

Submission Requirements

6.1 *Features of the Technology*

Matching, Screening and Filtering –

The custom Global File Registry (GFR)/CopyRouter application is a joint initiative with a leading, worldwide, networking company (the name of this partner can be provided under NDA) that runs on a carrier grade, router platform (together "CopyRouter"). Such device will be installed in-line with user's traffic at the campus' infrastructure. The application identifies Query Hit packets of the P2P Gnutella Protocol using multi-gigabit wire speed, stateful Layer 7 Deep Packet Inspection technology. Support for other protocols can be added.

The file hashes found in the query hit packets are matched at wire speed, against an in-memory look up table of known infringing files. This table contains information about DRM files corresponding to each of the infringing files in the table. The data for this look up table is sourced from GFR, and can be remotely updated to keep up with changes in the network.

Once a file hash has been matched against an entry in the look up table, the information about the corresponding DRM file is replaced into the packet, alongside other relevant information such as file size, file extension and in which Gnutella client this file can be found.

The cleaned up search result is then delivered to the end user's Gnutella client, which will treat the search result as just another bit of information coming from the P2P network.

To close the ecosystem of CopyRouter, there are also servers running Gnutella P2P software to serve the DRM files listed in the 'cleaned up' search results, and reporting station(s) where data is collected about most popular files seen in results (but not IPs or other private information).

CopyRouter, should the University be interested, can also be designed to handle a specific subscriber (a particular user of the network, cross referenced against billing info, etc) information to manage bandwidth allocation specifically for that subscriber. This extra feature will allow the University to manage bandwidth on select protocols and replace results for other select protocols.

6.1.1 *Network architecture*

The CopyRouter is a network device which, for optimal performance, should be installed inline with the relevant campus' network. Diagram 1 shows this basic configuration, where traffic from subscribers (users) is connected into the CopyRouter for analysis, and then passed back onto the network again, on its way to its destination. Traffic incoming from the network will follow the reverse path.

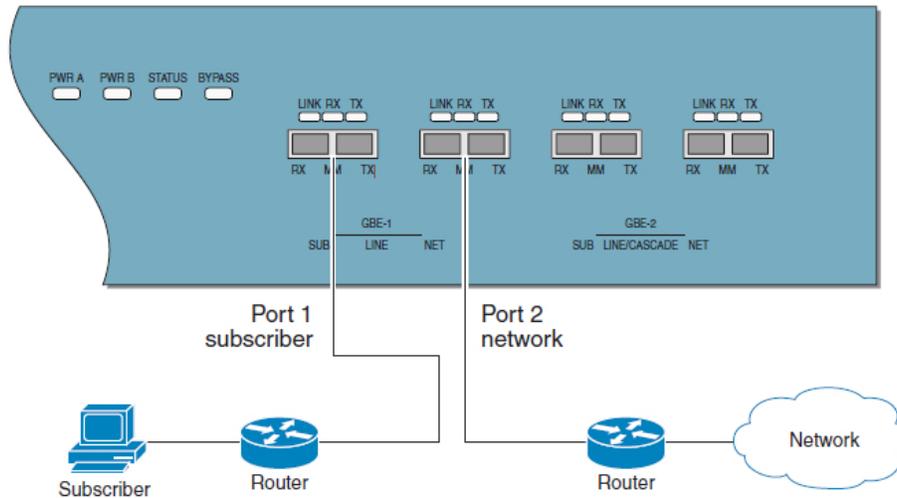


Diagram 1: Single inline configuration

Diagram 2 (below) shows how to connect two CopyRouters for automatic failover configuration. It is also possible to use external optical bypasses instead of a second network device. In this latter configuration, in the unlikely event of a complete failure of the CopyRouter, the traffic will pass unaltered via the external bypasses, although no traffic processing will take place.

