

Anagran Response to Technologies for Addressing Issues Associated with Unauthorized File Sharing on the University and College Campus

Joon Choi, Director of Product Management

joon@anagran.com

Anagran

June 2008

Introduction

Anagran produces a very high speed (2-48 Gbps) Flow Manager which is the world's leading system for monitoring and reporting all IP flows and for precisely controlling the rate of all IP flows. There are many important applications for the Anagran Flow Manager, but this response will focus on the possible uses in Universities and Colleges associated with controlling unauthorized file sharing. Anagran's Flow Manager is very different in design from other network equipment produced today since it does not examine the content of any packet as deep packet inspection (DPI) equipment does, nor does it route or queue every packet like a standard packet router. Both DPI and traditional queue-based packet routing require considerable processing capacity. Anagran keeps track of all the flow statistics for up to 4 million flows (sufficient for 40 Gbps of input capacity), measures the output load for thousands of traffic classes, and controls the rate of all the flows to meet many flexible criteria. Thus, a small 1 RU (1.75" high) rack mounted unit can both monitor and control 40 Gbps of traffic. Connected to an existing router port it can provide an output stream with complete NetFlow records of all traffic, or more usefully in this application, all the P2P traffic. When configured in-line, it can not only monitor the traffic but can also control the total rate per user (IP address) so that the capacity used by file sharing programs that spawn many flows can be controlled as desired. For example, one option is to control the total rate of all flows for every student so that all active users receive the same capacity. This allows P2P to be used for legal applications, but ensures that no single user can become a major distributor of any material unless white-listed. Also, all P2P usage can be limited to a maximum capacity if desired.

Anagran's Flow Manager passes packets through at line rate without introducing any significant delay or jitter. It also passes short gaming or interactive traffic at line rate even when the same user's P2P traffic is being metered. It is sufficiently small and economic to be used on any speed trunk from 100 Mbps to four 10 Gbps trunks. At the high end it becomes a very economic option to monitor and/or control traffic within the campus as well as at the external campus links.

Control of Unauthorized File Sharing

Unauthorized file sharing cannot be curbed today by trying to examine the content of the data stream since encryption can easily obscure the content. A recent French [EANTC test](#) has revealed that DPI systems detect only 66-77% of the P2P traffic. Moreover, even with 23% of the P2P programs remaining, each one spawns more flows as a result, and can still load the network to 90% or greater with P2P traffic (See Figure 1). This reduces

the average user's throughput to 10% of what it would be if the P2P users received the same capacity as other users.

