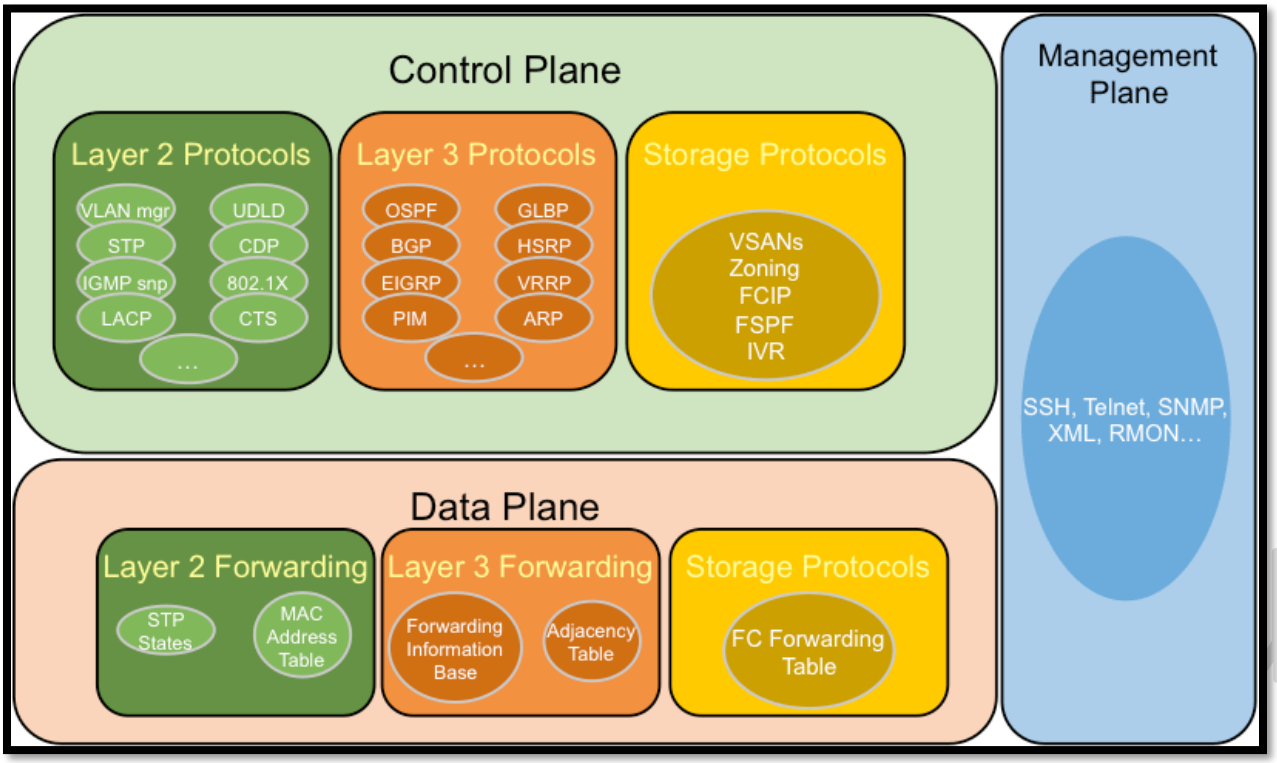

Networkforyou
Welcome
To
Network for you
CoPP
Networkforyou

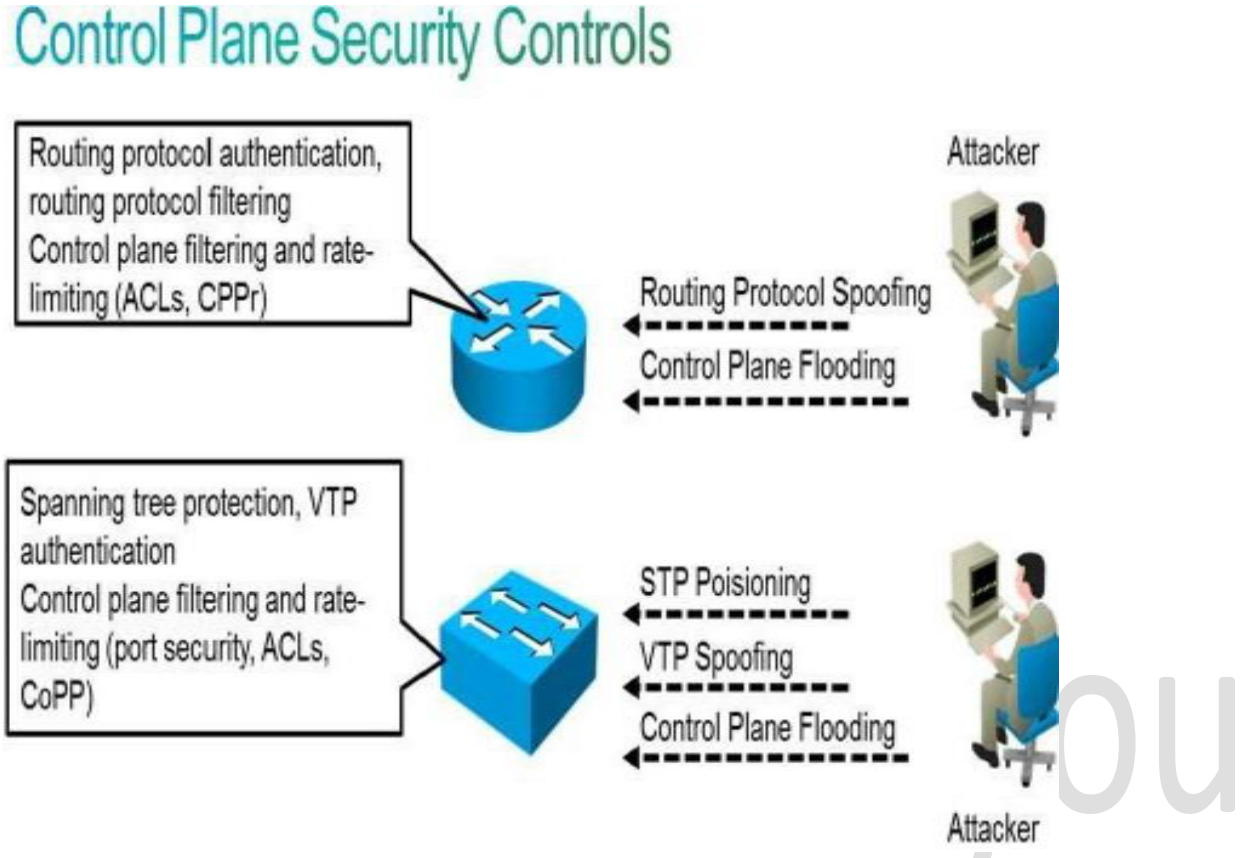
Control Plane Policing (CoPP): Allows you rate-limit traffic that goes to the route processor.

Before going to this we need to have Router/ Switch plan idea.

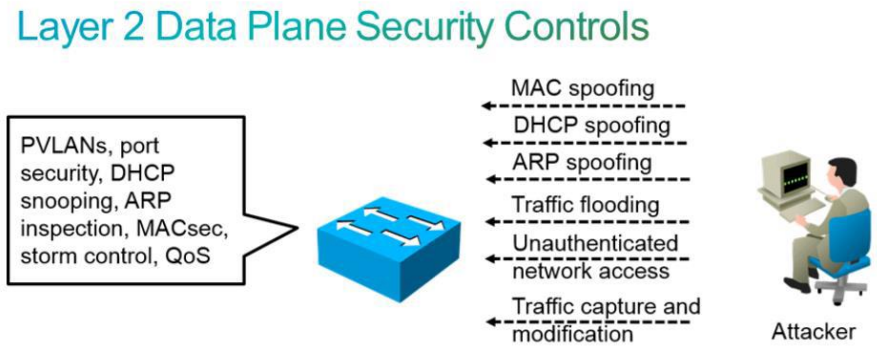


Control Plane: Control Plan traffic is from the **device to the device**. The control plane is responsible for exchanging routing information building the arp table etc. As given below the responsible of control plan.

- Learning MAC address to build a switch MAC address table
- Running STP to create a loop free topology.
- Building ARP tables
- Running routing protocols like OSPF, BGP, EIGRP etc. to build routing table.



