Table of Contents

Introduction ................................................................................................................................ 2
What’s the Problem? ................................................................................................................. 3
What’s the Solution? .................................................................................................................. 4
  Visibility – the keystone of *Network Intelligence* ................................................................. 4
  Optimizing traffic to deal with ever-growing bandwidth usage .............................................. 6
Optimizing Video Traffic using Intelligent Media Acceleration .................................................. 7
  Filtering illegal content .......................................................................................................... 8
  Increasing ARPU ................................................................................................................... 9
  Network security .................................................................................................................. 10
  Typical deployments ............................................................................................................ 11
Conclusion ............................................................................................................................... 11
Introduction

Today’s Internet Service Providers (ISPs) face numerous challenges in delivering high-quality broadband services to their subscribers. This is primarily due to the explosion of an endless range of increasingly popular applications (mainly video and file-sharing) navigating their infrastructures at all times. In fact, according to the Yankee Group’s 2007 DPI report, global bandwidth usage is expected to exceed 5.0 million Mbps by 2010, growing from its current level of approximately 2.5 million Mbps. With so many applications flooding the ISP network at all times, pipes are quickly congested and application performance is impaired.

Although the immediate response has often been to simply increase the bandwidth, this solution only creates additional costs for infrastructure expansion (CapEx) and additional maintenance costs related to it (OpEx). In addition, applications such as P2P and streaming are extremely quick to consume any bandwidth that becomes available and network operators are once again faced with the same congestion problems.

Broadband networks today deliver a wide variety of services, including a growing volume of “over-the-top” (OTT) Internet content and applications that ride on existing network infrastructure. Delivering this traffic over a network may raise a number of performance issues such as packet loss, packet latency and jitter. The aggregation of these quality impairments can be significant enough to affect customer satisfaction. In order to ensure the high Quality of Experience (QoE) subscribers expect, ISP network operators must approach OTT applications individually. This is because each application has different Quality of Service (QoS) requirements to ensure its optimal performance.
What’s the Problem?

- **Growing bandwidth demands driven by Internet video and P2P**
  
  One of the ISPs biggest challenges is how to maintain subscribers QoE (especially for Internet video) without sending bandwidth requirements and network costs through the roof. Even after network expansion, non-optimized bandwidth-aggressive applications such as P2P will consume as much of the bandwidth resource as they can.

- **Declining Revenues**
  
  In many regions, broadband penetration is saturated, prices are starting to decline, and there is a constant threat from competition. ISPs are looking for new ways of generating revenue streams and increasing ARPU. Providers need to be able to differentiate their offerings and build a more informed engagement strategy on a customer-by-customer basis.

- **Subscriber Churn**
  
  Since ISP revenues are currently declining, subscriber retention is of critical importance. During 2007-2008, service providers reported increased churn rates. ISPs are often unable to retain existing subscribers, despite the fact that attracting new subscribers is more expensive. Subscriber loyalty is at an all-time low with ISPs constantly competing with each other to offer more attractive packages, and the majority of subscribers flocking to the best deal.

- **Guaranteeing Consistent Quality of Experience (QoE)**
  
  As “Over-the-Top” (OTT) applications are increasingly being offered as network independent services, network operators are challenged to guarantee providing sufficient QoS for these applications and thus guarantee consistent QoE for their subscribers. Existing network infrastructure does not provide an adequate solution to this problem.

- **Security Threats**
  
  Security concerns are at the forefront of the service providers mind. The two main problems they are dealing with are DoS/DDoS attacks and outgoing spam generated by subscribers who are unwittingly infected with worms, zombie, or spambots and are using the ISP network as an attack launch pad.
What’s the Solution?

Allot’s solutions for Internet service providers are geared towards delivering actionable network intelligence – knowing your network and optimizing its performance.

Visibility – the keystone of Network Intelligence

Network and service visibility is at the core of every Allot service optimization solution, providing a clear and detailed understanding of subscriber behavior, application usage, and network performance. DPI-based visibility enables ISPs to see and understand how their bandwidth resources are being consumed by subscribers, content providers and applications across the entire network.

