JUNIPER FLOW MONITORING

J-Flow on J Series Services Routers and Branch SRX Series Services Gateways

Table of Contents

Table of Figures

Introduction

Rapid growth in IP networks have created a need for increased network bandwidth and better network manageability. Network operators require network-wide visibility to provide the best class of service for their users. J-Flow, a flow monitoring service on Juniper Networks devices, is a tool specifically designed to meet this need, providing network operators with access to IP flow information and improved visibility across their networks. With J-Flow, network devices such as routers, firewalls, and switches collect flow data and export that information to flow collectors. The collected data provides critical information about traffic in the network and aids in tasks such as billing, traffic engineering, capacity planning, and traffic analysis for peering policy decisions.

A flow is a sequence of packets with common characteristics such as same source and destination IP address, transport layer port information, and type of IP protocol. Network devices differentiate flows depending upon their architecture, implementation, and device configuration. Each of these devices collects flow information on traffic that is received or sent through it. This information can then be logged locally or sent to an external information collector that will provide fine-grained information on network visibility for a variety of purposes, such as enterprise accounting and departmental chargeback, Internet service provider (ISP) billing, data monitoring and profiling, security analysis, and data mining for marketing purposes.

J-Flow is Juniper Networks proprietary flow monitoring implementation. Juniper Networks® J Series Services Routers and SRX Series Services Gateways generate summarized flow records for sampled packets from the Packet Forwarding Engine (PFE). Such flow records are exported in an RFC or NetFlow-compliant standard packet format to an external flow information collector. J-Flow is interoperable with any NetFlow supported flow collector, so the external flow collector can be any third-party software that collects data exported from Juniper Networks devices.

Scope

The purpose of this document is to provide information on J-Flow, a flow monitoring service in J Series and SRX Series appliances. Though this document is concentrated on J-Flow version 9, some information is presented on version 5 and version 8. A discussion about external flow collectors is out of scope for this document.

Design Considerations

Hardware Requirements

- Juniper Networks J Series Services Routers (J2320, J2350, J4350, J6350)
- Juniper Networks SRX Series Services Gateways (SRX100, SRX2XX, SRX650)

Software Requirements

JUNOS OS RELEASE	J-FLOW WITH ROUTING ENGINE (RE)-BASED SAMPLING	J-FLOW WITH INLINE SAMPLING
Up to 9.4	v5 / v8	v5 / v8
9.4 to 10.4	v5 / v8	
10.4 onwards		v5 / v8 / v9

Description and Deployment Scenario

How J-Flow Works

As we have already seen, a flow is a bidirectional packet stream identified by a unique set of similar characteristics. J Series Services Routers and SRX Series Services Gateways have designed around a flow-based architecture. By default, these devices inspect the network and transport layer attributes of incoming packets and create flow sessions for a set of seven IP attribute values:

- Source IP address
- Destination IP address
- Source port address
- Destination port address
- IP protocol
- IP type of service (ToS)
- Incoming interface

Subsequent packets with the same value for these attributes refresh existing flows and no new flows are created. Any deviation in packets from the attributes listed above will create a new flow.

Similar to flow-based architecture, the J-Flow service on J Series and SRX Series devices creates a J-flow table (J-Flow cache) for a set of network and transport layer attributes. These attributes vary with different J-Flow versions. A flow record is created in the J-Flow table when the first packet of a flow is processed. It is maintained within cache until the flow is active. Each flow record in the table contains key fields that can be used at a later time for exporting data to a collection device. As a flow record becomes active in a device, all packets with similar characteristics are tracked and counted, and certain fields in the flow record are updated. The flow record or J-Flow table information is exported to a flow collector server periodically, based on flow timers. The collector contains a history of flow information exported by different devices. Juniper Networks Junos® operating system also provides command-line interface (CLI) commands to retrieve and display flow records in the J-Flow table within a device.

J-Flow Versions

In Junos OS running on J Series and SRX Series appliances, there are three different versions for creating and exporting flow records to the flow collector. These three versions are called J-Flow v5, J-Flow v8, and J-Flow v9. Each version has its own advantages over the others, and J-Flow v9 is the latest version supported on the J Series and SRX Series from Junos OS release 10.4 onwards.

