

Optimizing Networks for Business Precision

Fast and Reliable Applications | Visible and Secure Network | Simple and Efficient Management

Enterprises are becoming increasingly dependent on bandwidth-critical applications. At the same time, rich media, social networking and mobile devices are revolutionizing the networking environment and the consumption of enterprise bandwidth for both business and personal use is exploding. Continuing investment in broadband is essential for enterprises to remain competitive and responsive to their customers. But, it is crucial that bandwidth is used efficiently for business and customer-centric applications while being protected from disruption by recreational and non-essential traffic.



AscenFlow is an intelligent WAN Traffic Manager that ensures protection of critical services using Deep Packet Inspection (DPI) technology to analyze IP network traffic and apply QoS enforcement policies if necessary. AscenFlow delivers optimized IP traffic flow while providing unmatched traffic visibility and analysis.

AscenFlow is the ultimate product to provide the enterprise VISIBILITY and CONTROL of network traffic, applications and users.

Visibility

AscenFlow is completely transparent to network traffic up to multi-Gbit/s network speeds. While transparent to traffic, it will monitor, and provide real-time statistical analysis of latency, traffic flow; and user and Layer 7 application behavior.

Maximize Bandwidth Resources

AscenFlow ensures that bandwidth investment is used to its full potential through traffic management, shaping, policy enforcement, Authentication and more...

Flexible Management System

AscenFlow allows administrators to configure flexible Policies to enforce network QoS/Traffic Shaping. Policies can be set based on live traffic analysis or pre-existing network profiles to fit any preference, situation, or business model.

Improve Network Security

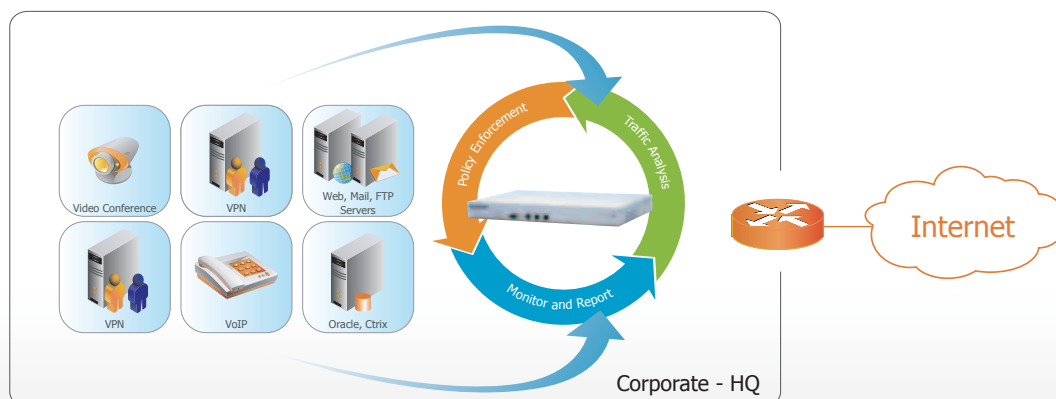
AscenFlow becomes part of the enterprise security portfolio by supporting internal and industry-standard Authentication, as well as IP/MAC mapping, Connection Limiting and the ability to "Black List" administrator-defined web sites.

Performance of Critical Applications

AscenFlow guarantees performance of critical applications such as VoIP, ERP, SAP and video streaming by prioritizing or guaranteeing bandwidth based on its DPI inspection and QoS policies.

Increase Productivity

AscenFlow improves network productivity by limiting bandwidth for recreational users, delaying the need for network bandwidth upgrades and preventing disruption of critical business applications.

