Solution Brief

CMTS Channel Awareness and Congestion Mitigation

Sept. 2014

Allot communications

Contents

Executive Summary **4**
Congestion – The #1 MSO Challenge 4
Visibility – The Danger-free Delaying Tactic 4
The Solution – Allot Service Gateway 4
Solution Highlights **5**
Cable Network Challenges 5
Monitoring 5
Enforcement 6
Solution Architecture **7**
DART Technology 7
CMTS 7
Cable Modems 8
SMP Server 8
Data Mediator 8
Allot Service Gateway 8
DPI and QoS Clustering 9
CMTS Visibility **9**
Allot ClearSee Analytics 9
Rich Set of Out-of-the-Box CMTS Reports 10
Self Service Reports 11
OSS Integration 11
CMTS Congestion Management **11**
Allot NetXplorer Central Management System 11
Congestion Policy Management 13
VAS-enabling Platform **13**
VoIP Quality Monitoring 13
Media Caching 14
URL Filtering 15
ServiceProtector—Network Threats Protection 17
Typical Deployment Scenario 18
About Allot Communications **18**
Playing a Profitable Role in the OTT Value Chain 18
Appendix A: Typical Reports **20**
Main Dashboard 20
Service Plan Usage 21
Heavy Users 22
AS Next Hop 23
AS Destinations 24
Application Trends 25

User Top Sites Report 26
User Device Usage Report 28
CMTS Usage 30
CMTS Channel Usage Trends 31
Self Service Report 32
Appendix B: Policy Examples 33
Monitoring 33
Alarms 34

Executive Summary

Congestion – The #1 MSO Challenge

Your subscribers' skyrocketing bandwidth consumption means that you must constantly deploy expensive new network infrastructure (new cabling projects, DOCSIS 3.0/3.1 CPE replacement, additional CMTSs, and complex re-engineering of the CMTS channel allocation) to keep them satisfied.

The ever increasing competitive pressures on cable operators (MSOs) drives revenues down, making capital expenditure on infrastructure something you want to avoid, or at least postpone for as long as possible. However…

Frustrated, bandwidth-choked subscribers first contact your help desk (if you're lucky), overloading this expensive resource and requiring added investment to keep response times reasonable.

If you're not lucky, or you cannot satisfy these subscribers, the resulting churn endangers your profitability, if not your very existence.

The most cost-effective way of increasing your subscriber base is to keep existing subscribers. Recruiting new ones requires an order of magnitude greater effort and expenditure.

Visibility – The Danger-free Delaying Tactic

Are you fully utilizing your existing network capacity? Perhaps a few peer-to-peer heavy users and abusers are choking more time-critical network traffic? Can you guarantee reasonable quality of experience (QoE) to VoIP and video streaming, and be service level agreement (SLA) compliant?

If you could accurately answer these questions, you would be able to mitigate many negative effects, and redistribute resources so that all your subscribers are satisfied, without deploying additional infrastructure. At the very least, you could delay implementing infrastructure expansion by several months, with direct, beneficial effects on your bottom-line profitability.

The Solution – Allot Service Gateway

With an Allot Service Gateway in your network you gain the granular visibility you require (of CMTS elements, traffic, applications, and subscribers), together with real-time, congestion avoidance capabilities thanks to the gateway's CMTS-aware, application-aware, and subscriber-aware bandwidth controls. Leveraging this powerful combination lets you delay capex outlays for many months.

Allot Service Gateway is also the platform from which you can quickly roll out value-added services (VAS) that enhance differentiation and stickiness, boost customer loyalty, while increasing revenue streams, ARPU, and profitability.

Additionally, the Allot Service Protector module, offers wide-ranging protection, against: zero-day attacks, network performance degradation, dangers to infrastructure integrity, brand image damage, and avoidance of blacklisting from outgoing spam.

Solution Highlights

Cable Network Challenges

Most cable network providers suffer from the following problems:

- Limited visibility into the network
    - Who consumes more? DOC 2.0 or DOC 3.0?
    - What causes the bottlenecks? YouTube? BitTorrent?
    - Who are the heavy users?
    - What is the level of QoE in your network?
- Upstream (US) channel congestion
    - US is more critical than downstream (DS), since you have less channels with less bandwidth—for every four DS channels, there will be a single DOCSIS 2.0 US channel. Because of this limited bandwidth, US channels are commonly the bottleneck. US congestion exists in all DOCSIS versions.
    - Most cable networks have DOCSIS 1.1, 2.0, and 3.0 modems sharing the same physical RF channels. DOCSIS 1.1 and 2.0 do not perform any load balancing, and use single downstream and upstream channels. Thus, even with the built-in DOCSIS 3.0 load balancing, it could well be that US will still be saturated at the bonding group level. Allot also has solutions for DOCSIS 3.0.
    - Small numbers of DOCSIS 1.1/ DOCSIS 2.0 users with high bandwidth service plans can cause channel congestion

To address these issues, the Allot Service Gateway boasts the following main capabilities:

Monitoring

- Upstream/downstream channel and bonding group level
    - accurate and reliable, even with bonding group overlap
    - differentiation between DOCSIS 2.0 and DOCSIS 3.0 traffic
- Auto-learning mode—the system:
    - auto learns the CMTS network topology
    - assigns channel/bonding group capacities and thresholds automatically
    - auto-calculates new capacities and thresholds, based on past usage patterns
    - automatically updates the system with channel capacity values at predefined intervals

- Close feedback loop
    - auto-calculates new capacities and thresholds, based on past usage patterns
    - automatically updates the system with channel capacity values at predefined intervals
- Static mode
    - administrator sets up static capacity and threshold per each interface/channel or bonding group

Enforcement

Highlights

- Real time channel congestion sensing and management
    - Real-time, dynamic "volume based" subscriber management solution
    - No time limitation. Enforcement is released when congestion is ended (not when time period ends)
- Multi hierarchy—real-time CMTS congestion management in addition to channel congestion management
- Flexible and friendly configuration—whereas other vendors trigger congestion states on every spike, Allot's friendly GUI lets you decide when there is a congestion state (after how many minutes, and for which bandwidth average the channel/bonding group is considered congested).

Enforcement Models

Allot CMTS Awareness solution uses two main enforcement models:

- Subscriber—change the service plan for all congested subscribers, where congestion is measured on network elements: interface/bonding group
- Application— apply QoS policy per application when traffic hits a pre-defined network element capacity threshold

Example

Heavy P2P traffic can be managed automatically, and in real time.

The system senses that a channel/bonding group is congested as traffic crosses your preset high threshold (say 80% of capacity). The default server policy is then temporarily replaced by a congestion policy, in which P2P traffic is throttled. As traffic is cleared and drops below your preset low threshold (say 60%), the default policy is reinstated.

Solution Architecture

DART Technology

Dynamic Actionable Recognition Technology (DART) is Allot's superior brand of DPI technology and foundation of Allot solutions. DART provides comprehensive network visibility, application control and subscriber management, and it serves as an enabler of application-based value added service deployment and profitability. The IP application awareness provided by DART at a per-subscriber granularity opens up new opportunities for cable providers to control network costs and to monetize the bandwidth explosion of Internet content and applications traversing their networks.

Hitless Signature Library Updates

DART employs hitless signature updates, enabling flows to be continuously and accurately detected and classified while the signature library is being updated, leaving surrounding systems completely unaffected.

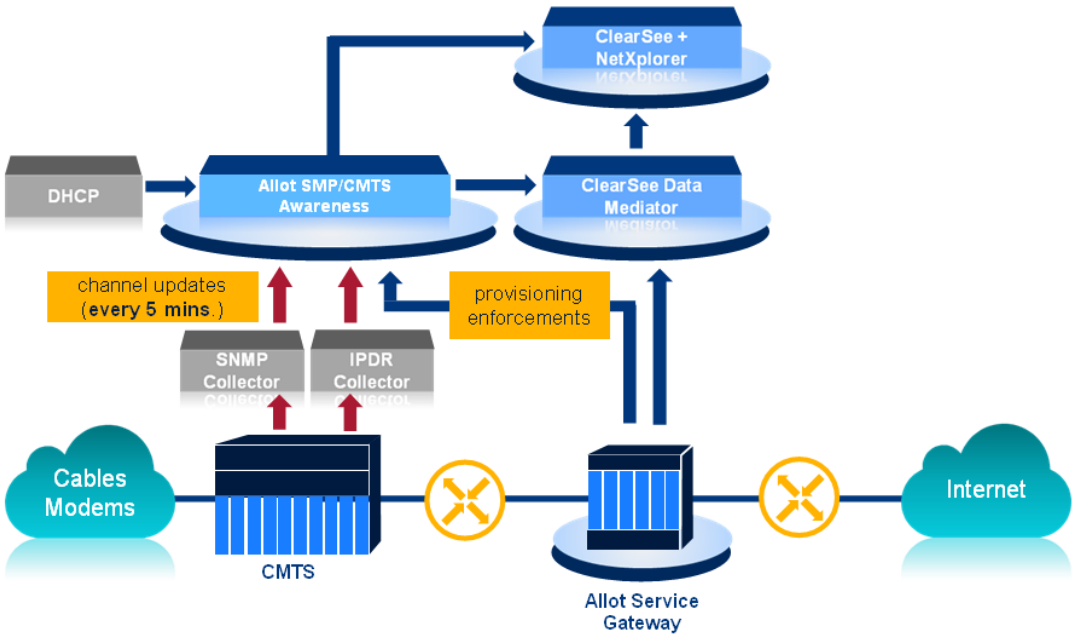


Figure 1: Allot Service Gateway in the Cable Network

CMTS

The Cable Modem Termination System provides broadband Internet service over CATV infrastructure. Each CMTS has multiple upstream and downstream interfaces, which are divided into multiple RF channels supporting multiple generations of cable modems (DOCSIS 1.1, 2.0, and 3.0). Each cable modem is allocated with upstream (US) and downstream (DS) RF channels.

The CMTS generates IPDR records (which approximate to CDRs) for billing, monitoring, and OSS/BSS integration.

Cable Modems

Tens/hundreds of thousands of these customer premises equipment (CPE) devices are currently deployed. They comprise legacy DOCSIS `1.1 and 2.0 and the modern DOCSIS 3.0 devices with enriched functionality, that coexist in the same network.

