Security Command Reference

Command Hierarchies

Configuration Commands

Security Commands

```
config
     — system
          — security
               — copy {user source-user | profile source-profile} to destination [overwrite]
               — [no] ftp-server
               — hash-control [read-version {1 | 2 | all}] [write-version {1 | 2}]
               — no hash-control
               — [no] per-peer-queuing
               — source-address
                    — application app [ip-int-name | ip-address]
                    — no application app
                    — application6 app ipv6-address
                    — no application6
               — [no] telnet-server
               — [no] telnet6-server
               — vprn-network-exceptions number seconds
```

LLDP Commands

```
configure
     — system
          — lldp
               — message-fast-tx time
               — no message-fast-tx
               — message-fast-tx-init count
               — no message-fast-tx-init
               — notification-interval time
               — no notification-interval
               — reinit-delay time
               — no reinit-delay
               — tx-credit-max count
               — no tx-credit-max
               — tx-hold-multiplier multiplier
               — no tx-hold-multiplier
               — tx-interval interval
               — no tx-interval
```

Management Access Filter Commands

```
config
     — system
          — security
               — [no] management-access-filter
                    — [no] ip-filter
                         — default-action {permit | deny}
                         — [no] entry entry-id
                              — action {permit | deny | deny-host-unreachable}
                              — no action
                              — description description-string
                              — no description
                              — dst-port value [mask]
                              — no dst-port
                              — [no] log
                              — protocol  protocol-id
                              — no protocol
                              — router {router-instance}
                              — no router
                              — src-ip {ip-prefix/mask | ip-prefix netmask}
                              — no src-ip
                              — src-port {port-id | cpm | lag lag-id }
                              — no src-port
                              — src-port old-entry-number new-entry-number
                         — renum old-entry-number new-entry-number
                         — [no] shutdown
                    — [no] ipv6-filter
                         — default-action {permit | deny | deny-host-unreachable}
                         — [no] entry entry-id
                              — action {permit | deny | deny-host-unreachable}
                              — no action
                              — description description-string
                              — no description
                              — dst-port value [mask]
                              — no dst-port
                              — flow-label value
                              — no flow-label
                              — [no] log
                              — next-header next-header
                              — no next-header
                              — router {router-instance}
                              — no router
                              — src-ip {ip-prefix/mask | ip-prefix netmask}
                              — no src-ip
                              — src-port {port-id | cpm | lag lag-id }
                              — no src-port
                         — renum old-entry-number new-entry-number
                         — [no] shutdown
                    — [no] mac-filter
                         — default-action {permit | deny}
                         — [no] entry entry-id
                              — action {permit | deny | deny-host-unreachable}
```

```
                        — no action
                        — description description-string
                        — no description
                        — [no] log
                        — match frame-type frame-type
                        — no match
                            — cfm-opcode {lt | gt | eq} opcode
                            — cfm-opcode range start end
                            — no cfm-opcode
                            — dot1p dot1p-value [dot1p-mask]
                            — dsap dsap-value [dsap-mask]
                            — dst-mac ieee-address [ieee-address-mask]
                            — no dst-mac
                            — etype 0x0600..0xfff
                            — no etype
                            — snap-oui {zero | non-zero}
                            — snap-pid snap-pid
                            — no snap-pid
                            — src-mac ieee-address [ieee-address-mask]
                            — no src-mac
                            — ssap ssap-value [ssap-mask]
                            — no ssap
                            — svc-id service-id
                            — no svc-id
                    — renum old-entry-number new-entry-number
                    — [no] shutdown
```

