

Introduction to Policy Based Routing

Concepts – Purposes – Configuration

Today's work

- What is PBR ?
- Why would you want to use PBR ?
- Hardware forwarding and PBR
- IOS implementation
- Case #1: Simple scenario
- Case #2: Load sharing based on source
- Case #3: Load sharing based on traffic
- Case #4: Security purposes
- JunOS implementation
- Case #5: Branch office

What is PBR ?

- PBR = Policy Based Routing
- **Traditional routing** = decision based on destination network (routing table, longest match)
- **PBR** = use other criteria to route packets (e.g.: source addresses, protocols, tags...)

Why would you want to use PBR ?

- Traffic path selection based on corporate policy
- Load sharing on different network links
- **Application layer** devices in use (AV, DPI, proxies, anti-spam...)
- DDoS mitigation

Hardware forwarding and PBR

- CEF (Cisco) and PBR
 - Supported since IOS 12.0
 - No special configuration required
 - CEF has to be enabled

IOS implementation

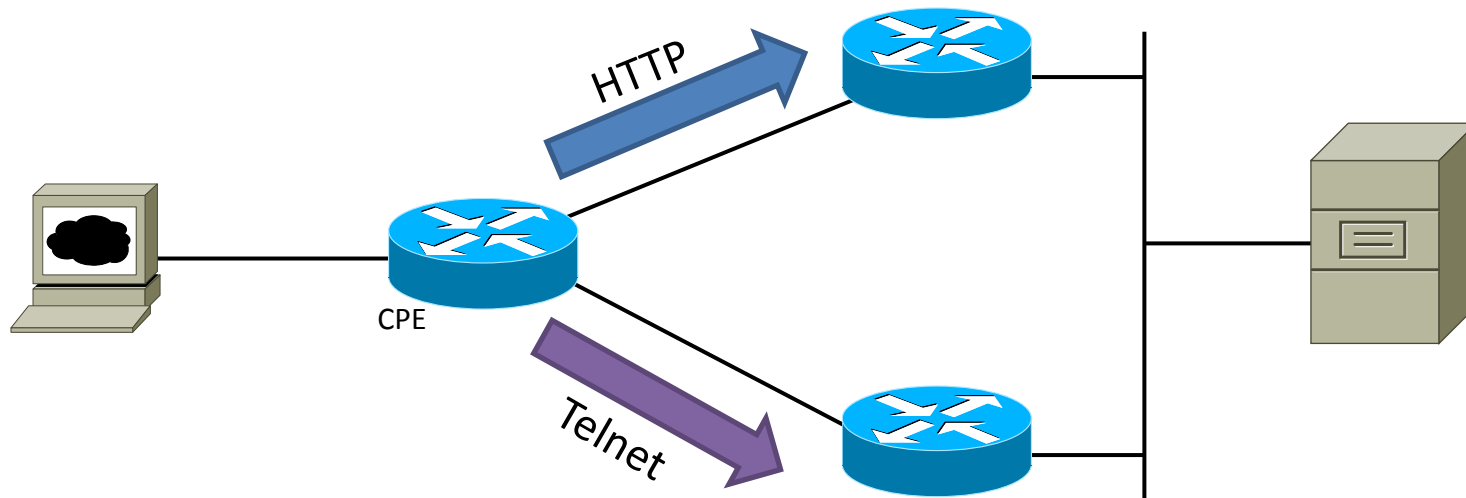
- Select your traffic with ACLs
 - ✓ `ip access-list extended HTTP-CAP`
- Define the manipulation with Route-Maps
 - ✓ `route-map POLICY permit 10`
- Apply the policy on the interfaces (in/out)
 - ✓ `int fX/X`
 - ✓ `ip policy route-map POLICY input`

IOS implementation

- Check your configuration
 - ✓ `show ip access-list`
 - ✓ `show route-map`
- Monitor packet / byte count
 - ✓ Policy routing matches: 68 packets, 4210 bytes