DOCSIS 3.0 cable modems (CMs) are currently replacing the legacy CMs. They have the advantage or using multiple US/DS channels (bonding groups), have higher bandwidth with wider coverage, and utilize US bandwidth more efficiently.

SMP Server

Allot Subscriber Management Platform gathers data from the multiple sources listed below. It outputs the resulting, formatted intelligence to the Data Mediator. Both Allot SMP Server and Data Mediator can be virtualized.

- DHCP—the DHCP/Radius supplies subscriber identification (mapping between the CM's MAC address to IP) in cases where the Allot Service Gateway is unable to obtain it from monitoring the traffic flow
- SNMP collector—updates the SMP server every 15 minutes with CMTS channel capacity and bonding group (BG) configuration, just like competitive vendors. However, it updates channel utilization every 5 minutes. This 5 minute cycle gives Allot devices its real-time capabilities, and represents a major competitive advantage
- IPDR Collector—maps subscribers to channel/BG, and channel utilization. The cycle for these updates is 15 minutes or longer
- Allot Service Gateway—supplies the SMP server with policy/provisioning enforcement data

Data Mediator

The Allot Data Mediator is a server that mediates between Allot in-line platforms and an external application such as Analytics systems, BI systems, or data warehouse systems. It integrates these disparate sources into output readable by the Allot ClearSee Analytics.

Allot Service Gateway

Allot Service Gateway is tightly integrated with other Allot components to provide comprehensive, detailed, and actionable insights into network traffic.

Highlights

- CMTS channel speed and channel utilization is read once every 5 minutes
- Bonding group configuration (channel list) is read every 15 minutes
- The cable modem (subscriber) is mapped to its channel or bonding group (per direction) according to the channel set indicated in the IPDR SAMIS records
- IPDR records can be collected via two interfaces:
    - Native CTMS IPDR streaming protocol

    - Export/FTP of IPDR/XDR files
- Monitoring and Reporting
    - Based on Cable Modem Detailed Records (CMDRs—similar to SDRs), which contain the DS and US channel ID/bonding group ID of the cable modem, and channel utilization data records. For every DS/US channel change, a new CMDR is created.
    - For deeper insight, you can drill down on DOCSIS 2.0 or 3.0 traffic.

DPI and QoS Clustering

In asymmetric environments, traffic management is more challenging due to the lack of visibility caused when different flows of a single connection are handled by different devices (possibly located at different sites).

To ensure accurate classification of asymmetric traffic in carrier networks, Allot supports clustering (DPI clustering and QoS clustering), both of which share a common synchronization channel that shares metadata among all installed platforms. Since there is no need to copy or send the total traffic through the synchronization links, the solution is extremely efficient with minimum impact on the network, (connectivity requirements and complexity), while maintaining scalability on very high levels of throughput and link density.

This common channel allows the cluster to operate as a single detection/enforcement platform and thus eliminates networking issues related to asymmetric traffic flows.

For more information, see the solution brief: Allot Asymmetric Traffic Solution

CMTS Visibility

Allot ClearSee Analytics

Allot ClearSee Analytics allows cable providers to extract valuable information and insights from the data traffic monitored by Allot Service Gateway and Allot NetEnforcer platforms. It is highly scalable and utilizes best-of-breed technologies, scalable database and business intelligence methodologies. The easy-to-use interface simplifies reporting and data mining for many different groups in an organization including: engineering, management, marketing, and operations.

Highlights

- **Software defined**: The solution is software-based, can potentially run on commodity hardware or deployable on cloud with support for virtualized platforms. It provides cross-platform support with accessibility via web or mobile devices
- **Cross-organizational**: Out-of-the-box report dashboards addressing various areas of interest. Reports can be subscribed for distribution to different users. Some of the reports if desired can be shared

- **Multi-tenancy**: Multiple role access control applicable at report level as well as data level. Advanced report subscription allows distribution of different reports data sets to different destinations.
- **Self Service Insights**: User-friendly interface for accessing reports and dashboards. Ad hoc self-service reports based on any attribute or measure in the data source. Custom homepage can be created by drag and drop of reports.

Rich Set of Out-of-the-Box CMTS Reports

- CMTS dashboard with drill down to channel/application utilization
- DOCSIS 2.0 vs. DOCSIS 3.0 bit rate report
- Top subscribers report (drill down to channel/interface)
- Top abusers by CMTS service plan
- Subscribers (Cable Modems) by devices and applications
- Service plan report by CMTS, Interface, DOCSIS version, etc
- QoE of applications by CMTS interface and channels

Sample Report

Figure 2: Report showing one subscriber's exaggerated BitTorrent usage

The lower graph shows traffic utilization per channel (single numbers) or per bonding group (multiple channels).

For more report examples, see: Appendix A: Typical Reports.

Self Service Reports

Allot ClearSee has a user-friendly interface for accessing reports and dashboards. You can generate ad hoc self-service reports based on any attribute or metric in the data source. A custom homepage can be created by drag and drop of reports.

Highlights

- Customize report/dashboard views to generate management-friendly reports
- Specific reports created by the user on the fly
- Aggregate reports to a single view based on user interests
- Export any report to PDF, XLS, CSV
- Schedule exports
- Create your own views for report export

OSS Integration

The monitoring and usage statistics provided by Allot solutions can be integrated and cross-referenced with data from existing OSS and cable systems (PCMM, IPDR) to provide a deeper level of visibility.

CMTS Congestion Management

Granular visibility and policy enforcement are at the heart of Allot CMTS congestion management solutions. Allot NetXplorer together with Allot SMP allow cable operators to define dynamic enforcement policy to control congestion on CMTS elements.

Allot NetXplorer Central Management System

Allot NetXplorer is the scalable management system for Allot platforms, and value added services. It supplies vital network intelligence that enables cable operators to understand how their CMTS channel resources are being consumed by applications and users on the network, and to define traffic management policies to alleviate congestion automatically and to ensure quality of experience. The system provides centralized visibility that is accessible to multiple clients and is designed to manage widely dispersed CMTS and other network infrastructure.

Enhanced Network Visibility and Powerful Policy Control

Allot NetXplorer provides unsurpassed visibility for proactive troubleshooting and traffic trend analysis to assist with capacity and service planning. Real-time and long-term reporting tools provide multi-dimensional views of application traffic, subscriber traffic, value-added service traffic, and HTTP traffic.

Allot NetXplorer also provides a powerful and granular Policy Enforcement Editor for configuring enforcement actions per subscriber, application, and CMTS element. The figure below shows a scenario in which a congestion service plan replaces the subscriber's regular (or default) service plan when congestion thresholds are reached. Once congestion has subsided, the regular service plan is automatically reinstated.

Figure 3: Default versus Congestion Policy in Allot Netxplorer

Figure 4 shows the before and after results of applying the congestion service plan. P2P traffic is temporarily rate-limited, enabling delay-sensitive applications such as VoIP to utilize the freed bandwidth.

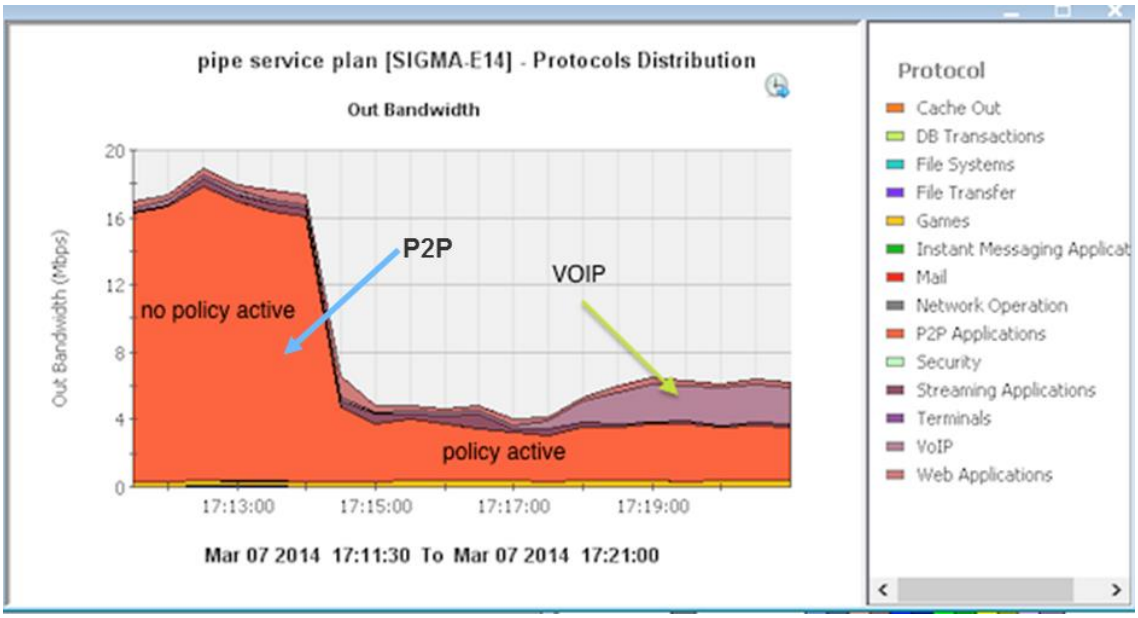
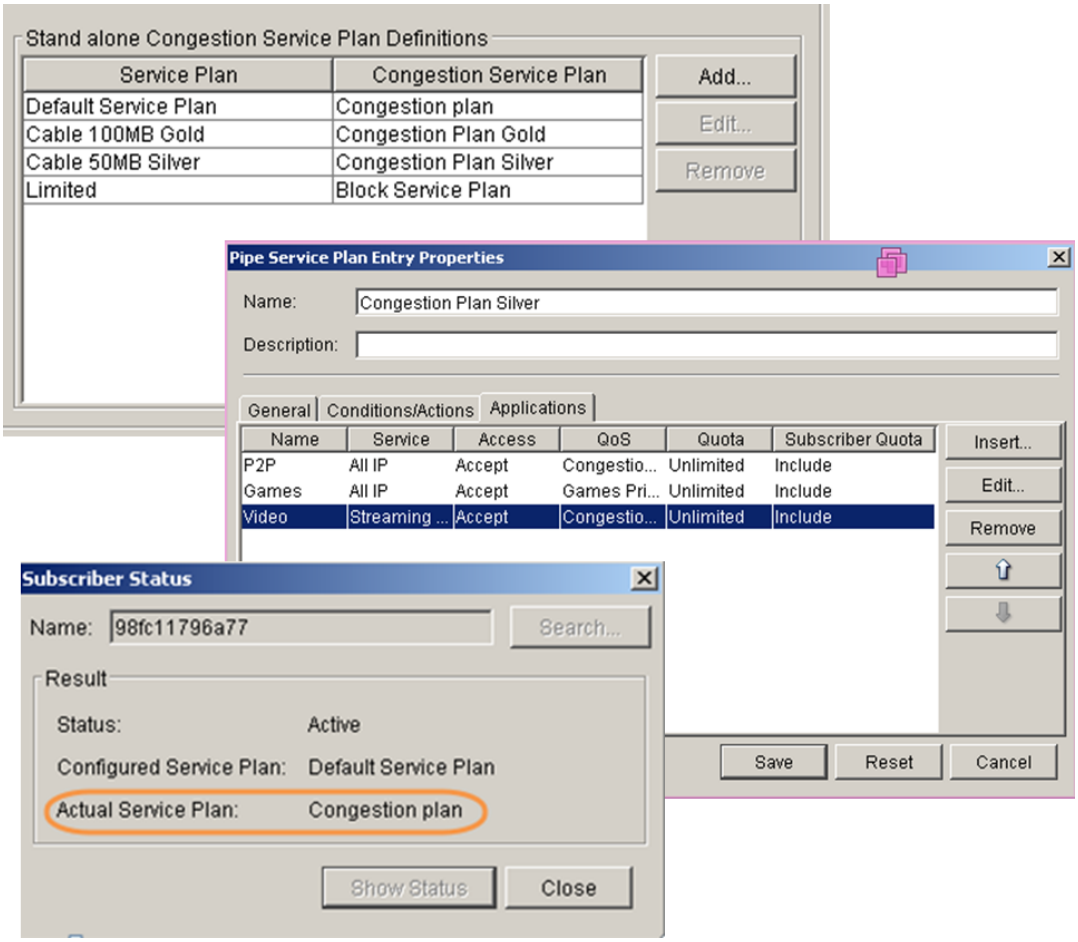


