

## AscenFlow Technical White Paper

### Overview

AscenFlow, a technological breakthrough product, is a policy-based bandwidth management appliance that provides network Quality of Service (QoS) and for users exchanging information over networks. Instead of providing the conventional QoS based on the IP address which has many flaws, AscenFlow uses the policy-based bandwidth management approach and provides powerful traffic analysis tools and alarm mechanism to detect abnormal traffic flows to optimize network usage.

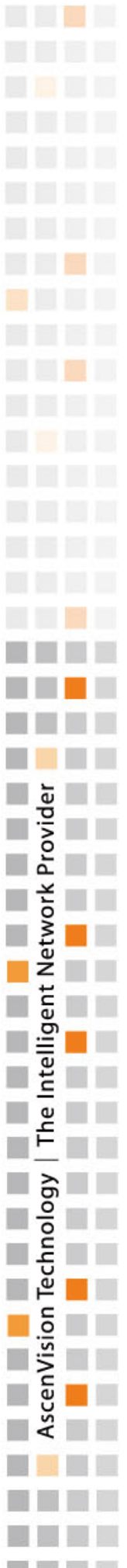
With the dramatic growth of the Internet technology, the mission-critical applications of businesses, government organizations and education institutions are ever more relying on the Internet. However non-mission critical applications such as online shopping, Instant Messaging (IM), peer-to-peer (P2P) file sharing and so on consume significant portion of valuable bandwidth. In order to solve such network bandwidth problem at the same time guarantee network QoS, traditionally, funding on expanding bandwidth is the first reaction but MIS personnel finds out it's not an effective approach. One of the better solutions is to apply traffic management technology to avoid network congestion by limiting or even blocking non work-related traffic flows. AscenFlow, the best choice for MIS personnel, provides policy-based bandwidth management and control helping network administrators gain optimal and visible control over bandwidth misuses.

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.



AscenFlow can be configured based on individual user bandwidth requirements. According to different users' needs, the bandwidth allocation needs to differ or to be prioritized. AscenFlow provides flexible bandwidth management mechanism on the basis of network services, type of individual or group users, time duration, network location, priority, the amount of bandwidth allocated, and combination of each. In addition to it, AscenFlow build-in authentication system can be seamlessly integrated with other account management systems such as NTLM, LDAP, RADIUS and Local Database. Combined with Even Allocation function, each individual user can obtain equal amount of bandwidth.

The increasing growth of applications makes network usage get more and more complex, for instance, bandwidth-consuming P2P applications and other unpredictable and unmanageable applications. In such cases, AscenFlow can be flexible in configurations to manage specific network service and usage, enforce bandwidth quotas and usage, and guarantee specific users or departments a certain amount of bandwidth at all times to fully utilize the valuable bandwidth resources.



## Product Features and Technical Details

Key features and its related technical details are:

### Excellent Price/Performance Ratio with user-friendly Hardware Design

Allow configuration based on actual individual user's bandwidth requirements thus yields the best price/performance ratio. Reduce corporate broadband investment while increasing productivity and application performance.

The combination of hardware and software failure with bypass ensures uninterrupted network services in the event of hardware or software failure.

Transparent Mode enables AscenFlow to be deployed in an existing network without significant changes to current configuration.

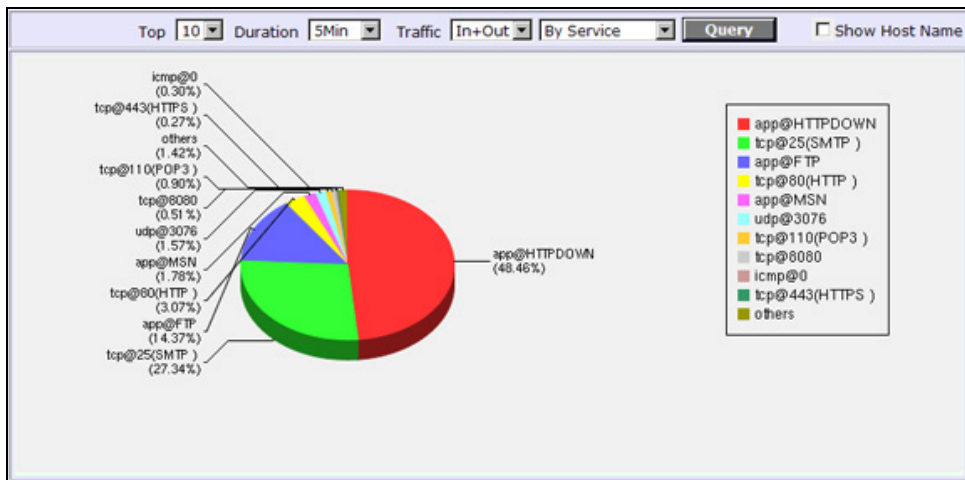
### Constant Traffic Analysis

Monitor real-time bandwidth usage patterns and alarm abnormal traffic flows via either SNMP or Email enabling network administrators to immediately gain accurate information thus to avoid network interruption.

Analyze based on a traffic source, destination, and network service in order to gain a better insight into the actual bandwidth usage patterns.

Identify and monitor a hundred of applications and protocols such as IM, P2P file sharing, video conference, and so on, helping network administrators optimize bandwidth usage and improve network QoS.

When abnormal traffic takes place, AscenFlow can automatically adjust bandwidth allocation to traffic usage patterns to provide non-stop services.

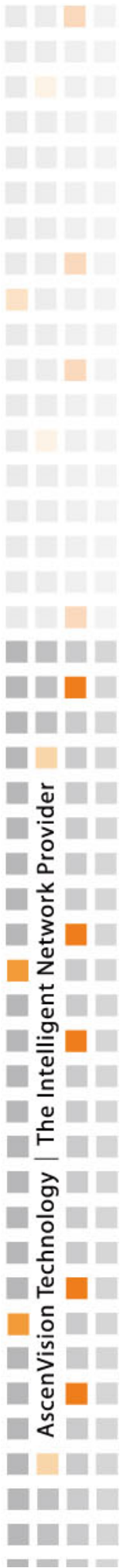


### Powerful Bandwidth Management

AscenFlow's policy-based bandwidth management allows defining class and rules based on grouping such as IP grouping, MAC grouping, authentication grouping, time grouping, service grouping and combination of each to meet business management policies.

