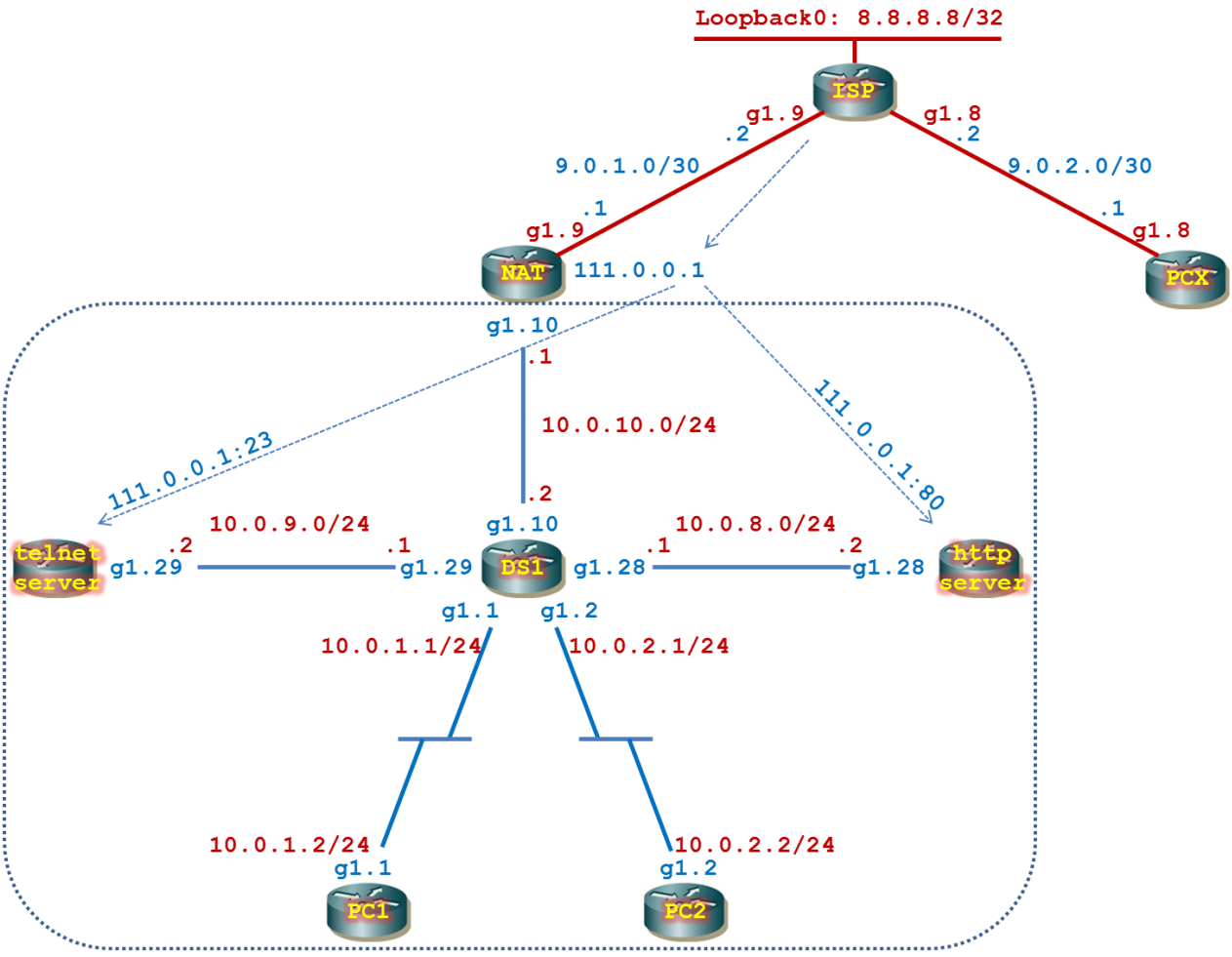
Virtual LAB - NAT, ACL

(CCNA Routing & Switching)



PHẦN 1 – YÊU CẦU CƠ BẢN

- **Xóa cấu hình, khởi động lại tất cả thiết bị với cấu hình trắng**
- **Thiết lập sơ đồ như hình minh họa**
- **Đặt hostname, gán địa chỉ IP tương ứng cho các thiết bị**
- **Cấu hình telnet không password trên tất cả các thiết bị**
- **Cấu hình câu lệnh chống trôi dòng lệnh "logging synchronous"**
  R(config)# line console 0
  R(config-line)# logging synchronous
- **Cấu hình câu lệnh bỏ qua cơ chế phân giải tên miền**
  R(config)# no ip domain-lookup

