Application Assurance — App-Profile, ASO and Control Policies

In This Chapter

This section provides information about Application Assurance (AA) app-profile, Application Service Options (ASOs) and control policy configurations.

Topics in this section include:

Applicability

This example is applicable to all 7750, 7450 and 7750-SRc chassis supporting Application Assurance and was tested on SR OS release 12.0.R4.

It is recommended to use the Alcatel-Lucent AppDB prior to configuring traffic control policies. The AppDB is a default configuration file to define all of the applications of interest, including all of the relevant application-groups, applications and app-filters to classify traffic, and can be obtained through Alcatel-Lucent's support organization.

Summary

In addition to providing valuable traffic analysis and statistics information using the Alcatel-Lucent 7750 Service Router (SR) or 7450 Ethernet Service Switch (ESS) and Application Assurance (AA), one of the key objectives of the AA solution is to provide the tools to manage subscriber traffic at the application level. Examples of traffic management actions include:

- Throttling low priority bandwidth hungry applications during peak hours.
- Prioritizing and remarking selected applications.
- Implementing a walled-garden environment providing open access to selected free web services only, redirecting all other requests from unregistered subscribers to a registration portal with payment services.
- Enrich HTTP Header with subscriber identification parameters to offer subscribers transparent access to premium content.
- In browser notification which triggers the display of administrative, informational or promotional messages in selected browser-sessions.
- Stateful session filtering with Application Level Gateway (ALG) support to protect subscribers against unsolicited flows.
- Parental control services interworking with an external Internet Content Adaptation Protocol (ICAP) server for rating the requested web sites.

Application traffic control policies can be applied as global policies for all subscribers, or they can be activated for individual subscribers or groups of subscribers.

This example describes the basics of activating Application Assurance on a given subscriber through the use of App-Profile and demonstrates the use of static or dynamic traffic control policies using Application Service Options (ASOs) and Application QoS Policies (AQP). It also provides detailed information for configuring Bandwidth, Flow-Count and Flow-Rate Policing including Time of Day (ToD) policing. Other policy control actions can be found in the Advanced Configuration Guide or in the MS-ISA User Guide.

Configuration

Activation of AA Services

App-Profile

Application profiles (app-profile) enable application assurance services for a given Enhanced Subscriber Management (ESM), Distributed Subscriber Management (DSM), or transit subscriber, or for a SAP or spoke SDP which are commonly referred to as **AA-subscribers** (**AA-sub)**. Each app-profile is unique in the system and defines the services that the AA subscriber will receive.

Assigning an app-profile to an ESM subscriber affects every host of that subscriber. Similarly, applying an app-profile to a SAP/spoke SDP will affect all traffic within that SAP/spoke SDP.

App-profiles are defined at the AA group partition level (in case of a partitioned ISA-AA group), see the configuration example below:

```
A:BNG# configure
    application-assurance group 1:1 policy
        app-profile "1-1/15M" create
            description "App-Profile Description"
            divert
            characteristic "Parental Control" value "enabled"
            capacity-cost 15
        exit
```

The app-profile parameters are:

- **divert** — Diverts all traffic from and to this subscriber to an ISA-AA. Configuring **no divert** effectively disables all AA services for subscribers using this app-profile. Default value: **no divert**.
- **characteristic** [<*characteristic-name*> **value** <*value-name*>] — one or more optional ASO service characteristics can be used to apply an AA control policy to the subscriber.
- **capacity-cost** <*cost*> — An application profile capacity cost is used to load balance AA subscribers across multiple ISA-AA cards. A common practice is to define a cost proportional to the expected peak BW for the subscribers using this profile (in Kbps or Mbps). The capacity cost is out of the scope of this example. The range is 1 to 65535, default 1.

This app-profile example uses the following naming convention:

<*group-id*>-<*partition-id*>/<*BW*>M where

- <*group-id*> — The ISA-AA group ID on which this profile is created.
- <*partition-id*> — The AA partition ID on which this profile is created.
- <*BW-label*> — Defines the maximum bandwidth used by the subscriber, which is used for aa-subscriber cost load balancing and subscriber rate limiting. The **M** stands for Mbps.

In general the operator can choose to use either ASO characteristics override or multiple app-profiles to apply different AA QoS policies to ESM Subscribers or Business VPN sites. For flexibility and scale it is recommended to use ASO overrides whenever possible. This is described in more details below.

Note: Prior to using special characters in a policy object name the operator should verify the list of special characters supported by the 5620 SAM; for instance the 5620 SAM does not support the use of ":" in the app-profile name therefore it should be avoided.

Residential and Wi-Fi Services

The app-profile can be assigned or modified for ESM, DSM or Transit IP subscribers either at subscriber creation time or while the subscriber is in service:

- Subscriber creation — An app-profile can be assigned at subscriber creation time through RADIUS, DHCP Option 82, Local User Database, static configuration or through a default app-profile.
- In service app-profile modification — An app-profile can be dynamically modified in service through a RADIUS Change of Authorization (CoA). From software release 12.0.R1 an app-profile can also be dynamically modified in service through Gx.

In case no app-profile is returned at subscriber creation by RADIUS, LUDB or DHCP, or when no static configuration is present, the system can apply a default app-profile if configured within the subscriber group-interface (or MSAP policy) sub-sla-mgmt:

```
sub-sla-mgmt
 def-app-profile "1-1/15M"
exit
```

Business VPN and other Service Interfaces

App-profiles are statically assigned to a given SAP, spoke SDP or transit prefix VPN site via the 5620 SAM or CLI.

