

수업 내용 정리 보고서

작성일: 2026년 6월 24일

챕터 구성

1. Interface Types and Data Link Layer Protocols
2. L2 Authentication and End-to-End Communication
3. Network Traffic Control and ACL Management

Interface Types and Data Link Layer Protocols

핵심 질문: 네트워크 환경(WAN/LAN)에 따라 물리적/논리적 연결 방식과 데이터 링크 계층(L2) 프로토콜은 어떻게 달라지는가?

1. 네트워크 환경에 따른 인터페이스 구분

네트워크 기기를 연결하는 환경은 통신 거리와 목적에 따라 크게 원거리 통신망(WAN)과 근거리 통신망(LAN)으로 구분됩니다. 이에 따라 사용되는 인터페이스의 동작 방식과 주소 체계가 결정됩니다.

구분	Serial Line (직렬 회선)	Ethernet Line (이더넷 회선)
주요 용도	WAN (원거리 통신망), 라우터 간 1:1 연결	LAN (근거리 통신망), 내부 네트워크 구성
연결 방식	Point-to-Point (점대점): 두 기기 간 전용선으로 직접 연결	Multi-Access (다중 접속): 스위치나 허브를 통해 다수 기기 연결
동작 원리	데이터를 1비트씩 순차적으로 전송	프레임(Frame) 단위로 데이터를 묶어 전송하며, MAC 주소 기반 스위칭 수행

* 적용 조건: 1:1 연결 환경에서는 복잡한 MAC 주소 체계 없이도 상대 대상을 명확히 구분할 수 있지만, 다중 접속 환경에서는 목적지 식별을 위해 MAC 주소와 같은 식별자가 필수적입니다.

2. WAN 구간의 데이터 링크 계층 프로토콜

Serial Line과 같은 WAN 구간에서 데이터를 안전하게 전달하기 위해 2계층(Data Link Layer)에서 사용하는 대표적인 캡슐화 프로토콜은 HDLC와 PPP입니다.

- HDLC (High-Level Data Link Control)
 - 특징: 구조가 단순하고 처리 속도가 빠르지만, 인증이나 오류 복구 같은 복잡한 기능이 생략되어 있습니다.
 - 주의사항: 표준 HDLC는 단일 프로토콜(IPv4)만 지원합니다. 특히 Cisco 장비는 자체적으로 수정한 'Cisco HDLC'를 기본값으로 사용하므로, 타사 장비와 연결 시 호환성 문제가 발생할 수 있습니다.
- PPP (Point-to-Point Protocol)
 - 특징: 호환성이 매우 높은 표준 프로토콜로, 다양한 상위 네트워크 프로토콜을 지원합니다.
 - 주요 구성 요소:
 - LCP (Link Control Protocol): 링크의 연결 설정, 유지, 해제 및 품질 모니터링을 담당합니다.
 - NCP (Network Control Protocol): IP, IPX 등 다양한 3계층 프로토콜을 동시에 지원하도록 돕습니다.

3. Frame Relay와 NBMA 환경의 이해

Frame Relay는 물리적으로는 다중 접속(Multi-Access)을 지원하지만, LAN과 달리 브로드캐스트 신호가 모든 방향으로 퍼지지 않는 NBMA(Non-Broadcast Multi-Access) 기술입니다.

- PVC (Permanent Virtual Circuit): 하나의 물리적 Serial 회선을 논리적으로 여러 개로 분할하여 구축한 영구 가상 회선입니다. 이를 통해 하나의 포트에 여러 목적지와 독립적인 1:1 연결을 수립할 수 있습니다.
- DLCI (Data-Link Connection Identifier): Frame Relay 환경에서 각 PVC를 식별하기 위해 사용하는 2계층 주소입니다. 실무에서는 관리 편의를 위해 통상 3자리 이하의 숫자로 구성합니다.
- L2-L3 주소 매핑:
 - Static (정적): 관리자가 IP 주소와 DLCI를 수동으로 매핑합니다. 명확한 Point-to-Point 구조에 적합합니다.
 - Dynamic (동적): IARP (Inverse ARP)를 통해 DLCI를 기반으로 상대방의 IP를 자동으로 찾아냅니다. Multi-Point 구조에서 유용하며 회선 활성화 속도가 빠릅니다.