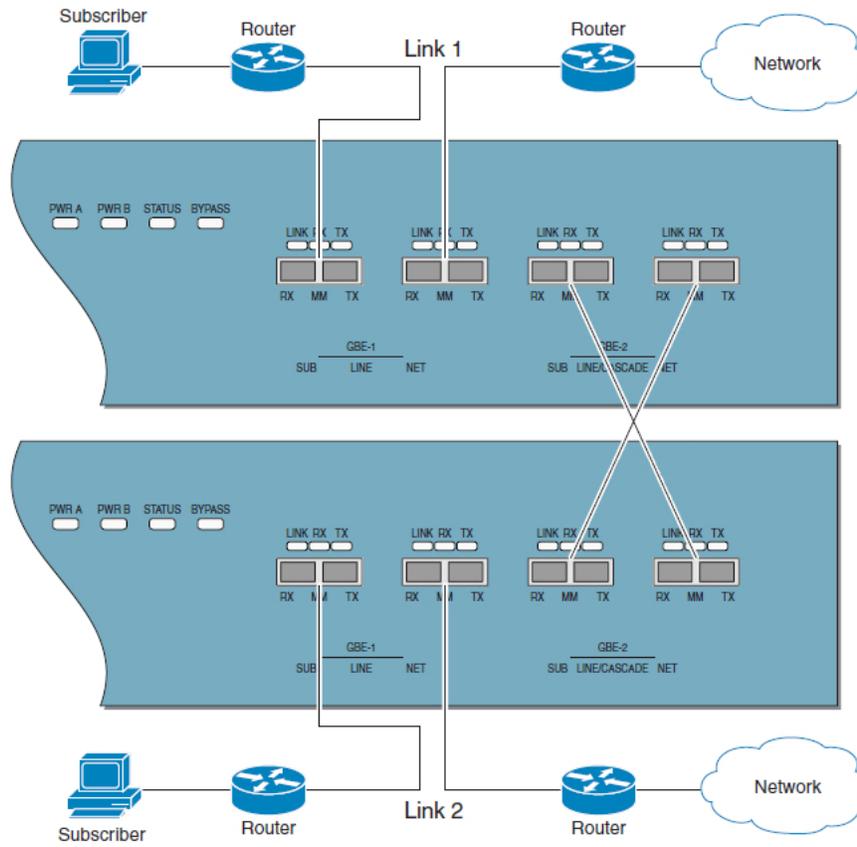


Diagram 2: Dual Link inline Topology for automatic fail-over configuration

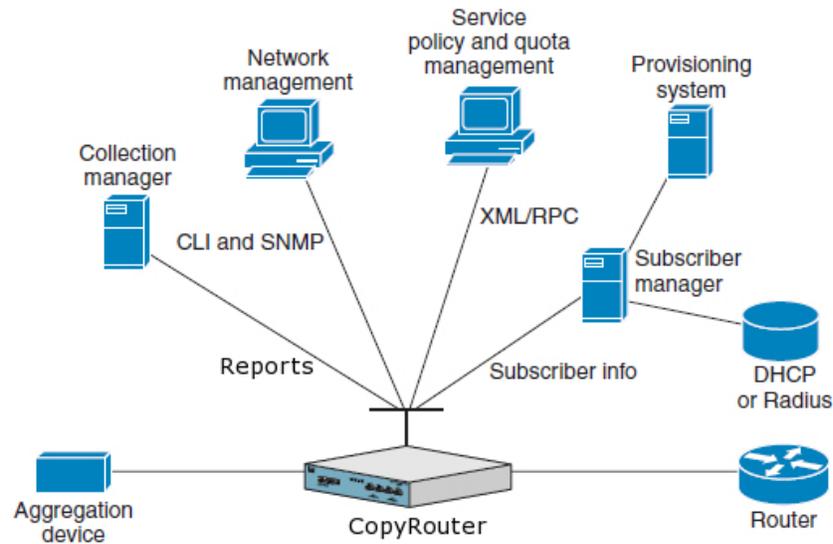


Diagram 3: SCE Platform Management Interfaces

6.1.2 Scalability

CopyRouter is an advanced IP service control solution offering throughput and capacity to support wire-speed processing of 4 Gbps of traffic over 2 gigabit links supporting 2 million unidirectional flows and using customized ASICs and hardware acceleration to help ensure carrier-grade performance. The device can keep track of 80,000 concurrent subscribers.

CopyRouter can be configured with additional network devices to provide 10 gigabit or multi-gigabit links, providing load-balancing of the IP traffic, while ensuring that the traffic of each IP flow and subscriber is processed by the same CopyRouter.

