13. VPN

ICT폴리텍대학

강 상 희

13. VPN

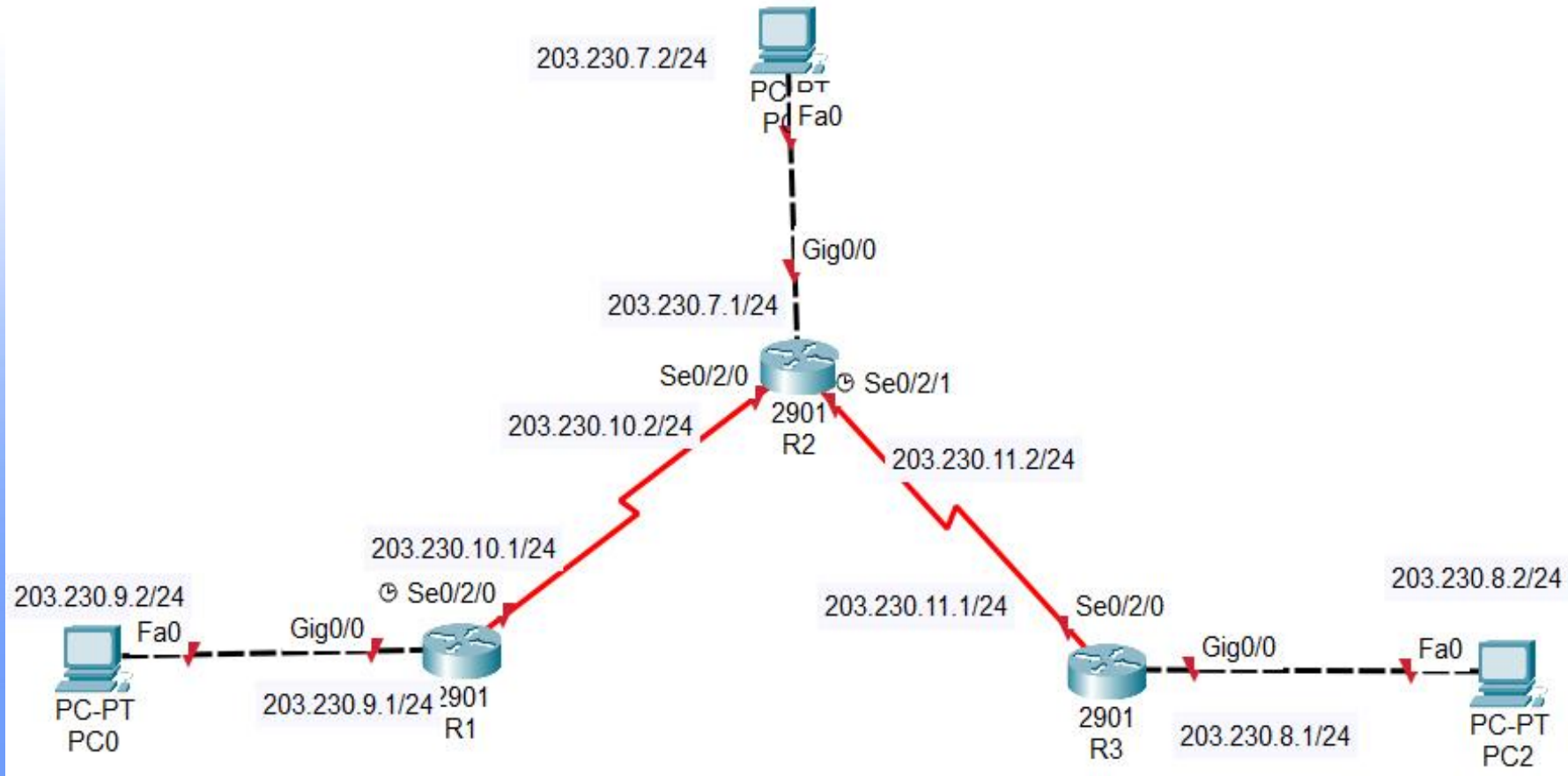
목 차

- GRE(Generic Routing Encapsulation) 터널링
- 터널링을 통한 트래픽 분산과 제어
- GRE 터널링 이용한 IPSec VPN
- VPN 정보 확인하기