[실습 분석] 서브 인터페이스(Sub-Interface) 및 Frame Relay 설정

하나의 물리 인터페이스를 논리적으로 쪼개어 가상 인터페이스를 만드는 방식은 PVC의 효율적 분할을 위해 필수적입니다.

1. 작업 목표: 물리 인터페이스(s1/0)를 서브 인터페이스(s1/0.12 등)로 분할하고 Frame Relay를 설정하여 가상 회선을 구축한다.
2. 수행 단계 예시:

```
R1(config)# interface s1/0.12
R1(config-subif)# ip add 1.1.1.1 255.255.255.0
R1(config-subif)# frame-relay interface-dlci 102
```

3. 성공 여부 확인 방법: show ip int bri 명령어를 통해 인터페이스의 Status(1계층)와 Protocol(2계층)이 모두 'up'인지 확인합니다. 또한

show frame-relay map을 통해 DLCI 매핑 상태를 점검합니다.

4. 실패 시 점검 포인트:

- **NBMA 설정 누락:** Frame Relay가 NBMA 환경일 경우, 정적 매핑 시 **broadcast** 옵션을 추가해야 정상 동작할 수 있습니다.
- **인터페이스 비활성화:** L3 포트는 기본적으로 **shutdown** 상태이므로 **no shutdown** 명령어가 실행되었는지 확인해야 합니다.
- **L2 매칭 오류:** show ip int bri에서 Protocol 상태가 'down'이라면 L2 프로토콜(HDLC, PPP, Frame Relay 등)이 양단 간에 일치하지 않는 것입니다.

L2 Authentication and End-to-End Communication

핵심 질문: 2계층 인증 메커니즘은 어떻게 동작하며, 서로 다른 L2 프로토콜이 혼재된 구간에서도 데이터 통신이 가능한 이유는 무엇인가?

1. PPP 인증 프로토콜의 보안성 비교

PPP는 링크를 활성화하기 위해 인접 장비 간의 인증 과정을 거칩니다. 인증 방식에 따라 보안 수준이 크게 달라집니다.

인증 방식	동작 원리	보안성 및 특징
PAP (Password Authentication Protocol)	ID와 Password를 평문(Plain text) 으로 전송	취약함: 스니핑(Sniffing) 공격 시 계정 정보가 그대로 노출됨.
CHAP (Challenge Handshake Authentication Protocol)	비밀번호를 단방향 해시(Hash) 처리하여 전송	안전함: 실제 비밀번호 대신 해싱된 값을 비교하므로, 패킷이 탈취되어도 원본 복원이 불가능함.

2. 계층 독립성에 따른 종단 간(End-to-End) 통신 원리

네트워크 통신 시 각 계층은 서로 독립적으로 동작합니다. 이는 서로 다른 L2 프로토콜이 섞여 있는 구간에서도 3계층(IP) 통신이 끊기지 않는 근거가 됩니다.

- 인증의 국지성(Locality):** PPP의 인증(CHAP, PAP)은 물리적으로 인접한 장비 간의 링크를 여는 **국지적 검증** 절차입니다. 라우터는 원격지에 있는 장비의 인증 정보를 대행하거나 요구하지 않습니다. 따라서 통신 양 끝단(R3와 R6)에 서로 다른 인증 정보를 설정하더라도 구간별 링크만 활성화 되면 통신이 가능합니다.
- 캡슐화와 페이로드 보존:** 데이터가 라우터를 통과할 때, 3계층의 IP 패킷(예: ICMP Ping)은 훼손되지 않고 그대로 보존됩니다. 라우터는 유입된 패킷의 기존 2계층 헤더를 해제(De-encapsulation)한 후, 다음 구간의 프로토콜에 맞는 새로운 2계층 헤더로 재포장(Re-encapsulation)합니다.
* 데이터 흐름 예시: $[PPP\ 헤더 + IP] \xrightarrow{(R1)} [Frame\ Relay\ 헤더 + IP] \xrightarrow{(R2)} [새로운\ PPP\ 헤더 + IP]$

[실습 분석] 인증 메커니즘 로그 및 보안 확인

터미널 디버깅 및 패킷 캡처를 통해 인증 과정을 분석할 수 있습니다.

