ERICSSON

Application Traffic Management Overview

TECHNICAL PRODUCT DESCRIPTION

221 02-CRA 119 1170/1-V1 Uen D

Contents

1 Application Traffic Management

Broadband service providers are increasingly challenged by the growth of bandwidth-intensive applications and the inability to generate revenue from bandwidth used. Key issues associated with these bandwidth-intensive technologies include:

- Differentiated upstream and downstream bandwidth demands.
- Aggressive use of network resources and its impact on network capacity.
- Unrealistic subscriber expectations of network capacity.
- Optimization of applications like VoIP and IPTV.

A significant portion of application traffic consists of file downloads of multimedia content that is often hundreds of megabytes in size. With these large file downloads, the traditional patterns of on and off periods of activity are replaced with constant traffic patterns. These new traffic patterns can create congestion on network links and make it difficult for operators to perform effective capacity planning.

In addition to illegal file-sharing, the amount of content provided directly by legal content providers is increasing; therefore, it is not an option to block all application traffic.

You can configure a SmartEdge® router to perform Deep Packet Inspection (DPI) and heuristics-based traffic classification services to get better visibility into subscriber traffic. Based on the information obtained from the traffic analysis, the router can:

- Control access to content, so that only subscribers with the proper subscription can receive the application service.
- Control the amount of bandwidth for individual subscribers on certain applications.
- Mark data traffic with a drop-precedence value corresponding to the Assured Forwarding (AF) class of the packet or a Differentiated Services Code Point (DSCP) value.
- Add latency, introduce jitter, drop or reorder packets, or reset the session.

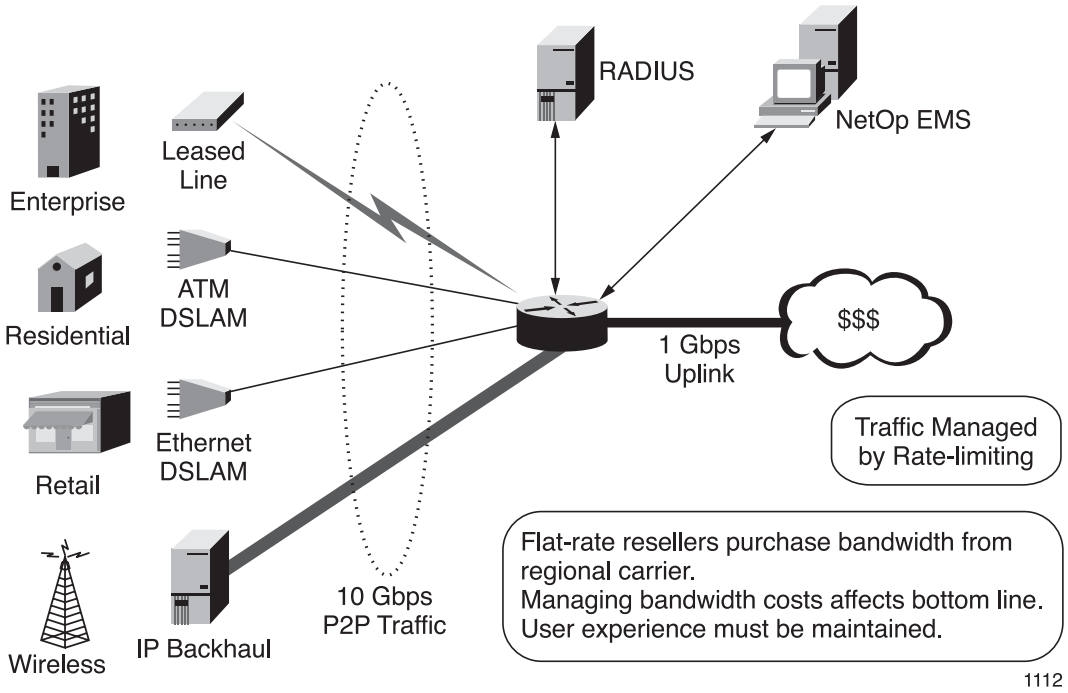
Application traffic management enables operators to manage application bandwidth and collect revenue from application traffic while providing the network performance that subscribers expect.

1.1 Application Bandwidth Management

You can manage bandwidth by optimizing services or optimizing network usage.