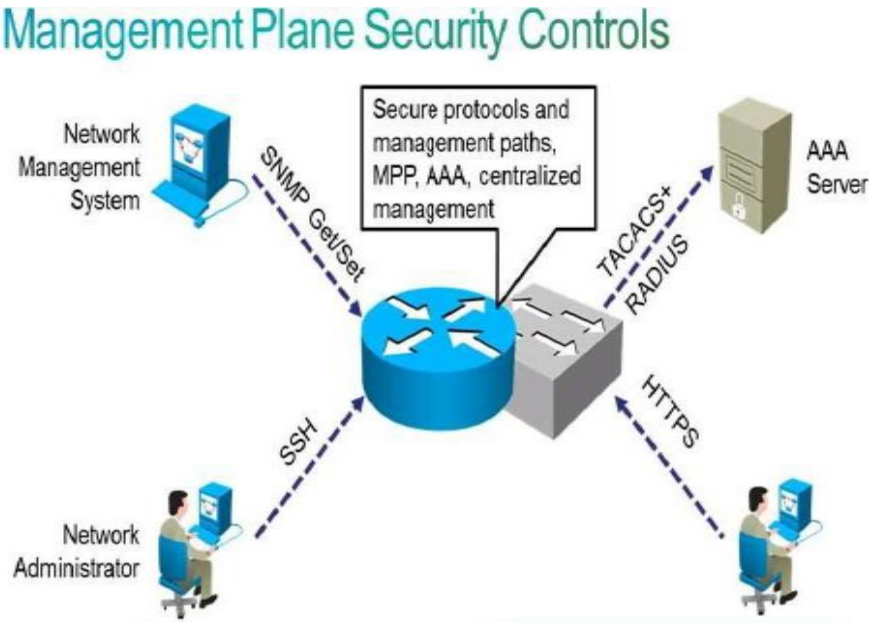
Data Plane: Data Plan traffic from the **user to the user**. Data plane is responsible for forwarding traffic and it relies on the information that gets from control plan. Here is some task that take care by Data Plan is given below.



Management Plane:

Management Plan traffic is from the **user to the device**. Is used for access and management of our network devices. Management Plane protocols are FTP, HTTP, HTTPS, SSH, SNMP, Talent, TFTP etc.

- Telnet
- SSH
- Console



Best Practices for Securing the Management Plane.

- Enforce password policy on devices.
- Maximum number of login attempts, minimum password length.
- Custom privilege level assignments to restrict users.
- Use AAA services to authenticate, authorize & audit any commands.
- Keep accurate time using secure Network Time Protocol (NTP).
- Use encrypted and authenticated versions of SNMP.
- Encrypted management protocols such as SSH, HTTPs, SNMPv3.
- Enable Logging and monitoring on all network devices.
- Disable any unnecessary services on network devices.

Best Practices for Protecting the Data Plane.

- Create and enable Access Control List on network devices.
- Create and deploy Private VLAN (Virtual Local Area Network).
- Enable Spanning Tree guard such as BPDU Guard and Root Guard.

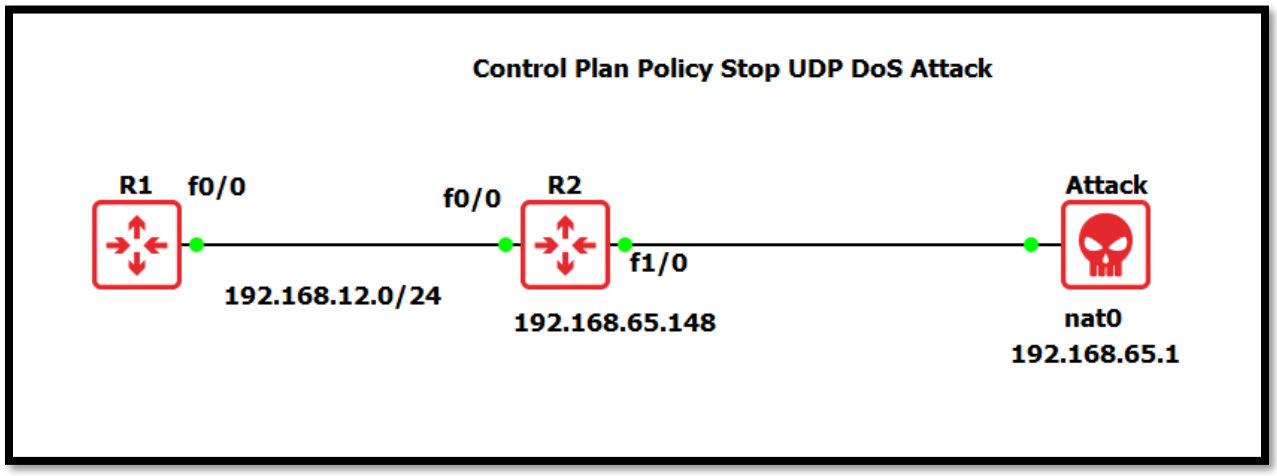
- Port security to protect against MAC address flooding and CAM overflow attacks.
- Enable DHCP snooping feature to prevent a rogue DHCP attack in the network.
- Dynamic ARP inspection (DAI) protect against ARP spoofing, ARP poisoning.

