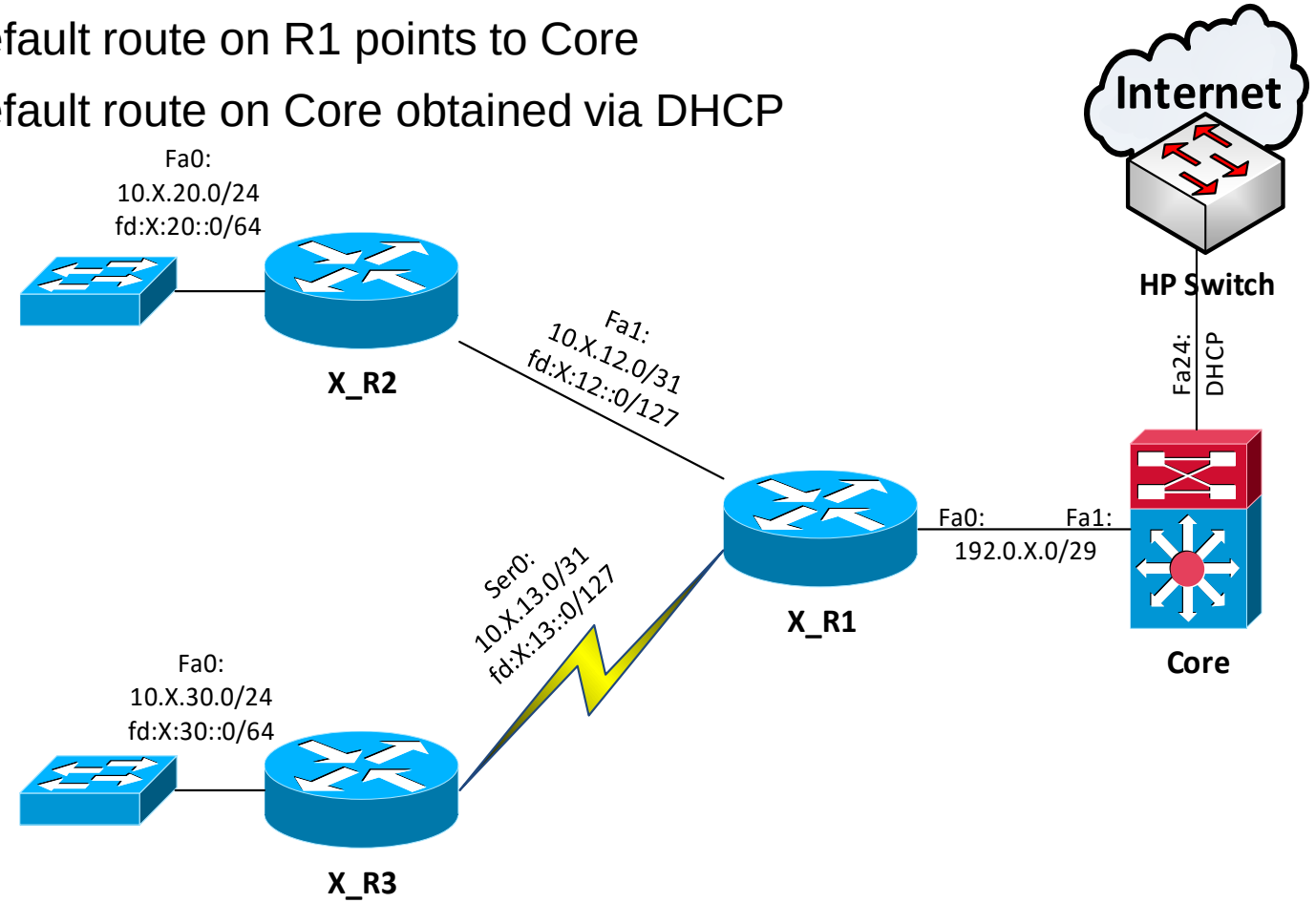
Internet Connectivity

ROUTE Module 6

Basic Topology

- Odd groups uses OSPF, even groups uses EIGRP
- Default routes
  - R1 announces def.route
  - Default route on R1 points to Core
  - Default route on Core obtained via DHCP