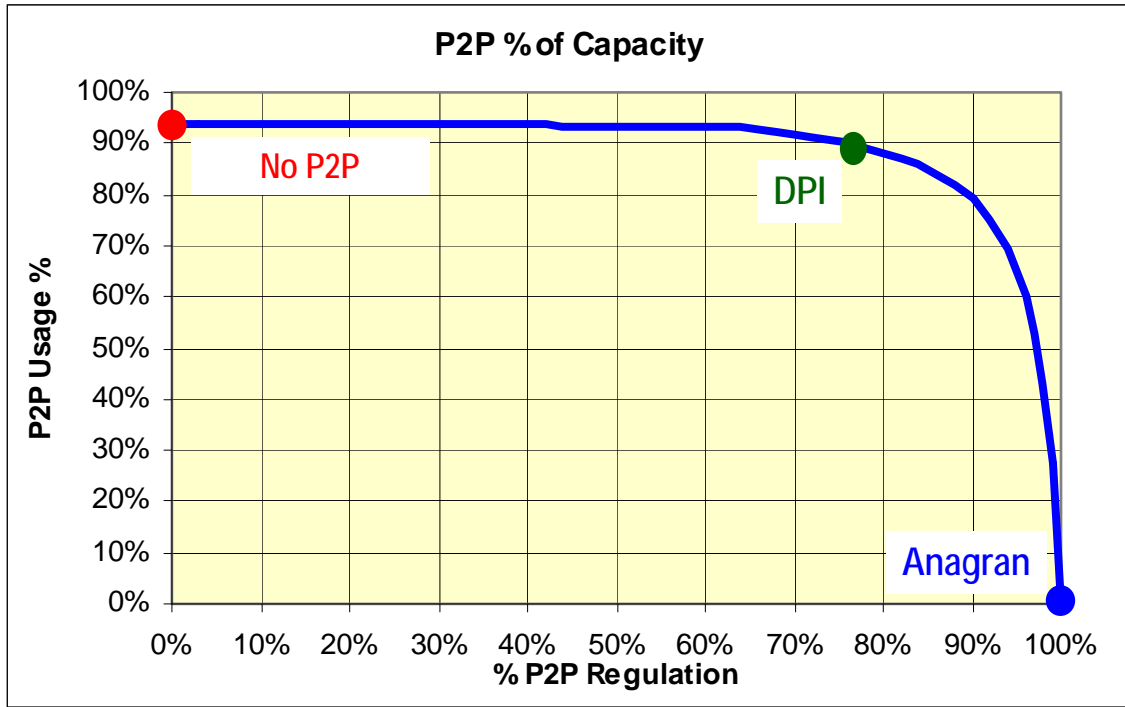


Figure 1: Impact if all P2P is not Rate Regulated

Widespread unauthorized file sharing on campus has a truly global negative impact. The larger Universities tend to have high Internet access bandwidth (1 Gbps-10 Gbps) with up to 90% being P2P traffic, even with DPI installed. If unauthorized file sharing is not tightly controlled here, the campus computers become a significant part of the problem. However, if tightly controlled so that the P2P users only receive limited capacity, Universities and Colleges will cease to be significant in terms of the worldwide problem. If, in addition, all P2P activity is monitored and recorded with NetFlow, the remaining users can be pinpointed if unauthorized file sharing is suspected.

Anagran's FR-1000

The Anagran Flow Manager is a very compact (1 RU) system with up to four front-loadable Interface Modules (IMs). Each IM supports 10 Gbps of traffic in each direction and has either one 10 Gbps Ethernet port or 12 10/100/1000 Mbps Ethernet ports. The system is non-blocking and can support 4,000,000 flows and 40 Gbps of traffic in and out.



Anagran FR-1000

The FR-1000 keeps information about every active flow (file transfer, voice call, video, etc.) including its start time, duration, bytes transferred, packets transferred, plus the source and destination address, ports, and protocol. This information allows the reporting, using NetFlow protocol, of all this information about every flow or selected flows. This is much more complete information than is typically received from routers since they are *complete* flow records, not sample packets. When configured to send only flows from users whose traffic profile pinpoints them to be P2P users, the NetFlow information precisely identifies the P2P transfers without invading the user's privacy.

If utilized in-line, the FR-1000 controls the rate or acceptance of every flow to ensure the peak output rate for a port or VLAN is less than a configured rate maximum, thereby ensuring that there is only very minor queuing at the output and thus microseconds of delay. Each flow can be weighted so that different classes of traffic receive different fractions of the overall capacity. In addition to measuring all output ports, VLANs, and classes, the traffic and flows from each address (user) are measured. This per-user information allows quick and precise identification of heavy users, typically those using P2P programs or running busy servers. When used to manage multi-flow file sharing and other overly aggressive use of the capacity, the rate of flows from heavy users can be adjusted so as to reduce or eliminate the inequity.

Features of the Technology

Audit Tools

Anagran does not supply audit tools.

Bandwidth Shaping

The Anagran FR-1000 features the world's most advanced bandwidth shaping. It can precisely control any TCP flow to any given rate. For fixed-rate flows like voice and video, the flow is accepted if there is sufficient capacity remaining and then protected to ensure no loss or delay as long as the flow does not exceed its allocated peak rate. Flows can be put into a class based on ACL commands which considers the standard address, port, protocol and DSCP information. This includes the ability to white-list addresses so that their flows will not be bandwidth shaped. Flows can also be put into classes such as "bulk" if their byte count, duration, or packet size exceeds specified limits. For example, bulk traffic can be given lower priority than interactive traffic, so that the bulk slows down as interactive peaks, and speeds up during slack periods. Flows can also be assigned a weight or priority based on their class or the heavy user classification. This allows P2P users to be weighted so that their total traffic receives either limited capacity or capacity equal to other users. If a P2P user is also using a white-listed server or is doing short-transaction gaming, these flows need not be slowed down. Thus, a student's normal work will not suffer as does his P2P traffic. The rules for uploading and downloading can be different. Configuration is typically done just once since there is no need for periodic signature updates. The importance of flow and user behaviour

measurement is that they allow near perfect P2P user identification, independent of encryption and signature changes.