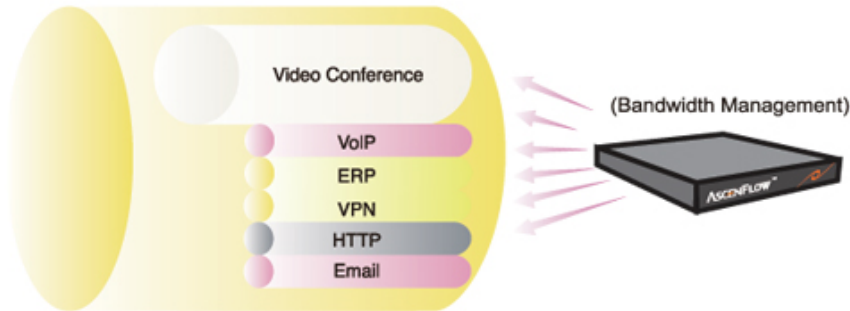
AscenFlow supports to assign bandwidth based on User/IP Address/Services/Time to increase management flexibility.

In addition, with proper definition of rules, AscenFlow can reserve bandwidth for mission-critical applications and limit bandwidth for non-business applications to avoid any misuse of bandwidth resources.



AscenFlow supports a variety of Layer-7 protocols and assigns minimum/maximum bandwidth accordingly based on the proper setting of policies.

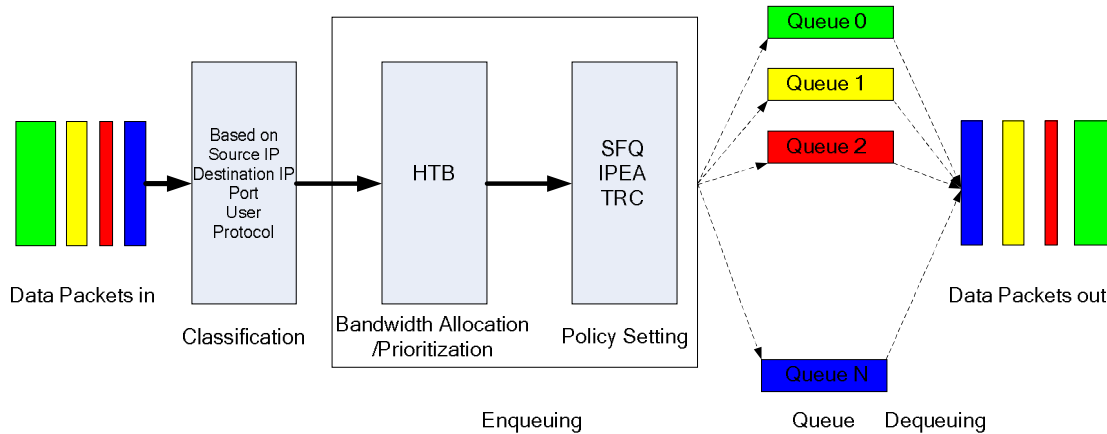
Hierarchical policy management makes AscenFlow a powerful solution to traffic shaping. Its Even Allocation function allocates each machine in the LAN with an even and maximum portion of bandwidth.



Below are the technical details of how AscenFlow bandwidth management works:

■ **Traffic Shaping Workflow**

The bandwidth of a WAN is much smaller than a LAN, therefore, when outbound traffic flows to the WAN, potential risks of loss of data or resending data may occur. AscenFlow bandwidth management mechanism effectively solves this problem. The figure below illustrates how this mechanism works:



Firstly, when data packets flow in, AscenFlow classifies it on the basis of source addresses, destination addresses, ports, users, and Layer-7 protocols for enqueueing.

Next, Hierarchical Token Bucket (HTB) queuing discipline is applied to assign bandwidth to and prioritize the packets.

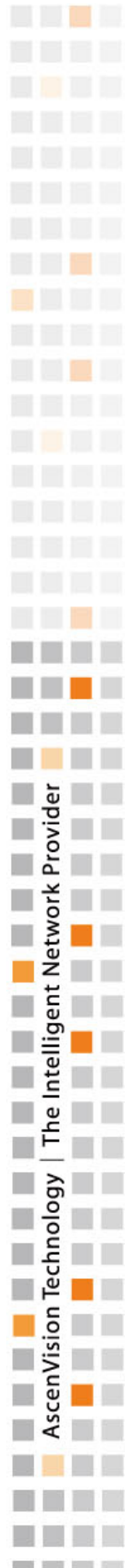
After that, three queuing disciplines: Stochastic Fairness Queuing (SFQ), IP Even Allocation (IPEA), and TCP Rate Control (TRC) are used to manage the packets. After enqueueing, the packets are dequeued and then flow out.

■ **Traffic Shaping Mechanism**

There are four key queuing mechanisms in AscenFlow traffic shaping mechanism:

▫ **Hierarchical Token Bucket (HTB)**

HTB, a classful queuing discipline, prioritizes and allocates bandwidth to the data packets. The two main functions of HTB are Prioritization and Bandwidth Allocation:



- **Prioritization:**

HTB assigns each queue a priority to divide critical and non-critical traffic flows. This is how the 7 priorities of AscenFlow achieved.

- **Bandwidth Allocation:**

HTB is able to control the use of outbound bandwidth on a link. It uses a physical link to simulate several slower links or deliver different kinds of traffic via different simulated links. HTB ensures each class can get at least a minimum amount of bandwidth it requests or a maximum amount of bandwidth assigned to it. If the class requests less bandwidth than the amount assigned, the excess bandwidth is then distributed to other classes that request more bandwidth. Therefore, we can control and prioritize different kinds of traffic flows.

- **Stochastic Fairness Queuing (SFQ)**

SFQ, an implementation of fair queuing algorithms family, requires less calculation while being almost perfectly fair. The key point in SFQ is the session (or flow). Traffic is divided into plenty of FIFO queues, one for each session; and then it is sent in a round-robin manner so that each session is given a chance to send data in turn. This is a fair approach to ensure the fairness of each session.

SFQ is called “stochastic” because that it doesn’t allocate a queue for each session but uses hashing algorithm to allocate all sessions over a limited number of queues. Due to hashing, a queue probably is allocated multiple sessions, which requires sharing of the bandwidth to allow each session sending a packet. In order to make it unnoticeable, SFQ changes its hashing algorithm frequently allowing colliding sessions to do it in only a small number of seconds.

