

네트워크 보안

정보보안분야 강사 임대선

교과목 목차

1. 네트워크 구성

2. 네트워크 보안

3. 네트워크 취약점 진단

네트워크 구성

1. 네트워크 기본 개념
2. Wireshark 설치 및 활용
3. IP, Subnet, Gateway 설명

네트워크 기본 개념

네트워크(Network)

- Net + work = 그물을 만들다 = 임의로 연결망을 만든다
- 전자신호를 통한 모든 기기의 **통신을 목적**으로 만든 하나의 망
- 복수의 컴퓨터 시스템을 연결하여 데이터나 장치들을 공유하게 하는 연결 통신망

프로토콜(Protocol)

- 컴퓨터 또는 전자기기 간의 원활한 통신을 위해 지키기로 약속한 규약
- IP, TCP, UDP, ICMP, FTP, Telnet, SSH, HTTP, SSL(TLS) 등

네트워크 기본 개념

주요 프로토콜 설명 (1/3) - 일반 통신

IP (Internet Protocol)	기기간 통신을 위해 사용하는 특수한 번호
TCP (Transmission Control Protocol)	신뢰성 연결 지향 통신
UDP (User Datagram Protocol)	비연결 지향 통신
ICMP (Internet Control Message Protocol)	네트워크 제어 메시지

※ UDP가 TCP에 비해 전송속도가 빠름

네트워크 기본 개념

주요 프로토콜 설명 (2/3) - 원격 접속

FTP (File Transfer Protocol)	파일 전송(평문)
SFTP (Secure FTP)	파일 전송(암호화)
SSH (Secure Shell)	원격 접속(Unix, CLI기반, 암호화)
Telnet	원격 접속(Win, Unix, CLI기반, 평문)
RDP (Remote Desktop Protocol)	원격 접속(Win, GUI기반, 평문)

※ CLI(Command-Line Interface) : 명령어 기반 인터페이스 = CUI(Character User Interface)

※ GUI(Graphical User Interface) : 그래픽 유저 인터페이스

※ 평문 : 그대로 보이는 문자(읽을수 있음)

※ 암호화 : 그대로 보이지 않도록 변환되어있는 문자(읽을수 없음)

네트워크 기본 개념

주요 프로토콜 설명 (3/3) - 어플리케이션 접속

HTTP (HyperText Transfer Protocol)	웹페이지 접속(평문)
SSL (Secure Socket Layer)	웹페이지 접속(암호화, HTTPS)
SMTP (Simple Mail Transfer Protocol)	메일 전송
NTP (Network Time Protocol)	시간 동기화

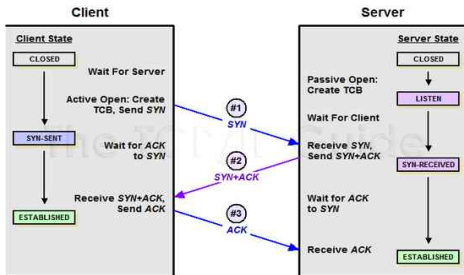
※ HTTPS (HTTP Secure) : HTTP + SSL(TLS)

※ TLS (Transport Layer Security) = SSL의 업그레이드 버전

네트워크 기본 개념

TCP 3-way Handshake - 세션 설정 (1/2)

- 양방향 신뢰성 보장을 위해 상대방과 사전에 세션(연결)을 설정하는 과정
- 양쪽 모두 데이터를 전송할 준비가 되었다는 것을 보장하고, 실제로 데이터 전달이 시작하기 전에 서로 상대방이 준비되었다는 것을 알 수 있도록 함



네트워크 기본 개념

TCP 3-way Handshake - 세션 설정 (2/2)

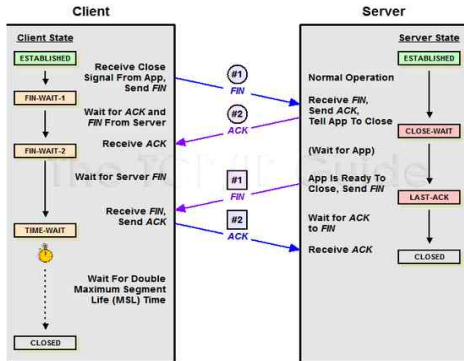
- 1단계 : 클라이언트는 서버에 접속을 요청하는 SYN 패킷을 보내고 SYN_SENT 상태가 된다.
이때 서버는 Listen 상태여야한다.
- 2단계 : 서버는 SYN 패킷을 받고 클라이언트에 SYN+ACK 패킷을 보내고 SYN_RECEIVED 상태가 된다.
- 3단계 : 클라이언트는 SYN+ACK 패킷을 받고 서버에 ACK를 보내고 ESTABLISHED 상태가 된다.
서버는 ACK을 받고 ESTABLISHED 상태가 된다.

※ 클라이언트 (Client) : 사용자, 종료가 가능한 기기
※ 서버 (Server) : 제공자, 종료가 불가능한 기기(상시 구동중)

네트워크 기본 개념

TCP 4-way Handshake - 세션 종료 (1/2)

- 이미 연결된 세션을 종료하기 위해 수행하는 절차



네트워크 기본 개념

TCP 4-way Handshake - 세션 종료 (2/2)

- 1단계 : 클라이언트는 연결을 종료한다는 FIN 플래그를 서버로 보낸다
- 2단계 : 서버는 FIN 플래그를 받고 ACK 패킷으로 응답 후 통신이 끝날때까지 대기한다
- 3단계 : 서버가 통신이 끝나면 연결이 종료되었다고 FIN 플래그를 클라이언트로 보낸다
- 4단계 : 클라이언트는 FIN 플래그를 받고 ACK 패킷으로 응답한다.

※ 플래그 : 패킷의 상태를 나타내는 부분(패킷의 일부)

네트워크 기본 개념

네트워크 명령어 실습

- 시작(좌클릭) > 명령 프롬프트(혹은 cmd)
- 시작(우클릭) > 실행 or 윈도우+R(단축키) 후 실행창에서 cmd 입력

ipconfig	windows ip 구성 확인 (ipconfig /all : 자세한 내용까지 확인)
tracert (ip or domain)	목적지까지 통과하는 경로 정보와 지연시간 출력
nslookup (domain)	DNS 서버의 IP주소 확인
ping (ip or domain)	네트워크의 상태를 진단, 점검

※ 항상 관리자 권한으로 실행하게 하는 방법

- 실행창에서 regedit 입력
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA의 값을 0으로 설정

네트워크 기본 개념

포트(Port)

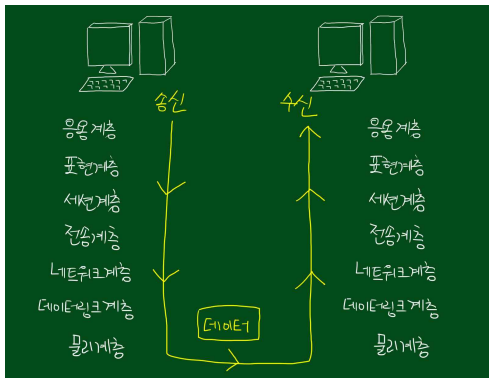
- 포트 번호는 컴퓨터별 0~65535번까지 총 65536개를 사용할 수 있음
- 일반적으로 0~1023번은 Well-known(알려진) 포트로 통칭

프로토콜	포트번호	서비스명	프로토콜	포트번호	서비스명
TCP	20	FTP(데이터 전송)			
TCP	21	FTP(연결제어)			
TCP	22	SSH			
TCP	23	Telnet			
TCP	25	SMTP			
TCP	53	DNS	UDP	53	DNS
TCP	80	HTTP	UDP	69	TFTP
TCP	111	RPC	UDP	111	RPC
TCP	137	NetBIOS	UDP	123	NTP
TCP	139	NetBIOS	UDP	161	SNMP
TCP	443	SSL	UDP	162	SNMP
TCP	445	NetBIOS	UDP	445	SMB
TCP	1433	MSSQL DB			
TCP	1501	Oracle DB			
TCP	3306	MYSQL DB			
TCP	3389	RDP			

