Cisco.com

CISCO NETWORK FOUNDATION PROTECTION: PROTECTING THE CISCO CATALYST SERIES PLATFORM

SECURITY TECHNOLOGY GROUP

JANUARY 2005

Agenda

- Introduction
- Configuring Control Plane Protection
- Deployment Guide
- Summary and References

INTRODUCTION

Risk Landscape

- Denial of Service (DoS) attacks target the network infrastructure by generating IP traffic streams to the control plane at very high rates
- The control plane is forced to spend an inordinate amount of time, processing this malicious traffic
- Results in excessive CPU utilization and CPU resource hijacking by the hackers
- Examples of such attacks include:
  - TCP SYN floods
  - IP Fragments
  - Internet Control Message Protocol (ICMP) Echo Requests
  - Fraggle Attacks

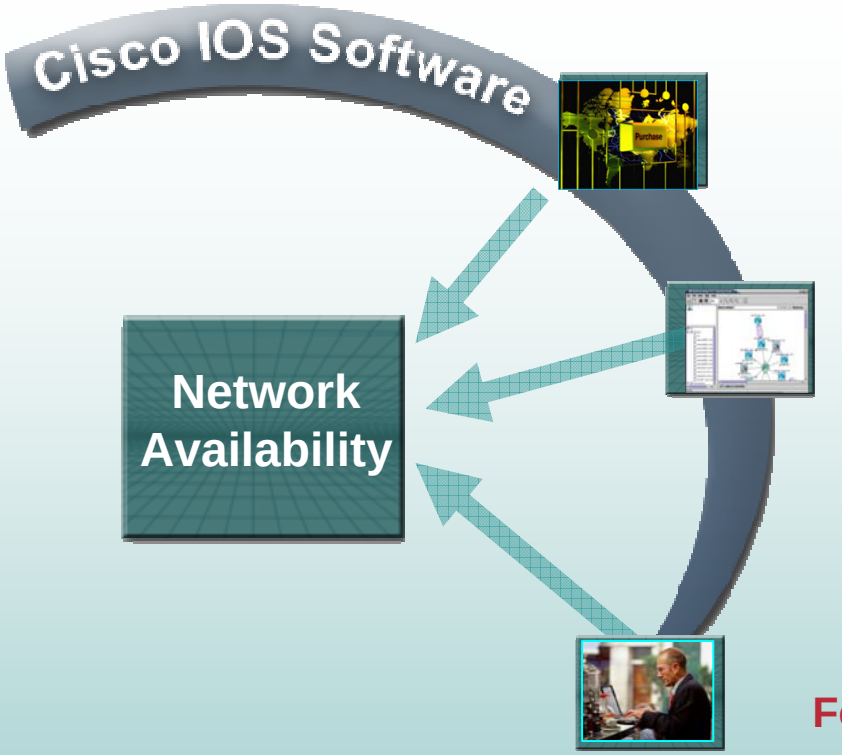
Risk Landscape (Cont.)

- **Attacks can devastate a network by causing:**
  - **High route processor CPU utilization (near 100%)**
  - **Loss of protocol keepalives and routing protocol updates**
  - **Route flaps and major network transitions**
  - **Slow or unresponsive interactive sessions via the CLI**
  - **Route Processor resource exhaustion**
    - **Resources such as memory and buffers are unavailable for legitimate IP data packets**
    - **Indiscriminate packet drops for all incoming packets**

Keys to Prevent Attacks at the Routers

- **To protect the router mechanisms have to:**
  - **Identify DoS attack packets from valid packets (Classification)**
  - **Once identified, mark, drop, or rate-limit (Service Policies)**
  - **Separate data plane packets from control plane packets**
  - **Provide DoS mechanisms independent from existing interface capabilities, but do not impact current performance**
  - **Provide global CLI to minimize configuration changes to deployed networks**

Securing the Router – Plane by Plane



Ability to Route → Secure **Control** Plane

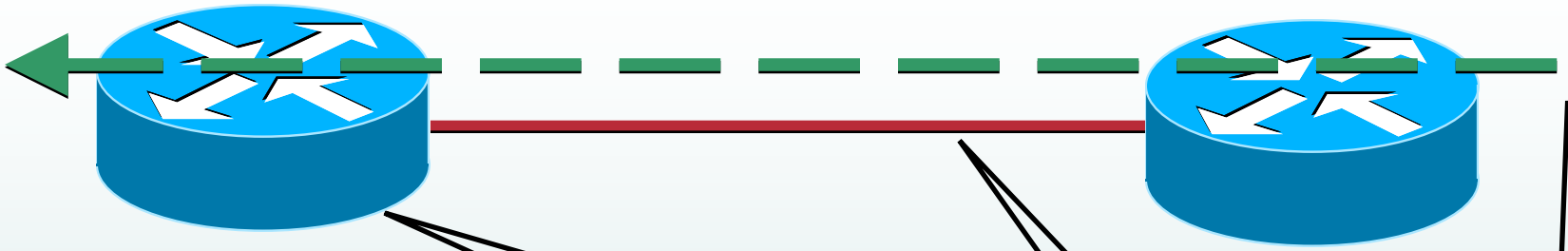
Ability to Manage → Secure **Management** Plane