13. VPN

- 공중망에 터널링 기술 이용하여 사설망(전용망) 처럼 이용
- **IPSec** 기술 이용
- **VPN 종류 : IPSec 기반, SSL 기반, MPLS VPN**
- **VPN 암호 알고리즘 : DES, 3DES, AES, RSA(비대칭)**
- 키 길이 : 길면 암호 해독 어렵고 전송 늦음

13. VPN


203.230.7.2/24
Fa0
Gig0/0
203.230.7.1/24
Se0/2/0
Se0/2/1
2901
R2
203.230.10.2/24
203.230.11.2/24
203.230.10.1/24
Se0/2/0
203.230.9.2/24
Fa0
Gig0/0
PC-PT
PC0
203.230.9.1/24
2901
R1
203.230.11.1/24
Se0/2/0
203.230.8.2/24
Gig0/0
Fa0
2901
R3
203.230.8.1/24
PC-PT
PC2

13. VPN

R1 설정 스크립트

1. **Router#conf t**
2. **Router(config)#hostname R1**
3. **R1(config)#int g0/0**
4. **R1(config-if)#ip add 203.230.9.1 255.255.255.0**
5. **R1(config-if)#no shut**
6. **R1(config)#int S0/2/0**
7. **R1(config-if)#ip add 203.230.10.1 255.255.255.0**
8. **R1(config-if)#clock rate 64000**
9. **R1(config-if)#no shut**
10. **R1(config-if)#exit**
11. **R1(config)#router ospf 7**
12. **R1(config-router)#network 203.230.9.1 0.0.0.0 area 0**
13. **R1(config-router)#network 203.230.10.1 0.0.0.0 area 0**
14. **R1(config-router)#do show ip int brief**
15. **R1(config-router)#do show ip route**

13. VPN

R2 설정 스크립트

```
1.  Router#conf t
2.  Router(config)#hostname R2
3.  R2(config)#int g0/0
4.  R2(config-if)#ip add 203.230.7.1 255.255.255.0
5.  R2(config-if)#no shut
6.  R2(config-if)#int S0/2/0
7.  R2(config-if)#ip add 203.230.10.2 255.255.255.0
8.  R2(config-if)#no shut
9.  R2(config-if)#int S0/2/1
10. R2(config-if)#ip add 203.230.11.2 255.255.255.0
11. R2(config-if)#clock rate 64000
12. R2(config-if)#no shut
13. R2(config-if)#exit
14. R2(config)#router ospf  7
15. R2(config-router)#network 203.230.7.1 0.0.0.0 area 0
16. R2(config-router)#network 203.230.10.2 0.0.0.0 area 0
17. R2(config-router)#network 203.230.11.2 0.0.0.0 area 0
18. R2(config-router)#do show ip int brief
19. R2(config-router)#do show ip route
```

13. VPN

R3 설정 스크립트

1. Router#conf t
2. Router(config)#hostname R3
3. R3(config)#int g0/0
4. R3(config-if)#ip add 203.230.8.1 255.255.255.0
5. R3(config-if)#no shut
6. R3(config-if)#int S0/2/0
7. R3(config-if)#ip add 203.230.11.1 255.255.255.0
8. R3(config-if)#no shut
9. R3(config)#router ospf 7
10. R3(config-router)#network 203.230.8.1 0.0.0.0 area 0
11. R3(config-router)#network 203.230.11.1 0.0.0.0 area 0
12. R3(config-router)#do show ip int brief
13. R3(config-router)#do show ip route

GRE(Generic Routing Encapsulation) 터널링

R1 터널 설정 스크립트

- **조건 : 터널링 네트워크 주소(163.180.116.1/24), R1(loopback 인터페이스 1번 생성,1.1.1.1/24), R3(loopback 인터페이스 1번 생성, 3.3.3.1/24), R1과 R3간 라우팅은 RIPv2 사용**