네트워크 기본 개념

OSI 7 Layer

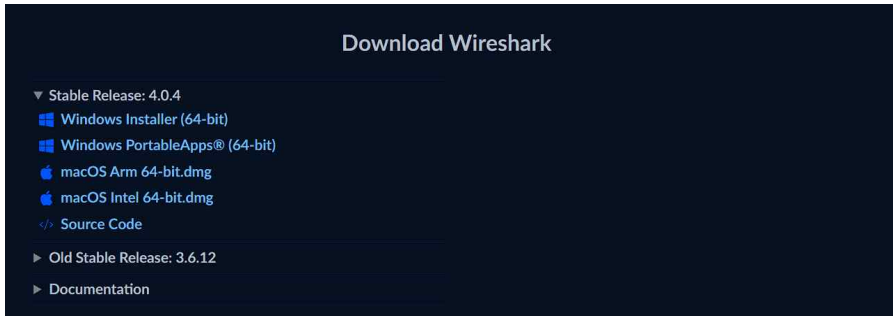
- 국제표준화기구(ISO)에서 개발한 모델



계층(Layer)	기능 / 프로토콜	PDU (Protocol Data Unit)
Application	컴퓨터의 응용프로그램 의미 (HTTP, FTP, WWW, Telnet)	Application data
Presentation	Data의 Format을 정의/압축, 암호화 기능 수행 (JPEG, MIDI, MPEG, EBCDIC)	
Session	네트워크 연결 성립, 제어, 관리, 종료 수행 (OS)	
Transport	Data의 전송 (TCP, UDP)	Segment
Network	Data 전송의 경로 설정 (IP, IPX, ICMP, ARP)	Packet
Data-Link	Data의 에러검출, 흐름제어 (Mac)	Frame
Physical	Data를 전기적인 신호로 변경 (Hub, Repeater)	Bit

Wireshark 설치 (1/2)

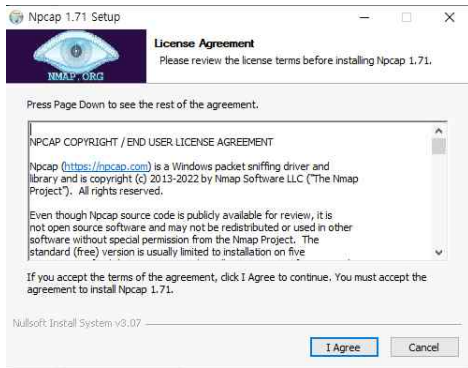
- 현재 클라이언트에서 요청/응답 패킷에 대해 실시간 캡처가 가능하며 패킷 파일을 별도로 저장하여 다양한 분석에 이용할 수 있음
- <http://www.wireshark.org>에서 다운로드(운영체제 확인)



Wireshark 설치 및 활용

Wireshark 설치 (2/2)

- 설치중 Npcap 설치를 요구하면 기본값으로 설치



Wireshark 설치 및 활용

Wireshark 실행

- 실행 후 패킷을 캡처할 네트워크 인터페이스를 지정한 다음 실시간 캡처 시작



Welcome to Wireshark

Capture

...using this filter:

이더넷

Adapter for loopback traffic capture 

로컬 영역 연결* 8

로컬 영역 연결* 7

로컬 영역 연결* 6

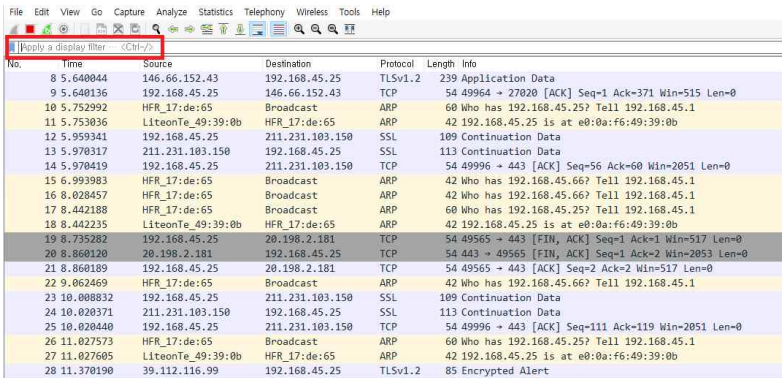
※ 이더넷 : 유선 인터넷 네트워크 카드

※ loopback : 자기 자신의 ip(=localhost ip=127.0.0.1)

Wireshark 설치 및 활용

Wireshark 사용 방법

- Apply a display filter 부분에 프로토콜,ip 등 분석자가 확인하고 싶은 정보를 필터링



Wireshark 설치 및 활용

Wireshark 필터 예시 (1/2)

프로토콜 입력	tcp, udp, icmp, ftp, http, ssh 등
ip입력	ip.src, ip.dst, ip.addr
사용자 정의 포트 입력	tcp.port, tcp.srcport, tcp.dstport

※ src(source) : 출발지

※ dst(destination) : 목적지

※ ip.addr : 출발지, 목적지 상관없이 해당 ip가 포함되어있는지 필터링

※ tcp.port : 출발지, 목적지 상관없이 해당 port가 포함되어있는지 필터링

Wireshark 설치 및 활용

Wireshark 필터 예시 (2/2)

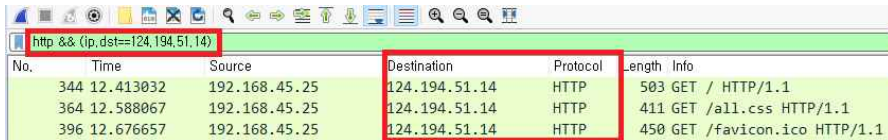
- 목적지 ip가 124.194.51.14인 패킷만 필터링(ip.dst==124.194.51.14)

ip.dst==124.194.51.14						
No.	Time	Source	Destination	Protocol	Length	Info
337	12.394699	192.168.45.25	124.194.51.14	TCP	66	49915 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
338	12.394872	192.168.45.25	124.194.51.14	TCP	66	49916 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
342	12.412850	192.168.45.25	124.194.51.14	TCP	54	49915 → 8000 [ACK] Seq=1 Ack=1 Win=131328 Len=0
343	12.412894	192.168.45.25	124.194.51.14	TCP	54	49916 → 8000 [ACK] Seq=1 Ack=1 Win=131328 Len=0
344	12.413032	192.168.45.25	124.194.51.14	HTTP	503	GET / HTTP/1.1
349	12.542949	192.168.45.25	124.194.51.14	TCP	54	49916 → 8000 [ACK] Seq=450 Ack=1294 Win=130048 Len=0
364	12.588067	192.168.45.25	124.194.51.14	HTTP	411	GET /all.css HTTP/1.1
373	12.610763	192.168.45.25	124.194.51.14	TCP	54	49916 → 8000 [ACK] Seq=807 Ack=1921 Win=131328 Len=0
396	12.676657	192.168.45.25	124.194.51.14	HTTP	450	GET /favicon.ico HTTP/1.1
403	12.687565	192.168.45.25	124.194.51.14	TCP	54	49916 → 8000 [ACK] Seq=1203 Ack=4841 Win=131328 Len=0
406	12.690759	192.168.45.25	124.194.51.14	TCP	54	49916 → 8000 [ACK] Seq=1203 Ack=6301 Win=131328 Len=0
414	12.702779	192.168.45.25	124.194.51.14	TCP	54	49916 → 8000 [ACK] Seq=1203 Ack=7457 Win=130048 Len=0

Wireshark 설치 및 활용

Wireshark 다중 필터

- ==(equal), &&(and), ||(or) 구문 및 괄호 활용이 가능
- http 프로토콜이면서 목적지 ip가 124.194.51.14인 패킷을 필터링



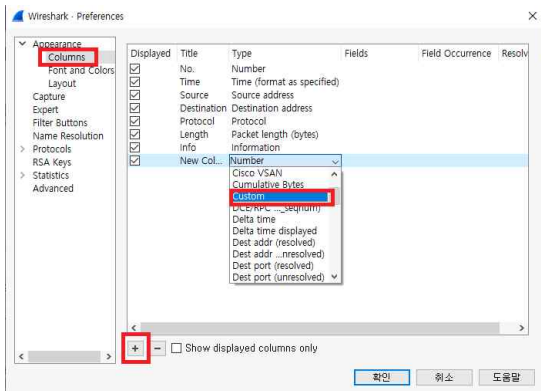
The screenshot shows the Wireshark interface. The packet filter bar at the top contains the expression `http && (ip.dst==124.194.51.14)`. Below it, a table displays the captured packets that match this filter.

