

수업 내용 정리 보고서

작성일: 2026년 7월 14일

챕터 구성

- RIP/RIPv2 라우팅 프로토콜의 동작 원리와 인터페이스 설정
- RIPv2 인증 메커니즘 및 패킷 분석 검증
- 네트워크 보안: 접근 제어와 정보 수집 기술

RIP/RIPv2 라우팅 프로토콜의 동작 원리와 인터페이스 설정

네트워크 장비 간에 경로 정보를 교환하여 최적의 길을 찾는 라우팅 프로토콜 중, RIP(Routing Information Protocol)은 가장 기초적인 **거리 벡터(Distance Vector)** 방식의 프로토콜입니다. 거리 벡터 방식은 인접한 라우터끼리 주기적으로 자신의 라우팅 테이블 정보를 교환하며, 이때 '거리(Hop Count)'를 기준으로 경로를 결정합니다.

1. 루프 방지를 위한 Split Horizon과 예외 상황

거리 벡터 프로토콜에서는 정보가 순환하며 네트워크 루프(Loop)를 형성하는 것을 방지하기 위해 **스플릿 호라이즌(Split Horizon)**이라는 메커니즘을 사용합니다. 이는 특정 인터페이스를 통해 들어온 라우팅 정보를 다시 동일한 인터페이스로 내보내지 않는 규칙입니다. RIP와 같은 거리 벡터 프로토콜에서는 이 기능이 기본적으로 적용되어 있습니다.

하지만 프레임 릴레이(Frame Relay)와 같이 물리적인 랩(Loop) 구조를 가진 환경에서는 스플릿 호라이즌이 오히려 경로 정보 전달을 방해할 수 있습니다. 이런 특수한 물리적 환경에서는 인터페이스 설정에서 해당 기능을 수동으로 꺼주어야 정상적인 라우팅 정보 교환이 가능합니다.

실제 설정 과정에서는 RIP 프로세스를 활성화한 후, 필요한 이웃(Neighbor) 관계를 정의하고, 특정 인터페이스에 진입하여 스플릿 호라이즌 기능을 비활성화하는 과정을 거칩니다.

no ip split-horizon 명령어

```
R1(config)#router rip
R1(config-router)#neighbor 123.1.1.2
R1(config-router)#neighbor 123.1.1.3
R1(config-router)#exit
R1(config)#int s1/0
R1(config-if)#no ip spl
R1(config-if)#no ip split-horizon
R1(config-if)#
```

RIP 프로토콜 설정 중 인터페이스의 split horizon 기능을 비활성화함

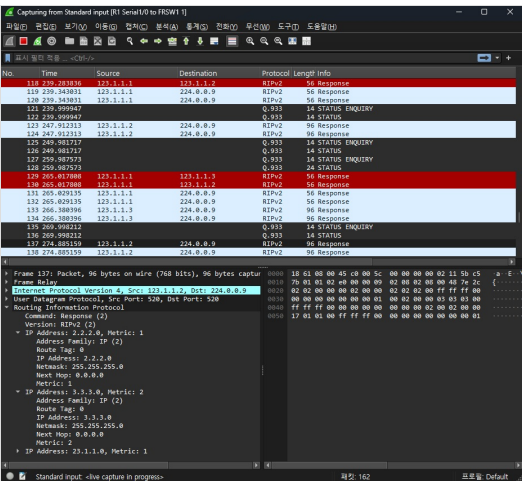
위 설정 화면을 통해 인터페이스(s1/0) 모드에서 `no ip split-horizon` 명령어를 입력하여 루프 방지 기능을 해제했음을 확인할 수 있습니다. 설정 후에는 해당 인터페이스를 통해 정보가 다시 전달될 수 있는 상태가 되었는지 확인해야 합니다.

2. 라우팅 업데이트 메커니즘

RIP는 기본적으로 주기적인 업데이트를 수행하지만, 효율성을 위해 **트리거드 업데이트(Triggered Update)** 방식을 병행합니다. 트리거드 업데이트는 라우팅 테이블에 변화가 생겼을 때 즉시 정보를 전송하는 방식이며, 일반적으로 30분 주기의 주기적 업데이트와 함께 작동합니다. 이때 안정적인 정보 교환을 위해서는 양쪽 라우터 모두에 관련 설정이 적용되어 있어야 합니다.