1. **R1(config)#int tunnel 13 /*터널 인터페이스 생성 */**
2. **R1(config-if)#ip add 163.180.116.1 255.255.255.0 /*터널 인터페이스 IP주소 */**
3. **R1(config-if)#tunnel source s0/2/0 /* 실제 패킷 전송될 물리적 인터페이스 설정 */**
4. **R1(config-if)#tunnel destination 203.230.11.1 /*터널이 도착할 주소 설정*/**
5. **R1(config-if)#no shut**
6. **R1(config-if)#int loopback 1**
7. **R1(config-if)#ip add 1.1.1.1 255.255.255.0**
8. **R1(config)#router rip /*터널주소와 주고받을 네트워크 선언**
9. **R1(config-router)#version 2**
10. **R1(config-router)#no auto-summary**
11. **R1(config-router)#network 1.0.0.0 /* 또는 1.1.1.1 */**
12. **R1(config-router)#network 163.180.0.0 /* 또는 163.180.116.1 */**
13. **R1(config-router)#do show ip route**

GRE(Generic Routing Encapsulation) 터널링

R3 터널 설정 스크립트

- **조건 : 터널링 네트워크 주소(163.180.116.2/24), R1(loopback 인터페이스 1번 생성,1.1.1.1/24), R3(loopback 인터페이스 1번 생성, 3.3.3.1/24), R1과 R3간 라우팅은 RIPv2 사용**

```
1.  R3(config)#int tunnel 13 /*터널 인터페이스 생성 */
2.  R3config-if)#ip add 163.180.116.2 255.255.255.0
3.  R3(config-if)#tunnel source s0/2/0
4.  R3(config-if)#tunnel destination 203.230.10.1
5.  R3(config-if)#no shut
6.  R3(config-if)#int lo 1
7.  R3(config-if)#ip add 3.3.3.1 255.255.255.0
8.  R3(config)#router rip
9.  R3(config-router)#version 2
10. R3(config-router)#no auto-summary
11. R3(config-router)#network 3.0.0.0              /* 또는 3.3.3.1 */
12. R3(config-router)#network 163.180.0.0          /* 또는 163.180.116.2 */
13. R3(config-router)#do show ip route
14. R3(config-router)#do show ip route  rip
```

GRE(Generic Routing Encapsulation) 터널링

1. **R1#show ip route rip**
2. **R1#show ip route ospf**
3. **R3#show ip route rip**