Data File Sharing Blocking

The measurement of the per-user flow count and traffic has already been described. Along with the ACL specification of white-listed addresses, there is the ability to black-list a user address based on DMCA notices or prior history. This will place the user in the P2P user class, but if they operate normally, they should see no difference. However, they *could* be blocked generating or receiving certain types of flows. Flows can be totally blocked if desired, but the usual practice would be to carefully slow down P2P flows or excessively large streaming flows if the user's total traffic is greater than average. These capabilities provide 100% control of P2P usage. Student servers can look like P2P and thus to permit heavy server activity by students, it is possible to white-list those registered server users. Even then, NetFlow records of their activity can be generated for later inspection and audit.

Matching, Screening and Filtering

The Anagran FR-1000 does not look into packet content so that matching a stored database is not possible. However, anything in the packet header can be matched with ACL commands and thereby classified for reporting, blocking, or shaping. Further, the behaviour of a flow (duration, byte count, etc) can be useful to additionally identify file transfers.

User Management and Communication

The Anagran FR-1000 does not communicate with the user.

Network Performance

The Anagran FR-1000, either in monitor mode or in-line flow management mode, can provide any specified subset, or all, of the flow records for every flow. These NetFlow records include the packet header information (addresses, port, and protocol) plus the byte count, start time, and duration of the flow. Selection can be based on many variables. All of a class can be reported or just a fraction of the flow records in a class. The class might be those users classified as P2P users or just the larger flows of such users. Given that this reporting is of the entire flow and potentially all the flows, there is no risk of missing any unauthorized file sharing flow. The Netflow stream can be securely tied to a server which is using any standard NetFlow collector. Anagran does not sell NetFlow collector programs but one is made available for trial and inexpensive purchase if desired. The procurement and operation of the NetFlow server is best kept under the responsibility of the College or University.

In addition to NetFlow data, Anagran's FR-1000 provides a GUI which is driven from the FR-1000 to any browser. This allows configuration, alarms, and the cumulative traffic level of each class of data. One output from this would be the total P2P traffic level.

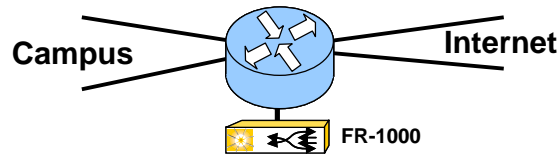
Network Architecture

At the Internet Access Interface

To monitor or control the incoming and outgoing traffic, the FR-1000 can be installed adjacent to the final router from which the Internet trunk(s) are connected. There are several options depending on the speeds and the preference of the school. If there are several Internet feeds they should all be managed by one FR-1000 system so all the P2P flows from a user appear in one system. The FR-1000 can manage traffic for several different feeds in one system.

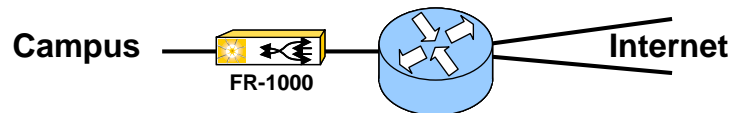
FR-1000 on a Router Port

This configuration is generally desirable when the total traffic is less than 1 Gbps. For monitoring, the router mirrors all the Internet traffic to the FR-1000. For in-line bandwidth control, the router policy-routes all the incoming and outgoing traffic to a 1 Gbps port which connects to the FR-1000. The FR-1000 processes all the traffic, and returns the shaped traffic to the router. The router then sends it where it should go. If the FR-1000 should fail for any reason, the router can either send the traffic to a second FR-1000, or if redundancy is not desired, forward the traffic.