이러한 업데이트 패킷을 통해 라우터는 인접 장비로부터 목적지 네트워크 주소와 해당 경로까지의 비용(Metric) 정보를 전달받습니다.

IP Address: 2.2.2.0, 3.3.3.0 등 라우팅 정보



RIPv2 응답 패킷을 통해 확인되는 네트워크 주소 및 메트릭 값

패킷 캡처 결과에서 확인할 수 있듯이, RIPv2 응답(Response) 메시지에는 목적지 네트워크 주소(예: 2.2.2.0, 3.3.3.0)와 함께 각 경로의 메트릭(Metric) 값이 포함되어 있습니다. 이를 통해 라우터는 어떤 경로가 더 가까운지를 판단하게 됩니다.

3. RIPv2 보안: 인증(Authentication) 방식

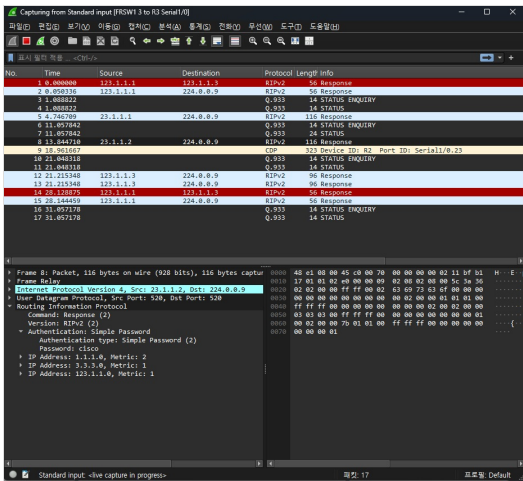
RIPv1과 달리 RIPv2는 보안 강화를 위해 **인증(Authentication)** 기능을 지원합니다. 관리자 간에 사전에 합의된 키 체인(Key Chain)을 사용하여, 신뢰할 수 있는 라우터가 보낸 패킷만 수용함으로써 잘못된 라우팅 정보 주입을 방지합니다. 인증 설정 시에는 키(Key) 번호와 암호 문자열(Key-string)을 관리합니다.

인증 방식은 크게 두 가지로 나뉩니다.

- **Simple Password (Plain Text) 인증:** 암호 정보가 패킷 내에 평문으로 포함되는 방식입니다. 설정은 간편하지만 패킷을 가로채면 암호가 그대로 노출된다는 취약점이 있습니다.
- **Keyed Message Digest (MD5) 인증:** 암호 정보를 해시 함수로 처리하여 전달하는 방식입니다. 실제 암호 대신 해시된 결과값을 사용하여 보안성이 훨씬 높습니다.

실습을 통해 두 방식의 차이를 패킷 관점에서 비교해 보겠습니다.

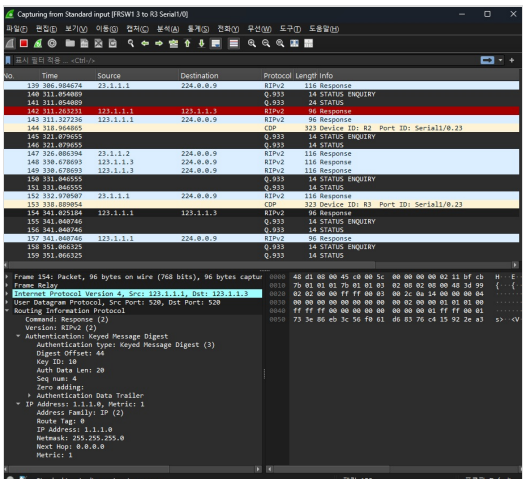
Authentication: Simple Password (Password: cisco)



RIPv2 패킷 내 Simple Password 인증 방식의 암호 정보 확인

Simple Password 방식의 경우, 위 화면처럼 인증 타입이 'Simple Password'로 표시되며, 패킷 내부를 살펴보면 'cisco'와 같은 암호 문자열이 그대로 노출되어 있음을 알 수 있습니다.

Authentication: Keyed Message Digest



Keyed Message Digest 인증이 적용된 RIPv2 패킷의 상세 데이터

반면, Keyed Message Digest 방식은 'Key ID'와 함께 'Digest Offset' 등의 정보를 포함하며, 실제 암호 대신 계산된 해시값이 포함되어 있어 패킷 캡처만으로는 원본 암호를 알아내기 어렵습니다.

