Configuring Cflowd with CLI

This section provides information to configure cflowd using the command line interface.

Topics in this section include:

Cflowd Configuration Overview

The 7750 SR OS implementation of cflowd supports the option to analyze traffic flow. The implementation also supports the use of traffic/access list (ACL) filters to limit the type of traffic that is analyzed.

Cflowd is not supported on the 7750 SR-1 chassis.

Traffic Sampling

Traffic sampling does not examine all packets received by a router. Command parameters allow the rate at which traffic is sampled and sent for flow analysis to be modified. The default sampling rate is every 1000th packet. Excessive sampling over an extended period of time, for example, more than every 1000th packet, can burden router processing resources.

The following data is maintained for each individual flow in the raw flow cache:

- Source IP address
- Destinations IP address
- Source port
- Destination port
- Input interface
- Output interface
- IP protocol
- TCP flags
- First timestamp (of the first packet in the flow)
- Last timestamp (timestamp of last packet in the flow prior to expiry of the flow)
- Source AS number for peer and origin (taken from BGP)
- Destination AS number for peer and origin (taken from BGP)
- IP next hop
- BGP next hop
- ICMP type and code
- IP version
- Source prefix (from routing)
- Destination prefix (from routing)
- MPLS label stack from label 1 to 6

Within the raw flow cache, the following characteristics are used to identify an individual flow:

- Ingress interface
- Source IP address
- Destination IP address
- Source transport port number
- Destination transport port number
- IP protocol type
- IP TOS byte
- Virtual router id
- ICMP type and code
- MPLS labels

The 7750 SR OS implementation allows you to enable cflowd either at the interface level or as an action to a filter. By enabling cflowd at the interface level, all IP packets forwarded by the interface are subject to cflowd analysis. By setting cflowd as an action in a filter, only packets matching the specified filter are subject to cflowd analysis. This provides the network operator greater flexibility in the types of flows that are captured.

Collectors

A collector defines the data flow for exporting sampled data from the cache. A maximum of 5 collectors can be configured. Each collector is identified by a unique IP address and UDP port value. Each collector can only export traffic in one version type, either V5, V8, V9, or V10.

The parameters within a collector configuration can be modified or the defaults retained.

The autonomous-system-type command defines whether the autonomous system information to be included in the flow data is based on the originating AS or external peer AS of the flow.

Aggregation

V8 aggregation allows for flow data to be aggregated into larger, less granular flows. Use aggregation commands to specify the type of data to be collected.

The following aggregation schemes are supported:

- AS matrix — Flows are aggregated based on source and destination AS and ingress and egress interface.

- Protocol-port — Flows are aggregated based on the IP protocol, source port number, and destination port number.
- Source prefix — Flows are aggregated based on source prefix and mask, source AS, and ingress interface.
- Destination prefix — Flows are aggregated based on destination prefix and mask, destination AS, and egress interface.
- Source-destination prefix — Flows are aggregated based on source prefix and mask, destination prefix and mask, source and destination AS, ingress interface and egress interface.
- Raw — Flows are not aggregated and are sent to the collector in a V5 record.

Basic Cflowd Configuration

This section provides information to configure cflowd and configuration examples of common configuration tasks. In order to sample traffic, the minimal cflowd parameters that need to be configured are:

- Cflowd must be enabled.
- At least one collector must be configured and enabled.
- Sampling must be enabled on either:
    → An IP filter entry and applied to a service or an port.
    → An interface applied to a port.

The following example displays a cflowd configuration.

```
A:ALA-1>config>cflowd# info detail
---------------------------------------------
        active-timeout 30
        cache-size 65536inactive-timeout 15
        overflow 1
        rate 1000
        collector 10.10.10.103:2055 version 9
            no aggregation
            autonomous-system-type origin
            description "V9 collector"
            no shutdown
        exit
        template-retransmit 330
        exit
        no shutdown
---------------------------------------------
A:ALA-1>config>cflowd#
```

Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure cflowd and provides the CLI commands. In order to begin traffic flow sampling, cflowd must be enabled and at least one collector must be configured.