To optimize services, the SmartEdge router can track bandwidth-intensive applications—for example, file sharing, video streaming, and online gaming—and increase revenue potential by using the following:

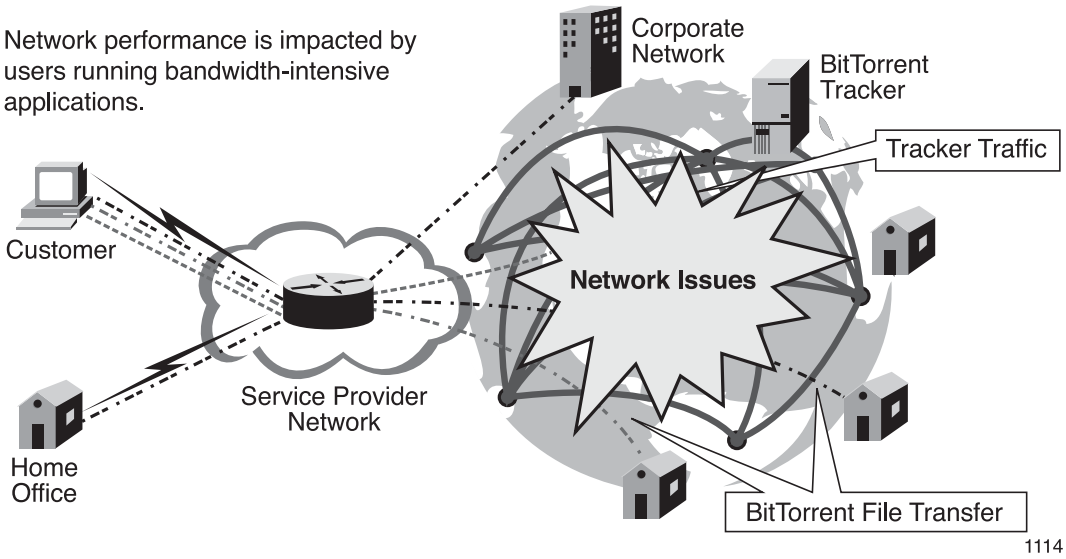
- Usage-based profiles: Based on usage or based on application, identify dominant protocols in the network and monitor bandwidth usage per protocol.
- Tiered service profiles: Based on throughput, apply application-based bandwidth throttling on dominant network protocols with rate-limiting profiles applied to individual applications.



To optimize network usage, the SmartEdge router can restrict the total bandwidth used by bandwidth-intensive applications to allow efficient use of the current network infrastructure:

- Network equipment optimization: For service carriers, application traffic management reduces network congestion and degraded network performance due to increased application traffic. Network equipment optimization is accomplished by identifying dominant application protocols in the network and applying application-based bandwidth throttling.
- Network traffic optimization: For multi-service operators, application traffic management helps manage upstream application traffic to reduce transit

fees, and maintains the network performance by applying rate-limiting profiles to upstream traffic from subscribers.



1.2 Protocol Detection

The SmartEdge router detects application protocol traffic, including application protocols masquerading as other types of traffic on well-known ports. Detection of application traffic is based on a combination of signature matching and heuristics; see Section 2 on page 5. Detection of some encrypted application traffic is supported; however, encrypted traffic can only be detected indirectly using flow metrics and other heuristics. Therefore, detection of encrypted application traffic is not guaranteed.

The SmartEdge router detects a number of protocols, including the following:

- FastTrack
- Ares
- BitTorrent
- eDonkey
- Gnutella

Analyzers are updated according to the newest available version of each protocol.

2 Traffic Analysis

The SmartEdge router uses three different traffic analysis methods to extract relevant information:

- Shallow packet inspection: Inspects basic Layer 3-4 information in the IP packet
- DPI: Uses knowledge of the protocol definition and reaches the upper layers (L4, L7) to get information about the application flow and headers
- Heuristic inspection: Uses empirical data about the traffic properties

