Application Assurance Commands

Application Assurance uses system components for some of its functionality. Refer to the following for details on:

- Configuration of Application Assurance Accounting policy including per accounting type record selection and customization of AA subscriber records.
- Configuration of AA ISA IOM QoS.

Generic Commands

description

Syntax **description** *description-string*
no description

Context config>app-assure>aarp
config>aa>group>statistics>aa-sub
config>app-assure>group>cflowd>collector
config>app-assure>group>cflowd>group>cflowd
config>app-assure>group>cflowd>group>cflowd>collector
config>app-assure>group>cflowd>group>cflowd>volume
config>app-assure>group>description
config>app-assure>group>http-enrich
config>app-assure>group>http-error-redirect
config>app-assure>group>http-redirect
config>app-assure>group>ip-prefix-list
config>app-assure>group>policer
config>app-assure>group>policer>tod-override
config>app-assure>group>policy>app-filter>entry
config>app-assure>group>policy>app-group
config>app-assure>group>policy>application
config>app-assure>group>policy>app-profile
config>app-assure>group>policy>app-qos-policy>entry
config>app-assure>group>policy>aqp>entry
config>app-assure>group>policy>aqp>entry>action>url-filter
config>app-assure>group>policy>custom-protocol
config>app-assure>group>policy>transit-ip-policy
config>app-assure>group>tod-override
config>app-assure>group>url-filter
config>app-assure>group>url-filter>icap
config>app-assure>protocol
config>app-assure>rad-acct-plcy
config>isa
config>isa>aa-group
config>app-assure>group>dns-ip-cache>dns-match
config>app-assure>group>gtp>gtp-filter
config>app-assure>group>url-list

Description This command creates a text description which is stored in the configuration file to help identify the content of the entity.

The **no** form of the command removes the string from the configuration.

Default **none**

Parameters *string* — The description character string. Allowed values are any string composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

shutdown

Syntax [**no**] **shutdown**

Context
config>app-assure>aarp
config>app-assure>group>cflowd
config>app-assure>group>cflowd tcp-performance
config>app-assure>group>cflowd volume
config>app-assure>group>cflowd>collector
config>app-assure>group>cflowd>comprehensive
config>app-assure>group>cflowd>rtp-performance
config>app-assure>group>event-log
config>app-assure>group>http-enrich
config>app-assure>group>http-error-redirect
config>app-assure>group>http-redirect
config>app-assure>group>policer>tod-override
config>app-assure>group>policy>app-filter>entry
config>app-assure>group>policy>app-qos-policy>entry
config>app-assure>group>policy>custom-protocol
config>app-assure>group>statistics>protocol
config>app-assure>group>transit-ip-policy>dhcp
config>app-assure>group>transit-ip-policy>radius
config>app-assure>group>transit-ip-policy>transit-auto-create
config>app-assure>group>url-filter
config>app-assure>group>url-filter>icap
config>app-assure>group>wap1x
config>app-assure>protocol

Description This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.

The **shutdown** command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Hardware Commands

card-type

Syntax **card-type** *card-type*
no card-type

Context config>card

Description This mandatory command adds an IOM o the device configuration for the slot. The card type can be preprovisioned, meaning that the card does not need to be installed in the chassis.

A card must be provisioned before an MDA, MCM or port can be configured .

A card can only be provisioned in a slot that is vacant, meaning no other card can be provisioned (configured) for that particular slot. To reconfigure a slot position, use the **no** form of this command to remove the current information.

A card can only be provisioned in a slot if the card type is allowed in the slot. An error message is generated if an attempt is made to provision a card type that is not allowed.

If a card is inserted that does not match the configured card type for the slot, then a medium severity alarm is raised. The alarm is cleared when the correct card type is installed or the configuration is modified.

A high severity alarm is raised if an administratively enabled card is removed from the chassis. The alarm is cleared when the correct card type is installed or the configuration is modified. A low severity trap is issued when a card is removed that is administratively disabled.

Because the IOM-3 integrated card does not have the capability in install separate MDAs, the configuration of the MDA is automatic. This configuration only includes the default parameters such as default buffer policies. Commands to manage the MDA such as **shutdown**, named buffer pool etc will remain in the MDA configuration context.

An appropriate alarm is raised if a partial or complete card failure is detected. The alarm is cleared when the error condition ceases.

Refer to the 7x50 SR OS Interfaces Configuration Guide and the 7450 ESS OS Interface Configuration Guide for information about slots, cards and MDAs.

The **no** form of this command removes the card from the configuration.

Default No cards are preconfigured for any slots.

Parameters *card-type* — The type of card to be configured and installed in that slot.

Values iom-20g, iom2-20g, iom-20g-b, iom3-20g, iom3-40g, iom3-xp, imm48-1gb-sfp, imm48-1gb-tx, imm4-10gb-xfp, imm5-10gb-xfp, imm8-10gb-xfp, imm12-10gb-SF+, imm1-40gb-tun, imm3-40gb-qsfp, imm1-oc768-tun, imm1-100g-cfp, iom3-xp, imm-2pac-fp3, iom3-xp, imm-2pac-fp3

mda-type

Syntax **mda-type** *mda-type*
no mda-type

Context config>card>mda

Description This mandatory command provisions a specific MDA type to the device configuration for the slot. The MDA can be preprovisioned but an MDA must be provisioned before ports can be configured. Ports can be configured once the MDA is properly provisioned. A maximum of two MDAs can be provisioned on an IOM. Only one MDA can be provisioned per IOM MDA slot. To modify an MDA slot, shut down all port associations.

A maximum of six MDAs or eight CMAs (or a combination) can be provisioned on a 7750 SR-c12. Only one MDA/CMA can be provisioned per MDA slot. To modify an MDA slot, shut down all port associations. CMAs do not rely on MCM configuration and are provisioned without MCMs. Note: CMAs are provisioned using MDA commands. A medium severity alarm is generated if an MDA/CMA is inserted that does not match the MDA/CMA type configured for the slot. This alarm is cleared when the correct MDA/CMA is inserted or the configuration is modified. A high severity alarm is raised when an administratively enabled MDA/CMA is removed from the chassis. This alarm is cleared if the either the correct MDA/CMA type is inserted or the configuration is modified. A low severity trap is issued if an MDA/CMA is removed that is administratively disabled.

An MDA can only be provisioned in a slot if the MDA type is allowed in the MDA slot. An error message is generated when an MDA is provisioned in a slot where it is not allowed.

A medium severity alarm is generated if an MDA is inserted that does not match the MDA type configured for the slot. This alarm is cleared when the correct MDA is inserted or the configuration is modified.

A high severity alarm is raised when an administratively enabled MDA is removed from the chassis. This alarm is cleared if the either the correct MDA type is inserted or the configuration is modified. A low severity trap is issued if an MDA is removed that is administratively disabled.

An alarm is raised if partial or complete MDA failure is detected. The alarm is cleared when the error

condition ceases. All parameters in the MDA context remain and if non-default values are required then their configuration remains as it is on all existing MDAs.

Refer to the 7750 SR OS Interface Guide or 7450 ESS OS Interface Guide for further information on command usage and syntax for the AA ISA and other MDA and ISA types.

The **no** form of this command deletes the MDA from the configuration. The MDA must be administratively shut down before it can be deleted from the configuration.

Default No MDA types are configured for any slots by default.

Parameters *mda-type* — Specifies the type of MDA for the slot position.

ISA-2: isa2-aa, isa2-bb, isa2-tunnel

7750: m60-10/100eth-tx, m10-1gb-sfp, m16-oc12/3-sfp, m8-oc12/3-sfp, m16-oc3-sfp, m8-oc3-sfp, m4- oc48-sfp, m1-oc192, m5-1gb-sfp, m12-chds3, m1-choc12-sfp, m1-10gb, m4-choc3-sfp, m2-oc192-xpxfp, m2-oc48-sfp, m20-100eth-sfp, m20-1gb-tx, m2-10gb-xfp, m2-oc192-xfp, m12-1gb-sfp, m12- 1gb+2-10gb-xp, m4-atmoc12/3-sfp, m16-atmoc3-sfp, m20-1gb-sfp, m4-chds3, m1-10gb-xfp, vsm-cca,m5-1gb-sfp-b, m10-1gb-sfp-b, m4-choc3-as-sfp, m10-1gb+1-10gb, isa-ipsec, m1-choc12-as-sfp, m12-chds3-as, m4-chds3-as, isa-aa, isa-tms, m12-1gb-xp-sfp, m12-1gb+2-10gb-xp, m10-1gb-hs-sfp, m1-10gb-hs-xfp, m4-choc3-ces-sfp, m1-choc3-ces-sfp, m4-10gb-xp-xfp, m2-10gb-xp-xfp, m1-10gb-xpxfp,m10-1gb-xp-sfp, m20-1gb-xp-sfp, m20-1gb-xp-tx, m1-choc12-ces-sfp, p1-100g-cfp, p10-10gsfp,p3-40g-qsfp, p6-10g-sfp, imm24-1gb-xp-sfp, imm24-1gb-xp-tx, imm5-10gb-xp-xfp, imm4-10gbxp-xfp, imm3-40gb-qsfp, imm1-40gb-qsfp, imm1-40gb-xp-tun, imm-1pac-fp3/p1-100g-tun, imm2-10gb-xp-xfp, imm12-10gb-xp-SF+, imm1-oc768-xp-tun, imm1-100gb-xp-cfp, isa-video, m1-10gbdwdm-tun, iom3-xp-b, m4-atmoc12/3-sf-b, m16-atmoc3-sfp-b, m16-oc12/3-sfp-b, m4-oc48-sfp-bisa2-aa, isa2-bb, isa2-tunnel

7750 SR-c12: m60-10/100eth-tx, m8-oc3-sfp, m5-1gb-sfp, m2-oc48-sfp, m20-100eth-sfp, m20-1gbtx,m4-atmoc12/3-sfp, m20-1gb-sfp, m5-1gb-sfp-b, m4-choc3-as-sfp, c8-10/100eth-tx, c1-1gb-sfp,c2-oc12/3-sfp-b, c8-chds1, c4-ds3, c2-oc12/3-sfp, c1-choc3-ces-sfp, m1-choc12-as-sfp, m12-chds3-as,m4-chds3-as, m4-choc3-ces-sfp, m10-1gb-xp-sfp, m20-1gb-xp-sfp, m20-1gb-xp-t, isa-aa, isa2-aa,

Note: Refer to the 7x50 SR OS Interfaces Configuration Guide and the 7450 ESS OS Interface Configuration Guide for further information.

Admin Commands

application-assurance

Syntax **application-assurance**

Context admin

Description This command enables the context to perform Application Assurance (AA) configuration operations.

upgrade

Syntax **upgrade**

Context admin>app-assure

Description Use this command to load a new isa-aa.tim file as part of a router-independent signature upgrade. An AA ISA reboot is required.

Application Assurance Commands

aarp

Syntax **aarp** *aarpId* [**create**]
no aarp *aarpId*

Context config>application-assurance

Description This command defines an Application Assurance Redundancy Protocol (AARP) instance. This instance is paired with the same *aarpId* in a peer node as part of a configuration to provide flow and packet asymmetry removal for traffic for a multi-homed SAP or spoke SDP.

The **no** form of the command removes the instance from the configuration.

Default no aarp

Parameters *aarpid* — An integer that identifies an AARP instance.

Values 1 — 65535

create — Keyword used to create the AARP instance.

master-selection-mode

Syntax **master-selection-mode** *mode*

Context config>app-assure>aarp

Description This command configures the AARP mode of operation with the peer instance. The modes affect the AARP state machine behavior according to the desired behavior. Minimize-switchover will change AARP state based on Master ISA failure, and be non-revertive in that when the priority ISA returns a switch does not occur, which is optimal for AA flow identification. Inter-chassis efficiency mode considers both priority (revertive) and the endpoint status of the AARP instance and will switch activity in case of EP failure in order to avoid sending all the traffic over the ICL. The priority-based-balance mode will be revertive after a priority master returns to service, but excludes EP status. The master-selection-mode configuration must match on both peer AARP instances, or the AARP operational status will stay down.

Default minimize-switchovers

Parameters *mode* — Specifies the the AARP master selection mode.

Values **minimize-switchovers** — Optimal AA flow detection continuity by minimizing AARP switchovers.
inter-chassis-efficiency — minimizes inter-chassis traffic.
priority-based-balance — AA load balance between AARP peers based on configured priority.

peer

Syntax **peer** *ip-address*
no peer

Context config>app-assure>aarp

Description This command defines the IP address of the peer router which must be a routable system IP address.

If no peer is configured and the AARP is **no shutdown**, it is configured as a single node AARP instance.

The **no** form of the command removes the IP address from the AARP instance.

Default no peer

Parameters *ip-address* — Specifies the IP address in the a.b.c.d format.

peer-endpoint

Syntax **peer-endpoint sap** *sap-id* **encap-type** {**dot1q**|**null**|**qinq**}
peer-endpoint spoke-sdp *sdp-id:vc-id*
no peer-endpoint

Context config>app-assure>aarp#

Description This command defines the peer endpoint ID of the SAP or spoke-SDP parent-aa-sub of the AARP peer.

The **no** form of the command removes the peer endpoint from the AARP instance.

Default no peer-endpoint

Parameters **sap** *sap-id* **—** Specifies the physical port identifier portion of the SAP definition.

sdp-id:vc-id — Specifies the spoke SDP ID and VC ID.

Values 1 — 17407
1 — 4294967295

encap-type {**dot1q**|**null**|**qinq**} **—** Specifies the encapsulation type.

priority

Syntax **priority** [*0..255*]
no priority

Context config>app-assure>aarp

Description This command defines the priority for the AARP instance. The priority value is used to determine the master/backup upon initialization or re-balance.

The **no** form of the command removes the priority.

Default priority 100

Parameters [*0 — 255*] — Specifies an integer that defines the priority of an AARP instance.

Values 0 — 255

bit-rate-high-wmark

Syntax **bit-rate-high-wmark** *high-watermark*

Context config>application-assurance

Description This command configures the high watermark for bit rate alarms.

Context max (disabled)

Parameters *high-watermark* — pecifies the high watermark for bit rate alarms. The value must be larger than or equal to the low-watermark value.

Values 1 — 10000, **max** megabits/sec

bit-rate-low-wmark

Syntax **bit-rate-low-wmark** *low-watermark*
no bit-rate-low-wmark

Context config>application-assurance

Description This command configures the utilization of the flow records on the ISA-AA Group when the full alarm will be cleared by the agent.

Default 0

Parameters *low-watermark* — Specifies the low watermark for bit rate alarms. The value must be lower than or equal to the high-watermark value.

Values 0 — 10000 megabits/sec

packet-rate-high-wmark

Syntax **packet-rate-high-wmark** *high-watermark*

Context config>app-assure

Description This command configures the packet rate on the ISA-AA when a packet rate alarm will be raised by the agent.

Default max = disabled

Parameters *high-watermark* — Specifies the high watermark for packet rate alarms. The value must be larger than or equal to the packet-rate-low-wmark value.

Values 1 — 14880952 , **max** packets/sec

packet-rate-low-wmark

Syntax **packet-rate-low-wmark** *low-watermark*
no packet-rate-low-wmark

Context config>app-assure

Description This command configures the system wide low watermark threshold for per-ISA throughput in packets/second when an high packet rate alarm will be cleared by the agent.. The value must be less than or equal to the packet-rate-high-wmark parameter.

The **no** form of the command sets the parameter to minimum (watermark disabled).

Default 0

Parameters *low-watermark* — Specifies the low watermark for packet rate alarms. T he value must be lower than or equal to the packet-rate-low-wmark value.

Values 0— 14880952 packets/sec

flow-setup-high-wmark

Syntax **flow-setup-high-wmark** *high-watermark*

Context config>application-assurance

Description This command configures the system wide high watermark threshold for per-ISA throughput in packets/second when an alarm will be raised by the agent. The value must be larger than or equal to the packet-rate-low-wmark parameter.

The **no** form of the command sets the parameter to maximum (watermark disabled).

Default 0

Parameters *high-watermark* — Specifies the high watermark for flow setup rate alarms. The value must be larger than or equal to the flow-setup-low-wmark value.

Values 1 — 200000, **max** flows/sec

flow-setup-low-wmark

Syntax **flow-setup-low-wmark** *low-watermark*
no flow-setup-low-wmark

Context config>application-assurance

Description This command configures the flow setup rate on the ISA-AA when a flow setup alarm will be raised by the agent.

Default 0

Parameters *low-watermark* — Specifies the low watermark for flow setup rate alarms. The value must be larger than or equal to the flow-setup-high-wmark value.

Values 1 — 200000, **max** flows/sec

application-assurance

Syntax **application-assurance**

Context config

Description This command enables the context to perform Application Assurance (AA) configuration operations.

flow-table-high-wmark

Syntax **flow-table-high-wmark** *high-watermark*
no flow-table-high-wmark

Context config>app-assure

Description The command configures the system-wide high watermark threshold as a percentage of the flow table size for the per-ISA utilization of the flow records when a full alarm will be raised by the agent.

Parameters *high-watermark* — Specifies the high watermark for flow table full alarms.

Values 0 — 100

Default 95%

flow-table-low-wmark

Syntax **flow-table-low-wmark** *low-watermark*
no flow-table-low-wmark

Context config>app-assure

Description This command configures the system-wide low watermark threshold as a percentage of the flow table size for per-ISA. The value must be lower than or equal to the **flow-table-high-wmark** *high-watermark* parameter.

Parameters *low-watermark* — Specifies the low watermark for flow table full alarms.

Values 0 — 100

Default 90%

protocol

Syntax **protocol** *protocol-name*

Context config>app-assure

Description This command configures the shutdown of protocols system-wide.

Parameters *protocol-name* — A string of up to 32 characters identifying a predefined protocol.

group

Syntax **group** *aa-group-id*[:*partition-id* [**create**]
no group *aa-group-id*:*partition-id*

Context config>app-assure

Description This command configures and enables the context to configure an application assurance group and partition parameters.

Parameters *aa-group-id* — Represents a group of ISA MDAs.

Values 1 — 255

partition-id — Specifies a partition within a group.

Values 1 — 65535

create — Keyword used to create the partition in the group.

aa-sub-remote

Syntax [**no**] **aa-sub-remote**

Context config>app-assure

Description This command specifies whether or not the from subscriber and to subscriber traffic direction is reversed for this group-partition.

Default no aa-sub-remote

cflowd

Syntax **cflowd**

Context config>app-assure>group

Description This command enables the context to configure cflowd parameters for the application assurance group.

dns-ip-cache

Syntax **dns-ip-cache** *dns-ip-cache-name* [**create**]

Context config>app-assure>group

Description This command configures a DNS IP cache used to snoop DNS requests generated by subscribers to populate a cache of IP addresses matching a specified list of domain names. In the context of URL content charging strengthening, it is also mandatory to specify a list of trusted DNS servers to populate the DNS IP cache.

Parameters *dns-ip-cache-name* — Specifies the Application Assurance DNS IP cache name.

create — Specifies a keyword used to create the DNS IP cache.

dns-match

Syntax **dns-match domain** *domain-name* **expression** *expression*

Context config>app-assure>group>dns-ip-cache

Description This command configures a domain expression to populate the DNS IP cache, up to 32 domains can be configured.