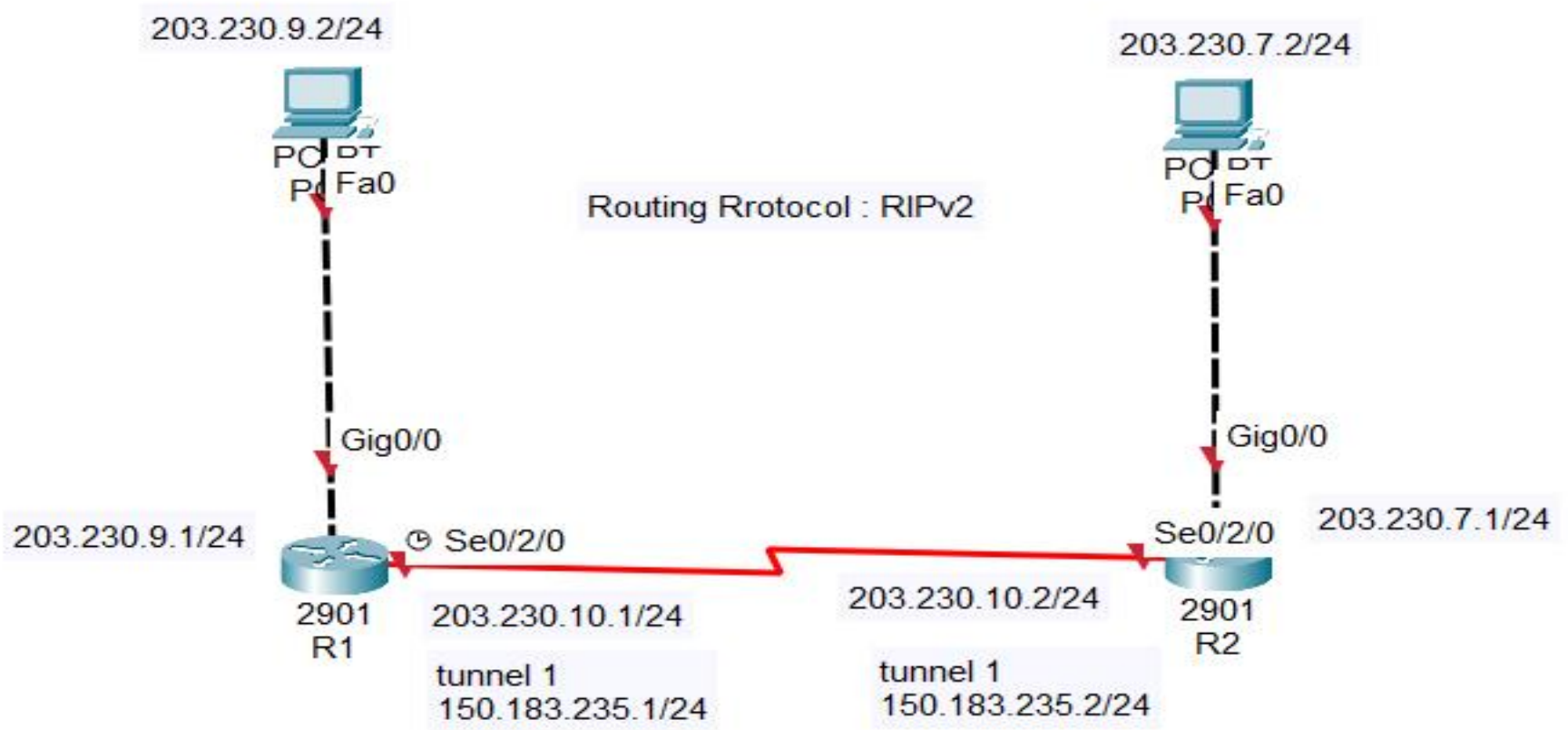
/* 물리적 인터페이스가 아닌 가상인터페이스 터널 사용

- 즉, **OSPF**는 물리적 인터페이스 사용하고 **RIP**는 논리적 인터페이스인 터널을 통해 주고 받음

1. **R1#traceroute 3.3.3.1 /*** 논리적 인터페이스 터널 ***/**
2. **R1#traceroute 203.230.8.2 /*물리적 인터페이스 경로 이용 */**

터널링을 통한 트래픽 분산과 제어

- **PC1 -> PC2로 Ping** 전송할 때 논리적 인터페이스 터널 사용하고 그 외는 물리적 인터페이스을 이용



터널링을 통한 트래픽 분산과 제어

R1 설정 스크립트

1. **Router#conf t**
2. **Router(config)#hostname R1**
3. **R1(config)#int g0/0**
4. **R1(config-if)#ip add 203.230.9.1 255.255.255.0**
5. **R1(config-if)#no shut**
6. **R1(config)#int S0/2/0**
7. **R1(config-if)#ip add 203.230.10.1 255.255.255.0**
8. **R1(config-if)#clock rate 64000**
9. **R1(config-if)#no shut**
10. **R1(config)#router rip**
11. **R1(config-router)#version 2**
12. **R1(config-router)#network 203.230.9.0**
13. **R1(config-router)#network 203.230.10.0**
14. **R1(config-router)#no auto-summary**
15. **R1(config-router)#exit**

터널링을 통한 트래픽 분산과 제어

R2 설정 스크립트

1. **Router#conf t**
2. **Router(config)#hostname R2**
3. **R2(config)#int g0/0**
4. **R2(config-if)#ip add 203.230.7.1 255.255.255.0**
5. **R2(config-if)#no shut**
6. **R2(config)#int S0/2/0**
7. **R2(config-if)#ip add 203.230.10.2 255.255.255.0**
8. **R2(config-if)#no shut**
9. **R2(config)#router rip**
10. **R2(config-router)#version 2**
11. **R2(config-router)#network 203.230.7.0**
12. **R2(config-router)#network 203.230.10.0**
13. **R2(config-router)#no auto-summary**
14. **R2(config-router)#exit**