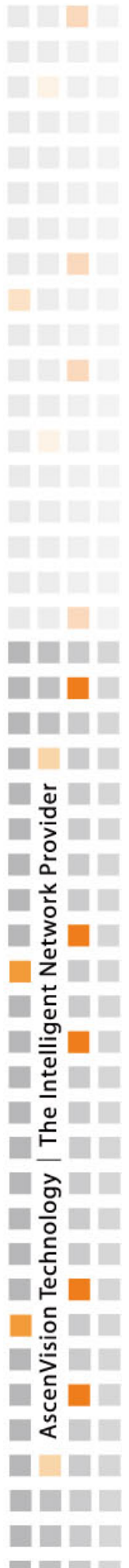
SFQ is work-conserving which makes the link always busy. In other words, SFQ immediately allocates the traffic once it receives the data.

- **IP Even Allocation (IPEA)**

IPEA, unique technology of AscenVision, evenly allocates each IP address fair and maximum amount of bandwidth.

- **TCP Rate Control (TRC)**

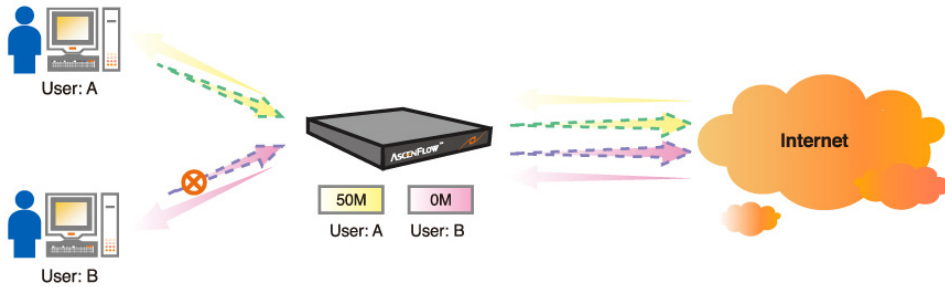
TRC improves TCP performance by controlling the size of data packets sent per second, which prevents losing data packets from network congestion. To do so, it enforces both inbound and outbound data packets to be sent at a constant rate (bits-per-second) avoiding bursting, loss or resending of data packets.



**Quota**

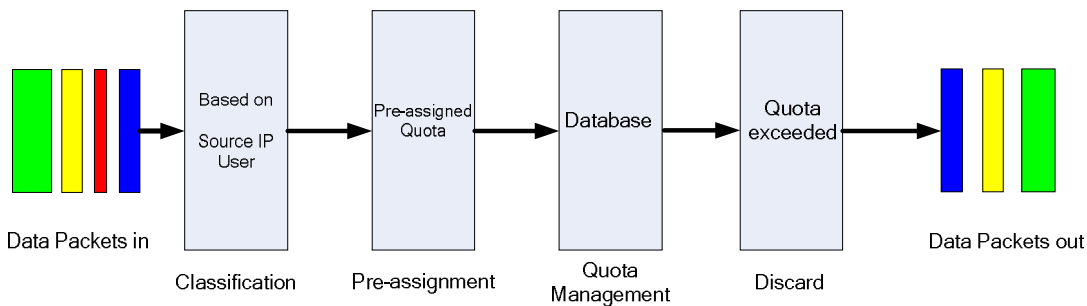
AscenFlow quota system, not commonly seen in Traffic Management and QoS devices, supports two types of quota mechanism: prepaid and periodic, offering ISPs flexible options in account management.

AscenFlow build-in authentication module can be seamlessly integrated with ISPs' authentication schemes such as NTLM, LDAP, RADIUS or Local Database, enhancing the efficiency of ISPs' user account management.



■ **Mechanism of Quota system**

AscenFlow quota system manages quota in a 4-step process. Firstly, AscenFlow classifies the traffic based on source IP addresses or users. Next, it pre-assigns an amount of quota to the IP address (or user). After that, a database is used to associate the IP address with the quota consumed. Lastly, AscenFlow drops off the quota exceeded to effectively avoid network resource abuses.



■ **Workflow of Quota system**

The main four steps of AscenFlow Quota system are:

▫ **Classification**

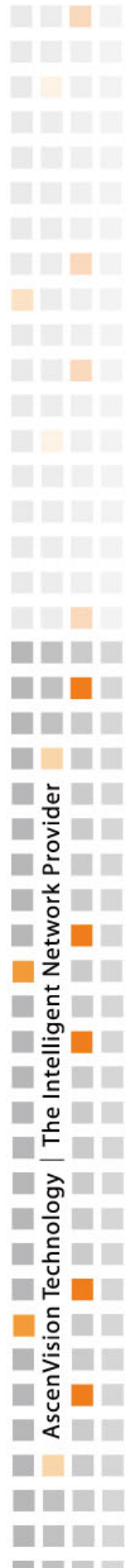
Classify the traffic based on the source IP address or the user and check whether the IP address (or user) is managed by the quota system. If the IP address matches with one of the policies, next action then takes effect. If not, AscenFlow will direct the traffic for bandwidth management.

▫ **Pre-assignment of Quota**

If the traffic flows in AscenFlow for the first time, it is pre-assigned with an amount of quota according to the policy setting in AscenFlow user interface. If not, this step is skipped.

▫ **Quota Management**

AscenFlow build-in database of quota management stores the data of quota consumed and quota left of every IP address (or user) according to the predefined either prepaid or periodic scheme. If there is quota left, AscenFlow allows the IP address (or user) to access the network and vice versa.



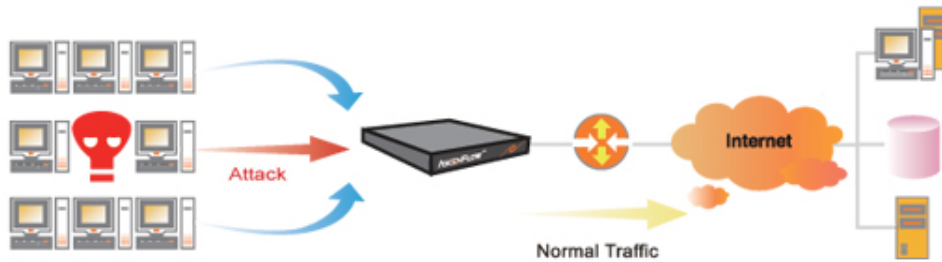
▫ **Discard**

When the traffic exceeds the pre-assigned quota, AscenFlow rejects the access and discards excess data packets.