4. 트러블슈팅: 인증 오류 발생 시

라우팅 업데이트가 정상적으로 이루어지지 않는다면, 가장 먼저 인증 설정의 일치 여부를 점검해야 합니다. 만약 양쪽 라우터의 키 체인 정보나 인증 방식이 일치하지 않으면, 라우터는 수신된 패킷을 유효하지 않은 것으로 판단하고 무시합니다.

이 과정은 라우터의 디버그(Debug) 로그를 통해 명확하게 확인할 수 있습니다.

ignored v2 packet from 123.1.1.1 (invalid authentication)

```
*Jul 14 11:48:53.623: RIP: Update queued
*Jul 14 11:48:53.623: RIP: Update sent via Loopback0
*Jul 14 11:48:53.627: RIP: Update sent via Serial1/0.23
R3#
*Jul 14 11:48:53.627: RIP: Update sent via Serial1/0.123
*Jul 14 11:48:53.635: RIP: ignored v2 packet from 3.3.3.3 (sourced from one of our ad
dresses)
R3#
*Jul 14 11:48:57.683: RIP: received v2 update from 23.1.1.1 on Serial1/0.23
*Jul 14 11:48:57.683: RIP: Update contains 1 routes
R3#
*Jul 14 11:49:03.827: RIP: ignored v2 packet from 123.1.1.1 (invalid authentication)
*Jul 14 11:49:03.879: RIP: ignored v2 packet from 123.1.1.1 (invalid authentication)
R3#
```

인증 정보 오류로 인해 RIPv2 패킷이 무시되는 라우터 로그

로그 메시지에서 ignored v2 packet from 123.1.1.1 (invalid authentication)라는 문구가 확인된다면, 이는 상대방으로부터 패킷은 수신되었으나 인증 정보(Key 또는 방식)가 맞지 않아 업데이트를 거부했음을 의미합니다. 이 경우 양쪽 장비의 key-string과 key 번호를 재점검해야 합니다.

실무 및 시험 대비 점검 리스트

- **Split Horizon 적용 여부:** 물리적 루프 구조(Frame Relay 등)에서 라우팅이 안 된다면 no ip split-horizon 설정을 확인했는가?
- **RIPv2 인증 일치성:** 인증 방식(Simple vs MD5)과 Key ID, Key-string이 양단 간에 동일하게 설정되었는가?
- **트리거드 업데이트 환경:** 라우팅 테이블 변경 시 즉시 반영되지 않는다면 양측의 업데이트 설정 상태를 확인했는가?
- **로그 분석:** 인증 실패 시 invalid authentication 로그가 발생하는지 확인하여 문제의 원인을 특정했는가?

RIPv2 인증 메커니즘 및 패킷 분석 검증

RIPv2(Routing Information Protocol version 2)는 거리 벡터(Distance Vector) 알고리즘을 사용하는 라우팅 프로토콜입니다. 거리 벡터 방식의 특성상 인접 라우터 간에 주기적으로 라우팅 테이블 정보를 교환하며, 이 과정에서 보안 취약점이 발생할 수 있습니다. 잘못된 정보를 가진 공격자가 라우팅 업데이트를 주입할 경우 네트워크 전체의 경로가 왜곡될 수 있으므로, 인접 라우터 간의 신뢰성을 확보하기 위한 **인증(Authentication)** 메커니즘이 필수적입니다.

1. Split Horizon과 인터페이스 설정

RIP 동작 시 발생할 수 있는 루핑(Looping)을 방지하기 위해 **Split Horizon** 기능이 기본적으로 적용됩니다. 이는 특정 인터페이스를 통해 들어온 라우팅 정보를 다시 해당 인터페이스로 내보내지 않는 기술입니다. 하지만 프레임 릴레이(Frame Relay)와 같은 특정 물리적 망 구조에서는 허브 앤 스포크(Hub-and-Spoke) 토 폴로지의 특성상 이 기능이 오히려 라우팅 업데이트를 차단할 수 있으므로, 상황에 따라 해당 기능을 비활성화해야 합니다.