The following configuration shows how to enable application assurance on a SAP or spoke SDP in a business VPRN service:

```
A:PE>config>service# vprn 100 customer 1 create
 description "L3 Service Customer 1"
 interface "to-site1" create
     address 192.168.1.1/24
     sap 1/1/10:11 create
          app-profile "1-1/15M"
     exit
interface "to-site2" create
     address 192.168.2.1/24
     spoke-sdp 12:100 create
          app-profile "1-1/15M"
     exit
no shutdown
```

Defining Application Service Options

ASOs for Traffic Control - Introduction

To determine which application control policies need to be applied to a AA-subscriber, an app-profile with a number of service characteristics (ASOs) is associated with each subscriber. These service characteristics are then used as match criteria in AQP policy rules to determine which rules to apply.

Therefore ASOs are service characteristics assigned to a subscriber and are used to identify the traffic control policy rule (AQP) applicable to a subscriber or a group of subscribers.

Most policy rules will be applicable to multiple subscriber profiles; nevertheless it is possible that a specific subscriber requires a dedicated policy.

ASO Characteristics and Values

For each service option that can be used by one or more subscribers, an ASO characteristic should be defined with a number of values that represent all available choices for that service characteristic. The names and values of the ASO characteristics are configurable string values; best practice is to use strings that provide a meaningful description of the service characteristic they represent.

Each ASO characteristic requires a default value and each app-profile inherits the default value of all the ASO characteristics created in a given partition unless a characteristic is referenced directly in the app-profile or overwritten as described below.

ASOs are defined at the AA group partition level (in case of a partitioned ISA-AA group). In the configuration example below two different ASO characteristics are defined: “Parental Control” and “P2P-Sub-DL”:

```
BNG>config>app-assure# group 1:1 policy
app-service-options
   characteristic "Parental Control" create
     value "disabled"
     value "enabled"
     default-value "disabled"
   exit
   characteristic "P2P-Sub-DL" create
     value "500k"
     value "1M"
     value "unlimited"
     default-value "unlimited"
   exit
```

The ASO values and default value of a characteristic can be displayed using a show command:

```
A:BNG# show application-assurance group 1:1 policy app-service-option "P2P-Sub-DL"
===============================================================================
Application-Assurance Application Service Options
===============================================================================
Characteristic "P2P-Sub-DL"
Value                           Default
-------------------------------------------------------------------------------
1M                              No
500k                            No
unlimited                       Yes
===============================================================================
```

When configuring service characteristics for optional service options, it is recommended to configure a default value which will not trigger any AQP policy action (the default value does not match any AQP match criteria) such that the behavior of existing subscribers and app-profiles will not change until the operator specifically configures or signals a non-default characteristic value for the subscriber or the app-profile. In the example above “Parental Control” “disabled” and “P2P-Sub-DL” “unlimited” would have no corresponding AQP by design; therefore if these particular service options were applied to a subscriber they would not match a QoS policy entry.

How to Specify Service Options for AA Subscribers

ASO Assignment in App-Profile

ASOs can be statically assigned in the app-profile; this type of ASO characteristic assignment is typically reserved to the default service options enabled on a large number of subscribers.

Figure 182 shows an example of AA service definition (ASO and app-profile) for a Gold and Bronze service tier definition with the following characteristics:

- Two app-profiles **Gold** and **Bronze**
- **Gold** app-profile — No specific policy actions or ASO characteristics are configured statically in the app-profile.
- **Bronze** app-profile — A specific ASO characteristic and value is assigned to the profile to limit Peer to Peer download traffic to 1Mbps (this example does not show the app-qos-policy nor policer configuration, this will be described later).

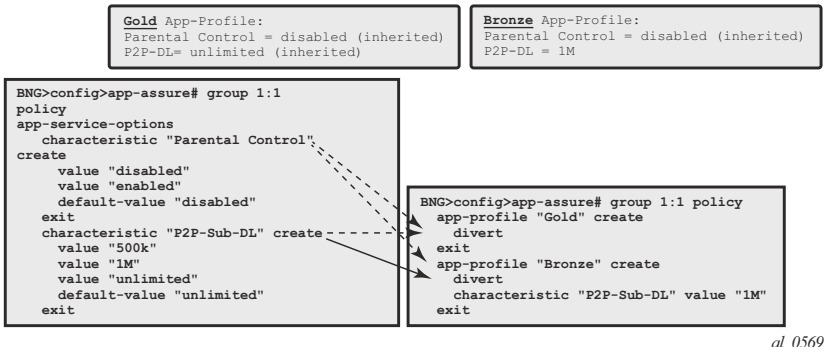

Figure 182: Service Tier Example using ASO, App-Profile and AQP

Each app-profile inherits the default values of all the ASO characteristics defined in a AA group-partition; in the example above this is reason why the app-profile Gold inherits “Parental Control” “disabled” and “P2P-Sub-DL” “unlimited”. The app-profile Bronze inherits “Parental Control” “disabled” while “P2P-Sub-DL” “1M” is assigned to this profile statically.