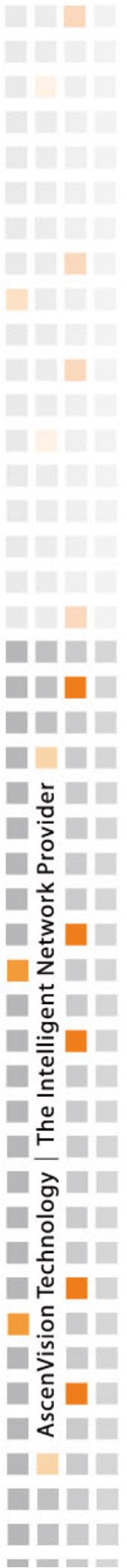
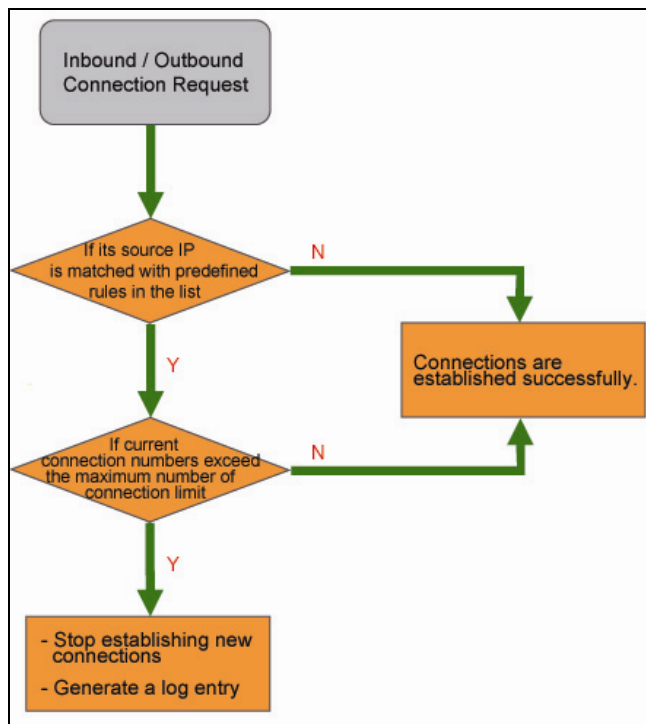
**Connection Limit and Network Attack Defense Module**

Connection Limit, also a unique function of AscenFlow, blocks subsequent connections due to either virus or network attacks to avoid excessive and fault connections originated from the infected machines, often times inside the Intranet. Connection Limit can be enforced 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/network attacks to a single PC in a LAN. The virus attacks that can be blocked include UDP Flood, SYN Flood, DDoS Flood and so on.



Furthermore, AscenLink Connection Limit function can manage inbound and outbound TCP, UDP, and ICMP traffic. Following figure illustrates how connection limit works.



Connection limit mechanism consists of two main processes:

- **Match Source Addresses with rules**

When the traffic either inbound or outbound, flows through, Connection Limit will automatically match the source IP address with predefined rules in the list to see if the IP of the connection is matched up. If the source IP of the traffic matches no rules in the list, AscenLink will allow the connection to be established successfully, and vice versa.

- **Check the maximum number of connections**

When the source IP address of the traffic matches the predefined rule in the list, Connection Limit will check whether the number of current connection from this IP address exceeds the maximum number of connection limit. If so, AscenLink will not allow the connection to be established so as to ensure network security and meanwhile generate a log entry. If not, AscenLink will allow the connection to be established successfully.

## User-friendly Management Interface

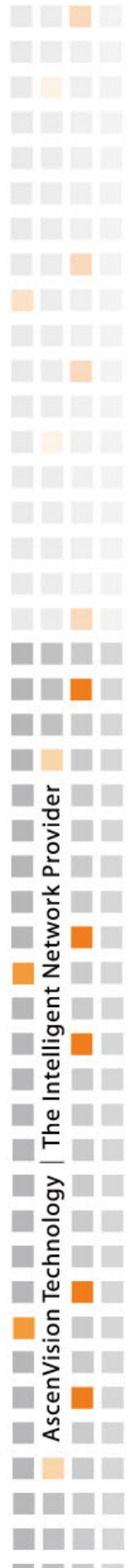
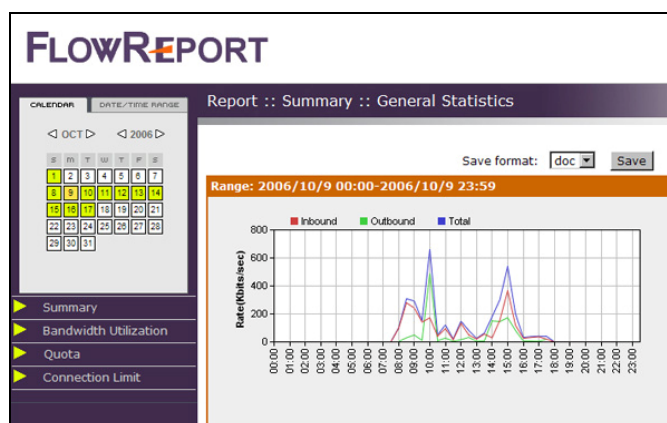
AscenFlow offers intuitive user interface helping MIS personnel easily and efficiently deploy and manage the network condition. It also supports multilingual user interfaces such as Traditional Chinese, Simplified Chinese, and English to accommodate diverse geographical users. In addition, the build-in authentication system can be seamlessly integrated with clients' user account management systems such as LDAP, NTLM, RADIUS, and so on to build a comprehensive billing system based on users' bandwidth usage.

## Comprehensive Traffic Control tool FlowReport

AscenFlow companion tool, FlowReport, provides comprehensive and multilingual 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.

In addition to it, FlowReport offers powerful functions as follows:

- Analyzing traffic pattern usage and detecting abnormal traffic which is helpful for network design and expansion
- Analyzing traffic on the basis of source, destination, service, and port to fully understand corporate network structure and bandwidth usage
- Querying IP and MAC addresses detected by AscenFlow and offering more user details
- Offering drill-down friendly charts based on traffic patterns to allow MIS personnel analyzing and enhancing network performance



## Case Study - AscenFlow in a district government IT center

AscenFlow are adoptable in many industry segments. The following case demonstrates how AscenFlow provides a district government with a highly reliable and cost-effective WAN traffic management solution.

