



# 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 QoS enforcement policies by applying deep packet inspection (DPI) technology. The system delivers optimized traffic flow as well as providing unmatched visibility for traffic and user analysis.

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



## Visibility

Provides real-time statistical analysis to monitor latency, traffic flow and user behavior based on layer 7 identification, offering total network transparency. Ideal for spontaneous cross interface configurations.

## Maximizes Bandwidth Resources

Ensures the bandwidth investment is used to its full potential through proper management, traffic shaping, policy enforcement, and more.

## Flexible Management System

QoS network enforcement based on policies set by system administrators is open to any configurations. Policies can be set based on live traffic analysis or pre-existing system procedures to fit any preference, any situation, and any enterprise.

## Improved Network Security

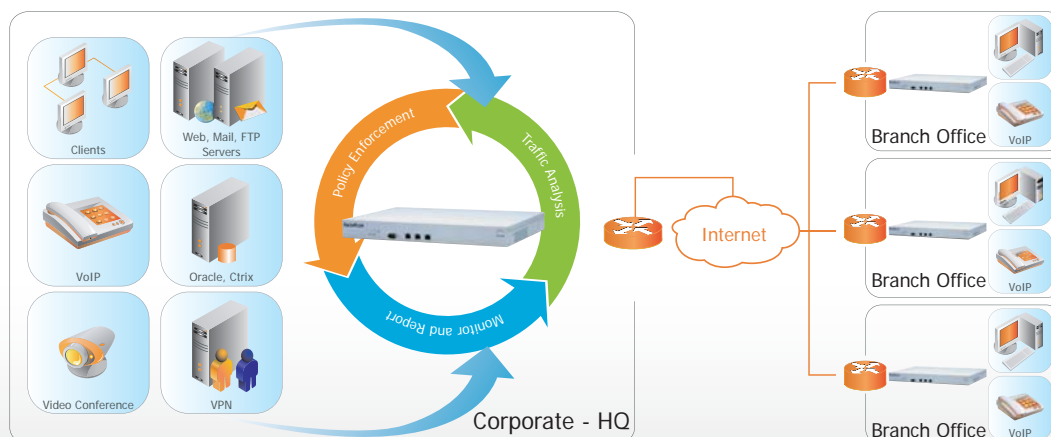
Filters all inbound and outbound traffic and identifies anomalies to prevent attacks by triggering connection restrictions. The process minimizes the impact of intrusions while leaving regular traffic undisturbed.

## Performance of Critical Applications

DPI technology and QoS policies guarantees performance of critical applications such as VoIP, ERP, SAP and video streaming by prioritizing traffic and designating bandwidth quota. This ensures critical applications are always reliable, available and fast.

## Increased Productivity

Improves network productivity by limiting bandwidth for recreational applications, prevents needless future upgrades while ensuring an optimized network and guarantees the performance of critical business applications.

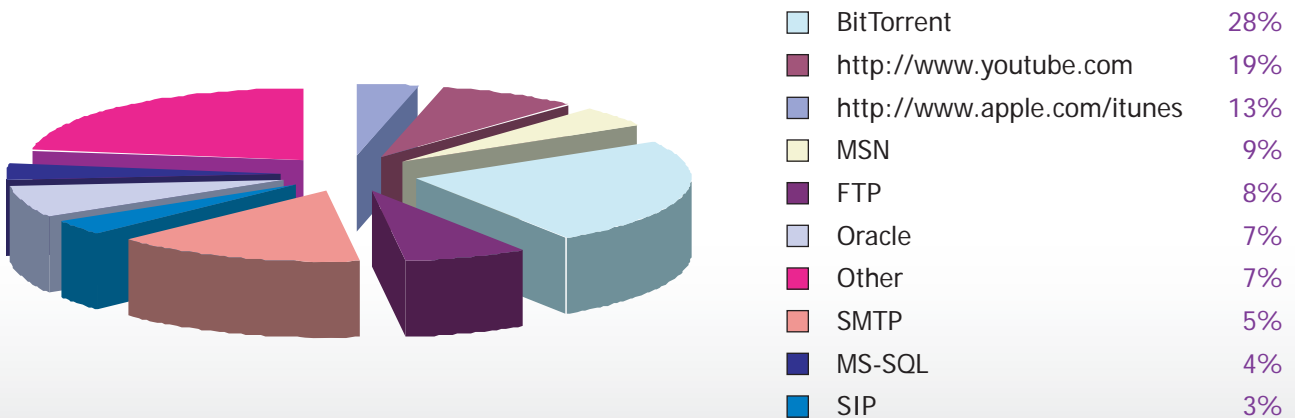


## AscenFlow Analysis Engine

Most enterprises solve bottlenecking by increasing investment in bandwidth, but this is a costly and unfeasible short term solution. The AscenFlow is ideal for predicting and preventing bandwidth bottlenecks. The engine uses DPI technology to penetrate into Layer 7 application traffic flow, conducting a full analysis capable of identifying, managing, prioritizing as well as measuring all kinds of traffic: recreational, critical, customer-related, and more. The aim is not only to secure bandwidth for critical applications, but to provide an efficient, reliable and secure foundation for which your enterprise can trust and prosper.