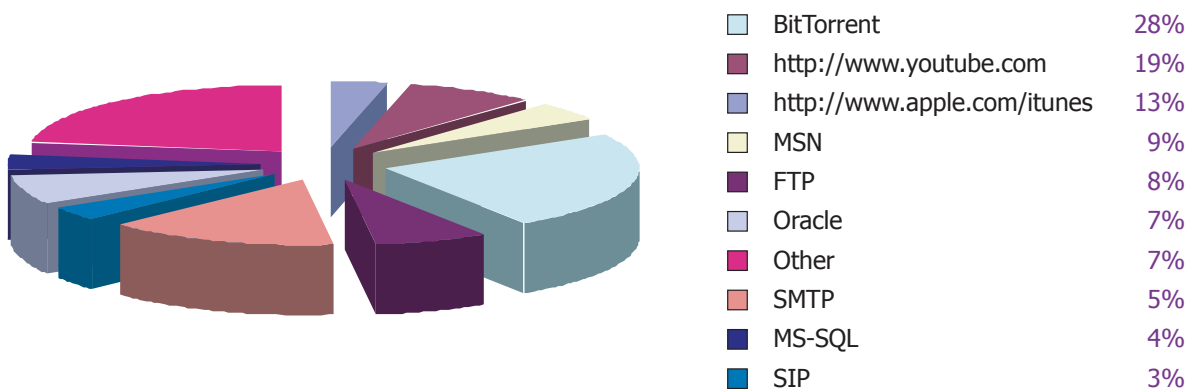


AscenFlow Traffic Analysis Engine

Most enterprises solve network bottlenecks by increasing the investment in bandwidth, but this can be costly and is often unfeasible in the short term. AscenFlow is ideal for predicting and preventing bandwidth bottlenecks. The AscenFlow Traffic Analysis Engine uses DPI technology to penetrate into Layer 7 application data flow, identifying, measuring, prioritizing and managing all kinds of traffic: critical, recreational, customer-related, and more.

AscenFlow provides detailed analysis of bandwidth usage for the enterprise to begin the first step towards network management visibility:

- DPI with Application Classification technology will instantly recognize Layer 7 applications and begin automatic traffic categorization. This keeps the network transparent while allowing administrators to observe resource usage
- Traffic Analysis measures bandwidth used by application, source, destination, URL, services, users and more. It aids administrators with network information on usage and traffic statistics, packet delivery quantity and user behavior
- Latency Analysis assists administrators onto the next step of identifying inefficient network applications to solve the bottleneck. The diagnosis will reveal the source of the bottleneck, which is either caused by traffic congestion or obstructions at the host servers
- Connection Analysis lets administrators instantly recognize traffic anomalies. If a sudden surge in connections occurs, administrators will be able to identify the unknown source by tracing IP addresses and perform the necessary actions to eliminate it

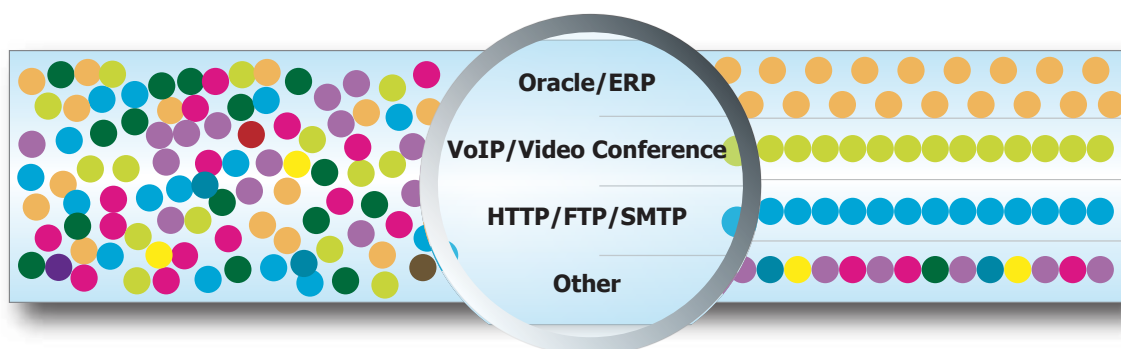


Combined, the Traffic Analysis functions help enterprises realize what portion of their bandwidth is occupied by non-business and low-priority traffic, and how that affects their business-critical applications. Once identified, effective application of bandwidth management Policies is a crucial capability in order for enterprises to reduce cost and increase efficiency and productivity.

AscenFlow Policy / Traffic Shaping Engine

Using the data from its Traffic Analysis Engine, AscenFlow's core Traffic Shaping Engine accurately controls or imposes restrictions on bandwidth usage, based on the administrator's custom-designed QoS Policies. Policies can include rules by source or destination IP, service, time-of-day, date, URL, L7 applications and application categories, authentication or any combination of these and others. The Policies are highly flexible and can be combined to match functional or business structures with different policies operating on different parts of the network. Xtera understands the complexity of business operations and therefore AscenFlow allows enterprises to set their own policies according to their needs a secure, easy-to-use and practical traffic management system.