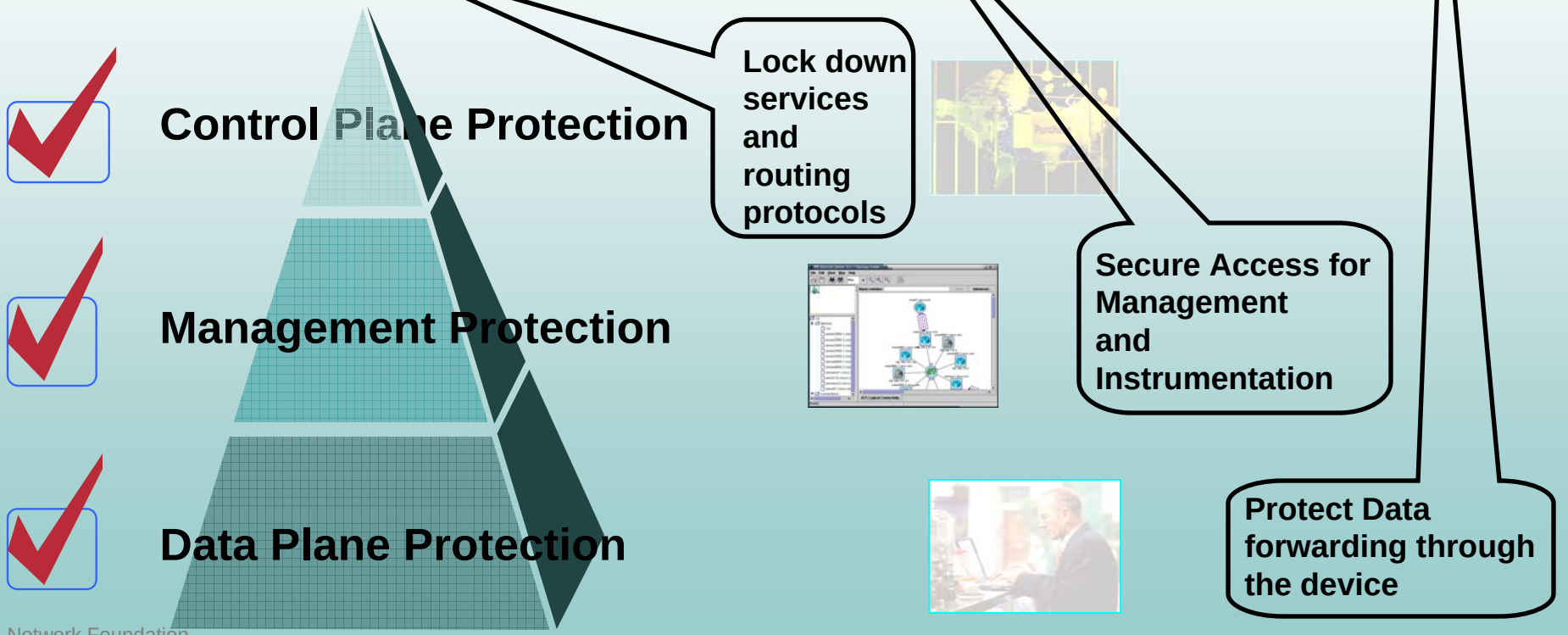
Ability to Forward Data → Secure **Data** Plane

Think "Divide and Conquer": Methodical Approach to Protect Three Planes

Cisco NFP – Network Foundation Protection Alcazar Program

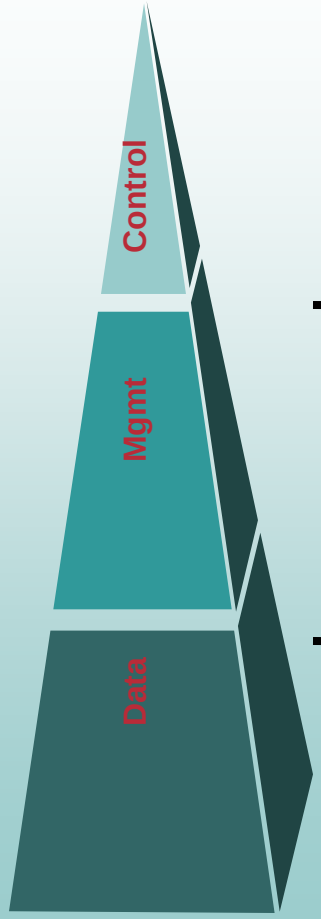
Secure Networks Must Be Built on a Secure Foundation