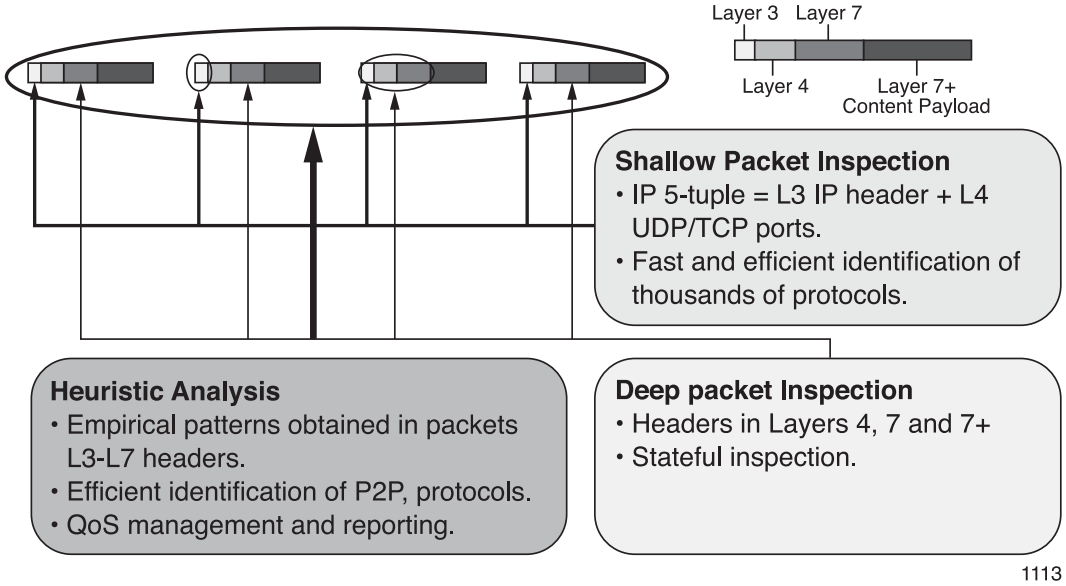


Figure 1 Application Traffic Analysis

Traffic classification can be based on any of these analysis methods. The application service class result of the classification is independent of the analysis approach followed, and it can be managed and controlled in exactly the same way, regardless of whether shallow inspection, deep inspection, or heuristic analysis have been used. You can create a powerful traffic-identification engine by defining application service classes that rely on more than one analysis approach at the same time.

2.1 Shallow Packet Inspection

Shallow inspection obtains the 5-tuple of the IP packet header:

- Source IP address
- Destination IP address

- Source UDP/TCP port number
- Destination UDP/TCP port number
- IP protocol number

Shallow inspection is stateless, because the 5-tuple exists in any IP packet.

Shallow inspection enables content type identification based on, for example:

- Application server IP address (for example, IMAP server, and so on)
- Well-known ports (for example, 143 = IMAP)
- Protocol number (for example, 1=ICMP)

Because shallow inspection is simple and requires minimum node resources, operators use it when the application service servers and ports are well-known and stable. However, shallow inspection cannot identify events within the user session (for example, a message transaction) or any application-specific information (for example, URI), and is sensitive to changes in the application service IP addresses and ports.

Shallow inspection requires the 5-tuple fields to be available. For example, if IPSec is used, the protocol number could be either 50 (ESP) or 51 (AH). If tunneling is used, the source and destination addresses identify only the tunnel end points.

2.2 Deep Packet Inspection

DPI on the SmartEdge router examines packets beyond the IP header and extracts parameters from higher layers (Layer 4 and 7).

DPI is more processing intensive than shallow inspection. Because it requires transparency of the inspected traffic, DPI does not work with compressed or encrypted traffic.

2.3 Heuristic Analysis

Heuristic analysis is based on a set of empirical pattern characteristics of a particular protocol or application, and it does not rely on the exact knowledge required by DPI.

Heuristic analysis is typically used by the SmartEdge router together with DPI. However, only heuristic analysis may be possible when the protocol used:

- Is proprietary
- Is encrypted and cannot be analyzed

- Tries to mimic other well-known protocols
- Is so new that a DPI protocol analyzer does not exist yet

Unlike shallow or deep inspection, the heuristics traffic analyzer makes a best-guess classification andidentification accuracy is not guaranteed to be 100%. For example, some sophisticated heuristic patterns need to inspect several packets before they can identify the protocol (the application tests three known ports in succession before initiating a transaction). In this case, the traffic that was used in the early stages of the detection is not buffered and cannot be classified later because it has already been transmitted. However, you can use heuristic analysis effectively for the following:

- Class-based differentiated QoS control—You can adjust the QoS of certain classes to your commercial strategy—for example, to guarantee the QoS of your own applications.
- Access control—Traffic patterns that indicate a security problem can be blocked. Even if not all traffic is blocked, the application service is unusable.
- Statistics—You have more visibility into the distribution of data traffic across classes, which can help you develop a commercial strategy.