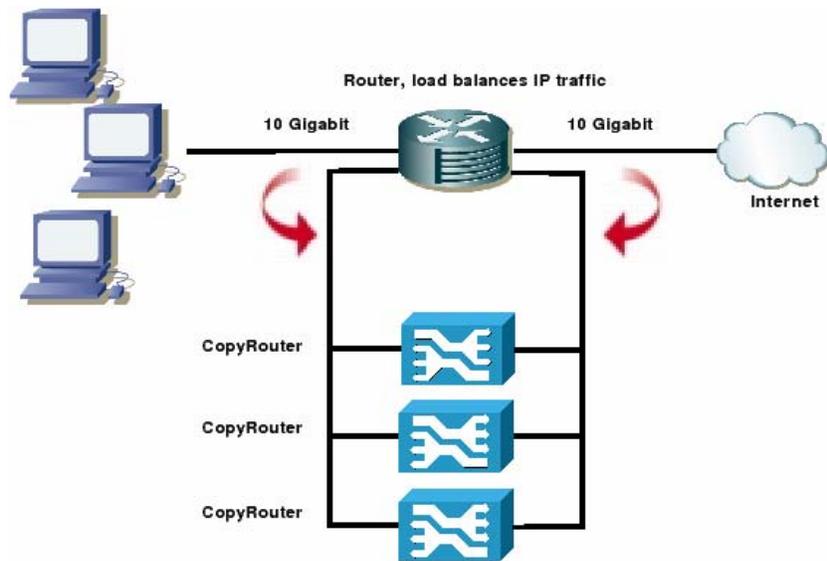


Diagram 4: Scalability of GFR CopyRouter

6.1.3 Protocol identification

The CopyRouter application performs stateful deep packet inspection, fully reconstructing individual traffic flows and the Layer 7 state of each individual application flow.

The platform supports more than 600 different protocols, and thanks to its programmable protocol detection, is extendible to new protocols and adapts to P2P recognition

For the current release of the CopyRouter, the Gnutella P2P network (in which a great amount of infringing activity occurs) is fully supported for content replacement. The CopyRouter application can be updated without interrupting the traffic, to provide for evolutions in protocols.

6.1.4 Granularity of protocols

It is very hard (and unreliable) to determine the level of infringement and intentions of users by looking at their searches – we don't focus on these at all. But when search results come back to those queries, one can easily tell whether the result is infringing or not. The GFR CopyRouter focuses solely on search results, replacing the information pointing to these infringing files with information that will take the users to non-infringing files.

This approach has the advantage of focusing on the infringement without needlessly interfering with the users' privacy.

Monitoring and the subsequent stopping of download requests is also available to University's should that be desired. This is a fully functional, programmable interface that easily allows for additional functionality as requested.

6.1.5 Product Configuration and Installation

Installing the device into the network can be done with minimal, if any, downtime for the rest of the network. During OS updates of the device, there is no interruption to network or application functionality. After the OS is updated, the device

needs to be rebooted, which takes approximately 8 minutes. Effects on the network can be eliminated by appropriate network management and design (such as several CopyRouter devices configured for fail over, redundant links, etc).

Upgrades to the device's application and table of file hashes are performed with no disruption to normal traffic. Updates to the application may induce application outages ranging between several seconds to up to 5 minutes, without impacting on network link.

No setup, changes or maintenance are required in individual PCs. The device becomes part of the network infrastructure.

The CopyRouter will have to be added inline with existing infrastructure. Depending on the nature of this infrastructure, different configurations may be needed, such as to support asymmetrical data flows, balanced IP traffic, etc.

The supporting systems, such as the server collecting the reports, are standard servers which can be installed as part of the University's server infrastructure, and then contact Altnet's GFR services via the Internet.

6.1.6 Content identification

The CopyRouter application identifies files in search results by their file hash – this works for any kind of file, regardless of their file type.

The reporting generated by the device allows our patented technology to focus on the most returned search results. Infringing files are identified out of band using Altnet GFR's database and systems, and the in-memory look up table of the device is updated periodically, at customizable intervals. The network owner can provide their own particular hashes they want to block regardless of their popularity in the network, allowing for a perfect balance between dynamically focusing on the most trafficked files and customization for the network's needs.

Information about query hits ("results" in the Gnutella network) is sent to the reporting servers, over the network, on a management interface. The reports generated contain the following information:

- "Match found" report : Protocol (P2P, transport); filename, extension, size and file hash of the original (infringing) file in the query hit ; extension, size and file hash of the replaced (clean) file; server IP and ports where the replaced (clean) file can be found; replacement error bitmap
- "Match not found" report : Protocol (P2P, transport); filename, extension, size and file hash of the file in the query hit
- "Download request, doesn't match known file" report : Protocol (P2P, transport); file hash; name of P2P application (if available)
- "Download request, matches known file" report : Protocol (P2P, transport); file hash; name of P2P application (if available)

The reporting servers reside in the university's own infrastructure, ensuring the ownership and security of the data generated by CopyRouter.