Best Practices for Protecting the Control Plane:

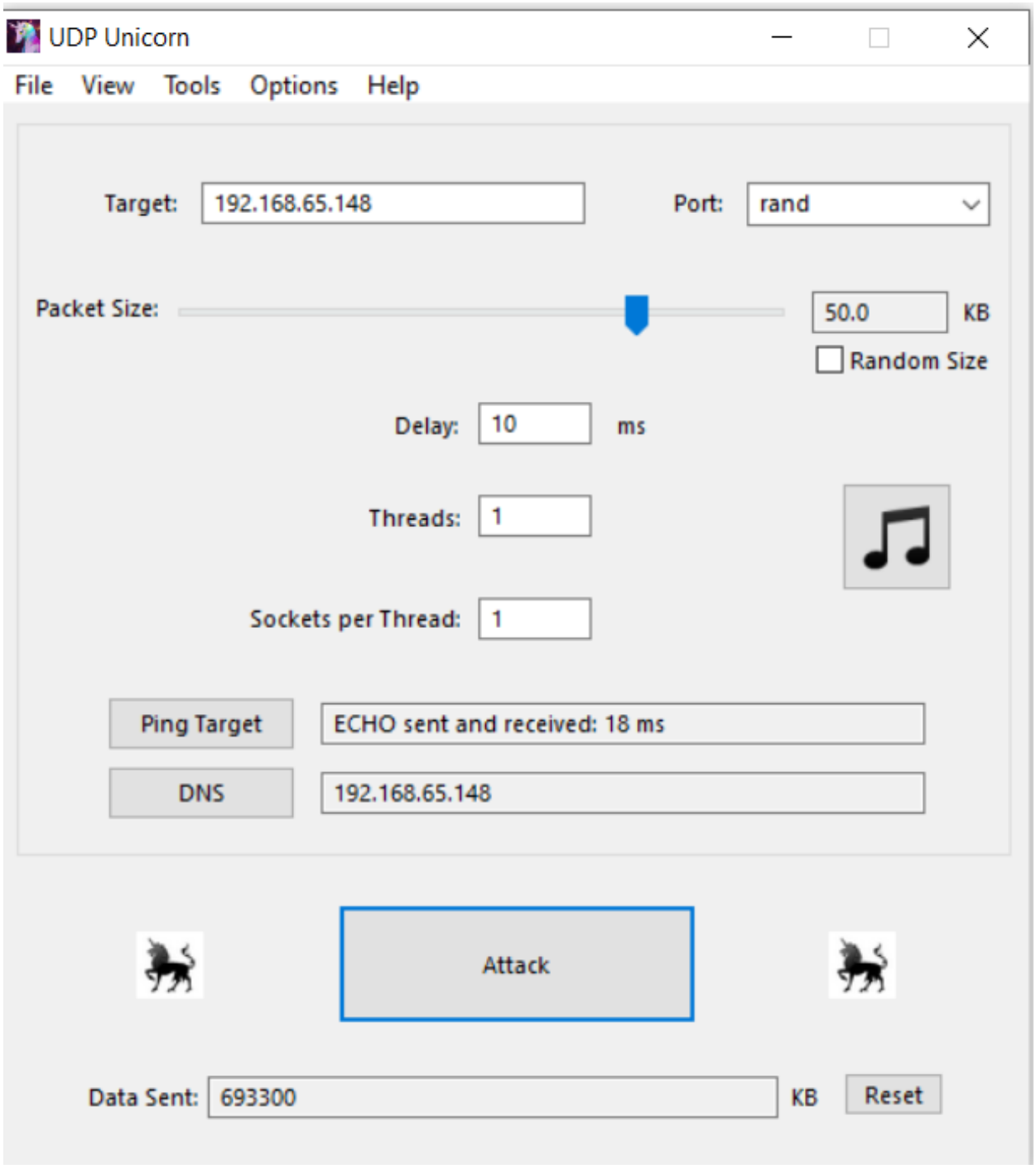
- Create and enable Control Plane Policing (CoPP) on devices.
- Identify type & rate of traffic reaches the control plane of Cisco IOS device.
- Allow users to manage the flow of traffic handled by the route processor.
- Prevent unnecessary traffic from overwhelming the route processor.
- Create and enable CPPr (Control Plane Protection) on network devices.
- Create and enable Port-filtering feature on network devices.
- Limits the number of packets for a specific protocol.
- Securing Routing Protocols use password authentication method.