- PAP 보안 취약점 확인:** 패킷 캡처 시 Authenticate-Request 단계에서 Peer-ID와 Password가 텍스트 형태로 적나라하게 노출되는 것을 확인할 수 있습니다.
- CHAP 보안성 확인:** `ppp debug` 명령어를 통해 로그를 확인하면, 라우터가 비밀번호 자체를 비교하는 것이 아니라 해싱된 값을 비교함을 알 수 있습니다. 따라서 패킷 상에서는 비밀번호가 보이지 않습니다.

Network Traffic Control and ACL Management

핵심 질문: ACL(Access Control List)을 사용하여 특정 서비스나 호스트에 대한 접근을 어떻게 정교하게 제어할 수 있는가?

1. ACL의 종류 및 주요 차이점

접근 제어는 목적과 정교함에 따라 표준(Standard)과 확장(Extended) ACL로 나뉩니다.

- **표준 ACL (Standard ACL, 1-99):** 출발지 IP 주소만을 기준으로 트래픽을 필터링합니다.
- **확장 ACL (Extended ACL, 100-199):** 출발지/목적지 IP 주소는 물론, 프로토콜(TCP/UDP/ICMP 등)과 포트 번호(eq 22, eq 80 등)를 사용하여 매우 세밀한 제어가 가능합니다.

2. 실무 시나리오별 ACL 적용 사례

ACL은 인터페이스의 Inbound(유입) 또는 Outbound(유출) 방향에 적용하여 트래픽을 제어합니다.

시나리오 A: 특정 서비스 접근 제한 (확장 ACL 활용)

- **SSH 차단:** 외부에서 서버로의 SSH(TCP 22) 접속을 막고 싶을 때

```
access-list 100 deny tcp any any eq 22
access-list 100 permit ip any any
interface s1/0
ip access-group 100 in
```

- **FTP/SMB 제한:** 특정 네트워크 대역에서만 파일 전송(FTP, SMB)이 가능하도록 설정

```
access-list 100 permit tcp 10.1.4.0 0.0.0.255 10.1.3.0 0.0.0.255 eq 20
access-list 100 permit tcp 10.1.4.0 0.0.0.255 10.1.3.0 0.0.0.255 eq 21
... (중략) ...
access-list 100 deny tcp any any eq 20
```

- **ICMP(Ping) 차단:** 내부망 보안을 위해 Ping 응답을 막고 싶을 때

```
access-list 100 deny icmp any any
access-list 100 permit ip any any
```

시나리오 B: 특정 호스트 접근 제어 (표준 ACL 활용)

- **Windows 호스트만 허용:** 특정 스토리지에 대해 Windows NI(Network Interface)를 가진 호스트만 접근을 허용하도록 설정합니다.

[운영 가이드] ACL 설정 및 관리 주의사항

ACL을 설정할 때 흔히 발생하는 실수와 관리 포인트를 정리합니다.