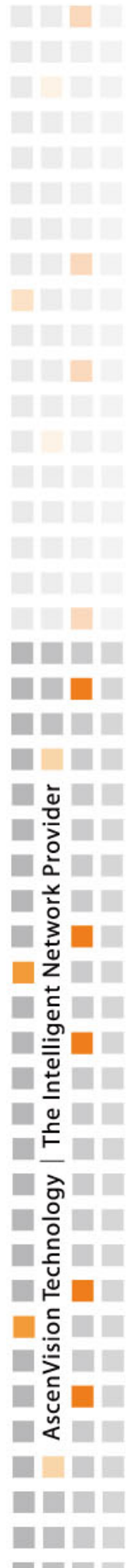
### Background

The district government is going to construct a digitized working environment to stimulate the development and utilization of district IT resources. It provides people with more convenient access to the government information and services to improve quality of services and offer more business opportunities. In addition, this digitized platform also supports the technical training of network security and technology, supervision and administration of network devices, and prevention of computer viruses.

### Challenge

Since the network topology of the district government IT center is extremely complicated and many mission-critical applications are dependent on the network, it requires high availability and reliability of the network to ensure application performance. Followings are the specific problems in the existing network:

- **Frequent network congestion**  
Non work-related applications consume significant amount of bandwidth leading to network congestion which is unacceptable to government to provide high-quality services.
- **Poor performance of critical applications**  
Lack of control and prioritization of network usage patterns results in poor performance of critical applications and services such as VPN data transfers, Web and Email services, online searching, online Survey and so on. It is imperative to understand how to reserve bandwidth to ensure performance of critical applications.
- **Bandwidth misuses due to P2P applications**  
The tremendous growth of using P2P applications brings significant impact on network performance. P2P applications contend for bandwidth with critical applications and consume as much bandwidth as possible. Containment and management of P2P applications, therefore, are imperative for network administrators to implement.
- **Ineffective control over Instant Messaging (IM) applications**  
Instant messaging applications bring us greater convenience in real-time communication with clients. Many employees, however, misuse it for chatting, file sharing, and so on which may cause poor productivity, risk of confidential data falling into the wrong hands, and other security issues. In order to ensure information security, it is requisite to control the use of IM applications.
- **Abnormal connections due to network attacks**  
A virus-infected PC in a LAN sends out a surge of false connection requests depleting network resources or even getting the network crashed. Network administrators, as a result, must figure out a way to prevent and defend against network attacks.
- **Misconception of network usage patterns due to lack of accurate traffic analysis**  
The digitized platform provides a variety of services and supports thousands of concurrent online users. How to easily identify and grab critical information, therefore, is another big challenge for MIS personnel.



## Why AscenFlow

After evaluating several traffic management devices other than AscenFlow, the government decided to choose AscenVision's AscenFlow as the WAN traffic management and QoS solution due to its high price/performance ratio, constant reliability, high level of security, powerful traffic management tools, and easy-to-use user interface. It proves that AscenFlow is an industry-leading WAN traffic management product and can be integrated into a very complicated network environment. AscenFlow can help the government achieve followings:

- Transparent mode allows AscenFlow to be integrated in to existing network topology without significant modification to existing configuration.
- Combination of software and hardware failure with bypass function enables AscenFlow to provide uninterrupted services in the event of hardware or software failure.
- Connection Limit enables to limit the number of connections based on a single IP address, an IP range or a subnet, offering more comprehensive administration of security.
- Offer an effective and visible control over IM and P2P applications to optimize the usage of network resources and enhance network performance.
- AscenFlow manages applications in Layer-7 which effectively ensures optimum bandwidth allocation and utilization.
- Highly cost-effective solution makes AscenFlow a competent product in its kind.

## Solution

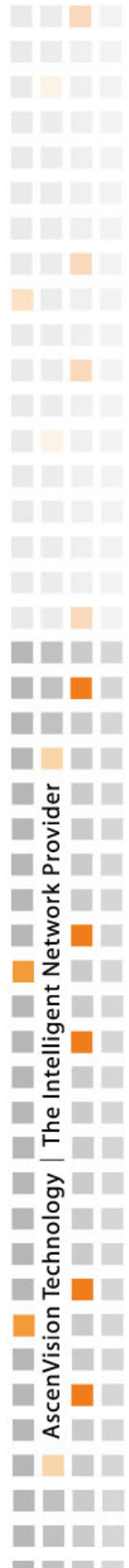
AscenFlow blocks P2P applications such as BitTorrent, eDonkey, eMule, Gnutella, and its variants by properly defining a set of rules to reserve valuable bandwidth for mission critical applications. The end result is that the government offers uninterrupted services such as Web, Mail services, online survey, and so on.

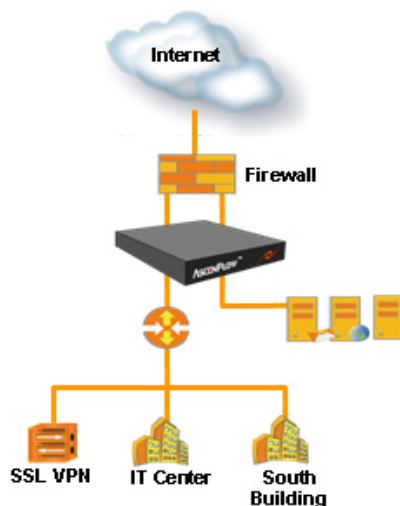
AscenFlow reserves sufficient amount of bandwidth for the government to transfer critical and confidential information over secure VPN tunnels accurately and in time. Mission critical applications therefore can function properly without any downtime and productivity is improved as well.

AscenFlow assigns limited amount of bandwidth to IM applications such as ICQ, MSN, Skype and so on to offload bandwidth consumption and prevents government officials from wasting time on non-business applications.

Connection limit function safeguards the network against virus/network attacks and avoids data loss and even worse damage. MIS personnel, as a result, is disburdened by getting virus or network attacks under control.

FlowReport, AscenFlow companion tool, offers comprehensive report and analysis for all major functions of AscenFlow helping network administrators easily and thoroughly understand and control the network status.