Global Cflowd Components

The components common (global) to all instances of cflowd include the following parameters:

- Active timeout
- Inactive timeout
- Cache size
- Overflow
- Rate
- Template retransmit

Configuring Cflowd

Use the CLI syntax displayed below to perform the following tasks:

CLI Syntax:
```
config>cflowd#
    active-timeout minutes
    cache-size num-entries
    inactive-timeout seconds
    template-retransmit seconds
    overflow percent
    rate sample-rate
    collector ip-address[:port] {version [5 | 8 | 9 |10]}
        aggregation
            as-matrix
            destination-prefix
            protocol-port
            raw
            source-destination-prefix
            source-prefix
        template-set {basic | mpls-ip}
        autonomous-system-type [origin | peer]
        description description-string
        no shutdown
    no shutdown
```

Enabling Cflowd

Cflowd is disabled by default. Executing the command configure cflowd will enable cflowd, by default cflowd is not shutdown but must be configured including at least one collector to be active.

Use the following CLI syntax to enable cflowd:

CLI Syntax: `config# cflowd`
            `no shutdown`

The following example displays the default values when cflowd is initially enabled. No collectors or collector options are configured.

```
A:ALA-1>config# info detail
...
#----------------------------------------
echo "Cflowd Configuration"
#----------------------------------------
    cflowd
        active-timeout 30
        cache-size 65536
        inactive-timeout 15
        overflow 1
        rate 1000
        template-retransmit 600
        no shutdown
    exit
#----------------------------------------
A:ALA-1>config#
```

Configuring Global Cflowd Parameters

The following cflowd parameters apply to all instances where cflowd (traffic sampling) is enabled.

Use the following CLI commands to configure cflowd parameters:

CLI Syntax: `config>cflowd#`
`active-timeout minutes`
`cache-size num-entries`
`inactive-timeout seconds`
`overflow percent`
`rate sample-rate`
`template-retransmit seconds`
`no shutdown`

The following example displays a common cflowd component configuration:

```
A:ALA-1>config>cflowd# info
#----------------------------------------
        active-timeout 20
        inactive-timeout 10
        overflow 10
        rate 100
#----------------------------------------
A:ALA-1>config>cflowd#
```

Configuring Cflowd Collectors

To configure cflowd collector parameters, enter the following commands:

CLI Syntax: `config>cflowd#`
```
    collector ip-address[:port] [version version]
        aggregation
            as-matrix
            destination-prefix
            protocol-port
            raw
            source-destination-prefix
            source-prefix
        autonomous-system-type [origin | peer]
        description description-string
        no shutdown
        template-set {basic | mpls-ip}
```

The following example displays a basic cflowd configuration:

```
A:ALA-1>config>cflowd# info
----------------------------------------
active-timeout 20
        inactive-timeout 10
        overflow 10
        rate 100
        collector 10.10.10.1:2000 version 8
            aggregation
                as-matrix
                raw
            exit
            description "AS info collector"
        exit
        collector 10.10.10.2:5000 version 8
            aggregation
                protocol-port
                source-destination-prefix
            exit
            autonomous-system-type peer
            description "Neighbor collector"
        exit
----------------------------------------
A:ALA-1>config>cflowd#
```

Version 9 Collector example:

```
collector 10.10.10.9:2000 version 9
          description "v9collector"
          template-set mpls-ip
          no shutdown
```

```
exit
```

Version 9 and Verison 10 Templates

If the collector is configured to use either version 9 or 10 formats, the flow data is sent to the designated collector using one of the pre-defined templates. The template used is based on the type of flow for which the data was collected(IPv4, IPv6, or MPLS), and the configuration of the template-set parameter. The following table indicates the relationship between these values and the corresponding template used to export the flow data.

Table 12: Template-Set

Traffic type	Basic	MPLS-IP
IPv4	Basic IPv4	MPLS-IPv4
IPv6	Basic IPv6	MPLS-IPv6
MPLS	Basic MPLS	MPLS-IP

Basic IPv4 Template:

```
0    IPv4 Src Addr (8)
0    IPv4 Dest Addr (12)
0    IPv4 Nexthop (15)
0    BGP Nexthop (18)
0    Iingress Interface (10)
0    Egress Interface (14)
0    Packet Count (2)
0    Byte Count (1)
0    Start Time (22)
0    End Time (21)
0    Flow Start Milliseconds (152)
0    Flow End Milliseconds (153)
0    Src Port (7)
0    Dest Port (11)
0    TCP control Bits (Flags) (6)
0    IPv4 Protocol (4)
0    IPv4 TOS (5)
0    IP version (60)
0    ICMP Type & Code (32)
0    BGP Source ASN (16)
0    BGP Dest ASN (17)
0    Source IPv4 Prefix Length (9)
0    Dest IPv4 Prefix Length (13)
```