CPM Filter Commands

```
config
    — system
        — security
            — [no] cpm-filter
                — default-action {accept | drop}
                — [no] ip-filter
                    — [no] entry entry-id
                        — action [accept | drop | queue queue-id]}
                        — no action
                        — description description-string
                        — no description
                        — log log-id
                        — no log
                        — match [protocol protocol-id]
                        — no match
                            — dscp dscp-name
                            — no dscp
                            — dst-ip {ip-address/mask | ip-address netmask | ip-
                              prefix-list prefix-list-name}
                            — no dst-ip
                            — dst-port [tcp/udp port-number] [mask]
                            — no dst-port
                            — fragment {true | false}
                            — no fragment
                            — icmp-code icmp-code
                            — no icmp-code
                            — icmp-type icmp-type
                            — no icmp-type
                            — ip-option [ip-option-value] [ip-option-mask]
                            — no ip-option
                            — multiple-option {true | false}
                            — no multiple-option
                            — option-present {true | false}
                            — no option-present
                            — port port-number
                            — port -list port-list-name
                            — port-range start end
                            — no port
                            — router
                            — src-ip {ip-address/mask | ip-address netmask | ip-
                              prefix-list prefix-list-name}
                            — no src-ip
                            — src-port[src-port-number] [mask]
                            — no src-port
                            — tcp-ack {true | false}
                            — no tcp-ack
                            — tcp-syn {true | false}
                            — no tcp-syn
                        — renum old-entry-id new-entry-id
                        — [no] shutdown
                — [no] ipv6-filter
                    — [no] entry entry-id
                        — action [accept | drop | queue queue-id]}
                        — no action
                        — description description-string
                        — no description
                        — log log-id
                        — no log
                        — match [next-header next-header]
                        — no match
                            — dscp dscp-name
                            — no dscp
                            — dst-ip ipv6-address/prefix-length
                            — dst-ip ipv6-prefix-list ipv6-prefix-list-name
                            — no dst-ip
                            — dst-port [tcp/udp port-number] [mask]
                            — dst-port port-list port-list-name
                            — dst-port range tcp/udp port-number tcp/udp port-num-
                              ber
                            — no dst-port
                            — flow-label value
                            — no flow-label
                            — fragment {true | false}
                            — no fragment
                            — hop-by-hop-opt {true | false}
                            — no hop-by-hop-opt
                            — icmp-code icmp-code
                            — no icmp-code
                            — icmp-type icmp-type
                            — no icmp-type
                            — port tcp/udp port-number [mask]
                            — port port-list port-list-name
```

```
                        — port range start end
                        — no port
                        — router service-name service-name
                        — router router-instance
                        — no router
                        — src-ip [ipv6-address/prefix-length] [ipv6-prefix-list
                          ipv6-prefix-list-name]
                        — no src-ip
                        — src-port [src-port-number] [mask]
                        — no src-port
                        — tcp-ack {true | false}
                        — no tcp-ack
                        — tcp-syn {true | false}
                        — no tcp-syn
          — renum old-entry-id new-entry-id
          — [no] shutdown


— [no] mac-filter
          — [no] entry entry-id
                    — action [accept | drop | queue queue-id]}
                    — no action
                    — description description-string
                    — no description
                    — log log-id
                    — no log
                    — match [frame-type frame-type]
                    — no match
                        — cfm-opcode {lt | gt | eq} opcode
                        — cfm-opcode range start end
                        — no cfm-opcode
                        — dsap dsap-value [dsap-mask]
                        — dst-mac ieee-address [ieee-address-mask]
                        — no dst-mac
                        — etype 0x0600..0xffff
                        — no etype
                        — src-mac ieee-address [ieee-address-mask]
                        — no src-mac
                        — ssap ssap-value [ssap-mask]
                        — no ssap
                        — svc-id service-id
                        — no svc-id
          — renum old-entry-number new-entry-number
          — [no] shutdown
```

CPM Queue Commands

```
config
    — system
        — security
            — [no] cpm-queue
                — [no] queue queue-id
                    — cbs cbs
                    — no cbs
                    — mbs mbs
                    — no mbs
                    — rate rate [cir cir]
                    — no rate
```

CPU Protection Commands

```
config
    — system
        — security
            — cpu-protection
                — link-specific-rate packet-rate-limit
                — no link-specific-rate
                — policy cpu-protection-policy-id [create]
                — no policy cpu-protection-policy-id
                    — [no] alarm
                    — description description-string
                    — no description
                    — eth-cfm entry entry levels levels opcodes opcodes rate packet-rate-
                      limit
                    — no eth-cfm
                    — out-profile-rate packet-rate-limit
                    — no out-profile-rate
                    — overall-rate packet-rate-limit
                    — no overall-rate
                    — per-source-rate packet-rate-limit
                    — no per-source-rate
                — port-overall-rate packet-rate-limit
                — no port-overall-rate
                — [no] protocol-protection [allow-sham-links]
```

Refer to the OS Services Guide and the Multi-Service ISA Guide for command, syntax, and usage information about applying CPU Protection policies to interfaces.