No.	Time	Source	Destination	Protocol	Length	Info
344	12.413032	192.168.45.25	124.194.51.14	HTTP	503	GET / HTTP/1.1
364	12.588067	192.168.45.25	124.194.51.14	HTTP	411	GET /all.css HTTP/1.1
396	12.676657	192.168.45.25	124.194.51.14	HTTP	450	GET /favicon.ico HTTP/1.1

Wireshark 설치 및 활용

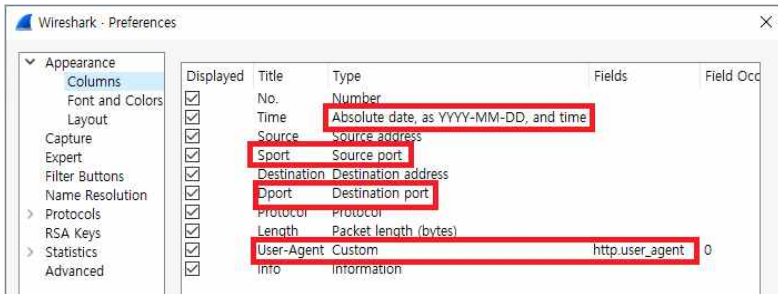
사용자 정의 필드 만들기

- 메뉴의 Edit - Preferences - Appearance - Columns에서 사용자 정의 형태로 필드추가/수정 가능



Wireshark 설치 및 활용

사용자 정의 필드 예시

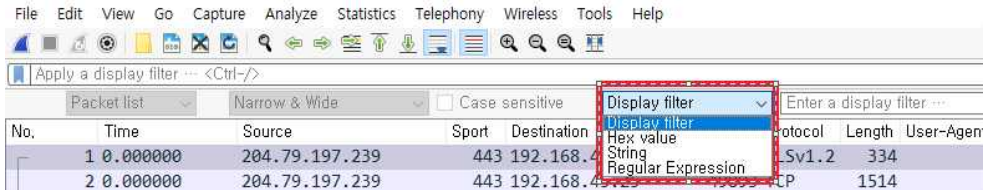


- ※ Absolute date, as YYYY-MM-DD, and time : 년-월-일 시:분:초 형식으로 설정
- ※ Fields : Type이 Custom일때 WireShark 필터링 방식으로 필드 설정
- ※ http.user_agent : 웹 통신시 사용되는 브라우저 or 프로그램

Wireshark 설치 및 활용

데이터 검색

- Ctrl + F로 원하는 데이터 검색 및 추가 필터링 가능



- ※ Display filter : 추가 필터링
- ※ Hex value : Hex data(16진수) 검색
- ※ String : 문자열 검색
- ※ Regular Expression : 정규표현식을 이용한 검색

Wireshark 설치 및 활용

데이터 일괄 다운로드

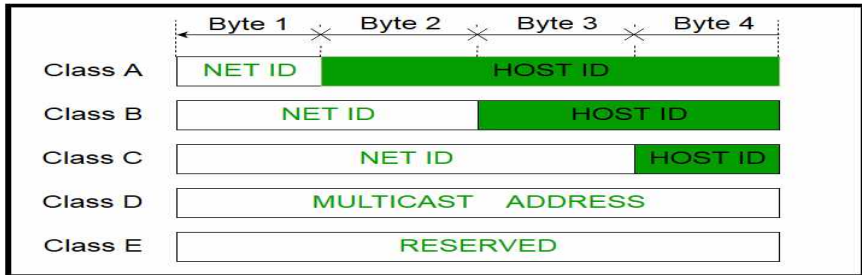
- 메뉴의 File - Export Packet Dissections - As CSV...

	A	B	C	D	E	F	G	H	I	J
1	No.	Time	Source	Sport	Destination	Dport	Protocol	Length	User-Agent	Info
2	1	2023-04-15 1:22	HFR_17:de:65		Broadcast		ARP	60		Who has 192.168.45.25? Tell 192.168.45.1
3	2	2023-04-15 1:22	LiteonTe_49:39:0b		HFR_17:de:65		ARP	42		192.168.45.25 is at e0:0a:f6:49:39:0b
4	3	2023-04-15 1:22	HFR_17:de:65		Broadcast		ARP	60		Who has 192.168.45.25? Tell 192.168.45.1
5	4	2023-04-15 1:22	LiteonTe_49:39:0b		HFR_17:de:65		ARP	42		192.168.45.25 is at e0:0a:f6:49:39:0b
6	5	2023-04-15 1:22	192.168.45.25	51033	204.79.197.200	443	TCP	54		51033 > 443 [FIN, ACK] Seq=1 Ack=1 Win=515 Len=0
7	6	2023-04-15 1:22	192.168.45.25	51038	124.194.51.14	8000	TCP	54		51038 > 8000 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
8	7	2023-04-15 1:22	192.168.45.25	51039	124.194.51.14	8000	TCP	54		51039 > 8000 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
9	8	2023-04-15 1:22	192.168.45.25	51065	124.194.51.14	8000	TCP	66		51065 > 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10	9	2023-04-15 1:22	192.168.45.25	51066	124.194.51.14	8000	TCP	66		51066 > 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
11	10	2023-04-15 1:22	204.79.197.200	443	192.168.45.25	51033	TCP	60		443 > 51033 [ACK] Seq=1 Ack=2 Win=16382 Len=0
12	11	2023-04-15 1:22	204.79.197.200	443	192.168.45.25	51033	TCP	54		443 > 51033 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
13	12	2023-04-15 1:22	124.194.51.14	8000	192.168.45.25	51039	TCP	54		8000 > 51039 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
14	13	2023-04-15 1:22	124.194.51.14	8000	192.168.45.25	51038	TCP	54		8000 > 51038 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
15	14	2023-04-15 1:22	124.194.51.14	8000	192.168.45.25	51066	TCP	66		8000 > 51066 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
16	15	2023-04-15 1:22	124.194.51.14	8000	192.168.45.25	51065	TCP	66		8000 > 51065 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
17	16	2023-04-15 1:22	192.168.45.25	51066	124.194.51.14	8000	TCP	54		51066 > 8000 [ACK] Seq=1 Ack=1 Win=131328 Len=0
18	17	2023-04-15 1:22	192.168.45.25	51065	124.194.51.14	8000	TCP	54		51065 > 8000 [ACK] Seq=1 Ack=1 Win=131328 Len=0
19	18	2023-04-15 1:22	192.168.45.25	51066	124.194.51.14	8000	HTTP	615	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36	GET / HTTP/1.1
20	19	2023-04-15 1:22	124.194.51.14	8000	192.168.45.25	51066	HTTP	265		HTTP/1.1 304 Not Modified
21	20	2023-04-15 1:22	192.168.45.25	51066	124.194.51.14	8000	TCP	54		51066 > 8000 [ACK] Seq=562 Ack=212 Win=131072 Len=0

IP, Subnet, Gateway 설명

IP 구성(Class)

- IP 주소 클래스(IP Address Class)
- IP 주소의 네트워크 영역과 호스트 영역 구분에 대한 규약
- IP 주소의 Class A, B, C, D, E로 구분
- IP를 클래스로 분류하는 이유는 효율적으로 IP주소를 배분하기 위함



IP, Subnet, Gateway 설명

A Class

- Network ID : 8bit
- host ID : 24bit
- A Class 범위 : 0.0.0.0 ~ 127.255.255.255

B Class

- Network ID : 16bit
- host ID : 16bit
- B Class 범위 : 128.0.0.0 ~ 191.255.255.255

IP, Subnet, Gateway 설명

C Class

- Network ID : 24bit
- host ID : 8bit
- C Class 범위 : 192.0.0.0 ~ 223.255.255.255

D Class

- 멀티캐스트용 클래스 ※ 멀티캐스트 : 1:多 패킷 송수신 방식(화상회의)
- D Class 범위 : 224.0.0.0 ~ 239.255.255.255

E Class

- 미래의 연구를 목적으로 하는 클래스(아직 사용하지 않음)
- E Class 범위 : 240.0.0.0 ~ 247.255.255.255

IP, Subnet, Gateway 설명

예시

- 예시 1 : 50.10.20.5
- A Class, 네트워크 : 50, 호스트 : 10.20.5

- 예시 2 : 150.42.5.1
- B Class, 네트워크 : 150.42, 호스트 : 5.1

- 예시 3 : 202.12.1.7
- C Class, 네트워크 : 202.12.1, 호스트 : 7

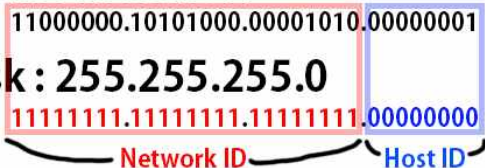
IP, Subnet, Gateway 설명

Subnet mask

- 기존 Class 방식으로는 ip주소 고갈 위험이 있으므로 효율적인 분배를 위해 중복된 ip를 하나의 그룹으로 묶기 위해서 도입

IP Address : 192.168.10.1

Subnet Mask : 255.255.255.0



※ 위의 IP 주소는 192.168.10.1/24로도 표현(CIDR 표기법)

