



ASCENFLOW

Intelligent WAN Traffic Manager

Optimizing Networks for Business Precision

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

Enterprises are becoming increasingly dependent on critical applications to operate their business. Investments in broadband are essential for enterprises to remain competitive and to further broaden their markets. It is therefore imperative the investments are used efficiently to prevent application delays and system downtime. Unmanaged and unstable bandwidth leads to poor productivity, damaged reputation, unwanted legal liabilities, and lost opportunities.



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

It is the ultimate device that provides flexible solutions for all your network problems...

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 behavior based on Layer 7 inspection.

Maximizes Bandwidth Resources

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

Flexible Management System

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

Improved Network Security

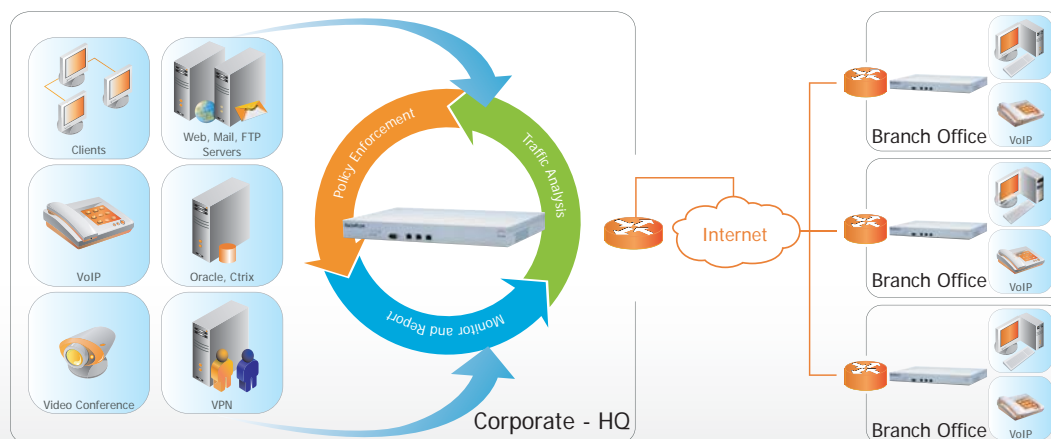
AscenFlow filters all inbound and outbound traffic and identifies anomalies to prevent attacks by triggering connection restrictions. This process minimizes the impact of intrusions while leaving regular traffic undisturbed.

Performance of Critical Applications

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

Increased Productivity

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



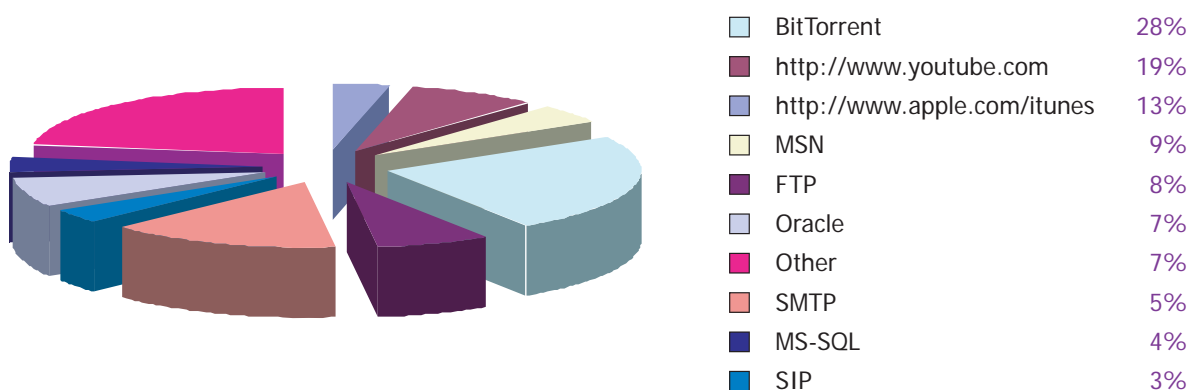
AscenFlow Analysis Engine

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 Analysis Engine uses DPI technology to penetrate into Layer 7 application traffic flow, identifying, measuring, prioritizing and managing all kinds of traffic: critical, recreational, customer-related, and more. It will not only secure bandwidth for critical applications but it will provide an efficient, reliable and secure IP network foundation on which your enterprise can trust and grow.

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

- 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 is a filter that 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.