CPU protection policies are applied by default (and customer policies can be applied) to a variety of entities including interfaces and SAPs. Refer to the appropriate guides (See Preface for document titles) for command syntax and usage for applying CPU protection policies. Examples of entities that can have CPU protection policies applied to them include:

configure>router>interface>cpu-protection *policy-id*

configure>service>epipe>sap>cpu-protection *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]]

configure>service>epipe>spoke-sdp>cpu-protection *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]]

configure>service>ies>interface>cpu-protection *policy-id*

configure>service>ies>interfac>sap>cpu-protection *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]]

configure>service>template>vpls-sap-template>cpu-protection *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]]

configure>service>vpls>sap>cpu-protection *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]]

configure>service>vpls>video-interface>cpu-protection *policy-id*

configure>service>vprn>interface>cpu-protection *policy-id*

configure>service>vprn >interface>sap>cpu-protection *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]]

configure>service>vprn>network-interface>cpu-protection *policy-id*

configure>service>vprn>subscriber-interface>group-interface>sap>cpu-protection *policy-id* [**mac-monitoring**]|[**eth-cfm-monitoring** [**aggregate**][**car**]]

configure>subscriber-mgmt>msap-policy>cpu-protection *policy-id* [**mac-monitoring**]

Distributed CPU Protection Commands

```
config
     — system
          — security
               — dist-cpu-protection
                    — policy policy-name [create]
                    — no policy
                         — description description-string
                         — no description
                         — [no] local-monitoring-policer policer-name [create]
                              — [no] description “description-string”
                              — rate {packets {ppi | max} within seconds [initial-delay
                                packets] | kbps {kilobits-per-second | max} [mbs size]
                                [bytes|kilobytes]}
                              — no rate
                              — exceed-action {discard | low-priority | none}
                              — [no] log-events [verbose]
                         — protocol name [create]
                         — no protocol name
                              — dynamic-parameters
                                   — detection-time seconds
                                   — exceed-action {discard [hold-down seconds] | low-
                                     priority [hold-down seconds] | none}
                                   — log-events [verbose]
                                   — no log-events
                                   — rate {packets {ppi | max} within seconds [initial-
                                     delay packets] | kbps {kilobits-per-second | max} [mbs
                                     size] [bytes|kilobytes]}
                              — enforcement {static policer-name | dynamic {mon-
                                policer-name | local-mon-bypass }}
                         — static-policer policer-name [create]
                         — no static-policer policer-name
                              — description description-string
                              — no description
                              — detection-time seconds
                              — no detection-time
                              — exceed-action {discard [hold-down seconds] | low-prior-
                                ity [hold-down seconds] | none}
                              — log-events [verbose]
                              — no log-events
                              — rate {packets {ppi | max} within seconds [initial-delay
                                packets] | kbps {kilobits-per-second | max} [mbs size]
                                [bytes|kilobytes]}
                              — no rate
```

```
config card x fp y
     — dist-cpu-protection
               — [no] dynamic-enforcement-policer-pool number-of-policers
```

Security Password Commands

```
config
     — system
               — ftp-server
                         — password
                                   — admin-password password [hash | hash2]
                                   — no admin-password
                                   — aging days
                                   — no aging
                                   — attempts count [time minutes1] [lockout minutes2]
                                   — no attempts
                                   — authentication-order [method-1] [method-2] [method-3] [exit-on-reject]
                                   — no authentication-order
                                   — [no] complexity [numeric] [special-character]  [mixed-case]
                                   — [no] health-check [interval interval]
                                   — minimum-length value
                                   — no minimum-length
                                   — [no] tacplus-map-to-priv-lvl [admin-priv-lvl]
```

Public Key Infrastructure (PKI) Commands

```
config
     — system
               — security
                         — pki
                                   — ca-profile name [create]
                                   — no ca-profile name
                                             — cert-file filename
                                             — no cert-file
                                             — cmp
                                                       — cmp-key-list
                                                           — key password [hash|hash2] reference reference-num-
                                                             ber
                                                           — no key reference reference-number
                                                       — cmp-url url-string [service-id service-id]
                                                       — no cmp-url
                                                       — http-response-timeout timeout
                                                       — no http-response-timeout
                                             — crl-file filename
                                             — no crl-file
                                             — description description-string
                                             — no description
                                             — ocsp
                                                       — responder-url url-string
                                                       — no responder-url
                                                       — service service-id
                                                       — no service
                                                       — verify-cert filename [allow-override]
                                                       — verify-cert ca-cert [allow-override]
```

```
                                    — no verify-cert
                               — [no] shutdown
                          — maximum-cert-chain-depth level
                          — no maximum-cert-chain-depth
admin
     — certificate
          — clear-ocsp-cache [entry-id]
          — display type {cert|key|crl|cert-request} url-string format {pkcs10|pkcs12|pkcs7-der|pkcs7-
            pem|pem|der} [password [32 chars max]]
          — export type {cert|key|crl} input filename output url-string format output-format [password [32
            chars max]] [pkey filename]
          — gen-keypair url-string [size {512|1024|2048}] [type {rsa|dsa}]
          — gen-local-cert-req keypair url-string subject-dn subject-dn [domain-name [255 chars max]] [ip-
            addr ip-address] file url-string
          — import type {cert|key|crl} input url-string output filename format input-format [password [32
            chars max]]
          — reload type {cert|key} filename
```