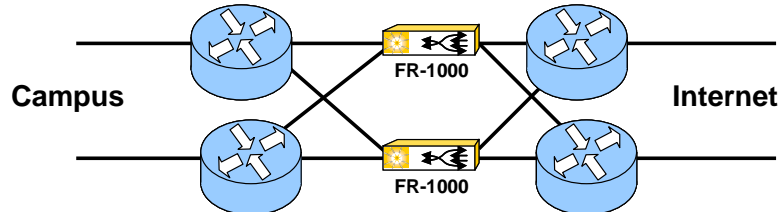
FR-1000 In-line as a Bump-in-the-Wire

A FR-1000's can be connected in-line just before the final router as a bump-in-the-wire.



FR-1000 Routed In-line

The FR-1000 incorporates full L3 routing and thus two systems can be connected in the standard criss-cross configuration. This provides full redundancy.

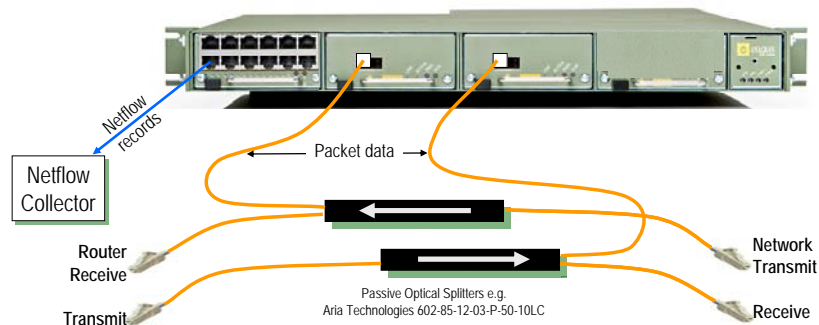


Inside Campus at 10 Gbps

Typically the LAN links around the campus are 10 Gbps and here it is possible to use the FR-1000 as a bump-in-the-wire, or as a router. They can be duplexed or not. Due to the high cost of typical router ports at 10 Gbps and the much lower cost of the FR-1000 10 Gbps ports, it is usually not desirable to add extra ports as would occur if they were connected to a router stub port.

Inside Campus Monitoring at 10 Gbps

To monitor at 10 Gbps and produce a NetFlow stream with all the P2P transfers, the FR-1000 can be easily connected using fiber splitters which duplicate the data stream. This adds no extra ports. If full redundancy is required, the same setup can be duplicated.



Scalability

Each FR-1000 supports up to 48 GE ports or four 10 GE ports. This is typically sufficient for one system but given the nature of this task, multiple systems can be used, each for a segment of the campus. The important configuration issue is that all traffic from one user comes through one system so all flows can be measured.

Protocol Identification

P2P protocols are not identified, nor is that necessary. Standard network protocols like HTTP are identified using ACL commands as described before from the addresses, ports, and protocol. Since the identification of P2P traffic does not depend on signature or protocol identification, no updates are required.

Granularity of protocols

Since flows can be classified by their duration or byte count, it is easy to separate the control and searching from the file data transfers.

Product Configuration and Installation

To install the system requires only a moment of outage to connect it in-line. For monitoring, there is no downtime; it can just be connected to a stub port. Installation will require the configuration of school-specific parameters, white-list addresses, and perhaps local address configuration. The time to do this depends on the situation but except for

the white-list, our experience is perhaps 30 minutes per system. There is no need for per-user configuration.

Content Identification

Anagran does not pry into user's content. This is a potentially serious privacy invasion and is not necessary to identify the P2P users or P2P flows.

Examination of network packets or file content

Anagran does not examine packet content beyond the header.

Distribution Systems

Since the identification of P2P users and flows is not dependent on identifying the protocol, there are no protocols that are normally identified. The NetFlow packets contain the addresses and ports. NetFlow collectors do recognize many addresses and protocols from this and to this extent, looking at the exported NetFlow records of P2P users provides considerable information on the type and distribution of their activity.

Resilience of the technology to countermeasures

There are no effective countermeasures to hide P2P activity at the user level. A user with multiple flows and high traffic levels, day-in and day-out is a P2P user, or if not, it is abusing the network just like a P2P user and may well be receiving and sending unauthorized files. Encryption, compression, fragmentation, tunneling, and proxy servers cannot hide the total traffic required.

Testing and Installed Base

The FR-1000 has been installed in various Universities and Government installations for over a year and has been working properly and is very stable. More recently, user measurement and P2P user recognition have been added, and have been tested in a few locations including one University. More installations will follow shortly. Experience shows the system to be very stable. The system is currently available.