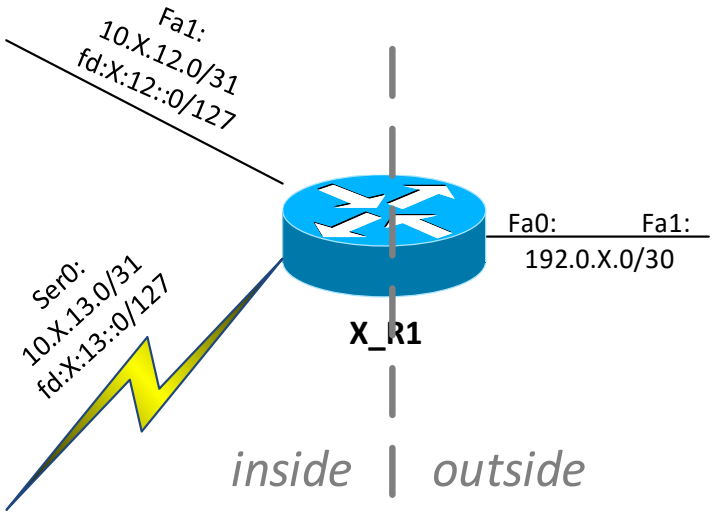


Lab 6.1: NAT

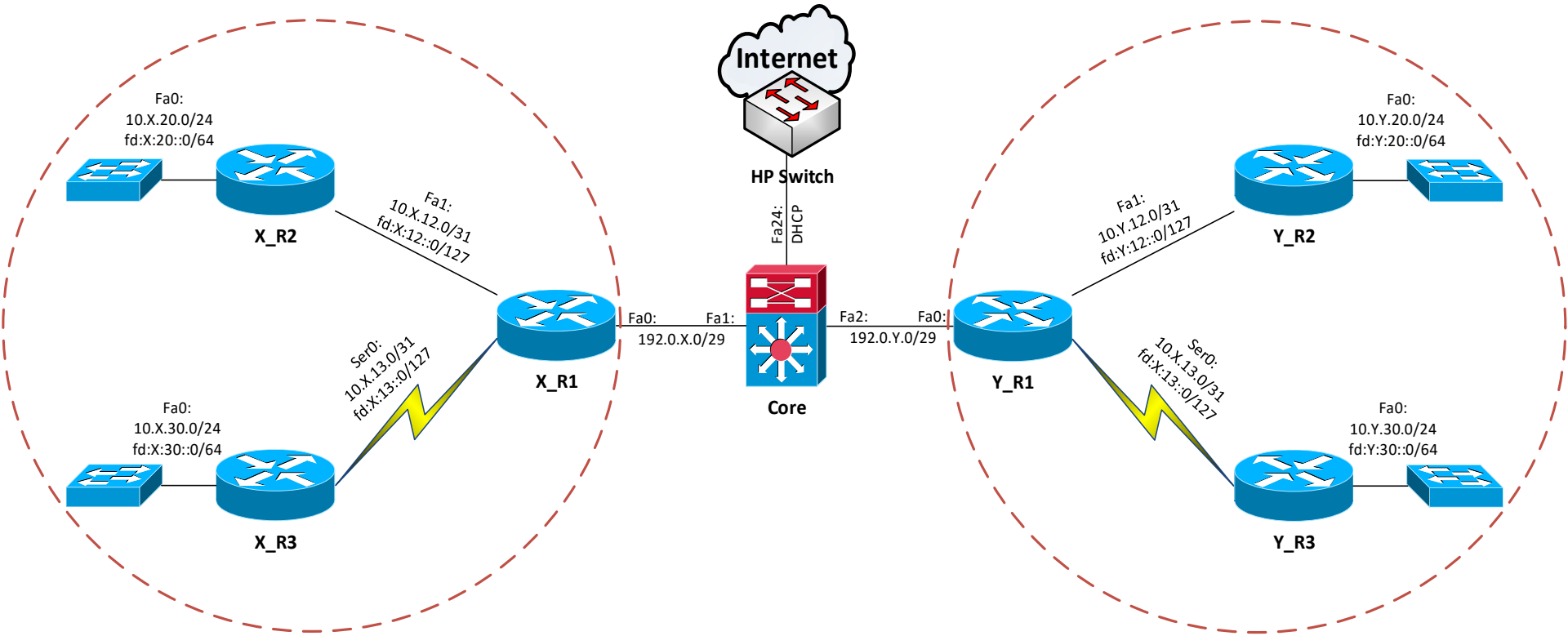
- R1:

```
interface {fa1|s0}
  ip nat inside
interface fa0
  ip nat outside
access-list 1 permit 10.0.0.0 0.255.255.255
ip nat pool NAT-POOL 192.0.X.2 192.0.X.6
ip nat inside source list 1 pool NAT-POOL overload
```

```
# show ip nat stat
# show ip nat translation
```



