

AscenFlow - P2P Solution

Background

P2P (Peer-to-Peer) technology was firstly designed and widely used by file-sharing applications which allows users to download, share, and search files among one another. As opposed to traditional Client-Server model, P2P technology makes each peer node act as both “Clients” and “Servers” to other nodes on the network, therefore, servers are not requisite in P2P networks.

Since broadband is affordable and deployed widely, plenty of P2P applications emerges and becomes popular such as KaKaA, eDonkey, Winny, Share, BiTorrent, Vagaa, eMule and much more. P2P protocols’ aggressive characteristic in consuming bandwidth, however, is threatening ISP and enterprises’ business operation.

Challenge

Due to P2P applications’ ease of access and convenience in file-sharing, using it to download and share music, video and software over enterprises’ high-speed networks becomes extremely common. Large portion of bandwidth is consumed by non-work applications; as a result, the performance of business-critical applications can not be ensured or even can be disrupted. This significant impact on enterprises’ networks could lead to poor business performance and losses of potential clients and revenue.

IDC’s survey reveals that 80% of an enterprise’s bandwidth is consumed by P2P applications which initially should be used for business-critical applications, and most of the content shared contains copyrighted materials such as music, movies, software and so on. The containment and management of P2P applications, therefore, are imperative for organizations such as government, enterprises, ISPs, colleges and so on.



■ Specific P2P Problems

□ ISPs

P2P applications aggressively consume as much bandwidth as possible by downloading and uploading file segments from different peers simultaneously, resulting in a big challenge for ISPs to provide highly reliable Internet connections.

P2P applications are very aggressive and assume bandwidth is unlimited and free so that are bursting to finish content transfers as fast as possible and squeeze out applications contending for the same bandwidth. Significant portion of bandwidth is consumed and it is one of the most significant problems causing network congestion.

P2P applications are active 24 hours; peak hours are often occurring at night and during weekends when MIS personnel are most stressed out.

□ Government and Enterprises

Employees spend plenty of working time on using P2P and recreational applications (such as gaming, Internet Radio/Video, etc.), which results in low working efficiency and poor productivity.

Bandwidth misuses consume large amount of corporate WAN bandwidth and threatens or even disrupts the performance of business-critical applications such as ERP, E-mail, VoIP, and so on.

□ Schools and Colleges

Educational network serves both educational resources sharing and students' recreational activities. Because of P2P applications' aggressive characteristics, bandwidth used for key educational applications can not be ensured.

In addition to the large amount of bandwidth consumption or even network congestion caused by P2P applications, the content shared over P2P networks varies and might contain sexually explicit and violence materials not suitable for students of minors.

Students spend too much time on recreational applications, which results in negative impact on studies.

■ Traditional Solutions to P2P Problems

Use devices such as firewall to open commonly used ports and block all the others. This might lead to accidentally blocking ports used by normal services.

Block the ports often used by P2P applications. P2P applications, however, are defensive and often hop ports, or even worse, some of them using port 80 to bypass the detection and blocking. Therefore, this is not an effective approach either.

Hide public IP address using NAT. In P2P networks, nodes that can successfully establish connections gain a high ID, and vice versa. The LAN user with only private IP, therefore, gets a low ID with which inbound and outbound traffics are limited; however, the increasing maturity of technologies such as UPnP and STUN (Simple Traversal of UDP over NAT) makes this approach ineffective.

Expanding bandwidth is typically the first reaction to improve critical application performance. Unfortunately, due to P2P applications' aggressive traits, the more bandwidth there is, the more attractive it is to P2P applications. Investing on expanding bandwidth eventually benefits P2P application performance but not business application performance.

Overall, it is imperative to figure out an effective and efficient WAN traffic management solution to manage and control P2P applications in order to ensure business-critical application performance.