- Bandwidth Guarantee and Bandwidth Reservation allow critical business applications to be prioritized and assigned specific minimum bandwidth. This applies to services such as ERP, VPN, VoIP, Video Conferencing, virtualization or other applications that are sensitive to delays caused by network congestion
- Bandwidth Limit imposes restrictions on non-business-critical or recreational, bandwidth-draining applications such as P2P, streaming video and gaming
- Even-Bandwidth-Allocation allows administrators to assign identical policies to all users on the network and is effective for public use networks such as hospitality or wireline and wireless ISPs
- Authentication allows administrators to manage bandwidth usage through user accounts by means of NTLM, LDAP, RADIUS, POP3 or a local database. This provides heightened security, account verification and user Class-of-Service policy capabilities
- Quota allows bandwidth to be managed based on the amount of packet traffic for specific users. Users can be restricted by volume or volume-over-time and can be redirected to billing sites, throttled or blocked if their Quota is exceeded
- Connection Limit allows each IP address a limited number of connections to other devices. This restriction prevents excessive connections from affecting critical business applications



AscenFlow Reporting and FlowReport

AscenFlow provides administrators with a real-time network reporting function capable of producing instant analysis, reports and diagnostics. Administrators can visualize and manage bandwidth on the live network.

- Traffic Statistics provides real-time updates with statistical charts and graphs to further enhance administrators' control over the network. A variety of live feeds that show bandwidth status can be selected: Long-Term (1 year / 3 months / 1 week), Short-Term (1 day / 1 hour / 5 minutes) and Real-Time (10 minutes / 30 seconds / 3 seconds)
- Traffic Latency displays real-time (1 day / 1 hour / 5 minutes) views of network latency for selected IP addresses, allowing analysis of network or server congestion
- Traffic Analysis shows graphical real-time Top 10-200 reports by Application, User, Policy IP address, URL and more
- Connection Analysis lists the Top 10-200 connections by internal IP address
- Latency Analysis shows the distribution of latency over time to aid in server and network troubleshooting

FlowReport

Long term analysis of gigabit-class networks results in the requirement to process billions of connection records. FlowReport's robust database and reporting tools expand the functionality of AscenFlow by performing additional analysis on network traffic from near-real-time to months or more. FlowReport takes AscenFlow's detailed, instantaneous statistics and creates in-depth long-term views of user and application traffic to provide unprecedented clarity of network usage and evolution. Pre-built and customized reports are simple to use and understand. Multiple operators can monitor all data or customized subsets as required.

FlowReport is the indispensable companion for AscenFlow, offering IT managers unique insights into the flow and trends of application data traversing their networks.



Flexible Network Integration

AscenFlow integrates easily into existing networks. AscenFlow supports two physical modes of operation. It can be transparently "bridged" with all traffic passing through the system or in "sniffer" mode, it can monitor SPAN or mirror ports or work with network TAPs. All AscenFlow platforms support multiple bridges and monitor ports to allow simultaneous and independent management of multiple network connections—the WAN/LAN and WAN/DMZ traffic flow, as an example.

AscenFlow also supports 2 functional modes. Traffic Analysis models monitor all network traffic for ongoing review and reporting. Traffic Shaping models add QoS Policies to Traffic Analysis to allow control of network traffic. Traffic Analysis models are in-service-upgradable to full Traffic Shaping models.