The identification is of an aggregated nature; granularity is at the level of the application service session (for example, to identify all P2P traffic from a subscriber's terminal).

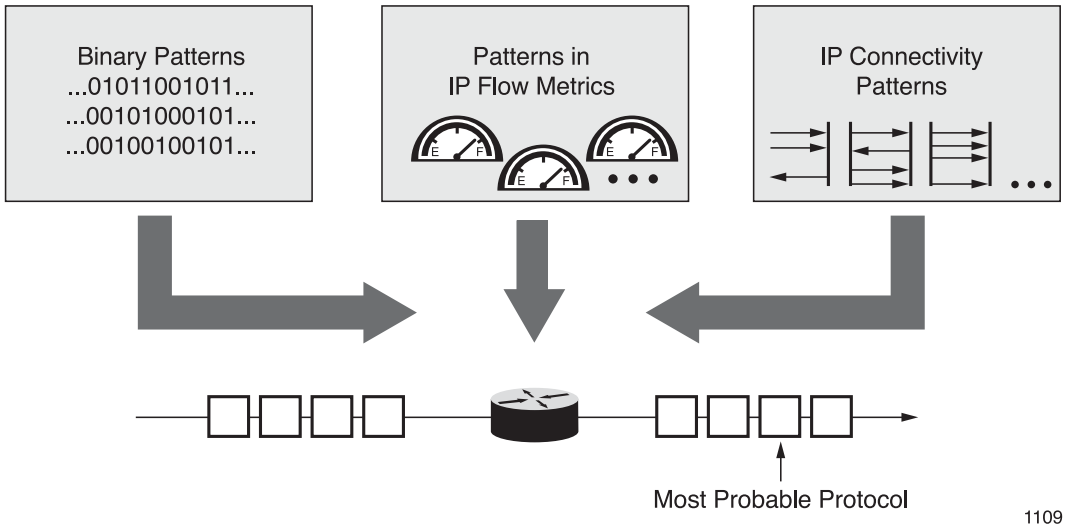


Figure 2 Heuristic Analysis

Three types of patterns are applied, which, when combined, provide the highest possible identification rates:

- Binary patterns in the IP payload: Signatures in the data bit stream that reveal the protocol type

- Patterns in IP flow metrics, such as average bit rate and average packet size: Patterns that reveal information about the nature of the traffic
- Connectivity patterns: Patterns that identify peculiar protocol activity that is characteristic of some clients (for example, scanning of certain port ranges, changes in protocol, and so on)

These heuristic patterns have been created based on the observation and analysis of real traffic.

3 Traffic Classification

When the SmartEdge router detects application traffic, the node applies an application traffic management policy.

Note: NAT and ASE services are mutually exclusive and cannot be applied together for a subscriber; only NAT will be applied if you attempt to apply both services to a subscriber.

An application traffic management policy includes a reference to an Access Control List (ACL) policy and an action policy.

An ACL policy is an ordered list of packet filters (rules), each of which defines a class of packets. Different actions can be applied to different classes of packets.

The ACL policy does not define the action applied to the traffic. The action is determined by the traffic management action policy. A traffic management action policy is a collection of class entries, with each class defining one or more actions for that class; see Figure 3.