Why AscenFlow

AscenFlow, the intelligent WAN traffic manager device from AscenVision, works on Layer-7 constantly monitoring and analyzing on-site traffic between the WAN and the LAN. With highly reliable AscenFlow, MIS personnel can deploy minimum/maximum bandwidth allowed on a service basis. Its powerful traffic analysis tools, alarm mechanism for abnormal bandwidth usage, and reporting tools enable administrators to monitor and analyze network usages, identify abnormal traffics, and immediately take corresponding corrective measures. Flexible policy-based traffic management framework enables network managers to tie organization's business needs to specific network management policies, therefore efficiently utilize valuable WAN bandwidth, which is critical to business success in today's Internet age.

With the increasing demand of enterprises in containment of P2P protocols, AscenVision established a sophisticated R&D team specializing in P2P protocol classification and to maintain up-to-date with the rapid changing variations of many dominant P2P protocols, and offer an industry-leading WAN traffic-shaping and QoS solution.

■ AscenFlow helps obtain following optimal controls over WAN traffics

Eliminate network congestion caused by bandwidth misuses from non work-related applications such as P2P sharing, Instant Messaging, Spam Mails and much more.

Avoid inefficient bandwidth resource allocation caused by lack of prediction of usage patterns and inaccurate traffic analysis.

Avoid poor performance and response time on business-critical applications such as ERP, CRM, Video conference, VoIP, etc. caused by lack of traffic management and prioritization.

Prevent mismatch of network usage policies from business requirements caused by lack of ability to manage network usage policies with business needs.

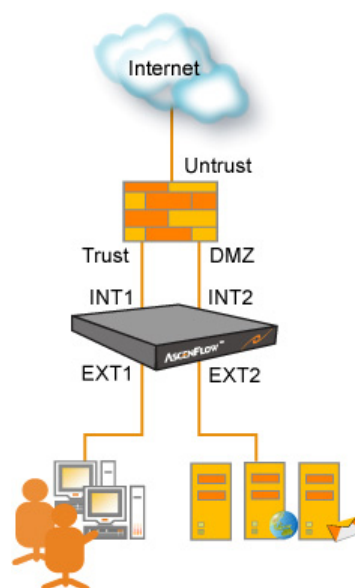
Solve low QoS and traffic usage caused by lack of centralized and intuitive policy management capability.

■ AscenFlow is easy-to-deploy and compatible in any network environments.

Transparent mode allows AscenFlow to be deployed seamlessly in existing network infrastructure without significant modification to configuration.

Combination of software and hardware failure with bypass function enables AscenFlow to provide uninterrupted services in the event of hardware or software failure.

User-friendly web-based user interface and centralized policy-based management enable IT managers to improve network QoS efficiently and easily.



Solution

AscenFlow introduces a three-step cyclic WAN traffic management solution which enables network administrators to analyze traffic usage patterns, deploy corresponding traffic-shaping policies, and monitor and track inbound and outbound traffic flows on a long-term time basis.



Step 1: Identification and Analysis

With our advanced layer-7 classification modules, AscenFlow is able to identify almost all popular P2P protocols, and other nearly a hundred protocols such as Instant Messaging, VoIP, Streaming Media, Oracle, Web, Mail, FTP, Citrix, etc..

■ Easy-to-deploy

With transparent mode, AscenFlow can be deployed in existing network topologies without significant changes to the existing configuration. AscenFlow provides an intuitive web-based administration user interface. After logging in as an administrator or a monitor, click “Bandwidth Management” and then “Analysis” on the menu bar, and then the analysis of traffic usage patterns is shown as a pie chart on a service basis by default; also, IT managers are able to query the usage pattern by source or destination IP address with selection from the drop-down list.