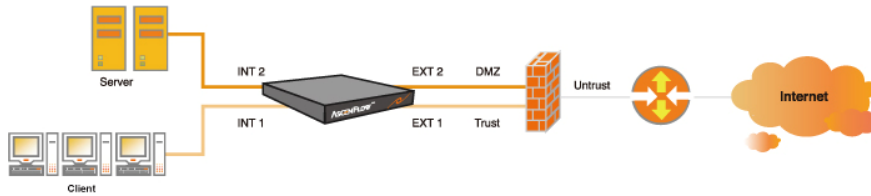
### Benefit

AscenFlow reserves sufficient bandwidth for VPN and critical applications to ensure accurate and on time data transfer and application performance. AscenFlow effectively curbs inbound traffic flows of P2P applications to avoid bandwidth misuses and ensure performance of critical applications.

AscenFlow ensures the government providing highly accessible outlets for interactive services to build up better government image. AscenFlow effective traffic management tools provide a cost-effective solution for government to improve quality of services, enhance productivity, and create more interactions with the civilian.

## Target Environments

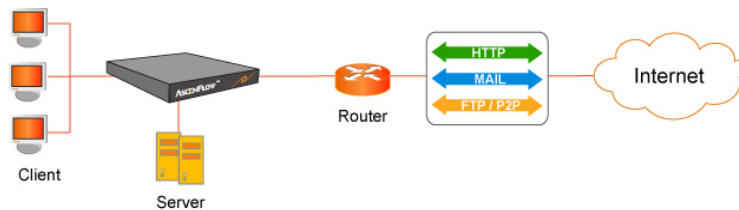
AscenFlow can be deployed in almost all types of network environments without significant changes to current configuration. In addition, its superior models yet offer LEM (LAN Expansion Module) which can be deployed in a network with a firewall and meanwhile can manage the inbound and outbound traffic of Trust and DMZ.



Followings are some typical network environments that AscenFlow is capable of:

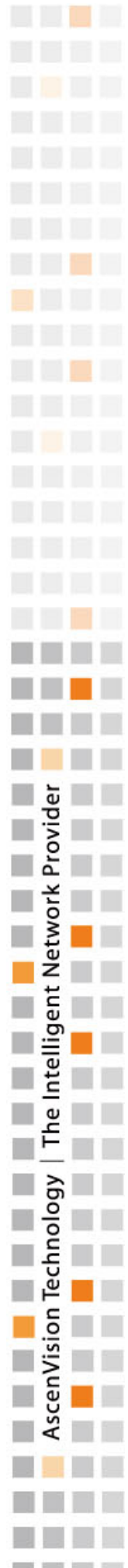
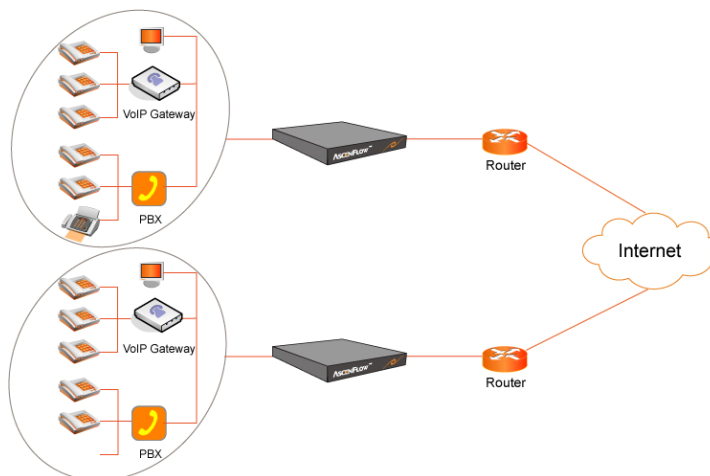
### Enterprise

AscenFlow can be configured to guarantee priority to mission-critical applications to enhance employees' productivity at the same time to prevent misuses of bandwidth resources. This enables network administrators to assign priority to mission-critical applications by guaranteeing the bandwidth while limiting non-business related traffic.



In addition, video conferencing is widely used in businesses today. Video conferencing is a real-time application which demands guaranteed bandwidth otherwise users will experience distorted video and choppy audio. Therefore, without an acceptable level of guaranteed bandwidth will negatively affect the meeting.

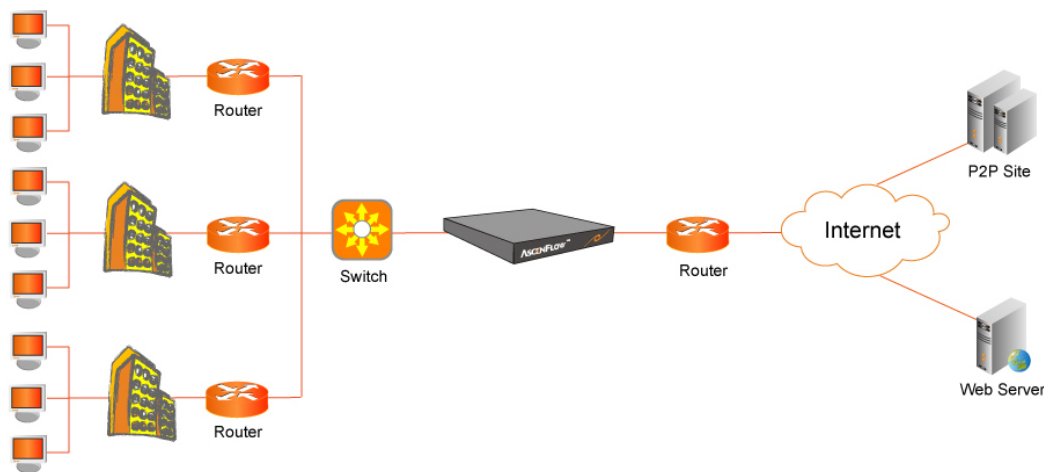
The solution is to install AscenFlow at each site and to define a policy to guarantee bandwidth for video conference applications and to prioritize video traffic over the internet. This will ensure the quality of video conferencing service.