Parameters *domain-name* — Specifies the name of the domain expression entry.

expression — Specifies a domain name expression string, up to 64 characters long, used to define a pattern match. This domain expression uses the same syntax as the expressions used in app-filters.

domain

Syntax **domain** *domain-name* **expression** *expression*
no domain *domain-name*

Context config>app-assure>group>dns-ip-cache

Description This command configures a domain expression to populate the DNS IP cache. Up to 32 domains can be configured.

Parameters *domain-name* — Specifies the name of the domain expression entry.

expression **—** Specifies a domain name expression string, up to 64 characters long, used to define a pattern match. This domain expression uses the same syntax as the expressions used in app-filters.

server-address

Syntax **server-address** *server-address* [**name** *server-address*]
no server-address *server-address*

Context config>app-assure>group>dns-ip-cache

Description This command configures a DNS server-address. DNS responses from this DNS server are used to populate the dns-ip-cache. Up to 64 server-addresses can be configured.

Parameters **server-address** *server-address* — Specifies the IPv4 or IPv6 address of the DNS.

Values	ipv4-address	a.b.c.d[/mask]	
			mask - [1..32]
	ipv6-address	x:x:x:x:x:x:x:x/prefix-length	
			x:x:x:x:x:x:d.d.d.d
			x - [0..FFFF]H
			d - [0..255]D
		prefix-length	[1..128]

name *server-name* **—** Specifies an optional server-name for a given server-address.

ip-cache

Syntax **ip-cache**

Context config>app-assure>group>dns-ip-cache

Description This command configures the dns-ip-cache cache parameters.

size

Syntax **size** *cache-size*

Context config>app-assure>group>dns-ip-cache>ip-cache

Description This command configures the maximum number of entries in the cache.

Default 10

Parameters *cache-size* — Specifies the maximum number of IP addresses that can be stored in the cache.

Values 10 — 5000

high-watermark

Syntax **high-watermark** *percent*

Context config>app-assure>group>cache>ip-cache

Description This command configures the high watermark value for the DNS IP cache. When the number of IP addresses stored in the cache crosses above this threshold the system will generate a trap.

Default 90

Parameters *percent* — Specifies the high-watermark value in percent

Values 0 — 100

low-watermark

Syntax **low-watermark** *percent*

Context config>app-assure>group>cache>ip-cache

Description This command configures the low watermark value for the dns-ip-cache. If the dns-ip-cache has previously crosses the high-watermark value, the system will clear the trap in case the number of IP addresses stored in the cache crosses below the low-watermark value.

Default 90

Parameters *percent* — Specifies the low-watermark value in percent.

Values 0 — 100

collector

Syntax **collector** *ip-address*[:*port*] [**create**]
no collector *ip-address*[:*port*]

Context config>app-assure>group>cflowd

Description This command defines a flow data collector for cflowd data. The IP address of the flow collector must be specified. The UDP port number is an optional parameter. If it is not set, the default of 2055 is used.

Parameters *ip-address* — The IP address of the flow data collector in dotted decimal notation.

:*port* **—** The UDP port of flow data collector.

Default 2055

Values 1— 65535

comprehensive

Syntax **comprehensive**

Context config>app-assure>group>cflowd

Description This command enables the context to configure cflowd comprehensive statistics output parameters.

rtp-performance

Syntax **performance**

Context config>app-assure>group>cflowd

Description This command configures the cflowd RTP performance export.

event-log

Syntax **event-log** *event-log-name* [**create**]
no event-log *event-log-name*

Context config>app-assure>group
config>app-assure>group>gtp
config>app-assure>group>gtp>gtp-filter

Description This command configures an event log.

buffer-type

Syntax **buffer-type** *buffer-type*

Context config>app-assure>group>evt-log

Description This command specifies the the type of buffer to be used in the event log.

Parameters *buffer-type* — Specifies the type of event type.

Values **linear** — Specifies a linear buffer which once full will stop recording events until it is cleared
circular — Specifies a circular buffer whereby older entries will be overwritten by newer entries.

max-entries

Syntax **max-entries** *max-entries*
no shutdown

Context config>app-assure>group>evt-log

Description This command configures the number of entries in the buffer.

Parameters *max-entries* — Specifies the maximum number of entries for the event log.

Values 1 — 100000

Default 500

app-group

Syntax [**no**] **app-group** *app-group-name* [*rate*]

Context config>app-assure>group>cflowd>rtp-performance
config>app-assure>group>cflowd>tcp-performance
config>app-assure>group>cflowd>comprehensive

Description Description This command configures application groups to export performance records with cflowd.

The no form of the command removes the parameters from the configuration.

Parameters *app-group-name* — Specifies the application group name.

rate — Specifies which sampling flow rate to use; flow-rate or flow-rate2.

Values flow-rate, flow-rate2

Default flow-rate

application

Syntax [**no**] **application** *application-name* [*rate*]

Context config>app-assure>group>cflowd>rtp-performance
config>app-assure>group>cflowd>tcp-performance
config>app-assure>group>cflowd>comprehensive

Description This command configures applications to export performance records with cflowd.

The **no** form of the command removes the parameters from the configuration.

Parameters *application-name* — Specifies the name defined for the application.

rate — Specifies which sampling flow rate to use; flow-rate or flow-rate2.

Values flow-rate, flow-rate2

Default flow-rate

flow-rate

Syntax **flow-rate** *sample-rate*
no flow-rat

Context config>app-assure>group>cflowd>rtp-performance
config>app-assure>group>cflowd>tcp-performance
config>app-assure>group>cflowd>comprehensive

Description This command configures specifies the per-flow sampling rate for the cflowd export of Application Assurance performance statistics.

The **no** form of the command reverts to the default.

Default no flow-rate

Parameters *sample-rate* — This is the rate at which to sample flows that are eligible for TCP performance measurement.

Values 1 — 1000

flow-rate2

Syntax **flow-rate2** *sample-rate*
no flow-rate2

Context config>app-assure>group>cflowd>rtp-performance
config>app-assure>group>cflowd>tcp-performance
config>app-assure>group>cflowd>comprehensive

Description This command configures specifies the per-flow second sampling rate for the cflowd export of Application Assurance performance statistics.

The **no** form of the command reverts to the default.

Default no flow-rate

Parameters *sample-rate* — This is the rate at which to sample flows that are eligible for TCP and/or RTP performance measurement.

Values 1 — 1000

template-retransmit

Syntax **template-retransmit** *seconds*
no template-retransmit

Context config>app-assure>group>cflowd

Description This command configures the period of time, in seconds, for the template to be retransmitted.

Parameters *seconds* — Specifies the time period for the template to be retransmitted.

Values 10 — 600

Default 600

tcp-performance

Syntax **tcp-performance**

Context config>app-assure>group>cflowd

Description This command enables the context to configure Cflowd TCP performance export parameters.

volume

Syntax **volume**

Context config>app-assure>group>cflowd

Description This command configures the cflowd volume export.

rate

Syntax **rate** *sample-rate*
no rate

Context config>app-assure>group>cflowd>volume

Description This command configures the sampling rate of packets for the cflowd export of application assurance volume statistics.

The **no** form of the command reverts to the default value.

Parameters *sample-rate* — This is the rate at which to sample packets for the cflowd export of application assurance volume statistics.

Values 1 — 10000

http-error-redirect

Syntax **http-error-redirect** *redirect-name* [**create**]
no http-error-redirect *redirect-name*

Context config>app-assure>group

Description This command configures an HTTP error redirect policy. The policy contains important information relevant to the redirect server.

The **no** form of the command removes the redirect name from the group configuration.

Default none

Parameters *redirect-name* — A string of up to 32 characters that identifies the HTTP error redirect policy.

error-code

Syntax **error-code** *error-code* [**custom-msg-size** *custom-msg-size*]
no error-code *error-code*

Context config>app-assure>group>http-error-redirect

Description This command refers to which HTTP status codes a redirect action is applied. Currently, only 404 http error code is supported. Only messages with sizes less than that configured here (custom-msg-size) are eligible for redirect action.

The no form of the command removes the parameters from the configuration.

Default Error code: none

Parameters *error-code* — Specifies the error code for a HTTP Error Redirect.

Values 0 — 4294967295

custom-msg-size — Specifies the maximum message size above which redirect will not be done.

Values 0 — 4294967295

http-host

Syntax **http-host** *http-host*
no http-host

Context config>app-assure>group>http-error-redirect

Description This is a string that refers to the http host name of the landing server (barefurit or xerocole). It is used in the HTTP GET operation from the client (which is being redirected) to the redirect search landing server. It must contain a valid IP address or HTTP host name / URI for the HTTP GET from the client to the landing server to work.

The **no** form of the command removes the HTTP host string from the configuration.

Default none

Parameters *http-host* — Specifies a string of 255 chars max length, that refers to the HTTP host name of the landing server (barefurit or xerocole).

participant-id

Syntax **participant-id** *participant-id*
no participant-id

Context config>app-assure>group>http-error-redirect

Description This command specifies a 32-character string assigned to the operator by Barefruit. It is used by barefruit landing servers (applies to template # 1 only).

Default None

Parameters *participant-id* — 32-char string supplied by the Barefruit

template

Syntax **template** *template-id*
no template

Context config>app-assure>group
config>app-assure>group>http-error-redirect

Description The redirect template refers to the template of parameters passed from the AA-ISA to the redirect server via JavaScript in the redirect packet. The template is specific to the redirect server being used in the network.

Currently, two partners are used and tested with AA-ISA redirect solution, Barefruit and Xerocole.

The **no** form of the command reverts to the default.

Default 1 = referring to redirect format for Barefruit landing server.

Parameters *template-id* — Specifies an HTTP error redirect template.
1 = Barefruit specific template
2= xerocole.specific template.

Values 0 — 4294967295

http-match-all-requests

Syntax [**no**] **http-match-all-requests**

Context config>app-assure>group
config>app-assure>group>policy>app-filter>entry

Description This command enables HTTP matching for all requests for a given HTTP expression.

The **no** form of the command restores the default (removes http-match-all-request for this particular expression) by this app-filter entry).

Default no http-match-all-requests

http-notification

Syntax **http-notification** *http-notification-name* [**create**]
no http-notification *http-notification-name*

Context config>app-assure>group

Description This command configures an http-notification object for subscriber in browser notification.

The **no** form of the command removes the http notification policy from the configuration.

Parameters *http-notification-name* — Specifies the name of the HTTP Notification policy.

create — Specifies the mandatory keyword to create the policy.

interval

Syntax **interval** {**one-time |** *minimum-interval*}

Context config>app-assure>group>http-notif#

Description This command configures the minimum interval in between notification messages. It can be set to one-time or a value in minutes from 1 to 1440.

The **no** form of the command removes the interval from the http-notification policy.

Parameters *minimum-interval* — Represents the minimum interval value in minutes in between two http notifications.

Values 1 — 1440.

template

Syntax **template** *value*
no template

Context config>app-assure>group>http-notif

Description This command configures the template which defines the format and parameters included in the http notification message.

The **no** form of the command removes the template from the configuration.

Parameters *value* — Specifies the template id of this HTTP Notification.

Values 1 — Javascript-url with SubID and optional Http-Url-Param
2 — Javascript-url and optional Http-Url-Param

script-url

Syntax **script-url** *script-url-name* [**create**]
no script-url

Context config>app-assure>group>http-notif

Description This command configures the url of the script used by the http notification policy.

The **no** form of the command removes the script-url from the http-notification policy.

Parameters *script-url-name* — Specifies the 255 characters long string representing the url of the script used in the http notification policy.

http-redirect

Syntax **http-redirect** *redirect-name* [**create**]
no http-redirect *redirect-name*

Context config>app-assure>group

Description This command configures an HTTP redirect.

The **no** form of the command removes the http redirect policy from the configuration.

Parameters *redirect-name* — Specifies the HTTP redirect that will be applied. If no redirect name is specified then HTTP redirect is not enabled.

captive-redirect

Syntax **captive redirect**

Context config>app-assure>group>http-redirect

Description This command configures the captive redirect capability for an HTTP redirect policy. HTTP redirect policies using captive redirect can be used in conjunction with a session filter policy and will terminate TCP flows in the ISA-AA card before reaching the Internet to redirect subscribers to the predefined redirect URL. Non-HTTP TCP flows are TCP reset. Captive redirect uses the provisioned VLAN id to send the HTTP response to subscribers; therefore this VLAN id must be properly assigned in the same VPN as the subscriber. The operator can select the URL arguments to include in the redirect URL using either a specific template id or by configuring the redirect URL using one of the supported macro substitution keywords.

vlan-id

Syntax **vlan-id** *service-port-vlan-id*
no vlan-id

Context config>app-assure>group>http-redirect>captive-redirect

Description This command configures the VLAN id for captive redirect. Captive redirect uses the provisioned VLAN id to send the HTTP response to subscribers; therefore this VLAN id must be properly assigned in the same VPN as the subscriber.

Parameters *service-port-vlan-id* — Specifies the vlan-id.

Values 1 - 4094

redirect-url

Syntax **redirect-url** *redirect-url*
no redirect-url

Context config>app-assure>group>http-redirect

Description This command configures the http redirect URL which is the URL (page) that the user is redirected to when an HTTP redirect takes effect.

The operator can select the URL arguments to include in the redirect-url using either a specific template-id or by configuring the redirect-url using one of the supported macro substitution keywords.

The **no** form of the command removes the redirect-url field from the configuration.

Parameters *redirect-url* — Specifies the URL of the landing page.

macro substitutions:

Values		
	$URL	The Request-URI in the HTTP GET Request received
	$SUB-	A string that represents the subscriber ID
	$IP-	A string that represents the IP address of the subscriber host
	$RTRID-	A string that represents the router ID
	$URLPRM-	The HTTP URL parameter associated with the subscriber

tcp-client-reset

Syntax [**no**] **tcp-client-reset**

Context config>app-assure>group>http-redirect

Description This command enables an HTTP-redirect policy to initiate a TCP reset towards the client if the AA policy results in a redirect with packet drop but the http redirect cannot be delivered.   Scenarios for this include HTTPs (TLS) sessions, blocking of non-HTTP TCP traffic, and blocking of existing flows after a policy re-evaluate of an existing subscriber.

The **no** form of the command disables the command.

template

Syntax **template** *template-id*
no template

Context config>app-assure>group>http-redirect

Description This command configures the template that defines which parameters are appended to the HTTP host redirect field in the redirect message.

The HTTP redirect template provides HTTP 302 redirect containing only the URL specified in the redirect policy, with no other parameters.

The **no** form of the command removes the template from the configuration.

Default none

Parameters *template-id* — Specifies the HTTP Policy Redirect template.

Values 1 — Javascript based redirect embedded in HTTP 200 OK response with a predefined number of arguments automatically appended to the redirect URL
2 — HTTP 302 Redirect with a predefined number of arguments automatically appended to the redirect URL.
3 — HTTP 302 Redirect with no parameters appended to the URL (empty).
4 — Empty Redirect format using Javascript.
5 — Redirect supporting macro substitution using HTTP 302.
6 — Redirect supporting macro substitution using Javascript.

http-x-online-host

Syntax [**no**] **http-x-online-host**

Context config>app-assure>group

Description This command specifies whether X-Online-Host header field is used as a replacement for the HTTP Host header field.

The **no** form of the command disables the use of X-Online-Host header field used as a replacement.

ip-prefix-list

Syntax **ip-prefix-list** *ip-prefix-list-name* [**create**]
no ip-prefix-list *ip-prefix-list-name*

Context config>app-assure>group

Description This command configures an IP prefix list.

Parameters **create —** Mandatory keywork used when creating an application profile. The create keyword requirement can be enabled/disabled in the environment>create context.

http-enrich

Syntax **http-enrich** *http-enrich_name* [**create**]
no http-enrich *http-enrich_name*

Context config>app-assure>group

Description This command configures an HTTP enrichment policy.

The **no** form of the command removes the http enrichment policy from the configuration

Default none.

Parameters *enrich-name* — Specifies the name of the http enrichment policy up to 32 characters in length.

create — Mandatory keywork used when creating an application profile. The create keyword requirement can be enabled/disabled in the environment>create context.

field

Syntax [**no**] **field** *field-name*

Context config>app-assure>group>http-enrich

Description This command configures what fields to be inserted into the HTTP header. The command is repeated for each field to be inserted. The same field cannot be inserted twice into the header under different header names.

The **no** form of the command removes the specified parameter so that it is not inserted into the http header.

Default none.

Parameters *field-name* — Specifies what parameter(s) to inserted into the header.

Values subscriber-ip, static-string

Where:

subscriber-ip: header name for the subscriber IP

static-string: header name for inserted string

subscriber-id: header name for subscriber ID

Default none

header-name — Specifies an operator defined string (max 32 char in length). It is inserted before the actual field name (e.g. x-subId = subscriberID).

Default none

name

Syntax **name** *header_name*

Context config>app-assure>group>http-enrich>field

Description This command configures an HTTP enrichment template field header name.

The **no** form of the command removes the http enrichment template field header name from the configuration.

Default none.

Parameters *header-name* — Specifies the name of the http enrichment policy. It is inserted before the actual field name (e.g. x-subId = subscriberID).

anti-spoof

Syntax [**no**] **anti-spoof**

Context config>app-assure>group>http-enrich>field

Description This command configures the HTTP header enrichment anti-spoofing functionality.

The **no** form of the command disables anti-spoofing functionality.

Default no anti-spoof

static-string

Syntax **static-string** *static-string*
no static-string

Context config>app-assure>group>http-enrich>field

Description This command configures an HTTP header enrichment template field static string.

The **no** form of the command removes the template field static string.

Default no static-string

Parameters *static-string* — Specifies a static string (max 32 char in length).

encode

Syntax **encode type** *type* **key** *key*
encode type *type* **key** *hash-key* **hash**
encode type *type* **key** *hash2-key* **hash2**
no encode

Context config>app-assure>group>http-enrich>field

Description This command configures an HTTP header enrichment template field static string.

The **no** form of the command removes the template field static string.

Default no static-string

Parameters *type* — md5

key — Specifies the key string, 64 characters maximum.

hash-key — Specifies the first hashed key..

hash-key2 — Specifies the second hashed key.

hash | *hash2* — Specifies the hashing scheme used in the hashed key.

Group Commands

Transit Subscriber Commands

transit-ip-policy

Syntax **transit-ip-policy** *ip-policy-id* [**create**]
no transit-ip-policy *ip-policy-id*

Context config>application-assurance>group

Description This command defines a transit AA subscriber IP policy. Transit AA subscribers are managed by the system through the use of this policy assigned to services, which determines how transit subs are created and removed for that service.

The **no** form of the command deletes the policy from the configuration. All associations must be removed in order to delete a policy.

Default no transit-ip-policy

Parameters *ip-policy-id* — An integer that identifies a transit IP profile entry.

Values 1 — 65535

create — Keyword used to create the entry.

Policer Commands

policer

Syntax **policer** *policer-name* **type** *type* **granularity** *granularity* [**create**]
policer *policer-name*
no policer *policer-name*

Context config>app-assure>group

Description This command creates application assurance policer profile of a specified type. Policers can be bandwidth or flow limiting and can have a system scope (limits traffic entering AA ISA for all or a subset of AA subscribers), subscriber scope or granularity (limits apply to each AA subscriber traffic).

The policer type and granularity can only be configured during creation. They cannot be modified. The policer profile must be removed from all AQPs in order to be removed. Changes to policer profile parameters take effect immediately for policers instantiated as result of AQP actions using this profile..

The **no** form of the command deletes the specified policer from the configuration.