IP, Subnet, Gateway 설명

사설(Private) IP

- 공인 환경(외부망)이 아닌 내부 사설 환경(내부망)에서 사용하는 주소

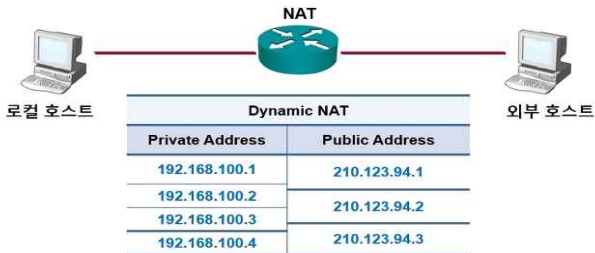
사설 IP 주소 범위

Class	Address Range	Prefix
A Class	10.0.0.0 ~ 10.255.255.255	10.0.0.0/8
B Class	172.16.0.0 ~ 172.31.255.255	172.16.0.0/12
C Class	192.168.0.0 ~ 192.168.255.255	192.168.0.0/16

IP, Subnet, Gateway 설명

NAT IP

- NAT(Network Address Translation) : 공인 IP를 사설 IP로 변환시키는 기술
- IPv4 주소 부족 문제를 해결하기 위한 방법
- 내부망은 사설 IP를 사용하고 내부망-외부망 통신시 NAT IP를 거쳐 공인 IP로 변환



IP, Subnet, Gateway 설명

Gateway

- 서로 다른 네트워크 사이의 통로 역할을 하는 장치

```
IPv4 주소 . . . . . : 192.168.45.25
서브넷 마스크 . . . . . : 255.255.255.0
기본 게이트웨이 . . . . . : 192.168.45.1
```

네트워크 보안

1. Packet Tracer 설치 및 실행
2. 네트워크 장비 구축 및 기본 명령어 실습
3. 네트워크 장비 운영 및 보안 설정

Packet Tracer 설치 및 실행

Packet Tracer 설치 방법 (1/8)

- <https://skillsforall.com/learningcollections/cisco-packet-tracer> 접속 후 하단에 Getting Started with Cisco Packet Tracer 클릭



Packet Tracer 설치 및 실행

Packet Tracer 설치 방법 (2/8)

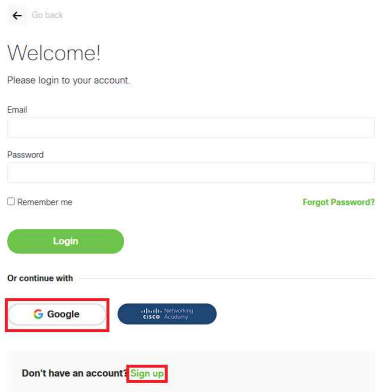
- GET Started 클릭



Packet Tracer 설치 및 실행

Packet Tracer 설치 방법 (3/8)

- 구글 계정 연동 or 회원가입 후 로그인



← Go back

Welcome!

Please login to your account.



Email

Password

☐ Remember me [Forgot Password?](#)

Login

Or continue with

 Google 

Don't have an account? [Sign up](#)

Packet Tracer 설치 및 실행

Packet Tracer 설치 방법 (4/8)

- 위에서 3개만 체크 후 Accept&Continue 클릭

Terms & Conditions

Terms and Conditions for Use of Cisco Networking Academy Websites and Services

1. **Background.** The sites NetAcad.com and SkillsForAll.com are websites ("Websites") within the Cisco Networking Academy Program ("Program"). Cisco operates and provides access to a range of Program related websites and microsites accessible to users (including students, nonstudents and alumni) who have a Cisco Username and Passwords. Websites contain content relevant to the Program and are also designed to enable social networking and collaboration ("Services") among users. The Services enable a user to create personal profiles (each, a "Profile") that can be searched and viewed by other users. The Services also support discussion forums, chat, electronic messaging, survey tools, blogs, wikis or other collaborative tools that Cisco elects to make available in its discretion. Cisco may modify, enhance, restrict or terminate Websites and Services in its discretion at any time and without notice.

The Program operates in accordance with global privacy laws, including laws that impact children's privacy. Registration or use of the Program is not intended for children. For the purposes of the Program, we consider an individual to be a child if the applicable law limits the processing of an individual's personal data because the individual is under a certain age (for example, individuals under 13 years of age

- ☒ agree to Cisco Networking Academy Sites and Services Terms and conditions. *
- ☒ agree to the collection & use of the personal information by Cisco. [Learn more](#) *
- ☒ agree to the retention and disposal of the personal information. [Learn more](#) *
- ☐ I would like to receive email communication about courses and learning offering from Cisco and its affiliates. I understand I can unsubscribe at any time. [Learn more](#).

Accept & Continue

Cancel

Packet Tracer 설치 및 실행

Packet Tracer 설치 방법 (5/8)

- 우측 프레임에서 Install Cisco Packet Tracer 클릭



Module 1: Download and Use Cisco Packet Tracer

Scroll down ⬇️ and select 'Install Cisco Packet Tracer' to begin.



Packet Tracer 설치 및 실행

Packet Tracer 설치 방법 (6/8)

- 하단에 Download Cisco Packet Tracer에서 downloads 링크 클릭

1.0.3 Download Cisco Packet Tracer



To obtain and install your copy of Cisco Packet Tracer, please follow the instructions from the link below:

<https://skillsforall.com/resources/lab-downloads>

Packet Tracer 설치 및 실행

Packet Tracer 설치 방법 (7/8)

- 하단에 Learning Resources에서 운영체제와 맞는 Packet Tracer 다운로드

Learning Resources



Cisco Packet Tracer

Cisco Packet Tracer, an innovative network configuration simulation tool, helps you hone your networking configuration skills from your desktop. Use Packet Tracer to experiment while building, managing & securing infrastructures.

To obtain and install your copy of Cisco Packet Tracer, please follow these simple steps:

Step 1. Download the version of Packet Tracer you require.

[Packet Tracer 8.2.1 MacOS 64bit](#)

[Packet Tracer 8.2.1 Ubuntu 64bit](#)

[Packet Tracer 8.2.1 Windows 64bit](#)

Step 2. Launch the Packet Tracer install program.

Step 3. Launch Cisco Packet Tracer by selecting the appropriate icon.

Step 4. When prompted, click on Skills For All green button to authenticate.

Step 5. Cisco Packet Tracer will launch and you are ready to explore its features.

If you need more guidance, please follow the [Cisco Packet Tracer Download and Install](#)

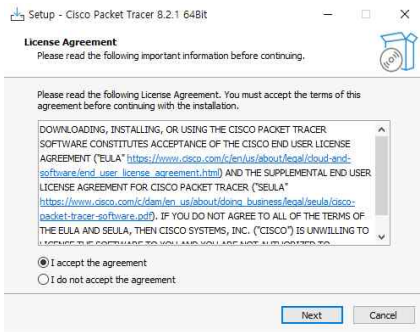
System Requirements:

Computer with either Windows (10, 11), MacOS (10.14 or newer) or Ubuntu (20.04, 22.0, 14 GB of free disk space

Packet Tracer 설치 및 실행

Packet Tracer 설치 방법 (8/8)

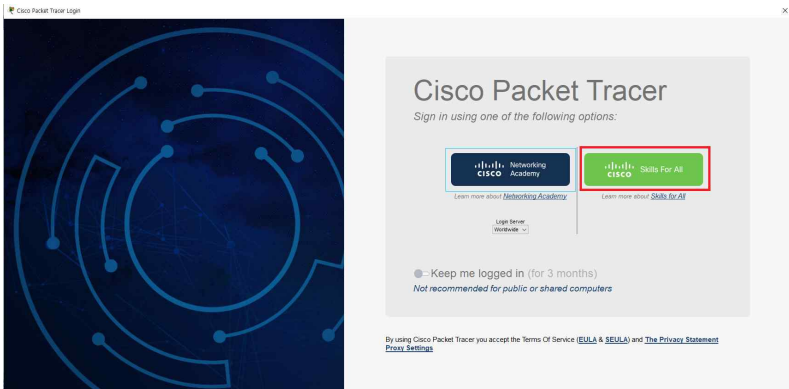
- 기본값으로 설치 진행



Packet Tracer 설치 및 실행

Packet Tracer 실행 방법 (1/2)