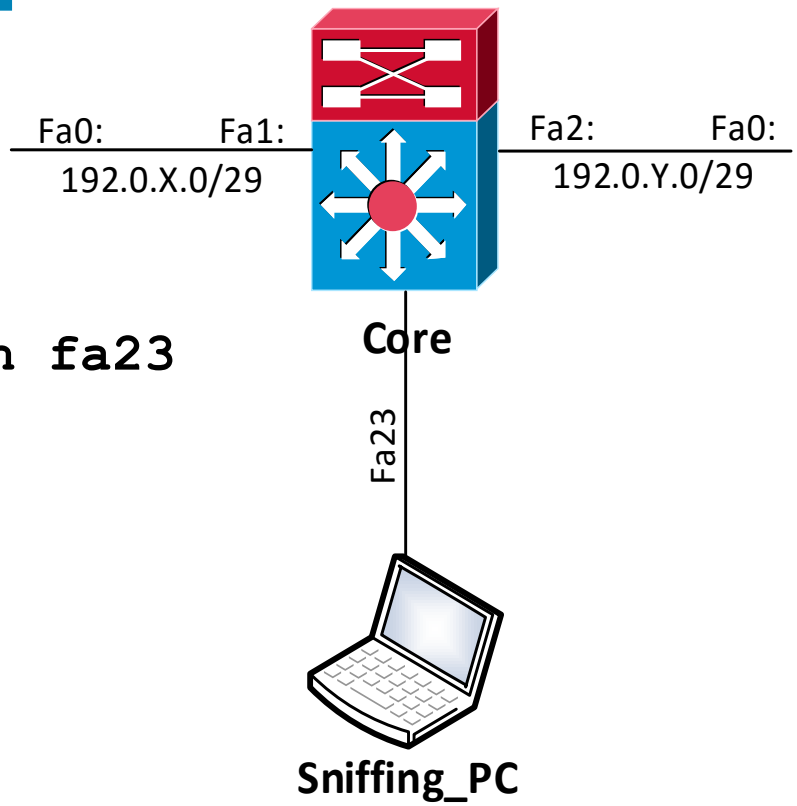
Lab 6.2: Extend Topology



Lab 6.3: Configure SPAN

- Core

```
(config)#
monitor session 1 source fa1
monitor session 1 destination fa23
   encapsulation replicate
```