Unlike the cursory visibility capabilities within routers or other network elements, the Allot solution inspects every IP flow and applies advanced methods to identify the application riding on top of this flow and the subscriber that generated it. This provides service providers with an invaluable complete and accurate picture of network utilization per application and per subscriber.

Providing both current (real time) and historical (long-term) network views, Allot’s solution features two separate monitoring mechanisms:

Real time monitoring tools

- Real time, multi-dimensional view of network traffic at a resolution as detailed as 30 second intervals. Real time monitoring is typically used to view and troubleshoot abnormal events on the network as they occur.
- Additional benefits: interactive tool, drill down capabilities, complete traffic statistics available for several days, application and subscriber awareness.

Long term monitoring tools

- Extended, multi-faceted display of the network over configurable periods of time: hours, days and even months.
- Efficient tools for planning, operations and marketing departments to determine application and subscriber usage trends, thereby facilitating more distinctive service offerings.
- Clear understanding of network utilization over time allowing intelligent network capacity planning.

Allot’s real time monitoring and advanced reporting capabilities provide valuable information such as:
- Top applications/subscribers
- Subscriber packages utilization
- Quota usage
- Individual reports per subscriber e.g. subscriber usage over time, most used applications etc.

**Examples of subscribers and applications usage reports**

**Solution Advantages:**

- **Network Intelligence:** NetXplorer allows ISPs to see and understand how their bandwidth is being consumed by applications and subscribers on the network, and to directly link service deployment and performance policies to their business goals.

For a detailed description of this solution, please read the *NetXplorer Report Binder*

**Solution Components:**

- **NetEnforcer or Service Gateway platforms:** in charge of enforcement of QoS policies and creation of application and subscriber based information.
• **NetXplorer**: centralized management system that provides control of Allot's NetEnforcer and Service Gateway devices, including in-depth network visibility, QoS policy definition and enforcement.

• **Subscriber Management Platform (SMP)**: in charge of managing subscribers in a dynamic environment - optional

**Optimizing traffic to deal with ever-growing bandwidth usage**

Once the solution is installed, the ISP can immediately start to reap the benefits of network intelligence and analyze the network traffic in terms of applications, subscribers, links and others. Based on these statistics, the service provider can define dynamic Quality of Service (QoS) policies to be applied to the IP traffic in order to manage the way in which available backhaul bandwidth is consumed by individual applications and subscribers, especially during high-congestion periods (peak hours). When crafting network congestion policies, the ISP may assign different priorities and conditions to different traffic categories, specifying the actions to be taken in each case. Allot solutions can accommodate different backhaul and peering-point configurations and arrangements, allowing the provider to distinguish between local traffic and peering traffic, and even to create different traffic policies for different peering links.

**Solution Advantages:**

• **Bandwidth Savings**: By managing bandwidth allocation according to traffic categories and priorities, ISPs can better utilize available capacity and thereby postpone the need for frequent bandwidth upgrades.

• **Ensure fair access and QoE**: By actively managing traffic flows, the ISP can avoid congestion and ensure that high-priority applications receive the necessary QoS and bandwidth allocation to perform well, while ensuring fair access and usage for all subscribers.

**Solution Components:**

• **NetEnforcer or Service Gateway platforms**: in charge of enforcement of QoS policies and creation of application and subscriber based information.

• **NetXplorer**: centralized management system that provides control of Allot's NetEnforcer and Service Gateway devices, including in-depth network visibility, QoS policy definition and enforcement.

• **Subscriber Management Platform (SMP)**: in charge of managing subscribers in the dynamic environment (optional).
Optimizing Video Traffic using Intelligent Media Acceleration

Internet video is today the fastest growing application in terms of bandwidth consumption and subscriber usage.