실습에서는 R1 라우터의 Serial 인터페이스(s1/0)에서 Split Horizon 기능을 해제하는 설정을 수행하였습니다. 명령어를 통해 해당 인터페이스의 루프 방지 메커니즘을 명시적으로 꺼줌으로써 라우팅 정보가 의도한 경로로 전달될 수 있도록 구성합니다.

설정이 완료되면 해당 인터페이스는 자신이 받은 정보를 다시 보낼 수 있는 상태가 됩니다. 이는 토폴로지 설계에 따라 통신 가능 여부를 결정짓는 중요한 설정 포인트입니다.

2. RIPv2 인증 방식의 종류 및 분석

RIPv2는 보안 강도에 따라 크게 두 가지 인증 방식을 지원합니다. 관리자 간에 사전에 합의된 **키 체인(Key Chain)**을 사용하여 인증 숫자와 문자열(Key-string)을 관리하는 것이 핵심입니다.

2.1 Simple Password 인증

Simple Password 방식은 인증을 위한 암호를 패킷 내에 평문(Clear text) 형태로 포함하여 전송합니다. 구현이 매우 간단하지만, 패킷을 캡처할 경우 암호가 그대로 노출된다는 치명적인 단점이 있습니다. 따라서 보안이 중요한 환경에서는 권장되지 않습니다.

Wireshark를 통한 패킷 분석 결과, 인증 타입이 'Simple Password'로 지정되어 있으며, 실제 암호 값이 'cisco'와 같이 평문으로 드러나는 것을 확인할 수 있습니다.

패킷 캡처를 통해 암호를 즉시 확인할 수 있다는 점은 이 방식이 보안 목적으로는 취약함을 시사합니다.

2.2 Keyed Message Digest 인증

더 높은 보안 수준을 요구할 경우 **Keyed Message Digest** 방식을 사용합니다. 이 방식은 암호 자체를 보내는 대신, 키와 패킷 내용을 조합하여 생성된 해시(Hash) 값을 전송합니다. 공격자가 패킷을 가로채더라도 원본 키를 알아내기 매우 어렵습니다.

분석된 패킷에서는 Authentication type이 'Keyed Message Digest'로 나타나며, 실제 암호 대신 Digest Offset과 Key ID 등이 포함된 암호화된 데이터 구조를 보여줍니다.

이 방식을 적용하면 인증 정보의 무결성(Integrity)을 보장할 수 있어, 인가되지 않은 라우터의 접근을 효과적으로 차단할 수 있습니다.

3. 트러블슈팅 및 패킷 검증

라우팅 업데이트가 정상적으로 이루어지지 않을 경우, 인증 설정의 불일치를 가장 먼저 의심해야 합니다. 설정된 키 체인의 내용이나 인증 방식이 서로 다를 경우 라우터는 해당 패킷을 수신하더라도 무시합니다.

라우터의 디버그(Debug) 로그를 확인하면, 특정 IP로부터 온 패킷이 'invalid authentication' 메시지와 함께 거부되었음을 확인할 수 있습니다. 이는 인증 키가 틀렸거나 인증 방식이 일치하지 않을 때 발생하는 명확한 오류 신호입니다.

이러한 로그가 발견된다면 양단 라우터의 key 값과 key-string이 동일한지, 인증 타입이 일치하는지 점검해야 합니다.

인증이 성공적으로 수행되면, 라우터는 패킷 내에 포함된 네트워크 정보를 바탕으로 자신의 라우팅 테이블을 업데이트합니다. 패킷의 페이로드(Payload) 섹션을 분석하면 인접 라우터로부터 전달받은 구체적인 네트워크 주소와 메트릭(Metric) 값을 확인할 수 있습니다.

패킷 분석을 통해 전달되는 목적지 네트워크(예: 2.2.2.0, 3.3.3.0)와 해당 경로의 거리(Metric)를 확인하는 것은 라우팅 업데이트의 정상 동작을 검증하는 최종 단계입니다.

실무 및 시험 핵심 점검 리스트

- **Split Horizon 주의사항:** 프레임 릴레이 환경에서 라우팅 업데이트가 차단된다면 no ip split-horizon 설정을 검토하십시오.
- **인증 방식 선택:** 보안 요구사항에 따라 평문 방식(Simple Password)과 해시 방식(Keyed Message Digest)을 구분하여 적용하십시오.
- **Key Chain 일치 여부:** 인증 실패 시 양쪽 라우터의 key 번호와 key-string이 완벽히 일치하는지 확인하십시오.
- **로그 분석:** invalid authentication 로그는 인증 메커니즘의 설정 오류를 의미하는 결정적인 증거입니다.