The operator can identify per app-profile which characteristics values are inherited from their default value and which are statically assigned using the following show command:

```
*A:BNG# show application-assurance group 1:1 policy app-profile "Gold"
    app-profile "Gold" create
        divert
        characteristic "P2P-Sub-DL" inherits default-value "unlimited"
        characteristic "Parental Control" inherits default-value "disabled"
    exit

A:BNG# show application-assurance group 1:1 policy app-profile "Bronze"
    app-profile "Bronze" create
        divert
        characteristic "P2P-Sub-DL" value "1M"
        characteristic "Parental Control" inherits default-value "disabled"
    exit
```

Note: Using ASO overrides, described later, it is possible to implement the same choice of AA service options using a single app-profile.

ASO Overrides per Subscriber via RADIUS or Gx

Prior to SR OS 12.0.R1 the operator can assign (and modify: CoA) the app-profile per ESM or Transit-IP subscribers using the “Alc-App-Prof-Str” [26-6527-45] RADIUS attribute.

SR OS 12.0.R1 added support for ASO characteristic overrides for ESM and Transit-IP subscribers via RADIUS using the attribute “Alc-AA-App-Service-Options” [26-6527-193].This attribute can be returned during the subscriber creation process or while the subscriber is in service through RADIUS CoA. Refer to Alcatel-Lucent SR OS 12.0 RADIUS Attributes Reference Guide for more details related to the use of the AA RADIUS attributes.

An example of a RADIUS CoA message returned to the system to modify both the app-profile and one ASO characteristic is provided below:

```
NAS-Port-Id = "1/1/5:4088"
Framed-IP-Address = 192.168.211.30
Alc-App-Prof-Str = "1-1/15M"
Alc-AA-App-Service-Options = "P2P-Sub-DL=1M"
```

The ASO characteristics and values assigned to a given subscriber (statically via app-profile or overridden) can be displayed using the following show command:

```
A:BNG# show application-assurance group 1:1 aa-sub esm "sub1" summary
===============================================================================
Application-Assurance Subscriber Summary (realtime)
===============================================================================
AA-Subscriber           : sub1 (esm)
ISA assigned            : 1/2
App-Profile             : 1-1/15M
App-Profile divert      : Yes
Capacity cost           : 1
Aarp Instance Id        : N/A
HTTP URL Parameters     : (Not Specified)
Last HTTP Notified Time : 2014/08/07 12:07:47
-------------------------------------------------------------------------------
Traffic                        Octets              Packets                Flows
-------------------------------------------------------------------------------
...
...
-------------------------------------------------------------------------------
Application Service Options (ASO)
-------------------------------------------------------------------------------
Characteristic                  Value                          Derived from
-------------------------------------------------------------------------------
P2P-Sub-DL                      1M                             dyn-override
Parental Control                disabled                       default
===============================================================================
```

In the show command output above, the **derived from** field describes how the characteristics and values are assigned to the subscriber:

- app-profile — The characteristic's value statically configured in the app-profile.
- dyn-override — The characteristic's value received from RADIUS or Gx.
- default — The characteristic's default value inherited (not statically configured in the app-profile nor dynamically modified).

SR OS 12.0.R1 also introduced support for signaling the app-profile or ASO characteristics override via Gx, see Application Assurance — App-Profile, ASO and Control Policies on page 1253 for more details.

ASO Overrides for Business VPN and Other Services

Since SR OS 9.0.R1, ASO characteristic override values can be statically assigned to business VPN SAP, spoke SDP and transit prefix subscribers.

The operator can provision the AA policy override parameters, multiple characteristics overrides per AA-sub can be defined per override policy, see the configuration example below:

```
A:BNG>config>app-assure# group 1:1 policy-override
    policy aa-sub sap 1/1/5:210 create
        characteristic "P2P-Sub-DL" value "1M"
        characteristic "Parental Control" value "enabled"
    exit
```

Application Control Policies

App-QoS-Policy (AQP)

App-Profile / ASO / AQP Workflow Summary

App-profiles enable application assurance services for a given AA-subscriber. Each app-profile is unique in the system and defines the service that the AA subscriber will receive.

To determine which control policies need to be applied to an AA-subscriber, a number of service characteristics (ASO) are associated with each AA-subscriber.

As described earlier, these service characteristics can either be configured directly within the app-profile or assigned using overrides and they are then used as match criteria in AQP policy rules to determine which application policy rules to apply.

The app-qos-policy (AQP) is an ordered list of entries defining policy actions for flows diverted to Application Assurance. Each AQP entry is composed of match criteria and action(s).

Flows are evaluated against all entries of the AA QoS policy defined in the AA group partition that the subscriber app-profile belongs to (in case of a partitioned AA group).