## E-Community

With the growing popularity of Internet usage, creating a connected community and Internet friendly environment have been one of the main consideration criteria for real-estate developers. It is an important selling point for brokers or building developers to market real-estate as being broadband-friendly. However, with the increasing amount of Internet users resulted in degradation of performance, particular P2P download which unfortunately consumes most of the bandwidth. Since network administrator is not empowered to block P2P application usage, the only choice is to deploy AscenFlow by enforcing bandwidth quota for such applications. This is a win-win situation whereby P2P users can continue using P2P applications at the same time it provides a better quality of service and protect the interests of non-P2P applications users.

In addition, AscenFlow Quota service supports both “Prepaid” and “Periodic” mechanisms. Combined with its build-in authentication system, quota system enables more effective user account management and meanwhile provides a flexible billing system.



## E-Campus

A classic AscenFlow application to provide bandwidth management is in the E-Campus environment. Under peak hour traffic conditions, limited bandwidth resources become a bottleneck to serve educators and students needs.

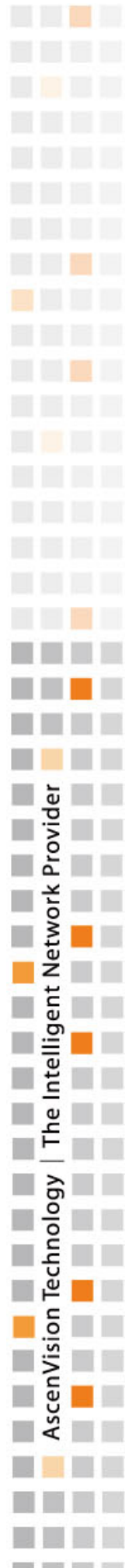
AscenFlow helps network administrators to analyze network traffic and allows policies to be defined in order to properly allocate reasonable bandwidth on a per IP address or user groups or application basis. Thus, without the need for bandwidth upgrade, educators are able to enjoy guaranteed bandwidth during lessons and students get a fair share of bandwidth for their applications.

AscenFlow powerful traffic analysis and management tools ensure the priority of educational applications to use the network resources; for example, sufficient bandwidth is reserved for e-learning video conferencing applications offering a low-latency and non-jitter e-learning environment.

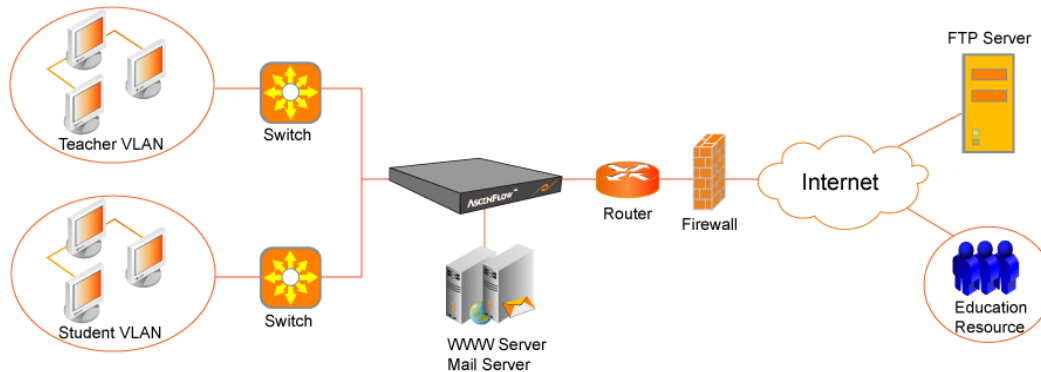
Furthermore, AscenFlow effectively manages and controls the use of P2P applications, Internet gaming, and other recreational applications. A good learning atmosphere, therefore, is created to prevent aspiring students from addiction.

Moreover, AscenFlow’s Quota system can define the amount of bandwidth by single IP or IP subnet so the bandwidth wouldn’t be misused.

If the Internet traffic still chocked after well management and accurate analysis, network administrators can



consider using load balancer such as AscenLink which has trunking technology to broaden the bandwidth.



## E-Government

E-government, a platform where people interacts with the government, demands reliable network to provide high quality of services thus to build up an image for sincerity and trust.

More and more critical applications of contemporary government institution heavily rely on the Internet such as VPN data transfers, Web and Email services, online searching, online Survey, and so on. The network reliability, therefore, is the key to ensure QoS. With AscenFlow comprehensive analysis of traffic usage patterns, network administrators can easily find out the reasons causing poor network performance and take corresponding corrective actions such as prioritizing critical applications to improve application performance and QoS.

AscenFlow offers an effective and visible control over P2P applications and other recreational applications to reserve and ensure sufficient bandwidth for critical applications such as VoIP, VPN, Video Conference, ERP, CRM, and so on.

In addition, AscenFlow assigns limited amount of bandwidth to IM applications such as ICQ, MSN, Skype and so on to ensure proper business-related communication, avoid bandwidth misuses, and provide partners and end-users with highly accessible outlets for uninterrupted services.

AscenFlow flexible policy-based traffic management mechanism improves productivity and optimizes bandwidth usage while saving cost on adding more WAN links.

## ISP (Internet Service Provider) and WISP (Wireless ISP)

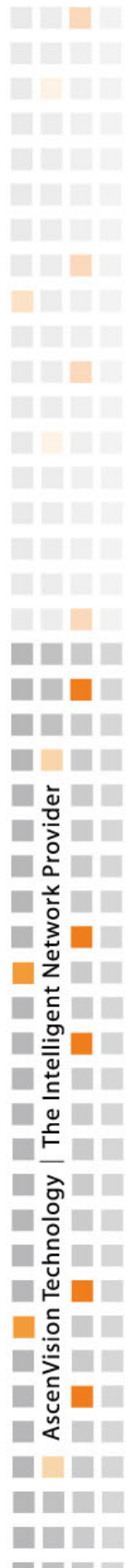
One of the most typical issues challenging ISP is to well-manage bandwidth resources in order to provide fast and reliable Internet access/connection to every subscriber.

AscenFlow's bandwidth distribution policy enables WAN bandwidth to be optimally distributed and to assign priority for each host to guarantee bandwidth. This will ensure a high quality Internet access/connection for subscribers.