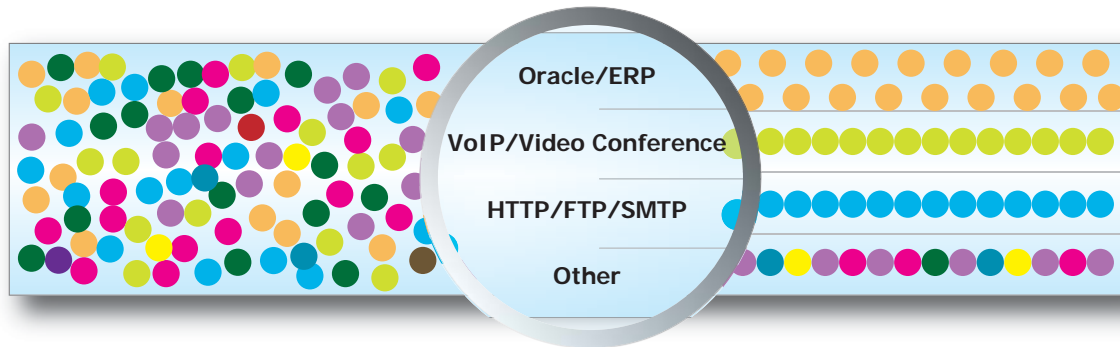
Traffic flow analysis helps enterprises realize what portion of their bandwidth is occupied by non-business and low-priority traffic, and how that affects their business-critical applications. Once identified, effective bandwidth management is a crucial capability in order for enterprises to reduce cost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



AscenFlow Policy / Shaping Engine

Using the data from its Analysis Engine, AscenFlow's core Traffic Shaping module 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, URL, application, authentication or any combination of these and others. The Policies are highly flexible and can be combined to form bandwidth structure Policies such as, management hierarchy, groups, classes, even-bandwidth-allocation (fair-use), auto discovery, user authentication and quota. 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.

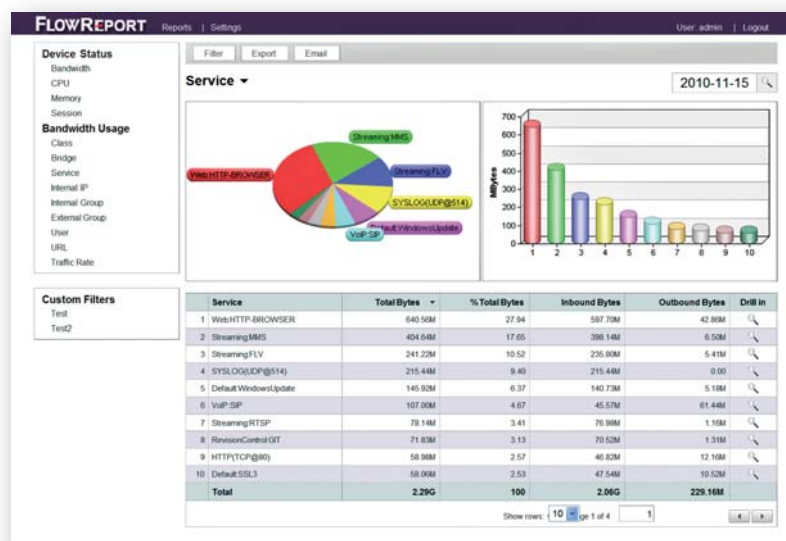
- **Bandwidth Guarantee** allows critical business applications to be prioritized and assigned specific minimum bandwidth. This applies to services such as ERP, VPN, VoIP, Video Conferencing, virtualization or other applications that are sensitive to delays caused by network congestion.
- **Bandwidth 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, ISPs or 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 denied access if the 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 Monitoring Engine and FlowReport

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

- Traffic Monitor 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 Monitor 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.
- FlowReport is AscenFlow's external companion software tool that supports long-term storage of AscenFlow statistics and additional reporting for more detailed analysis of network trends and activities.



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

Features

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) (Note 3)

Deployment

- In-Line Transparent

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
- Bridges (LAN/WAN pairs)
- Authenticated Users
- Classes containing any QoS/Shaping/Filter/Block parameters below :

QoS / Shape / Filter / Block Features

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

Authentication

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

Quota

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

Security

- Connection Limits by IP Address, Range or Subnet

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

1. Fiber SFP/SFP+ modules are not included and must be supplied by customer.
2. SFP Ports require optional, external fiber bypass modules.
3. Optional 2nd unit for M2000, M3000 & M6000 series.
4. This specification is subject to changes without notification.
5. Product names and logos belong to Xtera Communications.
6. For more information, you are cordially invited to visit our website at www.xtera.com