Figure 183 provides a configuration example summary with app-profile, ASO, AQP and policers:

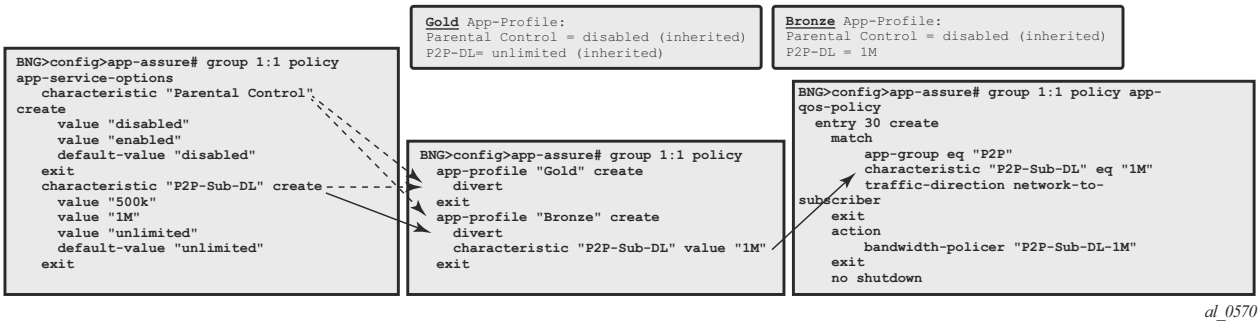

Figure 183: App-Profile, ASO, AQP Workflow Summary

Match and Action Criteria

AQP Match Criteria

Multiple match criteria can be specified per AQP entry in which case the action will only apply to flows that match all criteria. The most common match criteria are: characteristic, application, app-group and charging-group.

The following AA match criteria can be used in an AQP:

- **app-group** {**eq** | **neq**} *<app-group name>*
- **application** {**eq** | **neq**} *<app name>*
- **charging-group** {**eq** | **neq**} *<charging-group-name>*
- **traffic-direction** {**subscriber-to-network**|**network-to-subscriber**|**both**}
- **characteristic** *<characteristic-name>* <**eq**> *<value-name>*: up to 4 characteristics and values per AQP
- **ip-protocol-num** {**eq** | **neq**} *<protocol-id>*
- **src-ip** {**eq** | **neq**} *<ip-address>* or **ip-prefix-list** *<ip-prefix-list-name>*
- **dst-ip** {**eq** | **neq**} *<ip-address>* or **ip-prefix-list** *<ip-prefix-list-name>*
- **src-port** {**eq** | **neq**} *<port-num>* or **range** *<start-port-num><end-port-num>*
- **dst-port** {**eq** | **neq**} *<port-num>* or range *<start-port-num><end-port-num>*
- **dscp** {**eq** | **neq**} *<dscp-name>*
- **aa-sub** *<aa-sub-name>*

AQP Actions

The following AA traffic control policies can be specified in an AQP:

- **drop**
- **bandwidth-policer** *<policer-name>*
- **flow-count-limit** *<policer-name>*
- **flow-rate-limit** *<policer-name>*
- **remark dscp in-profile** *<dscp-*name> **out-profile** *<dscp-name>*
- **remark fc** *<fc-name>*
- **remark priority** *<priority-level>*
- **http-error-redirect** *<redirect-name>*

- **http-redirect** <*redirect-name*> **flow-type** <*flow-type*> — Redirect traffic to a landing page
- **mirror-source** [**all-inclusive**] <*mirror-service-id*>
- **session-filter** <*session-filter-name*> — Session filter firewall
- **url-filter** <*url-filter-name*>: category based URL Filtering using ICAP
- **http-notification** <*http-notification-name*>
- Additional drop actions:
  - **error-drop**: configure a drop action for packets cut-through due to IP packet errors (bad IP checksums, tcp/udp port 0, etc.)
  - **overload-drop**: configure a drop action for packets cut-through due to overload
  - **fragment-drop**: configure a drop action for IP fragmented packets

Default Versus Application-Specific AQP Policies

Application QoS Policy

It usually requires the examination of a few packets to identify the protocol/application of a flow. When AQP entries are defined to match on IP header criteria (IP address, IP prefix list, TCP/UDP Port Number, IP Protocol, DSCP) or application criteria (application, App-Group or charging group), the AQP action will only be applied to matching application flows after a flow has been classified as a given application.

Default QoS Policy

If the AQP entry does not include match criteria against application (application, app-group and charging-group) or IP header information (IP address, IP prefix list, TCP/UDP port number, IP protocol, DSCP) then the AQP policy will be applied to all matching flows starting with the first packet of a flow before protocol and application identification is complete. Such AQPs are called default subscriber policies.

For an AQP to be qualified as a default subscriber policy, the match criteria must be limited to any combination of ASO characteristic values, traffic direction and optional AA subscriber name.

AQP match and actions for the default QoS policy and application QoS policy are summarized in Table 6:

Table 6: Default QoS Policy, Application QoS Policy Table

Policy	AQP Match	AQP Action
Default QoS	ASO characteristic/values traffic direction aa-sub	Remark FC, DSCP, Priority Bandwidth, flow-count, flow-rate policing Session-filter Url-filter Mirror Error-drop, overload-drop, fragment-drop Drop

Table 6: Default QoS Policy, Application QoS Policy Table (Continued)

Policy	AQP Match	AQP Action
Application QoS	ASO characteristic/values traffic direction aa-sub application app-group charging-group IP address, IP Prefix List TCP/UDP Port Number DSCP IP Protocol Number	Remark FC, DSCP, Priority Bandwidth, flow-count, flow-rate policing HTTP Notification HTTP Redirect HTTP Enrichment Mirror Drop

To ensure fair access to the ISA-AA bandwidth and flow resources, it is recommended to configure default AQP policy entries limiting bandwidth and flow resources per AA sub.