- **암시적 거부(Implicit Deny):** 모든 ACL의 마지막에는 "모든 것을 거부한다(deny any)"는 규칙이 숨겨져 있습니다. 따라서 **허용할 규칙(permit)을 먼저** 작성하고, 마지막에 필요한 경우에만 deny를 작성해야 합니다.
- **작성 순서의 중요성:** ACL은 위에서부터 순차적으로 규칙을 적용합니다. '*모든 IP 허용(permit ip any any)*'을 맨 위에 작성하면, 그 아래에 작성한 특정 서비스 차단(deny tcp any any eq 22) 규칙은 무시됩니다. **구체적인 규칙에서 일반적인 규칙 순서**로 작성하십시오.
- **방향(Direction) 설정:** ip access-group [번호] [in/out] 명령 시, 트래픽이 인터페이스로 들어오는지(in) 나가는지(out)를 정확히 판단해야 합니다.
 - *Inbound:* 라우터 내부로 들어오는 패킷을 검사하여 라우팅 전 차단.
 - *Outbound:* 라우팅 결정 후 인터페이스를 통해 나가는 패킷을 검사하여 차단.
- **검증 방법:** 설정 후에는 반드시 실제 통신(Ping, Telnet, FTP 등)을 시도하여 의도한 대로 차단/허용이 이루어지는지 확인해야 합니다.

일일 보고서 06.22 + 06.23

team 403

1. Serial Line과 Ethernet Line의 개념 및 동작 원리

네트워크 기기를 연결하는 물리적/논리적 환경은 크게 원거리 통신망(WAN)에서 주로 쓰이는 Serial과 근거리 통신망(LAN)에서 쓰이는 Ethernet으로 구분.

구분	Serial Line (직렬 회선)	Ethernet Line (이더넷 회선)
주요 용도	WAN (원거리 통신망), 라우터 간 1:1 연결	LAN (근거리 통신망), 내부 네트워크 구성
연결 방식	Point-to-Point (점대점): 두 기기 간 전용선으로 직접 연결	Multi-Access (다중 접속): 스위치나 허브를 통해 다수의 기기가 연결
동작 원리	데이터를 1비트씩 순차적으로 전송.	프레임(Frame) 단위로 데이터를 묶어서 전송. MAC 주소를 기반으로 목적지를 찾아 스위칭함.

dynamic

```
R1(config)#int s1/0
R1(config-if)#no ip add
R1(config-if)#int s1/0.12
R1(config-subif)#ip add 1.1.1.1 255.255.255.0
R1(config-subif)#fra
R1(config-subif)#frame
R1(config-subif)#frame-relay inte
R1(config-subif)#frame-relay interface-dlci 102
R1(config-fr-dlci)#
```

static

frame relay는 nbma이기 때문에 b (broadcast) 옵션을 추가하여 해주어야 한다.

PDF 4쪽 실습 화면

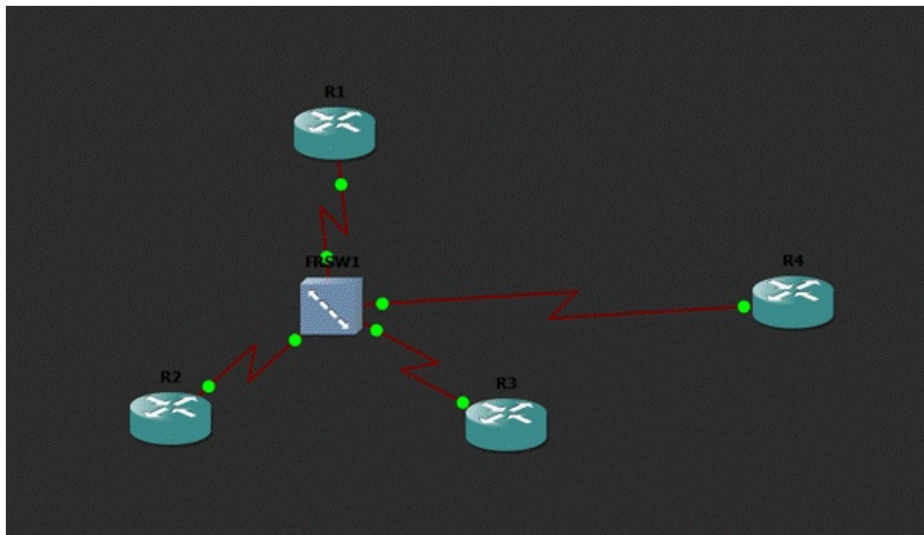
```
R1(config)#int s1/0
R1(config-if)#no ip add
R1(config-if)#int s1/0.12
R1(config-subif)#ip add 1.1.1.1 255.255.255.0
R1(config-subif)#fra
R1(config-subif)#frame
R1(config-subif)#frame-relay inte
R1(config-subif)#frame-relay interface-dlci 102
R1(config-fr-dlci)#
```