MPLS-IPv4 Template:

```
0    IPv4 Src Addr (8)
```

```
0    IPv4 Dest Addr (12)
0    IPv4 Nexthop (15)
0    BGP Nexthop (18)
0    Ingress Interface (10)
0    Egress Interface (14)
0    Packet Count (2)
0    Byte Count (1)
0    Start Time (22)
0    End Time (21)
0    Flow Start Milliseconds (152)
0    Flow End Milliseconds (153)
0    Src Port (7)
0    Dest Port (11)
0    TCP control Bits (Flags) (6)
0    IPv4 Protocol (4)
0    IPv4 TOS (5)
0    IP version (60)
0    ICMP Type & Code (32)
0    BGP Source ASN (16)
0    BGP Dest ASN (17)
0    Source IPv4 Prefix Length (9)
0    Dest IPv4 Prefix Length (13)
0    MPLS Label 1 (70)
0    MPLS Label 2 (71)
0    MPLS Label 3 (72)
0    MPLS Label 4 (73)
0    MPLS Label 5 (74)
0    MPLS Label 6 (75)
```

Basic-IPv6 Template:

```
0    IPv6 Src Addr (27)
0    IPv6 Dest Addr (28)
0    IPv6 Nexthop (62)
0    IPv6 BGP Nexthop (63)
0    IPv4 Nexthop (15)
0    IPv4 BGP Nexthop (18)
0    Iingress Interface (10)
0    Egress Interface (14)
0    Packet Count (2)
0    Byte Count (1)
0    Start Time (22)
0    End Time (21)
0    Flow Start Milliseconds (152)
0    Flow End Milliseconds (153)
0    Src Port (7)
0    Dest Port (11)
0    TCP control Bits (Flags) (6)
0    Protocol (4)
0    IPv6 Options Hdr (64)
0    IPv6 Next Header (193)
0    IPv6 Flow Label (31)
0    TOS (5)
0    IP version (60)
0    IPv6 ICMP Type & Code (139)
0    BGP Source ASN (16)
0    BGP Dest ASN (17)
```

```
0    IPv6 Src Mask (29)
0    IPv6 Dest Mask (30)
```

MPLS-IPv6 Template:

```
0    IPv6 Src Addr (27)
0    IPv6 Dest Addr (28)
0    IPv6 Nexthop (62)
0    IPv6 BGP Nexthop (63)
0    IPv4 Nexthop (15)
0    IPv4 BGP Nexthop (18)
0    Ingress Interface (10)
0    Egress Interface (14)
0    Packet Count (2)
0    Byte Count (1)
0    Start Time (22)
0    End Time (21)
0    Flow Start Milliseconds (152)
0    Flow End Milliseconds (153)
0    Src Port (7)
0    Dest Port (11)
0    TCP control Bits (Flags) (6)
0    Protocol (4)
0    IPv6 Option Hdr (64)
0    IPv6 Next Header (193)
0    IPv6 Flow Label (31)
0    TOS (5)
0    IP version (60)
0    IPv6 ICMP Type & Code (139)
0    BGP Source ASN (16)
0    BGP Dest ASN (17)
0    IPv6 Src Mask (29)
0    IPv6 Dest Mask (30)
0    MPLS Label 1 (70)
0    MPLS Label 2 (71)
0    MPLS Label 3 (72)
0    MPLS Label 4 (73)
0    MPLS Label 5 (74)
0    MPLS Label 6 (75)
```

Basic MPLS:

```
0    Start Time (22)
0    End Time (21)
0    Flow Start Milliseconds (152)
0    Flow End Milliseconds (153)
0    Ingress Interface (10)
0    Egress Interface (14)
0    Packet Count (2)
0    Byte Count (1)
0    MPLS Label 1 (70)
0    MPLS Label 2 (71)
0    MPLS Label 3 (72)
0    MPLS Label 4 (73)
0    MPLS Label 5 (74)
0    MPLS Label 6 (75)
```