터널링을 통한 트래픽 분산과 제어

R1 Tunnel 설정 스크립트

1. **R1(config)#int tunnel 1**
2. **R1(config-if)#ip add 150.183.235.1 255.255.255.0**
3. **R1(config-if)#tunnel source s0/2/0**
4. **R1(config-if)#tunnel destination 203.230.10.2**
5. **R1(config-if)#no shut**
6. **R1(config)#ip route 203.230.7.0 255.255.255.0 150.183.235.2**

터널링을 통한 트래픽 분산과 제어

R2 Tunnel 설정 스크립트

1. **R2(config)#int tunnel 1**
2. **R2(config-if)#ip add 150.183.235.2 255.255.255.0**
3. **R2(config-if)#tunnel source s0/2/0**
4. **R2(config-if)#tunnel destination 203.230.10.1**
5. **R2(config-if)#no shut**
6. **R2(config)#ip route 203.230.9.0 255.255.255.0 150.183.235.1**

터널링을 통한 트래픽 분산과 제어

PC0에서 PC1으로 tracert 명령어 전송

150.183.235.2의 경로를 거침 확인
(논리적인 인터페이스 사용)

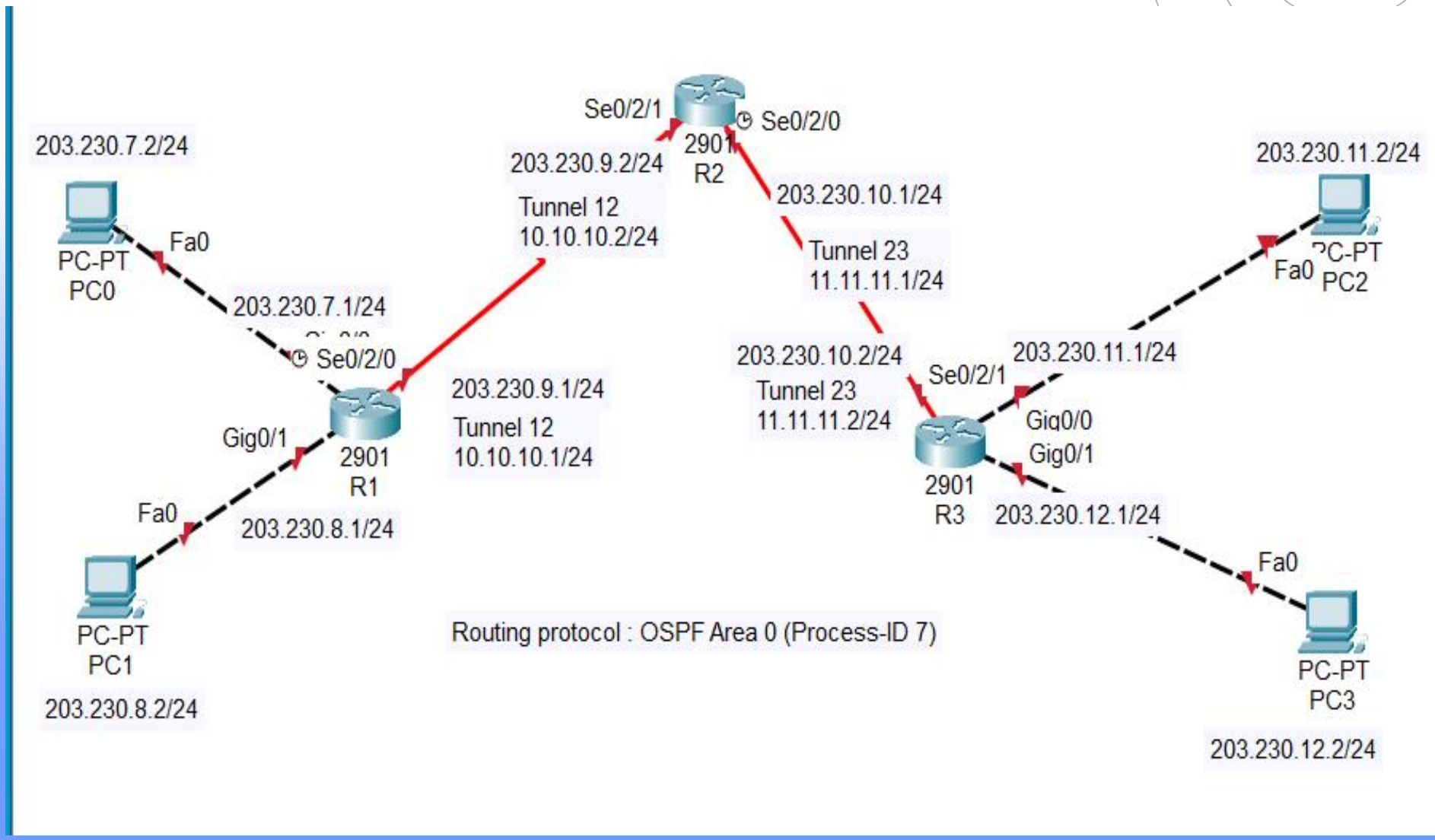
GRE 터널링 이용한 IPSec VPN

- **GRE터널링에는 데이터 자체 보안성 없음**
- **IPsec VPN을 GRE와 함께 사용하여 보안성 강화**

- **ISAKMP 정책(통신 당사자끼리 암호키 교환 위한 통신규약)**
  Authentication : pre-share
  Encryption : Advanced Encryption Standard 256 bit key
  Hash : sha
  Lifetime : 36000초

- **IPSec 정책**
  대상 트래픽 : 각 라우터의 시리얼 인터페이스를 통해 나가는 모든 트래픽
  Encapsulation : esp-3des
  Encryption : esp-aes 256 bit keys
  hash : esp-md5-hmac

GRE 터널링 이용한 IPSec VPN



GRE 터널링 이용한 IPSec VPN

R1 설정 스크립트

```
1.  Router#conf t
2.  Router(config)#hostname R1
3.  R1(config)#int g0/0
4.  R1(config-if)#ip add 203.230.7.1 255.255.255.0
5.  R1(config-if)#no shut
6.  R1(config)#int g0/1
7.  R1(config-if)#ip add 203.230.8.1 255.255.255.0
8.  R1(config-if)#no shut
9.  R1(config)#int S0/2/0
10. R1(config-if)#ip add 203.230.9.1 255.255.255.0
11. R1(config-if)#clock rate 64000
12. R1(config-if)#no shut
13. R1(config)#int tunnel 12                    /* 트래픽 터널 설정 */