Competitive Approach

The Anagran system takes a different approach from DPI systems. Based on processing flows rather than analyzing packets, it is 5-10 times lower power, size, and cost than DPI systems. However, due to the approach of examining all the flows and every user's activity, P2P users can be identified with near 100% accuracy and thus their P2P flows can be identified. Anagran has pioneered a new technology for flow rate management which allows precise rate control of any flow without the stalls and rate variations that result from ACK discard or random packet discards. Priority per flow is a standard feature, thus setting a new priority based on P2P user identification is straightforward. Further, due to the 40 Gbps throughput of the system, it can observe all the traffic on a multi Gbps trunk or trunks. Thus much larger organizations can be supported including those with 10 Gbps trunks. Finally, the ability to export complete flow records with NetFlow has never been achieved in a multi-Gbps system before.

Third Party Components

As mentioned, the NetFlow collector or a server to run it on is not sold by Anagran. However, a NetFlow collector is provided for trial and purchase if desired.

Comparison with Hypothetical Scenario

The solution outlined in the CSDS170 report is somewhat more perfect than can be achieved today. However, the Anagran FR-1000's inside the campus and at the gateways could report all P2P users and flows with NetFlow to a secure server. The recognition of a particular flow as an infringing file requires both an invasion into the user's privacy and an improbable up-to-the-second knowledge of all copyrighted material. But, given a complaint which identifies a time and destination, the corresponding flow can be found in the NetFlow database. This will identify the internal user address. This information could then be transferred to the campus judicial system.

Performance with respect to the Requirements Described in the 2007 Workshop Report

Identifying Infringing Traffic at the Campus Border

False positives when using the analysis of user behavior are extremely rare, so long as one is concerned with identifying P2P users. If a user is a P2P user his P2P flows will be recorded by NetFlow and later correlation with complaints will identify infringements. In this area false positives of legitimate P2P use is unimportant since there will be no complaints. When used in-line to reduce the impact of P2P on the network (and reduce its use) any user identified as a P2P user will have large flows slowed down unless the other address is white-listed. The only user activity that looks like P2P activity is server operation. Students permitted to run servers should be white-listed if the traffic and usage is approved. However, if the traffic is substantial (as we do see in many campus servers) such a server operation should be considered similar to and potentially equivalent to P2P as a source of potential infringement complaints. Thus, large flows to and from servers should also be recorded by NetFlow, even if the user is not slowed down. Outside of P2P and servers, false positives would require a user to be operating many flows at once with significant traffic, day and night. Thus, there cannot be false positives for individual FTP flows or other normal traffic.

False negatives today are the main problem since current DPI systems do not recognize all P2P and the remaining P2P will take over the unused capacity. The result is there are many documents moving that are not noticed and the network capacity is still saturated. The FR-1000 does not depend on signature recognition but rather looks for users with P2P activity patterns. One cannot move much traffic and not trigger this detection. Thus, the only false negatives that can occur are for P2P systems that reduce their traffic and flows sufficiently to look like a normal user. At this point they are not a significant threat for infringement and certainly not for network overload.

All critical traffic such as network control, routing protocol, and traffic for white-listed campus servers will not be slowed down under any circumstances. The Anagran system

has no delay or delay jitter, since packets are just streamed through without any output buffer queuing.

Upgrading the FR-1000 is as simple as plugging in additional interface modules until the 40 Gbps limit is reached. At that point additional systems would need to be installed, and each system connected to a segment of the campus.

Identifying Infringing Traffic Local to the Campus Network

To support monitoring a campus network, one system can be used to monitor many 1 Gbps points in the network and a few 10 Gbps points. For more distributed or larger networks, the systems should be distributed around the campus to examine all traffic as it enters the backbone. The NetFlow reports can be sent back through the network to a central server. The FR-1000 is perhaps the only system that can economically support a 10 Gbps campus network. For in-line control within the campus, the considerations are identical if internal rate control is desired.

Configuration of Local Campus Networks

The typical configuration for using the FR-1000 in the local campus network would either be inserting an FR-1000 into a 10 GE trunk using the bump in the wire concept or for full redundancy to use dual FR-1000 systems connected as routers in a typical criss-cross configuration. Also, since there are multiple ports, the FR-1000's can be used like any router.