MPLS-IP flows:

```
0    IPv4 Src Addr (8)
0    IPv4 Dest Addr (12)
0    IPv4 Nexthop (15)
0    IPv6 Src Addr (27)
0    IPv6 Dest Addr (28)
0    IPv6 Nexthop (62)
0    Ingress Interface (10)
0    Egress Interface (14)
0    Packet Count (2)
0    Byte Count (1)
0    Start Time (22)
0    End Time (21)
0    Flow Start Milliseconds (152)
0    Flow End Milliseconds (153)
0    Src Port (7)
0    Dest Port (11)
0    TCP control Bits (Flags) (6)
0    IPv4 Protocol (4)
0    IPv4 TOS (5)
0    IP version (60)
0    ICMP Type & Code (32)
0    MPLS Label 1 (70)
0    MPLS Label 2 (71)
0    MPLS Label 3 (72)
0    MPLS Label 4 (73)
0    MPLS Label 5 (74)
0    MPLS Label 6 (75)
```

Enabling Cflowd on Interfaces and Filters

This section discusses the following cflowd configuration management tasks:

- Dependencies on page 587
- Specifying Cflowd Options on an IP Interface on page 584
  - → Interface Configurations on page 584
  - → Service Interfaces on page 585
- Specifying Sampling Options in Filter Entries on page 586
  - → Interface Configurations on page 584

Specifying Cflowd Options on an IP Interface

When cflowd is enabled on an interface, all packets forwarded by the interface are subject to analysis according to the global cflowd configuration and sorted according to the collector configuration(s).

Refer to Table 13, Cflowd Configuration Dependencies, on page 588 for configuration combinations.

When the cflowd interface option is configured in the **config>router>interface** context, the following requirements must be met to enable traffic sampling on the specific interface:

1. Cflowd must be enabled.
2. At least one cflowd collector must be configured and enabled.
3. The **interface>cflowd interface** option must be selected. For configuration information, refer to the Filter Policy Overview section of the 7750 SR OS Router Configuration Guide.
4. To omit certain types of traffic from being sampled when the interface sampling is enabled, the **config>filter>ip-filter>entry>interface-disable-sample** option may be enabled via an ip-filter or ipv6-filter. The filter must be applied to the service or network interface on which the traffic to be omitted is to ingress the system.

Interface Configurations

CLI Syntax: `config>router>if#`
`cflowd {acl|interface}`
`no cflowd`

Depending on the option selected, either `acl` or `interface`, cflowd extracts traffic flow samples from an IP filter or an interface for analysis. All packets forwarded by the interface are analyzed according to the cflowd configuration.

The `acl` option must be selected in order to enable traffic sampling on an IP filter. Cflowd (`filter-sample`) must be enabled in at least one IP filter entry.

The `interface` option must be selected in order to enable traffic sampling on an interface. If cflowd is not enabled (`no cflowd`) then traffic sampling will not occur on the interface.

Service Interfaces

CLI Syntax: `config>service>vpls` *service-id*`# interface` *ip-int-name*
`cflowd {acl|interface}`

When enabled on a service interface, cflowd collects routed traffic flow samples through a router for analysis. Cflowd is supported on IES and VPRN services interfaces only. Layer 2 traffic is excluded. All packets forwarded by the interface are analyzed according to the cflowd configuration. On the interface level, cflowd can be associated with a filter (ACL) or an IP interface.

Specifying Sampling Options in Filter Entries

Packets are matched against filter entries to determine acceptability. With cflowd, only the first packet of a flow is compared. If the first packet matches the filter criteria, then an entry is added to the cflowd cache. Subsequent packets in the same flow are also sampled based on the cache entry.

Since a filter can be applied to more than one interface (when configured with a **scope template**), the **interface-disable-sample** option is intended to enable or disable traffic sampling on an interface-by-interface basis. The command can be enabled or disabled as needed instead creating numerous filter versions.

To enable for filtr traffic sampling, the following requirements must be met::

1. Cflowd must be enabled globally.

2. At least one cflowd collector must be configured and enabled.

3. On the IP interface being used, the **interface>cflowd acl** option must be selected. (See Interfcace Configuration) For configuration information, refer to the IP Router Confguration Overview section of the 7750 SR OS Router Configuration Guide.

4. On the IP filter being used, the **entry>filter-sample** option must be explicitly enabled for the entries matching the traffic that should be sampled. The default is **no filter-sample**. (See Filter Configuration for more information).

