Enabling Source Class and Destination Class Usage

For interfaces that carry IPv4, IPv6, or MPLS traffic, you can maintain packet counts based on the entry and exit points for traffic passing through your network. Entry and exit points are identified by source and destination prefixes grouped into disjoint sets defined as *source classes* and *destination classes*. You can define classes based on a variety of parameters, such as routing neighbors, autonomous systems, and route filters.

Source class usage (SCU) counts packets sent to customers by performing lookup on the IP source address. SCU makes it possible to track traffic originating from specific prefixes on the provider core and destined for specific prefixes on the customer edge. You must enable SCU accounting on both the inbound and outbound physical interfaces, and the route for the source of the packet must be in located in the forwarding table.

NOTE: SCU and DCU accounting do not work with directly connected interface routes. Source class usage does not count packets coming from sources with direct routes in the forwarding table because of software architecture limitations.

Destination class usage (DCU) counts packets from customers by performing lookup of the IP destination address. DCU makes it possible to track traffic originating from the customer edge and destined for specific prefixes on the provider core router.

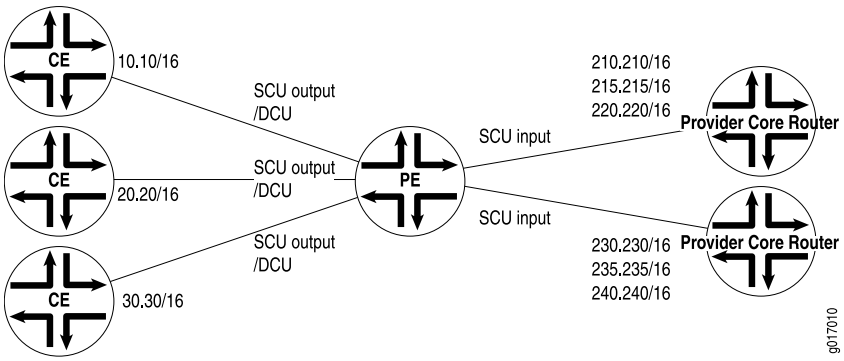
NOTE: SCU and DCU accounting are supported on the J-series routing platform only for IPv4 and IPv6 traffic.

NOTE: We recommend that you stop the network traffic on an interface before you modify the DCU or SCU configuration for that interface. Modifying the DCU or SCU configuration without stopping the traffic might corrupt the DCU or SCU statistics. Before you restart the traffic after modifying the configuration, enter the clear interfaces statistics command.

Figure 1 illustrates an Internet service provider (ISP) network. In this topology, you can use DCU to count packets customers send to specific prefixes. For example, you can have three counters, one per customer, that count the packets destined for prefix 210.210/16 and 220.220/16.

You can use SCU to count packets the provider sends from specific prefixes. For example, you can count the packets sent from prefix 210.210/16 and 215.215/16 and transmitted on a specific output interface.

Figure 1: Prefix Accounting with Source and Destination Classes



You can configure up to 126 source classes and 126 destination classes. For each interface on which you enable destination class usage and source class usage, the JUNOS software maintains an interface-specific counter for each corresponding class up to the 126 class limit.

NOTE: To configure source class and destination class usage, your routing platform must be equipped with the Internet Processor II ASIC.

For transit packets exiting the router through the tunnel, forwarding path features, such as RPF, forwarding table filtering, source class usage, and destination class usage are not supported on the interfaces you configure as the output interface for tunnel traffic. For firewall filtering, you must allow the output tunnel packets through the firewall filter applied to input traffic on the interface that is the next-hop interface towards the tunnel destination.

NOTE:

Performing DCU accounting when an output service is enabled produces inconsistent behavior in the following configuration:

- both scu-input and dcu are configured on the packet input interface
- scu-output is configured on the packet output interface
- interface-services is enabled on the output interface

For an incoming packet with source and destination prefixes matching the SCU and DCU classes respectively configured in the router, both SCU and DCU counters will be incremented. This behavior is not harmful or negative. However, it is inconsistent with non-serviced packets, in that only the SCU count will be incremented (because SCU class ID will override DCU class ID in this case).

To enable packet counting on an interface, include the accounting statement:

```
accounting {
```

```
    destination-class-usage;
    source-class-usage {
      direction;
    }
  }
```

direction can be one of the following:

- input—Configure at least one expected ingress point.
- output—Configure at least one expected egress point.
- input output—On a single interface, configure at least one expected ingress point and one expected egress point.

You can include these statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family (inet | inet6 | mpls)]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family (inet | inet6 | mpls)]

For SCU to work, you must configure at least one input interface and at least one output interface. An incoming packet is counted only once, and SCU takes priority over DCU. This means that when a packet arrives on an interface on which you include the source-class-usage input and destination-class-usage statements in the configuration, and when the source and destination both match accounting prefixes, the JUNOS software associates the packet with the source class only. To ensure the outgoing packet is counted, include the source-class-usage output statements in the configuration of the outgoing interface.

On T-series, M120, and M320 routing platforms, the source class and destination classes are not carried across the platform fabric. The implications of this are as follows:

- On T-series, M120, and M320 platforms, SCU and DCU accounting is performed before the packet enters the fabric.
- On T-series, M120, and M320 routing platforms, DCU is performed before output filters are evaluated. On other M-series platforms, DCU is performed after output filters are evaluated.
- If an output filter drops traffic on T-series, M120, and M320 routing platforms, the dropped packets are included in DCU statistics. If an output filter drops traffic on other M-series platforms, the dropped packets are excluded from DCU statistics.
- On T-series, M120, and M320 platforms, the destination-class and source-class statements are not supported at the [edit firewall family *family-name* > filter *filter-name* term *term-name* from] hierarchy level. On other M-series platforms, these statements are supported.