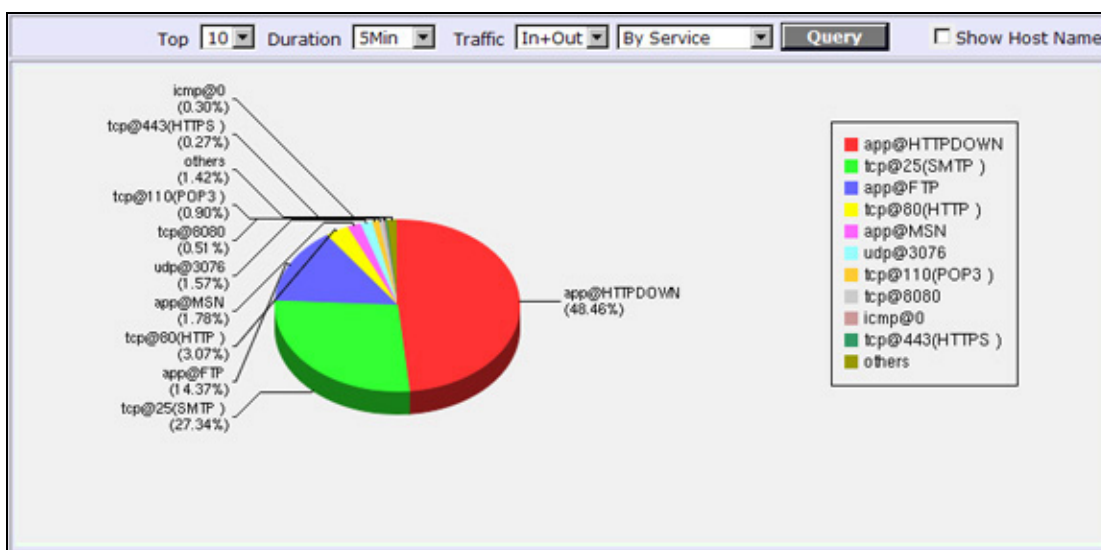


Figure1 Traffic Pattern Identification and Analysis of AscenFlow

Step 2: Traffic Shaping

■ Deploy traffic shaping policies to optimize bandwidth usage

AscenFlow provides policy-based traffic shaping mechanism to manage and prioritize both inbound and outbound traffic flows on a class basis. In order to effectively manage and control P2P applications, AscenFlow offers various means to manage traffic patterns as followings:

Filtering traffic flows by source IP address/IP range, destination IP address/IP range, or Subnet

Managing bandwidth based upon application-layer protocols or service ports

Setting time groups to separate working hours and idle hours

Applying authentication scheme to associate QoS policies with user identities

Assigning quota to users or user groups

■ Connection Limit and Network Attack Defense Module

Connection Limit, the unique function of AscenFlow, enables to block subsequent connections due to P2P applications so as to offload bandwidth consumption. It can be deployed on the basis of users, IP addresses, IP ranges or subnet.

In addition, the combination of Connection Limit and AscenFlow's embedded network attack defense module acts as a double safeguard against network crash caused by the virus attack to a single PC in a LAN. The virus attacks that can be blocked include UDP Flood, SYN Flood, DDoS Flood and so on.

Enable Log <input checked="" type="checkbox"/>			
Single IP			
<input type="button" value="+"/>	IP	Type	Limit
<input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="↑"/> <input type="button" value="↓"/>	10.16.0.19	Unlimit	
IP Range/Subnet			
<input type="button" value="+"/>	IP Range/Subnet	Type	Limit
<input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="↑"/> <input type="button" value="↓"/>	10.16.0.0/255.255.0.0	Limit	1000

Figure2 Connection Limit of AscenFlow

■ Hardware and Software failure with bypass

The combination of hardware and software failure with bypass ensures uninterrupted services in the event of hardware or software failure, which helps enterprises reduce potential risks caused by network interruption.

Step 3: Statistics and Reporting

AscenFlow companion tool, FlowReport, provides comprehensive report and analysis for all major functions of AscenFlow. It analyzes the large volume of log data generated by AscenFlow and generates a complete range of analysis and reports for MIS personnel to better understand the long-term trend of the traffic behaviors, typically not easily identifiable from AscenFlow built-in analysis tools.