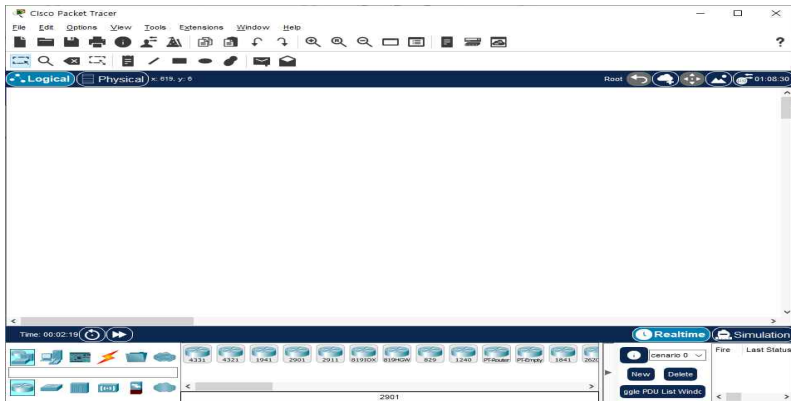
- 설치 후 실행 시 로그인 화면에서 Skills For All 클릭 후 로그인



Packet Tracer 설치 및 실행

Packet Tracer 실행 방법 (2/2)

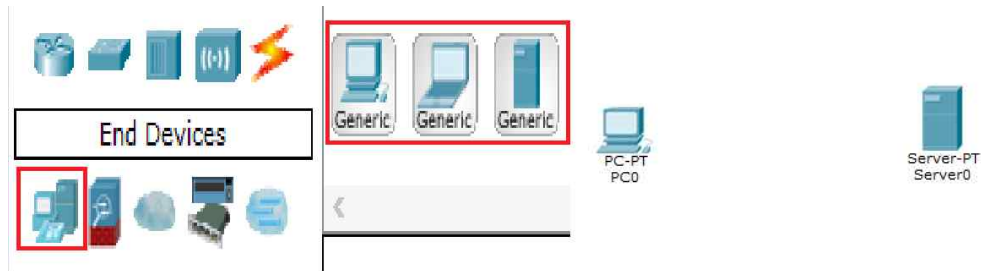
- 실행 완료



네트워크 장비 구축 및 기본 명령어 실습

기본 토폴로지 구성 연습 (1/7)

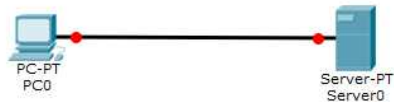
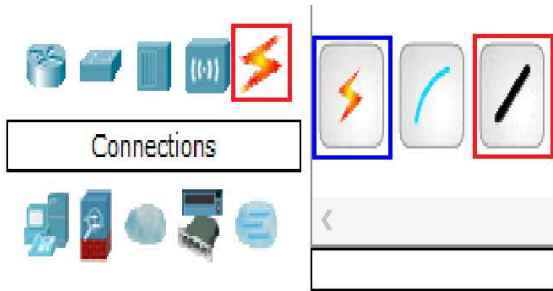
- 왼쪽 하단에 End Devices - PC(혹은 Laptop) , Server를 드래그 앤 드롭



네트워크 장비 구축 및 기본 명령어 실습

기본 토폴로지 구성 연습 (2/7)

- 왼쪽 하단에 Connections - Copper Straight-Through 선택 후 PC와 Server 연결
- 빨간색 불빛은 데이터 전송 불가를 의미(잘못 연결함)

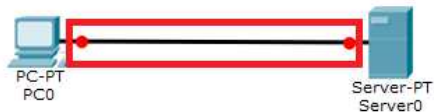


※ Copper Straight-Through : 다이렉트 케이블 (스위치와 스위치가 아닌 것을 연결)

네트워크 장비 구축 및 기본 명령어 실습

기본 토폴로지 구성 연습 (3/7)

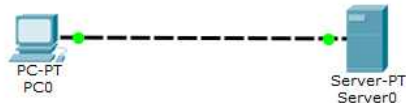
- 화면에 Delete 버튼을 누른 후 제거하고 싶은 부분을 클릭
- 혹은 키보드 Del키를 누른 후 제거하고 싶은 부분을 클릭



네트워크 장비 구축 및 기본 명령어 실습

기본 토폴로지 구성 연습 (4/7)

- 제거된 부분에 Copper Cross-Over 연결
- 초록색 불빛은 데이터 전송 가능

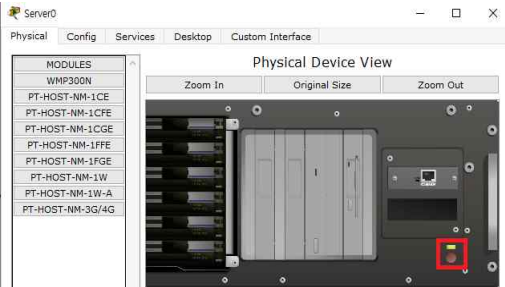
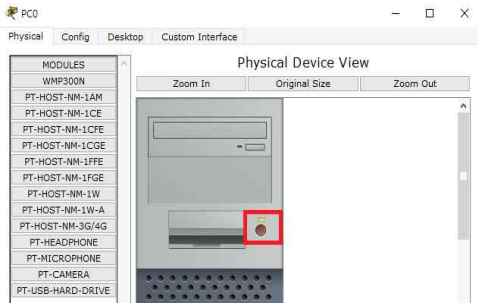


- ※ Copper Cross-Over : 크로스 케이블 (스위치 끼리 연결 or 스위치가 아닌 것끼리 연결)
- ※ 파란색 박스는 각 기기에 맞는 방식으로 자동으로 연결해줌

네트워크 장비 구축 및 기본 명령어 실습

기본 토폴로지 구성 연습 (5/7)

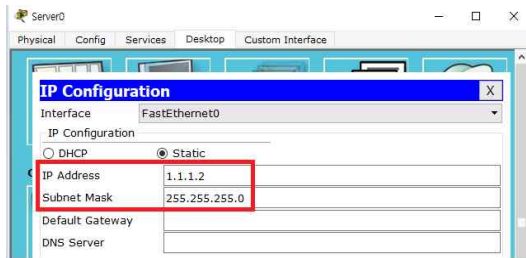
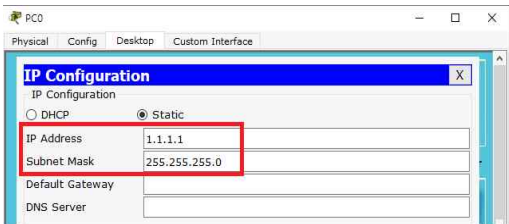
- PC와 서버를 각각 클릭하면 전원 버튼(초록색, 빨간색으로 ON/OFF 구분) 및 장착 가능한 모듈을 확인할 수 있음



네트워크 장비 구축 및 기본 명령어 실습

기본 토폴로지 구성 연습 (6/7)

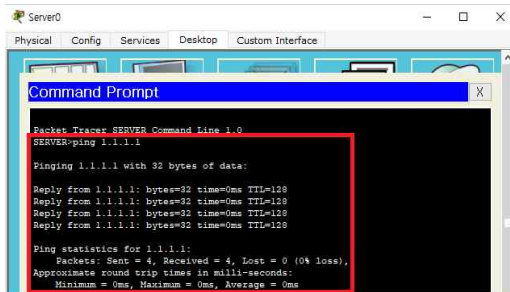
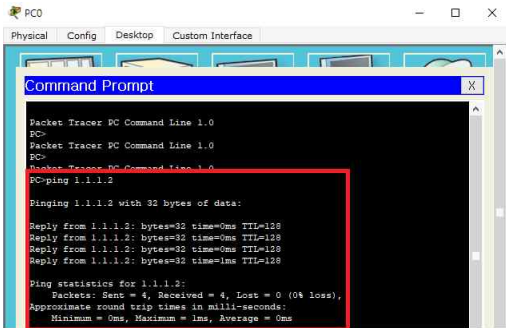
- 각 PC와 서버를 클릭하여 Desktop - IP Configuration을 클릭하여 IP 할당
- PC : IPv4 = 1.1.1.1, Subnet Mask = 255.255.255.0
- 서버 : IPv4 = 1.1.1.2, Subnet Mask = 255.255.255.0



