

Catalyst 6500 konfigurációs ajánlások

§ Catalyst 6500

Ø Nagy teljesítményű továbbítás

Ø Hardware felépítés

- Supervisor: PFCx + MSFCy
 - Továbbiakban PFC3 feature-k
- Vezérlés és továbbítás elválasztása
- Elosztott működésre is képes
 - DFC

§ Control-Plane védelem

§ Biztonsági megoldások

§ Layer2

- Ø CDP, VTP, DTP

§ Layer3

- Ø Routing protokollok

§ Menedzsment

- Ø Telnet, SSH

§ Speciális csomagok kezelése

- Ø IP Options, fragmentáció,
ICMP, RPF eldobás, ARP,
nem-IP csomagok

§ ACL

- Ø Log, ICMP unreachable,
bizonyos PBR funkció

§ Netflow

- Ø Első csomag
- Ø WCCP, TCP intercept, NAT,
PAT, CBAC, SLB, rACL

§ CEF ~500 kpps

Ø Process switching ~20kpps

§ CPU túlterheltség

Ø Routing szomszéd elvesztés

Ø STP BPDU skewing

Ø Logging késleltetés

Ø CLI problémák

- § Virtuális interface a Data-Plane és a Control-Plane között
- § Szabályozás:
 - Ø Hardware alapú – Rate Limiter
 - Ø Software alapú – Control Plane Policing
 - Ø Egyéb
- § Egyszerű konfiguráció
- § Hatékony működés
 - Ø DOS támadás ellen

PFC / DFC: 10 speciális hardware register

§ Unicast

- Ø ACL: input, output, VACL
- Ø CEF: glean, receive
- Ø IP: error, feature, ICMP, RPF failure
- Ø Layer2: L2TP
- Ø MTU/TTL failure

§ Multicast

- Ø Connected
- Ø Partial shortcut
- Ø FIB miss

```
C6500(config)#mls rate-limit
```

```
C6500#show mls rate-limit {usage}
```

§ Új interface típus

- Ø control-plane

§ Hagyományos MQC eszközök

- Ø Class-map

- Osztályok definiálása

- Ø Policy-map

- Osztályok forgalom korlátozása

- Ø Service-policy

- Interface-hez rendelés

```
C6500(config)# control-plane
```

```
C6500(config-cp)# service-policy input <policy_map>
```


Referencia: 9 forgalmi osztály

§ BGP

Ø Transmit

§ IGP

Ø Transmit

§ Interactive Management

Ø telnet, SSH, NTP, AAA

§ File Management

Ø FTP, TFTP

§ Reporting

Ø SLA

§ Monitoring

Ø Ping, Traceroute

§ Critical Applications

Ø GRE, HSRP, PIM

§ Undesirable

Ø Drop

§ Default

§ Routing protocol packet policing

Ø BGP + IGP

Ø LDP

Ø ND

Ø ARP

§ Az átmenő forgalomra is érvényes!!!

```
mls qos protocol <prot.> {pass-through|police}
```

```
show mls qos protocol
```

§ Access Control List (ACL)

§ Unicast Reverse Path Forwarding (uRPF)

§ MAC address monitoring

Access Control List



§ TCAM erőforrás

Ø 32k ACE, 4k label

Ø 64 LOU

§ Router ACL

Ø Layer3 subnet-k között

§ VLAN ACL

Ø Layer3 subnet-k/VLAN-k között

Ø VLAN-n belül

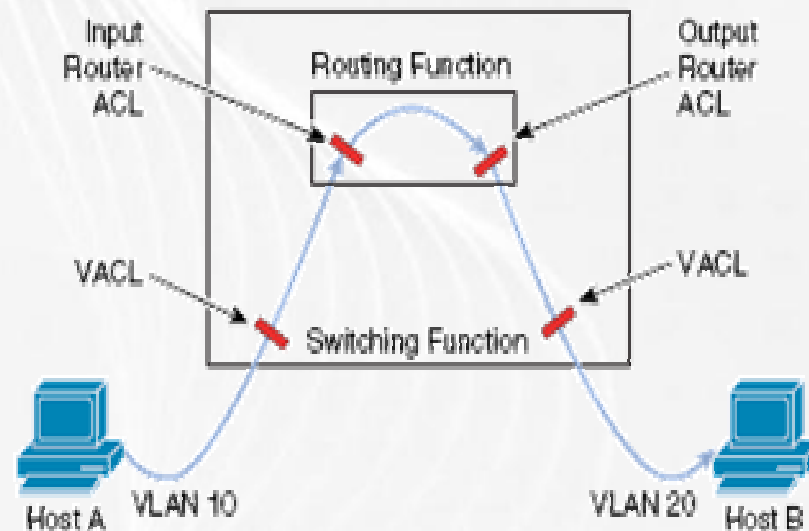
Ø Aka VLAN map

§ Port ACL

Ø CatOS

Ø IP/MAC

Ø Csak Input



```
show tcam interface <interface> acl {in | out} ip  
show tcam counts
```


§ Konfigurációs ajánlások

Ø Első rész

Ø További témakörök

- MAC address monitoring
- Traffic Storm Control
- Unicast and Multicast Flood Blocking
- Port Security
 - DHCP snooping
 - IP source guard
 - Dynamic ARP Inspection

Köszönöm a figyelmüket!