Figure 4: Congestion control frees up bandwidth for delay-sensitive applications

Congestion Policy Management

The screen captures below give an overview of the process of defining the policy for various congestion service plans. For more on setting up and viewing policies, see: Appendix B: Policy Examples.



VAS-enabling Platform

Allot solutions leverage its DART capabilities to provide value-added services like URL Filtering, Video Caching, and VoIP Quality Monitoring on a per-subscriber basis, helping cable operators deploy content delivery structures that enhance QoE.

These value-added services are highly cost-effective, as they leverage Allot Service Gateway's powerful subscriber management capabilities and its single point of integration with operator OSS and provisioning environments.

VoIP Quality Monitoring[1]

- Guarantee VoIP service quality and availability
- Track VoIP usage patterns for market analysis and network planning
- Troubleshoot the root causes for VoIP quality degradation

[1] For a detailed description of this solution, please read the Allot Solution Brief, *Enhanced VoIP Charging and Quality Monitoring – An Integrated Allot-Qosmos Solution*

In addition to creating and enforcing dynamic QoS policies especially for the needs of VoIP traffic, cable networks can further enhance their VoIP service by constantly monitoring the quality of VoIP sessions. Allot has integrated its extensive DART bandwidth management capabilities with advanced tools for monitoring VoIP session quality, collecting usage information and ensuring VoIP service quality. This integration enables service providers to monitor critical performance parameters for all types of VoIP applications through the generation of detailed call statistics, which support accurate, real-time troubleshooting, and can be used to trigger conditional QoS policies.

Media Caching

Allot MediaSwift E (MSWE) is a transparent media (P2P/video) caching service that provides the following benefits:

- **Reduce backhaul/peering costs**: In most cases Internet 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.
- **Add value to the supply chain**: Operators who implement delivery capabilities early in the game position themselves to become a necessary component of a viable and successful Internet video business, with revenue potential that can offset ongoing infrastructure investments.
- **Increase ARPU**: By providing accelerated delivery (particularly for HTTP video streaming) value-added services can be targeted to customers who are willing to pay a premium for faster downloads and a guaranteed viewing experience.

Cable networks are delivering a growing volume of "over-the-top" (OTT) Internet content and services that travel over the cable infrastructure but are not part of the operator's walled-garden of services. While cable operators are not the creators or providers of these OTT services, subscribers hold them responsible for service delivery and quality. With Allot subscriber management solutions, cable operators can create and enforce dynamic QoS policies that prioritize and ensure a quality online experience for users of rich-media delay-sensitive services such as video and interactive gaming.

In addition, Allot has integrated media caching with its extensive bandwidth and subscriber management capabilities, to provide a solution that allows operators to greatly enhance the Internet video viewer's quality of experience (QoE) while continuing to regulate opex and optimize network resources. This Allot solution simultaneously improves service quality and optimizes off-net traffic by providing content locally from the cache inside the service provider network. To achieve this optimization, a DART platform is deployed at the peering links to ensure that the video content is delivered mainly from the cache rather than from off-net Internet resources.

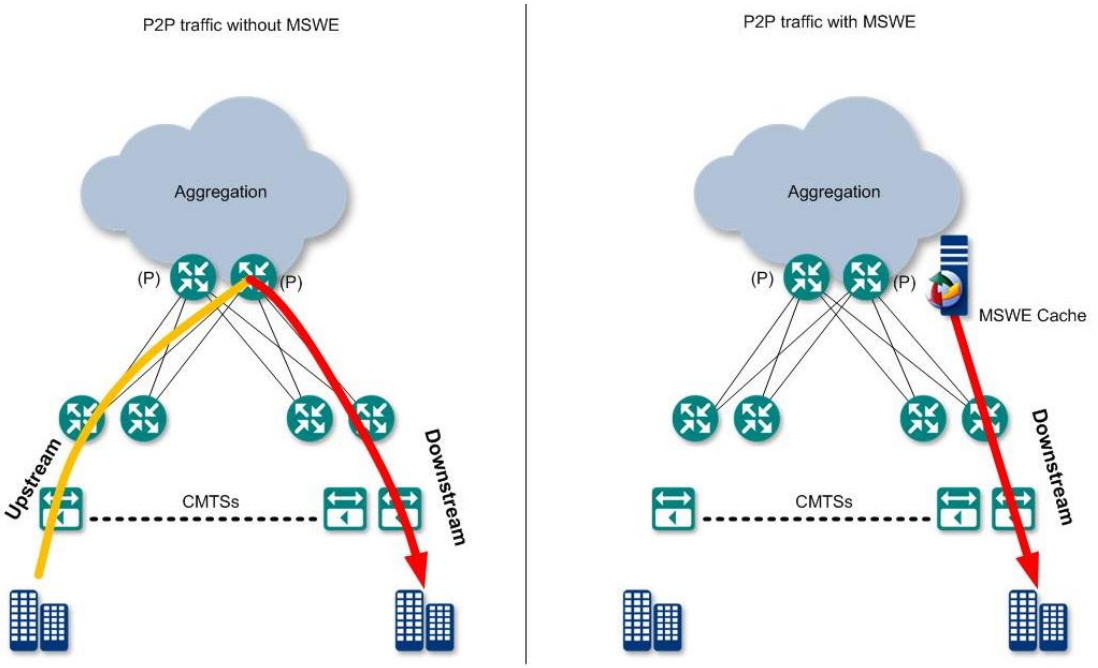


Figure 5: P2P traffic without Cache (left) and with Allot Cache (right)

URL Filtering

Allot WebSafe provides carrier-class URL filtering service designed to block access to blacklisted content at the network level, enabling fixed and mobile service providers to fulfill consumer demands for a safer and more protected Internet environment. The highlights of this VAS are:

- Carrier-class, high-availability solution for regulatory compliance
- Protects brand image
- Negligible impact on network performance or subscriber QoE
- Highly accurate filtering; no erroneous blocking
- Central management and control

Many countries have declared it illegal to distribute certain types of content over the Internet. The open nature of the Internet enables content to be created, hosted and accessed by anyone, anywhere and at anytime, while new Internet technologies and applications facilitate faster and wider distribution. This makes it harder to comply with legislation and regulations to combat illegal content. Many governments have mandated filtering of illegal content by the Internet Service Provider. Allot URL filtering solutions enable network providers to comply with these regulations.

Allot WebSafe is a licensed software option in Allot Service Gateway. This URL Filtering service utilizes encrypted URL blacklists, which are provided by a licensed third party who is responsible for maintaining and regularly updating the list.

Allot WebSafe is fully integrated with Internet Watch Foundation (IWF) allowing online updates from the IWF child abuse content-blocking list. WebSafe's open infrastructure allows easy integration with any local regulatory or watchdog body.

A single URL filtering blade supports 100,000 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.

ServiceProtector—Network Threats Protection

Allot ServiceProtector is a network protection service that runs on Allot platforms. It can be sold as a managed security service to the enterprise, and offers wide-ranging protection, including:

- 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 enhance their Internet experience
- Avoid escalation in call center complaints during outages
- Manage international bandwidth costs
- Profit from DoS/DDoS protection services for protecting online presence of enterprises and businesses

Service outages or sluggish response time caused by denial of service (DoS) or distributed DoS (DDoS) attacks on the network lead to customer dissatisfaction, lost productivity and brand damage for the operator who is failing to deliver on performance SLAs. The same is true for internal threats posed by subscribers who are unwittingly infected with worms, zombie, or spambots that use the cable network as an attack launch pad. Cable networks must protect themselves from external attack as well as potential blacklisting due to outgoing spam.

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

Allot ServiceProtector system provides scalable, carrier-grade performance compatible with 1GE and 10GE networks. Within seconds, Allot ServiceProtector sensors identify DoS/DDoS, Zero Day attacks and other traffic anomalies impacting network performance, enabling fast, surgical mitigation of offending traffic while allowing legitimate traffic to flow. ServiceProtector also detects subscriber zombies or bots who may be generating outgoing SPAM, DoS, worm propagation, and port scanning activities which cause latency and congestion on the network and can result in the cable operator being blacklisted as a spamming network.