네트워크 장비 구축 및 기본 명령어 실습

기본 토폴로지 구성 연습 (7/7)

- PC, 서버 각각 Desktop - Command Prompt 클릭
- ping 명령어로 상호간 통신 여부 확인 (PC : ping 1.1.1.2, 서버 : ping 1.1.1.1)



네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 기본 개념 (1/2)

- 라우터(Router) = 네트워크 라우터(Network Router)
- IP주소를 사용하여 네트워크 간의 데이터(패킷) 전송을 최적화된 경로로 수행하며, 이를 '라우팅'이라고 함
- 라우팅을 수행하려면 미리 라우팅 테이블에 네트워크 정보를 등록해야함



네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 기본 개념 (2/2)

- 스위치(Switch) : '같은 네트워크 내부'에서 데이터 전송을 수행하는 기기
- 스위치는 PC나 서버에 있어서 네트워크 입구에 해당하는 네트워크 기기
- 스위치는 MAC 주소를 사용하여 같은 네트워크의 LAN 포트 간 데이터 전송을 수행

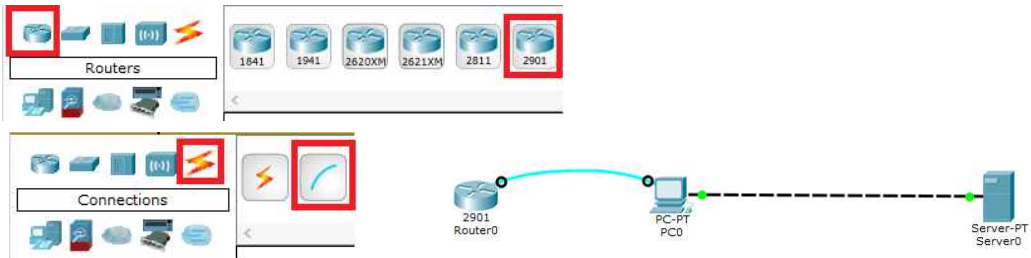


※ MAC(Media Access Control) : 물리적 주소, 12자리의 영어,숫자로 이루어져 있으며 장비마다 고유한 값을 가짐

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (1/28)

- 왼쪽 하단에 Network Devices - Routers - 2901을 드래그 앤 드롭
- 왼쪽 하단에 Connections - Console 선택하여 PC와 라우터를 연결
- 연결 시 PC의 RS-232와 라우터의 console 선택



※ Console : 물리적 케이블(직접 연결)

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (2/28)

- 라우터의 전원 ON/OFF 여부 확인



네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (3/28)

- 라우터의 전원이 꺼져있다면 전원을 켜서 장치 정상 동작여부 확인

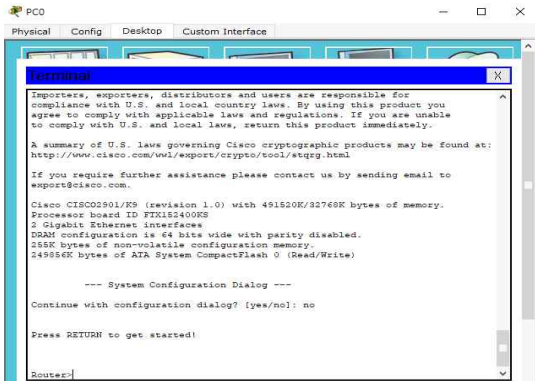
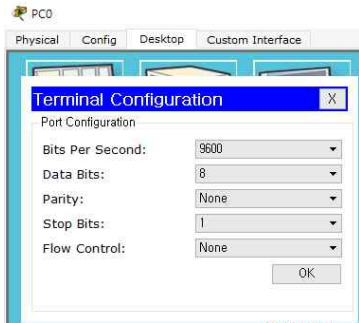
```
Digitally Signed Release Software  
program load complete, entry point: 0x81000000, size: 0x3bcd3d8  
Self decompressing the image :  
##### [OK]
```

```
--- System Configuration Dialog ---  
  
Continue with configuration dialog? [yes/no]: no  
  
Press RETURN to get started!  
  
Router>|
```


네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (4/28)

- PC를 클릭하여 Desktop - Terminal 클릭후 설정 내용을 확인하고 OK를 누르면 라우터의 CLI 모드로 접속됨



네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (5/28)

- enable(혹은 en) 명령을 이용하여 관리자 모드로 전환
- 라우터에 처음 접속하면 사용자 모드로 접속되며 사용자 모드는 제한적인 명령어만 사용가능

```
Router>enable  
Router#
```

```
Router>en  
Router#
```

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (6/28)

- configure terminal(혹은 conf t) 명령을 이용하여 라우터 전역 설정 모드 접근
- 라우터의 직접적인 설정이 가능

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

※ configure = config = conf : 설정

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (7/28)

- ? 명령을 이용하여 사용 가능한 명령어 확인

```
Router#?
Exec commands:
  <1-99>      Session number to resume
  auto        Exec level Automation
  clear       Reset functions
  clock       Manage the system clock
  configure   Enter configuration mode
  connect     Open a terminal connection
  copy        Copy from one file to another
  debug       Debugging functions (see also 'undebug')
  delete      Delete a file
  dir         List files on a filesystem
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  erase       Erase a filesystem
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  mkdir       Create new directory
  more        Display the contents of a file
  no          Disable debugging informations
  ping        Send echo messages
  reload      Halt and perform a cold restart
  resume      Resume an active network connection
  rmdir       Remove existing directory
  send        Send a message to other tty lines
--More--
```

```
Router(config)#?
Configure commands:
  aaa          Authentication, Authorization and Accounting.
  access-list  Add an access list entry
  banner       Define a login banner
  boot         Modify system boot parameters
  cdp          Global CDP configuration subcommands
  class-map    Configure Class Map
  clock        Configure time-of-day clock
  config-register Define the configuration register
  crypto       Encryption module
  do           To run exec commands in config mode
  dot11        IEEE 802.11 config commands
  enable       Modify enable password parameters
  end          Exit from configure mode
  exit         Exit from configure mode
  flow         Global Flow configuration subcommands
  hostname     Set system's network name
  interface    Select an interface to configure
  ip           Global IP configuration subcommands
  ipv6         Global IPv6 configuration commands
  key          Key management
  license      Configure license features
```

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (8/28)

- show clock : 시간 확인
- clock set hh:mm:ss day month year

```
Router#show clock
*0:19:49.671 UTC Mon Mar 1 1993
Router#clock set 13:00:00 1 march 2023
Router#show clock
*13:0:3.392 UTC Wed Mar 1 2023
```

※ show : 설정 확인

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (9/28)

- 기기 이름 설정 : configure terminal 입력 후 hostname 변경할 이름

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Lim-Teacher
Lim-Teacher(config)#
```

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (10/28)

- 라우터에서 설정 가능한 암호 종류
- Console Password : 사용자 모드(>)에 들어가기 전에 물어보는 암호
- Enable Password : 사용자 모드(>)에서 관리자 모드(#)로 들어갈때 물어보는 암호(평문)
- Enable Secret : Enable Password보다 강력한 암호(우선순위가 더 높음, 암호화)
- VTY(Virtual Terminal) password : Telnet으로 접속할 때 물어보는 암호(평문)

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (11/28)

- Console Password 설정
- configure terminal - line console 0 을 입력하여 콘솔 설정 모드에 접근
- password 패스워드
- login : 로그인시 패스워드 확인

```
Lim-Teacher#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Lim-Teacher(config)#line console 0
Lim-Teacher(config-line)#password cisco
Lim-Teacher(config-line)#login
Lim-Teacher(config-line)#exit
Lim-Teacher(config)#exit
Lim-Teacher#
%SYS-5-CONFIG_I: Configured from console by console

Lim-Teacher#
```


네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (12/28)

- 사용자 모드로 나가게 되면 패스워드를 물어보게 됨(입력한 값이 노출되지 않음)
- 방금 설정한 패스워드를 입력하여 사용자 모드 로그인 가능 여부를 확인