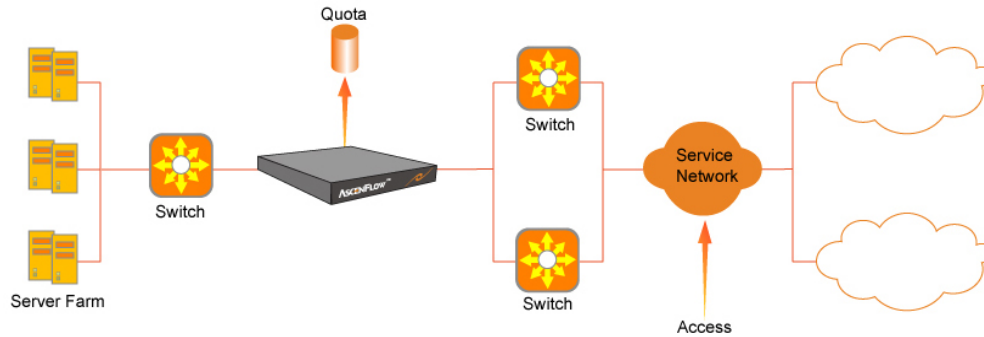
AscenFlow effectively controls P2P applications helping ISPs offload bandwidth consumption and ensure streamlining performance of critical applications.

The quota system of AscenFlow provides "Prepaid" and "Periodic" mechanisms on quota management. Combined with AscenFlow authentication system, ISPs can manage the user account and billing system flexibly.

With AscenFlow companion tool FlowReport, network administrators can establish a secure network environment, fully understand the network status and optimize bandwidth usage patterns while saving cost on network resources.



In order to ensure non-stop ISP services, network administrators can deploy WAN link load balancer such as AscenLink series to achieve absolute network availability, reliability, and fault tolerance.

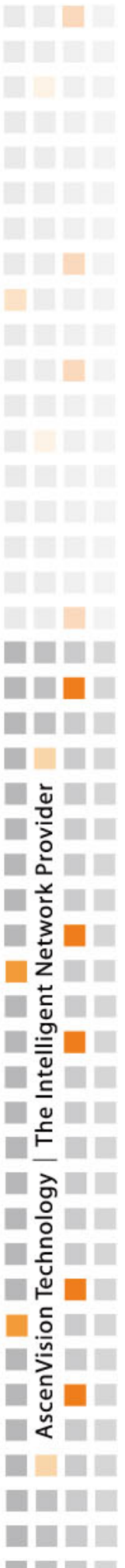


## IDC (Internet Data Center)

IDC offers its enterprise tenants with a variety of services such as Virtual Server, Internet domain name registration, Web hosting, Website design, Website promotion and so on. Since the number of clients is rapidly increasing, how to achieve efficient quota management and reasonable prioritization become main challenges to IDC.

AscenFlow powerful built-in authentication module, seamlessly integrated with numerous authentication systems such as Radius, LDAP, or Microsoft's NTLM, achieves proper user account management and ensures VIP clients' priority of using the network resources.

Combined with AscenFlow quota system, IDC is allowed to provide another billing system based on daily, weekly, or monthly quota consumed to satisfy requirements from different clients.



## Summary

AscenVision's versatile AscenFlow, the best choice for MIS personnel, offers an optimum and complete solution for identifying and analyzing, shaping (management), and reporting of network traffic flows in an organization. Its authentication and quota systems make AscenFlow a complete solution to various types of network environments instead of a pure traffic management device.

In addition to the core functions described above, AscenFlow's niche features listed below further strengthen its position as the choice for Layer 7 WAN traffic management solutions:

### ■ **Connection Limit**

Avoid network overload by limiting the number of subsequent connection requests allowed of each IP due to P2P applications. In addition, Connection Limit can also safeguard the network against virus or network attacks by impairing a surge of simultaneous connections from a virus-infected PC in the LAN. Going beyond the scope of QoS device, AscenFlow can act as a edge defense unit because of the Connection Limit function,

### ■ **Quota**

"Prepaid" and "Periodic" quota schemes can satisfy different clients and allow e-Community, ISPs, IDCs, and schools and colleges offering more flexible services and user account management. This unique feature further strengthens AscenFlow's position as a total traffic management solution.

### ■ **Authentication**

AscenFlow build-in authentication module supports various authentication mechanisms such as NTLM, LDAP, RADIUS, Local Database, and so on, allowing to manage bandwidth allocation on the basis of IP addresses or users. With integration to external directories, AscenFlow enable best policy-based traffic management according to real business needs, rather than the machine-dependent IPs, as seen in traditional QoS devices.

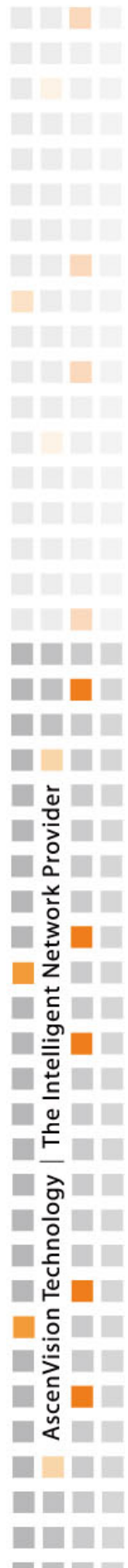
### ■ **FlowReport**

FlowReport, a comprehensive report and analysis tool, analyzes the large volume of log data generated by AscenFlow and generates short-term/long-term reports for MIS personnel to understand network status and accurately predict future network usage patterns.

## Benefit

AscenFlow benefits corporate network as follows:

- Avoid network congestion caused by misuses of bandwidth such as Http, email, P2P, IM and online shopping.
- Provide accurate network traffic analysis and reports to identify the possible causes and sources of network traffic congestion and predict potential congestion.
- Manage network resources to guarantee bandwidth for mission critical applications such as ERP, video conference, and VoIP to achieve an acceptable level of QoS.
- Avoid complex network design and enable easy-to-deploy and easy-to-use configuration to improve the network and application performance while saving cost of network resources.
- Display the bandwidth usage patterns, configure guaranteed bandwidth and maximum bandwidth, combine account management and give proper quota management, and limit the connection numbers of clients to meet the enterprises' needs.
- Government Institution: AscenFlow helps government institution gain effective control and management of network resources, enhancing the quality of services, improving interactions with



civilians, and building up better government image.

- ISP: The combination of AscenFlow build-in quota and authentication systems allows ISPs offering more flexible services and account management systems.
- Schools and Colleges: Effective containment and management on P2P applications and streaming applications offload network resource consumption, ensure performance of key educational applications, and prevent students from addiction to Internet gaming and other recreational applications.