Typical Deployment Scenario

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

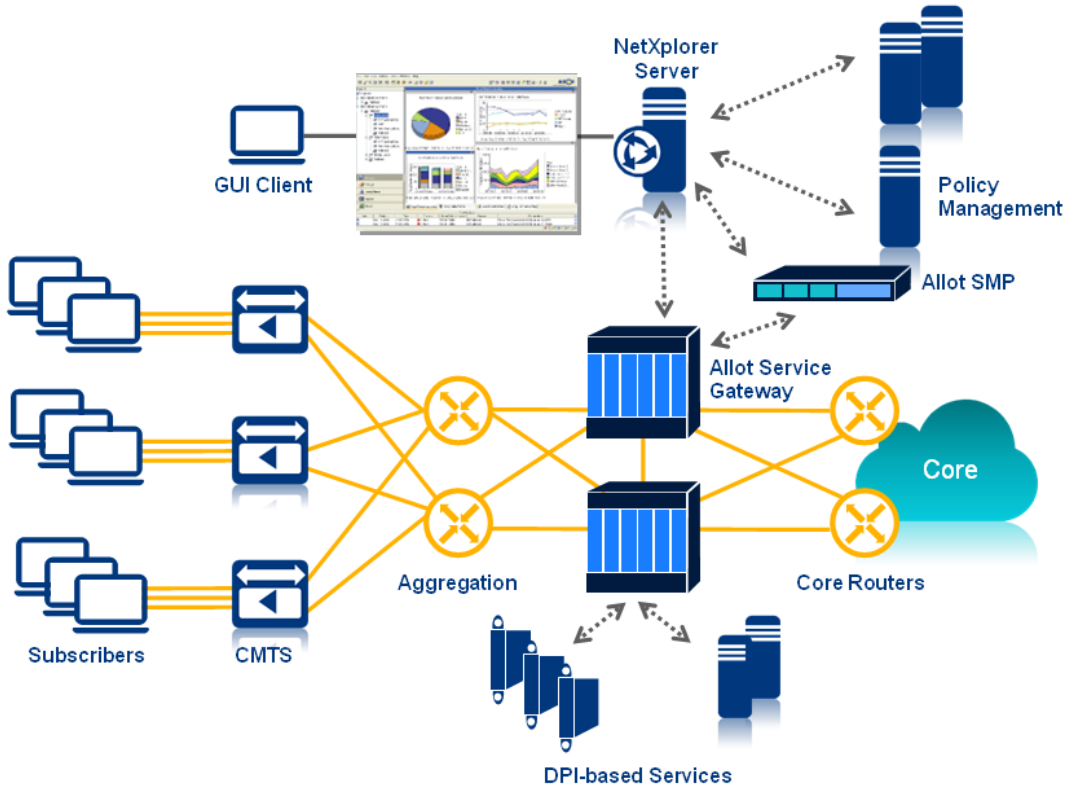


Figure 6: Allot solutions can be deployed at the core, aggregation or access network, per cable operator requirements

About Allot Communications

Allot Communications is a leading global provider of intelligent broadband solutions that put mobile, fixed and enterprise networks at the center of the digital lifestyle. Allot's DART-based solutions identify and leverage the business intelligence in data networks, empowering operators to shape digital lifestyle experiences and to capitalize on the network traffic they generate.

Allot's unique blend of innovative technology, proven know-how and collaborative approach to industry standards and partnerships enables network operators worldwide to elevate their role in the digital lifestyle ecosystem and to open the door to a wealth of new business opportunities.

Playing a Profitable Role in the OTT Value Chain

Fixed broadband networks face an ongoing demand for more bandwidth from both home and business customers. This has been complicated by the rise of multiple, powerful computing devices per household as well as increasing use of data-intensive services such as over-the-top video, online gaming, and IPTV. Not only are operators carrying ever-growing volumes of OTT Internet services, they are held accountable by consumers for the quality of experience. The sheer volume of this traffic is motivating

fixed carriers to expand traffic management measures, and to explore revenue-sharing models with OTT content providers as well as agreements with specialized content delivery networks (CDN).

As worldwide prices for DSL and cable services stagnate and competition from mobile broadband services increases, the shift to fixed-mobile convergence and everywhere-access is inevitable. Operators must be able to differentiate their offering to attract subscribers, as well as manage service policy, QoS, and charging across the converged infrastructure.

Appendix A: Typical Reports

This chapter presents a few examples of the most popular Allot ClearSee reports.

Main Dashboard

The Main Dashboard comprises four inter-related reports, the first, Subscriber Usage Percentile Distribution, groups the subscribers into percentile categories, and displays the volume (in GB) used by each group. Clicking any percentile bar displays information for just that group in the remaining reports—Device Usage by Volume, Subscriber Usage Classified by Volume, and Most Active Domains.

This dashboard provides in-depth understanding of network usage broken down into groupings, and permits rapid analysis of devices and domains used by each grouping, and data consumption for all categories of subscribers. You can use it to identify which segments of subscribers use which devices, access which domains and consume the most bandwidth.

Information drill-down:
Select any bar in the first graph to filter the remaining graphs to just that percentile group.

Data display options:
Bar Graphs and Data Grid.

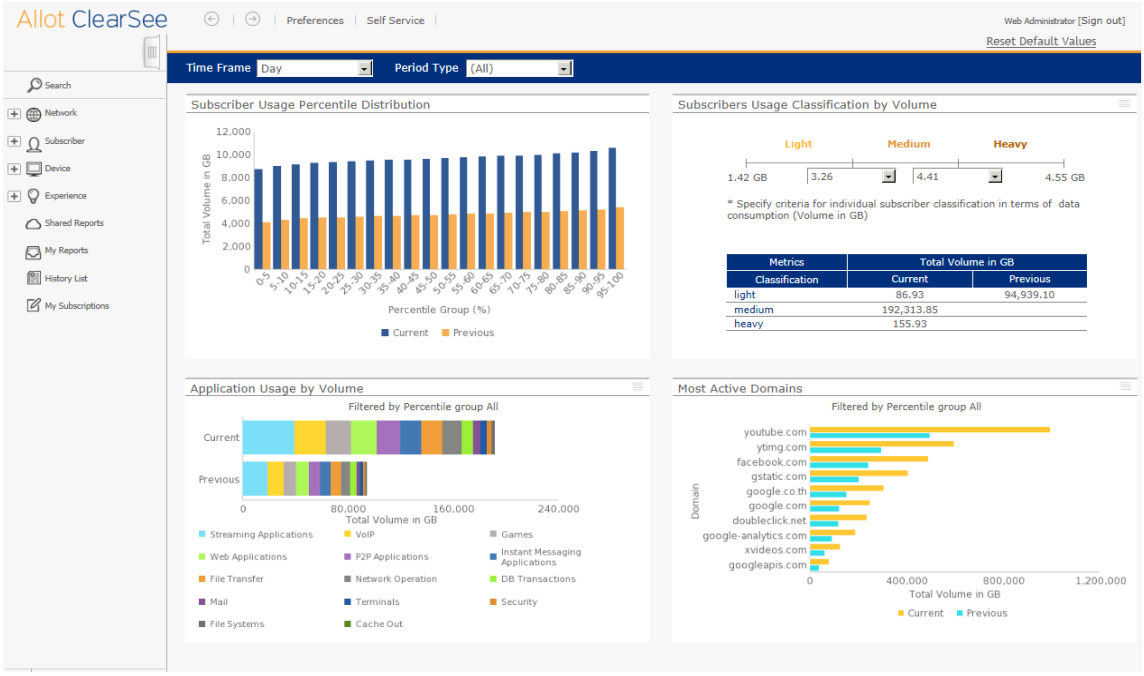


Figure 7: Main Dashboard

Service Plan Usage

This report identifies the top 50 service plans or any specific service plan as determined by their bandwidth or unique visitors. It is useful to identify volume metrics for top service plans—which service plans are associated with traffic at which hours of the day. You can drill into the data to determine which devices and applications are associated with that traffic.

Default presentation style: Line chart and Grid.

Information drill-down:
Application, Device OS, Device OS Version, Device Vendor

Display options:

Time Frame: Monthly, Daily, Hourly. Bandwidth or Unique Visitors. Service Plan. Total Volume in Mbps, Total Bandwidth in GB, Average Volume per Subscriber in GB. Unique Subscribers, Number of New Connections, Total Volume in GB, Average Session Duration in seconds, or Unique Subscribers.

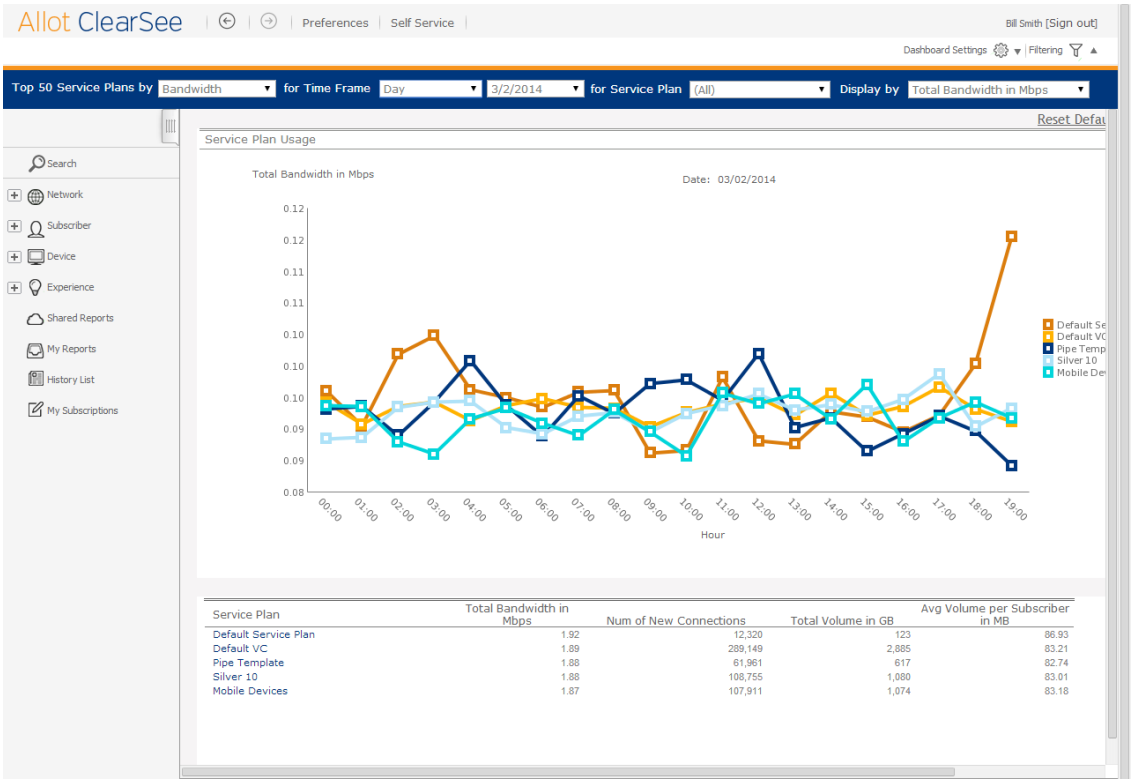


Figure 8: Service Plan Usage Report

Heavy Users

This report identifies the top twelve subscribers by volume or sessions (Graph) and the top one-thousand subscribers (grid). It is used to typify traffic patterns, destinations and protocols.