J-Flow v5

Attributes and fields in J-Flow v5 exported flow records are fixed, users are not allowed to make changes to flow record format.

J-Flow v8

J-Flow v8 has the same attributes and fields as J-Flow v5, but it allows the aggregation of flows with a specific attribute. J-Flow v8 supports five aggregation schemes, and it conserves memory and bandwidth by exporting targeted flow records rather than all aggregated traffic.

J-Flow v9

J-Flow v9 is very different from J-Flow v5 and J-Flow v8 in terms of exported flow record fields, and it is template based. Templates are defined by selecting a set of attributes for which flow aggregation is required. This gives flexibility for future enhancements and the addition of new attributes to J-Flow without changing to a newer version.

Template information is communicated from J Series and SRX Series devices to the flow collector, so the collector should expect flow records in vendor-defined template format. Also, this version adds support for IPv6 and MPLS flow records. J-Flow v9 which is based on RFC 3954 is now the protocol of choice for the IETF IP Information Export (IPFIX) working group (WG) and the IETF Packet Sampling WG (PSAMP).

J-Flow v9 Implementation on J Series and Branch SRX Series Devices

J-Flow consists of components that run on the Routing Engine (RE) and PFE. It is convenient to start looking at these components from the perspective of the packet path in the system. As a packet enters an interface, it needs to be picked for sampling, subject to policies. This is achieved by applying a firewall filter on the interface of interest. When a packet matches the firewall filter, the PFE marks the packet as a candidate for sampling (as depicted in Figure 1). The packet proceeds along its normal path completing all forwarding tasks. After the route lookup is performed, packets picked by the filter are handed over to the sampling logic. The sampling algorithm decides whether to make a copy and send it to the inline J-Flow service thread.