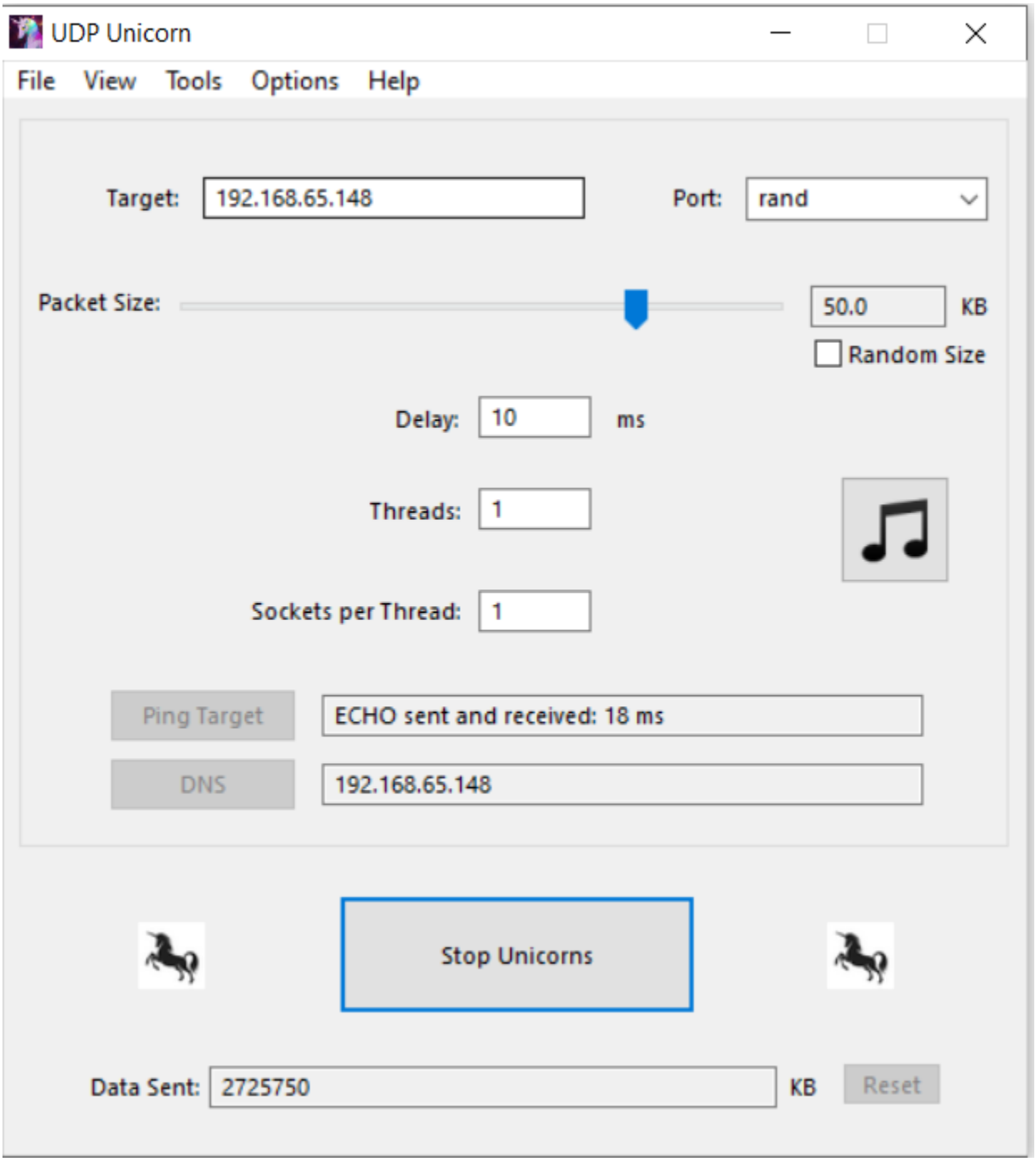
Name	Use for
Create ACL	Identify the Traffic create Access Control List
Class Map	Identify the Traffic Use already created ACL
Policy Map	Policy Map take Action on Class Map
Control Plan	Apply the Policy Map using Service Policy