Information drill-down:
Application, Policy VC, Service Plan.

Filtering options:
Date.

Display Options:
Connections, Total Volume

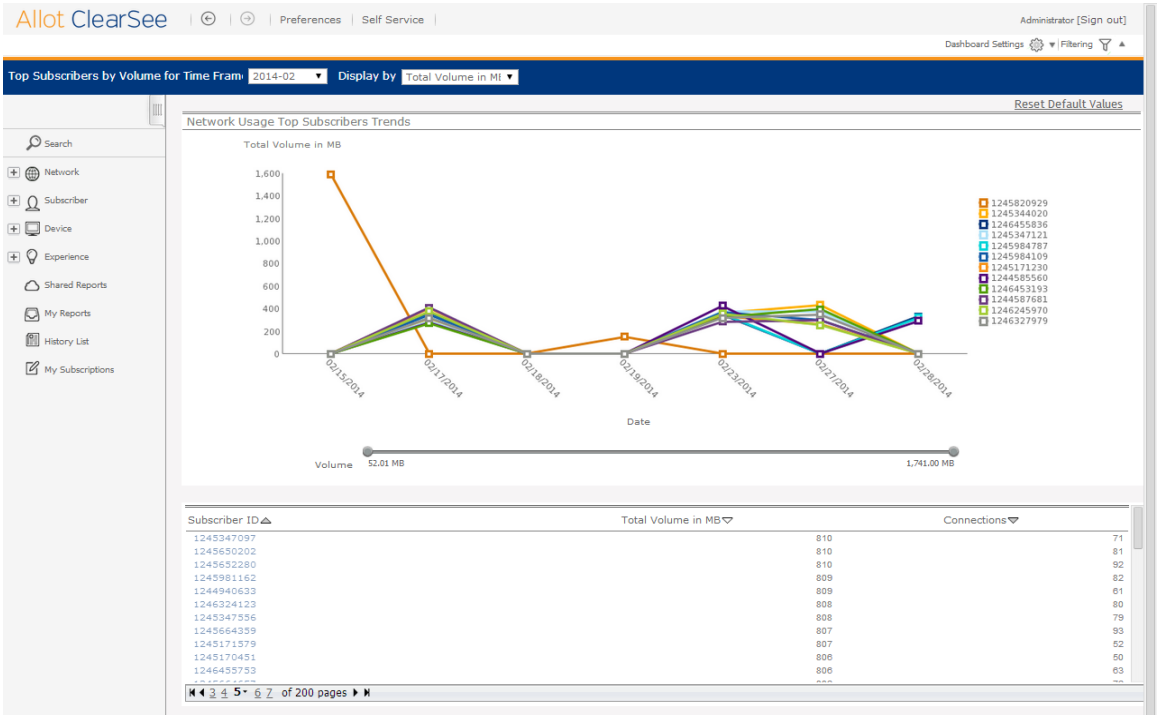


Figure 9: Heavy Users Report

AS Next Hop

This bubble graph depicts in- and out-band traffic from and to the next-hop autonomous system (AS, sometimes also referred to as routing domain). The size of each bubble illustrates the combined total bandwidth of both in-bound and out-bound traffic.

This report is useful for assessing which autonomous systems receive most usage by subscribers and the underlying application, host, subscriber and AS destinations associated with this hop.

Available presentation style: All

Information drill-down:
Drilling down into each Autonomous System "bubble" can permit correlation of Autonomous Systems to the related: Application, Host Internal, Subscriber, and Autonomous System Destination.

Grouping:
By Real-time Data, Day, Week, Month.

Filtering:
By individual Day, Week or Month

Figure 10: AS Next Hop Report

AS Destinations

This graph depicts in- and out-band traffic from and to autonomous systems destinations. You can use it to assess which autonomous systems destinations are most used by subscribers.

Note: The size of the bubble illustrates the combined total bandwidth of both in-bound and out-bound traffic.

Available presentation style: All

Information drill-down:
Drilling down into each Autonomous System "bubble" can permit correlation of Autonomous Systems Destinations to the Application, Host Internal, Subscriber, Autonomous System Destination.

Grouping:
By Real-time Data, Day, Week, Month.

Filtering:
By individual Day, Week or Month

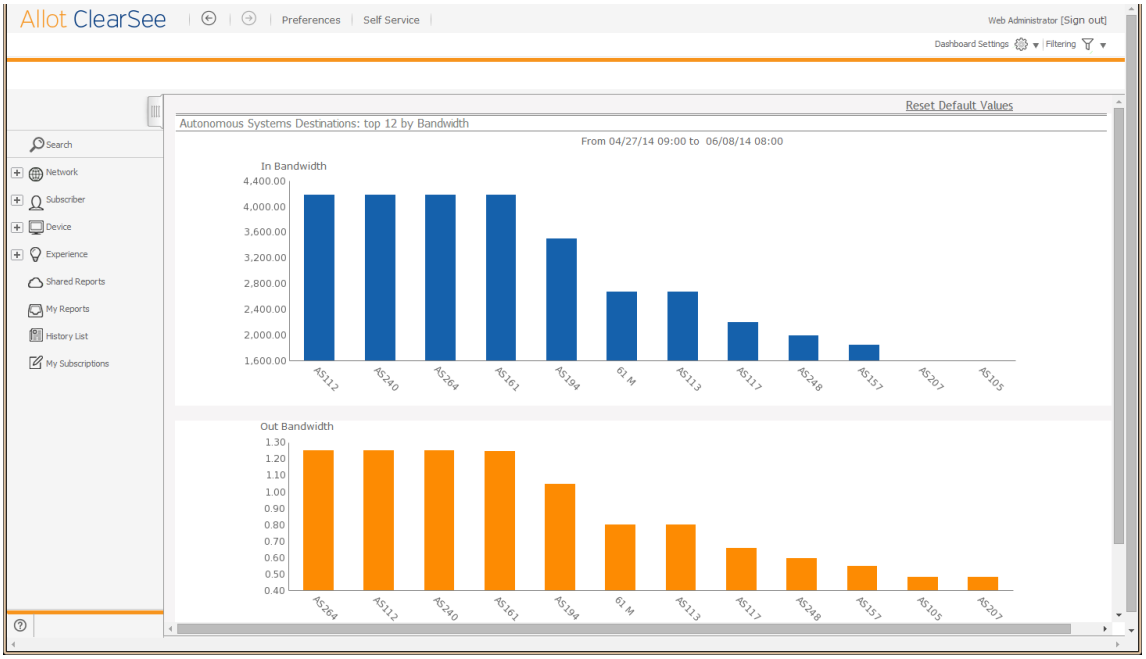


Figure 11: AS Destinations Report

Application Trends

This graph identifies the applications responsible for the most traffic, based on Bandwidth or Unique Subscribers. It identifies the top applications and which devices, subscribers, and destinations are using them.

Default presentation style: Line chart (top 12) and Grid (top 1,000). Drill-down reports in grid format.

Information drill-down: Device, Subscriber ID, Autonomous System Destination, Device Vendor, Device OS, Network cell, Network access technology.

Sort: Table can be sorted by Application, Total Bandwidth, Total Volume, Avg. Session Duration, Avg. Unique Subscribers

Display options:

Time Frame: Monthly, Daily, Hourly. Bandwidth or Unique Subscribers. Total Volume in Mbps, Total Bandwidth in GB, Average Session Duration in seconds, or Unique Subscribers.

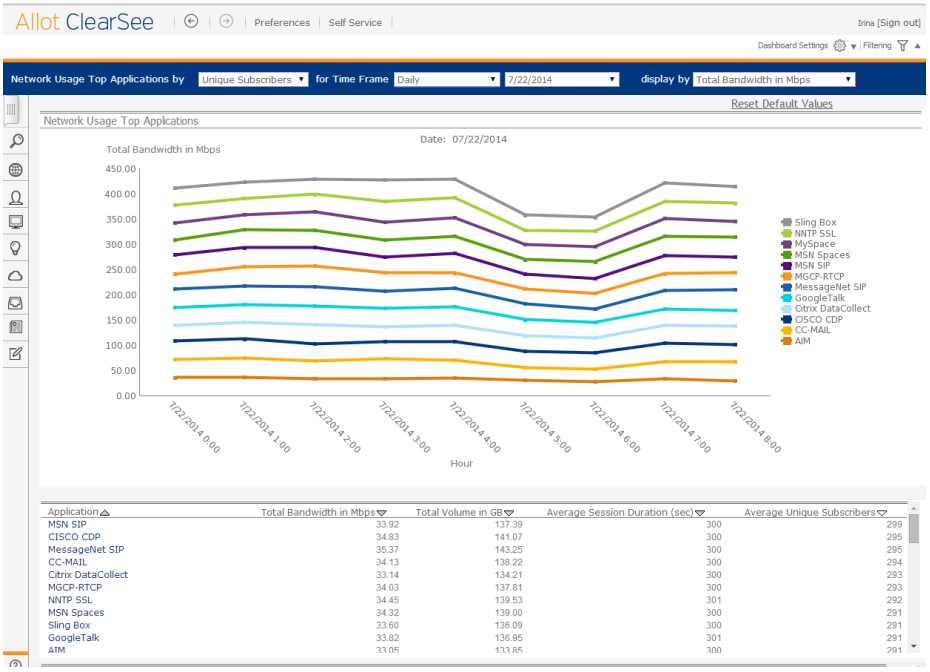


Figure 12: - Application Trends Report

User Top Sites Report

This is a detailed report for one subscriber, displaying site usage for each subscriber selected, and is useful for:

- Customizing the right service plan for a given customer
- Assessing typical use patterns by analyzing use patterns of random customers
- Understanding the "stickiness" of each website visited when "Avg Visit Duration in seconds" is selected.