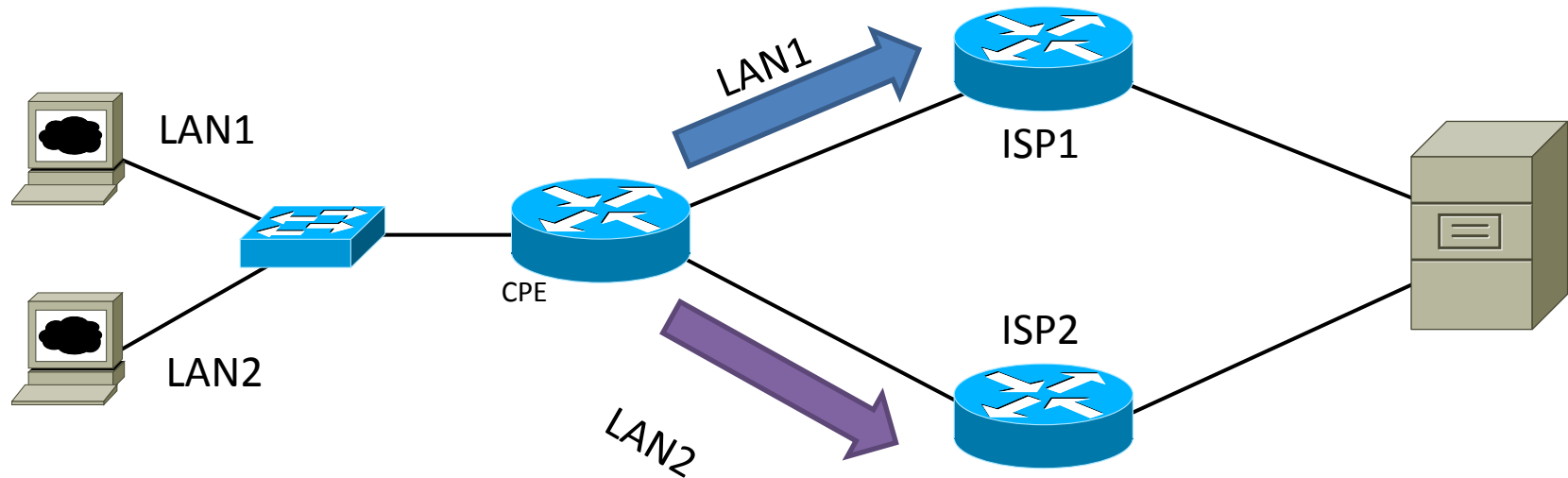
Case #1: Simple scenario

- Select different paths based on the traffic type
- Identify the traffic and change the next-hop



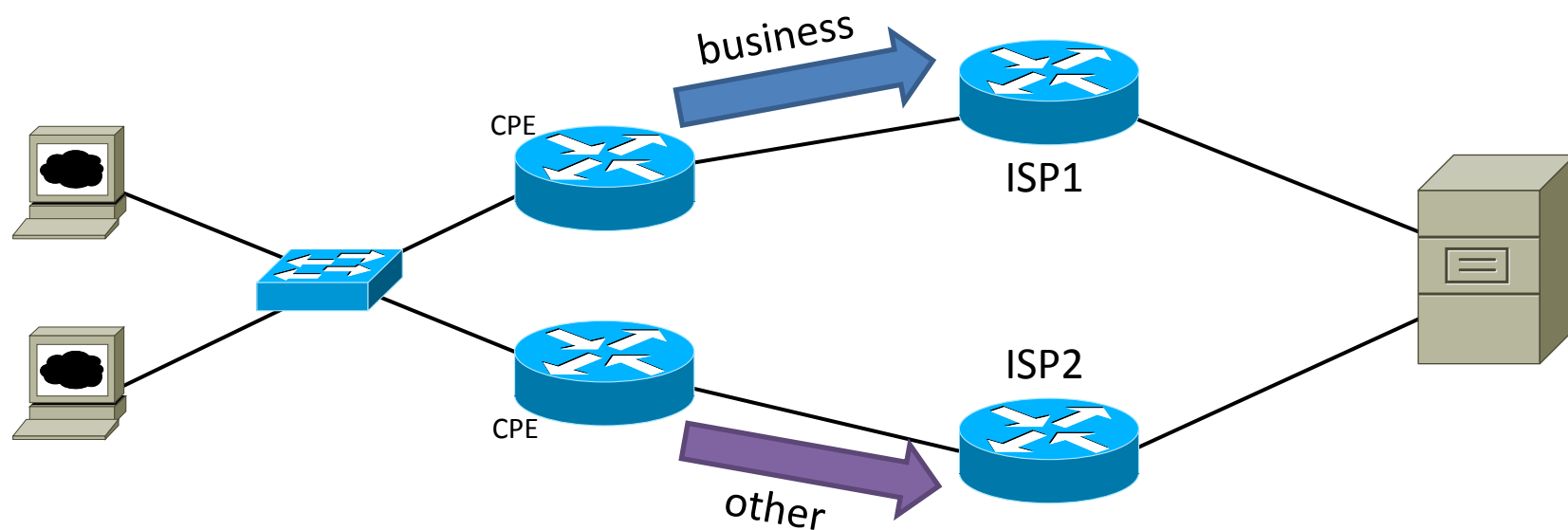
Case #2: Load sharing based on source

- Select different paths based on the source host
- Identify the source and change the next-hop