Supporting the Campus Judicial System

All systems distributed around the campus can send their NetFlow data back to a secure server for logging. The NetFlow communication is by secure login.

Avoiding Disruption of All Non-infringing Traffic.

Given the recommended configuration, no traffic is blocked, and only the P2P flows are slowed down. Traffic can be blocked if there is an infringement but it would not affect traffic to white listed servers or any network control traffic.

Considerations for Purchase and Operations

When monitoring only, there is no impact on any data flow. When controlling the P2P traffic, the operation is totally predictable, transparent, can be totally audited, and is scalable to any scale. Pricing is simple and predictable. Each component, base unit or IM has a standard purchase price and yearly support price.

Intellectual Property

Although many patents have been applied for, none have been issued yet.

Corporate Characteristics and Resources

Anagran was founded by Lawrence Roberts who designed and built the original Internet, the ARPANET. Since then he has designed and sold many different switches, routers, and network equipment. Anagran was started in 2004 and has shipped systems since

early 2007. Features have been added each quarter. There are about 50 systems sold and installed throughout the world.

Pilot Testing

The system can be installed and tested with a try-and-buy arrangement. Assuming the system performs as specified, the customer is expected to complete the purchase after two weeks of testing. Additional modules or systems can be added at any time.

Commercial Terms

The FR-1000 requires modest yearly support payments for software updates and warranty.



ANAGRAN

Eliminating the TCP Traffic Jam

Company: Anagran, Inc.
2055 Woodside Road
Redwood City, CA 94061 U.S.A.

Phone: (650) 298-9029

URL: www.anagran.com

Key Executives:

CEO Kim Niederman
Founder and Chairman Dr. Larry Roberts
Complete Executive List Visit our Website

Overview

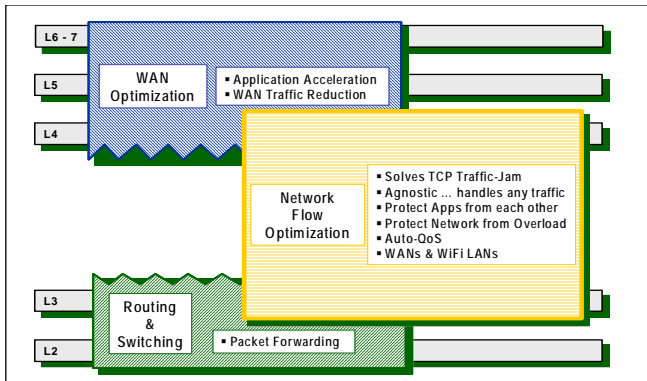
Anagran, founded in 2004 by Internet pioneer Dr. Larry Roberts, has developed a new class of *flow management appliances* based on its patented **Fast Flow Technology™** (FFT) that enable all traffic types – known or unknown, planned or unplanned, scheduled or ad-hoc, to cost-effectively co-exist with required performance and quality for all network users.

Today's Challenge ... The TCP Traffic Jam: A state of crisis is looming within today's TCP/IP networks. Traffic has changed ... capacity-hungry, 'greedy' applications like streaming video, P2P, gaming and video-on-demand are consuming a greater share of the network every day. No product available today adequately manages this unpredictable, ad-hoc mix of traffic that chokes bandwidth, adds delay and damages the user experience. This "TCP traffic jam" is occurring for two primary reasons:

1. A new generation of capacity-hungry, unpredictable traffic is placing increasing demands on networks that were never designed to carry such traffic
2. The universal feeling of **entitlement** shared by network users who run any application anywhere at any time, with no concern or consequence for their actions

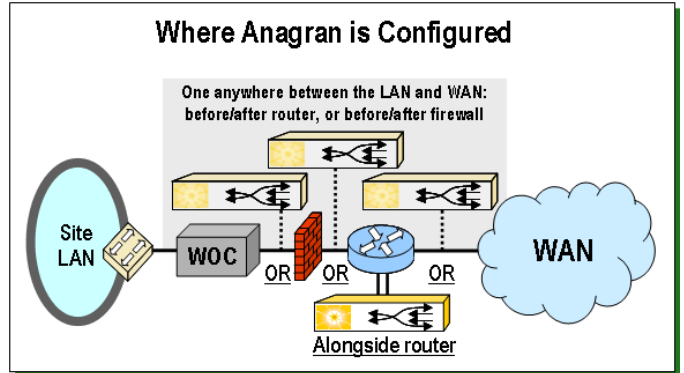
TCP traffic naturally consumes as much network capacity as possible, causing applications to "collide" and impact each other. The end result is slow interactive response times, dropped VoIP calls, jittery video, inconsistent web response, wasted network capacity, and costly network over-provisioning.