Cisco NFP – Three Planes Definitions

Cisco Network Foundation Protection (NFP) is a Cisco IOS® Technology suite that protects network devices, routing and forwarding of control information, and management of traffic bounded to the network devices



Control Plane Protection – protects the control plane traffic responsible for traffic forwarding

- Autosecure with rollback functionality
- Control Plane Protection
- CPU / Memory Threshold

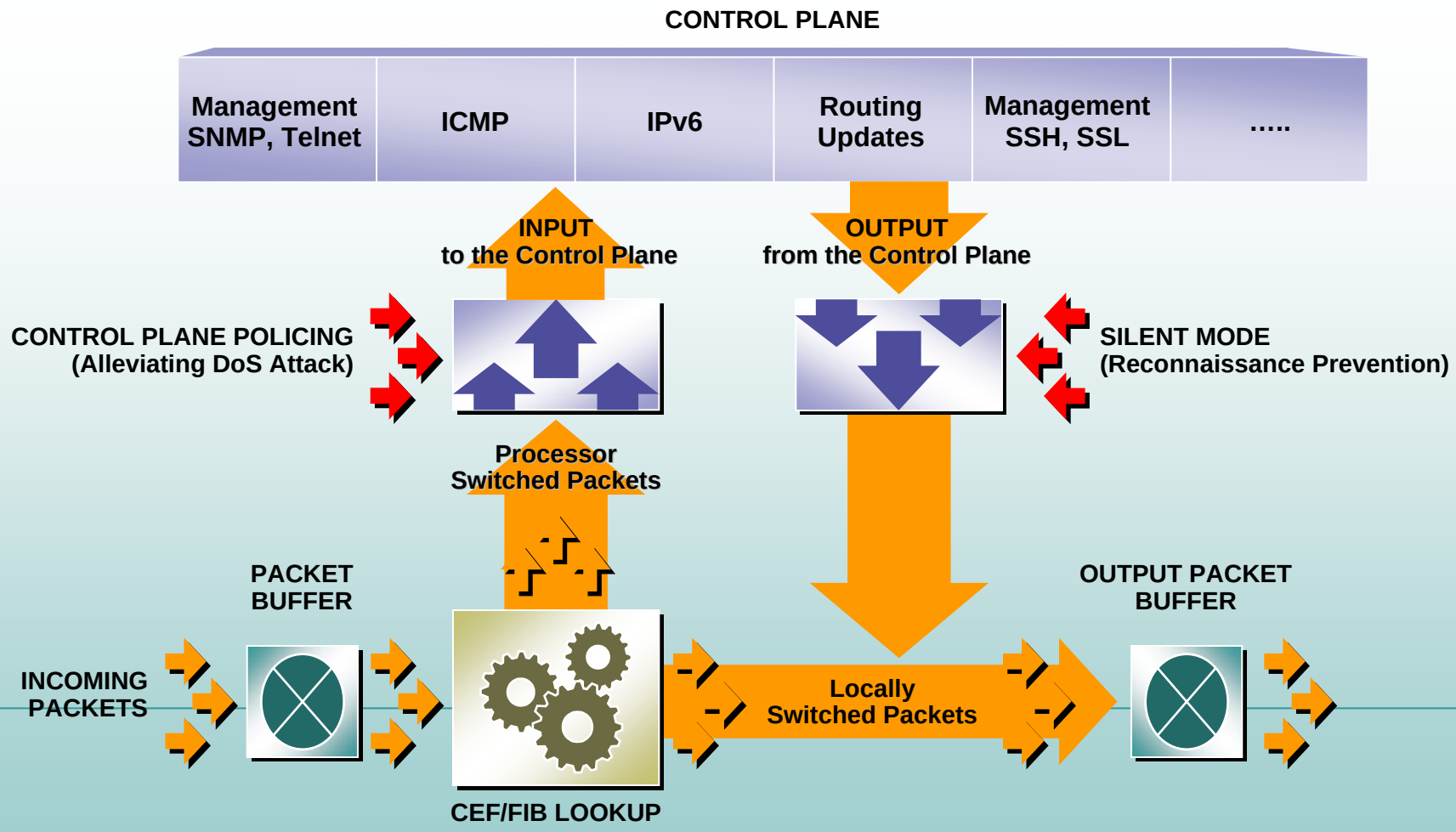
Management Plane Protection – protects the management plane from unauthorized management access and polling

- Secure Shell (SSH) only access
- VTY Access Control List (ACL)
- Cisco IOS Software login enhancement
- Command Line Interface (CLI) views