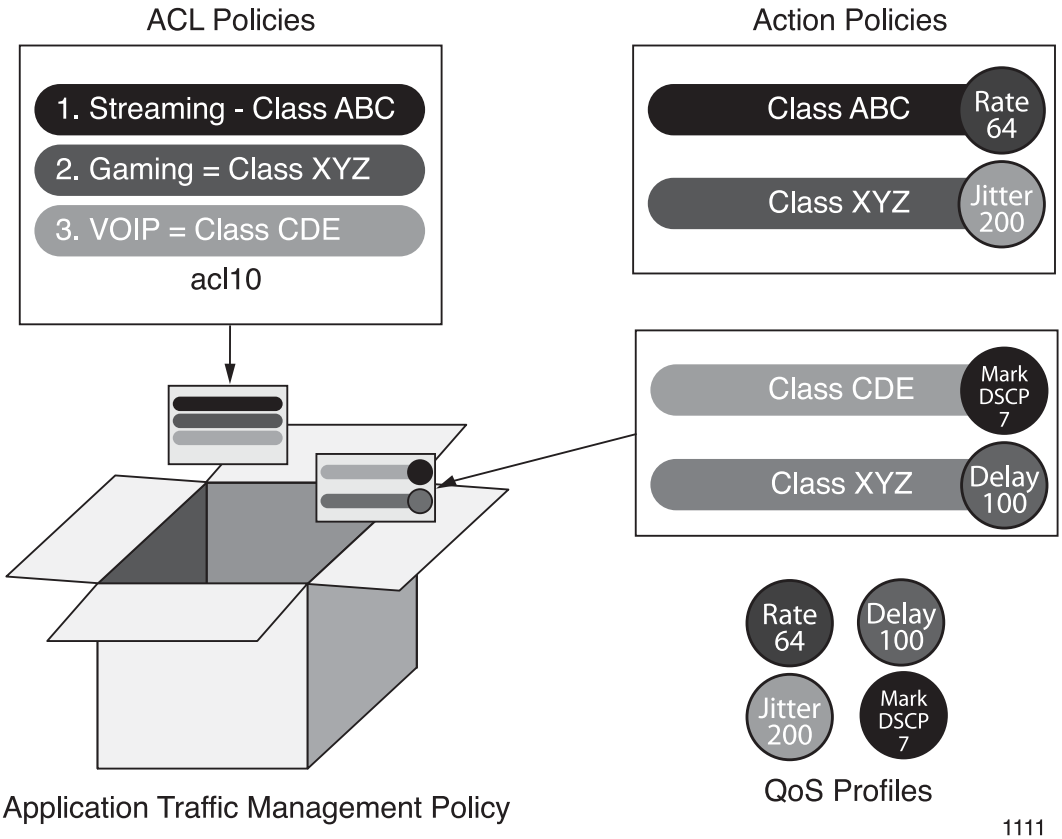


Figure 3 Actions Applied to Classes Through the Application Traffic Management Policy

Different actions can be applied for the same class of traffic; for example, the same BitTorrent traffic can be rate-limited for a bronze subscriber, but not rate-limited for a gold subscriber.

Multiple ACL rules can refer to the same class; however, any rate limit specified for the class is shared by all traffic mapping to that class. For example, if multiple ACLs refer to class A, and class A specifies a rate limit of 100 Kbps, then all traffic mapping to class A is subject to a combined rate limit of 100 Kbps; rate limits apply per class, not per ACL rule.

Traffic can be classified based on application protocol or transport protocol, or on application protocol category. A category groups applications or protocols used for a similar purpose; for example, streaming, messaging, file transfer, and so on. If a category is specified, all applications defined in the category are included.

By specifying the ACL policy and action policy as references, the ACL policy and action policy can be used by multiple application traffic management policies. For example, the same ACL policy can be referenced by three different traffic management policies to treat the same traffic differently for various user types. Similarly, the same traffic management action policy can be used with multiple ACL policies; see Figure 4.