New Products for Today's Networks: Anagran offers a family of flow management appliances built from the ground up to eliminate the TCP traffic jam by filling the performance and quality gap that currently exists between L2/L3 routers and WAN optimization controllers (WOCs) that operate at L4 – L7.



A *flow* is an end-to-end activity over the network, such as a file transfer, a video download, or a voice call. Operating primarily at Layers 3 and 4 of the OSI networking stack, Anagran's **Fast Flow Technology™** protects networks from overload and applications from each other to instantly improve the performance, quality, and effective capacity of any IP network.

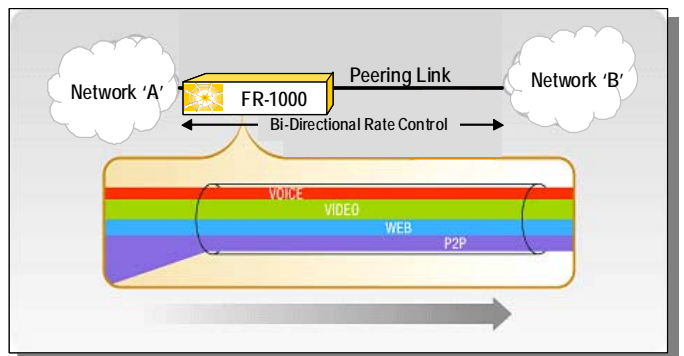
Where Anagran Fits in the Network: Anagran's FR-1000 is easily inserted next to an edge or aggregation router, wherever applications contend for a finite amount of network capacity. Since it is application, protocol, and format agnostic, one may be inserted on either side of the router, and also on either side of a firewall if one exists. Consider the following graphic.



Ultra-high Performance & Capacity: Anagran's flagship product is the FR-1000 Network Flow Manager. The FR-1000 is a 1RU platform with the capability to scale from less than 10Mbps to 48Gbps throughput, and handle up to 4,000,000 simultaneous flows and up to 4,000 classes. Since the product manages flows in both directions, a second FR-1000 is not needed at the other end of the WAN.



Leveraging the power of FFT, the FR-1000 instantly analyzes and intelligently rate-shapes *every flow*, to govern and protect applications from each other. By grouping all similar traffic types (e.g., voice, video, interactive, bulk), Anagran creates "virtual pipes within a pipe" that dynamically adapt to available capacity to keep different traffic types virtually separate, and unable to interfere with each other. **For the first time, voice, video, and data work perfectly together over WiFi!**



The Value of Managing Flows: Simply adding Anagran instantly benefits any IP network in the following key areas ...

- **Bi-Directional Traffic Management:** With the growth of Metro Ethernet, along with the challenge to deliver quality voice and video over WiFi, popular optimization techniques only address part of the problem. FFT is the first and only cost-effective way to optimize today's high-volume traffic mix over the WAN and WiFi LAN, in both directions, **without requiring equipment at both ends of the network.**
- **Virtual Bandwidth Allocation (VBA):** Creates dynamic "virtual pipes" allowing each type of traffic to flow separately and freely without impacting other traffic; eliminates performance limitations caused by application contention.
- **Dynamic Rate Control:** Dynamic rate control protects and controls up to 2000 local **or remote links**, requiring just a single device to fine-tune the overall maximum rate of traffic destined to any location in your network.
- **Application Protection:** Guaranteed quality for critical applications, always, regardless of how busy the network – even over WiFi networks. **For the first time, video, voice, and data applications can provide pristine quality over WiFi, regardless of the traffic mix or volume!**
- **Transport Network Optimization:** Instantly makes the transport network, routers, and WAN Optimization Controllers (WOCs) more efficient by increasing WAN and WiFi link utilization levels by **up to 10X with zero added delay**, to ensure consistent real-time application quality.