Parameters *type* — Specifies the policer type.

single-bucket-bandwidth — Creates a profile for a single bucket (PIR) bandwidth limiting policer.
dual-bucket-bandwidth — Creates profile for a dual backet (PIR, CIR) bandwidth limiting policer.
flow-rate-limit — Creates profile for a policer limiting rate of flow set-ups.
flow-count-limit — Creates profile for a policer limiting total flow count.
gtp-traffic — Creates a profile for a policer that operates at the GTP tunnel level.

granularity — Specifies the granularity type.

Values **system** — Creates a system policer provile for a policer that limits the traffic in the scope of all or a subset of AA subscribers on a given AA ISA.
subscriber — Creates a policer profile for a policer for each AA subscriber that limits the traffic in the scope of that subscriber.

create — Keyword used to create the policer name and parameters.

Default none

Parameters *policer-name* — A string of up to 32 characters that identifies policer.

gtp-traffic

Syntax [**no**] **gtp-traffic**

Context config>app-assure>group>policer

Description This command provides a mechanism to configure a policer to function at the GTP tunnel level. GTP tunnels are defined by a TEID and destination IP address as oppose to normal flows that are defined by IP 5 tuple values. By setting this value, the policer then can be used to limit GTP traffic (SeGW GTP firewall application).

The **no** form of the command resets policer behavior to act at the normal 5 tuple flow level and not at the GTP tunnel level

Default no gtp-traffic

action

Syntax **action** {**priority-mark** | **permit-deny**}

Context config>app-assure>group>policer

Description This command configures the action to be performed by single-bucket bandwidth policers for non-conformant traffic.

Dual bucket bandwidth policers cannot have their action configured and always mark traffic below CIR in profile, between CIR and PIR out of profile, and drop traffic above PIR.
Flow policers always discard non-conformant traffic.
When multiple application assurance policers are configured against a single flow (including policers at both subscriber and system), the final action done to the flow/packet will be a logical OR of all policersí actions. For example, if only of the policers requires the packet to be discarded, the packet will be dropped regardless of the action of the other policers.

Default permit-deny

Parameters **priority-mark** — Non-conformant traffic will be marked out of profile and the conformant traffic will be marked in profile. The new marking will overwrite any previous IOM QoS marking done to a packet.

permit-deny — Non-conformant traffic will be dropped.

adaptation-rule

Syntax **adaptation-rule pir** {**max** | **min** | **closest**} [**cir** {**max** | **min** | **closest**}]
no adaptation-rule

Context config>app-assure>group>policer

Description This command defines the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined option. To change the CIR adaptation rule only, the current PIR rule must be part of the command executed.

The **no** form of the command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific adaptation-rule is removed, the default constraints for rate and cir apply.

Default closest

Parameters **max —** The operational PIR or CIR for the queue will be equal to or less than the administrative rate specified using the **rate** command.

min — The operational PIR or CIR for the queue will be equal to or greater than the administrative rate specified using the **rate** command.

closest — The operational PIR or CIR for the queue will be the rate closest to the rate specified using the **rate** command.

flow-count

Syntax **flow-count** *flow-count*
no flow-count

Context config>app-assure>group>policer

Description This command configures the flow count for the flow-count-limit policer. It is recommended to configure flow count subscriber-level policer for AA subscribers to ensure fair usage of flow resources between AA subscribers.

Parameters *flow-count* — Specifies the flow count for the flow-count-limit policer.

cbs

Syntax **cbs** *committed-burst-size*
no cbs

Context config>app-assure>group>policer

Description This command provides a mechanism to configure the committed burst size for the policer. It is recommended that CBS is configured larger than twice the maximum MTU for the traffic handled by the policer to allow for some burstiness of the traffic. CBS is configurable for dual-bucket bandwidth policers only.

The **no** form of the command resets the cbs value to its default.

Default 0

Parameters *committed-burst-size* — An integer value defining size, in kbytes, for the CBS of the policer.

Values 0 — 131071

mbs

Syntax **mbs** *maximum-burst-size*
no mbs

Context config>app-assure>group>policer
config>app-assure>group>tod-override

Description This command provides a mechanism to configure the maximum burst size for the policer. It is recommended that MBS is configured larger than twice the MTU for the traffic handled by the policer to allow for some burstiness of the traffic. MBS is configurable for single-bucket, dual-bucket bandwidth and flow setup rate policers only.

The **no** form of the command resets the MBS value to its default.

Default 0

Parameters *maximum-burst-size* — An integer value defining either size, in kbytes, for the MBS of the bandwidth policer, or flow count for the MBS of the flow setup rate policers.

Values 0 — 131071

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context config>app-assure>group>policer
config>app-assure>group>tod-override

Description This command configures the administrative PIR and CIR for bandwidth policers and flow setup rate limits for flow policers. The actual rate sustained by the flow can be limited by other policers that may be applied to that flow's traffic. This command does not apply to flow-count-limit policers. The **cir** option is applicable only to dual-bucket bandwidth policers. It is recommended to configure flow setup rate subscriber-level policer for AA subscribers to ensure fair usage of flow resources between AA subscribers.

The **no** form of the command resets the values to defaults.

Default 0

Parameters *pir-rate* — An integer specifying either the PIR rate in Kbps for bandwidth policers.

Values 1 — 100000000, max or flows

cir-rate — An integer specifying the CIR rate in Kbps.

Values 0 — 100000000, max

tod-override

Syntax **tod-override** *tod-override-id* [**create**]
no tod-override *tod-override-id*

Context config>app-assure>group>policer

Description This commands creates a time of day override policy for a given policer. Up to 8 overrides can be configured per policer. Rate/mbs/cbs/flow-rate/flow-count configured in each override-id will override the default policer values at the specified time of day configured in the override.

Default none

Parameters *tod-override-id* — Specify the time of day override ID.

Values 1 — 255

time-range

Syntax **time-range daily start** *start-time* **end** *end-time* [**on** *day* [*day*...(upto 7 max)]]
time-range weekly start *start-time* **end** *end-time*
no time-range

Context config>app-assure>group>tod-override

Description This command configures the time-range applicable to a particular override-id. The time-range can be configured as daily or weekly policies.

When using a daily override the operator can select which day(s) during the week from Sunday to Saturday it is applicable along with the start/end hour/min time range repeated over the(se) day(s).

When using a weekly override the operator can select between which days in the week the policy start up to the hours/min for both start day and end day.

Default no time-range

Parameters **daily** **—** Schedule the override as a daily occurrence.

weekly **—** Schedule the override as a daily occurrence.

Values	start-time	daily	<hh>:<mm>
		weekly	<day>,<hh>:<mm>
			<hh> : 0..23
			<mm> : 0|15|30|45
	end-time	daily	<hh>:<mm>
		weekly	<day>,<hh>:<mm>
			<hh> 0..23
			<mm> 0|15|30|45
	day	sunday|monday|tuesday|wednesday|thursday|friday|saturday	

Policy Commands

policy

Syntax **policy**

Context config>app-assure>group>policy

Description This command enables the context to configure parameters for application assurance policy. To edit any policy content begin command must be executed first to enter editing mode. The editing mode is left when the abort or commit commands are issued.

abort

Syntax **abort**

Context config>app-assure>group>policy

Description This command ends the current editing session and aborts any changes entered during this policy editing session.

begin

Syntax **begin**

Context config>app-assure>group>policy

Description This command begins a policy editing session.

The editing session continues until one of the following conditions takes place:

- Abort or commit is issued.
- Control complex resets.

The editing session is not interrupted by:

- HA activity switch.
- CLI session termination (for example, as result of closing a Telnet session).

commit

Syntax **commit**

Context config>app-assure>group>policy

Description This command commits changes made during the current editing session. None of the policy changes done will take effect until commit command is issued. If the changes can be successfully committed, no errors detected during the commit during cross-reference verification against exiting application assurance configuration, the editing session will also be closed.

The newly committed policy takes affect immediately for all new flows, existing flows will transition onto the new policy shortly after the commit.

app-group

Syntax **app-group** *application-group-name* [**create**]
no app-group *application-group-name*

Context config>app-assure>group>policy

Description This command creates an application group for an application assurance policy.

The **no** form of the command deletes the application group from the configuration. All associations must be removed in order to delete a group.

Default no app-group

Parameters *application-group-name* — A string of up to 32 characters uniquely identifying this application group in the system.

create — Mandatory keywork used when creating an application group. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

charging-group

Syntax **charging-group** *charging-group-name* [**create**]
no charging-group

Context config>app-assure>group>policy
config>app-assure>group>policy>app-group

Description This command creates a charging group for an application assurance policy.

The **no** form of the command deletes the charging group from the configuration. All associations must be removed in order to delete a group.

Default no charging-group

Parameters *charging-group-name* — A string of up to 32 characters uniquely identifying this charging group in the system.

create — Mandatory keywork used when creating a charging group group. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

charging-group

Syntax **charging-group** {**eq** | **neq**} *charging-group-name*
no charging-group

Context config>app-assure>group>policy>application
config>app-assure>group>policy>app-group

Description This command associates an application or app-group to an application assurance charging group.

The **no** form of the command deletes the charging group association.

Default no charging-group

Parameters *charging-group-name* — Specifies a string of up to 32 characters uniquely identifying an existing charging group in the system.

export-id

Syntax **export-id** *export-id*
no export-id

Context config>app-assure>group>policy>application
config>app-assure>group>policy>application>charging-group
config>app-assure>group>policy>app-group

Description This command assigns an export-id value to a charging group app-group or application to be used for accounting export identification in RADIUS accounting. This ID is encoded in the top 2 bytes of the RADIUS accounting VSA to identify which charging group the counter value represents.

If no export-id is assigned, that counter cannot be added to the aa-sub stats RADIUS export-type. Once a charging group index is referenced, it cannot be deleted without removing the reference.

The no form of the command removes the export-id from the configuration.

Default no export-id

Parameters *export-id* — An integer that identifies an export-id.

Values 1 — 255

app-filter

Syntax **app-filter**

Context config>app-assure>group>policy

Description This command enables the context to configure an application filter for application assurance.

app-qos-policy

Syntax **app-qos-policy**

Context config>app-assure>group>policy

Description This command enables the context to configure an application QoS policy.

app-service-options

Syntax **app-service-options**

Context config>app-assure>group>policy

Description This command enables the context to configure application service option characteristics.

default-charging-group

Syntax **default-charging-group** *charging-group-name*
no default-charging-group

Context config>app-assure>group>policy

Description This command associates a charging group to any applications or app-groups that are not explicitly assigned to a charging group, for an application assurance policy.

The **no** form of the command deletes the default charging group from the configuration.

Default no default-charging-group

Parameters *charging-group-name* — A string of up to 32 characters uniquely identifying an existing charging group in the system

diff

Syntax **diff**

Context config>app-assure>group>policy

Description This command compares the newly configured policy against the operational policy.

application

Syntax **application** *application-name* [**create**]
no application *application-name*

Context config>app-assure>group>policy

Description This command creates an application of an application assurance policy.

The **no** form of the command deletes the application. To delete an application, all associations to the application must be removed.

Default none

Parameters *application-name* — Specifies a string of up to 32 characters uniquely identifying this application in the system.

create — Mandatory keyword used when creating an application. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

policy-override

Syntax **policy-override**

Context config>app-assure>group>policy

Description This command enables the context to configure policy override parameters.

policy aa-sub

Syntax **policy aa-sub** {**sap** *sap-id* **|** **spoke-sdp** *sdp-id:vc-id*} [**create**]
no policy aa-sub {**sap** *sap-id* **|** **spoke-sdp** *sdp-id:vc-id*}

Context config>app-assure>group>policy>policy-override

Description This command specifies a given SAP or SDP to be used for a static policy override.

The **no** form of the command removes the policy override.

Parameters **sap** *sap-id* **—** Specifies the physical port identifier portion of the SAP definition.

sdp-id:vc-id — Specifies the spoke SDP ID and VC ID.

Values 1 — 17407
1 — 4294967295

characteristic

Syntax **characteristic** *characteristic-name* **value** *value-name*
no characteristic *characteristic-name*

Context config>app-assure>group>policy>policy-override

Description This command configure an override characteristic and value.

Parameters *characteristic-name* — Specifies the characteristic name up to 32 characters in length.

value *value-name* **—** Specifies the override characteristic value for the application profile characteristic used by the Application assurance subscriber.

app-group

Syntax **app-group** *application-group-name*

Context config>app-assure>group>policy>application

Description This command associates an application with an application group of an application assurance policy.

Default none

Parameters *application-name* — A string of up to 32 characters uniquely identifying an existing application in the system.

Application Filter Commands

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context config>app-assure>group>policy>app-filter

Description This command creates an application filter entry.

App filter entries are an ordered list, the lowest numerical entry that matches the flow defines the application for that flow.

An application filter entry or entries configures match attributes of an application.

The **no** form of this command deletes the specified application filter entry.

Default none

Parameters *entry-id* — An integer that identifies an app-filter entry.

Values 1 — 65535

create — Keyword used to create the entry.

application

Syntax **application** *application-name*

Context config>app-assure>group>policy>application
config>app-assure>group>policy>app-filter>entry

Description This command assigns this application filter entry to an existing application. Assigning the entry to **Unknown** application restores the default configuration.

Default unknown application

Parameters *application-name* — Specifies an existing application name.

expression

Syntax **expression** *expr-index expr-type* {**eq | neq**} *expr-string*
no expression *expr-index*

Context config>app-assure>group>policy>app-filter>entry

Description This command configures string values to use in the application definition.

Parameters *expr-index* — Specifies an index value which represents .expression substrings.

Values 1 — 4

expr-type — Represents a type (and thereby the expression substring).
http-host|http-uri|http-referer|http-user-agent|
sip-ua|sip-uri|sip-mt|citrix-app|h323-product-id|tls-cert-subj-org-name|tls-cert-subj-common-name| rtsp-host|rtsp-uri|rtsp-ua

http-host — Matches the string against the HTTP Host field or TLS Server Name Indicator (SNI).
http-uri — Matches the string against the HTTP URI field.
http-referer — Matches the string against the HTTP Referer field.
http-user-agent — Matches the string against the HTTP User Agent field.
sip-ua — Matches the string against the SIP UA field.
sip-uri — Matches the string against the SIP URI field.
sip-mt — Matches the string against the SIP MT field.
citrix-app — Matches the string against the Citrix app field.
h323-product-id — Matches the string against the h323-product-id field.
tls-cert-subj-org-name — Matches the TLS Certificate Subject Organization Name substring.
tls-cert-subj-common-name — Matches the TLS Certificate Subject Common Name substring.
rtsp-host — Matches the Real Time Streaming Protocol (RTSP) substring host.
rtsp-uri — Matches the RTSP URI substring.
rtsp-ua — Matches the RTSP UA substring.
rtmp-page-host — Matches against the RTMP Page Host Field
rtmp-page-uri — Matches against the RTMP Page URI Field
rtmp-swf-host — Matches against the RTMP Swf Host Field
rtmp-swf-uri — Matches against the RTMP Swf URI Field

eq — Specifies the equal to comparison operator to match the specified HTTP string.

neq — Specifies the not equal to comparison operator to match the specified HTTP string.

expr-string — Specifies an expression string, up to 64 characters, used to define a pattern match. Denotes a printable ASCII substring used as input to an application assurance filter match criteria object.

- The following syntax is permitted within the substring to define the pattern match criteria:

  ^<substring>* - matches when <substring> is at the beginning of the object.

  <substring> - matches when <substring> is at any place within the object.

  *<substring>$ - matches when <substring> is at the end of the object.

  ^<substring>$ - matches when <substring> is the entire object.

  * - matches zero to many of any character. Note that a single wildcard as infix in the expression is allowed.

  \. - matches any single character

  \d - matches any single decimal digit [0-9]

  \I - forces case sensitivity (by default, the expression match are case insensitive), the \I can be specified anywhere between

  the leading [^*] and trailing [$*]

  * - matches the asterisk character
- Rules for <substring> characters:

<substring> must contain printable ASCII characters.

<substring> must not contain the “double quote” character or the “ ” (space) character on its own.

<substring> match is case in sensitive by default.

<substring> must not include any regular expression meta-characters other than "*", "\I", "\.", "*" and "\d".

- The “\” (slash) character is used as an ESCAPE sequence. The following ESCAPE sequences are permitted within the <substring>:

Character to match	<substring> input
Hexidecimal Octet YY	\xYY

Note: A <substring> that uses the '\' (backslash) ESCAPE character which is not followed by a “\” or “\x” and a 2-digit hex octet is not valid.

Operational notes:

1. When matching a TCP flow against HTTP-string based applications, the HTTP header fields are collected from the first HTTP request (for example a GET or a POST) for a given TCP flow. The collected strings are then evaluated against each HTTP flow created within the given TCP flow to determine whether a given HTTP flow matches the application. By not specifying a protocol, the HTTP expressions are matched against all protocols in the HTTP family. By specifying a specific HTTP protocol (for example, http_video) the expression match can be constrained to a subset of the HTTP protocols.

2. To uniquely identify a SIP-based application a protocol match is not required in the app-filter entry with the SIP expression. The SIP expression match is performed against any protocol in the SIP family (such as sip and rtp_sip). By specifying a specific SIP protocol (like rtp_sip) the expression match can be constrained to a subset of the SIP protocols.

flow-setup-direction

Syntax **flow-setup-direction {subscriber-to-network | network-to-subscriber | both}**

Context config>app-assure>group>policy>app-filter>entry

Description This command configures the direction of flow setup to which the application filter entry is to be applied.

Parameters **subscriber-to-network —** Specifies that the app-filter entry will be applied to flows initiated by a local subscriber.

network-to-subscriber — Specifies that the app-filter entry will be applied to flows initiated from a remote destination towards a local subscriber.

both — Specifies that the app filter entry will be applied for subscriber-to-network and network-to-subscriber traffic.

Default both

ip-protocol-num

Syntax **ip-protocol-num** {**eq** | **neq**} *protocol-id*
no ip-protocol-num

Context config>app-assure>group>policy>app-filter>entry

Description This command configures the IP protocol to use in the application definition.

The **no** form of the command restores the default (removes IP protocol number from application criteria defined by this app-filter entry).

Default none

Parameters **eq —** Specifies that the value configured and the value in the flow must be equal.

neq — Specifies that the value configured differs from the value in the flow.

protocol-id — Specifies the decimal value representing the IP protocol to be used as an IP filter match criterion. Well known protocol numbers include ICMP (1), TCP (6), UDP (17).

The **no** form the command removes the protocol from the match criteria.

Values 1 — 255 (Decimal, Hexadecimal, or Binary representation).
Supported IANA IP protocol names:
crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, sctp, stp, tcp, udp, vrrp
* - udp/tcp wildcard

network-address

Syntax **network-address** {**eq** | **neq**} *ip-address*
network-address {**eq** | **neq**} **ip-prefix-list** *ip-prefix-list-name*
no network-address

Context config>app-assure>group>policy>app-filter>entry

Description This command configures the network address to use in application definition. The network address will match the destination IP address in a from-sub flow or the source IP address in a to-sub flow.

The **no** form of the command restores the default (removes the network address from application criteria defined by this entry).

Default no net-address

Parameters **eq —** Specifies a comparison operator indicating that the value configured and the value in the flow are equal.

neq — Specifies a comparison operator indicating that the value configured differs from the value in the flow.

ip-address — Specifies a valid unicast address.