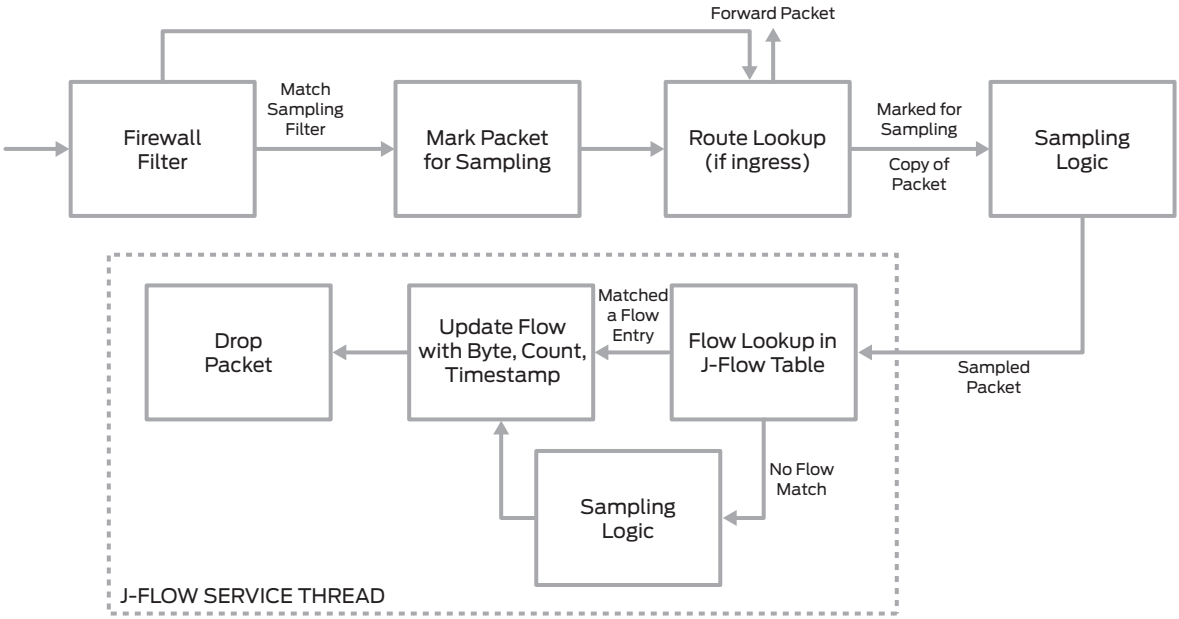

Figure 1: J-Flow components in forwarding plane

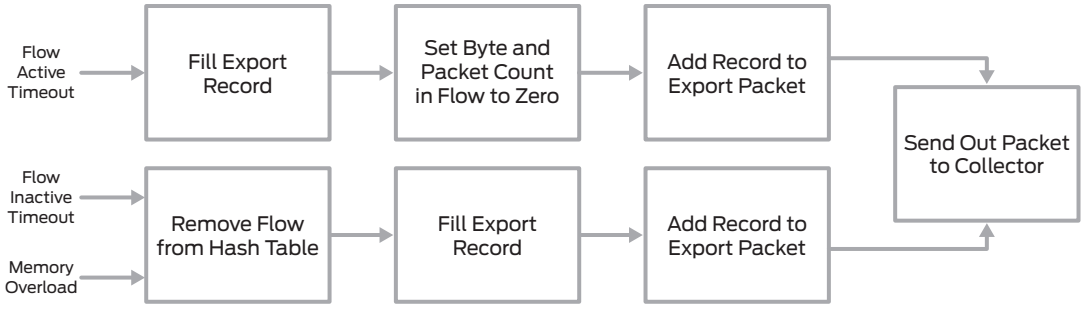

Figure 2: JFLOWD on control plane

Once the inline J-Flow service receives a sampled packet, it updates statistics in its J-Flow table. The packet is mapped to a flow entry, and a new entry is created if there is no preexisting flow. The flow entry packet and byte counts are updated. Depending on the timeout values maintained by JFLOWD daemon on control plane, the flow entry has an associated event scheduled for flow export.

J-Flow v9 Parameters

Sampling Parameters

As you can see, performance of J-Flow is largely dependent on sampling parameters. There are three knobs to control the behavior of J-Flow—sampling rate, sampling run length, and flow timeout values.

- Sampling rate and run length: Finer sampling rate and higher run length increases the granularity of J-Flow at a cost of lower throughput
- Flow timeout values: Flow timeout values control the load of export packets on the CPU. The higher the timeout values, the lower the rate of export packets.

System Overload Behavior

According to RFC 3954, if a system encounters internal constraints like memory exhaustion or flow counter wrapping, flows are forced to delete prematurely and records are exported to a flow collector.

Active and Inactive Timeout

A flow is inactive if it has not seen a packet for a duration that is longer than the "inactive timeout" value specified in the configuration. As long as a flow is not inactive, it is considered active. When inactive timeout is triggered (i.e., the timer expires and finds that the flow has not received any packets for the duration of inactive timeout), the J-Flow service thread deletes the flow from its flow table and generates an export record for that flow.

In a similar manner, active timeout is triggered when the active timer expires and finds that the flow is still active. Active timeout is intended to capture information about long-lived flows. In the absence of an active timeout mechanism, it is possible that a collector will not get any information on a flow until it expires due to inactivity. Hence the goal is to send periodic updates about a flow that has not expired. When a flow sees an active timeout event, its start time stamp is not reset. In this way, the collector can look at a sequence of active timeout export packets and use the start time to identify a long-lived flow.

J-Flow and TCP/IP Protocol Specifics (Flags, Fragments, Anomalies)

J-Flow tracks flows as unidirectional streams of packets. It is not aware of application-level session properties or protocol details. However, there is some minimal awareness of properties of TCP/IP. The following list details some of these specific exceptions:

- TCP flags are accumulated in a running "OR" operation, so that the export record has all of the flags received for a flow. This information can then be used by commercial software applications to provide distributed denial of service (DDoS) detection services.
- J-Flow expires a flow on receiving FIN, or FIN-ACK, or register suppression time (RST). It then generates an export record.
- Since no IP reassembly is performed by J-Flow, it only looks at non-fragmented packets and packets with a fragment offset of zero (the first fragment in a chain). All subsequent packets in a fragment chain are ignored by J-Flow.