14. R1(config-if)#ip add 10.10.10.1 255.255.255.0
15. R1(config-if)#tunnel source s0/2/0
16. R1(config-if)#tunnel destination 203.230.9.2
17. R1(config-if)#no shut
18. R1(config-if)#exit
19. R1(config)#license boot module c2900 technology-package securityk9
20. ------------------
21. ACCEPT?[yes/no] : yes
22. R1(config)#do write
23. R1(config)#exit
24. R1#reload                       /* 재부팅 */
```

GRE 터널링 이용한 IPSec VPN

R1 설정 스크립트

```
1.  R1(config)#crypto isakmp policy 10          /* ISAKMP에서 사용할 정책 선언 */
2.  R1(config-isakmp)#encryption aes 256
3.  R1(config-isakmp)#authentication pre-share
4.  R1(config-isakmp)#lifetime 36000
5.  R1(config-isakmp)#hash sha
6.  R1(config-isakmp)#exit
7.  R1(config)#crypto ipsec transform-set strong esp-3des esp-md5-hmac  /*IPSec 정책 선언*/
8.  R1(config)#crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0  /*인증암호 선언 */
9.  R1(config)#crypto map vpn 10 ipsec-isakmp     /* 트래픽를 IPSec 또는 ISAKMP 적용 설정 */
10. R1(config-crypto-map)#set peer 203.230.9.2
11. R1(config-crypto-map)#set transform-set strong
12. R1(config-crypto-map)#match address 110
13. R1(config-crypto-map)#exit
14. R1(config)#access-list 110 permit gre host 203.230.9.1 host 203.230.9.2  /*정책 적용범위 ACL
    정의 */
15. R1(config)#int S0/2/0
16. R1(config-if)#crypto map vpn                  /* VPN 동작 선언 */
17. R1(config-if)#no shut
18. R1(config-if)#router ospf 7                 /* full-routing 실시 */
19. R1(config-router)#network 203.230.7.1 0.0.0.0 area 0
20. R1(config-router)#network 203.230.8.1 0.0.0.0 area 0
21. R1(config-router)#network 203.230.9.1 0.0.0.0 area 0
22. R1(config-router)#network 10.10.10.1 0.0.0.0 area 0
23. R1(config-router)#exit
```

