



Application Brief: The “P2P-Resistant” University and College Network – Ensuring Application Quality and Performance in the Face of Growing P2P Traffic

Premise: Anagran’s Fast Flow Technology™ manages all P2P traffic to ensure perfect-quality VoIP, HD video, and data under all traffic conditions, even over WiFi.

Challenge: Growing volumes of P2P traffic harm the quality of voice, data, and SD/HD video applications. DPI devices cannot find and manage all P2P.

Solution: Anagran is the first vendor to solve the P2P traffic problem in a truly network-neutral manner, without requiring invasive deep packet inspection, for perfect quality voice, video, and data on any college campus, even over WiFi.

Many universities and colleges are facing a dilemma which threatens their ability to provide a quality interactive learning experience for their students, as well as their ability to maintain their key administrative functions. The problem is obvious and pervasive – their networks are being over-run with peer-to-peer (“P2P”) file sharing traffic. Often “disguised” via encryption or other means, P2P is notorious for consuming as much network capacity as possible, often to the detriment of key applications like SD/HD teleconferencing, interactive collaboration, VoIP, distance learning, and even basic Internet access. Left unmanaged, a single P2P user can wreak havoc on a multitude of others within dorms, in class rooms, in the administrative offices, or “distance learning” from a remote campus or over the Internet.

University networks are typically comprised of two primary, distinct environments, each of which with its own IT/networking needs:

- Learning & Administrative: Lecture halls, administrative offices (admissions, ops, etc.), libraries, research labs
- Housing: Student dormitories and off-campus residences

While the class rooms and administrative offices often run critical, delay sensitive applications over the campus network, by far the greatest volume of network traffic originates and terminates within student housing, especially on-campus residence halls. These buildings have a high concentration of students, all of whom have campus network and Internet access over high-speed wired or WiFi interfaces. Armed with the means to download and distribute massive amounts of shared music, video, and image files via P2P at any time, that is just what many college students are doing. And it only takes a very small percentage of the student population to generate enough P2P traffic to impede the quality and performance of educational and administrative applications within the dorms and across the campus.

In response to this persistent invasion of P2P traffic, some universities and colleges have deployed deep packet inspection (DPI) technology to first identify any of the various flavors of P2P traffic along with those users consuming the bulk of it, and then

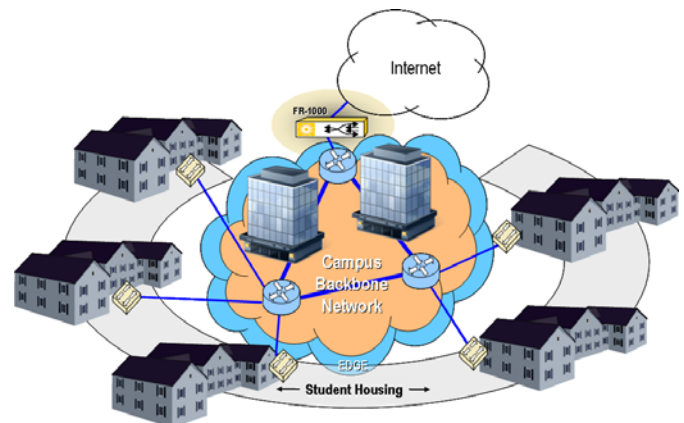
mitigating the impact of P2P by invoking policies to either reduce the P2P traffic or stop it altogether. DPI, as the name implies, looks deep into user packet content in an attempt to find a telltale byte sequence called a “signature” that uniquely identifies that packet as part of a P2P flow. Unfortunately for universities and colleges, DPI has proven inadequate in limiting P2P because:

1. Signatures used to ID various P2P-based applications constantly change in order to disguise P2P traffic. Staying current with these dynamic signatures is impossible.
2. Most P2P traffic is now being encrypted at the source to thwart any attempts to identify it, accurate signature or not. DPI is useless when traffic of any kind is encrypted.
3. Since DPI looks inside the user content portion of traffic flows, it opens the door to user privacy invasion complaints
4. Growing traffic volumes and faster link speeds make DPI less realistic as a traffic management tool in general; since DPI is extremely processing-intensive and does not economically scale beyond speeds of a few hundred megabits per second.

The Answer: High-Capacity Behavioral Traffic Management

Fortunately for networks suffering from unrelenting P2P traffic, Anagran offers the FR-1000 high capacity flow manager, the first product designed from the ground up to effectively manage all network traffic including P2P, encrypted or not, at speeds from less than 10 Mbps to **up to 10 Gbps** in an extremely economical 1RU form factor. And it poses zero threat of user privacy invasion.

Usually located next to the campus Internet aggregation router, the FR-1000 precisely manages the rate of every flow to and from the campus network and the building routers or wireless access points distributed throughout the university campus.