Models	M2001	M2005	M2010	M2020	M2020M	M3020	M3050	M3100	M3100M	M6100	M6200	M6300	M6300M
Application Environment	SOHO	SOHO/Branch	Branch	SME	SME	Medium	Medium	Large	Large	Large	Large	Large	HQ
Operating System	FlowOS												
WAN Bandwidth (Mb/s)	10	50	100	200	200	500	1000	1000	2000	2000	3000	3000	3000
Maximum Connections	100K	500K	500K	1M	1M	1M	2M	2M	4M	4M	8M	8M	8M
Classes	128	512	512	1024	1024	1024	2048	2048	3072	3072	4096	4096	4096
Network Interface LAN/WAN Bridge Pairs													
Base Unit													
10/100/1000 Base-TX	2	2	2	2	2	2	2	2	2	2	2	2	2
1000 Base (SFP) (Note 1)	-	-	-	-	-	2	2	2	2	2	2	2	2
Pairs with Bypass (Note 2)	2	2	2	2	2	2+2 (Option)	2+2 (Option)	2+2 (Option)	2+2 (Option)	2+2 (Option)	2+2 (Option)	2+2 (Option)	2+2 (Option)
Optional Internal Module LAN/WAN Bridge Pairs													
1000 Base-SX with Bypass	-	-	-	-	-	-	-	-	1	1	1	1	1
10000 Base (SFP+) (Note 1)	-	-	-	-	-	-	-	-	1	1	1	1	1
Other Ports													
Management/Console Ports	2	2	2	2	2	2	2	2	2	2	2	2	2
Physical Specifications													
Dimension (mm) (WxDxH)	443x292x44	443x292x44	443x292x44	443x292x44	426x396x44	426x396x44	426x396x44	431x580x88	431x580x88	431x580x88	431x580x88	431x580x88	431x580x88
RU	1U	1U	1U	1U	1U	1U	1U	2U	2U	2U	2U	2U	2U
Weight (kg)	3.2	3.2	3.2	3.2	6.2	6.2	6.2	19	19	19	19	19	19
Max. Power Consumption(W)	30	30	30	30	105	105	105	225	225	225	225	225	225
Power Supply Unit	100-240 VAC 80W	100-240 VAC 80W	100-240 VAC 80W	100-240 VAC 80W	100-240 VAC 270W	100-240 VAC 270W	100-240 VAC 270W	100-240 VAC 500W Redundant Hot-swappable	100-240 VAC 500W Redundant Hot-swappable	100-240 VAC 500W Redundant Hot-swappable	100-240 VAC 500W Redundant Hot-swappable	100-240 VAC 500W Redundant Hot-swappable	100-240 VAC 500W Redundant Hot-swappable

Features

Monitor License

Fault Tolerance

- Hardware / Electrical Failure Bypass of Copper WAN/LAN Interfaces
- Optional Hardware / Electrical Failure Bypass of Fiber WAN/LAN Interfaces
- Software Safeguard
- HA (High Availability)³

Deployment

- In-Line Transparent
- Off-Line Sniffer Mode

Traffic Analysis by

- Internal IP Address, External IP Address, MAC Addresses, Subnets, Services / Protocols (L4-L7), URL (+wild-cards)
- Service/Protocol Categories: Bank, File, IM, P2P, Streaming, Games, Remote Control, Revision Control, VoIP, Web, Proxy, Mail, VPN, Database, Stock, Default
- Classes containing any QoS/Shaping/Filter/Block parameters
- Bridges (LAN/WAN pairs)
- Authenticated Users
- Classes containing any QoS/Shaping/Filter/Block parameters

Statistics Reports

- Real Time and Short-Term Statistics, System / Traffic Logs, Alerts via Email / SNMP
- FlowReport offers a comprehensive set of historical reports based on Internal and External IP Addresses and Ranges; URLs; Users; Protocols; Groups; Classes and Interfaces
- Auto-Generated Regular Email Reports

Management

- System Status Monitoring, Configuration Backup / Restore, Firmware Updates, Protocol Signature Updates
- SNMP MIB, Web Admin / https / SSH security, Console and CLI capable
- Auto Protocol Signature Updates
- Secure Remote Assistance for GUI and Engineering support behind firewalls

Note 1: Fiber SFP/SFP+ are not included and must be supplied by customer.

Note 2: SFP Ports require optional, external fiber bypass modules.

Note 3: Optional 2nd unit for all models.

Note 4: This specification is subject to changes without notification.

Note 5: Product names and logos belong to Xtera Communications.

Note 6: For more information, you are cordially invited to visit our website at www.xtera.com

Shaping License

QoS / Shape / Filter / Block Features

- Shape, Filter, Block by: any/all Traffic shown above plus: IP Address Range, IP Address Group, URL Group, Subnets, Internal/External MAC Address, MAC Group, Classes (containing any of the above parameters)
- Multiple Priority Levels (7 levels), Guaranteed Min/Max Bandwidth, Reserved Bandwidth, Bandwidth Even-Allocation (fair use), Identity/Authentication-based Policies, Ignore List

Security

- Connection Limits by IP Address, Range or Subnet
- IP-MAC Binding
- Logout Notification

Quota

- Prepaid and Periodical (Day, Week or Month) Quota limits by Authenticated User, User Group, IP Address or Address Range and/or Subnet

Authentication

- LDAP, NTLM, RADIUS, POP3, Local (AscenFlow) Authentication databases
- Customer Defined Authorization GUI Pages

Licenses

- Demo Licenses with full functionality - 30-day increments
- Monitor License for Traffic Analysis only (Features from left column)
- Traffic Shaping License with full functionality (Features from both columns)
- Model Upgrade Licenses for simple Performance Upgrades within Platforms
- Update License for Software Feature Releases