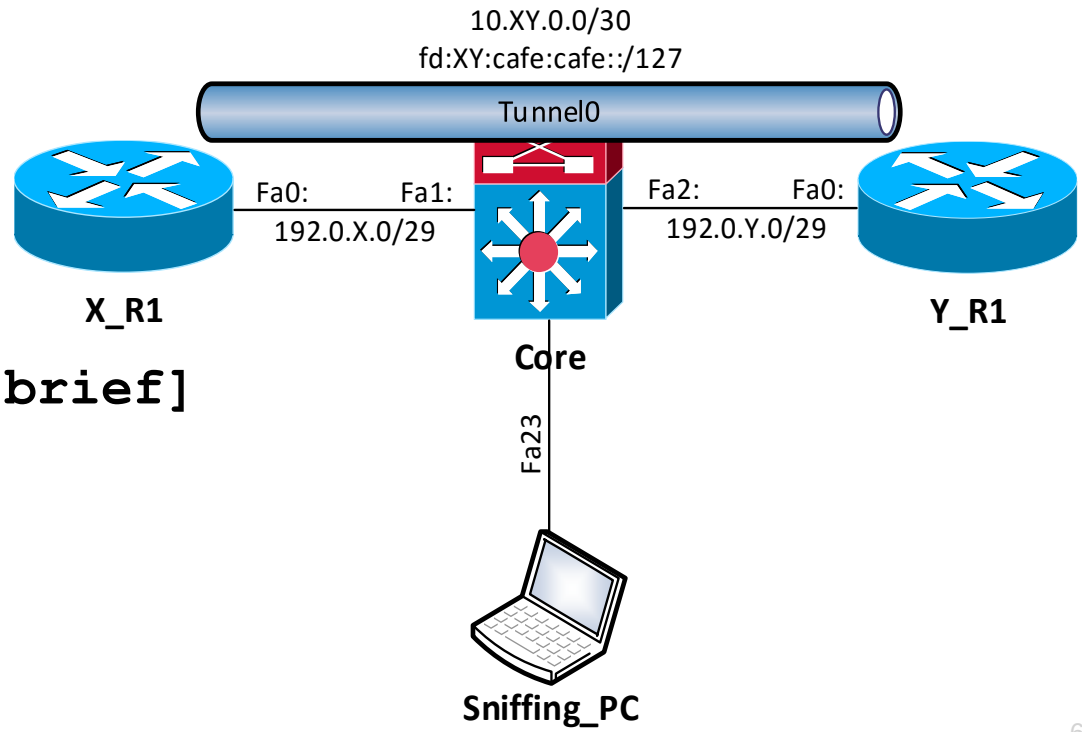
- Start Wireshark onSniffing_PC

- Ping between X_R1 and Y_R1

Lab 6.4: GRE Tunnel

- X_R1, Y_R1:

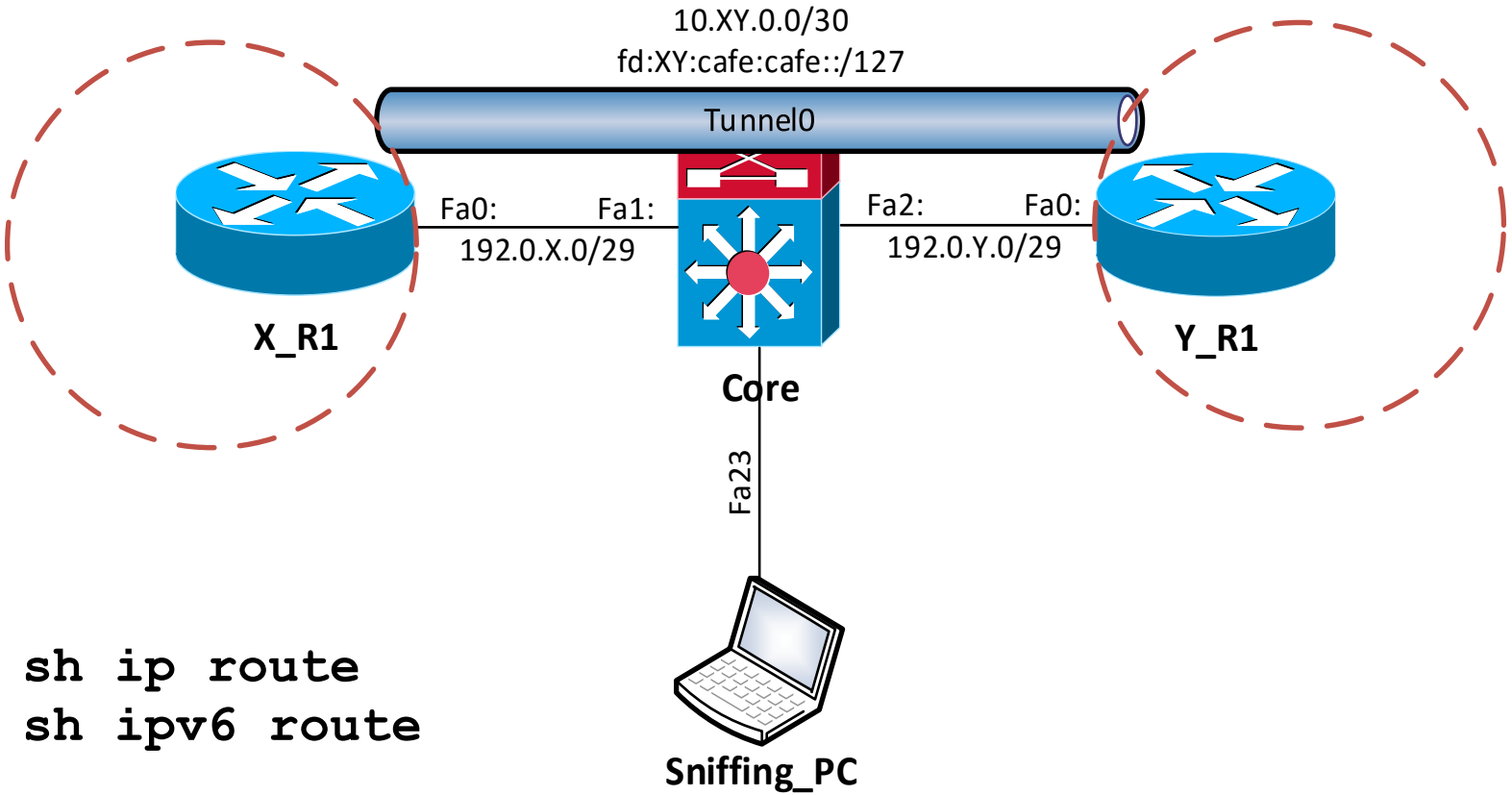
```
(config)# interface Tunnel0
 bandwidth 100000
 tunnel source fa0
 tunnel destination 192.0.{X|Y}.2
 ip address 10.XY.0.{1|2} 255.255.255.252
 ipv6 address
```




```
# sh ip ro
# sh ip interface [brief]
# ping
```