6.1.7 Examination of network packets or file content

The application is based on Layer-7 stateful deep packet inspection. The first few bytes of data in network packets are inspected to determine if they match specific types of messages belonging to Gnutella traffic. Once a flow has been identified as not useful for the application, it is **not** inspected any further. The contents of files transferred are **NOT** inspected.

The reporting generated is in Netflow v9 format. Extra fields are added, as per Section 6.1.6.

If desired, a set of debugging reports exist which are disabled by default, as they are intended for debugging. These reports extend the reports listed in Section 6.1.6 by adding:

- IP address & port of host receiving the Gnutella search result
- IP address & port of host providing the Gnutella search result
- IP address & port of host where the file pointed by the search result can be found.

6.1.8 *Distribution systems*

At this point, Gnutella is supported. The underlying CopyRouter platform supports over 600 different protocols. Although not all of them are approachable in the same way, many of the protocols will be able to function in a similar fashion, by providing specific targeting of infringing content.

6.1.9 *Resilience of the technology to countermeasures*

Countermeasures by file sharing software:

- The CopyRouter application performs specially targeted changes on specific packets to keep Gnutella search results traffic in unencrypted and uncompressed forms.

Circumvention efforts by users

- Because our technology is not reliant on particular ports or IPs being used, it is immune to port tunnelling and proxying approaches.
- Encryption can be used to hide the nature of data.
- An attack based on packet fragmentation would have to be so carefully architected and implemented (so as to split every filehash in a search result across fragments) as to be impractical to effect the replacement process of CopyRouter.

Attacks against components:

- The CopyRouter device acts as a bridge – the only IP assigned to it are on management interfaces – it follows that these interfaces would ideally be on a separate, management network protected from attacks.
- Reporting servers should be placed on this management network, or firewalled to only accept connections from the CopyRouter devices. Even in the event of a failure of this component, the CopyRouter device itself will continue operating normally without any detrimental effect on the campuses networks.
- GFR public servers are protected by state of the art anti-DDOS measures. Even in the event of an outage (related or not to any attacks that may happen), the CopyRouter device and networks in campuses networks will not be affected.

6.1.10 *Testing and installed base*

The GFR system is a proven technology which has been in use, with the approval of the record labels, to prevent copyright infringing in the Kazaa P2P application with several million simultaneous users since 2006. It is also being used in several products currently under active development.

The CopyRouter device incorporates GFR in a router platform from the world's leading router manufacturer, which is a proven technology used in hundreds of major ISPs around the world, as a core component of their Service Control initiatives.

A market pilot of the GFR CopyRouter solution is under way in Australia, with the participation of the record labels, IFPI, local ISPs, Altnet and the router manufacturer.

6.1.11 Competitive approaches

The advantages of CopyRouter over other technologies include:

- built on top of proven, patented file identification technology and carrier grade, multi-gigabit hardware.
- Specifically targets search results pointing to infringing files. Infringement is prevented regardless of the action the user takes.
- Application is far less intrusive to user's privacy than other solutions.
- It allows for specific targeting of content of any kind by the University owner of the network.
- When users download any of the clean results, they get access to high quality, legal content using proven DRM technology.
- Programmable, extensible interface makes it an adaptable platform for the future.

6.1.12 Third-party components

No third-party components are contemplated in GFR/CopyRouter.

6.1.13 Comparison with Hypothetical Scenario

- CopyRouter considers Privacy issues and focuses on infringing content without identifying the user, unless required.
- CopyRouter does not block p2p applications but rather specific, infringing files.
- CopyRouter offers a solution to infringing content by substituting infringing content for non-infringing content at wire speed.
- CopyRouter is scalable and programmable allowing for additional customizable functionality as required by specific University's.

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

6.2.1 Identifying Infringing Traffic at the Campus Border

GFR provides a back office system which allows each customer to manage and control which file hashes are being targeted at any given moment. Although the system can be left to run automatically (targeting the most common infringing search results), specific items can be added or removed, either manually or via web-services based API.

Industry-standard application programming interfaces (APIs) to ensure easy integration with:

- Provisioning systems
- Operations support systems (OSSs)
- Management systems
- Billing systems

The following carrier grade features make the system, when properly setup, provide for high availability and, in worse case, "fail open":

- High Availability

- Dual-cascaded system design to provide redundancy and failover protection
- System Bypass for Link Preservation
 - Internal electrical bypass mechanism (one per Gigabit Ethernet link)
 - Support for external optical bypass module (one per Gigabit Ethernet link)
- Field-Replaceable Units
 - Power supplies
 - Fan unit
- Internal Redundancy
 - Redundant Power Supplies
 - Redundant Fans
- Line feeds
 - Dual AC and DC Power

Generation of reports from the device can be managed independently from the execution of the application handling the traffic. These reports can be sent to one or several reporting stations.