Allot’s network intelligence solution allows broadband providers to identify and distinguish the different types of video traffic on the network and to enforce Quality of Service (QoS) policies per individual application or across the board per traffic category. Allot’s full complement of bandwidth management and policy provisioning tools make it easy to build QoS policies especially for the needs of video traffic. Policy definitions may include any combination of priority, bandwidth allocation, access, traffic-shaping and quota actions to be applied per application or per subscriber to ensure QoE.

To further enhance and guarantee video viewing, Allot has incorporated media caching into its network intelligence solution.

In addition to dramatically cutting bandwidth costs on peering links and improving subscriber QoE, the caching solution gives ISPs an opportunity to increase ARPU by offering new value-added services, providing accelerated content delivery (particularly for HTTP video streaming). Such services can be targeted at heavy multimedia subscribers who are willing to pay more for faster downloads and better quality of experience.

Solution Advantages:

- **Reduce Backhaul/Peering Costs:** In most cases video requests will be served by the cache rather than being served from an external Internet source, greatly reducing the traffic on expensive backhaul and peering links.

- **Reduction in churn and support costs:** Even though bandwidth utilization on the peering links is essentially reduced, video delivery quality and content download time improve significantly.

- **Increase ARPU:** ISPs can offer premium video services to subscribers or alternatively offering premium, faster bandwidth packages to increase ARPU.

For a detailed description of this solution, please read the Allot Solution Brief, *Enhancing Internet Content Delivery*

Solution Components:

- **NetEnforcer or Service Gateway platforms:** in charge of enforcement of QoS policies and creation of application and subscriber based information.
- **NetXplorer**: centralized management system that provides control of Allot's NetEnforcer and Service Gateway devices, including in-depth network visibility, QoS policy definition and enforcement.

- **Subscriber Management Platform (SMP)**: in charge of managing subscribers in the dynamic environment - optional

- **Caching device**: provides caching, acceleration and control of multimedia over HTTP and P2P traffic.

### Filtering illegal content

The open nature of the Internet and specifically user-generated content websites enable content to be created and accessed by anyone, anywhere and at anytime, thus facilitating illegal content faster and wider distribution.

While the definition of illegal content varies from country to country, it always includes child pornography. Many governments have mandated filtering of illegal content by the ISP. Allot URL Filtering solutions enable internet providers to comply with these regulations.

Allot's solution for Network-level Filtering of Illegal Content is a value-added DPI service of the Allot Service Gateway. The solution is based on a URL Filtering blade that plugs into the Service Gateway chassis. Allot URL Filtering utilizes encrypted URL blacklists, which are provided by a licensed third party who is responsible for maintaining and regularly updating the list.

A single URL filtering blade supports 50,000 URL entries with automatic update via the web or via local file upload. Enforcement actions include redirect, block, or continue to monitor the illegal traffic. In case of blocking, subscriber access to the offending website is dropped and a warning page is displayed. Allot provides full monitoring reports for blacklisted traffic and detailed log files.

**Solution Advantages:**

- Carrier-class, high-availability solution for regulatory compliance
- Protects brand image
- Negligible impact on mobile Internet service or subscriber QoE
- Highly accurate filtering; no erroneous filtering

**Solution Components:**

- **Service Gateway platforms**: including URL filtering blade - the network element in charge of enforcement of QoS policies and creation of application and subscriber based information.
• **NetXplorer**: centralized management system that provides control of Allot's NetEnforcer devices, including in-depth network visibility, QoS policy definition and enforcement.

• **Subscriber Management Platform (SMP)**: in charge of managing subscribers in the dynamic environment - **optional**

**Increasing ARPU**

The per-subscriber visibility, QoS policy control and quota management provided by Allot solutions facilitate the rapid deployment of service tiers that give subscribers the choice Internet experience they want at a variety of price points. These capabilities also allow operators to manage network congestion in a fair and efficient manner and to control excessive use that could negatively impact online service for the majority of subscribers. As a result of tiered subscription and quota models, ISPs are able to enlarge their revenues from broadband access services by moving away from the flat rate charging system. This increased flexibility in service packaging means that packages may be built on a tier-by-tier basis or even for an individual customer.

