Intelligent Traffic Control

Before using the procedures in this chapter, it is recommended that you select the configuration example that best meets your service model, and configure the required elements as per that model.

This chapter contains the following topics:

Overview

Intelligent Traffic Control (ITC) enables you to configure a set of customizable policy definitions that enforce and manage service level agreements for a subscriber profile, thus enabling you to provide differentiated levels of services for native and roaming subscribers.

In 3GPP2 service ITC uses a local policy look-up table and permits either static EV-DO Rev 0 or dynamic EV-DO Rev A policy configuration.

Important ITC includes the class-map, policy-map and policy-group commands. Currently ITC does not include an external policy server interface.

ITC provides per-subscriber/per-flow traffic policing to control bandwidth and session quotas. Flow-based traffic policing enables the configuring and enforcing bandwidth limitations on individual subscribers, which can be enforced on a per-flow basis on the downlink and the uplink directions.

Flow-based traffic policies are used to support various policy functions like Quality of Service (QoS), and bandwidth, and admission control. It provides the management facility to allocate network resources based on defined traffic-flow, QoS, and security policies.

ITC and EV-DO Rev A in 3GPP2 Networks

Important The Ev-Do Rev is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

You can configure your system to support both EV-DO Rev A and ITC. ITC uses flow-based traffic policing to configure and enforce bandwidth limitations per subscriber. Enabling EV-DO Rev A with ITC allows you to control the actual level of bandwidth that is allocated to individual subscriber sessions and the application flows within the sessions.

For more information on EV-DO Rev A, refer to the *Policy-Based Management and EV-DO Rev A* chapter. For setting the DSCP parameters to control ITC functionality, refer to the *Traffic Policy-Map Configuration Mode Commands* chapter in the *Command Line Reference*.

Bandwidth Control and Limiting

Bandwidth control in ITC controls the bandwidth limit, flow action, and charging action for a subscriber, application, and source/destination IP addresses. This is important to help limit bandwidth intensive applications on a network. You can configure ITC to trigger an action to drop, lower-ip-precedence, or allow the flow when the subscriber exceeds the bandwidth usage they have been allotted by their policy.

Licensing

The Intelligent Traffic Control is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

How it Works

ITC enables you to configure traffic policing on a per-subscriber/per-flow basis with the potential to manipulate Differentiated Services Code Points (DSCPs), queue redirection (for example, move traffic to a Best Effort (BE) classification), or drop profile traffic.

In flow-based traffic policies, policy modules interact with the system through a set of well defined entry points, provide access to a stream of system events, and permit the defined policies to implement functions such as access control decisions, QoS enforcement decisions, etc.

Traffic policing can be generally defined as

policy: condition >> action

- **condition**: Specifies the flow-parameters like source-address, destination-address, source-port, destination-port, protocol, etc. for ingress and/or egress packet.

- **action**: Specifies a set of treatments for flow/packet when condition matches. Broadly these actions are based on:
  - Flow Classification: Each flow is classified separately on the basis of source-address, destination-address, source-port, destination-port, protocol, etc. for ingress and/or egress packet. After classification access-control allowed or denied by the system.
  - QoS Processing for individual flow and DSCP marking: Flow-based traffic policing is implemented by each flow separately for the traffic-policing algorithm. Each flow has its own bucket (burst-size) along with committed data rate and peak data rate. A Token Bucket Algorithm (a modified trTCM) [RFC2698] is used to implement this flow-based QoS traffic policing feature.

    Refer to the *Traffic Policing and Shaping* chapter for more information on Token Bucket Algorithm.

Configuring Flow-based Traffic Policing

Traffic Policing is configured on a per-subscriber basis for either locally configured subscribers on the system or subscriber profiles configured on a remote RADIUS server.

Flow-based traffic policy is configured on the system with the following building blocks:

- Class Maps: The basic building block of a flow-based traffic policing. It is used to control over the packet classification.
- Policy Maps: A more advanced building block for a flow-based traffic policing. It manages admission control based on the Class Maps and the corresponding flow treatment based on QoS traffic-police or QoS DSCP marking.
- Policy Group: This is a set of one or more Policy Maps applied to a subscriber. it also resolves the conflict if a flow matches to multiple policies.

This section provides instructions for configuring traffic policies and assigning to local subscriber profiles on the system.

For information on how to configure subscriber profiles on a remote RADIUS server, refer to the *StarentVSA* and *StarentVSA1* dictionary descriptions in the *AAA and GTP Interface Administration and Reference*.

Important This section provides the minimum instruction set for configuring flow-based traffic policing on an AGW service. Commands that configure additional properties are provided in the *Command Line Interface Reference*.

These instructions assume that you have already configured the system-level configuration as described in product administration guide.