Values ipv4-address a.b.c.d[/mask]
mask - [1..32]

ipv6-address	x:x:x:x:x:x:x:x/prefix-length x:x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D	
	prefix-length	[1..128]

server-address

Syntax **server-address** {**eq** | **neq**} *ip-address*
server-address {**eq** | **neq**} **ip-prefix-list** *ip-prefix-list-name*
no server-address

Context config>app-assure>group>policy>app-filter>entry

Description This command configures the server address to use in application definition. The server IP address may be the source or destination, network or subscriber IP address.

The **no** form of the command restores the default (removes the server address from application criteria defined by this entry).

Default no net-address

Parameters **eq** — Specifies a comparison operator that the value configured and the value in the flow are equal.

neq — Specifies a comparison operator that the value configured differs from the value in the flow.

ip-address — Specifies a valid unicast address.

Values			
	ipv4-address	a.b.c.d[/mask] mask - [1..32]	
	ipv6-address	x:x:x:x:x:x:x:x/prefix-length x:x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D	
		prefix-length	[1..128]

server-port

Syntax **server-port** {**eq** | **neq** | **gt** | **lt**} *server-port-number*
server-port {**eq** | **neq**} **range** *start-port-num end-port-num*
server-port {**eq**} {*port-num* | range*start-port-num end-port-num*} {**first-packet-trusted** | **first-packet-validate**}
no server-port

Context config>app-assure>group>policy>app-filter>entry

Description This command specifies the server TCP or UDP port number to use in the application definition.

The **no** form of the command restores the default (removes server port number from application criteria defined by this app-filter entry).

Default no server-port (the server port is not used in the application definition)

Parameters **eq** — Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

gt — Specifies all port numbers greater than server-port-number match.

lt — Specifies all port numbers less than server-port-number match.

server-port-num — Specifies a valid server port number.

Values 0 — 65535

start-port-num, end-port-num — Specifies the starting or ending port number.

Values 0 — 65535

Server Port Options:

- **No option specified:** TCP/UDP port applications with full signature verification:
  - AA ensures that other applications that can be identified do not run over a well-known port.
  - Application-aware policy applied once sugnature-based identification completes (likely requiring several packets).
- **first-packet-validate:** TCP/UDP trusted port applications with signature verification:
  - Application identified using well known TCP/UDP port based filters and re-identified once signature identification completes.
  - AA policy applied from the first packet of a flow while continuing signature-based application identification. Policy re-evaluated once the signature identification completes, allowing to detect improper/unexpected applications on a well-known port.
- **first-packet-trusted:** TCP/UDP trusted port applications - no signature verification:
  - Application identified using well known TCP/UDP port based filters only.
  - Application Aware policy applied from the first packet of a flow.
  - No signature processing assumes operator/customer trusts that no other applications can run on the well-known TCP/UDP port (statistics collected against trusted_tcp or trusted_udp protocol).

protocol

Syntax **protocol** {**eq** | **neq**} *protocol-name*
no protocol

Context config>app-assure>group>policy>app-filter>entry

Description This command configures protocol signature in the application definition.

The **no** form of the command restores the default (removes protocol from match application defined by this app-filter entry).

Default no protocol

Parameters **eq —** Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

protocol-name — A string of up to 32 characters identifying a predefined protocol.

Sample Output

```
*A:7x50-E11# show application-assurance protocol
===============================================================================
Application Assurance Protocols
===============================================================================
                        Protocol : Description
-------------------------------------------------------------------------------
                       aim_oscar : America Online Oscar Instant Messaging.
             aim_oscar_file_xfer : America Online Oscar File Transfer.
           aim_oscar_video_voice : America Online Oscar Video and Voice
                                   Traffic.
                         aim_toc : America Online Talk to Oscar Instant
                                   Messaging.
                            ares : Ares P2P File Sharing Protocol
                    betamax_voip : Betamax VoIP Protocol traffic.
                             bgp : IETF RFC 4271: Border Gateway Protocol
                      bittorrent : BitTorrent peer to peer protocol.
                      citrix_ica : Citrix ICA protocol.
                      citrix_ima : Citrix IMA protocol.
                         cnnlive : CNN Live Streaming Video
                            cups : Common Unix Printing Service.
                     cut_through : Traffic that cannot be categorized. Only
                                   default subscriber policy is applied.
   cut_through_by_default_policy : Traffic that has been cut-through due to a
                                   subscriber default policy.
                             cvs : Concurrent Versions System.
                            daap : iTunes Digital Audio Access Protocol media
                                   sharing protocol.
                          dcerpc : DCERPC Remote Procedure Call.
        denied_by_default_policy : Traffic that was denied by a default
                                   subscriber flow policer.
                            dhcp : Dynamic Host Configuration Protocol
                                   traffic.
                             dht : Peer to Peer Distributed Hash Table
                                   exchange.
                  direct_connect : Direct Connect peer to peer protocol
                             dns : IETF RFC 1035: Domain Name System.
                          domino : IBM Domino-Notes.
                       empty_tcp : TCP flows that close without ever having
                                   exchanged any data.
                           emule : eMule/eDonkey peer to peer protocol.
                        existing : Traffic that was in progress or with no
                                   start of flow.
                       fasttrack : FastTrack peer to peer protocol.
                             fix : FIX (Financial Information eXchange)
                                   protocol.
                           fring : Fring Mobile traffic.
                     ftp_control : IETF RFC 959: File Transfer Protocol
                                   control traffic.
                        ftp_data : IETF RFC 959: File Transfer Protocol data
                                   traffic.
                        funshion : Funshion Streaming Video
                      gamecenter : Apple Game Center
                        gnutella : Gnutella/Gnutella2 peer to peer protocol.
           google_talk_file_xfer : Google Talk Instant Messaging file
                                   transfer.
```

```
       google_talk_im : Google Talk Instant Messaging.
google_talk_voicemail : Google Talk Instant Messaging voice mail.
                  gtp : GTP (GPRS Tunneling Protocol).
                 h225 : ITU H.225 Multimedia Call Signalling
                        Protocol
                 h245 : ITU H.245 Control Protocol for MultiMedia
                        Communication
             headcall : Headcall Protocol traffic.
              hotline : Hotline Communications: A client-server
                        protocol for file sharing and chatting.
                 http : IETF RFC 2616: Hypertext transfer protocol.
           http_audio : HTTP transported Audio content.
  http_shockwaveflash : HTTP transported Shockwave Flash content.
           http_video : HTTP transported Video content.
         http_webfeed : RSS or ATOM Web Feed
                 hulu : HULU media traffic.
                 iax2 : InterAsterisk Exchange Protocol.
               ibmdb2 : IBM DB2 Database Server.
                  icq : ICQ protocol traffic.
                ident : IETF RFC 1413 Identification Protocol
                 iiop : CORBA IIOP Network Protocol.
                imap4 : IETF RFC 3501: Internet Message Access
                        Protocol V.4.
              iplayer : BBC iPlayer media traffic.
                  ipp : Internet Printing Protocol.
          ipsec_nat_t : IETF RFC 3948: UDP Encapsulated IPsec ESP.
                  irc : RFC 1459 Internet Relay Chat
               isakmp : IETF RFC 2408 4306: Internet Security
                        Association and Key Management Protocol.
                iscsi : ISCSI Protocol.
                 jolt : Oracle JOLT (Java OnLine Transactions)
                        Protocol.
             justintv : Justin.tv media traffic.
             kerberos : Kerberos Version 5 Network Authentication
              kontiki : Kontiki Distribution Protocol
                 ldap : IETF RFC 4510: Lightweight Directory
                        Access Protocol.
                llmnr : LLMNR Protocol.
              mail_ru : mail.ru messaging protocol
             manolito : Manolito P2P File Sharing Protocol
               megaco : Media Gateway Control Protocol.
                 mgcp : Media Gateway Control Protocol.
                  mms : Multimedia Messaging Service over HTTP.
      ms_communicator : Microsoft Communicator Client.
           msexchange : MS Exchange MAPI Interface.
             msn_msgr : MSN Messenger client/server protocol.
   msn_msgr_file_xfer : MSN Messenger initiated P2P file transfer.
       msn_msgr_video : MSN Messenger Video Chat.
            mssql_smb : MS SQL Server Named Pipe traffic.
            mssql_tcp : MS SQL Server over TCP.
            mssql_udp : MS SQL Server Monitoring Service.
                mysql : MySQL Network Protocol.
            net2phone : Net2Phone protocol.
       net2phone_voip : Net2Phone VOIP
              netbios : IETF RFC 1001: Network Basic Input Output
                        System.
              nimbuzz : Nimbuzz Protocol.
                 nntp : IETF RFC 3977: Network News Transfer
                        Protocol.
          non_tcp_udp : Non TCP or UDP traffic.
                  ntp : IETF RFC1305 RFC2030: Network Time
                        Protocol.
            octoshape : Octoshape Streaming Video
               onlive : OnLive Cloud Streaming Services
                oovoo : ooVoo Protocol.
               openft : openft peer to peer protocol.
              openvpn : OpenVPN: open source virtual private
                        network protocol.
           opera_mini : Opera Mini mobile web browser.
           oracle_net : Oracle TNS (Transparent Network Subtrate)
                        Protocol.
           pcanywhere : Symantec PcAnywhere.
                 pop3 : IETF RFC 1939: Post Office Protocol V.3.
           postgresql : PostgreSQL Network Protocol.
               pplive : PPLive Peer to Peer Video Streaming
                        Protocol
             ppstream : PPStream Chinese P2P streaming video.
                 pptp : Point-to-Point Tunneling Protocol.
                 q931 : ITU Q.931 Call Signalling Protocol
                   qq : QQ Instant Messaging Protocol
                 qvod : QVOD: Streaming media on demand.
                  rdp : Remote Desktop Protocol.
                  rdt : Realnetworks Data Transport protocol.
                  rfb : Remote Framebuffer protocol.
               rlogin : IETF RFC 1258 rlogin virtual terminal
                        protocol widely used between Unix hosts
                  rsh : Unix remote shell command
                rsync : Open source file transfer protocol
                 rtmp : RTMP: Adobe Real Time Messaging Protocol.
                rtmpe : RTMPE: Encrypted Adobe Real Time Messaging
                        Protocol.
                rtmpt : RTMPT: HTTP Tunneled Adobe Real Time
                        Messaging Protocol.
                  rtp : IETF RFC 3550: Real-time Transport
                        Protocol.
              rtp_aim : America Online RTP Video/Voice.
             rtp_h323 : H323 RTP Voice.
         rtp_msn_msgr : MSN Messenger RTP Voice.
             rtp_rtsp : RTSP RTP Data
              rtp_sip : SIP RTP Data
           rtp_skinny : Skinny RTP Data
         rtp_yahoo_im : Yahoo Instant Messenger RTP Voice.
                 rtsp : IETF RFC 2326: Real Time Streaming
                        Protocol.
                  sap : SAP Protocol.
            shoutcast : SHOUTcast audio streaming protocol.
               siebel : Siebel Suite.
                  sip : IETF RFC 3261: Session Initiation Protocol.
               skinny : Skinny Call Control Protocol.
                skype : Skype
             slingbox : SlingBox: TV video streaming and remote
                        control
                  smb : Server Message Block protocol over TCP.
          smb_netbios : Server Message Block protocol over NetBIOS.
                 smtp : IETF RFC 2821: Simple Mail Transfer
                        Protocol.
                 snmp : Simple Network Management Protocol traffic.
                socks : SOCKS Proxy.
             soulseek : SoulSeek P2P File Sharing Protocol
              spotify : Spotify Protocol.
                  ssh : IETF RFC 4251: Secure shell protocol.
           starcraft2 : Starcraft II Protocol
```

```
                           steam : Steam Gaming Protocol.
                    steam_gaming : Steam Online Gaming Protocol.
                            stun : IETF RFC 3489: Simple Traversal of UDP
                                   through NATs.
                          sunrpc : SUNRPC Remote Procedure Call.
                             svn : Subversion Version Control System.
                       sybase_db : SYBASE Database Network Protocol.
                          syslog : IETF RFC 3164: syslog protocol.
                            t125 : ITU T.125 Multipoint communication service
                                   protocol
                       teamspeak : TeamSpeak Protocol traffic.
                          telnet : IETF RFC 854: Telnet Network Virtual
                                   Terminal protocol.
                          teredo : Teredo: IPv6 packets in IPv4 UDP datagrams
                                   tunneling protocol.
                            tftp : IETF RFC 1350: Trivial File Transfer
                                   Protocol.
                            tivo : TiVo Service
                             tls : IETF RFC 4346: Transport Layer Security
                                   protocol.
                          tn3270 : IETF RFC1576 RFC2355: TN3270 terminal
                                   emulation via telnet.
                             tor : Tor internet anonymity protocol.
                     trusted_tcp : Traffic identified using a trusted TCP
                                   port number.
                     trusted_udp : Traffic identified using a trusted UDP
                                   port number.
                          tuxedo : Oracle TUXEDO Protocol.
                             tvu : TVU Networks media traffic.
                        ultravox : Ultravox streaming media protocol.
                     unknown_tcp : Unknown or unidentified TCP traffic.
                     unknown_udp : Unknown or unidentified UDP traffic.
                         ustream : Ustream media traffic.
                             utp : uTP: Micro Transport Protocol.
                        ventrilo : Ventrilo Protocol traffic.
                           viber : Viber Mobile traffic.
                          vmware : VMware Traffic.
                            vudu : VUDU on-demand video distribution
                           webex : Cisco Webex web conferencing
                          weixin : Weixin Instant Messaging Protocol
                        whatsapp : WhatsApp Protocol.
                           winmx : WinMX P2P File Sharing Protocol
                             wow : World of Warcraft Protocol
                        wsp_http : WSP transported HTTP traffic.
                        xboxlive : Xbox Live: Microsoft online game and media
                                   delivery service.
                            xmpp : IETF RFC 3920: Extensible Messaging and
                                   Presence Protocol.
                   xmpp_facebook : Facebook XMPP traffic.
                          xunlei : Xunlei Client.
                        xwindows : X Window System: A graphical user
                                   interface for networked computers
                 yahoo_file_xfer : Yahoo Instant Messaging Protocol File
                                   Transfer.
                        yahoo_im : Yahoo Instant Messaging Protocol.
                     yahoo_video : Yahoo Instant Messaging Protocol Webcam
                                   Video.
                         youtube : YouTube RTMP/RTMPE traffic.
==============================================================================
Number of protocols          : 181
*A:7x50-E11#
```

Application Profile Commands

app-profile

Syntax **app-profile** *app-profile-name* [**create**]
no app-profile *app-profile-name*

Context config>app-assure>group>policy

Description This command creates an application profile and enables the context to configure the profile parameters.

The **no** form of the command removes the application profile from the configuration.

Default none

Parameters *app-profile-name* — Specifies the name of the application profile up to 32 characters in length.

create — Mandatory keywork used when creating an application profile. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

capacity-cost

Syntax **capacity-cost** *cost*
nocapacity-cost

Context config>app-assure>group>policy>app-profile

Description This command configures an application profile capacity cost. Capacity-Cost based load balancing allows a cost to be assigned to diverted SAPs (with the app-profile) and this is then used for load-balancing SAPs between ISAs as well as for a threshold that notifies the operator if/when capacity planning has been exceeded.

Parameters *cost* — Specifies the profile capacity cost.

Values 1 — 65535

characteristic

Syntax **characteristic** *characteristic-name* **value** *value-name*
no characteristic *characteristic-name*

Context config>app-assure>group>policy>app-profile

Description This command assigns one of the existing values of an existing application service option characteristic to the application profile.

The **no** form of the command removes the characteristic from the application profile.

Default none

Parameters *characteristic-name* — Specifies the name of an existing ASO characteristic.

value *value-name* **—** Specifies the name for the application profile characteristic up to 32 characters.

divert

Syntax [**no**] **divert**

Context config>app-assure>group>policy>app-profile

Description This command enables the redirection of traffic to AA ISA for the system-wide forwarding classes diverted to application assurance (**divert-fc**) for AA subscribers using this application profile.

The **no** form of the command stops redirect of traffic to AA ISAs for the AA subscribers using this application profile.

Default no divert

aa-sub-suppressible

Syntax aa-sub-suppressible
no aa-sub-suppressible

Context config>app-assure>group>policy>app-profile

Description This command configures an app-profile as “aa-sub-suppressible”, this function is used in the context of an SRRP group interface. If an SRRP group interface is configured as “suppress-aa-sub” then subscribers with an app-profile configured as “aa-sub-suppressible” will not be diverted to Application Assurance.

The **no** form of the command restores the default behavior.

Default no aa-sub-suppressible

Application QoS Policy Commands

entry

Syntax [**no**] **entry** *entry-id* [**create**]

Context config>app-assure>group>policy>aqp

Description This command creates an application QoS policy entry. A flow that matches multiple Application QoS policies (AQP) entries will have multiple AQP entries actions applied. When a conflict occurs for two or more actions, the action from the AQP entry with the lowest numerical value takes precedence.

The **no** form of this command deletes the specified application QoS policy entry.

Default none

Parameters *entry-id* — An integer identifying the AQP entry.

Values 1 — 65535

create — Mandatory keyword creates the entry. The **create** keyword requirement can be enabled/ disabled in the **environment>create** context.

action

Syntax **action**

Context config>app-assure>group>policy>aqp>entry

Description This command enables the context to configure AQP actions to be performed on flows that match the AQP entry's match criteria.

bandwidth-policer

Syntax **bandwidth-policer** *policer-name*
no bandwidth-policer

Context config>app-assure>group>policy>aqp>entry>action

Description This command assigns an existing bandwidth policer as an action on flows matching this AQP entry. The match criteria for the AQP entry must specify a uni-directional traffic direction before a policer action can be configured. If a policer is used in one direction in an AQP match entry the same policer name cannot be used by another AQP entry which uses a different traffic direction match criteria.

When multiple policers apply to a single flow, the final action on a packet is the worse case of all policer outcome (for example, if one of the policers marks packet out of profile, the final marking will reflect that).

The **no** form of the command removes bandwidth policer from actions on flows matching this AQP entry.

Default no bandwidth-policer

Parameters *policer-name* — The name of the existing flow setup rate policer for this application assurance profile. The *policer-name* is configured in the **config>app-assure>group>policer** context.

drop

Syntax [**no**] **drop**

Context config>app-assure>group>policy>aqp>entry>action

Description This command configures the drop action on flows matching this AQP entry. When enabled, all flow traffic matching this AQP entry will be dropped. When drop action is part of a set of multiple actions to be applied to a single flow as result of one or more AQP entry match, drop action will be performed first and no other action will be invoked on that flow.

The **no** form of the command disables the drop action on flows matching this AQP entry.

Default no drop

error-drop

Syntax **error-drop** [**event-log** *event-log-name*]
no error-drop

Context config>app-assure>group>policy>aqp>entry>action

Description This command configures a drop action for error flows (bad IP checksums, tcp/udp port 0, etc.).

flow-count-limit

Syntax **flow-count-limit** *policer-name*
no flow-count-limit

Context config>app-assure>group>policy>aqp>entry>action

Description This command assigns an existing flow count limit policer as an action on flows matching this AQP entry.

The match criteria for the AQP entry must specify a uni-directional traffic direction before a policer action can be configured. If a policer is used in one direction in an AQP match entry the same policer name cannot be used by another AQP entry which uses a different traffic direction match criteria.

When multiple policers apply to a single flow, the final action on a packet is the worse case of all policer outcome (for example, if one of the policers marks packet out of profile, the final marking will reflect that).

