hijacked hosts are prevented from having unrestricted access to blast the internet with spam.

### POWERFUL MTA

The IronPort C60 email security appliance is a powerful Mail Transfer Agent (MTA) built from the ground-up to address the challenges corporations face managing email. IronPort designed it's email security appliance specifically for high volume environments like Charter's.

IronPort Systems' AsyncOS is a new software architecture engineered to address concurrency-based communications bottlenecks and limitations of file-based queuing. Supporting in excess of several hundred thousand messages per hour, the IronPort C60 appliance allowed Charter to reduce the total number of servers required to manage email while ensuring a scalable platform for the future.

"IronPort's scalability and email throttling help us combat spam and conserve network resources," said Bob Bosco, director HSD Mail at Charter Communications.



**IRONPORT™**

**IronPort Systems, Inc.**  
1100 Grundy Lane, Suite 100  
San Bruno, California 94066  
tel 650.989.6500 fax 650.989.6543  
email info@ironport.com  
www.ironport.com

### ABOUT IRONPORT SYSTEMS

IronPort Systems is the leading email security provider for organizations ranging from small businesses to the Global 2000. The company has developed a family of email security appliances, the IronPort C-Series™, that offer breakthrough performance, unprecedented ease of use and reduced total cost of ownership. IronPort is driving new standards and providing innovative products for those faced with the monumental task of managing, protecting, and growing mission-critical email systems. For more information on IronPort products and services, visit: [www.ironport.com](http://www.ironport.com)