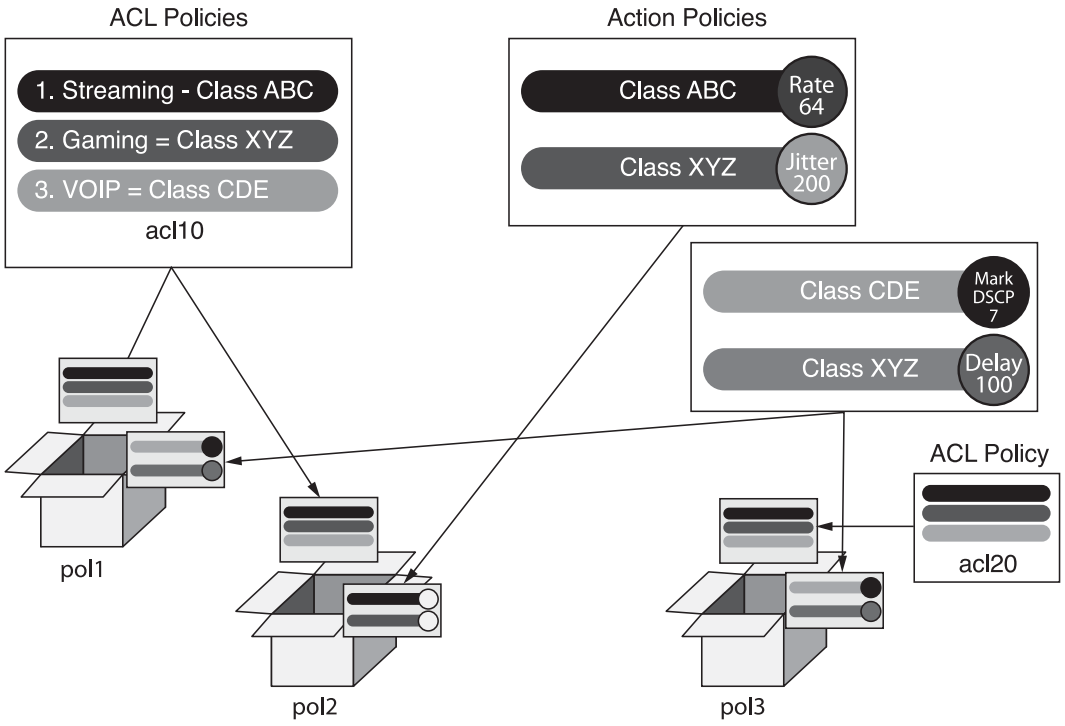


Figure 4 Application Traffic Management Policies Reference ACL Policies and Action Policies

For information on configuring application traffic management, see Reference [1].

4 Statistics Collection

The node collects subscriber statistics per application protocol for inbound and outbound directions.

4.1 Subscriber Statistics

Subscriber statistics are collected per subscriber for upstream and downstream traffic. Inbound traffic is traffic originating from the subscriber; outbound traffic is traffic destined toward the subscriber.

Even though rate limiting can be specified for a group of protocols, statistics are collected per subscriber, per protocol. Statistics are collected and reported for all protocols detected, not just for those configured in the ACL rules.

The node maintains cumulative statistics counters; however, the counters that are reported in the periodic statistics reports are incremental counters. Only those protocols with activity during the previous reporting interval are reported. When a user logs out, any counters with activity since the last statistics report are reported.

Table 1 describes the statistics collected per subscriber, per protocol, for upstream and downstream traffic.

Table 1 Statistics Collected Per Subscriber Per Protocol

Statistic (Field in Log)	**Description**
Packets subject to application traffic detection (PktInsp)	Number of packets that were subject to pattern matching; typically, only the first few packets of a session are subject to pattern matching. Does not include packets with zero application payload length.
Bytes subject to application traffic detection (ByteInsp)	Number of bytes that were subject to pattern matching; typically, only the first few kilobytes of a session are subject to pattern matching. Does not include bytes with zero application payload length.
Packets dropped (PktDrop)	Number of packets dropped due to rate limiting.
Bytes dropped (ByteDrop)	Number of bytes in packets dropped due to rate limiting.

Statistic (Field in Log)	Description
Packets sent (PktTx)	Packets received minus packets dropped.
Bytes sent (ByteTx)	Bytes received minus bytes dropped.
Number of flows (Flows)	Number of unidirectional flows detected as belonging to an application traffic session. The counter is incremented once per unidirectional flow.
Packet direction (Src, Dest)	Subscriber to Internet or Internet to subscriber.

4.2 Log Format

Table 2 describes the fields that appear in the generated logs. Statistics are reported per subscriber, per class, per subscriber group, and per protocol, for upstream and downstream traffic. The counters are incremental since the last statistics report; only those protocols with activity during the previous reporting interval are reported. When a user logs out, any counters with activity since the last statistics report are reported.

Table 2 Description of Log Fields

Log Field	Description
AppProto	Application or protocol for which data is generated in the format **`numeric-id/application-string`**; for example, 1/bittorrent.
Area	Internal message data. Log area.
ByteDrop	Number of bytes in packets dropped due to rate limiting.
ByteInsp	Number of bytes that were subject to pattern matching; typically, only the first few bytes of a session are subject to pattern matching. Does not include bytes with zero application payload length.
ByteRx	Number of bytes received.
ByteTx	Bytes received minus bytes sent in a single direction since the last statistics message. Reported per direction, per user, and per protocol.
Class	Traffic classification value for which data is generated.