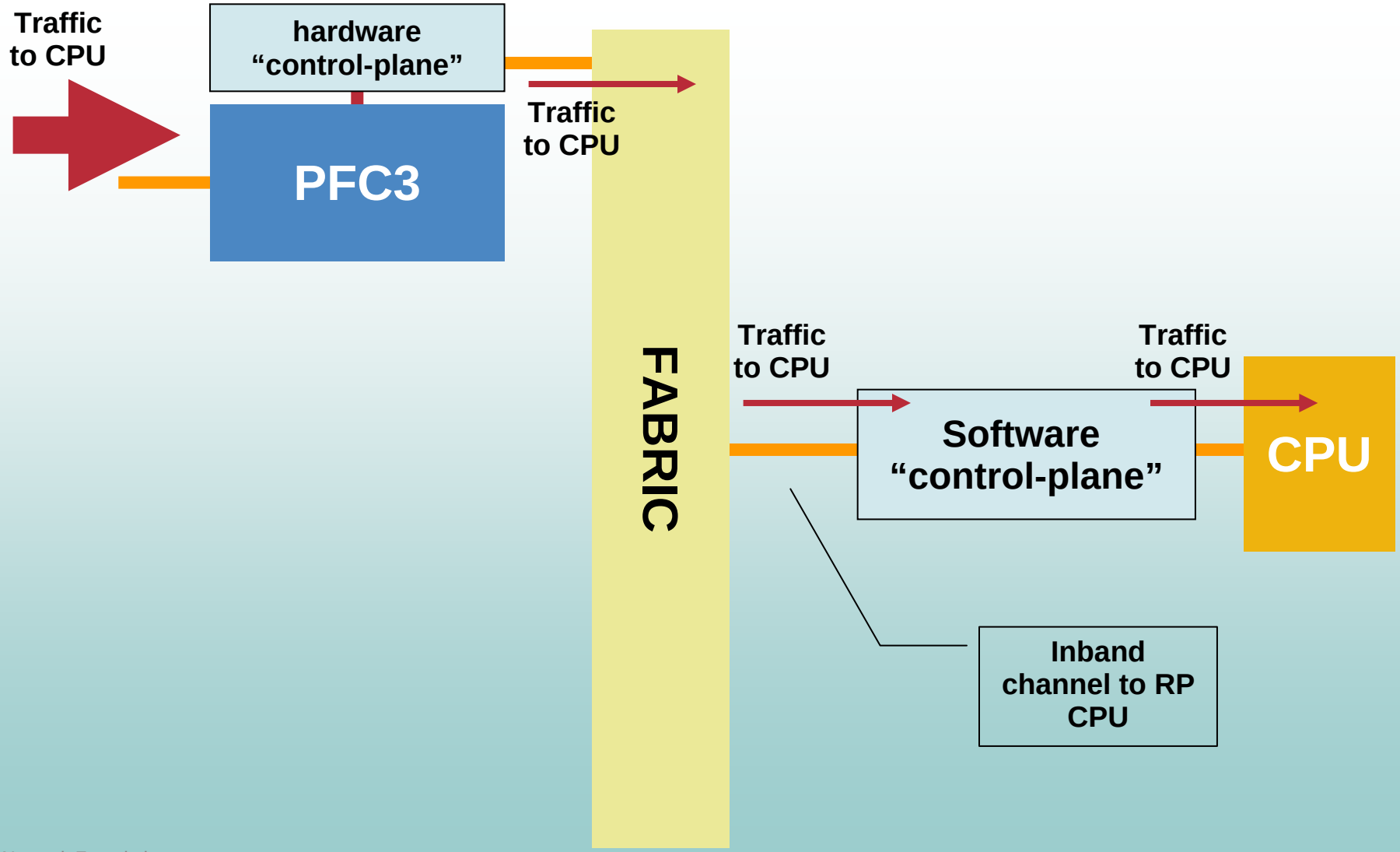
Data Plane Protection – protects the data plane from malicious traffic

- Unicast RPF for anti-spoofing
- Control Plane Protection for Data traffic
- Committed Access Rate (CAR)