Default presentation style: Horizontal Bar Chart

Information drill-down: None

Filter Options: None

Display Options:
Total Volume in MB
Number of Visits
Avg Visit Duration in seconds

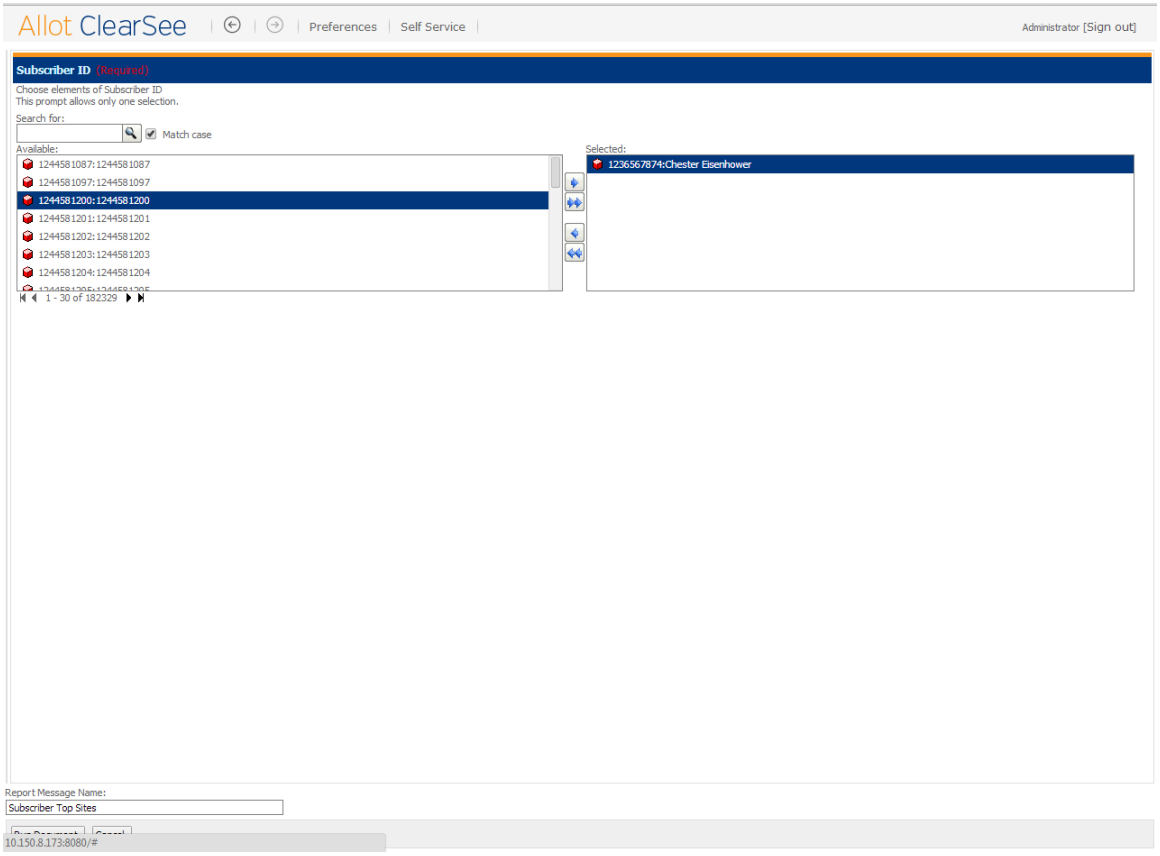


Figure 13: User Top Sites Report Selecting Filter Criteria

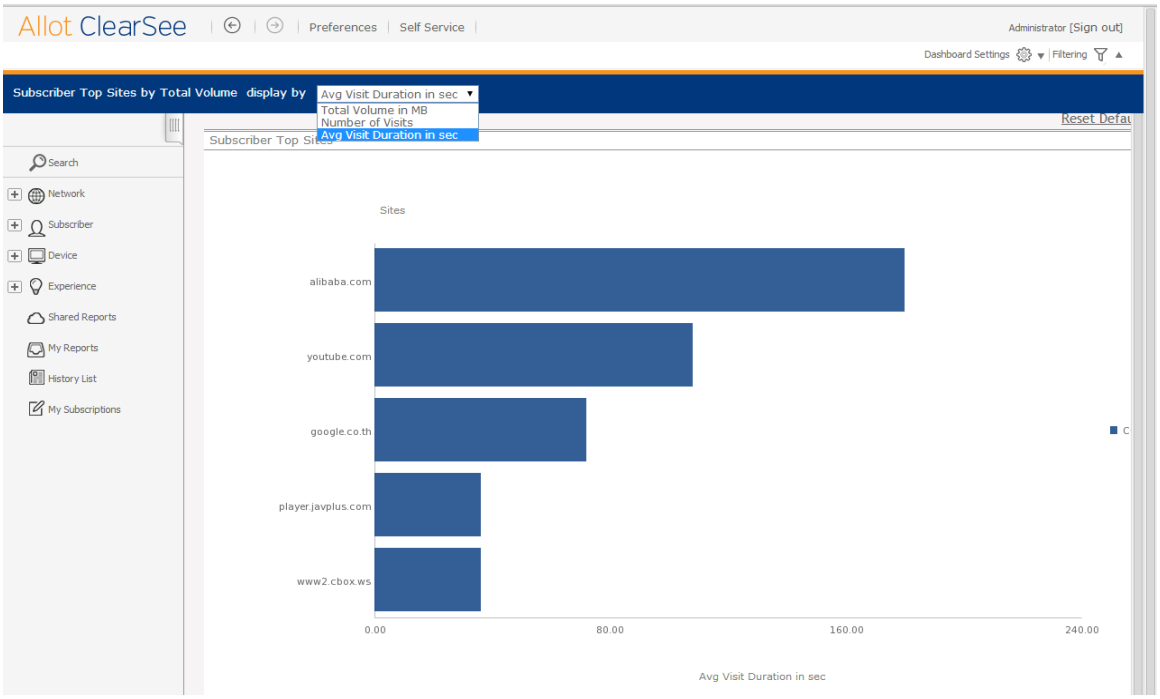


Figure 14: User Top Sites Report

User Device Usage Report

This is a detailed report for one subscriber, displaying network traffic (in MB) for each of the devices used by that subscriber. It is useful for:

- Customizing the right service plan for a given customer
- Assessing typical use patterns by analyzing use patterns of random customers.