The **no** form of the command removes this flow policer from actions on flows matching this AQP entry.

Default no flow-count-limit

Parameters *policer-name* — The name of the existing flow setup rate policer for this application assurance profile. The *policer-name* is configured in the **config>app-assure>group>policer** context.

flow-rate-limit

Syntax **flow-rate-limit** *policer-name* [**event-log** *event-log-name*]
no flow-rate-limit

Context config>app-assure>group>policy>aqp>entry>action

Description This command assigns an existing flow setup rate limit policer as an action on flows matching this AQP entry.

The match criteria for the AQP entry must specify a uni-directional traffic direction before a policer action can be configured. If a policer is used in one direction in an AQP match entry the same policer name cannot be used by another AQP entry which uses a different traffic direction match criteria.

When multiple policers apply to a single flow, the final action on a packet is the worse case of all policer outcome (for example, if one of the policers marks packet out of profile, the final marking will reflect that).

The **no** form of the command removes this flow policer from actions on flows matching this AQP entry.

Default no flow-rate-limit

Parameters *policer-name* — Specifies the policer name up to 32 characters in length.

event-log *event-log-name* — Specifies the event-log-name up to 32 characters in length which will be used when event logging is enabled.

fragment-drop

Syntax **fragment-drop** {**all** | **out-of-order**} [**event-log** *event-log-name*]
no fragment-drop

Context config>app-assure>group>policy>aqp>entry>action

Description This command specifies the action to apply to fragments.

Parameters **all** — All the fragments will be dropped.

out-of-order — All out of order fragments will be dropped.

event-log *event-log-name* — specifies if the dropping of fragments should be logged to the specified event log name.

gtp-filter

Syntax **gtp-filter** *gtp-filter-name*
no gtp-filter

Context config>app-assure>group>policy>aqp>entry>action

Description This command assigns an existing gtp filter as an action on flows matching this AQP entry.

The **no** form of the command removes this gtp filter from actions on flows matching this AQP entry.

Default no gtp-filter

Parameters *gtp-filter-name* — The name of the existing gtp-filter for this application assurance profile. The *gtp-filter-name* is configured in the **config>app-assure>group[:partition]>gtp>gtp-filter** context.

sctp-filter

Syntax **sctp-filter** *sctp-filter-name*
no sctp-filter

Context config>app-assure>group>policy>aqp>entry>action

Description This command assigns an existing sctp filter as an action on flows matching this AQP entry.

The **no** form of the command removes this sctp filter from actions on flows matching this AQP entry.

Default no gtp-filter

Parameters *sctp-filter-name* — The name of the existing sctp-filter for this application assurance profile. The *sctp-filter-name* is configured in the **config>app-assure>group[:partition]>sctp-filter** context.

http-enrich

Syntax **http-enrich** *http-enrich-name*
no http-enrich

Context config>app-assure>group>policy>aqp>entry>action

Description This command configures a the HTTP header enrichment template name that will be applied as defined in the tmnxBsxHttpEnrichTable. An empty value specifies no HTTP header enrichment template.

Parameters *http-enrich-name* — Specifes the HTTP header enrichment template name up to 32 characters inlength.

http-redirect

Syntax **http-redirect** *http-redirect–name* **flow-type** *flow-type*

no http-redirect

Context config>app-assure>group>policy>aqp>entry>action

Description This command assigns an existing http redirect policy as an action on flows matching this AQP entry.

The redirect only takes effect if the matching flows are HTTP and the condition specified after the **http-redirect** command, admitted flows or dropped-flows, is met. The condition specified by “dropped-flows” means the flow is dropped due to an AQP actions such as “flow rate/count policers” or “drop” actions. HTTP Policy Redirect on admitted-flows allows the operator to redirect HTTP traffic to a web portal while allowing non-HTTP matching the same AQP rule to be forwarded.

Note: No HTTP redirect will take place if HTTP redirect action and a “drop/flow-police” action are part of the default AQP policy, because in this case, any flow drop actions will take place before identification of the application/application-group.

The **no** form of the command removes http redirect from actions on flows matching this AQP entry.

Default no http-redirect

Parameters *http-redirect-name* — Specifies the name of the existing http policy redirect for this application assurance profile. The HTTP redirect name is configured in the **config>appassure>group>http-redirect** context.

flow-type *flow-type* **—**

Values **admitted-flows** — Redirect HTTP flows matching the AQP criteria.
dropped-flows — Redirects those HTTP flows that are dropped due to an AQP action.

http-error-redirect

Syntax **http-error-redirect** *redirect-name*
no http-error-redirect

Context config>app-assure>group>policy>aqp>entry>action

Description This command specifies the HTTP error redirect that will be applied as defined in the redirect table. An empty value specifies no HTTP error redirect.

Parameters *redirect-name* — Specifies an http-error redirect action, up to 32 characters in length, for flows matching this entry.

http-redirect

Syntax **http-redirect** *redirect-name* **flow-type** *flow-type*
no http-redirect

Context config>app-assure>group>policy>aqp>entry>action

Description This command configures an HTTP redirect action for flows of a specific type matching this entry

Default no http-redirect

Parameters *redirect-name* — Specifies the HTTP error redirect that will be applied as defined in the tmnxBsxHttpRedirErrTable. An empty value specifies no HTTP error redirect.

flow-type *flow-type* **—** Specifies the type of flow that will be redirected.

Values **admitted-flows** — This allows HTTP redirect for selective traffic steering of HTTP traffic while not affecting other traffic.
dropped-flows — This allows HTTP redirect on blocked traffic.

url-filter

Syntax **url-filter** *url-filter-name*
no url-filter *url-filter-name*

Context config>app-assure>group>aqp>entry>action

Description This command configures a url-filter action for flows matching this entry.

Parameters *url-filter-name* — The name of the url-filter policy.

characteristic

Syntax **characteristic** *characteristic-name*

Context config>app-assure>group>aqp>entry>action

Description This command enables the system to use the value of the characteristic name specified in the app-qos-policy url-filter action for the configurable ICAP x-header name provisioned in the url-filter policy. The ICAP server can then use this value to decide which url-filter policy to apply instead of applying a filter policy based on the subscriber name.

Parameters *characteristic-name* — Specifies the name of the characteristic.

http-notification

Syntax **http-notification** *http-notification*
no http-notification

Context config>app-assure>group>policy>aqp>entry>action

Description This command configures an HTTP notification action for flows matching this entry.

Parameters *http-notification* — specifies the Application-Assurance HTTP Notification that will be applied as defined in the tmnxBsxHttpNotifTable. If no string is configured then no HTTP notification will occur.

mirror-source

Syntax **mirror-source** [**all-inclusive**] *mirror-service-id*
no mirror-source

Context config>app-assure>group>policy>aqp>entry>action

Description This command configures an application-based policy mirroring service that uses this AA ISA group's AQP entry as a mirror source. When configured, AQP entry becomes a mirror source for IP packets seen by the AA (note that the mirrored packet is an IP packet analyzed by AA and does not include encapsulations present on the incoming interfaces).

Default no mirror-source

Parameters **all-inclusive —** Specifies that all packets during identification phase that could match a given AQP rule are mirrored in addition to packets after an application identification completes that match the AQP rule. This ensures all packets of a given flow are mirrored at a cost of sending unidentified packets that once the application is identified will no longer match this AQP entry.

mirror-service-id — Specifies the mirror source service ID to use for flows that match this policy.

Values 1 — 214748364
svc-name: 64 char max

remark

Syntax **remark**

Context config>app-assure>group>policy>aqp>entry>action

Description This command configures remark action on flows matching this AQP entry.

dscp

Syntax **dscp in-profile** *dscp-name* **out-profile** *dscp-name*
no dscp

Context config>app-assure>group>policy>aqp>entry>action>remark

Description This command enables the context to configure DSCP remark action or actions on flows matching this AQP entry. When enabled, all packets for all flows matching this AQP entry will be remarked to the configured DSCP name.

DSCP remark can only be applied when the entry remarks forwarding class or forwarding class and priority. In-profile and out-of profile of a given packet for DSCP remark is assessed after all AQP policing and priority remarking actions took place.

The **no** form of the command stops DSCP remarking action on flows matching this AQP entry.

Parameters **in-profile** *dscp-name* — Specifies the DSCP name to use to remark in-profile flows that match this policy.

out-profile *dscp-name* **—** Specifies the DSCP name to use to remark out-of-profile flows that match this policy.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

fc

Syntax **fc** *fc-name*
no fc

Context config>app-assure>group>policy>aqp>entry>action>remark

Description This command configures remark FC action on flows matching this AQP entry. When enabled, all packets for all flows matching this AQP entry will be remarked to the configured forwarding class.

The **no** form of the command stops FC remarking action on packets belonging to flows matching this AQP entry

Parameters *fc-name* — Configure the FC remark action for flows matching this entry.

Values be, l2, af, l1, h2, ef, h1, nc

priority

Syntax **priority** *priority-level*
no priority

Context config>app-assure>group>policy>aqp>entry>action>remark

Description This command configures remark discard priority action on flows matching this AQP entry. When enabled, all packets for all flows matching this AQP entry will be remarked to the configured discard priority.

Default no priority

Parameters *priority-level* — Specifies the priority to apply to a packet.

Values high, low

session-filter

Syntax **session-filte**r *session-filter-name*
no session-filter

Context config>app-assure>group>policy>aqp>entry>action

Description This command specifies the Application-Assurance session filter that will be evaluated. If no session filters are specified then no session filters will be evaluated.

Default none

Parameters *session-filter-name* — Specifies the session filter to be applied.

match

Syntax **match**

Context config>app-assure>group>policy>aqp>entry

Description This command enables the context to configure flow match rules for this AQP entry. A flow matches this AQP entry only if it matches all the match rules defined (logical and of all rules). If no match rule is specified, the entry will match all flows.

aa-sub

Syntax **aa-sub esm** {**eq** | **neq**} *sub-ident-string*
aa-sub sap {**eq** | **neq**} *sap-id*
aa-sub spoke-sdp {**eq** | **neq**} *sdp-id:vc-id*
aa-sub transit {**eq** | **neq**} *transit-aasub-name*
no aa-sub

Context config>app-assure>group>policy>aqp>entry>match

Description This command specifies a Service Access Point (SAP) or an ESM subscriber as matching criteria.

The **no** form of the command removes the SAP or ESM matching criteria.

Parameters **eq —** Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

sub-ident-string — Specifies the name of an existing application assurance subscriber.

sap-id — Specifies the SAP ID.

sap *sap-id* **—** Specifies the physical port identifier portion of the SAP definition.

sdp-id:vc-id — Specifies the spoke SDP ID and VC ID.

Values 1 — 17407
1 — 4294967295

transit-aa-sub-name — Specifies the name of a transit AA subscriber.

app-group

Syntax **app-group** {**eq** | **neq**} *application-group-name*
no app-group

Context config>app-assure>group>policy>aqp>entry>match

Description This command adds app-group to match criteria used by this AQP entry.

The **no** form of the command removes the app-group from match criteria for this AQP entry.

Default no app-group

Parameters **eq —** Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

application-group-name — The name of the existing application group entry. The application-group-name is configured in the **config>app-assure>group>policy>aqp>entry>match** context.

application

Syntax **application** {**eq** | **neq**} *application-name*
no application

Context config>app-assure>group>policy>aqp>entry>match

Description This command adds an application to match criteria used by this AQP entry.

The **no** form of the command removes the application from match criteria for this AQP entry.

Default no application

Parameters **eq —** Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

application-name — The name of name existing application name. The application-group-name is configured in the **config>app-assure>group>policy>aqp>entry>match** context.

characteristic

Syntax **characteristic** *characteristic-name* **eq** *value-name*
no characteristic

Context config>app-assure>group>policy>aqp>entry>match

Description This command adds an existing characteristic and its value to the match criteria used by this AQP entry.

The **no** form of the command removes the characteristic from match criteria for this AQP entry.

Default no characteristic

Parameters **eq —** Specifies that the value configured and the value in the flow are equal.

characteristic-name — The name of the existing ASO characteristic up to 32 characters in length.

value-name — The name of an existing value for the characteristic up to 32 characters in length.

charging-group

Syntax **charging-group** {**eq** | **neq**} *charging-group-name*
no charging-group

Context config>app-assure>group>policy>aqp>entry>match

Description This command adds charging-group to match criteria used by this AQP entry.

The **no** form of the command removes the charging-group from match criteria for this AQP entry.

Default no charging-group

Parameters **eq** — Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

charging-group-name — The name of the existing application group entry. The application-group nameis configured in the **config>app-assure>group>policy>aqp>entry>match** context.

dscp

Syntax **dscp** {**eq** | **neq**} **dscp-name**
no dscp

Context config>app-assure>group>policy>aqp>entry>match
config>app-assure>group>sess-fltr>entry>match

Description This command adds a DSCP name to the match criteria used by this entry.

The no form of the command removes dscp from match criteria for this entry.

Default no dscp

Parameters **eq** — Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

dscp-name — The DSCP name to be used in match.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

dst-ip

Syntax **dst-ip** {**eq** | **neq**} *ip-address*
dst-ip {**eq** | **neq**} *ip-prefix-list ip-prefix-list-name*
no dst-ip

Context config>app-assure>group>policy>aqp>entry>match
config>app-assure>group>sess-fltr>entry>match

Description This command specifies a destination IP address to use as match criteria.

Parameters **eq** — Specifies a that a successful match occurs when the flow matches the specified address or prefix.

neq — Specifies that a successful match occurs when the flow does not match the specified address or prefix.

ip-address — Specifies a valid unicast address.

Values	ipv4-address	a.b.c.d[/mask]	
		mask - [1..32]	
	ipv6-address	x:x:x:x:x:x:x:x/prefix-length	
		x:x:x:x:x:x:d.d.d.d	
		x - [0..FFFF]H	
		d - [0..255]D	
		prefix-length	[1..128]

dst-port

Syntax **dst-port** {**eq** | **neq**} *port-num*
dst-port {**eq** | **neq**} **range** *start-port-num end-port-num*
no dst-port

Context config>app-assure>group>policy>aqp>entry>match
config>app-assure>group>sess-fltr>entry>match

Description This command specifies a destination TCP/UDP port or destination range to use as match criteria.

The **no** form of the command removes the parameters from the configuration.

Parameters **eq** — Specifies that a successful match occurs when the flow matches the specified port.

neq — Specifies that a successful match occurs when the flow does not match the specified port.

port-num — Specifies the destination port number.

Values 0 — 65535

start-port-num end-port-num — Specifies the start or end destination port number.

Values 0 — 65535

ip-protocol-num

Syntax **ip-protocol-num** {**eq** | **neq**} *protocol-id*
no ip-protocol-num

Context config>app-assure>group>policy>aqp>entry>match

Description This command configures the IP protocol to use to use as match criteria.

The **no** form the command removes the protocol from the match criteria.

Default none

Parameters **eq** — Specifies that the value configured and the value in the flow must be equal.

neq — Specifies that the value configured differs from the value in the flow.

protocol-id — Specifies the decimal value representing the IP protocol to be used as an IP filter match criterion. Well known protocol numbers include ICMP (1), TCP (6), UDP (17).

Values 1 — 255 (Decimal, Hexadecimal, or Binary representation).
Supported IANA IP protocol names:
crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, sctp, stp

src-ip

Syntax **src-ip** {**eq** | **neq**} *ip-address*
src-ip {**eq** | **neq**} *ip-prefix-list ip-prefix-list-name*
no src-ip

Context config>app-assure>group>policy>aqp>entry>match
config>app-assure>group>sess-fltr>entry>match

Description This command specifies a source TCP/UDP address to use as match criteria.

Parameters **eq** — Specifies that a successful match occurs when the flow matches the specified address or prefix.

neq — Specifies that a successful match occurs when the flow does not match the specified address or prefix.

ip-address — Specifies a valid IPv4 unicast address.

ip-address — Specifies a valid unicast address.

Values

ipv4-address	a.b.c.d[/mask]	
	mask - [1..32]	
ipv6-address	x:x:x:x:x:x:x:x/prefix-length	
	x:x:x:x:x:x:d.d.d.d	
	x - [0..FFFF]H	
	d - [0..255]D	
	prefix-length	[1..128]

src-port

Syntax **src-port** {**eq** | **neq**} *port-num*
src-port {**eq** | **neq**} **range** *start-port-num end-port-num*
no src-port

Context config>app-assure>group>policy>aqp>entry>match
config>app-assure>group>sess-fltr>entry>match

Description This command specifies a source IP port or source range to use as match criteria.

The **no** form of the command removes the parameters from the configuration.

Parameters **eq** — Specifies that a successful match occurs when the flow matches the specified port.

neq — Specifies that a successful match occurs when the flow does not match the specified port.

port-num — Specifies the source port number.

Values 0 — 65535

start-port-num end-port-num — Specifies the start or end source port number.

Values 0 — 65535

traffic-direction

Syntax **traffic-direction** {**subscriber-to-network | network-to-subscriber | both**}

Context config>app-assure>group>policy>aqp>entry>match

Description This command specifies the direction of traffic where the AQP match entry will be applied.

To use a policer action with the AQP entry the match criteria must specify a traffic-direction of either subscriber-to-network or network-to-subscriber.

Default both

Parameters **subscriber-to-network —** Traffic from a local subscriber will macth this AQP entry.

network-to-subscriber — Traffic to a local subscriber will match this AQP entry.

both — Combines subscriber-to-network and network-to-subscriber.

Application Service Options Commands

characteristic

Syntax **characteristic** *characteristic-name* [**create**]
no characteristic *characteristic-name*

Context config>app-assure>group>policy>aso

Description This command creates the characteristic of the application service options.

The **no** form of the command deletes characteristic option. To delete a characteristic, it must not be referenced by other components of application assurance.

Default none

Parameters *characteristic-name* — Specifies a string of up to 32 characters uniquely identifying this characteristic.

create — Mandatory keywork used to create when creating a characteristic. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

default-value

Syntax **default-value** *value-name*
no default-value

Context config>app-assure>group>policy>aso>char

Description This command assigns one of the characteristic values as default.

When a default value is specified, app-profile entries that do not explicitly include this characteristic inherit the default value and use it as part of the AQP match criteria based on that app-profile.

A default-value is required for each characteristic. This is evaluated at commit time.

The **no** form of the command removes the default value for the characteristic.

Default none

Parameters *value-name* — Specifies the name of an existing characteristic value.

value

Syntax [**no**] **value** *value-name*

Context config>app-assure>group>policy>aso>char

Description This command configures a characteristic value.

The **no** form of the command removes the value for the characteristic.

Default none

Parameters *value-name* — Specifies a string of up to 32 characters uniquely identifying this characteristic value.

Custom Protocol Commands

custom-protocol

Syntax **custom-protocol** *custom-protocol-id* [**ip-prot-num {tcp | udp} create**]
custom-protocol *custom-protocol-id*
no custom-protocol *custom-protocol-id*

Context config>app-assure>group>policy

Description This command creates and enters configuration context for custom protocols. Custom protocols allow the creation of TCP and UDP-based custom protocols (based on the *ip-protocol-num* option) that employ pattern-match at offset in protocol signature definition.

Operator-configurable custom-protocols are evaluated ahead of any Alcatel-Lucent provided protocol signature in order of **custom-protocol-id** (the lower ID is matched first in case of flow matching multiple custom-protocols) within the context the protocol is defined.