Lab Time:



R1 Basic Configuration	R2 Basic Configuration
en config t hostname R1 int f0/0 ip add 192.168.12.1 255.255.255.0 no sh router ospf 1 int f0/0 ip ospf 1 area 0	en config t hostname R2 int f0/0 ip add 192.168.12.2 255.255.255.0 no sh int f1/0 ip add dhcp no sh router ospf 1 int f0/0 ip ospf 1 area 0


UDP Unicorn
File View Tools Options Help
Target: 192.168.65.148
Port: rand
Packet Size:
50.0
KB
Random Size
Delay: 10 ms
Threads: 1
Sockets per Thread: 1
Ping Target
ECHO sent and received: 18 ms
DNS
192.168.65.148
Attack
Data Sent: 693300
KB
Reset


UDP Unicorn
File View Tools Options Help
Target: 192.168.65.148
Port: rand
Packet Size:
50.0 KB
Random Size
Delay: 10 ms
Threads: 1
Sockets per Thread: 1
Ping Target
ECHO sent and received: 18 ms
DNS
192.168.65.148
Stop Unicorns
Data Sent: 2725750 KB
Reset

Control Plan Policy Stop UDP DoS Attack
R2(config)#ip access-list extended test R2(config-ext-nacl)#permit udp any any R2(config)#class-map cmap R2(config-cmap)#match access-group name test R2(config)#policy-map pmap R2(config-pmap)#class cmap R2(config-pmap-c)#police 8000 conform-action transmit exceed-action drop R2(config-pmap-c-police)#exit R2(config-pmap-c)#exit R2(config-pmap)#exit R2(config)#control-plane R2(config-cp)#service-policy input pmap
R2#show policy-map control-plane

We can in R2:

```
R2#show policy-map control-plane
 Control Plane

  Service-policy input: pmap

    Class-map: cmap (match-all)
      3566142 packets, 5369177227 bytes
      5 minute offered rate 63676000 bps, drop rate 63670000 bps
      Match: access-group name test
      police:
          cir 8000 bps, bc 1500 bytes
        conformed 471 packets, 547869 bytes; actions:
          transmit
        exceeded 3565671 packets, 5368629358 bytes; actions:
          drop
        conformed 8000 bps, exceeded 63670000 bps

    Class-map: class-default (match-any)
      150 packets, 13760 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

Control Plan Policy Stop Ping Flood
R2(config)#ip access-list extended test R2(config-ext-nacl)#permit icmp any any R2(config)#class-map cmap R2(config-cmap)#match access-group name test R2(config)#policy-map pmap R2(config-pmap)#class cmap R2(config-pmap-c)#police 8000 conform-action transmit exceed-action drop R2(config-pmap-c-police)#exit R2(config-pmap-c)#log R2(config-pmap-c)#exit R2(config-pmap)#exit R2(config)#control-plane R2(config-cp)#service-policy input pmap
R2#show policy-map control-plane