6.2.2 Responding to Infringing Traffic at the Campus Border

There is currently no support for reporting infringing traffic, because by the nature of the application, the results pointing to infringing traffic are removed.

Requests for infringing downloads are logged using the standard reporting interfaces. The information can be polled from the reporting databases at any time to obtain the information desired about illegal downloads – white listings can easily be applied at this stage.

6.2.3 Identifying Infringing Traffic Local to the Campus Network

The CopyRouter works based on identifying traffic going through it, be it local (private IPs), or not. Reporting, identification of subnets, etc. are all performed outside of the device itself, in the reporting server. The current design is for **not** logging IP addresses of parties to the traffic due to privacy concerns, but we can work with each universities own requirements in this regard.

6.2.4 Responding to Infringing Traffic Local to the Campus Network

CopyRouter, due to its flexible nature, can run on monitoring only mode to flag infringements and not replace the file with non-infringing content, if this is the desired outcome. The technology requires all traffic through inspection devices (the SCE). They are not point of failure if they are configured properly (even with 1 SCE + external optical bypasses we can assure no loss of traffic in case of SCE failure).

6.2.5 Supporting the Campus Judicial System

CopyRouter provides the utmost flexibility as necessitated by the individual requirements of the University's. On detection of infringing content, the automated issuance of DMCA notices can easily be programmed into the interface, and collection of data specific to the needs of each institution, is highly flexible. Such data will be communicated to the University systems through a tamper-proof method.

6.2.6 Avoiding Disruption of All Non-infringing Traffic

Due to the flexibility of the in-memory, remote, updatable lookup table, it is possible to temporarily allow certain files to be shared – it is fully under the control of the network's owner, if they so desire.

6.2.7 Considerations for Purchase and Operations

As discussed in the below Section 6.6 and elsewhere in this document, there are a number of considerations and models that will work for each, unique University requirement. There are many options in this respect and is best left for discussion depending on specific requirements.

6.3 Intellectual Property

GFR/CopyRouter is protected by a number of issued Patents owned by Kinetech, a wholly owned subsidiary of Brilliant Digital Entertainment, Inc. The Patents fall under U.S. Patent Nos. 5,978,791, 6,415,280, and 6,928,442. Further details and an abstract of the Patents can be provided upon request.

6.4 Corporate Characteristics and Resources

Brilliant Digital Entertainment, Inc. (BDE) is the parent company of Altnet, Inc. (owner of GFR and licenses to major label content) and Kinetech, Inc. (owner of several Patents relevant to the GFR product). BDE was formed in 1996 and formed its Altnet subsidiary in 2002. BDE has offices in Sherman Oaks, California and Sydney, Australia and has a total of approximately 20 employees and consultants working in areas that include R&D, Business Development, Project Management and Marketing. (Further Information can be provided under a Non-Disclosure Agreement (NDA).

6.5 Pilot Testing

We understand that some Universities may be interested in a test and evaluation of the CopyRouter solution without making a formal commitment. We are confident in the viability of our solution but also understand that there are many unique requirements for each of the University's. Therefore we welcome involvement in a real life test with those University's that want to conduct an evaluation of our technology. Depending on the complexities of each test, we do anticipate that it can be conducted for little or no out of pocket cost to the University.

6.6 Commercial Terms

As is often the case, the commercial terms will vary by University, depending on the unique requirements of each institution. However, we anticipate that the most attractive business model that will be adopted by the University's is payment by the Universities of: (1) a one time set-up fee, and (2) cost of equipment. In turn, Altnet will share with the University's an agreed upon revenue share from any revenue generated from sales related to infringing file substitution.

An alternative business model to the above, should the University prefer to minimize their initial out of pocket expenses, is payment by the University of an agreed upon monthly license fee.

6.7 Additional Information

While we have attempted to provide you with as much detail as possible in this RFI in order for you to fully evaluate our solution from this material alone, you should be aware that we cannot provide all relevant details due to the confidential nature of some of the material and information. All the benefits of our solution, due to its complexity and the varied requirements of the Universities, cannot be described in one document. Therefore, we encourage your additional

questions and dialog by contacting us directly so that we can answer any further questions you may have in order to arrive at an informed decision.

Contact: Anthony Neumann

Email: aneumann@altnet.com