Profile Commands

```
config
     — system
          — security
               — [no] profile user-profile-name
                    — default-action {deny-all | permit-all | none}
                    — [no] entry entry-id
                         — action {deny | permit}
                         — description description-string
                         — no description
                         — security command-string
                         — no security
                    — renum old-entry-number new-entry-number
```

RADIUS Commands

```
config
     — system
          — security
               — [no] radius
                    — access-algorithm {direct | round-robin}
                    —  no access-algorithm
                    — [no] accounting
                    — accounting-port port
                    — no accounting-port
                    — [no] authorization
                    — port port
                    — no port
                    — retry count
                    — no retry
                    — server server-index address ip-address secret key [hash | hash2]
                    — no server server-index
                    — [no] shutdown
                    — timeout seconds
                    — no timeout
                    — [no] use-default-template
```

SSH Commands

```
config
     — system
          — security
               — ssh
                    — [no] preserve-key
                    — [no] server-shutdown
                    — [no] version SSH-version
```

TACPLUS Commands

```
config
     — system
          — security
               — [no] tacplus
                    — accounting [record-type {start-stop | stop-only}]
                    — no accounting
                    — [no] authorization
                    — [no] interactive-authentication
                    — server server-index address ip-address secret key [hash | hash2] [port port]
                    — no server server-index
                    — [no] shutdown
                    — timeout seconds
                    — no timeout
                    — [no] use-default-template
```

User Commands

```
config
     — system
          — security
```

```
                          — [no] user user-name
                                    — [no] access [ftp] [snmp] [console] [li]
                                    — console
                                              — [no] cannot-change-password
                                              — login-exec url-prefix::source-url
                                              — no login-exec
                                              — member user-profile-name [user-profile-name…(up to 8 max)]
                                              — no member user-profile-name
                                              — [no] new-password-at-login
                                    — home-directory url-prefix [directory] [directory/directory…]
                                    — no home-directory
                                    — password [password] [hash | hash2]
                                    — [no] restricted-to-home
                                    — [no] rsa-key "public-key-name" key-id
                                    — snmp
                                              — authentication {[none] | [[hash] {md5 key-1 | sha key-1 } privacy
                                                {none|des-key|aes-128-cfb-key key-2}]}
                                              — group group-name
                                              — no group
```

User Template Commands

```
config
      — system
                — security
                          — user-template {tacplus_default | radius_default}
                                    — [no] access [ftp] [console]
                                    — console
                                              — login-exec url-prefix:source-url
                                              — no login-exec
                                    — home-directory url-prefix [directory][directory/directory..]
                                    — no home-directory
                                    — profile user-profile-name
                                    — no profile
                                    — [no] restricted-to-home
```

Dot1x Commands

```
config
      — system
                — security
                          — dot1x
                                    — radius-plcy name
                                              — retry count
                                              — no retry
                                              — server (dot1x) server-index address ip-address secret key [port port]
                                              —  source-address ip-address
                                              — [no] shutdown
                                              — timeout seconds
                                              — no timeout
                                    — [no] shutdown
```