GRE 터널링 이용한 IPSec VPN

R2 설정 스크립트

```
1.  Router#conf t
2.  Router(config)#hostname R2
3.  R2(config)#int S0/2/0
4.  R2(config-if)#ip add 203.230.10.1 255.255.255.0
5.  R2(config-if)#clock rate 64000
6.  R2(config-if)#no shut
7.  R2(config)#int S0/2/1
8.  R2(config-if)#ip add 203.230.9.2 255.255.255.0
9.  R2(config-if)#no shut
10. R2(config)#int tunnel 12                    /* 트래픽 터널 설정 */
11. R2(config-if)#ip add 10.10.10.2 255.255.255.0
12. R2(config-if)#tunnel source s0/2/1
13. R2(config-if)#tunnel destination 203.230.9.1
14. R2(config)#int tunnel 23                    /* 트래픽 터널 설정 */
15. R2(config-if)#ip add 11.11.11.1 255.255.255.0
16. R2(config-if)#tunnel source s0/2/0
17. R2(config-if)#tunnel destination 203.230.10.2
18. R2(config-if)#no shut
19. R2(config-if)#exit
20. R2(config)#license boot module c2900 technology-package securityk9
21. ------------------
22. ACCEPT?[yes/no] : yes
23. R2(config)#do write
24. R2(config)#exit
25. R2#reload                          /* 재부팅 */
```

GRE 터널링 이용한 IPSec VPN

R2 설정 스크립트

1. **R2(config)#crypto isakmp policy 10 /* ISAKMP에서 사용할 정책 선언 */**
2. **R2(config-isakmp)#encryption aes 256**
3. **R2(config-isakmp)#authentication pre-share**
4. **R2(config-isakmp)#lifetime 36000**
5. **R2(config-isakmp)#hash sha**
6. **R2(config-isakmp)#exit**
7. **R2(config)#crypto ipsec transform-set strong esp-3des esp-md5-hmac /*IPSec 정책 선언*/**
8. **R2(config)#crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 /*인증암호 선언 */**
9. **R2(config)#crypto map vpn 10 ipsec-isakmp /* 트래픽를 IPSec 또는 ISAKMP 적용 설정 */**
10. **R2(config-crypto-map)#set peer 203.230.9.1**
11. **R2(config-crypto-map)#set transform-set strong**
12. **R2(config-crypto-map)#match address 110**
13. **R2(config-crypto-map)#exit**
14. **R2(config)#crypto map vpn 20 ipsec-isakmp /* 트래픽를 IPSec 또는 ISAKMP 적용 설정 */**
15. **R2(config-crypto-map)#set peer 203.230.10.2**
16. **R2(config-crypto-map)#set transform-set strong**

GRE 터널링 이용한 IPSec VPN

R2 설정 스크립트

```
1.  R2(config-crypto-map)#match address 120
2.  R2(config-crypto-map)#exit
3.  R2(config)#access-list 110 permit gre host 203.230.9.2 host 203.230.9.1
4.  R2(config)#access-list 110 permit gre host 203.230.10.1 host 203.230.10.2
5.  R2(config)#int S0/2/0
6.  R2(config-if)#crypto map vpn                    /* VPN 동작 선언 */
7.  R2(config-if)#no shut
8.  R2(config)#int S0/2/1
9.  R2(config-if)#crypto map vpn                    /* VPN 동작 선언 */
10. R2(config-if)#no shut
11. R2(config-if)#router ospf 7              /* full-routing 실시 */
12. R2(config-router)#network 203.230.9.2 0.0.0.0 area 0
13. R2(config-router)#network 203.230.10.1 0.0.0.0 area 0
14. R2(config-router)#network 10.10.10.2 0.0.0.0 area 0
15. R2(config-router)#network 11.11.11.1 0.0.0.0 area 0
16. R2(config-router)#exit
```