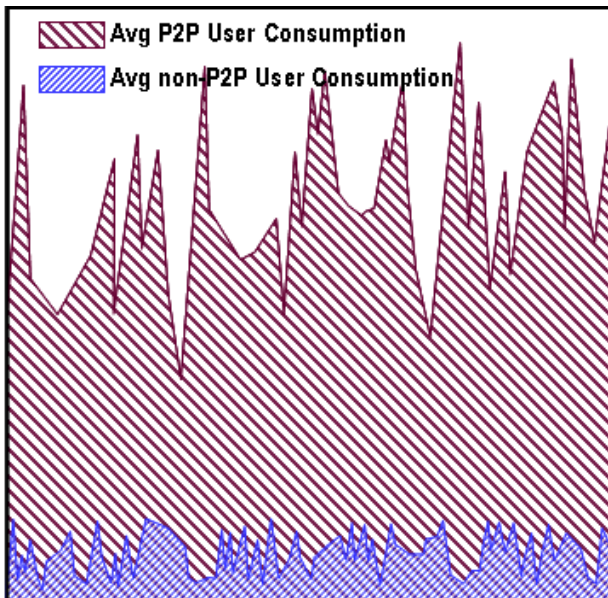


By precisely managing the rate of each flow, the FR-1000 instantly determines which users consume the most network capacity by correlating the amount of traffic and the number of flows to or from each user over any given time period. All P2P traffic consuming the vast majority of network resources is immediately managed in spite of any efforts to masquerade via encryption, port hopping, or any other means by which clever programmers try to disguise it. For the first time, universities and colleges can “P2P proof” their network by simply adding FR-1000s at key aggregation points.

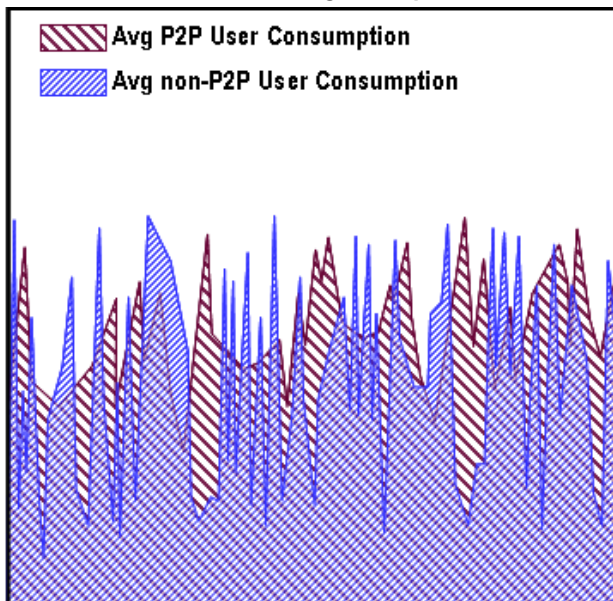
Equal Capacity for All Users

The FR-1000 can also automatically equalize the amount of network capacity available to all users of the same class (e.g., students), and on the same wireless access point. For example, for all students within a residence housing cluster, the FR-1000 ensures equal capacity at all times. If there is little overall traffic (e.g., 3am), then all students will enjoy an equal amount of extra network capacity. At 8:00pm when network video, voice, and data services are much more active, all students continue to receive exactly the same capacity, albeit at a lower amount. Consider the following graphics representing the total amount of capacity on a given interface:

Traffic Mix Without Anagran



Traffic Mix With Anagran Equalization



Easy to set up within minutes, this ability to guarantee equal access among students, at all times, keeps P2P abusers from consuming more than their fair share of the network, while ensuring consistent service quality for all other users. This is especially effective in wireless networks, where overall capacity within any given access point can be dominated by a single P2P user. By automatically equalizing the capacity among all users on any given AP, even the most aggressive P2P users get no more than their fair share of the limited bandwidth, which means perfect voice and Internet access for other students, all the time.

ANAGRAN FEATURE SPOTLIGHT

Key Anagran Features That Manage P2P and Protect the Quality of Key University Applications

Instant P2P Control:

- Manages *all* P2P traffic, encrypted or not, to enable precise control via simple policy setting. All other key network applications are instantly protected from P2P.

Automatic Per-User Equalization:

- Settable on the FR-1000 within minutes, automatic equalization ensures equal capacity for all users within any given class (e.g. students) and on any wireless access point, all the time. Intense P2P users are equitably moderated to no more than their own fair share.

Unsurpassed Scalability and Economy:

- Economically scaling from less than 10 Mbps to *up to 10 Gbps* per port in a 1RU form factor, the FR-1000 breaks new ground for top-tier traffic management per dollars-per-megabit value.

Conclusion:

University and college networks are facing a serious threat that endangers the performance and quality of their voice, video and data applications – P2P file sharing. With Internet access now available to all students 24 hours a day, P2P traffic can visibly harm video, interrupt or even drop voice calls, and turn Internet access and gaming into painfully tedious experiences at any time. This is especially evident in wireless networks across campus and within student residence halls.

With DPI approaches proven to be ineffective against P2P, Anagran delivers the only “P2P proof” technology that manages P2P in all its many forms and also ensures equal capacity for all users. P2P traffic is instantly rendered harmless while P2P users get no less than their fair share of the network. Key learning and administrative applications can be protected and progressive new applications can be rolled out with confidence at any time.

Instantly protect your university or college from P2P traffic and preserve the performance and quality of rich media applications with Anagran.