PHẦN 2 – YÊU CẦU CHÍNH

1. PAT

- **Cấu hình PAT tại router NAT cho phép các mạng 10.0.1.0/24 & 10.0.2.0/24 có thể ping được Internet 8.8.8.8.**

2. NAT

- **Tại router ISP cấp địa chỉ 111.0.0.1 xuống cho router NAT bằng câu lệnh "ip route 111.0.0.1 255.255.255.255 9.0.1.1".**
- **Cấu hình Static NAT Port tại router NAT chuyển hướng lưu lượng telnet từ 111.0.0.1 cho telnet server 10.0.9.2.**
- **Tại PCX thực hiện câu lệnh "telnet 111.0.0.1 23" để kiểm tra kết nối telnet tới telnet server 10.0.9.2:23.**
- **Cấu hình Static NAT Port tại router NAT chuyển hướng lưu lượng http từ 111.0.0.1 cho http server 10.0.8.2.**
- **Tại PCX thực hiện câu lệnh "telnet 111.0.0.1 80" để kiểm tra kết nối http tới world wide web 111.0.0.1:80.**

3. ACL

- **(1) Cấu hình ACL tại DS1 sao cho các PC nội bộ không thể giao tiếp được với nhau nhưng vẫn có thể truy cập được tới các server (telnet server, http server), truy cập được Internet (ping được tới 8.8.8.8).**
- **(2) Cấu hình ACL tại DS1 sao cho telnet server 10.0.9.2 không thể giao tiếp được tới http server 10.0.8.2 nhưng vẫn cho phép tất cả các thiết bị còn lại có thể giao tiếp với 2 hệ thống server này.**
- **(3) Cấu hình ACL tại DS1 và router NAT sao cho chỉ cho phép các PC có địa chỉ ip 10.0.1.2 & 10.0.2.2 mới có thể telnet vào 2 thiết bị này. PC1 thay đổi địa chỉ thành 10.0.1.3 xem có còn telnet hoặc http tới các server được nữa hay không. PC2 thay đổi địa chỉ thành 10.0.2.3 xem có còn telnet hoặc http tới các server được nữa hay không.**
- **(4) Cấu hình ACL tại router NAT và áp dụng theo chiều đi vào cổng g1.10 không cho phép các PC nội bộ ping tới 9.0.2.1; vẫn có thể ping được tới các thiết bị còn lại.**
- **(5) Cấu hình ACL tại router NAT và áp dụng theo chiều đi vào cổng g1.9 sao cho PCX chỉ có thể http vào http server 10.0.8.2; PCX không thể telnet tới telnet server 10.0.9.2.**
- **(6) Cấu hình ACL tại DS1 sao cho chỉ cho phép lưu lượng telnet tới tới telnet server 10.0.9.2. PC1 vs PC2 và các thiết bị còn lại không thể ping được tới telnet server. Các PC vẫn có thể telnet được tới telnet server 10.0.9.2.**
- **(7) Cấu hình ACL tại DS1 sao cho chỉ cho phép lưu lượng http tới tới http server 10.0.8.2. PC1 vs PC2 và các thiết bị còn lại không thể ping hoặc telnet được tới http server. Các PC vẫn có thể http được tới http server 10.0.8.2.**