PDF 4쪽에서 추출한 실습 이미지

```
R1
terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Soft Multiscreen Tuning Packages Settings Help
Quick connect... 1 R1 R1 R1
R1(config)#no ip add
% Incomplete command.

R1(config)#int s1/0
R1(config-if)#no ip add
R1(config-if)#int s1/0.12
R1(config-subif)#ip add 1.1.1.1 255.255.255.0
R1(config-subif)#fra
R1(config-subif)#frame
R1(config-subif)#frame-relay inte
R1(config-subif)#frame-relay interface-dlci 102
R1(config-fr-dlci)#exit
R1(config-subif)#int s1/0.21 mul
R1(config-subif)#ip add 1.1.2.1 255.255.255.0
R1(config-subif)#frame
R1(config-subif)#frame-relay map ip 1.1.2.2 112 b
R1(config-subif)#
```

PDF 5쪽에서 추출한 실습 이미지



PDF 6쪽에서 추출한 실습 이미지

```

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 1.23.0.0 255.255.0.0 1.123.0.2
R1(config)#ip route 1.23.0.0 255.255.0.0 1.123.0.3
R1(config)#ip route 1.34.0.0 255.255.0.0 1.123.0.3
R1(config)#ip route 1.43.0.0 255.255.0.0 1.123.0.3
R1(config)#end
R1#wr
Building configuration...
[OK]
R1#
*Jun 22 15:07:46.263: %SYS-5-CONFIG_I: Configured from console by console
R1#sh ip int bri

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
Serial1/0	unassigned	YES	unset	up	up
Serial1/0.1234	1.123.0.1	YES	manual	up	up
Serial1/1	unassigned	YES	unset	administratively down	down
Serial1/2	unassigned	YES	unset	administratively down	down
Serial1/3	unassigned	YES	unset	administratively down	down
Ethernet2/0	unassigned	YES	unset	administratively down	down
Ethernet2/1	unassigned	YES	unset	administratively down	down
Ethernet2/2	unassigned	YES	unset	administratively down	down
Ethernet2/3	unassigned	YES	unset	administratively down	down
SSLVPN-VIF0	unassigned	NO	unset	up	up

```

R1#sh fram
R1#sh frame-relay map
Serial1/0.1234 (up): ip 1.123.0.2 dlci 102(0x66,0x1860), static,
broadcast,
CISCO, status defined, active
Serial1/0.1234 (up): ip 1.123.0.3 dlci 103(0x67,0x1870), static,
broadcast,
CISCO, status defined, active

```

PDF 7쪽에서 추출한 실습 이미지

```

R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 1.34.0.0 255.255.0.0 1.123.0.2
R2(config)#ip route 1.43.0.0 255.255.0.0 1.123.0.2
R2(config)#end
R2#wr
Building configuration...
[OK]
R2#
*Jun 22 15:06:28.895: %SYS-5-CONFIG_I: Configured from console by console
R2#sh ip int bri