Figure 184 shows a default subscriber policy limiting the downstream bandwidth (network-to-subscriber direction) to 25Mbps per subscriber:

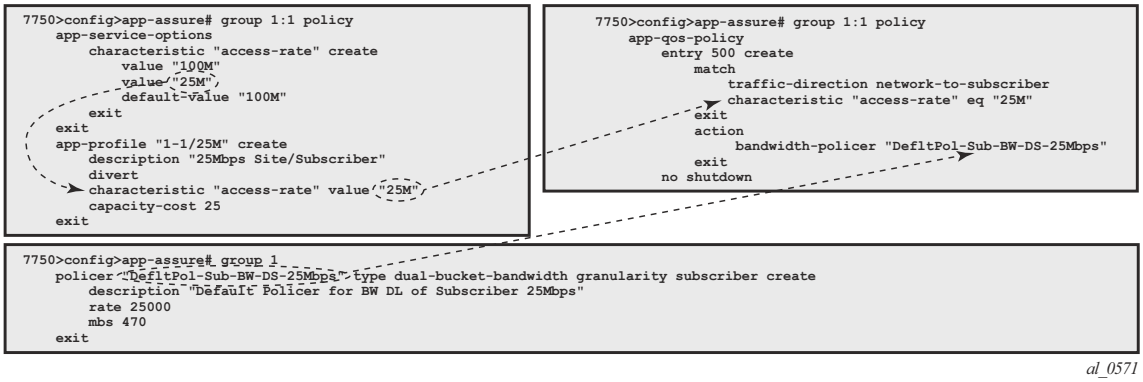

Figure 184: Default Downstream Bandwidth Policing

Implicit Default Subscriber Policy

Session-filter, url-filter, overload-drop, fragment-drop and error-drop can only be used as part of a default subscriber policy; therefore these actions are not compatible with application or IP header match criteria within the same AQP.

AQP Entries Evaluation

Multiple AQP Match Entries Per Flow

A single flow can match multiple AQP entries, in which case multiple actions can be selected based on the AQP entry's order (the lowest number entry has the highest priority); the drop action takes precedence over any other AQP entry. The maximum numbers of actions that can be applied on a single flow are:

- 1 drop action
- Any combination of (applied only if no drop action is selected)
  - Up to 1 mirror action
  - Up to 1 FC, 1 priority and 1 DSCP remark action
  - Up to 4 BW policers (1 single rate AA-Sub, 1 dual rate AA-Sub, 2 single rate system level)
  - Up to 12 flow policers (3 subscriber flow-count, 3 subscriber flow-rate, 3 system flow-count, 3 system flow-rate)
  - Up to 1 HTTP Redirect
  - Up to 1 HTTP Error Redirect
  - Up to 1 HTTP Enrichment
  - Up to 1 URL-Filter
  - Up to 1 HTTP-Notification
  - Up to 1 Session-Filter Firewall
- 1 error-drop
- 1 overload-drop
- 1 fragment-drop

An AQP entry match that would cause the above limits to be exceeded is ignored (no actions from that rule are selected) and the conflict counter for this AQP is incremented.

The operator can display hits and potential conflicts per AQP entry using the following show command:

```
A:BNG# show application-assurance group 1:1 policy app-qos-policy
===============================================================================
Application QOS Policy Table
===============================================================================
Entry         Admin State                    Flow Hits          Flow Conflicts
-------------------------------------------------------------------------------
30            in-service                             0                      0
-------------------------------------------------------------------------------
No. of AQP entries: 1
===============================================================================
```

AQP Evaluation

Flows are evaluated against all entries of the AA QoS Policy at different steps during the lifetime of the flow:

- **Flow creation** — The default subscriber policy AQP entries for matching flows are applied starting with the first packet of a flow so before application identification completes.
- **Application identification completion**— The application QoS policies are applied once flow identification has been completed.
  Note: The default QoS policy entries are applied to the subscriber's flows for packets received before and after application identification is completed.
- **Policy change** — When a configuration change is applied to the AA policy by executing the commit command on the AA group:partition policy, all diverted flows for subscribers using this policy partition will be evaluated again against all AQP entries. This re-evaluation happens as a paced background task; hence AQP control changes may not be applied immediately to all existing flows.

Policing

Policers

AA policer templates are configured as part of the AA Group configuration by specifying the policer name, type and granularity. Policers are unidirectional by definition so that separate policers must be defined per flow direction if the traffic needs to be policed in both directions (a separate AQP for each flow direction is therefore required as well).

The operator can configure the following types of policers:

- Bandwidth Policers
  - Single bucket system level
  - Single bucket AA subscriber level
  - Dual bucket AA subscriber level
- Flow Count Policer: system or AA subscriber level
- Flow Setup-Rate Policer: system or AA subscriber level

Subscriber level policers are instantiated per AA sub, meaning:

- The system automatically uses a dedicated policer for every single subscriber, even when multiple subscribers match the same AQP entry.
- The same policer can be referenced in different AQP entries; in this case all subscribers' flows matching any of these AQP entries are policed by the same subscriber policer. Example: if the same subscriber level policer '1Mbps' is referenced in AQP entry 100 matching application BitTorrent and in AQP entry 110 matching application EDonkey, then the sum of both the BitTorrent and EDonkey traffic cannot exceed 1Mbps.

System level policers on the other hand are shared by all AA subscribers matching a given AQP entry. These policers are typically used in residential and Wi-Fi service deployments to limit the total bandwidth for an application or application group, for all subscribers or for a group of subscribers on the system or partition. An example would be a system level 500Mbps policer to limit the aggregated downstream bandwidth of "Peer to Peer" applications for all subscribers with a "Bronze" app-profile to 500Mbps.