Application, protocol, and format agnostic, Anagran's products protect and govern key real-time, delay-sensitive streaming and interactive applications including all UDP, compressed, and encrypted traffic, which continue to consume more of the overall network capacity.

"The QoS Problem" SOLVED: Traditional methods of addressing Quality of Service (QoS) such as Deep Packet Inspection (DPI) were developed years ago to address data-specific applications such as web browsing, e-mail, and file transfer. These products attempt to identify traffic by class or application by inspecting the initial contents of every packet, and based on what is "seen", either

- allow that packet to continue
- add delay, then continue after other higher-priority traffic
- get blocked

Unfortunately, data "signatures" used to identify specific traffic constantly change, making it very difficult to stay current. Also, processing-intensive DPI products face extreme scalability and cost challenges when confronted with current-day streaming, compressed, and encrypted network traffic that can exceed gigabit speeds. In contrast, Anagran's FFT is **behavioral-based** and does NOT inspect packet contents. Rather, it closely watches flow **behavior** at wire-rate speeds up to 10Gbps, and then proactively meters select flows, with zero added delay, if necessary. This real-time behavioral flow awareness allows the FR-1000 to ensure perfect voice, video and interactive traffic quality all the time, while easily scaling to speeds that far surpass the capabilities of DPI technology.

The Perfect Complement to Routers and WOCs: Adding Anagran to an existing network makes the network resilient to sudden traffic surges and complements existing infrastructure.

- **Routers become more effective,** since they are protected from overload and unaffected by traffic surges
- **WOCs become more effective,** since the underlying transport network is now free to carry a greater mix of traffic in higher volumes with much less network-induced delay, and with application contention mitigated
- **WiFi LANs become more effective,** since for the first time, voice and video enjoy perfect quality all the time

By instantly reducing transmission, capital and operational costs, Anagran delivers a typical ROI 'breakeven' within six (6) months!

Summary

Anagran's patented, bi-directional **Fast Flow Technology™ eliminates the TCP traffic jam** to deliver applications with the highest levels of performance, economy, and fairness, ranging from speeds of under 10Mbps to over 40Gbps and beyond. By managing flows, Anagran flow management appliances represent a new class of product that complements existing networks to enable all applications, regardless of volume, protocol, or format, to cost-effectively flourish on a truly converged IP network. The next wave of rich, diverse, and dynamic network applications and services is now limited only by the imaginations of developers and users!

Common Applications ...

- Bi-Directional Rate Control:
- Dynamic QoS:
- WiFi Network Convergence:
- Video HD & Telepresence:
- Minimize MPLS Services:
- Complement Routing & WOCs:
- Network Consolidation:
- Replication and Synchronization:
- WAN Optimization:
- Standby Backup Links:

Common Markets ...

- Enterprise:
- Education & Research:
- Finance:
- Government:
- Video and Surveillance:
- Healthcare:
- Tier 2/3 Service Providers:

Benefit(s) / Advantages

controls trunk speeds, save \$\$\$ on Internet access, prevent overage charges
 "set it and forget it", no more 'tuning', automatically adjusts real-time to state of network
 enable HD Video, VoIP and Data to run with perfect quality on WiFi
 eliminate separate networks, additional hardware, or bandwidth purchases
 use metro Ethernet or low-cost leased lines instead
 eliminate need for over-provisioning, protect routers and WOCs from overload
 Voice, Video, Data, CRM, bulk traffic etc. on a single converged network
 real-time storage replication / synchronization without impact on other traffic, any time of day
 recapture up to 50% more WAN capacity by improving utilization to a sustained 90%+
 reduce expenses for WAN backup links and leverage them during normal WAN operations

Benefit(s) / Advantages

optimizes routers and WOCs, eliminates network congestion and bottlenecks
 manages P2P, enables high-quality video distance learning and long-distance collaboration
 reduces transaction latency and increases transaction speeds; protects VoIP
 resolves general congestion, enables real-time backups
 high quality streaming, storage and backup requirements
 enable HD Telemedicine and real-time access to huge files e.g. X-rays
 enables cost-effective, efficient delivery of quad-play services