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
Serial1/0	unassigned	YES	unset	up	up
Serial1/0.123	1.23.0.1	YES	manual	up	up
Serial1/0.1234	1.123.0.2	YES	manual	up	up
Serial1/1	unassigned	YES	unset	administratively down	down
Serial1/2	unassigned	YES	unset	administratively down	down
Serial1/3	unassigned	YES	unset	administratively down	down
Ethernet2/0	unassigned	YES	unset	administratively down	down
Ethernet2/1	unassigned	YES	unset	administratively down	down
Ethernet2/2	unassigned	YES	unset	administratively down	down
Ethernet2/3	unassigned	YES	unset	administratively down	down
SSLVPN-VIF0	unassigned	NO	unset	up	up

```

R2#sh fram
R2#sh frame-relay map
Serial1/0.1234 (up): ip 1.123.0.3 dlci 201(0xC9,0x3090), static,
broadcast,
CISCO, status defined, active
Serial1/0.1234 (up): ip 1.123.0.1 dlci 201(0xC9,0x3090), static,
broadcast,
CISCO, status defined, active
Serial1/0.123 (up): point-to-point dlci, dlci 203(0xCB,0x30B0), broadcast
status defined, active

```

PDF 8쪽에서 추출한 실습 이미지

```

R3#sh ip int bri
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES unset administratively down down
Serial1/0 unassigned YES unset up up
Serial1/0.123 1.23.0.2 YES manual up up
Serial1/0.134 1.34.0.1 YES manual up up
Serial1/0.143 1.43.0.1 YES manual up up
Serial1/0.1234 1.123.0.3 YES manual up up
Serial1/1 unassigned YES unset administratively down down
Serial1/2 unassigned YES unset administratively down down
Serial1/3 unassigned YES unset administratively down down
Ethernet2/0 unassigned YES unset administratively down down
Ethernet2/1 unassigned YES unset administratively down down
Ethernet2/2 unassigned YES unset administratively down down
Ethernet2/3 unassigned YES unset administratively down down
SSLVPN-VIF0 unassigned NO unset up up
R3#sh fram
R3#sh frame-relay map
Serial1/0.1234 (up): ip 1.123.0.2 dlci 301(0x12D,0x48D0), static,
broadcast,
CISCO, status defined, active
Serial1/0.1234 (up): ip 1.123.0.1 dlci 301(0x12D,0x48D0), static,
broadcast,
CISCO, status defined, active
Serial1/0.123 (up): point-to-point dlci, dlci 302(0x12E,0x48E0), broadcast
status defined, active
Serial1/0.134 (up): ip 1.34.0.2 dlci 304(0x130,0x4C00), static,
broadcast,
CISCO, status defined, active
Serial1/0.143 (up): point-to-point dlci, dlci 314(0x13A,0x4CA0), broadcast
status defined, active
R3#sh ip ro
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

1.0.0.0/16 is subnetted, 4 subnets
C 1.23.0.0 is directly connected, Serial1/0.123
C 1.34.0.0 is directly connected, Serial1/0.134
C 1.43.0.0 is directly connected, Serial1/0.143
C 1.123.0.0 is directly connected, Serial1/0.1234

```

PDF 9쪽에서 추출한 실습 이미지

```

R4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#ip route 1.123.0.0 255.255.0.0 1.34.0.1
R4(config)#ip route 1.123.0.0 255.255.0.0 1.43.0.1
R4(config)#ip route 1.23.0.0 255.255.0.0 1.34.0.1
R4(config)#ip route 1.23.0.0 255.255.0.0 1.43.0.1
R4(config)#end
R4#wr
Building configuration...
[OK]
R4#
*Jun 22 15:02:41.779: %SYS-5-CONFIG_I: Configured from console by console
R4#sh ip int bri
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES unset administratively down down
Serial1/0 unassigned YES unset up up
Serial1/0.134 1.34.0.2 YES manual up up
Serial1/0.143 1.43.0.2 YES manual up up
Serial1/1 unassigned YES unset administratively down down
Serial1/2 unassigned YES unset administratively down down
Serial1/3 unassigned YES unset administratively down down
Ethernet2/0 unassigned YES unset administratively down down
Ethernet2/1 unassigned YES unset administratively down down
Ethernet2/2 unassigned YES unset administratively down down
Ethernet2/3 unassigned YES unset administratively down down
SSLVPN-VIF0 unassigned NO unset up up
R4#sh fram
R4#sh frame-relay map
Serial1/0.134 (up): ip 1.34.0.1 dlci 403(0x193,0x6430), static,
broadcast,
CISCO, status defined, active
Serial1/0.143 (up): point-to-point dlci, dlci 413(0x19D,0x64D0), broadcast
status defined, active
R4#ping 1.23.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.23.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/55/72 ms
R4#ping 1.123.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.123.0.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/80/92 ms