J-Flow v9 Restrictions on the J Series and SRX Series

There are a few J-Flow v9 restrictions on J Series and SRX Series devices.

- As of now, only IPv4 flows are supported. A fix template ipv4-template is configurable.
- J-Flow v9 is not supported on J Series and SRX Series devices operating in a chassis cluster environment.
- J-Flow v9 service is not available for a non default virtual router.
- RE-based sampling is not supported with J-Flow v9.

J-Flow v9 Configuration Example

Configure J-Flow v9 template. (As of now, only IPv4 template is supported.)

```
services {
    flow-monitoring {
        version9 {
            template <template name> {
                ipv4-template;
            }
        }
    }
}
```

External flow collector and its port address are configured. J-Flow v9 template is associated with external flow collector. Up to eight flow collectors can be configured simultaneously.

```
sampling {
    family inet {
        output {
            flow-server <Flow collector> {
                port <Flow collector port>;
                version9 {
                    template {
                        <J-Flow v9 Template>;
                    }
                }
            }
         }
    }
}
```

Inline J-Flow is configured so that sampling and the J-Flow service thread are implemented in the forwarding engine.

```
sampling {
    family inet {
        output {
            inline-jflow {
                source-address <Local IP address>;
            }
        }
    }
}
```

Sampling rate and sampling run length are configured.

```
sampling {
    input {
        rate <Sampling Rate>;
        run-length <Sampling Run Length>;
    }
  }
}
```

And finally, the sampling filter is configured on an interface (or interfaces) in the direction where J-Flow service is required.

```
interfaces {
    <Interface name> {
        unit 0 {
            family inet {
                sampling {
                    < input | output >;
                }
                address <IP address>;
            }
        }
    }
}
```

Only “interested traffic” that matches desired conditions can be sampled and sent to J-Flow processing by applying firewall filtering on the interface.

```
firewall {
    filter <filter name> {
        term <term name> {
            from {
                # match conditions for interested traffic
            }
            then {
                sample;
                accept;
            }
        }
    }
}
interfaces {
    <Interface name> {
        unit 0 {
            family inet {
                filter {
                    < input | output > <filter name>;
                }
                address <IP address>;
            }
        }
    }
}
```

Here we show a sample configuration for the J-Flow v9 template ipv4-test, flow collector 172.19.101.85 (port 2222) with sampling rate 1:100 and run length as 0.

```
set services flow-monitoring version9 template ipv4-test ipv4-template
set forwarding-options sampling input rate 1
set forwarding-options sampling input run-length 0
set forwarding-options sampling family inet output flow-server 172.19.101.85 port
2222
set forwarding-options sampling family inet output flow-server 172.19.101.85
version9 template ipv4-test
set forwarding-options sampling family inet output inline-jflow source-address
172.19.101.132
set interfaces ge-0/0/14 unit 0 family inet sampling input
set interfaces ge-0/0/14 unit 0 family inet address 23.23.23.1/24
```

J-Flow v9 Performance Comparison with v5 and v8

Test Methodology

J-Flow v9 throughput performance is compared with v5 and v8 on the SRX240. RFC 2544 test methodology is simulated in IxAutomate. The test parameters being used are:

1. Packet size 64, 1518
2. Bidirectional 1:1 traffic
3. IP + UDP packets
4. Sampling configured at input of one interface
5. Packet-based configuration
6. Static routing

For each version, the sampling rate is varied (1:1, 1:10, 1:100 and no sampling) and throughput performance for a single flow is noted.