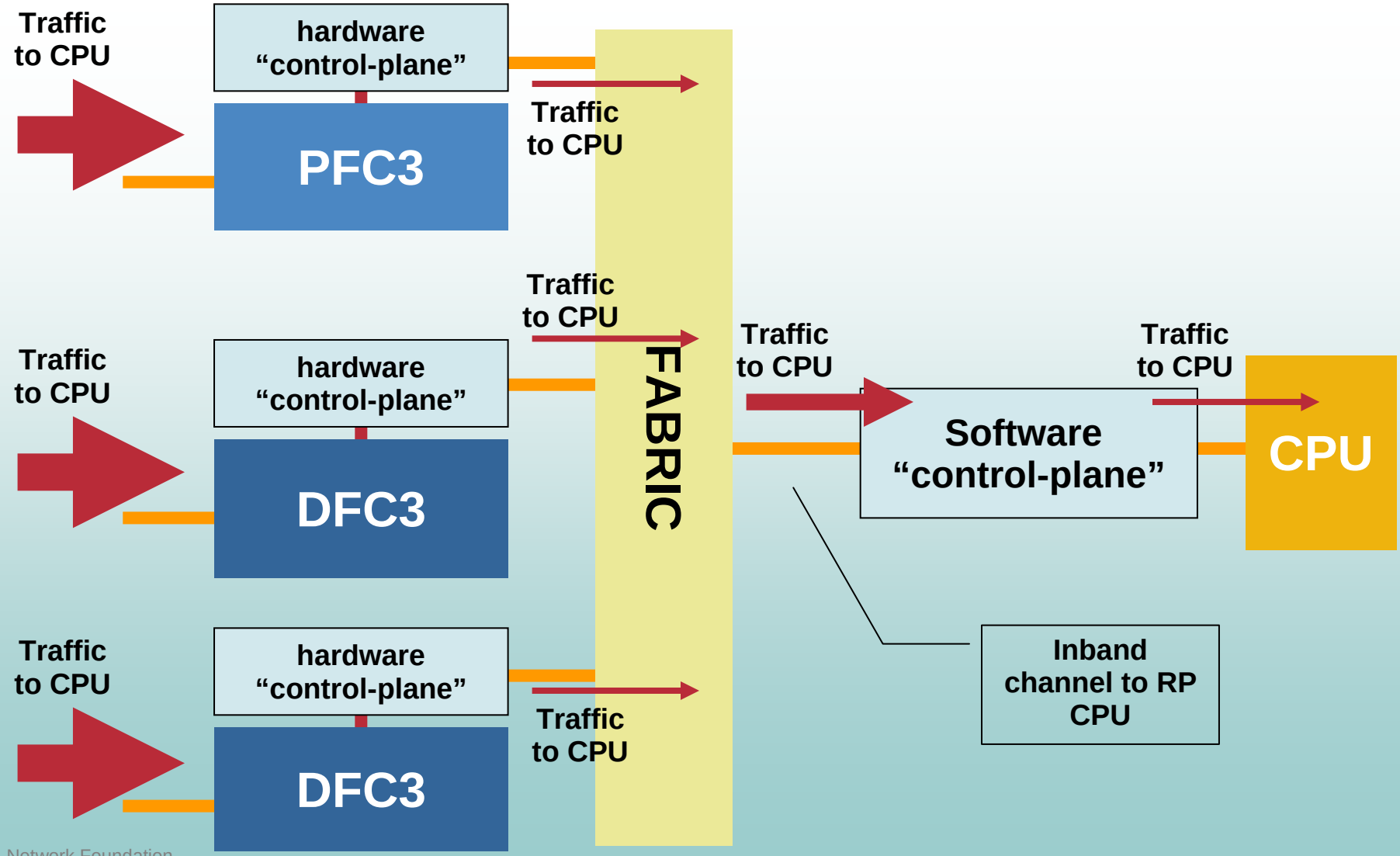
Introduction – Control Plane Protection Policing



Control Plane Protection – Policing for Cisco Catalyst Series Platform



Control Plane Protection – Policing for Cisco Catalyst Series Platform



Introduction – What CPU Rate Limiters Are Available?

Unicast Rate Limiters	
CEF Receive	Traffic destined to the Router
CEF Glean	ARP packets
CEF No Route	Packets with not route in the FIB
IP Errors	Packets with IP checksum or length errors
ICMP Redirect	Packets that require ICMP redirects
ICMP No Route	ICMP unreachables for unroutable packets
ICMP ACL Drop	ICMP uncreachables for admin deny packets
RPF Failure	Packets that fail uRPF check
L3 Security	CBAC, Auth-Proxy, and IPSEC traffic
ACL Input	NAT, TCP Int, Reflexive ACLs, Log on ACLs
ACL Output	NAT, TCP Int, Reflexive ACLs, Log on ACLs
VACL Logging	CLI notification of VACL denied packets
IP Options	Unicast traffic with IP Options set
Capture	Used with Optimized ACL Logging

B/BXL

Unicast Rate Limiters	
Multicast FIB-Miss	Packets with no mroute in the FIB
IGMP	IGMP packets
Partial Shortcut	Partial shortcut entries
Directly Connected	Local multicast on connected interface
IP Options	Multicast traffic with IP Options set
V6 Directly Connect	Packets with no mroute in the FIB
V6*, G M Bridge	IGMP Packets
V6*, G Bridge	Partial shortcut entries
V6 S, G Bridge	Partial shortcut entries
V6 Route Control	Partial shortcut entries
V6 Default Route	Multicast traffic with IP Options set
V6 Second Drop	Mulicast traffic with IP Options set