5. The filter must be applied to a service or a network interface. The service or port must be enabled and operational.

Filter Configurations

CLI Syntax: `config>filter>ip-filter>entry#`
`    [no] filter-sample`
`    [no] interface-disable-sample`

When a filter policy is applied to a service or a network interface, sampling can be configured so that traffic matching the associated IP filter entry is sampled when the IP interface is set to cflow ACL mode and the **filter-sample** command is enabled. If cflowd is either not enabled (**no filter-sample**) or set to the **cflowd interface** mode, then sampling does not occur.

When the **interface-disable-sample** command is enabled, then traffic matching the associated IP filter entry is not sampled if the IP interface is set to cflowd ACL mode.

Dependencies

In order for cflowd to be operational, the following requirements must be met:

*   Cflowd must be enabled on a global level. If cflowd is disabled, any traffic sampling instances are also disabled.
*   At least one collector must be configured and enabled in order for traffic sampling to occur on an enabled entity.
*   If a specific collector UDP port is not identified then, by default, flows are sent to port 2055.

Cflowd can also be dependent on the following entity configurations:

*   Interface Configurations on page 584
*   Service Interfaces on page 585
*   Filter Configurations on page 586

Depending on the combination of interface and filter entry configurations determine if and when flow sampling occurs. Table 13 displays the expected results when specific features are enabled and disabled.

Table 13: Cflowd Configuration Dependencies

Interface Setting	router>interface cflowd [acl | interface] Setting	Command ip-filter entry	Expected Results
IP-filter mode	ACL	`filter-sampled`	Traffic matching is sampled at specified rate.
IP-filter mode	ACL	`no filter-sampled`	No traffic is sampled on this interface.
IP-filter mode or cflowd not enabled on interface	ACL	`interface-disable-sample`	Command is ignored. No sampling occurs.
Interface mode	`interface`	`interface-disable-sample`	Traffic matching this IP filter entry is not sampled.
Interface mode	`interface`	`none`	All IP traffic ingressing the interface is subject to sampling.
Interface mode	`interface`	`filter sampled`	Filter level action is ignored. All traffic ingressing the interface is subject to sampling.

Cflowd Configuration Management Tasks

This section discusses the following cflowd configuration management tasks:

Modifying Global Cflowd Components

Cflowd parameter modifications apply to all instances where cflowd or traffic sampling is enabled. Changes are applied immediately. Use the following cflowd commands to modify global cflowd parameters:

CLI Syntax:
```
config>cflowd#
    active-timeout minutes
    no active-timeout
    cache-size num-entries
    no cache-size
    inactive-timeout seconds
    no inactive-timeout
    overflow percent
    no overflow
    rate sample-rate
    no rate
    [no] shutdown
    template-retransmit seconds
    no template-retransmit
```

The following example displays the cflowd command usage to modify configuration parameters:

Example:
```
config>cflowd# active-timeout 60
config>cflowd# no inactive-timeout
config>cflowd# overflow 2
config>cflowd# rate 10
```

The following example displays the common cflowd component configuration:

```
A:ALA-1>config>cflowd# info
#--------------------------------------
        active-timeout 60
        overflow 2
        rate 10
#--------------------------------------
A:ALA-1>config>cflowd#
```

Modifying Cflowd Collector Parameters

Use the following commands to modify cflowd collector and aggregation parameters:

CLI Syntax:
```
config>cflowd#
    collector ip-address[:port] [version version]
    no collector ip-address[:port]
        [no] aggregation
            [no] as-matrix
            [no] destination-prefix
            [no] protocol-port
            [no] raw
            [no] source-destination-prefix
            [no] source-prefix
        [no] autonomous-system-type [origin | peer]
        [no] description description-string
        [no] shutdown
        template-set {basic | mpls-ip}
```

If a specific collector UDP port is not identified then, by default, flows are sent to port 2055.

The following displays basic cflowd modifications:

```
A:ALA-1>config>cflowd# info
----------------------------------------
    active-timeout 60
        overflow 2
        rate 10
        collector 10.10.10.1:2000 version 5
            description "AS info collector"
        exit
        collector 10.10.10.2:5000 version 8
            aggregation
                source-prefix
                raw
            exit
            description "Test collector"
        exit
----------------------------------------
A:ALA-1>config>cflowd#
```