```
User Access Verification
```

```
Password:
```

```
Lim-Teacher>
```

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (13/28)

- Enable Password / Enable Secret 설정
- configure terminal로 라우터 전역 설정 모드 접근 후
- enable password 패스워드 : **평문** 형태로 저장
- enable secret 패스워드 : **암호화**되어 저장(enable password보다 우선순위가 높음)

```
Lim-Teacher>en
Lim-Teacher#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Lim-Teacher(config)#enable password cisco2
Lim-Teacher(config)#enable secret cisco3
Lim-Teacher(config)#
```

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (14/28)

- 사용자 모드 > 관리자 모드 진입시 방금 설정한 각각의 패스워드 확인
- enable password에 입력한 값으로는 관리자 모드 진입이 **불가능**
- enable secret에 입력한 값으로 관리자 모드 진입이 **가능**

```
Lim-Teacher>enable
Password:
Password:
Lim-Teacher#
Lim-Teacher#
```

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (15/28)

- VTY(Virtual Terminal) Password 설정
- configure terminal로 라우터 전역 설정 모드 접근 후
- line vty 0 4
- password 패스워드
- login

```
Lim-Teacher#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Lim-Teacher(config)#line vty 0 4
Lim-Teacher(config-line)#password telnet
Lim-Teacher(config-line)#login
Lim-Teacher(config-line)#exit
Lim-Teacher(config)#exit
Lim-Teacher#
%SYS-5-CONFIG_I: Configured from console by console

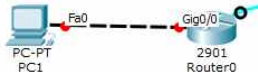
Lim-Teacher#
```

※ line vty 0 4 : Virtual line을 0~4번까지 총 5개 설정(최대 5개까지 동시 접속 가능)

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (16/28)

- IP 주소 할당
- configure terminal로 라우터 전역 설정 모드 접근 후
- interface 인터페이스이름 : GigabitEthernet이면 Gig0/0, FastEthernet이면 Fa0/0
- ip address IP주소 서브넷마스크



```
Lim-Teacher#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Lim-Teacher(config)#interface Gig0/0
Lim-Teacher(config-if)#ip address 1.1.1.3 255.255.255.0
Lim-Teacher(config-if)#exit
Lim-Teacher(config)#exit
Lim-Teacher#
%SYS-5-CONFIG_I: Configured from console by console

Lim-Teacher#
```

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (17/28)

- 할당한 ip를 활성화 하려면 인터페이스에서 no shutdown을 입력

```
Lim-Teacher#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Lim-Teacher(config)#interface Gig0/0
Lim-Teacher(config-if)#no shutdown

Lim-Teacher(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

Lim-Teacher(config-if)#exit
Lim-Teacher(config)#exit
Lim-Teacher#
%SYS-5-CONFIG_I: Configured from console by console

Lim-Teacher#
```

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (18/28)

- 인터페이스에 설명(Description) 정의
- configure terminal로 라우터 전역 설정 모드 접근 후 설명을 기입할 인터페이스에 접근
- description 설명문

```
Lim-Teacher#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Lim-Teacher(config)#interface Gig0/0
Lim-Teacher(config-if)#description 1st-Router
Lim-Teacher(config-if)#exit
Lim-Teacher(config)#exit
Lim-Teacher#
%SYS-5-CONFIG_I: Configured from console by console

Lim-Teacher#
```

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (19/28)

- 인터페이스 상태, IP주소 할당 현황 확인
- 관리자 모드(#)에서 show ip interface brief
- Status : 물리적인 활성화 여부(no shutdown = up)
- Protocol : 논리적인 활성화 여부(제대로 연결이 되어있으면 up)

```
Lim-Teacher#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0       1.1.1.3         YES manual up           up
GigabitEthernet0/1       unassigned      YES unset   administratively down down
Vlan1                    unassigned      YES unset   administratively down down
Lim-Teacher#
```


네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (20/28)

- 기기 설정 현황 전체 조회
- show running-config

```
Lim-Teacher#show running-config
Building configuration...

Current configuration : 760 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Lim-Teacher
!
!
enable secret 5 $1$mERz$DDLxK21ZSsG6Xb6b90AHH/
enable password cisco2
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2901/K9 sn FTX15245929
```

```
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
description 1st-Router
ip address 1.1.1.3 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
```

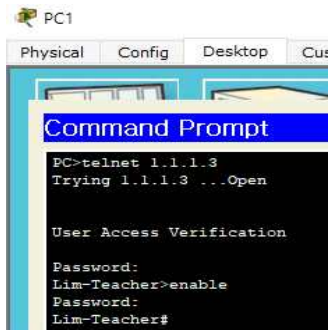
```
line con 0
password cisco
login
!
line aux 0
!
line vty 0 4
password telnet
login
!
!
!
end

Lim-Teacher#
```

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (21/28)

- VTY 접속 확인
- 라우터에 연결된 PC의 Command Prompt에서 Telnet 명령어를 통해 라우터에 접근
- Telnet 라우터IP주소
- 기존 VTY 패스워드로 로그인 성공여부 확인



네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (22/28)

- CLI에서 명령어를 잘못 입력하거나 장치의 이름을 잘못 입력할 경우 DNS 서버를 찾아 해결하려고 함
- 취소하려면 ctrl + shift + 6을 누르거나 configure terminal로 라우터 전역 설정 모드 접근 후 no ip domain-lookup을 입력하여 불필요한 실행 요청을 방지

```
Lim-Teacher#aaaaaaa
Translating "aaaaaaa"...domain server (255.255.255.255) % Name lookup aborted
Lim-Teacher#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Lim-Teacher(config)#no ip domain-lookup
Lim-Teacher(config)#exit
Lim-Teacher#
%SYS-5-CONFIG_I: Configured from console by console

Lim-Teacher#aaaaaaa
Translating "aaaaaaa"
% Unknown command or computer name, or unable to find computer address

Lim-Teacher#
```

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (23/28)

- show version : 라우터 버전 확인

```
Lim-Teacher#show version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M4,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
```

```
ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco2901 uptime is 14 hours, 6 minutes, 35 seconds
System returned to ROM by power-on
System image file is "flash0:c2900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload
```

```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
```

```
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
--More-- |
```

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (24/28)

- 라우터에 저장되어 있는 모든 사용자 모드 비밀번호에 대해 암호화 적용
- configure terminal로 라우터 전역 설정 모드 접근 후 service password-encryption 입력

```
enable secret 5 $1$mERr$DDLuXZ1ZSsG6Xb6b90AHH/  
enable password cisco2
```



```
enable secret 5 $1$mERr$DDLuXZ1ZSsG6Xb6b90AHH/  
enable password 7 0822455D0A1657
```

```
Lim-Teacher#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Lim-Teacher(config)#service password-encryption  
Lim-Teacher(config)#exit  
Lim-Teacher#  
%SYS-5-CONFIG_I: Configured from console by console  
  
Lim-Teacher#
```

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (25/28)

- show ? : 여러가지 show 명령어를 확인할 수 있음

```
Lim-Teacher#show ?
aaa                Show AAA values
access-lists       List access lists
arp                Arp table
cdp                CDP information
clock              Display the system clock
controllers        Interface controllers status
crypto             Encryption module
debugging          State of each debugging option
dhcp               Dynamic Host Configuration Protocol status
dot11              IEEE 802.11 show information
file               Show filesystem information
flash:             display information about flash: file system
flow               Flow information
frame-relay        Frame-Relay information
history            Display the session command history
hosts              IP domain-name, lookup style, nameservers, and host table
interfaces         Interface status and configuration
ip                 IP information
ipv6               IPv6 information
license            Show license information
line               TTY line information
logging            Show the contents of logging buffers
--More-- |
```

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (26/28)

- show protocols : 현재 설정되어 있는 프로토콜 확인

```
Lim-Teacher#show protocols
Global values:
  Internet Protocol routing is enabled
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 1.1.1.3/24
GigabitEthernet0/1 is administratively down, line protocol is down
Vlan1 is administratively down, line protocol is down
Lim-Teacher#
```

- show flash : 플래시 메모리 정보 확인

```
Lim-Teacher#show flash

System flash directory:
File   Length  Name/status
  3    33591768  c2900-universalk9-mz.SPA.151-4.M4.bin
  2     28282   sigdef-category.xml
  1     227537   sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (27/28)

- show interface : 모든 인터페이스 확인

```
Lim-Teacher#show interface
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 0060.708b.3701 (bia 0060.708b.3701)
  Description: 1st-Router
  Internet address is 1.1.1.3/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    136 packets input, 5529 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 watchdog, 1017 multicast, 0 pause input
  --More-- |
```


