

# Control plane protection: the Rosetta stone

Greg Hankins, Nokia NLNOG Live! (Sep 2020)



#### Control plane protection introduction

- Nokia routers with FP ASICs support extensive layers of configurable hardware protection mechanisms to protect the CPU from being flooded with control plane traffic
  - Filters (ACLs)
  - Classification
  - Queuing
  - Rate-limiting
- CPMs also use the same packet processing ASICs that are used on the line cards for control plane traffic
  - Network processor provides line-rate filtering and prioritization
  - QoS manager has access to thousands of queues to provide fairness and isolation
  - All control plane protection is implemented in the forwarding hardware except for out-of-band management Ethernet port filters



#### Interface isolation

**Protocol isolation** 

Peer isolation

#### Control plane protection overview

- In-band: control plane traffic flows from the line cards to the CPM
  - Line cards
    - Filters (ACLs): IPv4, IPv6, MAC
    - Anti spoofing (uRPF, MAC learning)
    - Distributed CPU protection: distributed set of rate limiting functions that run on the network processor
  - CPM
    - CPM filters: IPv4, IPv6, MAC
    - Centralized CPU protection: set of rate limiting functions that run on the network processor
    - Per-peer queues, per-protocol queues, CPM queues
- Out-of-band Ethernet port: MAF filters



### Control plane packet flow



Not all mechanism apply to all platforms

## Distributed CPU protection (DCP)

- Provides granular rate-limiting for control plane traffic per-SAP/interface and per-protocol distributed to the line cards
  - Rate-limit scale and flexibility provided using static or dynamically instantiated rate-limit policers
  - Option to mark excess traffic as low-priority instead of rate-limit discard action
  - Example protocol list: all-unspecified, arp, bfd-cpm, bgp, dhcp, eth-cfm, http-redirect, icmp, igmp, isis, ldp, mld, mpls-ttl, ndis, ospf, pim, pppoe-pppoa, rsvp



#### Per-protocol queues

- Provides protocol isolation by separating different protocols into dedicated hardware queues to the CPM
  - Discards per-protocol traffic in case there is more work than the CPU can handle instead of dropping other protocols
  - Multicore CPU and multiprocess software architecture and scheduler provides additional fairness





#### Control plane interface filter

- Interface filter provides an additional layer of protection together with DCP
  - Allow BGP packets from configured BGP neighbors
  - Drop all other BGP packets going to the CPM

```
[ex:configure filter]
A:grhankin@brl-nyc# info flat
    match-list ip-prefix-list "bgp-neighbors" apply-path bgp-peers 1 group ".*"
    match-list ip-prefix-list "bgp-neighbors" apply-path bgp-peers 1 neighbor ".*"
    ip-filter "179" entry 10 match protocol tcp
    ip-filter "179" entry 10 match src-ip ip-prefix-list "bgp-neighbors"
    ip-filter "179" entry 10 match dst-port eq 179
    ip-filter "179" entry 10 action accept
    ip-filter "179" entry 20 match protocol tcp
    ip-filter "179" entry 20 match dst-port eq 179
    ip-filter "179" entry 20 match dst-port eq 179
    ip-filter "179" entry 20 action accept
    ip-filter "179" entry 20 action accept
    ip-filter "179" entry 20 action accept
    ip-filter "179" entry 20 action drop-when extracted-traffic
```



# Control plane protection summary and recommendations

Protection mechanism	Advantage	Recommendation and comments	Enabled by default?
CPM filters and queues	Provides accept/drop rules based on IP/MAC filter criteria in hardware (drop unwanted protocols/sources) CPM filter optional action to map packets into CPM queues to isolate specific traffic	CPM filters are recommended in all environments CPM queues are only recommended for debugging purposes	No
CPU protection (including protocol protection)	Provides interface isolation by rate-limiting total control traffic per-SAP/interface in hardware at the CPM level and optionally drop unconfigured protocols	Recommended in all environments	Yes (protocol protection not enabled by default)
Per-peer queues (PPQ)	Provides isolation between peers in dedicated hardware queues for BGP, LDP, MSDP from the rest of the control traffic	Recommended in all environments	Yes
Per-protocol queues	Provides default isolation between protocols in dedicated hardware queues	Recommended in all environments	Yes
Management access filter (MAF)	Provides centralised accept/drop filter rules in CPU for management traffic	Recommended when the out-of-band management Ethernet port is used	No
Distributed CPU protection (DCP)	Provides granular rate-limiting for control plane traffic per- SAP/interface and per-protocol distributed to the line cards (per-interface per-protocol isolation)	Recommended in all environments	Yes
Line card IP filters	Drop traffic on ingress or egress line card interfaces based on IP/MAC filter criteria (L3, L4, packet length, TTL, rate-limit).	Recommended in all environments	Νο

#### Resources

- All control plane protection features are described in the System Management Guide section 2.3. Control and Management Traffic Protection
  - PDF: <u>https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE15829AAACTQZZA01\_V1\_7450%20ESS%207750%20SR%207950%20XRS%20and%20VSR%20System%20Management%20Guide%2020.7.R1.pdf</u>
  - HTML: https://infocenter.nokia.com/public/7750SR207R1A/topic/com.sr.system.mgmt/html/security.html?cp=21\_ 1\_2#droberts5ipjdbqqhh8
- New security best practice and hardening guide is planned with Release 20.10.R1 (October)
  - Check <u>https://documentation.nokia.com</u>