Custom protocols must be created before they can be used in application definition but do not have to be enabled. To reference a custom protocol in application definition, or any other CLI configuration one must use protocol name that is a concatenation of “custom_” and <custom-protocol-id>, (for example custom_01, custom_02 ... custom_10, etc.). This concatenation is also used when reporting custom protocol statistics.

Parameters *custom-protocol-id* — Specifies the index into the protocol list that defines a custom protocol for application assurance.

Values 1 — 10

protocol-id — Specifies the IP protocol to match against for the custom protocol.

Values 6, 17, Protocol numbers accepted in DHB,
keywords: udp, tcp

create — Mandatory keyword used when creating custom protocol. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

expression

Syntax **expression** *expr-index* **eq** *expr-string* **offset** *payload-octet-offset* **direction** direction
no expression expr-index

Context config>app-assure>group>policy>custom-protocol

Description This command configures an expression string value for pattern-based custom protocols match. A flow matches a custom protocol if the specified string is found at an offset of a TCP/UDP of the first payload packet.

Options:

client-to-server — A pattern will be matched against a flow from a TCP client.

server-to-client — A pattern will be matched against a flow from a TCP server.

any – A pattern will be matched against a TCP/UDP flow in any direction (towards or from AA subscriber)

The **no** form of this command deletes a specified string expression from the definition.

Parameters *expr-index* — Specifies the expression substring index.

Values 1

expr-string — Denotes a printable ASCII string, up to 16 characters, used to define a custom protocol match. Rules for expr-string characters:

- Must contain printable ASCII characters.
- Must not contain the “double quote” character or the “ ” (space) character on its own.
- Match is case sensitive.
- Must not include any regular expression meta-characters.

The “\” (slash) character is used as an ESCAPE sequence. The following ESCAPE sequences are permitted within the expr-string:

Character to match	expr-string input
Hexidecimal Octet YY	\xYY

Note: An expr-string that uses the '\' (backslash) ESCAPE character which is not followed by a “\” or “\x” and a 2-digit hex octet is not valid.

offset *payload-octet-offset* **—** specifies the offset (in octets) into the protocol payload, where the expr-string match criteria will start.

Values 0 — 127

direction *direction* **—** Specifies the protocol direction to match against to resolve to a custom protocol.

Values client-to-server, server-to-client, any

Session Filter Commands

session-filter

Syntax **session-filter** *session-filter-name* [**create**]
no session-filter *session-filter-name*

Context config>app-assure>group

Description This command creates a session filter.

Parameters *session-filter-name* — Creates a session filter name up to 32 characers in length.

default-action

Syntax **default-action** {**permit** | **deny**} [**event-log** *event-log-name*]
no default-action

Context config>app-assure>group>sess-fltr

Description This command specifies the default action to take for packets that do not match any filter entries.

The **no** form of the command reverts the default action to the default value (forward).

Default **deny**

Parameters **deny —** Packets matching the criteria are denied

permit — Packets matching the criteria are permitted.

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context config>app-assure>group>policy>sess-fltr

Description This command configures a particular Application-Assurance session filter match entry. Every session filter can have zero or more session filter match entries. An application filter entry or entries configures match attributes of an application.

The **no** form of this command deletes the specified entry.

Default none

Parameters *entry-id* — An integer that identifies the entry.

Values 1 — 65535

create — Keyword used to create the entry.

match

Syntax **match**

Context config>app-assure>group>sess-fltr>entry

Description This command enables the context to configure session conditions for this entry.

dns-ip-cache

Syntax **dns-ip-cache** *dns-ip-cache-name*

Context config>app-assure>group>sess-fltr>entry>match

Description This command configures a DNS IP cache using session filter DST IP match criteria. It is typically combine with an allow action in the context of captive-redirect.

Parameters *dns-ip-cache-name* — Specifies the name of the dns-ip-cache policy.

action

Syntax **action** {**permit|deny**} [**event-log** *event-log-name*]

Context config>app-assure>group>sess-fltr>entry

Description This command configures the action for this entry.

Parameters **deny —** Packets matching the criteria are denied

permit — Packets matching the criteria are permitted.

http-redirect

Syntax **http-redirect** *http-redirect-name*

Context config>app-assure>group>sess-fltr>entry>action

Description This command configures a session filter entry action to HTTP redirect the subscriber flows. The HTTP redirect policy referenced within this session filter entry is configured for captive redirect with the appropriate VLAN id assigned.

Parameters *http-redirect-name* — Specifies the name of the http-redirect-policy.

Statistics Commands

statistics

Syntax **statistics**

Context config>app-assure>group

Description This command enables the context to configure accounting and billing statistics for this AA ISA group.

app-group

Syntax **app-group** *app-group-name* **export-using** *export-method* [*export-method*...(up to 2 max)]
app-group *app-group-name* **no-export**
no app-group *app-group-name*

Context config>app-assure>group>statistics>aa-sub

Description This command enables the context to configure accounting and statistics collection parameters per system for application groups of application assurance for a given AA ISA group/partition.

The **no** form of the command removes the application group name.

Default none

Parameters *app-group-name* — Specifies an existing application group name up to 32 characters in length.

export-using *accounting-policy* — Specifies that the method of stats export to be used.

no-export — Allows the operator to enable the referred to app-grp to be selected (via Diameter) for Gx-usage monitoring. Gx usage monitoring is enabled automatically (and this command is not shown) if the **export-using** parameter is selected for the respective app group.

Note: usage-monitoring must be enabled at the group:partition level (**config>app-assure>group>statistics>aa-sub>usage-monitoring**) as well in order to allow any application/ application group/charging group usage-monitoring.

aa-sub

Syntax **aa-sub**

Context config>app-assure>group>statistics

Description This command enables the context to configure accounting and statistics collection parameters per application assurance subscribers.

aa-sub-study

Syntax **aa-sub-study** *study-type*

Context config>app-assure>group>statistics

Description This command enables the context to configure accounting and statistics collection parameters per application assurance special study subscribers.

Parameters *study-type* — Specifies special study protocol subscriber stats.

Values application, protocol

application

Syntax **application** *application-name* **export-using** *export-method*
application *application-name* **no-export**
no application *application-name*

Context config>app-assure>group>statistics>aa-sub

Description This command configures aa-sub accounting statistics for export of applications of a given AA ISA group/partition.

The no form of the command removes the application name.

Default none

Parameters *application-name* — Specifies an existing application name up to 32 characters in length.

export-using *accounting-policy* — Specifies that the method of stats export to be used. Accounting-policy is the only option for application statistics.

no-export — Allows the operator to enable the referred application group to be selected (via Diameter) for Gx-usage monitoring. Gx usage monitoring is enabled automatically (and this command is not shown) if the **export-using** parameter is selected for the respective application group.

Note: usage-monitoring must be enabled at the group:partition level (**config>app-assure>group>statistics>aa-sub>usage-monitoring**) as well in order to allow any application/application group/charging group usage-monitoring.

charging-group

Syntax **charging-group** *charging-group-name* **export-using** *export-method* [*export-method*...(up to 2 max)]
charging-group *charging-group-name* **no-export**
no charging-group *charging-group-name*

Context config>aa>group>statistics>aa-sub

Description This command configures aa-sub accounting statistics for export of charging groups of a given AA ISA group/partition.

The **no** form of the command removes the parameters from the configuration.

Default none

Parameters *charging-group-name* — The name of the charging group. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

export-using *export-method* **—** Specifies that the method of stats export to be used.

Values accounting, policy, radius-accounting-policy

no-export — Allows the operator to enable the referred to a charging group to be selected (via Diameter) for Gx-usage monitoring. Gx usage monitoring is enabled automatically (and this command is not shown) if the **export-using** parameter is selected for the respective charging group.

Note: usage-monitoring must be enabled at the group:partition level (**config>app-assure>group>statistics>aa-sub>usage-monitoring**) as well in order to allow any application/application group/charging group usage-monitoring.

accounting-policy

Syntax **accounting-policy** *acct-policy-id*

Context
config>app-assure>group>statistics>app-grp
config>app-assure>group>statistics>app
config>app-assure>group>statistics>protocol
config>app-assure>group>statistics>aa-partition
config>app-assure>group>statistics>aa-sub
config>app-assure>group>statistics>aa-sub-study
config>isa>aa-grp>statistics

Description This command specifies the exisiting accounting policy to use for AA. Accounting policies are configured in the **config>log>accounting-policy** context.

Parameters *acct-policy-id* — Specifies the exisiting accounting policy to use for applications.

Values 1 — 99

aggregate-stats

Syntax
aggregate-stats export-using *export-method*
aggregate-stats no-export

Context config>app-assure>group>statistics>aa-sub

Description This command configures aa-sub accounting statistics for export of aggregate statistics of a given subscriber.

Default none

Parameters **export-using** *export-method* **—** Specifies the method of statistics export to be used.

Values accounting-policy (this is the only option for sub-aggregate statistics, and it is only supported in residential and VPN sub-scale modes).

no-export — Disables the export.

protocol

Syntax **protocol**

Context config>app-assure>group>statistics

Description This command enables the context to configure accounting and statistics collection parameters per-system for protocols of application assurance for a given AA ISA group/partition.

aa-sub

Syntax [**no**] **aa-sub** {**esm** *sub-ident-string* **| sap** s*ap-id*} **| spoke-sdp** *sdp-id:vc-id* | **transit** *transit-aasub-name*}

Context config>app-assure>group>statistics>aa-sub-study

Description This command adds an existing subscriber identification to a group of special study subscribers (for example, subscribers for which per subscriber statistics and accounting records can be collected for protocols and applications of application assurance).

The **no** form of the command removes the subscriber from the special study subscribers.

Up to 100 subscribers can be configured into the special study group for protocols and up to a 100 potentially different subscribers can be configured into the special study group for applications.

When adding a subscriber to the special study group, accounting records and statistics generation will commence immediately. When removing a subscriber from the group, special study statistics and accounting records for that subscriber in the current interval will be lost.

Default none

Parameters *sub-ident-string* — The name of a subscriber ID. Note that the subscriber does not need to be currently active. Any sub-ident-string will be accepted. When the subscriber becomes active, statistics generation will start automatically at that time.

esm *sub-ident-string* **—** Specifies an existing subscriber identification policy name.

sap *sap-id* **—** Specifies the physical port identifier portion of the SAP definition.

spoke-id *sdp-id:vc-id* — Specifies the spoke SDP ID and VC ID.

Values 1 — 17407
1 — 4294967295

transit *transit-aasub-name* **—** Specifies an existing transit subscriber name string up to 32 characters in length.

collect-stats

Syntax [**no**] **collect-stats**

Context config>app-assure>group>statistics>app-grp
config>app-assure>group>statistics>application
config>app-assure>group>statistics>protocol
config>app-assure>group>statistics>aa-partition
config>app-assure>group>statistics>aa-sub
config>app-assure>group>statistics>aa-sub-study
config>isa>aa-grp>statistics

Description This command enables statistic collection within the applicable context.

Default disabled

traffic-type

Syntax [**no**] **traffic-type**

Context config>app-assure>group>statistics>aa-partition

Description This command enables traffic type statistics collection within an aa-partition.

The no form of the command disables traffic type statistics collection.

exclude-tcp-retrans

Syntax [**no**] **exclude-tcp-retrans**

Context config>app-assure>group>statistics>aa-sub

Description This command is to only to EPC. When enabled, TCP errors and retransmission packets are not counted for the purpose of CBC. This setting has no impact on app/app-group aggregate AA stats.

max-throughput-stats

Syntax [**no**] **max-throughput-stats**

Context config>app-assure>group>statistics>app-sub

Description This command enables the collection of max-throughput statistics.

The **no** form of the command disables the collection.

protocol

Syntax **protocol** *protocol-name* **export-using** *export-method*

no protocol

Context config>app-assure>group>statistics>app-sub

Description This command configures aa-sub accounting statistics for export of protocols of a given AA ISA group/partition.

The no form of the command removes the protocol name.

Default none

Parameters *protocol-name* — Specifies an existing protocol name up to 32 characters in length.

export-using *export-method* **—** Specifies that the method of stats export to be used. Accounting-policy is the only option for protocol statistics.

radius-accounting-policy

Syntax **radius-accounting-policy** *rad-acct-plcy-name*
no radius-accounting-policy

Context config>aa>group>statistics>aa-sub

Description This command specifies an existing subscriber RADIUS based accounting policy to use for AA. RADIUS Accounting policies are configured in the **config>application-assurance>radius-accounting-policy** context.

Parameters *rad-acct-plcy-name* — The name of the policy. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

usage-monitoring

Syntax [**no**] **usage-monitoring**

Context config>aa>group>statistics>aa-sub

Description This command enables Gx usage monitoring the given AA group/partition. It can only be enabled if there is enough usage monitoring resources for all existing subs. Once disabled, all monitoring instances for AA subscriber(s) are silently removed (no PCRF notifications) and all subsequent AA Gx usage monitoring messages are ignored.

Default Disabled for Gx usage monitoring.

Policy Commands

transit-ip-policy

Syntax **transit-ip-policy** *ip-policy-id* [**create**]
no transit-ip-policy *ip-policy-id*

Context config>application-assurance>group>policy

Description This command defines a transit AA subscriber IP policy. Transit AA subscribers are managed by the system through the use of this policy assigned to services, which determines how transit subs are created and removed for that service.

The **no** form of the command deletes the policy from the configuration. All associations must be removed in order to delete a policy.

Default no transit-ip-policy

Parameters *ip-policy-id* — An integer that identifies a transit IP profile entry.

Values 1 — 65535

create — Keyword used to create the entry.

gtp

Syntax **gtp**

Context config>app-assure>group:[partition]

Description This command allows AA to treat traffic on UDP port number 2152 as GTP-u. Without further specifying any other parameters within this GTP context, AA performs basic GTP-u header sanity checks and discards packets that are malformed. This GTP context allows the operator to configure various GTP filters (maximum of 128 GTP filters).

Default shutdown

Parameters *event-log* — specifies the event log name to be used to log discards due to GTP-u basic header sanity checks.

gtp-filter

Syntax **gtp-filter** *filter-name*
no gtp-filter

Context config>app-assure>group>gtp

Description This command allows AA to treat traffic on UDP port number 2152 as GTP-u. Without further specifying any other parameters within this GTP context, AA performs basic GTP-u header sanity checks and discards packets that are malformed. This GTP context allows the operator to configure various GTP filters (maximum of 128 GTP filters).

Default no gtp-filter

Parameters *event-log* — specifies the event log name to be used to log discards due to GTP filter configured actions. This includes discards due to packet exceeding maximum configured packet length, packet discarded due to message type filtering and/or packets that fail the extensive GTP-u header validation performed for GTP-U messages that are allowed by the filter.

max-payload-length — Specifies the maximum allowed packet length.

message-type — Creates profile for a GTP filter that filters certain message types.

create — Keyword used to create the GTP filter name and parameters.

max-payload-length

Syntax **max-payload-length** *bytes*
no max-payload-length

Context config>app-assure>group>gtp>gtp-filter

Description This command specifies the maximum allowed GTP payload size.

The **no** form of the command removes this gtp message length filter.

Default no max-payload-length

Parameters *bytes* — Packet length in bytes.

message-type

Syntax **message-type**

Context config>app-assure>group>gtp>gtp-filter

Description This command specifies the context for configuration of GTP message-type filtering.

Default *none* — if no message-type is specified within a filter, then all GTP message types are allowed.

default-action

Syntax **default-action** {**permit** |**deny**}

Context config>app-assure>group>gtp>gtp-filter>message-type

Description Thios command configures the default action for all GTP message types.

Parameters **permit —** Specifies to permit packets that do not match any message entries.

deny — Specifies to deny packets that do not match any message entries.

entry

Syntax **entry** *entry-id* **value** *gtp-message-value* **action** {**permit|deny**}
no entry *entry-id*

Context config>app-assure>group>gtp>gtp-filter>message-type

Description This command configures an entry for a specific GTP message type value.

Parameters *entry-id* — Specifies the index into the GTP message value list that defines a custom message-type action.

Values 1 — 255

value *gtp-message-value* **—** Specifies a GTP message value.

Values 1 — 255 or 256 characters in length

action {**permit|deny**} **—** Specifies the action to take for packets that match this GTP filter message entry.

value

Syntax **value** *gtp-message-value* **action** {**permit | deny**}

Context config>app-assure>group>gtp>gtp-filter>message-type

Description This command specifies if a GTP message-type is allowed or not.

The **no** form of the command removes this gtp message-type. The “default action “ for the gtp-filter>message-type is applied.

Default none

Parameters *gtp-message-value* **—** specifies the GTP-u message type, either as numeric value [1..255] or as a string: { echo-request, echo-response, error-indication, g-pdu, supported-extension-headers-notification}.

action{**permit |deny**} **—** Allow or deny the configured message type.

sctp-filter

Syntax **sctp-filter** *filter-name*
no sctp-filter

Context config>app-assure>group

Description This command enables the context to configure Stream Control Transmission Protocol (SCTP) parameters.

The **no** form of the command removes this filter.

Default no sctp-filter

Parameters *filter-name* — Specifies the SCTP filter name up to 32 characters in length.

ppid

Syntax **ppid**

Context config>app-assure>group>policy>sctp-filter

Description This command enables the context to configure actions for specific or default Payload Protocol Identifiers (PPIDs).

default-action

Syntax **default-action** {**permit** |**deny**}

Context config>app-assure>group>policy>sctp-filter>ppid

Description This command configures the default action for all SCTP PPIDs.

Default permit

Parameters **permit —** Specifies to permit packets that do not match any PPID entries.

deny — Specifies to deny packets that do not match any PPID entries.

ppid-range

Syntax **ppid-range min** *min-ppid* **max** *max-ppid*

Context config>app-assure>group>policy>sctp-filter

Description This command specifies the range of PPID values that are allowed by AA SCTP filter firewall.

The **no** form of the command removes this PPID range.

Default None

Parameters **min** *min-ppid* — specifies the minimum SCTP Payload Protocol Identifier (PPID) to be permitted by the SCTP filter. The value must be less than or equal to the **max** *max-ppid* value.

max *max-ppid* — Specifies the minimum SCTP Payload Protocol Identifier (PPID) to be permitted by the SCTP filter. The value must be less greater or equal to the **max** *max-ppid* value.

Values 0 — 4294967295

entry

Syntax **entry** *ppid-value* **action** {**permit|deny**}
no entry *ppid-value*

Context config>app-assure>group>policy>sctp-filter>ppid

Description This command specifies if an SCTP PPID value is allowed or not.

The **no** form of the command removes this PPID. In which case, the default action for the **sctp-filter>ppid** is applied.

Default None

Parameters *ppid-value* — Specifies the PPID value, either as numeric value or as a string.

Values 0 — 4294967295 D, 256 chars max

action {**permit** | **deny**} **—** Specifies to allow or deny the configured PPID.

aqp-initial-lookup

Syntax **aqp-initial-lookup**
no aqp-initial-lookup

Context config>app-assure>group:[partition]

Description This command allows AA to perform AQP lookups on flows prior to complete application identification. As usual, AQP will be looked up again on identification complete. Without this, AA executes AQPs that are part of what so called "sub-default policy". Sub-default policy is formed by regular AQPs that contain ASOs, subID and/or flow direction as matching condition(s).

This behavior is required, for example, in order to be able apply GTP and SCTP filtering on the first packet of a new GTP/SCTP flow (AQP matching conditions in this case contains protocol id).