B/BXL

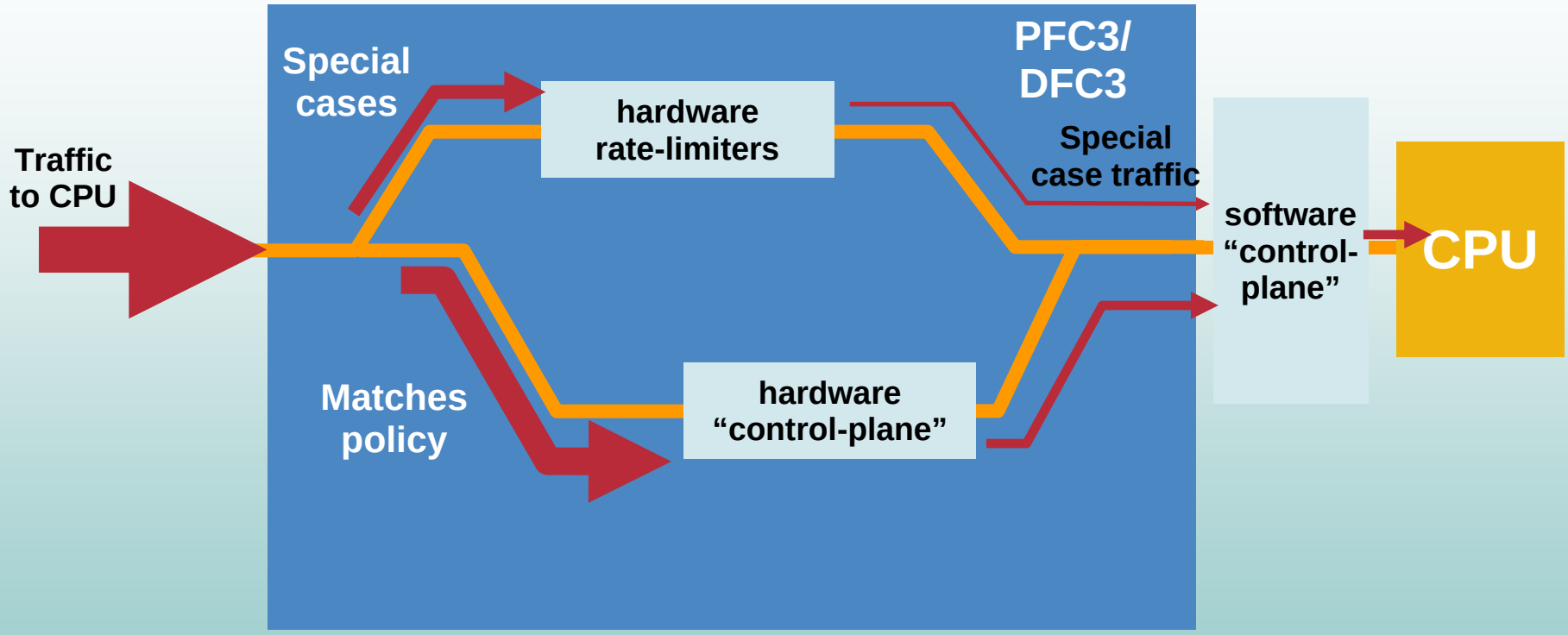
Shared across the 10 hardware Revocation Lists.

Layer 2 Rate Limiters	
L2PT	L2PT encapsulation/decapsulation
PDU	Layer 2 PDUs

General Rate Limiters	
MTU Failure	Packets requiring fragmentation
TTL Failure	Packets with TTL<=1

Interaction Between Control Plane Protection, Policing, and CPU Rate Limiter

Special-case Rate Limiters OVERRIDE Hardware Control Plane Policing!



Test Setup – Mitigation of Multiple Attacks

- **CPP configuration**

```
policy-map CoPP
 class cpp-bgp
   police 32000 1500 1500 conform-action transmit exceed-action transmit
 class cpp-igp
   police 32000 1500 1500 conform-action transmit exceed-action transmit
 class cpp-managment
   police 32000 1500 1500 conform-action transmit exceed-action transmit
 class cpp-monitoring
   police 600000 18750 18750 conform-action transmit exceed-action drop
 class cpp-critical
   police 32000 1500 1500 conform-action transmit exceed-action transmit
 class cpp-undesirable
   police 320000 10000 10000 conform-action drop exceed-action drop
 class cpp-default
   police 620000 19375 19375 conform-action transmit exceed-action drop
```

- **CPU Rate Limiter configuration**

```
mls rate-limit multicast ipv4 partial 1000 100
mls rate-limit unicast ip options 1000 10
mls rate-limit all ttl-failure 1000 10
```