Note: In case multiple ISA-AA cards are used per system, the overall maximum throughput using a system level policer is equal to the policer rate limit times the number of ISA cards in the system.

Bandwidth Policing

Single Bucket Subscriber/System Bandwidth Policer

Single bucket policers police the matching traffic against a configured peak-information-rate (PIR). Traffic above the PIR can be marked as out of profile or dropped.

The configuration template for a single rate bandwidth policer is as follows:

```
BNG>config>app-assure# group 1
    policer <policer-name> type single-bucket-bandwidth
                                  granularity {subscriber|system} create
        description <string>
        rate <pir-rate-in-Kbps>
        mbs <max-burst-size-in-Kbytes>
        adaptation-rule pir {max|min|closest}
        tod-override <tod-override-id>
        action permit-deny|priority-mark
```

where:

- **action** — Defines the action that must be taken by the policer for non-conforming traffic.
- **permit-deny** — Non-conforming packets will be dropped.
- **priority-mark** — Non-conforming traffic will be marked as out of profile (increasing the chances that non-conforming packets will be discarded in case of congestion on the egress queues).
- **rate —** Peak information rate in Kbps.
- **mbs —** Maximum burst size in Kbytes.
- **adaptation-rule pir <max|min|closest>** — The policers work at discrete operational rates supported by the hardware. The adaptation rule specifies how the actual operational policer rate (supported by the hardware) must be selected as compared to the configured PIR. During operation, both the operational and configured rate can be displayed using the operational **show application-assurance group** <*n*> **policer** <*policer-name*> **detail** command.
- **tod-override** — Defines a time of day override policy applicable to a policer, this is described in more detail at the end of the policing section.

A single bucket subscriber level policer configuration example is shown below:

```
BNG>config>app-assure# group 1
    policer "P2P-Sub-DL-1M" type single-bucket-bandwidth granularity subscriber create
        rate 1000
        mbs 19
    exit
```

A single bucket system level policer configuration example is shown below:

```
BNG>config>app-assure# group 1
    policer "P2P-Sys-DL-100M" type single-bucket-bandwidth granularity system create
        rate 100000
        mbs 1875
    exit
```

Dual Bucket Subscriber Bandwidth Policer

Dual-bucket policers police the matching traffic against a configured peak information rate (PIR) and committed information rate (CIR). Traffic below CIR is marked in profile, traffic between CIR and PIR is marked as out of profile, and traffic above the PIR is dropped.

Dual-bucket policers can only be used as subscriber policers; system policers cannot be defined as dual-bucket policers.

The configuration is similar to the single-bucket policer, but adds the configuration of a CIR and a Committed Burst Size (CBS), and the action cannot be configured:

```
BNG>config>app-assure# group 1
    policer <policer-name> type dual-bucket-bandwidth
                                granularity {subscriber|system} create
        description <string>
        rate <pir-rate-in-Kbps> cir <cir-rate-in-Kbps>
        mbs <max-burst-size-in-Kbytes>
        cbs <committed-burst-size-in-Kbytes>
        adaptation-rule pir {max|min|closest} cir {max|min|closest}
```

A dual-bucket subscriber level policer configuration example is shown below:

```
BNG>config>app-assure# group 1
    policer "P2P-Sub-DL-2M-DB" type dual-bucket-bandwidth granularity subscriber create
        rate 2000 cir 1000
        cbs 19
        mbs 38
    exit
```

MBS/CBS Calculation for Bandwidth Policers

The default MBS/CBS value of a bandwidth policer is set to 0. This value can and should be modified by the operator to allow proper interworking with TCP based applications.

The formula to calculate the MBS or CBS buffer size, as documented in RFC 6349, *Framework for TCP Throughput Testing*, is:

Buffer (B) = Rate (bps) / 8 * RTT (s)

For Internet applications it is recommended to use a common Round Trip Time (RTT) of 150 msec.

An example using a single bucket subscriber level policer rate of 10000 Kbps:

MBS (B) = 1,000,000 / 8 * 0.150 = 18750 Bytes or 190 KB.

Note that these policer values may need to be further adjustment depending on the application.

Flow Rate Limit Policer

Flow rate limit policers police the maximum number of new flows that are accepted per second for matching traffic. The configuration is similar to the single-bucket bandwidth policer, with the rate and MBS now expressed in flows/sec and flows, respectively.

```
BNG>config>app-assure# group 1
    policer <policer-name> type flow-rate-limit granularity {subscriber|system} create
          description <string>
          rate <flow-rate-in-flows/sec>
          mbs <max-burst-size-in-flows>
          adaptation-rule pir  {max|min|closest}
          action permit-deny|priority-mark
```

This type of policer is primarily used for the default subscriber AQP policy in order to limit the maximum number of flow/seconds allocated per AA subscriber.

Note that in case the policer is used as part of the default AA subscriber policy then the **priority-mark** action has the effect to cut-through non conformant traffic in the ISA instead of drop using **permit-deny**.

Flow Count Limit Policer

Flow count limit policers police the maximum number of concurrent flows for matching traffic:

```
BNG>config>app-assure# group 1
    policer <policer-name> type flow-count-limit granularity {subscriber|system} create
        description <string>
        action permit-deny|priority-mark
        flow-count <max-number-of-flows>
```

This type of policer is primarily used for the default subscriber AQP policy in order to limit the maximum number of concurrent flows allocated per AA subscriber.