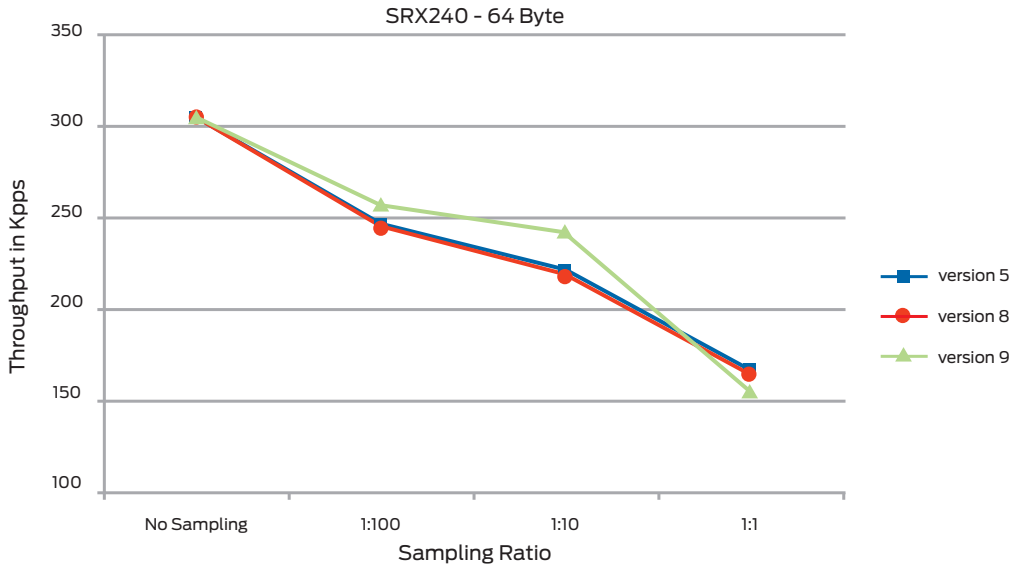

Figure 3: J-Flow SRX240 64 byte sampling

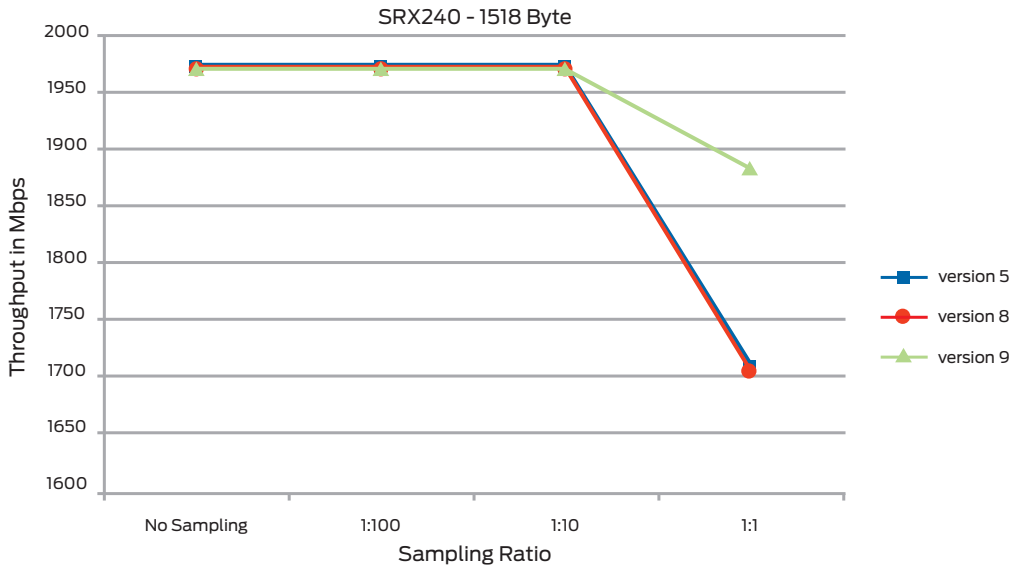

Figure 4: J-Flow SRX240 1518 byte sampling

Summary

With the rapid growth in IP networks has come an increased need for more network bandwidth and better network manageability. J-Flow—Juniper's proprietary flow monitoring service—gives network operators the IP flow information they need for improved visibility across their networks. With J-Flow, network devices such as routers, firewalls, and switches collect flow data and export that information to flow collectors. The collected data provides critical information about traffic in the network and aids in tasks such as billing, traffic engineering, capacity planning, and traffic analysis for peering policy decisions.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

3500204-001-EN Mar 2011 Printed on recycled paper