CPU Rate Limiters Recommendations

- **Use all eight Layer 3 rate limiters!**
  - **Easy task**
- **Consider most likely attack vectors for the network environment**
  - **Enable the rate limiters most likely to be used**
- **Do not waste a rate-limiter on VACL logging, if it is not happening**
  - **No mls rate-limit unicast acl vacl**
- **Disable redirects and save a rate limiter**
  - **Hardware forwarding platform reduces need for redirect efficiency**
- **Maximum Transmission Unit (MTU) limiter is not required, if all interfaces have same MTU**

CONFIGURING CONTROL PLANE PROTECTION

Configuring Control Plane Protection – Policing Four Step Process

1. **Define a packet classification criteria**

```
router(config)# class-map <traffic_class_name>
router(config-cmap)# match <access-group>
```

2. **Define a service policy**

```
router(config-pmap)# policy-map<service_policy_name>
router(config-pmap)# class <traffic_class_name>
router(config-pmap)# police <rate> conform-action transmit
                      exceed-action drop
```

3. **Enter control-plane configuration mode**

```
router(config)# control-plane
router(config-cp)#
```

4. **Apply QoS Policy**

```
router(config-cp)# service-policy input  <service_policy_name>
```

Control Plane Policing Configuration

- Must enable QoS globally! (mls qos)
  - Otherwise, CoPP is performed in software only
- Define ACLs to match traffic
  - Permit means traffic will belong to class; deny means will fall through
- Define class-maps (class-map <name>)
  - Use “match” statements to identify traffic associated with the class
  - match {access-group | ip {precedence | dscp}}
- Define policy-map (policy-map <name>) and associate classes and actions to it
  - Policing is the only supported action
  - Usual Cisco Catalyst 6500 Series Switch policing syntax
- Tie the policy-map to the control-plane interface

```
mls qos

ip access-list extended CPP-MANAGEMENT
 remark Remote management
 permit tcp any any eq SSH
 permit tcp any eq 23 any
 permit tcp any any eq 23

class-map match-all CPP-MANAGEMENT
 description Important traffic,
 eg management
```

Configuring CPU Rate Limiter

Apply a CPU Rate Limiter at a specific rate

Router(config)# mls rate-limit <all | unicast | multicast | layer 2> <special_case_rate_limiter> <packets_per_second>

Example: Rate Limit traffic with TTL=1 to 1000pps

Router(config)# mls rate-limit all ttl-failure 1000

DEPLOYMENT GUIDE

Deployment Guide – Step I
Classify and Permit All Traffic

- Identify traffic of interest and classify it into multiple traffic classes
  - BGP
  - IGP
  - Management
  - Reporting
  - Monitoring
  - Critical Applications
  - Undesirable and Default
- Use ACLs to identify traffic in each class
  - Match criteria supported includes:
    - ip standard ACL 1-99
    - ip extended ACL 100-199
- Use protocol and port number for Modular Quality of Service (QoS) Command Line Interface (MQC) match
- Last ACL entry permits ip any any
  - Otherwise, implicit deny statement
- Apply ACLs to class-maps and permit traffic in each class

Deployment Guide – Step II
Review ACL Counters and Initial Policy

- **show policy-map control-plane and show mls qos ip command**
  - **Displays dynamic information for monitoring control plane policy**
  - **Statistics include rate information and number of packets/bytes confirmed or exceeding each traffic classes**
- **show access-lists command**
  - **Provides packet count statistics per ACL entry (ACE), when traffic matches a particular entry**
  - **This data is used to develop a policy that ensures that identified traffic is matching as expected**
  - **Absence of any hits on an entry indicate lack of traffic matching the ACE criteria –the rule might be re-written**

Deployment Guide – Step III
Define Control Plane Policy

- Explicitly allow needed and known critical protocols such as BGP and EIGRP
  - Conform and exceed action → transmit
- Define other required, but not critical traffic, such as ICMP, SNMP, SSH, Telnet, and default
  - Conform action → transmit, exceed action → drop
- Drop all other undesirable traffic
- Depending on class defined, apply appropriate policy
  - Routing Protocol traffic (BGP, IGP) - no rate limit
  - Management traffic (SNMP, SSH, NTP, and etc) – conservative rate limit
  - Reporting traffic (SAA combined with DSCP) – conservative rate limit
  - Monitoring traffic (ICMP, traceroute) – conservative rate limit
  - Critical traffic (HSRP, SIP/VoIP, DLSw) – conservative rate limit
  - Default traffic – low rate limit
  - Undesirable traffic (DoS Attacks) – drop

Deployment Guide – Step IV
Define CPU Rate Limiters

- **Use all eight Layer 3 rate limiters!**
  - **Easy task**
- **Consider most likely attack vectors for the network environment**
  - **Enable the rate limiters, which are most likely to be used**
- **Do not waste a rate-limiter on VACL logging, if it is not happening**
  - **No mls rate-limit unicast acl vacl**
- **Disable redirects and save a rate limiter**
  - **Hardware forwarding platform reduces need for redirect efficiency**
- **MTU limiter is not required, if all interfaces have same MTU**
- **Configure PDU Layer 2 rate limiter with care**
  - **Calculate expected/possible number of valid PDUs (ballpark), double or triple them and include BPDUs, DTP, VTP, PAgP/LACP, UDLD, and etc.**
  - **Remember that Revocation Lists do not discriminate between "good" frames and "bad" frames**

Deployment Guide – Step IV
Which CPU Rate Limiters are Needed?