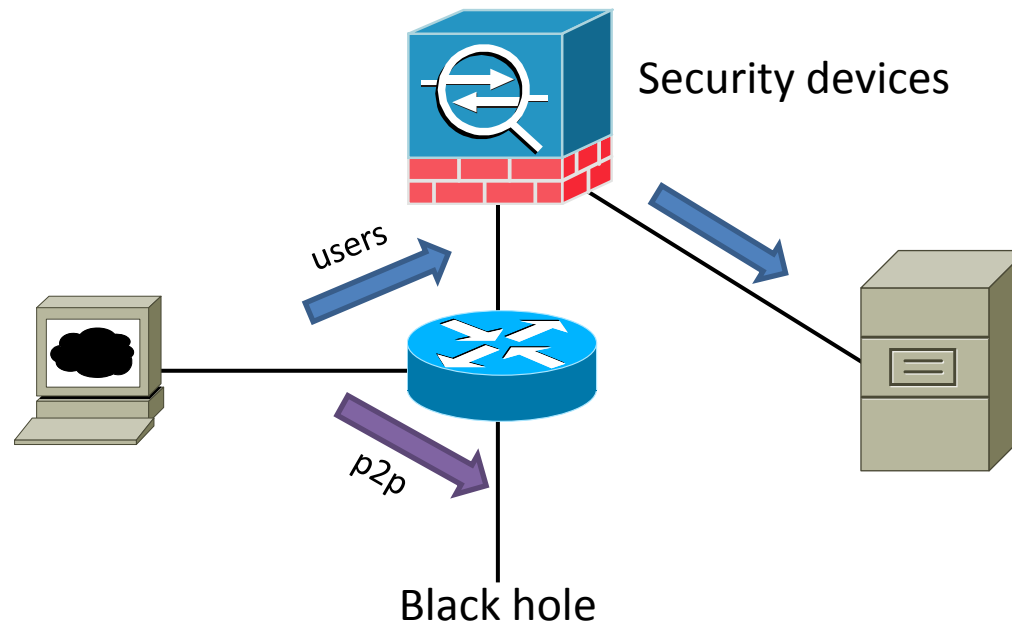
Case #3: Load sharing based on traffic

- Select different paths based on the traffic type
- Identify the traffic and change the next-hop
- Handle the redundancy using HSRP



Case #4: Security Purposes

- Identify traffic and redirect it to security devices
- Blackhole undesirable traffic using PBR
- Use NBAR to classify traffic (be careful)



Evolution

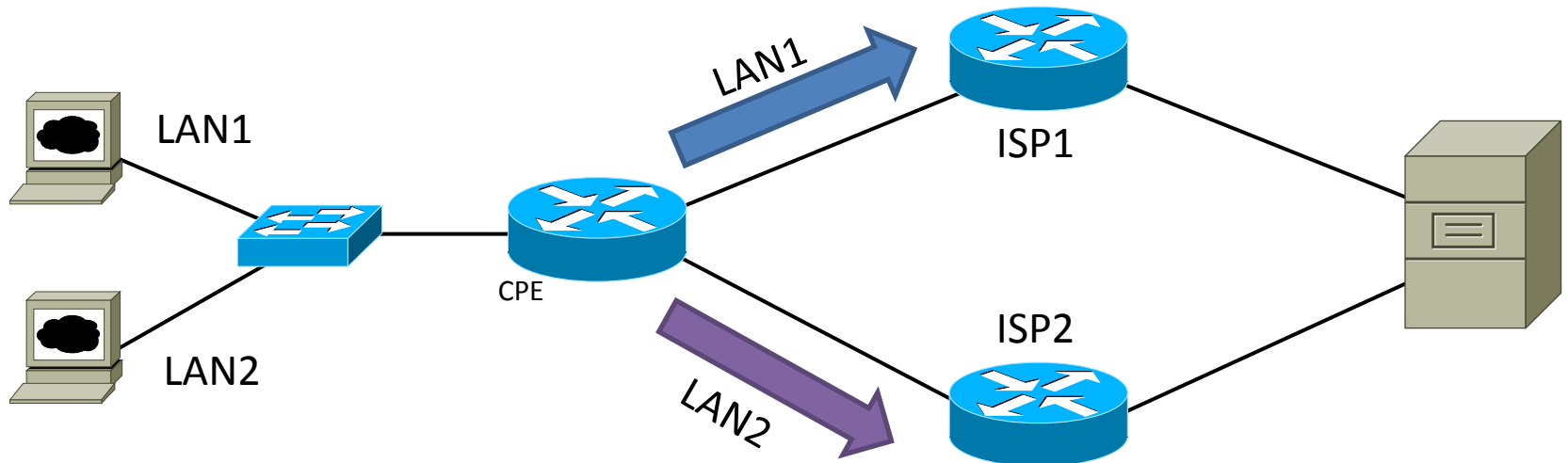
- Make PBR dynamic and adaptive
- Gather network knowledge from different sources (e.g.: netflow)
- Cisco has this technology: **PfR** (Performance Routing)
- Automatically set up PBR and perform advanced packet routing depending on network conditions

JunOS - Filter Based Forwarding Bonus

- Setup interfaces
- Define routing instances
- Merge routing information
- Setup firewall filters
- Verify your configuration

Case #5: Branch office

- PBR load-share based on source addresses (firewall filter)
- Two routing instances: 1 for ISP1 and 1 for ISP2



Questions ?



Going further

- Cisco documentation
- http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml
- http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcftp_br_ps1835_TSD_Products_Configuration_Guide_Chapter.html
- <http://www.ciscopress.com/articles/article.asp?p=1613547&seqNum=4>
- Juniper documentation
- http://www.juniper.net/techpubs/en_US/nsm2012.1/topics/concept/security-service-firewall-screens-policy-based-routing-overview.html