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

- Deep Application Classification technology will instantly recognize Layer 7 applications and begin automatic traffic categorization. This makes the network transparent and allows administrators to observe the usage of the resources.
- Traffic Analysis is a filter that designates bandwidth to traffic such as host, URL and service applications. It aides administrators with network information regarding bandwidth usage statistics, package delivery quantity, as well as details of 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.



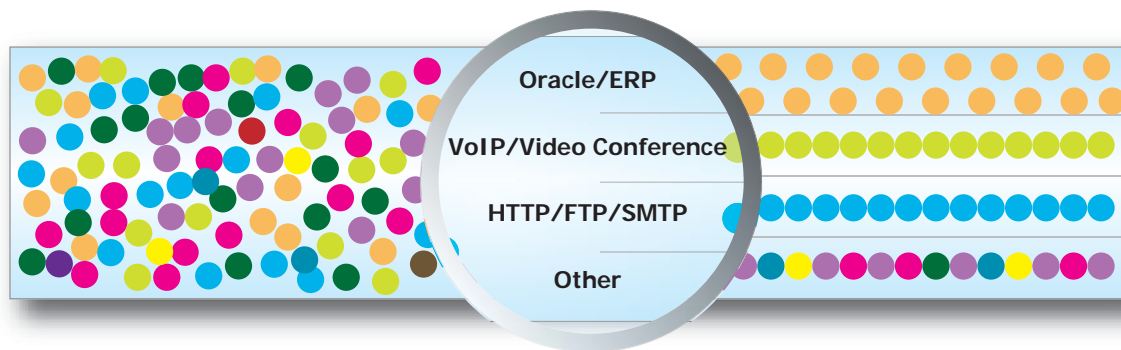
## AscenFlow Policy Shaping Engine

Traffic flow analysis helps enterprises realize that the vast majority of their bandwidth is occupied by non-business related traffic, while critical business applications has to survive by competing in a chaotic network environment. These circumstances represent a gross misuse of bandwidth, and leads to inefficiency and a waste of valuable resources. Therefore effective bandwidth management is a crucial factor for enterprises to reduce cost, increase efficiency and productivity.

AscenFlow has core traffic shaping module that accurately controls and imposes restrictions on bandwidth based on administrator's custom assigned QoS policies such as by host, service, time, URL, user behavior, or in any variation. The modules are highly flexible and can be combined to form bandwidth structure policies such as management hierarchy, groups, classes, even bandwidth allocation, auto-discovery, user authentication, quota, and connection limit. AscenFlow understands the complexity of business operations therefore it allows users to set their own policies according to their needs as well as providing a secure and practical network management system:

- **Bandwidth Guarantee** allows critical business applications to be prioritized and assign designated bandwidth, applies for services such as ERP, VPN, VoIP and Video conferencing. Applications that are sensitive to delays can also be protected. **Bandwidth Limit** imposes restrictions on non-business related, bandwidth draining applications such as P2P, online video and gaming, and is highly effective in solving the problem of bandwidth wasting.
- **Even Bandwidth Allocation** allows administrators to assign identical policies to all IP addresses on the same network, instead of enforcing the policy on each IP individually. This is especially effective for ISPs and large scale WANs.
- **Auto Discovery** allows administrators to make instant configurations and retain control of the network when anomalies occur. The system will detect applications occupying unusually large bandwidth and administrators can then add new policies immediately.
- **Connection Limit** allows each IP address limited amount of connections. This restriction prevents excessive connections from affecting critical business applications. The restriction also allows sufficient time for administrators to make the necessary configurations to avoid network congestion.

- Authentication allows administrators to manage bandwidth usage through user accounts such as NTLM, LDAP, RADIUS, POP3 and Local Database. This not only improves security, but also provides account verification on bandwidth usage where new policies can be created.
- Quota allows administrators to manage bandwidth based on the quantity of package transfers. This offers an additional dimension for administrators to allocate bandwidth based on volume or time and prevents user access to bandwidth when the quota is exceeded.



## AscenFlow Monitoring and Report Engine

AscenFlow provides administrators with real-time network monitoring function capable of producing instant analysis, reports and diagnostics. Live feeds allow administrators to visualize bandwidth management and achieve complete network control.



- Traffic Monitor 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: from Long-term (year / month / week), short-term (day / hour / minute), to instantaneous (minute / second).
- FlowReport is a tool that supplies detailed statements on the performance of all tasks and functions while providing complete document control.