Default presentation style: Horizontal Bar Chart

Information drill-down:
None

Filter Options:
One Subscriber Only

Display Options:
Bar Graph, Data Grid or Both

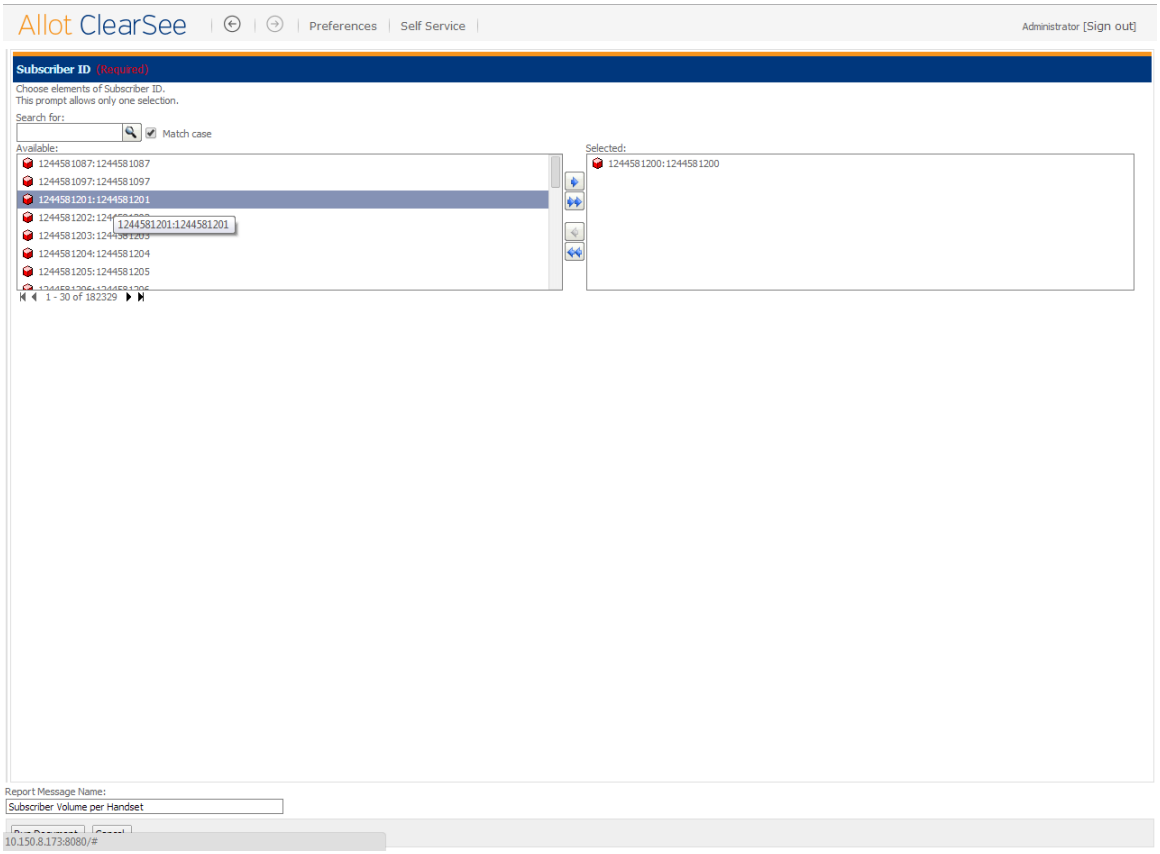


Figure 15: User Device Usage Report Selecting Filter Criteria

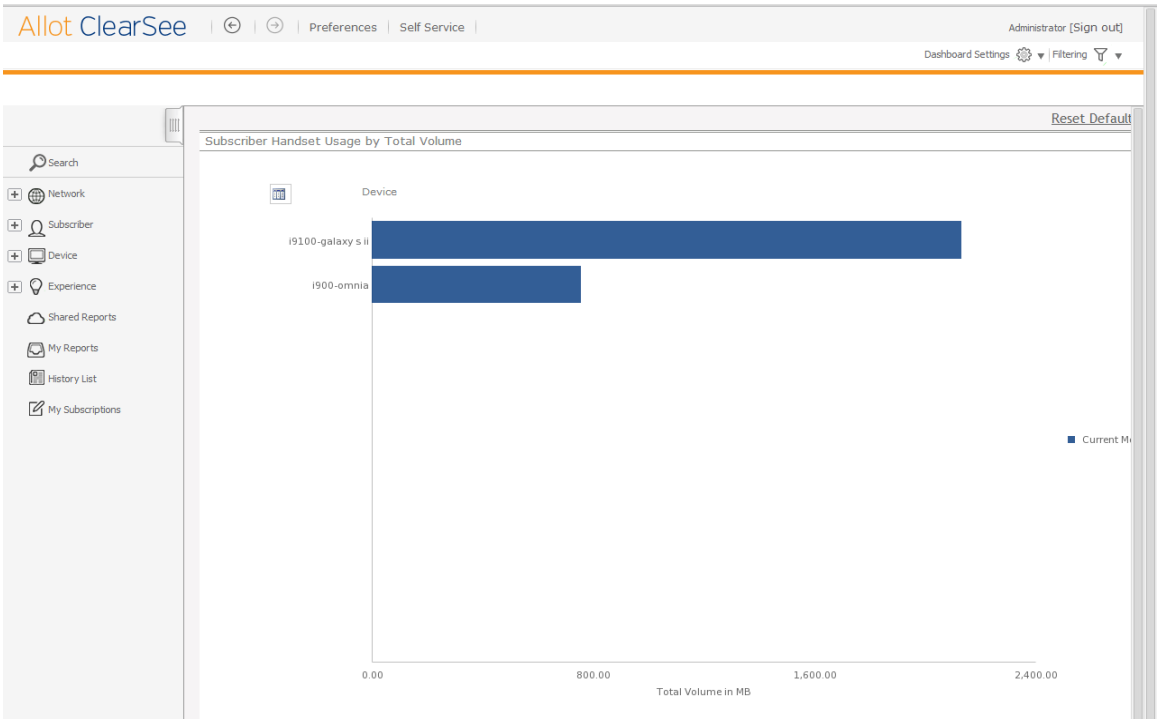


Figure 16: User Device Usage Report

CMTS Usage

Displays CMTS Usage for either Interface type—Bonding Group or Channel—for upstream or downstream traffic, displaying Bandwidth together with Unique Subscribers. This is useful for understanding CMTS capacity and usage by: Interface Down, Application, Device, Subscriber ID or DOCSIS Type.

Default presentation style: Bar Graph

Information drill-down: Interface, Application, Device, Subscriber ID or DOCSIS Type

Display options: Interface types: Bonding group or Channel

Filtering: Time Frame (Day or Month), Data direction (Up Stream or Down Stream).

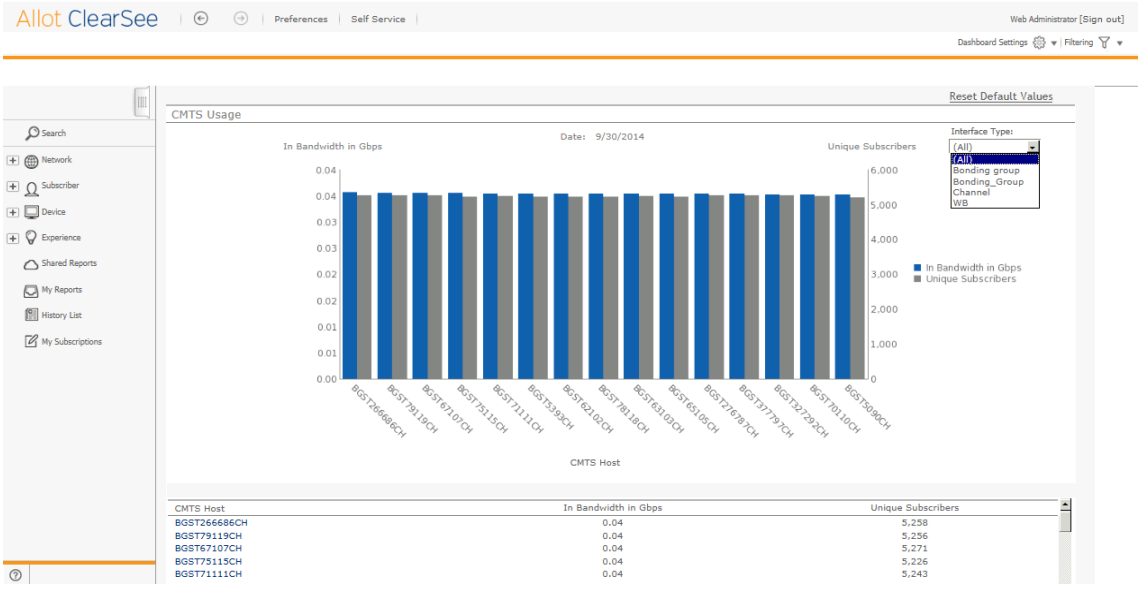


Figure 17: CMTS Usage Report

CMTS Channel Usage Trends

CMTS report displays both Bonding Group and Channel, or just Bonding Group or Channel, for up stream or down stream traffic by period. This report can identify volume metrics for CMTS interface types. You can drill into the data to determine which applications, devices, subscribers, CMTS Host or DOCSIS type are associated with that traffic.

Default presentation style: Line Graph

Information Drill Down: DOCSIS Type, Application, Device, Subscriber ID

Display options: Time Frame: Day, Month. Data direction: Up Stream or Down Stream. Bonding Group or Channel. Bandwidth or Unique Subscribers

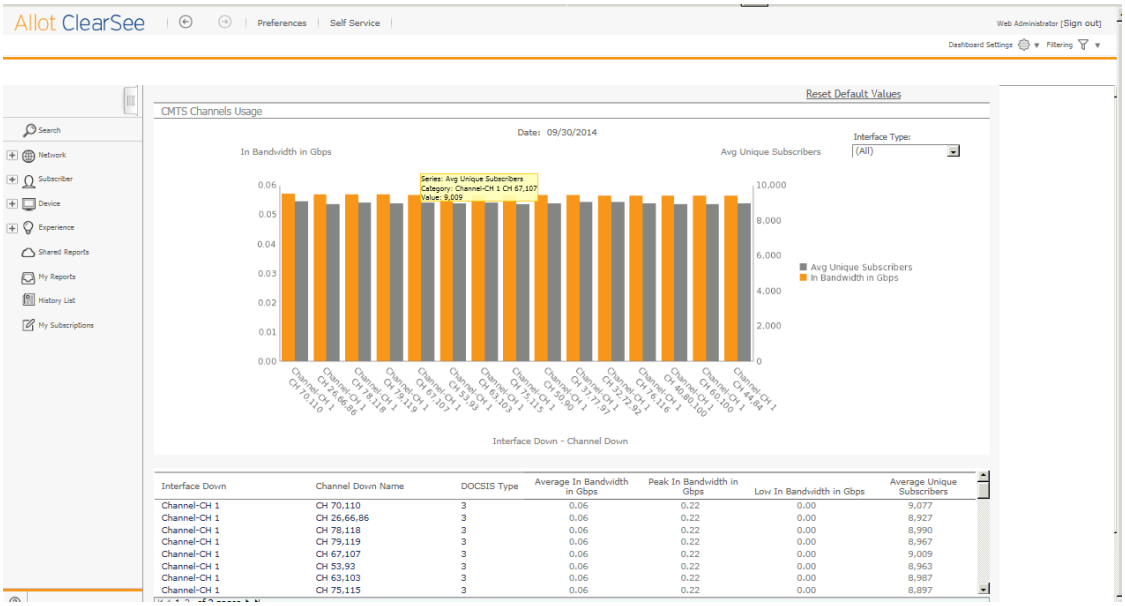


Figure 18: CMTS Channel Usage Trends Report (Bandwidth)

Self Service Report

You select "Self Service" on the Allot ClearSee title bar, and are prompted for the dataset of interest (If there are any reports and CSV Exports that have been previously generated for this data set they will appear for selection). You control to whom the report is sent, its attributes, metrics and time frame.

Various methods of presentation possible: line graphs, bar graphs, pie graphs, and grid. Allot ClearSee makes a recommendation as to which method of presentation might be most applicable to the information selected.

You can then select the filter criteria, metrics for display, and the axes for presenting the information.

A display similar to the figure below is then displayed.