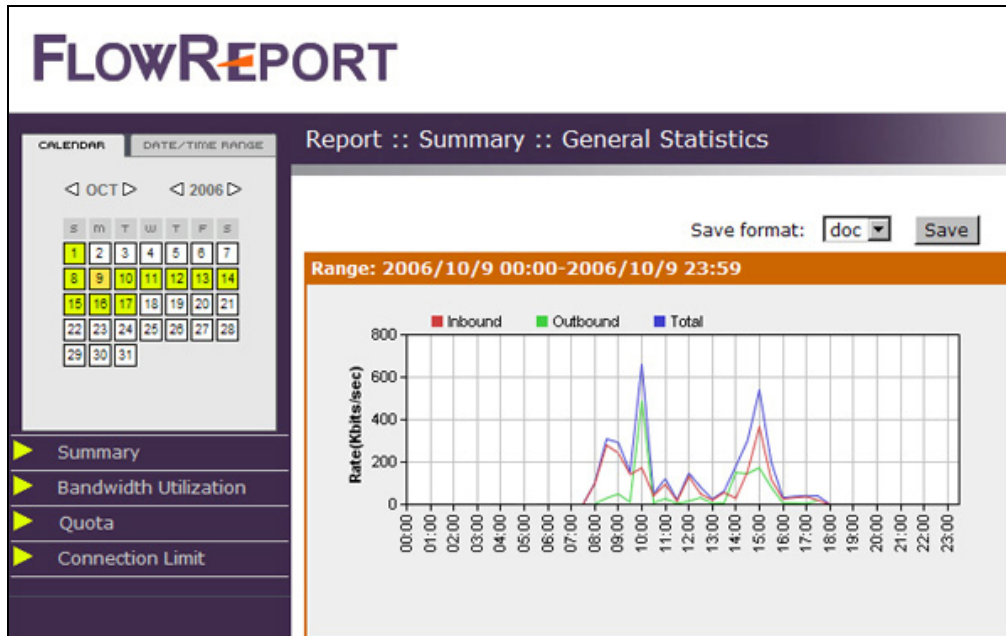


Figure3 FlowReport

Case Study

A firm with a 2Mbps fiber suffers from heavy traffic flows of P2P applications, leading to a significant impact on business performance. The deployment of AscenFlow in the network effectively ensures the performance of critical applications and highly improves business operation.

Solution

■ Service Grouping

Set a service group named as “P2P Group” and include a variety of P2P protocols.