PHẦN 3 – GỢI Ý CẤU HÌNH

! Cấu hình trên router DS1

```
hostname DS1
interface g1
  no shutdown
```

```
 exit
interface g1.1
 encapsulation dot1q 1 native
 ip address 10.0.1.1 255.255.255.0
 no shutdown
 exit
interface g1.2
 encapsulation dot1q 2
 ip address 10.0.2.1 255.255.255.0
 no shutdown
 exit
interface g1.8
 encapsulation dot1q 8
 ip address 10.0.8.1 255.255.255.0
 no shutdown
 exit
interface g1.9
 encapsulation dot1q 9
 ip address 10.0.9.1 255.255.255.0
 no shutdown
 exit
interface g1.10
 encapsulation dot1q 10
 ip address 10.0.10.2 255.255.255.0
 no shutdown
 exit
ip route 0.0.0.0 0.0.0.0 10.0.10.1
no ip domain-lookup
line vty 0 4
 privilege level 15
 no login
 exit
line console 0
 logging synchronous
 exit


! Cấu hình trên router telnet server
hostname telnet_server
interface g1
 no shutdown
 exit
interface g1.29
 encapsulation dot1q 29
 ip address 10.0.9.2 255.255.255.0
 no shutdown
 exit
ip route 0.0.0.0 0.0.0.0 10.0.9.1
no ip domain-lookup
line vty 0 4
 privilege level 15
 no login
```

```
 exit
line console 0
 logging synchronous
 exit


! Cấu hình trên router http server
hostname http_server
interface g1
 no shutdown
 exit
interface g1.28
 encapsulation dot1q 28
 ip address 10.0.8.2 255.255.255.0
 no shutdown
 exit
ip route 0.0.0.0 0.0.0.0 10.0.8.1
ip http server
ip http authentication local
username cisco privilege 15 password cisco
no ip domain-lookup
line vty 0 4
 privilege level 15
 no login
 exit
line console 0
 logging synchronous
 exit


! Cấu hình trên router PC1
hostname PC1
interface g1
 no shutdown
 exit
interface g1.1
 encapsulation dot1q 1 native
 ip address 10.0.1.2 255.255.255.0
 no shutdown
 exit
ip route 0.0.0.0 0.0.0.0 10.0.1.1
no ip domain-lookup
line vty 0 4
 privilege level 15
 no login
 exit
line console 0
 logging synchronous
 exit


! Cấu hình trên router PC2
```

```
hostname PC2
interface g1
 no shutdown
 exit
interface g1.2
 encapsulation dot1q 2
 ip address 10.0.2.2 255.255.255.0
 no shutdown
 exit
ip route 0.0.0.0 0.0.0.0 10.0.2.1
no ip domain-lookup
line vty 0 4
 privilege level 15
 no login
 exit
line console 0
 logging synchronous
 exit


! Cấu hình trên router PCX
hostname PCX
interface g1
 no shutdown
 exit
interface g1.8
 encapsulation dot1q 8
 ip address 9.0.2.1 255.255.255.252
 no shut
 exit
ip route 0.0.0.0 0.0.0.0 9.0.2.2
no ip domain-lookup
line vty 0 4
 privilege level 15
 no login
 exit
line console 0
 logging synchronous
 exit


! Cấu hình cơ bản & PAT trên router NAT
hostname NAT
interface g1
 no shutdown
 exit
interface g1.9
 encapsulation dot1q 9
 ip address 9.0.1.1 255.255.255.252
 ip nat outside
 no shutdown
 exit
```

```
interface g1.10
  encapsulation dot1q 10
  ip address 10.0.10.1 255.255.255.0
  ip nat inside
  no shut
  exit
ip route 0.0.0.0 0.0.0.0 9.0.1.2
ip route 10.0.1.0 255.255.255.0 10.0.10.2
ip route 10.0.2.0 255.255.255.0 10.0.10.2
ip route 10.0.8.0 255.255.255.0 10.0.10.2
ip route 10.0.9.0 255.255.255.0 10.0.10.2
ip nat inside source list 1 interface g1.9 overload
access-list 1 permit 10.0.1.0 0.0.0.255
access-list 1 permit 10.0.2.0 0.0.0.255
access-list 1 permit 10.0.8.0 0.0.0.255
access-list 1 permit 10.0.9.0 0.0.0.255
access-list 1 permit 10.0.10.0 0.0.0.255
no ip domain-lookup
line vty 0 4
  privilege level 15
  no login
  exit
line console 0
  logging synchronous
  exit


ip nat inside source static tcp 10.0.9.2 23 111.0.0.1 23
ip nat inside source static tcp 10.0.8.2 80 111.0.0.1 80


! Cấu hình trên router ISP
hostname ISP
interface g1
  no shutdown
  exit
interface g1.9
  encapsulation dot1q 9
  ip address 9.0.1.2 255.255.255.252
  no shut
  exit
interface g1.8
  encapsulation dot1q 8
  ip address 9.0.2.2 255.255.255.252
  no shut
  exit
interface loopback 0
  ip address 8.8.8.8 255.255.255.255
  no shut
  exit
ip dhcp pool WAN1
  network 9.0.1.0 255.255.255.252
```

```
 default-router 9.0.1.2
 dns-server 8.8.8.8
 exit
ip dhcp pool WAN2
 network 9.0.2.0 255.255.255.252
 default-router 9.0.2.2
 dns-server 8.8.8.8
 exit
ip dhcp excluded-address 9.0.1.2
ip dhcp excluded-address 9.0.2.2
ip route 111.0.0.1 255.255.255.255 9.0.1.1


ip http server
ip http authentication local
username cisco privilege 15 password cisco
no ip domain-lookup
line vty 0 4
 privilege level 15
 no login
 exit
line console 0
 logging synchronous
 exit
```