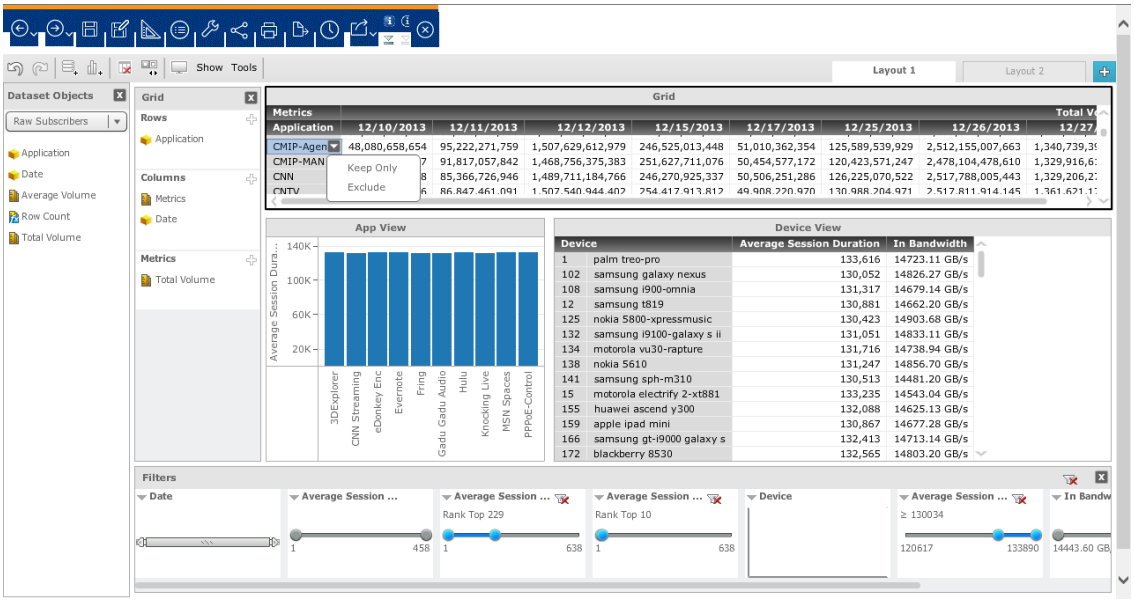


Figure 19: Self Service Report

Appendix B: Policy Examples

Monitoring

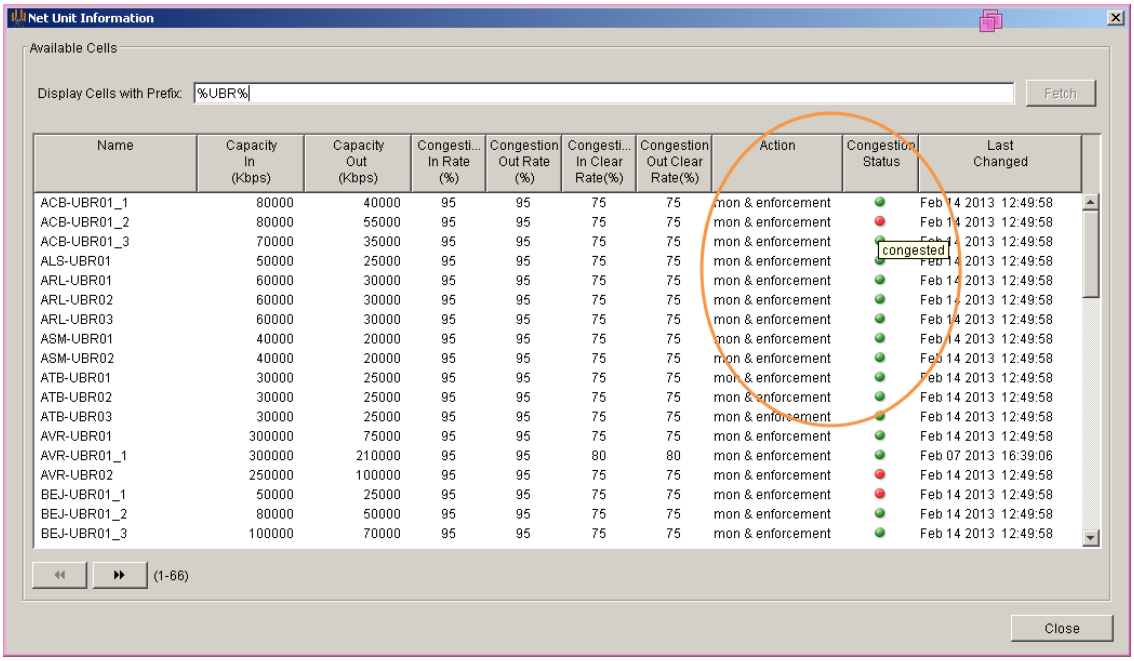


Figure 20: Congestion Dashboard

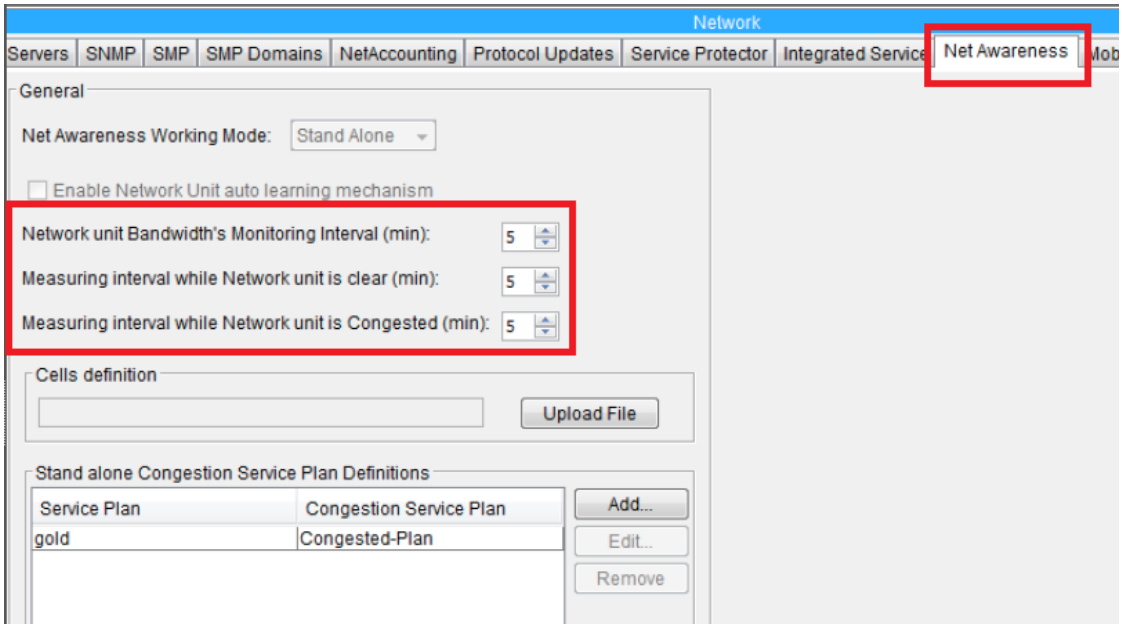


Figure 21: Flexible Congestion Monitoring Interface

Alarms

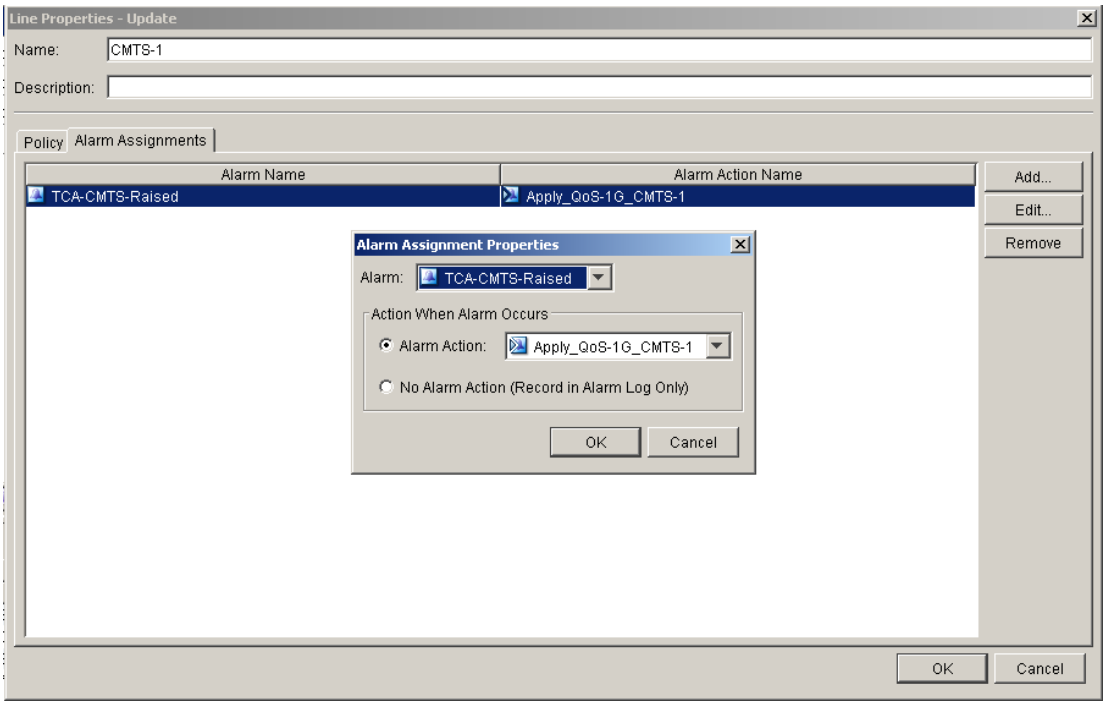


Figure 22: Setting Alarm and Action on Alarm per CMTS

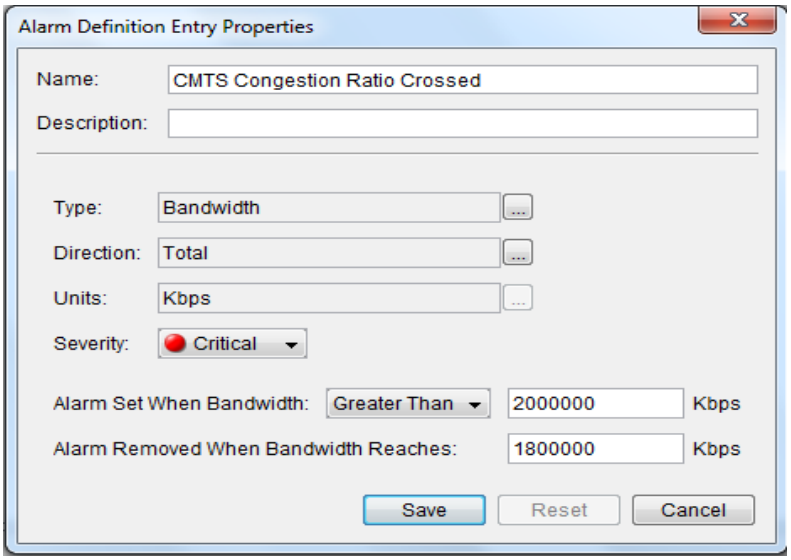


Figure 23: Setting Criteria to Trigger and Clear Alarms