1. **Cisco Express Forwarding glean**
   - Limits traffic requiring ARP for a next hop
   - Does NOT limit ARP traffic!
2. **Multicast default adjacency**
   - Limits traffic punted to establish multicast control plane state (e.g.: new S,G traffic)
3. **ACL bridged input**

   ACL bridged output
   - Limit packets with ACL bridge result (eg, “log” ACEs)
4. **TTL failure**
   - Limits unicast traffic with expiring TTL
5. **Unicast IP options**
   - Limits unicast packets with IP options
6. **Multicast IP options**
   - Limits multicast packets with IP options

Deployment Guide – Step IV
Which CPU Rate Limiters are Needed?

7. ICMP unreachables no-route

   ICMP unreachables ACL-drop

   Limit unroutable or ACL-denied traffic

8. IP errors

   Limits error packets (e. g.: bad L3 checksum, L2/L3 length mismatch)

9. IP RPF traffic

   Limits uRPF failed traffic

   Freebie along with above limiters

10. ICMP redirect

    Limits traffic punted to trigger a redirect

11. Multicast IGMP (Layer 2)

    Limits IGMP packets to the SP CPU

12. Layer 2 PDU (Layer 2)

    Limits Layer 2 protocol data units (BPDUs, VTP, DTP, PAgP, etc)

Deployment Guide – Step V
Fine Tune the Policy

- Ensure that unexpected results are investigated
- Increasingly restrict source and destination addresses
  - Only certain hosts send SNMP polls, ICMP requests, or SSH/telnet into a router
- BGP peers are using loopback
- Use class-default to identify unclassified packets
- Remove permit ip any any when confident with results
- Additional information:
  - www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_white_paper09186a0080211f39.shtml

Control Plane Policy Template

- **class-map match-all cpp-bgp**
  - **BGP**
- **class-map match-all cpp-igp**
  - **EIGRP, OSPF, etc...**
- **class-map match-all cpp-management**
  - **SNMP, NTP, SSH, TACACS, TFTP, etc…**
- **class-map match-all cpp-reporting**
  - **Echo, echo-reply with DSCP marking per class**
- **class-map match-all cpp-monitoring**
  - **ICMP, traceroute, etc…**
- **class-map match-all cpp-critical-applications**
  - **HSRP, DLSw, SIP/VoIP, etc…**
- **class-map match-all cpp-layer-2-protocols**
  - **ARP**
- **class-map match-all cpp-default**
  - **Non-specifically marked traffic**
- **class-map match-any cpp-deny**
  - **Classified attack traffic**

SUMMARY AND REFERENCES

Summary – Control Plane Protection Policing

- **Unicast Traffic**

  Hardware mechanism for defining and implementing sophisticated router protection schemes

- **Multicast Traffic**

  Hardware independent mechanism for defining and implementing sophisticated router protection scheme after first pass through CPU rate limiters

- **Protection against DoS attacks targeted towards the network infrastructure**
- **Easy deployment by leveraging existing MQC infrastructure**
- **Consistent implementation strategy across all Cisco hardware**
- **Increased reliability, security, and availability of the network**

References

- **Cisco IOS Security Infrastructure**

  www.cisco.com/go/autosecure/

- **Cisco IOS Software Release 12.2(18)SXD**

  www.cisco.com/go/release122s/

- **Deploying Control Plane Protection - Policing**

  www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_white_paper09186a0080211f39.shtml

- **Control Plane Protection – Policing Feature Guide**

  www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a00801afad4.html

- **QoS Command Reference Guide**

  www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_book09186a00801a7ec7.html

Hardware Support

Hardware	Availability
• Cisco 7600 Series Router • Cisco Catalyst® 6500 Series Switch	• Cisco IOS Software Release 12.2(18)SXD1
• Cisco 7200 Series Router • Cisco 7500 Series Router	• Cisco IOS Software Release 12.2(18)S
• Cisco 12000 Series Internet Router	• Cisco IOS Software Release 12.0(29)S
• Cisco 1751 Series Router • Cisco 2600-XM Series • Cisco 3700 Series Router • Cisco 7200 Series Router	• Cisco IOS Software Release 12.3(4)T