네트워크 보안: 접근 제어와 정보 수집 기술

네트워크 보안은 단순히 외부 침입을 막는 것에 그치지 않고, 라우팅 프로토콜의 안정성을 확보하여 경로 루프를 방지하는 것부터 시작하여, 호스트에 대한 접근을 제어하고, 공격자가 수행하는 정보 수집 단계(Reconnaissance)를 차단하는 과정까지를 모두 포함합니다.

1. 라우팅 프로토콜의 안정성 및 인증 (RIPv2 중심)

라우팅 프로토콜이 동작할 때 잘못된 정보가 전달되어 네트워크 루프(Loop)가 발생하면 서비스 불능 상태에 빠질 수 있습니다. 이를 방지하기 위한 메커니즘과 보안을 위한 인증 절차를 학습합니다.

Split Horizon 및 업데이트 메커니즘

Split Horizon은 라우팅 정보가 유입된 인터페이스를 통해 다시 동일한 정보를 내보내지 않도록 하는 기술입니다. 이는 거리 벡터(Distance Vector) 프로토콜에서 경로 루프를 방지하기 위해 기본적으로 적용되는 중요한 메커니즘입니다.

하지만 프레임 릴레이(Frame Relay)와 같은 특정 물리적 랩 환경에서는 토폴로지 특성상 정보를 다시 전달해야 하는 경우가 발생할 수 있으며, 이때는 의도적으로 Split Horizon 기능을 비활성화해야 합니다. 또한, 라우팅 테이블이 변경되었을 때 즉시 정보를 전파하는 **Triggered Update**를 설정하여 네트워크 수렴 속도를 높일 수 있습니다. (단, 양쪽 라우터 모두 설정이 필요합니다.)

실습에서는 R1 라우터의 Serial 인터페이스에서 Split Horizon 기능을 비활성화하는 설정을 확인하였습니다.

R1의 인터페이스 설정 모드에서 no ip split-horizon 명령어를 입력하여 해당 인터페이스의 루프 방지 기능을 해제합니다.

이 설정이 완료되면 해당 인터페이스를 통해 들어온 경로 정보가 다시 해당 인터페이스로 송출될 수 있는 상태가 됩니다.

RIPv2 인증 방식과 보안

라우팅 업데이트 패킷에 인증을 적용하면, 인가되지 않은 라우터가 잘못된 경로 정보를 주입하는 것을 방지할 수 있습니다. RIPv2에서는 **Key Chain** 방식을 사용하여 관리자끼리 사전에 합의된 키(Key)와 문자열(Key-string)을 공유합니다.

- **Simple Password 인증:** 암호가 평문(Plain Text) 형태로 패킷에 포함됩니다. 설정은 간편하지만, 패킷 스니핑을 통해 암호를 쉽게 알아낼 수 있다는 치명적인 약점이 있습니다.

Wireshark 패킷 분석을 통해 Simple Password 방식의 패킷을 확인하면, 인증 타입이 'Simple Password'로 표시되며 실제 암호 문자열이 노출되는 것을 볼 수 있습니다.

이 방식은 암호가 그대로 드러나므로 보안성이 낮아 실제 운영 환경에서는 권장되지 않습니다.

- **Keyed Message Digest 인증:** 암호 대신 해시(Hash) 값을 사용하는 방식입니다. 키 체인을 통해 관리되며, 패킷에는 암호 자체가 아닌 계산된 메시지 다이제스트(Digest)가 포함되어 보안성이 훨씬 높습니다.

Keyed Message Digest 방식의 패킷은 단순 암호와 달리 Key ID와 Digest 값을 포함하고 있어, 공격자가 패킷을 가로채더라도 원본 암호를 알아내기 어렵습니다.

이와 같은 방식은 데이터의 무결성과 인증을 동시에 보장합니다.

인증 오류 및 troubleshooting

라우터 간에 설정된 Key 또는 Key-string이 일치하지 않으면 인증 실패가 발생합니다. 이 경우 라우터는 해당 패킷을 무시하며, 시스템 로그를 통해 오류를 알립니다.