Log Field	Description
ConnDrop	Number of flows which have been dropped since the last statistics message in this direction.
Ctxt	Context in SmartEdge router from which data is generated.
Dest	Destination of traffic: Internet (data upload) or Subscriber (data download).Together with Src, indicates direction of the traffic.
DestIP	Destination IP address.
DestPort	Destination port.
DevId	System hostname and ASP Device Identifier [*node-id*]/*slot/port*
Flows	Number of unidirectional flows detected as belonging to an application traffic session. The counter is incremented once per unidirectional flow (that is, incremented by two per bidirectional application traffic session).
Group	Subscriber group for whom data is generated.
Level	Log level.
Module	Internal message data. Module that generated the log; for example, Infra, DPI, Firewall, IKE, IPsec.
MsgId	Internal message data. Message identifier.
PktDrop	Number of packets dropped due to rate limiting.
PktInsp	Number of packets that were subject to pattern matching; typically, only the first few packets of a session are subject to pattern matching. Does not include packets with zero application payload length.
PktRx	Number of packets received.
PktTx	Packets transmitted in a single direction since the last statistics message. Reported per direction, per user, and per protocol.

Log Field	Description
Policy	Policy applied to the subscriber.
Src	Source of traffic: Internet (data download) or Subscriber (data upload). Together with Dest, indicates direction of the traffic.
SrcIP	Source IP address.
SrcPort	Source port.
Svcs	A space-separated list of ***Service:Policy*** values
TransProto	Transport protocol (TCP or UDP).
TS	Time stamp.
TZ	Time zone of the node.
User	Subscriber for whom data is generated.
Ver	Version of the protocol used for sending messages.

In addition, if any of the following RADIUS attributes are configured for a subscriber, they are included in each DPI log message following the "User" field:

- Calling-station-ID
- Accounting-Session-ID
- NAS-Port-ID
- NAS-Identifier
- NAS-IP-Address
- NAS-Port
- NAS-Port-Type
- RB-MAC-Address

Note: RADIUS attributes are not included in subscriber group class statistics log messages.

If no explicit RADIUS configuration exists, only the subscriber username is propagated. For information on configuring RADIUS attributes, see Reference [2].

The following examples illustrate log format and output for subscriber login, subscriber logout, subscriber protocol statistics, subscriber protocol detection, subscriber class statistics, and subscriber group class statistics.

```
TZ="GMT+0:0" TS="Wed Apr 22 18:59:01 2009" Ver=2 MsgId=0x100000c8
Module="Infra" DevId="akari/1/2" Area="Sub" Level="Notice" Ctxt="m1"
User="user1@m1" NAS-Port="67174400" NAS-Port-Type=5 NAS-Port-ID="4/1
vlan-id 1" NAS-Identifier="akari" MAC-Address="00:00:64:03:01:02"
Accounting-Session-Id="0300FFFF68000002-4C07C323" Svcs="dpi-tm:abc"
```

Example 1 Subscriber Login Log

```
TZ="GMT+0:0" TS="Wed Apr 22 18:59:01 2009" Ver=2 MsgId=0x100000c9
Module="Infra" DevId="akari/1/2" Area="Sub" Level="Notice" Ctxt="m1"
User="user1@m1" NAS-Port="67174400" NAS-Port-Type=5 NAS-Port-ID="4/1
vlan-id 1" NAS-Identifier="akari" MAC-Address="00:00:64:03:01:02"
Accounting-Session-Id="0300FFFF68000002-4C07C323"
```

Example 2 Subscriber Logout Log

```
TZ="GMT+0:0" TS="Wed Apr 22 19:01:41 2009" Ver=2 MsgId=0x10000727
Module="DPI-TM" DevId="akari/1/2" Area="Stats:I" Level="Info"
Ctxt="m1" User="user1@m1" NAS-Port="67174400" NAS-Port-Type=5
NAS-Port-ID="4/1 vlan-id 1" NAS-Identifier="akari"
MAC-Address="00:00:64:03:01:02"
Accounting-Session-Id="0300FFFF68000002-4C07C323" Policy="NULL"
AppProto="1/bit-torrent" Src="Internet" Dest="Subscriber"
PktTx=84357 ByteTx=108510480 PktDrop=0 ByteDrop=0 Flows=1 ConnDrop=0

TZ="GMT+0:0" TS="Wed Apr 22 19:01:41 2009" Ver=2 MsgId=0x10000727
Module="DPI-TM" DevId="akari/1/2" Area="Stats:I" Level="Info"
Ctxt="m1" User="user1@m1" NAS-Port="67174400" NAS-Port-Type=5
NAS-Port-ID="4/1 vlan-id 1" NAS-Identifier="akari"
MAC-Address="00:00:64:03:01:02"
Accounting-Session-Id="0300FFFF68000002-4C07C323" Policy="NULL"
AppProto="1/bit-torrent" Src="Subscriber" Dest="Internet"
PktTx=84475 ByteTx=3545988 PktDrop=0 ByteDrop=0 Flows=1 ConnDrop=0
```