GRE 터널링 이용한 IPSec VPN

R3 설정 스크립트

```
1.  Router#conf t
2.  Router(config)#hostname R3
3.  R3(config)#int g0/0
4.  R3(config-if)#ip add 203.230.11.1 255.255.255.0
5.  R3(config-if)#no shut
6.  R3(config)#int g0/1
7.  R3(config-if)#ip add 203.230.12.1 255.255.255.0
8.  R3(config-if)#no shut
9.  R3(config)#int S0/2/1
10. R3(config-if)#ip add 203.230.10.2 255.255.255.0
11. R3(config-if)#no shut
12. R3(config)#int tunnel 23                    /* 트래픽 터널 설정 */
13. R3(config-if)#ip add 11.11.11.2 255.255.255.0
14. R3(config-if)#tunnel source s0/2/1
15. R3(config-if)#tunnel destination 203.230.10.1
16. R3(config-if)#no shut
17. R3(config-if)#exit
18. R3(config)#license boot module c2900 technology-package securityk9
19. ------------------
20. ACCEPT?[yes/no] : yes
21. R3(config)#do wirte
22. R3(config)#exit
23. R3#reload                       /* 재부팅 */
```

GRE 터널링 이용한 IPSec VPN

R3 설정 스크립트

```
1.  R3(config)#crypto isakmp policy 10          /* ISAKMP에서 사용할 정책 선언 */
2.  R3(config-isakmp)#encryption aes 256
3.  R3(config-isakmp)#authentication pre-share
4.  R3(config-isakmp)#lifetime 36000
5.  R3(config-isakmp)#hash sha
6.  R3(config-isakmp)#exit
7.  R3(config)#crypto ipsec transform-set strong esp-3des esp-md5-hmac  /*IPSec 정책 선언*/
8.  R3(config)#crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0  /*인증암호 선언 */
9.  R3(config)#crypto map vpn 10 ipsec-isakmp     /* 트래픽를 IPSec 또는 ISAKMP 적용 설정 */
10. R3(config-crypto-map)#set peer 203.230.10.1
11. R3(config-crypto-map)#set transform-set strong
12. R3(config-crypto-map)#match address 110
13. R3(config-crypto-map)#exit
14. R3(config)#access-list 110 permit gre host 203.230.10.2 host 203.230.10.1  /*정책 적용범위
    ACL정의 */
15. R3(config)#int S0/2/1
16. R3(config-if)#crypto map vpn                  /* VPN 동작 선언 */
17. R3(config-if)#no shut
18. R3(config-if)#router ospf 7                /* full-routing 실시 */
19. R3(config-router)#network 203.230.10.2 0.0.0.0 area 0
20. R3(config-router)#network 203.230.11.1 0.0.0.0 area 0
21. R3(config-router)#network 203.230.12.1 0.0.0.0 area 0
22. R3(config-router)#network 11.11.11.2 0.0.0.0 area 0
23. R3(config-router)#exit
```

VPN 정보 확인하기

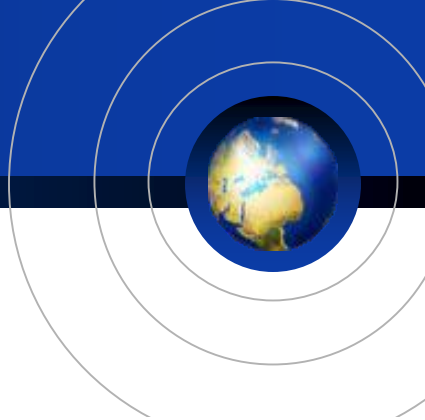
show crypto ipsec sa : 인터페이스별 VPN 정보 확인

1. **R3(config)#show crypto ipsec sa**

show crypto ipsec transform-set : IPSec 설정 정보와 인터페이스 동작 확인

1. **R3(config)#show crypto ipsec transform-set**

show crypto isakmp policy : 설정된 ISAKMP 확인
Show crypto isakmp sa : VPN 출발지와 도착지 확인 및 현재상태 확인
Show crypto map : VPN 연결정보 및 ACL 트래픽 정의 정보



Q & A

감 사 합 니 다`