To configure the flow-based traffic policing on an AGW service:

1. Configure the traffic class maps on the system to support flow-based traffic policing by applying the example configuration in Configuring Class Maps, on page 4.
2. Configure the policy maps with traffic class maps on the system to support flow-based traffic policing by applying the example configuration in Configuring Policy Maps, on page 5.

3. Configure the policy group with policy maps on the system to support flow-based traffic policing by applying the example configuration in Configuring Policy Groups, on page 5.
4. Associate the subscriber profile with policy group to enable flow-based traffic policing for subscriber by applying the example configuration in Configuring a Subscriber for Flow-based Traffic Policing, on page 6.
5. Verify your flow-based traffic policing configuration by following the steps in Verifying Flow-based Traffic Policing Configuration, on page 6.
6. Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring Class Maps

This section describes how to configure Class Maps on the system to support Flow-based Traffic Policing.

Important In this mode classification match rules added sequentially with **match** command to form a Class-Map. To change and/or delete or re-add a particular rule user must delete specific Class-Map and re-define it.

```
configure
      context <vpn_context_name> [ -noconfirm ]
            class-map name <class_name> [ match-all | match-any ]
                  match src-ip-address <src_ip_address> [ <subnet_mask> ]
                  match dst-ip-address <dst_ip_address> [ <subnet_mask> ]
                  match source-port-range <initial_port_number> [ to
<last_port_number> ]
                 match dst-port-range <initial_port_number> [ to <last_port_number>
 ]
                  match protocol [ tcp | udp | gre | ip-in-ip ]
                  match ip-tos <service_value>
                  match ipsec-spi <index_value>
                  match packet-size [ gt | lt ] <size>
                  end
```

Notes:

- <*vpn_context_name*> is the name of the destination context in which you want to configure the flow-based traffic policing.
- <*class_name*> is the name of the traffic class to map with the flow for the flow-based traffic policing. A maximum of 32 class-maps can be configured in one context.
- For description and variable values of these commands and keywords, refer to the *Class-Map Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Configuring Policy Maps

This section provides information and instructions for configuring the policy maps on the system to support flow-based traffic policing.

```
configure
     context <vpn_context_name>
          policy-map name <policy_name>
               class <class_name>
               type { static | dynamic }
               access-control { allow | discard }
               qos traffic-police committed <bps> peak <bps> burst-size
<byte> exceed-action { drop | lower-ip-precedence | allow } violate-action
 { drop | lower-ip-precedence | allow }
               qos encaps-header dscp-marking [ copy-from-user-datagram
| <dscp_code> ]
               end
```

Notes:

- <*vpn_context_name*> is the name of the destination context in which is configured during Class-Map configuration for flow-based traffic policing.
- <*policy_name*> is the name of the traffic policy map you want to configure for the flow-based traffic policing. A maximum of 32 policy maps can be configured in one context.
- <*class_name*> is the name of the traffic class to map that you configured in *Configuring Class Maps* section for the flow-based traffic policing.
- For description and variable values of these commands and keywords, refer to the *Traffic Policy-Map Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Configuring Policy Groups

This section provides information and instructions for configuring the policy group in a context to support flow-based traffic policing.

```
configure
     context <vpn_context_name>
          policy-group name <policy_group>
               policy <policy_map_name> precedence <value>
               end
```

Notes:

- <*vpn_context_name*> is the name of the destination context which is configured during Class-Map configuration for flow-based traffic policing.
- <*policy_group*> is name of the traffic policy group of policy maps you want to configure for the flow-based traffic policing. A maximum of 32 policy groups can be configured in one context.
- <*policy_map_name*> is name of the traffic policy you configured in *Configuring Policy Maps* section for the flow-based traffic policing. A maximum of 16 Policy Maps can be assigned in a Policy Group.

- For description and variable values of these commands and keywords, refer to the *Traffic Policy-Map Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Configuring a Subscriber for Flow-based Traffic Policing

This section provides information and instructions for configuring the subscriber for Flow-based Traffic Policing.

```
configure
      context <vpn_context_name>
            subscriber name <user_name>
                  policy-group <policy_group> direction [ in | out ]
                  end
```

Notes:

- <*vpn_context_name*> is the name of the destination context configured during Class-Map configuration for flow-based traffic policing.
- <*user_name*> is the name of the subscriber profile you want to configure for the flow-based traffic policing.
- <*policy_group*> is name of the traffic policy group you configured in *Configuring Policy Groups* section for the flow-based traffic policing. A maximum of 16 Policy groups can be assigned to a subscriber profile.
- For description and variable values of these commands and keywords, refer to the *Traffic Policy-Group Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Verifying Flow-based Traffic Policing Configuration

Verify that your flow-based traffic policing is configured properly by entering the following command in Exec Mode:
show subscribers access-flows full

The output of this command displays flow-based information for a subscriber session.