Once you enable accounting on an interface, the JUNOS software maintains packet counters for that interface, with separate counters for inet, inet6, and mpls protocol families. You must then configure the source class and destination class attributes

in policy action statements, which must be included in forwarding-table export policies.

For a complete discussion about source and destination class accounting profiles, see the *JUNOS Network Management Configuration Guide*. For more information about MPLS, see the *JUNOS MPLS Applications Configuration Guide*.

Examples: Enabling Source Class and Destination Class Usage

Configure DCU and SCU output on one interface:

```
[edit]
interfaces {
   so-6/1/0 {
      unit 0 {
         family inet {
            accounting {
               destination-class-usage;
               source-class-usage {
                  output;
               }
            }
         }
      }
   }
}
```

Complete SCU Configuration

Source routers A and B use loopback addresses as the prefixes to be monitored. Most of the configuration tasks and actual monitoring occur on transit Router SCU.

The loopback address on Router A contains the origin of the prefix that is to be assigned to source class A on Router SCU. However, no SCU processing happens on this router. Therefore, configure Router A for basic Open Shortest Path First (OSPF) routing and include your loopback interface and interface so-0/0/2 in the OSPF process.

Router A

```
[edit]
interfaces {
   so-0/0/2 {
      unit 0 {
         family inet {
            address 10.255.50.2/24;
         }
      }
   }
   lo0 {
      unit 0 {
         family inet {
            address 10.255.192.10/32;
         }
      }
   }
}
protocols {
   ospf {
```

```
        area 0.0.0.0 {
            interface so-0/0/2.0;
            interface lo0.0;
        }
    }
}
```

Router SCU Router SCU handles the bulk of the activity in this example. On Router SCU, enable source class usage on the inbound and outbound interfaces at the [edit interfaces *interface-name* unit *unit-number* family inet accounting] hierarchy level. Make sure you specify the expected traffic: input, output, or, in this case, both.

Next, configure a route filter policy statement that matches the prefixes of the loopback addresses from routers A and B. Include statements in the policy that classify packets from Router A in one group named scu-class-a and packets from Router B in a second class named scu-class-b. Notice the efficient use of a single policy containing multiple terms.

Last, apply the policy to the forwarding table.

```
[edit]
interfaces {
    so-0/0/1 {
        unit 0 {
            family inet {
                accounting {
                    source-class-usage {
                        input;
                        output;
                    }
                }
                address 10.255.50.1/24;
            }
        }
    }
    so-0/0/3 {
        unit 0 {
            family inet {
                accounting {
                    source-class-usage {
                        input;
                        output;
                    }
                }
                address 10.255.10.3/24;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.255.6.111/32;
            }
        }
    }
```

```
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/1.0;
            interface so-0/0/3.0;
        }
    }
}
routing-options {
    forwarding-table {
        export scu-policy;
    }
}
policy-options {
    policy-statement scu-policy {
        term 0 {
            from {
                route-filter 10.255.192.0/24 orlonger;
            }
            then source-class scu-class-a;
        }
        term 1 {
            from {
                route-filter 10.255.165.0/24 orlonger;
            }
            then source-class scu-class-b;
        }
    }
}
```

Router B Just as Router A provides a source prefix, Router B's loopback address matches the prefix assigned to scu-class-b on Router SCU. Again, no SCU processing happens on this router, so configure Router B for basic OSPF routing and include your loopback interface and interface so-0/0/4 in the OSPF process.

```
interfaces {
    so-0/0/4 {
        unit 0 {
            family inet {
                address 10.255.10.4/24;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.255.165.226/32;
            }
        }
    }
}
protocols {
    ospf {
        area 0.0.0.0 {
```

```
        interface so-0/0/4.0;
        interface lo0.0;
      }
    }
  }
```

Enabling Packet Counting for Layer 3 VPNs

You can use SCU and DCU to count packets on Layer 3 VPNs. To enable packet counting for Layer 3 VPN implementations at the egress point of the MPLS tunnel, you must configure a virtual loopback tunnel interface (vt) on the PE router, map the virtual routing and forwarding (VRF) instance type to the virtual loopback tunnel interface, and send the traffic received from the VPN out the source class output interface, as shown in the following example:

1. Configure a virtual loopback tunnel interface on a provider edge router equipped with a tunnel PIC:

```
[edit interfaces]
vt-0/3/0 {
  unit 0 {
    family inet {
      accounting {
        source-class-usage {
          input;
        }
      }
    }
  }
}
```

2. Map the VRF instance type to the virtual loopback tunnel interface.

   For SCU and DCU to work, you must not include the vrf-table-label statement at the [edit routing-instances *instance-name*] hierarchy level.

```
[edit routing-instances]
VPN-A {
  instance-type vrf;
  interface at-2/1/1.0;
  interface vt-0/3/0.0;
  route-distinguisher 10.255.14.225:100;
  vrf-import import-policy-A;
  vrf-export export-policy-A;
  protocols {
    bgp {
      group to-r4 {
        local-address 10.27.253.1;
        peer-as 400;
        neighbor 10.27.253.2;
      }
    }
  }
}
```

3. Send traffic received from the VPN out the source class output interface:

```
[edit interfaces]
```

```
at-2/1/0 {
    unit 0 {
        family inet {
            accounting {
                source-class-usage {
                    output;
                }
            }
        }
    }
}
```

For more information about VPNs, see the *JUNOS VPNs Configuration Guide*. For more information about virtual loopback tunnel interfaces, see the *JUNOS Services Interfaces Configuration Guide*.