• The subscriber awareness provided by SMP (Subscriber Management Platform) allows ISPs to create **tiered service plans** and to provision individual QoS policies that enforce how each subscriber’s traffic is treated, ensuring a high-quality online experience for everyone on the network.

• **Quota management capabilities** provided by SMP allow operators to monitor real time subscriber usage and to implement consumption-based billing models or quota thresholds. Quota limits may be set independently for every subscriber and for each application in a service plan. Allot’s NetEnforcer dynamically enforces the usage quota, automatically notifying operator OSS when the quota limit is reached, and supports redirection to an operator portal where subscribers can be given options to view their usage history, pay to extend their quota, or switch to another service plan.

• **Accounting capabilities** provided by the SMP solution utilize a standard interface for exporting subscriber based accounting usage records for billing purposes.

Allot solutions for tiered service control and quota management create an unlimited opportunity for innovative service packaging and pricing. Even non-provisioned services such as gaming and competing VoIP applications can also become a source of revenue as Allot SMP meters their usage, enforces QoS and generates usage statistics and accounting CDRs.
**Solution Components:**

- **NetEnforcer or Service Gateway platforms:** in charge of enforcement of QoS policies and creation of application and subscriber based information. Additional services can be easily integrated into the Service Gateway using additional blades.

- **NetXplorer:** centralized management system that provides control of the NetEnforcer and Service Gateway devices, including in-depth network visibility, QoS policy definition and enforcement.

- **Subscriber Management Platform (SMP):** in charge of managing subscribers in the dynamic environment

**Network security**

Allot ServiceProtector is an anomaly detection system (ADS) which employs advanced detection and analysis technologies to provide real time elimination of network attacks and subscriber originated attacks that disrupt performance and integrity of network services. ServiceProtector coupled with in-line enforcement elements such as the Service Gateway platform and NetEnforcer devices, provide vital intelligence to anomaly prevention systems (APS), which block, limit or isolate malicious and unwanted traffic. ServiceProtector also works with other in-line network elements such as routers, firewalls, IPS, traffic shapers and traffic scrubbers for mitigating attacks.

Within seconds, Allot’s security solutions identify DoS/DDoS, Zero Day attacks and other traffic anomalies impacting network performance. ServiceProtector also detects subscriber zombies or bots that may be generating outgoing spam, DoS, worm propagation, and port scanning activities which cause latency and congestion on the network and can result in operator blacklisting as a spamming network.

**Solution Advantages:**

- Genuine Zero Day attack protection
- Protect network performance and integrity of infrastructure on which revenue generating network services and applications are based
- Protect brand image and avoid blacklisting from outgoing spam.
- Facilitate clean-up of infected subscribers and ultimately enhancing their Internet experience
- Avoid escalation in call center complaints during outages
- Manage international bandwidth costs
Optimize BB Networks for Performance and Profit

- Profit from DoS/DDoS protection services for protecting on-line presence of enterprises and businesses

**Solution Components:**

- **NetEnforcer or Service Gateway platforms:** in charge of enforcement of QoS policies and creation of application and subscriber based information.
- **NetXplorer:** centralized management system that provides control of Allot's NetEnforcer and Service Gateway devices, including in-depth network visibility, QoS policy definition and enforcement.
- **Subscriber Management Platform (SMP):** in charge of managing subscribers in the dynamic environment
- **ServiceProtector:** detects and mitigates the attacks.

**Typical deployments**

Depending on the Allot solution(s) desired, the Internet service provider will usually deploy Allot DPI platforms and management elements as shown below.

**Conclusion**

Allot provides ISPs with tools which make cost-effective traffic management easy and allow enhanced service offerings to their subscribers. Allot solutions provide ISPs with unsurpassed network-wide visibility allowing service providers to incorporate advanced traffic management policies which assure quality of service and efficient utilization of network resources. Therefore ISPs can significantly save on CapEx & OpEx and offer superior value to their business and residential subscribers which translate instantly into higher ARPU.

Allot Communications