



With QVISION™ Aliant Identifies Source of Increasing Bandwidth Resulting in Significant Cost Savings

Company at-a-glance:

- Global internet service provider based in Atlantic Canada
- Network supports approximately 140,000 dial-up customers and 60,000 high speed customers

“For the first time our network specialist in core network engineering has been able to discover and stop denial of service attacks before they take down part of our network.”

Bob Justason
VP of engineering, Aliant
Telecom, Inc.

QVISION provided verification of network misuse and abuse which enabled swift and appropriate response.

The Situation

Bandwidth is extremely important to an internet service provider (ISP). When excessive bandwidth is used, it can result in high costs and slow service for customers. When Aliant, a global ISP based in Atlantic Canada, saw a doubling of traffic utilization on their backbone it turned to QVISION™ for answers.

Aliant was reaching traffic of 1200 Megabits per second per month. Since the ISP was paying its Tier 1 provider based on usage, bandwidth costs were skyrocketing. The current bandwidth costs were causing an expense budget of \$5.8 million to be overrun to \$7.5 million.

The Solution

After installing QVISION, Aliant was able to see that the traffic was a combination of Denial of Service/Distributed Denial of Service attacks and extensive peer-to-peer file sharing applications.

Using the aggregate information available through QVISION, Aliant created filters and network routes to improve the use of its bandwidth. The ISP drilled down further into the graph to look at remote destinations so popular content could be mirrored more effectively.

The Result

These adjustments allowed the bandwidth subscription from the Tier 1 backbone provider to remain under 1000 Megabits. Over an eight-month period, this resulted in a **\$1.6 million savings** in expenses, and it improved customer service substantially.

Aliant estimated that 50 percent of cancellations of service were attributed to Denial of Service attacks, which caused service failure or congestion. The estimated annual revenue protection provided by implementing QVISION is \$2.09 million. The estimated annual expense protection in terms of acquiring a customer is \$1.18 million. The total estimated 12-month expense reduction and revenue protection is \$3.27 million.

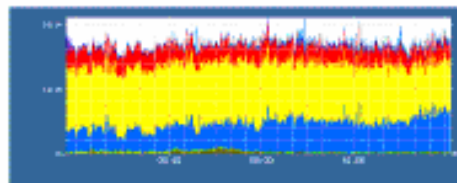


Illustration 1: network utilization visualized as soon as QVISION™ was installed

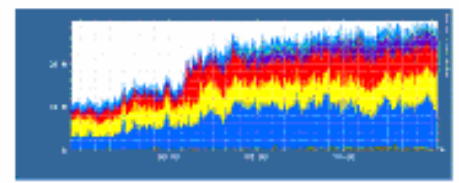


Illustration 2: network utilization visualized once corrective actions were taken based on QVISION™ visualization

The first illustration (Illustration 1) shows traffic before optimization, incoming from two backbone internet providers (yellow, and blue), from a sibling internet service provider (red), and from a local caching mechanism (purple and cyan).

By optimizing their network (Illustration 2), the ISP significantly reduced their use of expensive bandwidth from one backbone provider (yellow), and increased its use of cheaper caching (purple, cyan) and sibling (red) traffic.