Lab 6.5: Routing through Tunnel

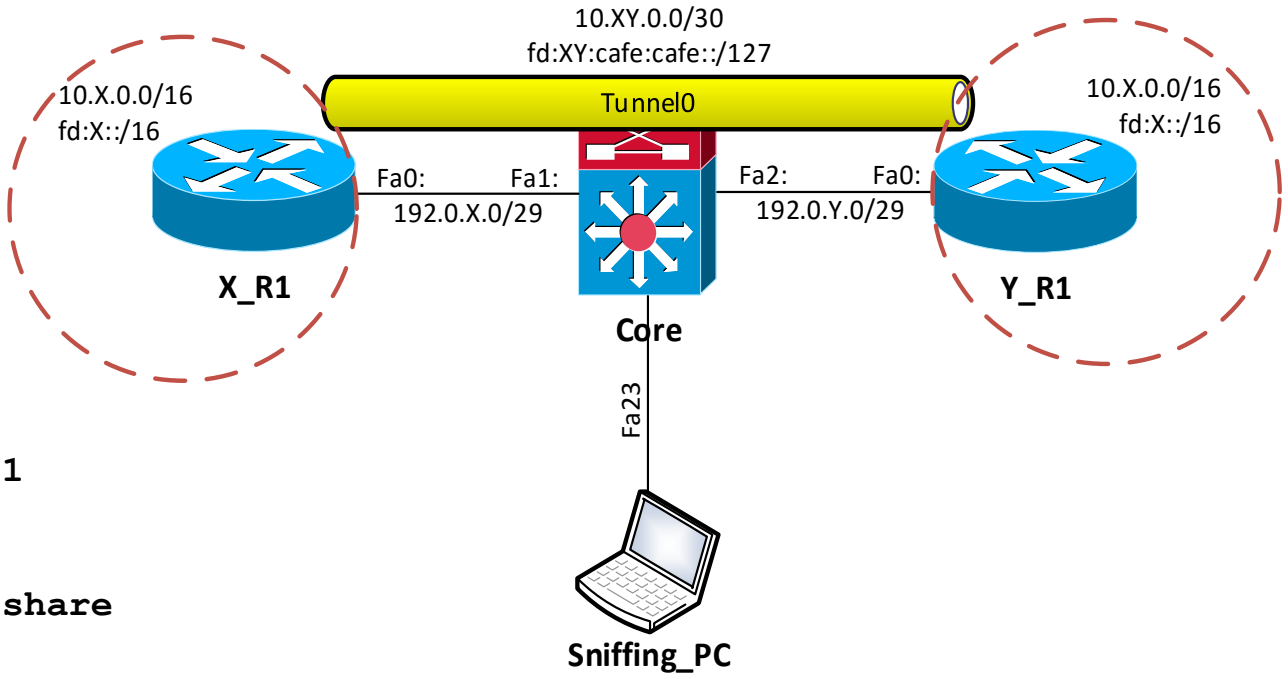
- Add tunnel interface into routing process on X_R1, Y_R1




```
# sh ip route
# sh ipv6 route
```

Lab 6.6: Site-to-Site VPN (GRE over IPsec)

- X_R1, Y_R1:




```
crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
  lifetime 3600
crypto isakmp key 0 cisco address 192.0.{X|Y}.2
crypto ipsec transform-set ESP-AES-SHA esp-aes 256 esp-sha-hmac
crypto ipsec profile KRYPTUJ
  set transform-set ESP-AES-SHA
interface Tunnel0
  tunnel protection ipsec profile KRYPTUJ
```

- Observe Wireshark in Sniffing_PC

Labs created by Vladimír Veselý for C1P practice.

Last updated: 2016-03-21