Note that the “priority-mark” has the effect to cut-through non conformant traffic in the ISA instead of drop using “permit-deny”.

Time of Day Policing

Software release 11.0.R1 introduced support for time-of-day (ToD) policer override. Up to 8 override rates with time of day specifications can be defined per policer, this time of day override using the system local time.

ToD overrides are supported for all policer types described in the previous section (bandwidth, flow-count, flow-rate) and can be configured using either daily or weekly patterns.

The configuration of ToD override on daily or weekly basis is shown in the following template:

```
BNG>config>app-assure# group 1
    policer "P2P-Sub-DL-1M-TOD" type single-bucket-bandwidth
                                          granularity subscriber create
        action permit-deny
        rate 1000
        mbs 19
        adaptation-rule pir closest
        tod-override <override-id>
            description <string>
            time-range daily start <start-time> end <end-time>
                                      [on <day> [<day>...(upto 7 max)]]
            time-range weekly start <day,start-time> end <day,end-time>
            rate 2000
            mbs 38
```

where:

- **tod-override** <*override-id*> — Up to 8 override-ids (with value 1-255) can be configured per policer.

- **time-range** — Can be configured to be triggered.
  - On a daily basis at the indicated start/end-time on the specified days.
  - On a weekly basis at the indicated start day+time and end-day+time.
  - Times can be indicated as <hh>:<mm> with a 15-minute granularity for the minutes (mm = 0|15|30|45).

A configuration example for a single bucket system level bandwidth policer with the following ToD-override patterns follows:

- Default Rate Limit: 300Mbps
- Rate Limit override to 100Mbps between 5PM and 10PM
- Rate Limit override to 200Mbps between 10PM and 12PM

```
BNG>config>app-assure# group 1
     policer "P2P-Sys-DL-300M-TOD" type single-bucket-bandwidth
                                          granularity system create
        description "Peer to Peer Policer System level Policer"
        rate 300000
        mbs 5625
        tod-override 1 create
            description "Override busy hour #1"
            time-range daily start 17:00 end 22:00
            rate 100000
            mbs 1875
            no shutdown
        exit
        tod-override 2 create
            description "Override busy hour #1"
            time-range daily start 22:00 end 24:00
            rate 200000
            mbs 3750
            no shutdown
        exit
```

The operator can display which policing rate is applied at any moment in time together with all configured override rates using the following command:

```
show application-assurance group <n> policer <policer-name> detail
```

Design and Configuration Examples

Default AA QoS Policy

To ensure fair access for all subscribers to the ISA-AA resources, and avoid that a disproportionate amount of ISA-AA resources are used by one or more subscribers which are misbehaving or receiving large traffic bursts from the Internet, it is recommended to configure the following three types of subscriber-level default AA QoS policies:

- **A default bandwidth policer** to limit the downstream bandwidth per subscriber (upstream bandwidth is already limited by ESM/SAP access ingress IOM QoS).
- **A default flow count policer** to limit the maximum number of active flows per traffic direction per subscriber. The operator can choose to drop or cut-through non conforming traffic.
- A **default flow rate policer** to limit the maximum flow setup rate per traffic direction per subscriber. The operator can choose to drop or cut-through non conforming traffic.

The minimum set of app-profiles used in a network is typically determined by the different access bandwidth rates; services characteristics are then used for each profile to apply a default QoS policy to limit bandwidth and flow resources accordingly.

In theory, it is possible to configure a set of default policers for every individual access bandwidth rate that is offered to a subscriber. This would however result in a large number of policers and corresponding ASO values plus app-profiles that need to be configured. Therefore, a best practice guideline is to define a small number of bandwidth ranges (not more than five to ten) that cover the full offered access bandwidth spectrum, and define for each bandwidth range a default bandwidth policer plus flow policers with appropriate limits.

As an example, assuming a residential deployment with 2 bandwidth ranges of up to 25Mbps and 100Mbps, the configuration below provides:

- Complete ASO and app-profile configuration.
- Default QoS policy for subscribers in the 25Mbps range including bandwidth.
- Flow count and flow rate policers are configured by default as permit-deny. Non conforming traffic is dropped which is common for residential deployments; alternatively the operator can decide to configure these policers as priority-mark to cut-through traffic in the ISA-AA.

In this example the resources are limited per subscriber based on their access rate maximum speed from which flow count and flow rate are derived.

App-Profile and ASO

The configuration below provides the app-profile and ASO characteristics used for the default subscriber AQP policy for the 25Mbps and 100Mbps access bandwidth range:

```
BNG>config>app-assure# group 1:1 policy
    app-service-options
        characteristic "access-rate" create
            value "100M"
            value "25M"
            default-value "100M"
        exit
    exit
    app-profile "1-1/25M" create
        description "25Mbps Site/Subscriber"
        divert
        characteristic "access-rate" value "25M"
        capacity-cost 25
    exit
    app-profile "1-1/100M" create
        description "100Mbps Site/Subscriber"
        divert
        characteristic "access-rate" value "100M"
        capacity-cost 100
    exit
```

Default Bandwidth Policing – 25Mbps AA-Sub

```
BNG>config>app-assure# group 1
    policer "DefltPol-Sub-BW-DS-25Mbps" type dual-bucket-bandwidth
                                                granularity subscriber create
        description "Deflt downstream BW policer for 25Mbps Subs"
        rate 25000
    mbs
```

The AQP entry below will act as a default AQP policy since it does not include application or IP Header match criteria:

```
BNG>config>app-assure# group 1:1 policy
    app-qos-policy
        entry 500 create
            description "Deflt downstream BW policer for 25Mbps Subs"
            match
                traffic-direction network-to-subscriber
                characteristic "access-rate" eq "25M"
            exit
            action
```

```
                bandwidth-policer "DefltPol-Sub-BW-DS-25Mbps"
            exit
            no shutdown
        exit
```

Note: A similar configuration can be implemented for the 100Mbps access rate service option.