The **no** form of the command forces complete AQP look up on identification finish stage only

Default no aqp-initial-lookup

dhcp

Syntax **dhcp**

Context config>app-assure>group>policy>transit-ip-policy

Context This command enables dynamic DHCP-based management of transit aa-subs for the transit-ip-policy. This is mutually exclusive to other types management of transit subs for a given transit-ip-policy.

ipv6-address-prefix-length

Syntax **ipv6-address-prefix-length** *IPv6 prefix length*
no ipv6-address-prefix-length

Context config>app-assure>group>policy>transit-ip-policy

Description This command configures a transit IP policy IPv6 address prefix length.

Default 0

Parameters *IPv6 prefix length* — Specifies the prefix length of IPv6 addresses in this policy for both static and dynamic transits.

Values 32 — 64

radius

Syntax **radius**

Context config>app-assure>group>policy>transit-ip-policy

Description This command enables dynamic radius based management of transit aa-subs for the transit-ip-policy. This is mutually exclusive to other types management of transit subs for a given transit-ip-policy.

authentication-policy

Syntax **authentication-policy** *name*
no authentication-policy

Context config>app-assure>group>policy>transit-ip-policy>radius

Description This command configures the RADIUS authentication-policy for the IP transit policy.

seen-ip-radius-acct-policy

Syntax **seen-ip-radius-acct-policy** *rad-acct-plcy-name*
no seen-ip-radius-acct-policy

Context config>app-assure>group>policy>transit-ip-policy>radius

Description This command refers to a RADIUS accounting-policy to enable seen-IP notification.

The no form of the command removes the policy.

Default no seen-ip-radius-acct-policy

static-aa-sub

Syntax **static-aa-sub** *transit-aasub-name*
static-aa-sub *transit-aasub-name* **app-profile** *app-profile-name* [**create**]
no static-aa-sub transit-aasub-name

Context config>app-assure>group>policy>transit-ip-policy

Description This command configures static transit aa-subs with a name and an app-profile. A new transit sub with both a name and an app-profile is configured with the create command. Static transit aa-sub must have an explicitly assigned app-profile. An existing transit sub can optionally be assigned a different app-profile, or this command can be used to enter the static-aa-sub context.

The **no** form of the command deletes the named static transit aa-sub from the configuration.

Default no transit-ip-policy

Parameters *transit-aasub-name* — Specifies the name of a transit subscriber up to 32 characters in length.

app-profile-name — Specifies the name of an existing application profile up to 32 characters in length.

create — Keyword used to create a new app-profile entry.

ip

Syntax [**no**] **ip** *ip-address*

Context config>app-assure>group>policy>transit-ip-policy>static-aa-sub

Description This command configures the /32 ip address for a static transit aa-sub.

The **no** form of the command deletes the ip address assigned to the static transit aa-sub from the configuration.

Default no ip

Parameters *ip-address* — Specifies the IP address in a.b.c.d form.

Values ipv6-address/prefix: ipv6-address x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x [0 — FFFF]H
d [0 — 255]D
prefix-length /32 to /64

sub-ident-policy

Syntax **sub-ident-policy** *sub-ident-policy-name*

Context config>app-assure>group>policy>transit-ip-policy

Description This command associates a subscriber identification policy to this SAP. The subscriber identification policy must be defined prior to associating the profile with a SAP in the config>subscribermgmt>sub-ident-policy context.

Subscribers are managed by the system through the use of subscriber identification strings. A subscriber identification string uniquely identifies a subscriber. For static hosts, the subscriber identification string is explicitly defined with each static subscriber host.

For dynamic hosts, the subscriber identification string must be derived from the DHCP ACK message sent to the subscriber host. The default value for the string is the content of Option 82 CIRCUIT-ID and REMOTE-ID fields interpreted as an octet string. As an option, the DHCP ACK message may be processed by a subscriber identification policy which has the capability to parse the message into an alternative ASCII or octet string value.

When multiple hosts on the same port are associated with the same subscriber identification string they are considered to be host members of the same subscriber.

A sub-ident-policy can also used for identifying dynamic transit subscriber names.

The **no** form of the command removes the default subscriber identifcationidentification policy from the SAP configuration.

Default no sub-ident-policy

transit-auto-create

Syntax **transit-auto-create**

Context config>app-assure>group>transit-ip

Description This command enables seen-IP auto creation of transit subscribers using the transit-IP-policy name nd subscriber IP address as the AA-sub name. The default app-profile configured against the transit-ip-policy is applied to these subscribers.

Default disabled

transit-prefix-ipv4-entries

Syntax **transit-prefix-ipv4-entries** *entries*
no transit-prefix-ipv4-entries

Context config>isa>aa-grp

Description This command defines the number of transit-prefix IPv4 entries for an ISA.

The **no** form of the command removes the assignment of entries space from the configuration. All entries must be removed in order to delete the configuration.

Parameters *entries* — Specifies an integer that determines the number of transit-prefix-ipv4 entries.

Values 0 — 16383

transit-prefix-ipv4-remote-entries

Syntax **transit-prefix-ipv4-remote-entries** *entries*
no transit-prefix-ipv4-remote-entries

Context config>isa>aa-grp

Description This command configures the ISA-AA-group transit prefix IPv4 remote entry limit. This entry space is allocated on the IOM within a common area with the second MDA/ISA position of the IOM and also used for IPv4filter entries for system SDPs. The per-ISA size allocated for transit-prefix-ipv4 entries should be set to allow sufficient space on the IOM for SDP IPv4 filters.

The **no** form of the command removes the assignment of entries space from the configuration. All entries must be removed in order to delete the configuration.

Parameters *entries* — Specifies the ISA-AA-Group transit prefix IPv4 remote entry limit.

Values 0 — 2047

transit-prefix-ipv6-entries

Syntax **transit-prefix-ipv6-entries** *entries*
no transit-prefix-ipv6-entries

Context config>isa>aa-grp

Description This command configures the ISA-AA-group transit prefix IPv6 entry limit for each ISA in the group. This entry space is allocated on the IOM within a common area with the second MDA / ISA position of the IOM and also used for ipv6-filter entries for system SDPs. The per-ISA size allocated for transit-prefix-ipv6 entries should be set to allow sufficient space on the IOM for SDP ipv6-filters.

The **no** form of the command removes the assignment of entries space from the configuration. All entries must be removed in order to delete the configuration.

Parameters *entries* — Specifies the ISA-AA-Group transit prefix IPv6 entry limit.

Values 0 — 8191

transit-prefix-ipv6-remote-entries

Syntax **transit-prefix-ipv6-remote-entries** *entries*
no transit-prefix-ipv6-remote-entries

Context config>isa>aa-grp

Description This command configures the ISA-AA-group transit prefix IPv6 remote entry limit. This entry space is allocated on the IOM within a common area with the second MDA/ISA position of the IOM and also used for IPv6filter entries for system SDPs. The per-ISA size allocated for transit-prefix-ipv6 entries should be set to allow sufficient space on the IOM for SDP IPv6 filters.

The **no** form of the command removes the assignment of entries space from the configuration. All entries must be removed in order to delete the configuration.

Parameters *entries* — Specifies the ISA-AA-Group transit prefix IPv6 remote entry limit.

Values 0 — 1023

transit-prefix-policy

Syntax **transit-prefix-policy** *prefix-policy-id* [**create**]
no transit-prefix-policy *prefix-policy-id*

Context config>service>ies>if>sap
config>service>ies>if>spoke-sdp
config>service>vprn>if>sap
config>service>vprn>if>spoke-sdp
config>service>epipe>sap

config>service>epipe>spoke-sdp
config>service>ipipe>sap
config>service>ipipe>spoke-sdp
config>service>vpls>sap
config>service>vpls>spoke-sdp

Description This command associates a transit aa subscriber prefix policy to the service. The transit prefix policy must be defined prior to associating the policy with a SAP in the config>application assurance>group>policy>transit-prefix-policy context.

The **no** form of the command removes the association of the policy to the service.

Parameters *prefix-policy-id* — Specifies an integer that identifies a transit ip profile entry.

Values 1 — 65535

create — Mandatory keyword used when creating transit prefix policy. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

transit-prefix-policy

Syntax **transit-prefix-policy** *prefix-policy-id* [**create**]
no transit-prefix-policy *prefix-policy-id*

Context config>app-assure>group

Description This command defines a transit aa subscriber prefix policy. Transit AA subscribers are managed by the system through the use of this policy assigned to services, which determines how transit subs are created and removed for that service.

The **no** form of the command deletes the policy from the configuration. All associations must be removed in order to delete a policy.

Parameters *prefix-policy-id* — Indicates the transit prefix policy to which this subscriber belongs.

Values 1 — 65535

create — Mandatory keyword used when creating transit prefix policy. The create keyword requirement can be enabled/disabled in the environment>create context.

entry

Syntax **entry** *entry-id* [**create**]
entry *entry-id*
no entry *entry-id*

Context config>app-assure>group>transit-prefix-policy

Description This command configures the index to a specific entry of a transit prefix policy.

The **no** form of the command removes the entry ID from the transit prefix policy configuration.

Default none

Parameters *entry-id* — Specifies a transit prefix policy entry.

Values 1 — 4294967295

aa-sub

Syntax **aa-sub** *transit-aasub-name*
no aa-sub

Context **config>app-assure>group>transit-prefix-policy>entry**

Description This command configures a transit prefix policy entry subscriber.

The **no** form of the command removes the transit subscriber name from the transit prefix policy configuration.

Default none

Parameters *transit-aasub-name* — specifies the name of the transit prefix AA subscriber up to 32 characters in length.

match

Syntax **match**

Context config>app-assure>group>transit-prefix-policy>entry

Description This command enables the context to configure transit prefix policy entry match criteria.

aa-sub-ip

Syntax **aa-sub-ip** *ip-address*[/*mask*]
no aa-sub-ip

Context config>app-assure>group>transit-prefix-policy>entry>match

Description This command configures a transit prefix subscriber ip address prefix. It is used when the site is on the local side, being the same side of the system as the parent SAP. The local aa-sub-ip addresses represent the src-IP in the from-SAP direction and dest-IP in the to-SAP direction.

The **no** form of the command deletes the aa-sub-ip address assigned from the entry configuration.

Default no aa-sub-ip

Parameters *ip-address[/mask]* — Specifies the address type of the subscriber address prefix associated with this transit prefix policy entry.

Values <ip-address[/mask]>: ipv4-address - a.b.c.d[/mask]
mask - [1..32]

ipv6-address - x:x:x:x:x:x:x:x/prefix-length
x:x:x:x:x:x:d.d.d.d
x - [0..FFFF]H
d - [0..255]D
prefix-length [1..128]

network-ip

Syntax **network-ip** *ip-address*[/*mask*]
no network-ip

Context config>app-assure>group>transit-prefix-policy>entry>match

Description This command configures an entry for an address of prefix transit aa-sub and is used when the site is a remote site on the same opposite side of the system as the parent SAP. The network IP addresses represents the dest-IP in the from-SAP direction and src-IP in the to-SAP direction.

The **no** form of the command removes the network IP address/mask from the match criteria.

Parameters *ip-address[/mask]* — specifies the network address prefix and length associated with this transit prefix policy entry.

Values <ip-address[/mask]>: ipv4-address - a.b.c.d[/mask]
mask - [1..32]
ipv6-address - x:x:x:x:x:x:x:x/prefix-length
x:x:x:x:x:x:d.d.d.d
x - [0..FFFF]H
d - [0..255]D
prefix-length [1..128]

static-aa-sub

Syntax **static-aa-sub** *transit-aasub-name*
static-aa-sub *transit-aasub-name* **app-profile** *app-profile-name* [**create**]
no static-aa-sub *transit-aasub-name*

Context config>app-assure>group>transit-prefix-policy
config>app-assure>group>transit-ip-policy>static

Description This command configures a static transit aa-sub with a name and an app-profile. A new transit sub with both a name and an app-profile is configured with the create command. Static transit aa-sub must have an explicitly assigned app-profile. An existing transit sub can optionally be assigned a different app-profile, or this command can be used to enter the static-aa-sub context.

The **no** form of the command deletes the named static transit aa-sub from the configuration.

Parameters *transit-aasub-name* — Specifies a transit aasub-name up to 32 characters in length.

app-profile-name — Specifies the name of an existing application profile up to 32 characters in length.

create — Keyword used to create a new app-profile entry

static-remote-aa-sub

Syntax **static-remote-aa-sub** *transit-aasub-name*
static-remote-aa-sub *transit-aasub-name* **app-profile** *app-profile-name* [**create**]
no static-remote-aa-sub *transit-aasub-name*

Context config>app-assure>group>transit-prefix-policy

Description This command configures static remote transit aa-subs with a name and an app-profile. Remote transit subscribers are configured for sites on the opposite side of the system as the parent SAP/spoke-SDP. A new remote transit sub with both a name and an app-profile is configured with the create command. Static remote transit aa-subs must have an explicitly assigned app-profile. An existing remote transit sub can optionally be assigned a different app-profile.

The **no** form of the command removes the name from the transit prefix policy.

Parameters *transit-aasub-name* — Specifies a transit aasub-name up to 32 characters in length.

app-profile-name — Specifies the name of an existing application profile up to 32 characters in length.

create **—** Keyword used to create a new app-profile entry.

aa-sap-interface

Syntax **sap** *card/mda/aa-svc:vlan* [**create**]
no sap

Context config>service>vprn>aa-if
config>service>ies>aa-if

Description This commands specifies which ISA card and which VLAN is used by a given AA Interface.

Default no sap

Parameters *card/mda/aa-svc:vlan* — specifies AA ISA card slot/port and VLAN information.

create — Specifies keyword used to created the AARP instance.

group

Syntax **group** *aa-group-id*

Context admin>app-assure>

Description This commands performs a group-specific upgrade.

url-list

Syntax **url-list** *url-list-name* [**create**]

no url-list

Context admin>app-assure>group

Description This command configures a url-list object. The url-list points to a file containing a list of URLs located on the system Compact Flash. The url-list is then referenced in a url-filter object in order to filter and redirect subscribers when a URL from this file is accessed.

The **no** form of the command removes the url-list object.

Parameters *url-list-name* — Specify the Application-Assurance url-list

decrypt-key

Syntax **decrypt-key** *key***|***hash-key***|***hash2-key* [**hash | hash2**]
no decrypt-key

Context config>app-assure>group>url-list

Description In case the file is encrypted this command is used to configure the decryption key used to read the file.

The **no** form of the command removes the url-list object.

Parameters *key|hash-key|hash2-key* — Specify the Application-Assurance url-list decryption key

Hash|hash2 — Specify the hashing scheme used in the hashed key

file

Syntax **file** *file-url*
no file

Context config>app-assure>group>url-list

Description This command specifies the file for the URL list.

The **no** form of the command removes the url-list object.

Parameters *file-url* — Specifies the flash ID or file path.

Values [*cflash-id/*]*file-path* : [200 chars max]
cflash-id : - cf1:|cf1-A:|cf1-B:|cf2:|cf2-A:|cf2-B:|cf3:|cf3-A:|cf3-B:

url-filter

Syntax **url-filter** *url-filter-name* [**create**]
no url-filter

Context config>app-assure>group

Description This command configures a URL filter action for flows of a specific type matching this entry.

If no URL filters are specified then no URL filters will be evaluated.

Parameters *url-filter-name* — Specifies the Application-Assurance URL filter that will be evaluated.

aa-interface

Syntax **aa-interface** *aa-int-name* [**create**]
no aa-interface

Context config>service>ies/vprn

Description This commands creates a new AA interface within an IES or VPRN service. It is used by the aa-isa to send/receive IPv4 traffic. In the context of ICAP url-filtering this interface is used by the ISA to establish ICAP TCP connections to the ICAP server(s).

This interface supports /31 subnet only, and uses by default .1q encapsulation.

The system will automatically configure the ISA IP address based on the address configured by the operator under the aa-interface object (which represents the ISA sap facing interface on the ISA).

Default no aa-interface

Parameters *aa-int-name* — specifies the name of the AA Interface.

create — Specifies keyword used to created the AARP instance.

default-action

Syntax **default-action allow**
default-action block-all
default-action block-http-redirect *http-redirect-name*
no default-action

Context config>app-assure>group>policy>aqp>entry>action>url-filter

Description This command configures the default action to take when the ICAP server is unreachable.

Parameters **allow —** Allows all requests.

block-all — Blocks all requests.

block-http-redirect *http-redirect-name* **—** Blocks and redirects requests.

http-request-filtering

Syntax **http-request-filtering** {**all** | **first**}

Context config>app-assure>group>url-filter

Description HTTP Filtering can either be enabled for all HTTP request within a flow or limited to the first HTTP request in a flow.

Default all

Parameters **all** — Specifies all HTTP Request within a flow.

first — Specifies the first HTTP Request within a flow.

http-redirect

Syntax **http-redirect** *http-redirect-name*
no http-redirect

Context config>app-assure>group>url-filter

Description This command specifies the HTTP redirect that will be applied when the Internet Content Adaptation Protocol (ICAP) server blocks an HTTP request.

Default none

Parameters *http-redirect-name* — Specifies the ICAP HTTP redirect name up to 32 characters in length.

server

Syntax **server** *ip-address*[:*port*] [**create**]
no server *ip-address*[:*port*]

Context config>app-assure>group>url-filter>icap

Description This command configures the IP address and server port of the ICAP server.

Default none

Parameters *ip-address*[:*port*] — Specifies the ICAP server IP address and port.

vlan-id

Syntax **vlan-id** *service-port-vlan-id*
no vlan-id

Context config>app-assure>group>url-filter

Description This command configures the VLAN ID on which the ISA-AA is expected to be emitting traffic mapping to a pre-configured aa-interface.

custom-x-header

Syntax **custom-x-header** *x-header-name*
no custom-x-header

Context config>app-assure>group>url-filter>icap

Description This command configures the url-filter ICAP policy to include a new x-header field; the content of the x-header is populated based on AQP url-filter action which can optionally specify the ASO characteristic value to include in the x-header.

Parameters *x-header-name* — The name of the x-header added to the ICAP request.

local-filtering

Syntax **local-filtering**

Context config>app-assure>group>url-filter

Description This command configures a URL filter policy for local filtering in order to filter traffic based on a list of URLs located on a file stored in the router compact flash.

url-list

Syntax [**no**] **url-list** *url-list-name*

Context admin>app-assure>group>url-filter>local-filtering

Description This command adds a URL list to the local filtering URL filter policy.

The **no** form of the command removes the URL list object.

Parameters *url-list-name* — Specify the URL list.

wap1x

Syntax **wap1x**

Context config>app-assure>group

Description This command configures the Wireless Application Protocol (WAP) 1.X.

packet-rate-high-wmark

Syntax **packet-rate-high-wmark** *high-watermark*

Context config>app-assure

Description This command configures the packet rate on the ISA-AA when a packet rate alarm will be raised by the agent.

Default max = disabled

Parameters *high-watermark* — Specifies the high watermark for packet rate alarms. The value must be larger than or equal to the packet-rate-low-wmark value.

Values 1 — 14880952 , **max** packets/sec

Syntax **packet-rate-low-wmark** *low-watermark*
no packet-rate-low-wmark

Context config>app-assure

Description This command configures the the packet rate on the ISA-AA when a packet rate alarm will be cleared by the agent.

The **no** form of the command reverts to the default.

Default 0

Parameters *low-watermark* — Specifies the low watermark for packet rate alarms. T he value must be lower than or equal to the packet-rate-low-wmark value.

