

# A Quick Introduction to DRDL

## Introduction

Listening to just a word or one sentence in a phone conversation won't tell you much about the discussion. Listening to only what one person is saying will probably give you a better idea, but still lead to some misinterpretation in what the discussion is all about. Listening to the exchange of information between both parties, in the correct order, gives an accurate picture. You probably won't even have to listen to the whole conversation to get a complete picture. You will also have the opportunity to pick up some other relevant details about the conversation by understanding the context. The same goes for Internet traffic, or rather IP traffic, where two parties – a client and a server – always exchange information in a “conversation”.

## DRDL™

### Datastream Recognition Definition Language

IP traffic consists of packets. Internetworking has traditionally been managed packet-based which offers Best Effort at its best. This is due to a legacy where IP from the beginning was utilizing excessive capacity in existing networks. Today's new IP-based services require quality beyond Best Effort. In order to apply this quality, it is required to put packets in a context – that context is called a flow.

The packet-based approach to granular traffic control is called Deep Packet Inspection (DPI). DPI is like listening to a word or a sentence without a context. Looks can be deceiving – both FTP and SMTP respond “220 Welcome

to [...]” when a new connection is being established. But this is not the only challenge. IP, especially TCP, will send fragments of packets, packets will come in incorrect order and packets will be resent.

Now consider that the two parties having a phone discussion, decides that one of them is to call a third party and tell him what has been decided. So he does. Instantly when the third person picks up the receiver he starts feeding him information. This becomes a cryptic “conversation” unless you have the knowledge from the previous phone call. This is equivalent to application protocols (Services) that use separate control and data sessions, e.g. FTP, SIP and Direct Connect.

But a flow puts it all straight. The handshake for a new flow, a.k.a. connection or data stream, is considered as a whole, which means that no false-positives occur in the identification. This kind of identification of IP traffic requires that the detection engine looks far into a new connection to exclude all wrong options. The flow-based detection engine in PacketLogic™ is called DRDL™ (Datastream Recognition Definition Language). It is during the identification process that DRDL extracts the detailed traffic properties. DRDL does not only look at flow by flow but can also relate parent and child connections, like in the case of FTP, SIP and Direct Connect in the previous paragraph.

This way of managing traffic will give a brand new experience to someone who is

by Jon Lindén  
Vice President of Product Management  
Procera Networks, Inc.

## Quick Facts on DRDL

### No of services:

1000+ DRDL signatures

### Main benefits:

- Accuracy; no false-positive – combines multiple criteria in the identification process
- Granularity
- Combines parent and child connections
- Manages tunneling
- Possibility to script new signatures for proprietary and new services

used to aggregating traffic information from routers/switches. The difference between router/switch information and DPI shows the importance of proper identification. PacketLogic uses the DPI information to give real-time traffic views, to produce traffic reports, to filter hazardous traffic, to shape over-consuming applications, to launch new broadband services and much more. It all relies on DRDL. A Service Management System is for example useless if the user can sneak by the defined preferences and use Skype when he has only paid for web and mail. DPI opens a world of possibilities for a service provider (xSP), operator or telco.

## Case Studies

### Parent and Child Connections

FTP has a control session and a data session. Blocking the control session (FTP) will deny FTP as a whole. Shaping the control session makes no difference since the actual data is sent over a new separate connection (FTP DATA). This data session contains no flow header and is established based on the information provided by the control session. This means that unless you get the information from the control session, you will not be able to correctly detect the FTP DATA flow. The option is to shape all traffic on port 21, which will miss all FTP (data) traffic on other ports, and shape all other traffic that comes over port 21. Several Services, like SIP, KaZaA and Direct Connect, are today using multiple related sessions.

### Protocol Tunneling

Not looking hard enough can give the wrong picture. KaZaA typically uses HTTP (web) as the protocol for the data session. The KaZaA data session is initiated over HTTP, a.k.a. protocol tunneling. By looking deep enough and by putting it in a flow-context, DRDL can identify KaZaA sessions running over HTTP and manage them accordingly in PacketLogic.

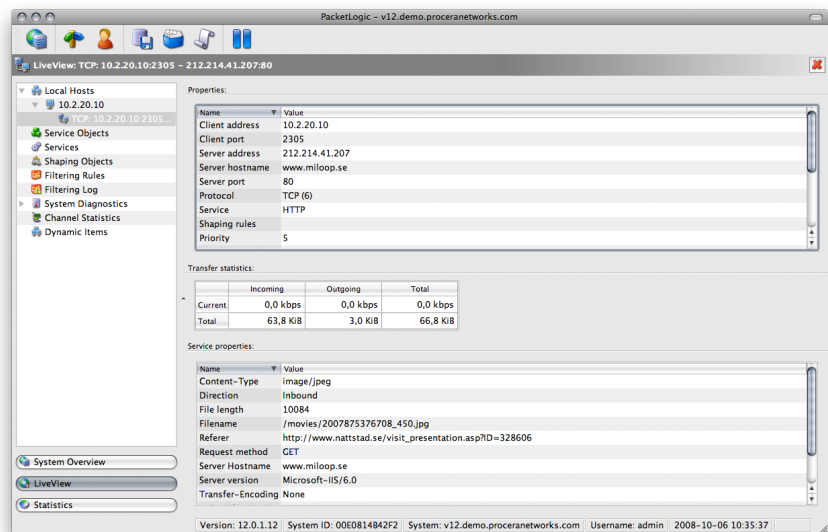
### Port Definitions

Port definitions have been obsolete since the beginning of Peer-to-Peer filesharing. P2P applications were blocked in the firewall. The solution was to use other ports to get by the firewalls. The applications got more intelligent and performed a port scan to detect open ports with the best speed. Bitorrent, the currently most popular P2P filesharing

protocol, establishes one connection per remote host, which can be hundreds of hosts in the case of a popular content, and uses all ports and all available bandwidth.

### Encryption

Encryption affects DPI. DRDL never decrypts traffic which means that no properties can be provided in some cases. In other case there are flow properties that are not encrypted, e.g. server and client version in SSH. The flow-based approach will anyhow be useful since it means that application protocol still can be properly identified based on multiple properties using recognizable patterns. An example is the Japanese P2P protocol Winny that initiates a new connection by exchanging what looks like random keys to establish the encryption tunnel.



Granular connection information, including DPI properties (Service Properties) in PacketLogic

Corporate Offices  
Procera Networks, Inc.  
100-C Cooper Court  
Los Gatos, CA 95032  
P. +1 408-890-7100  
F. +1 408-354-7211

European Headquarters  
Procera Networks  
Birger Svenssons Väg 28D  
432 40 Varberg, Sweden  
P. +46 (0)340-48 38 00  
F. +46 (0)340-48 38 28

Asia/Pacific Headquarters  
Procera Networks Pty Ltd.  
Office 206, 566 St Kilda Road  
Melbourne VIC 3004, Australia  
P. +61 (0)3-9526 8495  
F. +61 (0)3-9526 8483