Default Flow-Count-Limit Policing – 25Mbps AA-Sub

```
BNG>config>app-assure# group 1
    policer "DefltPol-Sub-FlowCount-US-25Mbps" type flow-count-limit
                                                granularity subscriber create
        description "Deflt policer to limit active upstream flows for 25Mbps Subs”
        flow-count 10000
        action permit-deny
    exit
    policer "DefltPol-Sub-FlowCount-DS-25Mbps" type flow-count-limit
                                                granularity subscriber create
        description "Deflt policer to limit active downstream flows for 25Mbps Subs”
        flow-count 10000
        action permit-deny
    exit
```

The AQP entry below will act as a default AQP policy since it does not include application or IP Header match criteria:

```
BNG>config>app-assure# group 1:1 policy app-qos-policy
    entry 510 create
        description " Deflt policer to limit active upstream flows for 25Mbps Subs"
        match
            traffic-direction subscriber-to-network
            characteristic "access-rate" eq "25M"
        exit
        action
            flow-count-limit "DefltPol-Sub-FlowCount-US-25Mbps"
        exit
        no shutdown
    exit
    entry 515 create
        description " Deflt policer to limit active downstream flows for 25Mbps Subs"
        match
            traffic-direction network-to-subscriber
            characteristic "access-rate" eq "25M"
        exit
        action
            flow-count-limit "DefltPol-Sub-FlowCount-DS-25Mbps"
        exit
        no shutdown
    exit
```

Note: A similar configuration can be implemented for the 100Mbps access rate service option.

Default Flow-Rate-Limit Policing – 25Mbps AA-Sub

```
BNG>config>app-assure# group 1
    policer "DefltPol-Sub-FlowRate-US-25Mbps" type flow-rate-limit
                                                    granularity subscriber create
        description "Deflt policer to limit upstream flow setup rate for 25Mbps Subs”
        rate 200
        action permit-deny
    exit
    policer "DefltPol-Sub-FlowRate-DS-25Mbps" type flow-rate-limit
                                                  granularity subscriber create
        description "Deflt policer to limit downstr flow setup rate for 25Mbps Subs"
        rate 200
        action permit-deny
    exit
```

The AQP entry below will act as a default AQP policy since it does not include application or IP Header match criteria:

```
BNG>config>app-assure# group 1:1 policy app-qos-policy
    entry 520 create
        description "Deflt policer to limit upstream flow setup rate for 25Mbps Subs"
        match
            traffic-direction subscriber-to-network
            characteristic "access-rate" eq "25M"
        exit
        action
            flow-rate-limit "DefltPol-Sub-FlowRate-US-25Mbps"
        exit
        no shutdown
    exit
    entry 525 create
        description "Deflt policer to limit downstr flow setup rate for 25Mbps Subs"
        match
            traffic-direction network-to-subscriber
            characteristic "access-rate" eq "25M"
        exit
        action
            flow-rate-limit "DefltPol-Sub-FlowRate-DS-25Mbps"
        exit
        no shutdown
    exit
```

Note: A similar configuration can be implemented for the 100Mbps access rate service option.

Application BW Policing (Per Subscriber)

The configuration example below provides a per AA subscriber peer-to-peer rate limit of 1Mbps. It does not include the app-profile configuration since the ASO characteristic and values can be either statically configured within the app-profile or dynamically signaled through RADIUS or Gx using ASO overrides.

AA subscribers with service characteristic "P2P-Sub-DL" value of "1M" will have a bandwidth policer of 1Mbps applied to peer to peer traffic in the network to subscriber direction:

```
BNG>config>app-assure# group 1
    policer "P2P-Sub-DL-1M" type single-bucket-bandwidth granularity subscriber create
         description "Per-subscr BW policer to limit P2P downstream traffic to 1Mbps"
         rate 1000
         mbs 19
         action permit-deny
    exit

BNG>config>app-assure# group 1:1 policy
    app-service-options
        characteristic "P2P-Sub-DL" create
            value "10M"
            value "1M"
            value "unlimited"
            default-value "unlimited"
        exit

BNG>config>app-assure# group 1:1 policy app-qos-policy
    entry 30 create
        description "Per-subscr BW policer to limit P2P downstream traffic to 1Mbps"
        match
            app-group eq "Peer to Peer"
            traffic-direction network-to-subscriber
            characteristic "P2P-Sub-DL" eq "1M"
        exit
        action
            bandwidth-policer "P2P-Sub-DL-1M"
        exit
        no shutdown
    exit
```

Conclusion

This example provides detailed information to properly configure and use app-profiles, ASOs and AQPs to successfully configure application policy control rules using Application Assurance.