Values 0— 14880952 packets/sec

wa-shared-high-wmark

Syntax **wa-shared-high-wmark** *percent*
no wa-shared-high-wmark

Context config>isa>aa-grp>qos>egress>from-sub
config>isa>aa-grp>qos>egress>to-sub

Description This command configures the high watermark for the weighted average utilization of the shared buffer space in the **from-subscriber** buffer pool for each ISA. When a buffer pool is not in the overload state and the wa-shared buffer utilization for an ISA crosses above the high watermark value in the ISA **from-subcriber** buffer pool enters an overload state and an overload notification is raised.

Default 100

Parameters *percent* — Specifies the weighted average shared buffer utilization high watermark

Values 0 — 100

wa-shared-low-wmark

Syntax **wa-shared-low-wmark** *percent*
no wa-shared-low-wmark

Context config>isa>aa-grp>qos>egress>from-sub
config>isa>aa-grp>qos>egress>to-sub

Description This command configures the low watermark for the weighted average utilization of the shared buffer space in the **from-subscriber** buffer pool. When a buffer pool is in an overloaded state and the wa-shared buffer utilization for an ISA drops below low watermark value ISA **from-subcriber** buffer pool leaves the overload state and a is sent to indicate the overload state has cleared.

Default 0

Parameters *percent* — Specifies the weighted average shared buffer utilization low watermark

Values 0 — 100

protocol

Syntax **protocol** *protocol-name*

Context config>app-assure

Description This command configures the shutdown of protocols system-wide

Parameters *protocol-name* — Specifies a shutable (disable) protocol name.

shutdown

Syntax [**no**] **shutdown**

Context config>app-assure>protocol

Description This command administratively disables the protocol specified in **protocol** *protocol-name*.

The **no** form of the command enables the protocol.

radius-accounting-policy

Syntax **radius-accounting-policy** *rad-acct-plcy-name* [**create**]
no radius-accounting-policy *rad-acct-plcy-name*

Context config>app-assure
config>aa>group>statistics>aa-sub

Description This command specifies an existing subscriber RADIUS-based accounting policy to use for AA. RADIUS accounting policies are configured in the **config>application-assurance>radius-accounting**-policy context.

Default none

Parameters *name* — Specifies the policy name. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

interim-update-interval

Syntax **interim-update-interval** *minutes*
no interim-update-interval

Context config>app-assure>rad-acct-plcy

Description This command configures the interim update interval.

The **no** form of the command reverts to the default.

Default no interim-update-interval

Parameters *minutes* — Specifies the interval at which subscriber accounting data will be updated. If set no value is specified then no interim updates will be sent.

Values 5 — 1080

radius-accounting-server

Syntax **radius-accounting-server**

Context config>app-assure>rad-acct-plcy

Description This command creates the context for defining RADIUS accounting server attributes under a given session authentication policy.

access-algorithm

Syntax **access-algorithm** {**direct** | **round-robin**}
no access-algorithm

Context config>app-assure>rad-acct-plcy>server

Description This command configures the algorithm used to access the list of configured RADIUS servers.

Default direct

Parameters **direct** — Specifies that the first server will be used as primary server for all requests, the second as secondary and so on.

round-robin — Specifies that the first server will be used as primary server for the first request, the second server as primary for the second request, and so on. If the router gets to the end of the list, it starts again with the first server.

retry

Syntax **retry** *count*

Context config>app-assure>rad-acct-plcy>server

Description This command configures the number of times the router attempts to contact the RADIUS server for authentication, if not successful the first time.

The **no** form of the command reverts to the default value.

Default 3

Parameters *count* — Specifies the retry count.

Values 1 — 10

router

Syntax **router** *router-instance*
router service-name *service-name*
no router

Context config>app-assure>rad-acct-plcy>server

Description This command specifies the number of times the router attempts to contact the RADIUS server for authentication, if not successful the first time.

The **no** form of the command reverts to the default value.

server

Syntax **server** *server-index* **address** *ip-address* **secret** *key* [**hash | hash2**] [**port** *port*] [**create**]
no server *server-index*

Context config>app-assure>rad-acct-plcy>server

Description This command adds a RADIUS server and configures the RADIUS server IP address, index, and key values.

Up to five RADIUS servers can be configured at any one time. RADIUS servers are accessed in order from lowest to highest index for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other RADIUS servers are queried.

The **no** form of the command removes the server from the configuration.

Default none

Parameters *server-index* — The index for the RADIUS server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.

Values 1 — 16 (a maximum of 5 accounting servers)

address ip-address — The IP address of the RADIUS server. Two RADIUS servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

secret *key* **— Values**The secret key to access the RADIUS server. This secret key must match the password on the RADIUS server.
secret-key — A string up to 20 characters in length.
hash-key — A string up to 33 characters in length.
hash2-key — A string up to 55 characters in length.

hash — Specifies the key is entered in an encrypted form. If the hash parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the hash2 parameter is not used, the less encrypted hash form is assumed.

port — Specifies the UDP port number on which to contact the RADIUS server for authentication.

Values 1 — 65535

source-address

Syntax **source-address** *ip-address*
no source-address

Context config>app-assure>rad-acct-plcy>server

Description This command configures the source address of the RADIUS packet. The system IP address must be configured in order for the RADIUS client to work. See Configuring a System Interface in the 7750 SR OS Router Configuration Guide. Note that the system IP address must only be configured if the source-address is not specified. When the no source-address command is executed, the source address is determined at the moment the request is sent. This address is also used in the nas-ip-address attribute: over there it is set to the system IP address if no sourceaddress was given.

The **no** form of the command reverts to the default value.

Default systemIP address

Parameters *ip-address* — The IP prefix for the IP match criterion in dotted decimal notation.

Values 0.0.0.0 - 255.255.255.255

timeout

Syntax **timeout** *seconds*

Context config>app-assure>rad-acct-plcy>server

Description This command configures the number of seconds the router waits for a response from a RADIUS server.

The **no** form of the command reverts to the default value.

Default 5

Parameters *seconds* — Specifies the time the router waits for a response from a RADIUS server.

Values 1 — 90

vlan-id

Syntax **vlan-id** *service-port-vlan-id*
no vlan-id

Context config>app-assure>rad-acct-plcy>server

Description

significant-change

Syntax **significant-change delta**
no significant-change

Context config>app-assure>rad-acct-plcy

Description This command configures the significant change required to generate the record.

The **no** form of the command reverts to the default.

Default no significant-change

Parameters **delta —** Specifies the delta change (significant change) that is required for the charging-group counts to be included in the RADIUS Accounting VSA(s) .

Values 0 — 4294967295

System Persistence Commands

persistence

Syntax **persistence**

Context config>system

Description This command enables the context to configure persistence parameters on the system.

The persistence feature enables state on information learned through DHCP snooping across reboots to be retained. This information includes data such as the IP address and MAC binding information, lease-length information, and ingress SAP information (required for VPLS snooping to identify the ingress interface).

If persistence is enabled when there are no DHCP relay or snooping commands enabled, it will simply create an empty file.

Default no persistence

application-assurance

Syntax **application-assurance**

Context config>system>persistence

Description This command enables the context to configure application assurance persistence parameters.

location

Syntax **location** *cflash-id*
no location

Context config>system>persistence>subscriber-mgmt

Description This command instructs the system where to write the file. The name of the file is: appassure.db. On boot the system scans the file systems looking for appassure.db, if it finds it, it starts to load it.

In the subscriber management context, the location specifies the flash device on a CPM card where the data for handling subscriber management persistency is stored.

The **no** form of this command returns the system to the default. If there is a change in file location while persistence is running, a new file will be written on the new flash, and then the old file will be removed.

Default no location

ISA Commands

Application Assurance Group Commands

application-assurance-group

Syntax **application-assurance-group** *application-assurance-group-index* [**create**] [**aa-sub-scale** *sub-scale*]
no application-assurance-group *application-assurance-group-index*

Context config>isa

Description This command enables the context to create an application assurance group with the specified system-unique index and enables the context to configure that group's parameters.

The **no** form of the command deletes the specified application assurance group from the system. The group must be shutdown first.

Default none

Parameters *application-assurance-group-index* — Specifies an integer to identify the AA group

Values 1

create — Mandatory keyword used when creating an application assurance group in the ISA context. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

aa-sub-scale *sub-scale* **—** Specifies the set of scaling limits that are supported with regards to the maximum number of AA subscribers per ISA and the corresponding policies that can be specified.

Values		
	residential:	Scaling limits for residential operation.
	vpn:	Scaling limits for VPNs.
	mobile-gateway:	Scaling limits for operation as a mobile gateway.

Default residential

backup

Syntax [**no**] **backup** *mda-id*

Context config>isa>aa-grp

Description This command assigns an AA ISA configured in the specified slot to this application assurance group. The backup module provides the application assurance group with warm redundancy when the primary module in the group is configured. Primary and backup modules have equal operational status and when both module are coming up, the ones that becomes operational first becomes the active module. A module can serve as a backup for multiple AA ISA cards but only one can fail to it at one time.

On an activity switch from the primary module, configurations are already on the backup MDA but flow state information must be re-learned. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is not supported.

Operator is notified through SNMP events when:

- When the AA service goes down (all modules in the group are down) or comes back up (a module in the group becomes active).
- When AA redundancy fails (one of the modules in the group is down) or recovers (the failed module comes back up).
- When an AA activity switch occurred.

The **no** form of the command removes the specified module from the application assurance group.

Default no backup

Parameters *mda-id* — Specifies the card/slot identifying a provisioned module to be used as a backup module.

Values	mda-id:	*slot*/*mda*	
		slot	1 — up to 10 depending on chassis model
		mda	1 — 2

divert-fc

Syntax [**no**] **divert-fc** *fc-name*

Context config>isa>aa-grp

Description This command selects a forwarding class in the system to be diverted to an application assurance engine for this application assurance group. Only traffic to/from subscribers with application assurance enabled is diverted.

To divert multiple forwarding classes, the command needs to be executed multiple times specifying each forwarding class to be diverted at a time.

The **no** form of the command stops diverting of the traffic to an application assurance engine for this application assurance group.

Default no divert-fc

Parameters *fc-name* — Creates a class instance of the forwarding class fc-name.

Values be, l2, af, l1, h2, ef, h1, nc

fail-to-open

Syntax [**no**] **fail-to-open**

Context config>isa>aa-grp

Description This command configures mode of operation during an operational failure of this application assurance group when no application assurance engines are available to service traffic. When enabled, all traffic that was to be inspected will be dropped. When disabled, all traffic that was to be inspected will be forwarded without any inspection as if the group was not configured at all.

Default no fail-to-open

isa-capacity-cost-high-threshold

Syntax **isa-capacity-cost-high-threshold** *threshold*
no isa-capacity-cost-high-threshold

Context config>isa>aa-grp

Description This command configures the ISA-AA capacity cost high threshold.

The **no** form of the command reverts the threshold to the default value.

Default 4294967295

Parameters *threshold* — Specifies the capacity cost high threshold for the ISA-AA group.

Values 0 — 4294967295

isa-capacity-cost-low-threshold

Syntax **isa-capacity-cost-low-threshold** *threshold*
no isa-capacity-cost-low-threshold

Context config>isa>aa-grp

Description This command configures the ISA-AA capacity cost low threshold.

The **no** form of the command reverts the threshold to the default value.

Default 0

Parameters *threshold* — Specifies the capacity cost low threshold for the ISA-AA group.

Values 0 — 4294967295

isa-overload-cut-through

Syntax [**no**] **isa-overload-cut-through**

Context config>isa>aa-grp

Description This command configures the ISA group to enable cut-through of traffic if an overload event occurs, triggered when the IOM weighted average queues depth exceeds the wa-shared-high-wmark. In this ISA state, packets are cut-through from application analysis but retain subscriber context with default subscriber policy applied.

The **no** form of the command disables cut-through processing on overload.

Default isa-overload-cut-through

minimum-isa-generation

Syntax **minimum-isa-generation** *min-isa-generation*

Context config>isa>aa-grp

Description This command configures the scale parameters for the ISA group. When min-isa-gen is configured as 1, the group and per-ISA limits are the MS-ISA scale.

If there is a mix of ISA 1s and 2s, the min-isa-gen must be left as 1.

When min-isa-gen is configured as 2, the per-isa resource limits shown in the **show isa application-assurance-group 1 load-balance** output will increase to show ISA2 limits.

Default 1

Parameters *min-isa-generation* — Specifies the minimum ISA Generation allowed in this group.

Values 1 –ISA (ISA1)
2 – ISA2

partitions

Syntax [**no**] **partitions**

Context config>isa>aa-grp

Description This command enables partitions within an ISA-AA group. When enabled, partitions can be created

The **no** form of the command disables partitions within an ISA-AA group.

Default disabled

primary

Syntax [**no**] **primary** *mda-id*

Context config>isa>aa-grp

Description This command assigns an AA ISA module configured in the specified slot to this application assurance group. Primary and backup ISAs have equal operational status and when both ISAs are coming up, the one that becomes operational first becomes the active ISA.

On an activity switch from the primary ISA, all configurations are already on the backup ISA but flow state information must be re-learned. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is not supported.

Operator is notified through SNMP events when:

- When AA service goes down (all ISAs in the group are down) or comes back up (an ISA in the group becomes active)
- When AA redundancy fails (one of the ISAs in the group is down) or recovers (the failed MDA comes back up)
- When an AA activity switch occurred.

The **no** form of the command removes the specified ISA from the application assurance group.

Default no primary

Parameters *mda-id* — Specifies the slot/mda identifying a provisioned AA ISA.

Values	mda-id:	*slot*/*mda*	
		slot	1 — up to 10 depending on chassis model
		mda	1 — 2

qos

Syntax **qos**

Context config>isa>aa-grp

Description This command enables the context for Quality of Service configuration for this application assurance group.

statistics

Syntax **statistics**

Context config>isa>aa-grp

Description This command enables the context to configure statistics generation.

performance

Syntax **performance**

Context config>isa>aa-grp>statistics

Description This command configures the ISA group to enable the aa-performance statistic record. This record contains information on the traffic load and resource consumption for each ISA in the group, to allow tracking of ISA load for long term capacity planning and short term anomalies. The user can configure the accounting policy to be used, and enables the record using the [no]collect-stats command

egress

Syntax **egress**

Context config>isa>aa-grp>qos

Description This command enables the context for IOM port-level Quality of Service configuration for this application assurance group in the egress direction (traffic entering an application assurance engine).

from-subscriber

Syntax **from-subscriber**

Context config>isa>aa-grp>qos>egress

Description This command enables the context for Quality of Service configuration for this application assurance group form-subscriber logical port, traffic entering the system from AA subscribers and entering an application assurance engine.

pool

Syntax **pool** [*pool-name*]
no pool

Context config>isa>aa-grp>qos>egress>from-subscriber
config>isa>aa-grp>qos>egress>to-subscriber
config>isa>aa-grp>qos>ingress

Description This command enables the context to configure an IOM pool as applicable to the specific application assurance group traffic. The user can configure resv-cbs (as percentage) values and slope-policy similarly to other IOM pool commands.

Default default

Parameters *pool-name* — The name of the pool.

Values default

resv-cbs

Syntax **resv-cbs** *percent-or-default*
no resv-cbs

Context config>isa>aa-grp>qos>egress>from-subscriber>pool
config>isa>aa-grp>qos>egress>to-subscriber>pool
config>isa>aa-grp>qos>ingress>pool

Description This command defines the percentage or specifies the sum of the pool buffers that are used as a guideline for CBS calculations for access and network ingress and egress queues. Two actions are accomplished by this command.

- A reference point is established to compare the currently assigned (provisioned) total CBS with the amount the buffer pool considers to be reserved. Based on the percentage of the pool reserved that has been provisioned, the over provisioning factor can be calculated.
- The size of the shared portion of the buffer pool is indirectly established. The shared size is important to the calculation of the instantaneous-shared-buffer-utilization and the average-shared-buffer-utilization variables used in Random Early Detection (RED) per packet slope plotting.

Note that this command does not actually set aside buffers within the buffer pool for CBS reservation. The CBS value per queue only determines the point at which enqueuing packets are subject to a RED slope. Oversubscription of CBS could result in a queue operating within its CBS size and still not able to enqueue a packet due to unavailable buffers. The resv-cbs parameter can be changed at any time.

If the total pool size is 10 MB and the resv-cbs set to 5, the ‘reserved size’ is 500 KB.

The **no** form of this command restores the default value.

Default default (30%)

Parameters *percent-or-default* — Specifies the pool buffer size percentage.

Values 0 — 100, default

slope-policy

Syntax **slope-policy** *name*
no slope-policy

Context config>isa>aa-grp>qos>egress>from-subscriber>pool
config>isa>aa-grp>qos>egress>to-subscriber>pool
config>isa>aa-grp>qos>ingress>pool

Description This command specifies an existing slope policy which defines high and low priority RED slope parameters and the time average factor. The slope policy is defined in the **config>qos>slope-policy** context.

queue-policy

Syntax **queue-policy** *network-queue-policy-name*
no queue-policy

Context config>isa>aa-grp>qos>egress>from-subscriber
config>isa>aa-grp>qos>egress>to-subscriber
config>isa>aa-grp>qos>ingress

Description This command assigns an IOM network queue policy as applicable to specific application assurance group traffic.

Default default

Parameters *network-queue-policy-name* — The name of the network queue policy defined in the system.

wa-shared-high-wmark

Syntax **wa-shared-high-wmark** *percent*
no wa-shared-high-wmark

Context config>isa>aa-grp>qos>egress>from-sub
config>isa>aa-grp>qos>egress>to-sub

Description This command configures the high watermark for the weighted average utilization of the shared buffer space in the **from-subscriber** buffer pool for each ISA. When a buffer pool is not in the overload state and the wa-shared buffer utilization for an ISA crosses above the high watermark value in the ISA **from-subcriber** buffer pool enters an overload state and an overload notification is raised.

Default 100

Parameters *percent* — Specifies the weighted average shared buffer utilization high watermark

Values 0 — 100

wa-shared-low-wmark

Syntax **wa-shared-low-wmark** *percent*
no wa-shared-low-wmark

Context config>isa>aa-grp>qos>egress>from-sub
config>isa>aa-grp>qos>egress>to-sub

Description This command configures the low watermark for the weighted average utilization of the shared buffer space in the **from-subscriber** buffer pool. When a buffer pool is in an overloaded state and the wa-shared buffer utilization for an ISA drops below low watermark value ISA **from-subcriber** buffer pool leaves the overload state and a is sent to indicate the overload state has cleared.

Default

Default 0

Parameters *percent* — Specifies the weighted average shared buffer utilization low watermark

Values 0 — 100

port-scheduler-policy

Syntax **port-scheduler-policy** *port-scheduler-policy-name*
no port-scheduler-policy

Context config>isa>aa-grp>qos>egress>from-subscriber
config>isa>aa-grp>qos>egress>to-subscriber

Description This command assigns an existing port scheduler policy as applicable to the specific application assurance group traffic.

Default default

Parameters *port-scheduler-policy-name* — specifies the name of an existing port scheduler policy.

to-subscriber

Syntax **to-subscriber**

Context config>isa>aa-grp>qos>egress

Description This command enables the context for Quality of Service configuration for this application assurance group to-subscriber logical port, traffic destined to AA subscribers and entering an application assurance engine.

ingress

Syntax **ingress**

Context config>card>mda>network>ingress

Description This command enables the context for MDA-level IOM Quality of Service configuration.