```

PDF 11쪽에서 추출한 실습 이미지

```
R4#ping 1.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/57/92 ms
R4#ping 1.16.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.16.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/59/76 ms
R4#ping 1.32.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.32.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/56/64 ms
R4#ping 1.48.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.48.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/66/92 ms
R4#ping 1.64.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.64.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/32/36 ms
R4#ping 1.96.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.96.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/35/52 ms
R4#ping 1.112.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.112.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R4#ping 2.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.0.0.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/77/96 ms
```

```

R4#ping 3.112.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.112.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 148/157/176 ms
R4#ping 3.96.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.96.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/128/160 ms
R4#ping 3.80.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.80.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 108/124/144 ms
R4#ping 3.64.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.64.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/107/128 ms
R4#ping 2.64.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.64.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/116/152 ms
R4#ping 2.80.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.80.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 116/137/156 ms
R4#ping 2.96.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.96.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/76/80 ms
R4#ping 2.112.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.112.0.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/111/132 ms

```

PDF 13쪽에서 추출한 실습 이미지

```

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s1/0
R1(config-if)#enc ppp
R1(config-if)#ip add 1.1.1.1 255.255.255.0
R1(config-if)#end
R1#wr
Building configuration...
[OK]
R1#
*Jun 23 10:17:51.459: %SYS-5-CONFIG_I: Configured from console by console
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s1/0
R1(config-if)#no shut
R1(config-if)#
*Jun 23 10:18:33.407: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R1(config-if)#end
R1#
*Jun 23 10:18:33.407: %ENTITY_ALARM-6-INFO: CLEAR INFO Se1/0 Physical Port Administra
tive State Down
R1#
*Jun 23 10:18:34.439: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, chan
ged state to up
*Jun 23 10:18:34.847: %SYS-5-CONFIG_I: Configured from console by console
R1#wr
Building configuration...
[OK]
R1#ping 1.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/28/36 ms
R1#

```

PDF 14쪽에서 추출한 실습 이미지

```
R2(config)#username R1 password cisco
R2(config)#int s1/0
R2(config-if)#ppp authentication pap
R2(config-if)#ppp pap sent-username R2 password cisco
R2(config-if)#
*Jun 23 10:29:37.119: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R2(config-if)#
```

PDF 14쪽에서 추출한 실습 이미지

7	10.633329	N/A	N/A	PPP LCP	16 Echo Request
8	14.804944	N/A	N/A	PPP LCP	18 Configuration Request
9	14.820254	N/A	N/A	PPP LCP	18 Configuration Request
10	14.820254	N/A	N/A	PPP LCP	18 Configuration Ack
11	14.835006	N/A	N/A	PPP LCP	18 Configuration Ack
12	14.835006	N/A	N/A	PPP PAP	17 Authenticate-Request (Peer-ID='R2', Password='cisco')
13	14.850235	N/A	N/A	PPP PAP	17 Authenticate-Request (Peer-ID='R1', Password='cisco')
14	14.850235	N/A	N/A	PPP PAP	9 Authenticate-Ack (Message='')
15	14.865410	N/A	N/A	PPP PAP	9 Authenticate-Ack (Message='')
16	14.865410	N/A	N/A	PPP IP...	14 Configuration Request
17	14.880530	N/A	N/A	PPP IP...	14 Configuration Request
18	14.880530	N/A	N/A	PPP IP...	14 Configuration Ack
19	14.880530	N/A	N/A	PPP CD...	8 Configuration Request

PDF 14쪽에서 추출한 실습 이미지