Example 3 Subscriber Protocol Statistics Log

```
TZ="GMT+0:0" TS="Wed Apr 22 18:59:35 2009" Ver=2 MsgId=0x10000728
Module="DPI-TM" DevId="akari/1/2" Area="Detect" Level="Notice"
Ctxt="m1" User="user1@m1" NAS-Port="67174400" NAS-Port-Type=5
NAS-Port-ID="4/1 vlan-id 1" NAS-Identifier="akari"
MAC-Address="00:00:64:03:01:02"
Accounting-Session-Id="0300FFFF68000002-4C07C323"
AppProto ="1/bit-torrent" Policy="NULL"
PxtInsp=0 ByteInsp=0 SrcIP="12.1.5.8" DestIP="121.2.1.1"
TransProto="tcp" SrcPort=32768 DestPort=6881
```

Example 4 Subscriber Protocol Detection Log

```
TZ="GMT+0:0" TS="Wed Apr 22 18:59:29 2009" Ver=2 MsgId=0x10000729
Module="DPI-TM" DevId="akari/1/2" Area="Stats:[C,I]" Level="Notice"
Ctxt="m1" User="user1@m1" NAS-Port="67174400" NAS-Port-Type=5
NAS-Port-ID="4/1 vlan-id 1" NAS-Identifier="akari"
MAC-Address="00:00:64:03:01:02"
Accounting-Session-Id="0300FFFF68000002-4C07C323" Policy="tmg-pol"
Class="C1" Src="Subscriber"Dest="Internet" Pktxt=990 ByteTx=782100
PktRx=0 ByteRx=0 PktDrop=98 ByteDrop=43512 Flows=11 ConnDrop=0
```

Example 5 Subscriber Class Statistics Log

```
TZ="GMT+0:0" TS="Mon May 03 00:21:36 2010" Ver=2 MsgId= 0x1000072a
Module="DPI-TM" DevId="/6/2" Area="Stats:[C,I]" Level="Info"
Group="group1" Policy="tmg-pol" Class=”C1” Src="Subscriber"
Dest="Internet"  PktTx=990 ByteTx=782100 PktRx=0 ByteRx=0
PktDrop=98 ByteDrop=43512
```

Example 6 Subscriber Group Class Statistics Log

5 Quality of Service Management

Quality of Service (QoS) policies create and enforce QoS levels and bandwidth rates, and prioritize how incoming and outgoing packets are scheduled. A QoS policy may be used to manage application traffic by:

- Marking packets
- Applying rate limiting to packets
- Adding jitter
- Adding latency
- Introducing loss
- Reordering packets
- Resetting TCP connections
- Dropping packets

For application traffic management QoS policies, application protocol level QoS actions apply to an aggregate of inbound and outbound directions; separate values for inbound and outbound packets are not supported. You can apply QoS actions per application protocol, or to a group of application protocols.

For more information on QoS class-based marking and rate-limiting, see Reference [3].

6 Operations and Management

The SmartEdge router is operated and configured using a command-line interface (CLI). For information on basic router configuration, including an introduction to SmartEdge OS concepts and the user interface, privilege levels, and managing the configuration file, see Reference [4], Reference [5], Reference [6], and Reference [7].

Glossary

ACL
Access Control List

AF
Assured Forwarding

ByteDrop
Bytes dropped

ByteInsp
Bytes subject to application traffic detection

ByteTx
Bytes sent

DPI
Deep Packet Inspection

DSCP
Differentiated Services Code Point

PktDrop
Packets dropped

PktInsp
Packets subject to application traffic detection

PktTx
Packets sent

QoS
Quality of Service

Reference List

[1] *Application Traffic Management Configuration and Operation*, 1543-CRA 119 1170/1-V1

[2] *Configuring RADIUS*, 65/1543-CRA 119 1170/1-V1

[3] *Configuring Rate-Limiting and Class-Limiting*, 55/1543-CRA 119 1170/1-V1

[4] *SmartEdge OS Product Overview*, 3/221 02-CRA 119 1170/1

[5] *Managing Configuration Files*, 5/1543-CRA 119 1170/1-V1

[6] *Performing Basic Configuration Tasks*, 6/1543-CRA 119 1170/1-V1

[7] *Using the CLI*, 3/190 80-CRA 119 1170/1-V1