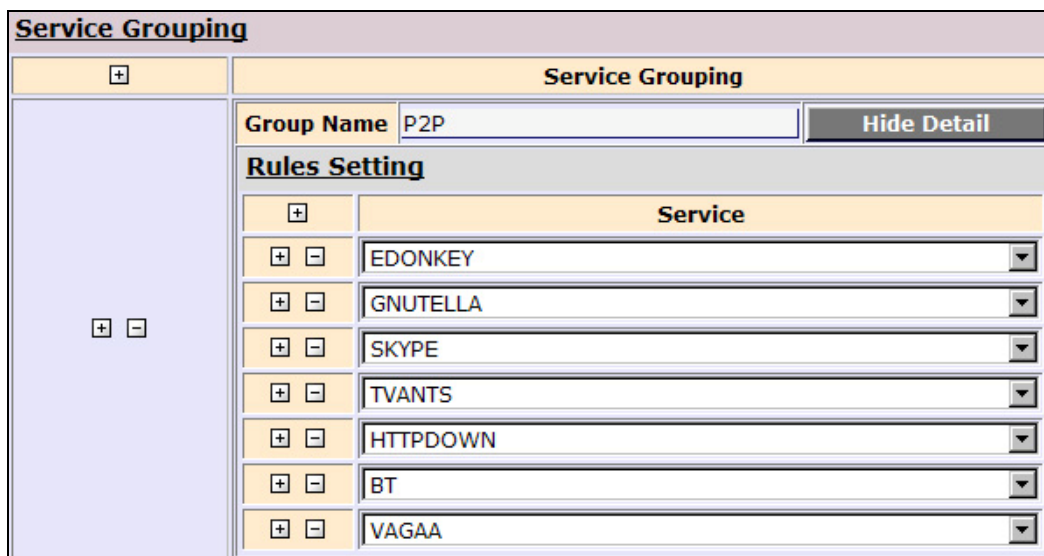


Figure4 Settings of Service Grouping

■ Time Grouping

Define a time group to specify working hours so as to ensure the performance of business-critical applications and allow employees using the network more freely after work.

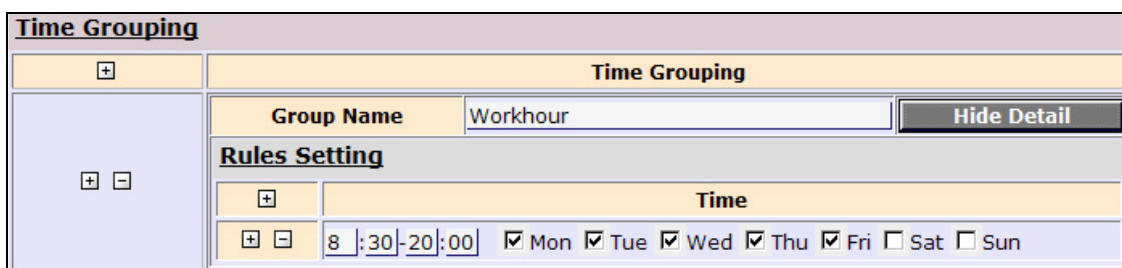


Figure5 Settings of Time Grouping

■ Traffic Shaping

Add two pieces of policies “P2P-IN” and “P2P-OUT” under class “INBOUND” and “OUTBOUND” respectively, and then input “20Kbps” to the maximum bandwidth of both. Together with the service and time group established in previous two steps, it inhibits bandwidth misuses of P2P applications during working hours and allows employees to enjoy the high-speed network after work.

Class List					
Class	Brief				
	E		Min	Max	Pri
INBOUND				50000	
httpdown	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1000	2000	N
QQlive	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	1000	N
QQ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	N
skype-in	<input checked="" type="checkbox"/>	<input type="checkbox"/>	128	256	H-
P2P-IN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	20	20	L+
Default			0	50000	
OUTBOUND				50000	
httpdown	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1000	2000	N
QQlive	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	1000	N
QQ-out	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	N
skype-out	<input checked="" type="checkbox"/>	<input type="checkbox"/>	128	256	N
P2P-OUT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	20	20	L+
Default			0	50000	

Edit	
Name	P2P-IN
Enable	<input checked="" type="checkbox"/>
Min	20
Max	20
Priority	Low
Enable Even Allocation	
Enable	<input type="checkbox"/>
IP Counts in Pool	
Max Bandwidth per IP	
Filter List	
Filter	
Source	Any
Destination	IPGROUP:TKT-IP
Service	SERVICEGROUP:P2P
Time	TIMEGROUP:Workhour
Authentication	Any

Figure6 Settings of Traffic Shaping

■ Short-term statistics

Following figure shows apparent changes after management policies taking effects.