R3 라우터의 로그에서 invalid authentication 메시지가 출력된다면, 상대방이 보낸 패킷의 인증 정보가 설정된 값과 다르다는 것을 의미합니다.

이런 로그가 발생하면 양쪽 라우터의 Key Chain 설정과 Key-string이 정확히 일치하는지 점검해야 합니다.

라우팅 데이터 검증

인증이 성공하여 정상적으로 수신된 RIPv2 응답 패킷을 분석하면, 현재 네트워크에 존재하는 목적지 IP 주소와 해당 경로의 메트릭(Metric, 거리) 값을 확인할 수 있습니다.

패킷 내부의 IP Address와 Metric 필드를 통해 라우팅 테이블에 반영될 경로 정보를 검증할 수 있습니다.

2. 호스트 기반 접근 제어 (TCP Wrapper)

네트워크 장비뿐만 아니라 개별 호스트(서버)에서도 접근 제어가 필요합니다. **TCP Wrapper**는 호스트 기반으로 네트워크 서비스에 대한 접근을 제어하는 프로그램입니다.

- **/etc/hosts.allow**: 접근을 허용할 호스트나 서비스의 IP 주소/도메인을 지정합니다.
- **/etc/hosts.deny**: 접근을 차단할 호스트나 서비스를 지정합니다.

일반적으로 `hosts.deny`에 모든 접근을 차단(ALL: ALL)하도록 설정한 뒤, `hosts.allow`에 필요한 서비스만 선별적으로 허용하는 방식이 보안상 안전합니다.

3. 정보 수집 기술과 방어 전략

공격자는 본격적인 공격에 앞서 대상의 정보를 수집합니다. 이를 방어하기 위해서는 공격자의 행위를 이해하고 선제적인 방어 조치를 취해야 합니다.

Kill Chain과 정보 수집 단계

Kill Chain 개념에 따르면, 공격자는 정보 수집 단계에서 대상의 취약점을 파악합니다. 만약 공격자의 의도가 명백히 느껴진다면, 방어자는 수동적인 대응을 넘어 공격자의 정보를 역으로 수집하거나 선제적으로 차단하는 전략을 고려할 수 있습니다.

- **배너 그래빙 (Banner Grabbing)**: 서비스에 접속했을 때 서버가 스스로 응답하는 정보(OS 버전, 서비스 이름 등)를 가로채는 기법입니다. 이를 방어하기 위해서는 서버 설정에서 표출되는 배너(Banner) 내용을 임의의 문구로 바꾸거나 정보를 최소화해야 합니다.
- **포트 스캐닝 (Port Scanning)**: 대상 서버에서 어떤 포트가 열려 있고 어떤 프로토콜이 서비스 중인지 확인하는 행위입니다. **nmap**과 같은 도구가 대표적입니다.

Nmap 주요 옵션 정리

옵션	설명
-sS	TCP SYN 스캔 (Half-open 스캔)
-sT	TCP Connect() 스캔 (Full handshake)
-sN	TCP Null 스캔
-sF	TCP FIN 스캔
-sX	TCP X-mas 스캔
-sP	Ping 스캔 (호스트 생존 여부 확인)
-sU	UDP 스캔
-sV	열린 서비스 및 버전 정보 확인
-O	운영체제(OS) 탐지
-A	OS, 버전, 스크립트, 경로 추적 등 종합 탐지

실무 및 시험 대비 체크리스트

- **라우팅 루프 방지**: Distance Vector 프로토콜 사용 시 Split Horizon이 기본 적용되어 있는지, 특수 환경(Frame Relay 등)에서 비활성화가 필요한지 확인한다.
- **RIPv2 보안**: Simple Password는 평문 노출 위험이 있으므로, 반드시 Keyed Message Digest(Key Chain) 사용을 권장한다.
- **인증 트러블슈팅**: 라우터 로그에 `invalid authentication`이 발생하면 Key ID와 Key-string 일치 여부를 최우선으로 점검한다.
- **호스트 보안**: TCP Wrapper 설정 시 `hosts.deny`를 통한 기본 차단 정책을 수립했는지 확인한다.
- **정보 유출 방지**: 서버 접속 시 불필요한 시스템 정보가 노출되지 않도록 배너 설정을 관리한다.