Keychain Commands

```
config
      — system
— security
    — [no] keychain keychain-name
        — description description-string
        — no description
        — direction {uni | bi}
            — bi
                — entry entry-id key [authentication-key | hash-key | hash2-key] [hash | hash2] algorithm algorithm
                    — begin-time [date] [hours-minutes] [UTC] [now] [forever]
                    — [no] shutdown
                    — tolerance [seconds | forever]
            — uni
                — receive
                — entry entry-id key [authentication-key | hash-key | hash2-key] [hash | hash2] algorithm algorithm
                    — begin-time [date] [hours-minutes] [UTC] [now] [forever]
                    — end-time [date][hours-minutes] [UTC] [now] [forever]
                    — [no] shutdown
                    — tolerance [seconds | forever]
                — send
                  — entry entry-id key [authentication-key | hash-key | hash2-key] [hash | hash2] algorithm algorithm
                    — begin-time [date] [hours-minutes] [UTC] [now] [forever]
                    — [no] shutdown
        — [no] shutdown
        — tcp-option-number
            — receive option-number
            — send option-number
```

TTL Security Commands

```
config
    — router
        — bgp
            — group
                — ttl-security min-ttl-value
                — neighbor
                    — ttl-security min-ttl-value
config
    — router
        — ldp
            — peer-parameters
                — peer
                    — ttl-security min-ttl-value
config
    — system
        — login-control
            — ssh
                — ttl-security
```

```
config
    — system
        — login-control
            — telnet
                — ttl-security
```

Login Control Commands

```
config
    — system
        — login-control
            — [no] exponential-backoff
            — ftp
                — inbound-max-sessions value
                — no inbound-max-sessions
            — idle-timeout {minutes | disable}
            — no idle-timeout
            — [no] login-banner
            — motd {url url-prefix: source-url | text motd-text-string}
            — no motd
            — pre-login-message login-text-string [name]
            — no pre-login-message
            — ssh
                — disable-graceful-shutdown
                — inbound-max-sessions
                — outbound-max-sessions
                — ttl-security
            — telnet
                — enable-graceful-shutdown
                — inbound-max-sessions value
                — no inbound-max-sessions
                — outbound-max-sessions value
                — no outbound-max-sessions
                — ttl-security
```

Show Commands

Security

```
show
     — system
          — security
               — access-group [group-name]
               — authentication [statistics]
               — communities
               — cpm-filter
                    — ip-filter [entry entry-id]
                    — ipv6-filter [entry entry-id]
                    — mac-filter [entry entry-id]
               — cpm-queue queue-id
               — cpu-protection
                    — eth-cfm-monitoring [ {service-id service-id sap-id sap-id} | {service-id ser-
                      vice-id sdp-id sdp-id:vc-id} ]
                    — excessive-sources [service-id service-id sap-id sap-id]
                    — policy [policy-id] association
                    — protocol-protection
                    — violators [port] [interface] [sap] [video] [sdp]
               — dist-cpu-protection
                    — policy [policy-id] [association detail]
               — keychain keychain-name [detail]
               — management-access-filter
                    — ip-filter [entry entry-id]
                    — ipv6-filter  [entry entry-id]
                    — mac-filter [entry entry-id]
               — password-options
               — per-peer-queuing [detail]
               — per-peer-queuing
               — profile [user-profile-name]
               — source-address
               — ssh
               — user [user-name] [detail]
               — user [user-name] lockout
               — view [view-name] [detail]
     — certificate
          — ca-profile
          — ca-profile name [association]
          — ocsp-cache [entry-id]
          — statistics
```

Login Control

```
show
     — user
```

Clear Commands

Authentication

```
clear
     — router
```

```
          — authentication
                    — statistics [interface ip-int-name | ip-address]
```

CPM Filter

```
     — cpm-filter
          — ip-filter [entry entry-id]
          — ipv6-filter [entry entry-id]
          — mac-filter [entry entry-id]
```

CPU Protection

```
clear
     — cpu-protection
          — excessive-sources
          — protocol-protection
          — violators [port] [interface] [sap]
```

Clear CPU Stats

```
clear
     — cpm-queue queue-id
```

Clear RADIUS Proxy Server

```
clear
     — router
          — radius-proxy-server server-name statistics
```

Debug Commands

```
debug
     — radius [detail] [hex]
     — no radius
     — [no] ocsp
          — [no] ocsp profile-name
```

Tools Commands

```
tools
     —  dump
          —  security
               — dist-cpu-protection
                    — violators enforcement {sap|interface} card slot-number [fp fp-number]
                    — violators local-monitor {sap|interface}  card slot-number [fp fp-number]
     — perform
          — security
               — dist-cpu-protection
                    — release-hold-down interface interface-name [protocol protocol] [static-
                      policer name]
                    — release-hold-down sap sap-id [protocol protocol] [static-policer name]
```