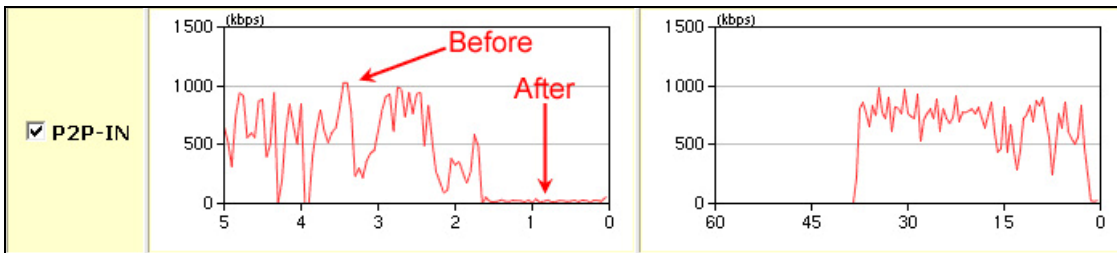


Figure7 Short-term Statistics

Benefit

■ Government and Enterprises

AscenFlow effectively inhibits inbound traffic flows of P2P applications and ensures performance of business-critical applications such as ERP, CRM, VoIP, VPN, Video Conference, and so on.

AscenFlow ensures organizations providing highly accessible outlets for outbound services to guarantee partners and end-users to enjoy uninterrupted services.

AscenFlow effective traffic management tools provide a cost-effective solution for enterprises to improve productivity and business performance with valuable bandwidth.

■ ISPs

AscenFlow reduces inbound traffic flows of P2P applications and ensures ISP providing streamlined internet services.

AscenFlow quota system supports two quota mechanisms: prepaid and periodical, enabling ISPs to offer more flexible services. AscenFlow built-in authentication system, seamlessly integrated with ISP's user account management system such as Radius, LDAP, or Microsoft's NTLM, further enhances the usability and effectiveness of the Quota system.

FlowReport offers powerful tools to better understand and manage network usage patterns.

■ Schools and Colleges

AscenFlow assures the priority and performance of key educational applications and helps create a high-speed e-Learning environment.

AscenFlow inhibits traffic flows of recreational applications avoiding students to be addicted to gaming, violence, and sexually explicit materials

AscenFlow quota system supports network administrators to assign quota either by IP addresses or by users. Combined with the authentication module, the quota system is particularly useful to the proper management of the student dormitory and campus network.

■ Conclusion

Since the increasing popularity of P2P sharing brings significant impact on organizations' business-critical application performance, enterprises must take appropriate reactions to impair bandwidth misuses and improve business performance. Network usage policies is not sufficient and effective to control P2P file sharing usage, however, with AscenFlow, enterprises can associate QoS and business needs with network usage policies and enforce the policy to take effect. Put it another way, AscenFlow provides an ideal, easy-to-deploy, and cost-effective WAN traffic management and QoS solution helping enterprises gain optimal and visible control over P2P applications and protocols.

Appendix: List of P2P applications and protocols that AscenFlow can identify:

Type of Application	Application Name	Protocol or Software Name
P2P	BT	
		Bitcomet
		BitSpirit
		BitTorrent Deadman Walking
		BitTorrent
		BitTorrent Plus!
		BitVampire-win32
		BTogether
		eXeem Lite
		FlashBT
		TurboBT
		GreedBT
	Gnutella	
		acquisition
		BearShare
		FreeWire
		LimeWire
		Gtk-Gnutella
		Gnucleus
		NeoNapaser
		Nova
		Phex
		Shareaza
		Xolox
	Edonkey	
		eMule
		eMule Plus
		eDonkey
		eDonkey 2000
		Zcom
	POCO	
		POCO
		PP2005
		magbox
		vika
		Kubao
	Vagaa	
		Vagaa(KAD,EDK)
	QQLive	
		QQlive
	PPLive	
		PPLive
	PPStream	
		PPStream
	Share	
		Share

Winny	
	Winny
iEbook	
	iEbook
TVants	
	TVants
Xplus	
	Xplus
Multimedia	
	MMS RTSP
flashget	
	HTTPDown,MMS,RTSP
netant	
	HTTPDown,MMS,RTSP
DuDu	
	HTTPDown,MMS,RTSP
Thunder	
	HTTPDown,MMS,RTSP
HttpDown	
	HttpDown