Model	M50	M200	M501	M1001	M3020	M3050	M3100	M5000	M10000
Bandwidth	10 Mbps	40 Mbps	100 Mbps	200 Mbps	200 Mbps	500 Mbps	1 Gbps	1 Gbps	2 Gbps
Maximum Connections	50,000	200,000	500,000	1,000,000	1,000,000	1,000,000	2,000,000	2,000,000	3,000,000
Classes	128	512	1024	1024	1024	1024	2048	2048	2048
<b>Network Interface</b>									
Management Port	1	1	1	1	1	1	1	1	1
10/100 Base-TX	2	2	N	N	N	N	N	N	N
10/100/1000 Base - TX	N	N	4	4	4	4	4	Option <sup>1</sup>	Option <sup>1</sup>
1000 Base SX/LX	N	N	N	N	4(SX/LX) <sup>2</sup>	4(SX/LX) <sup>2</sup>	4(SX/LX) <sup>2</sup>	Option <sup>1</sup>	Option <sup>1</sup>
<b>Fault Tolerance</b>									
Hardware Failure Bypass - Copper Ports	Y	Y	Y	Y	Y	Y	Y	Y	Y
Hardware Failure Bypass - Fiber Ports	N	N	N	N	Option <sup>3</sup>	Option <sup>3</sup>	Option <sup>3</sup>	Y	Y
Software Failure Bypass	Y	Y	Y	Y	Y	Y	Y	Y	Y
HA (High Availability)	N	N	Y	Y	Y	Y	Y	Y	Y
<b>Deployment</b>									
In-Line Transparent	Y	Y	Y	Y	Y	Y	Y	Y	Y
<b>Traffic Analysis</b>									
By Host / Service / URL / Class	Y	Y	Y	Y	Y	Y	Y	Y	Y
Latency Analysis	Y	Y	Y	Y	Y	Y	Y	Y	Y
Connection Analysis	Y	Y	Y	Y	Y	Y	Y	Y	Y
<b>QoS Feature</b>									
Multiple Priority Level ( 7 Levels )	Y	Y	Y	Y	Y	Y	Y	Y	Y
Guaranteed min/max Bandwidth	Y	Y	Y	Y	Y	Y	Y	Y	Y
TCP Rate Control	Y	Y	Y	Y	Y	Y	Y	Y	Y
Layer-7 Protocol Support	Y	Y	Y	Y	Y	Y	Y	Y	Y
Identity-Based Policies	Y	Y	Y	Y	Y	Y	Y	Y	Y
By URL	Y	Y	Y	Y	Y	Y	Y	Y	Y
Bandwidth Even Allocation	Y	Y	Y	Y	Y	Y	Y	Y	Y
Auto Discovery	Y	Y	Y	Y	Y	Y	Y	Y	Y
Ignore List	Y	Y	Y	Y	Y	Y	Y	Y	Y
<b>Authentication</b>									
LDAP	Y	Y	Y	Y	Y	Y	Y	Y	Y
NTLM	Y	Y	Y	Y	Y	Y	Y	Y	Y
Radius	Y	Y	Y	Y	Y	Y	Y	Y	Y
POP3	Y	Y	Y	Y	Y	Y	Y	Y	Y
Local Database	Y	Y	Y	Y	Y	Y	Y	Y	Y
User Define Auth. Page	Y	Y	Y	Y	Y	Y	Y	Y	Y
<b>Quota</b>									
Prepaid / Periodical	Y	Y	Y	Y	Y	Y	Y	Y	Y
<b>Security</b>									
Connection Limit	Y	Y	Y	Y	Y	Y	Y	Y	Y
Layer-7 Access Control	Y	Y	Y	Y	Y	Y	Y	Y	Y
<b>Statistics / Report</b>									
Real-time Statistics	Y	Y	Y	Y	Y	Y	Y	Y	Y
System / Traffic Logs	Y	Y	Y	Y	Y	Y	Y	Y	Y
FlowReport Support	Y	Y	Y	Y	Y	Y	Y	Y	Y
Alert via Email / SNMP	Y	Y	Y	Y	Y	Y	Y	Y	Y
<b>Management</b>									
System Status Monitoring	Y	Y	Y	Y	Y	Y	Y	Y	Y
Configuration Backup / Restore	Y	Y	Y	Y	Y	Y	Y	Y	Y
Firmware Upgrade	Y	Y	Y	Y	Y	Y	Y	Y	Y
Protocol Analysis Engine Upgrade	Y	Y	Y	Y	Y	Y	Y	Y	Y
SNMP	Y	Y	Y	Y	Y	Y	Y	Y	Y
Web Admin / HTTPS	Y	Y	Y	Y	Y	Y	Y	Y	Y
Console / CLI	Y	Y	Y	Y	Y	Y	Y	Y	Y
Dimension (LxDxH) mm / Weight KG	440x270x44/4.3/1U	440x270x44/4.3/1U	505 x 330 x 88 / 8 / 2U	505x330x88/8/2U	426x396x44.4/8.2/1U	426x396x44.4/8.2/1U	426x396x44.4/8.2/1U	437x653x178/33.6/ 4U	437x653x178/33.6/4U

1. There are four slots available, the slot interface options are : Copper, 1000 Base SX and 1000 Base LX.

2. Xtera does not provide SFP modules in the M3000 series when shipping. Customers should prepare SX or LX SFP modules according to the type of their peer network devices.

3. An optional, external Fiber Bypass module is required for Fiber Bypass function.

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](http://www.xtera.com)