네트워크 장비 구축 및 기본 명령어 실습

라우터, 스위치 구축 및 기본 설정 (28/28)

- show user : 현재 접속하고 있는 user들 확인

```
Lim-Teacher#show user
```

Line	User	Host(s)	Idle	Location
* 0 con 0		idle	00:00:00	
390 vty 0		idle	00:00:10	1.1.1.1

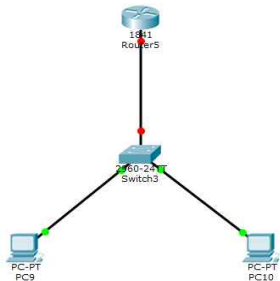
Interface	User	Mode	Idle	Peer Address
Lim-Teacher#				

※ '*'은 현재 내가 접속중인 기기

네트워크 장비 구축 및 기본 명령어 실습

DHCP 설정 (1/5)

- DHCP (Dynamic Host Configuration Protocol) : IP주소 자동 할당, 관리
- 아래와 같이 네트워크 기본 토폴로지 구성(각 기기의 이름은 무시)



네트워크 장비 구축 및 기본 명령어 실습

DHCP 설정 (2/5)

- 라우터에 IP 할당(100.0.0.1/24)

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fa0/0
Router(config-if)#ip address 100.0.0.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up

Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
_
```



네트워크 장비 구축 및 기본 명령어 실습

DHCP 설정 (3/5)

- configure terminal로 라우터 전역 설정 모드 접근 후 아래 내용처럼 입력
- ip dhcp excluded-address : DHCP설정시 제외할 주소(라우터ip 제외)
- ip dhcp : DHCP 이름 설정
- network : DHCP로 할당되는 IP주소 및 대역 설정
- dns-server : DNS서버 주소
- default-router : 기본 게이트웨이

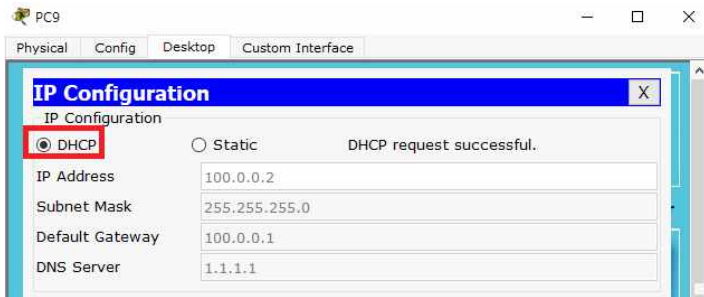
```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp excluded-address 100.0.0.1
Router(config)#ip dhcp pool dhcptest
Router(dhcp-config)#network 100.0.0.0 255.255.255.0
Router(dhcp-config)#dns-server 1.1.1.1
Router(dhcp-config)#default-router 100.0.0.1
Router(dhcp-config)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

네트워크 장비 구축 및 기본 명령어 실습

DHCP 설정 (4/5)

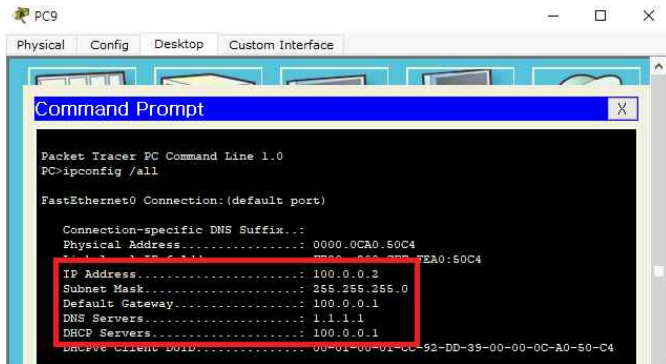
- 연결된 PC에서 DHCP를 이용한 IP 자동할당이 이루어지도록 설정 변경
- Desktop - IP Configuration - DHCP를 클릭하면 자동으로 설정이 변경됨



네트워크 장비 구축 및 기본 명령어 실습

DHCP 설정 (5/5)

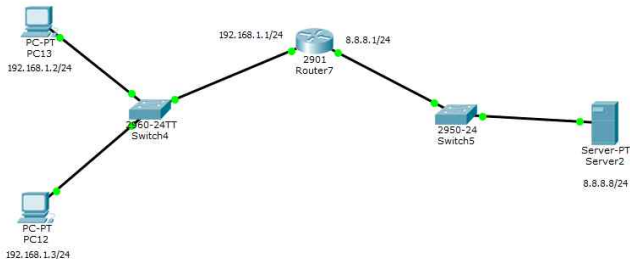
- Command Prompt에서 ipconfig /all로 구체적인 내용 확인 가능



네트워크 장비 운영 및 보안 설정

NAT 설정 (1/6)

- 아래와 같이 네트워크 기본 토폴로지 구성(각 기기의 이름은 무시)
- ip주소,서브넷 마스크, 기본 게이트웨이 주소까지 다음과 같이 설정



네트워크 장비 운영 및 보안 설정

NAT 설정 (2/6)

- 관리자 모드의 configure terminal로 라우터 전역 설정 모드 접근 후
- 사설 ip쪽(192.168.1.1)이 내부망이 되도록 ip nat inside를 입력
- 공인 ip쪽(8.8.8.1)이 외부망이 되도록 ip nat outside를 입력

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gig0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface gig0/0
Router(config-if)#ip nat outside
Router(config-if)#
Router(config-if)#exit
Router(config)#
```


NAT 설정 (3/6)

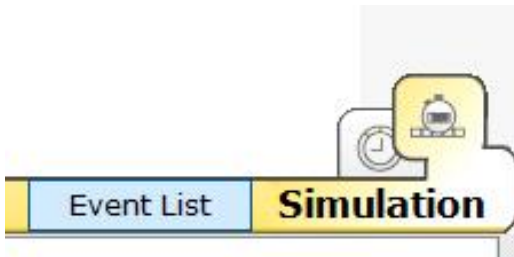
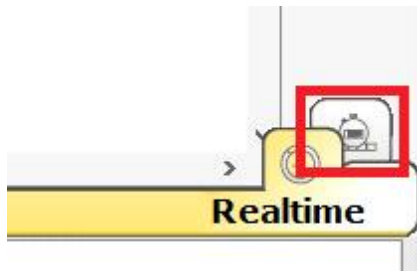
- 192.168.1.2 PC에 공인 ip인 8.8.8.1을 부여

```
Router(config)#ip nat inside source static 192.168.1.2 8.8.8.1
Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

NAT 설정 (4/6)

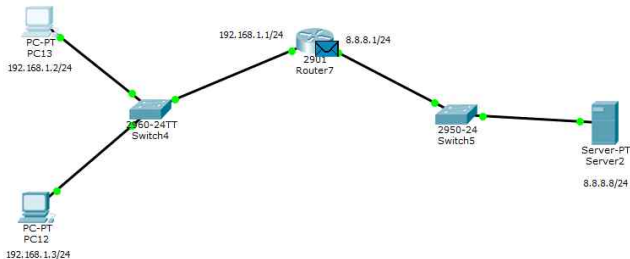
- 오른쪽 밑의 Realtime을 Simulation으로 변경



네트워크 장비 운영 및 보안 설정

NAT 설정 (5/6)

- 192.168.1.2의 PC - Desktop - Command Prompt에서 ping 8.8.8.8로 외부 서버에 ping 시도후 우측의 Capture/Forward로 라우터까지 진행



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC13	ICMP	
	0.001	PC13	Switch4	ICMP	
<input checked="" type="checkbox"/>	0.002	Switch4	Router7	ICMP	

Reset Simulation ☒ Constant Delay Captured to: 0.002 s

Play Controls

Back Auto Capture / Play **Capture / Forward**

네트워크 장비 운영 및 보안 설정

NAT 설정 (6/6)

- 메일이미지를 클릭후에 INBOUND의 SRC IP와 OUTBOUND의 SRC IP를 비교

PDU Information at Device: Router7

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 00D0.5853.2502		SRC MAC: 00E0.F7E5.3EA0	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 128			
ID: 0x17			0x0	0x0		
TTL: 128		PRO: 0x1	CHKSUM			
SRC IP: 192.168.1.2						
DST IP: 8.8.8.8						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

PDU Information at Device: Router7

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 0060.5C91.D665		SRC MAC: 00D0.5853.2501	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

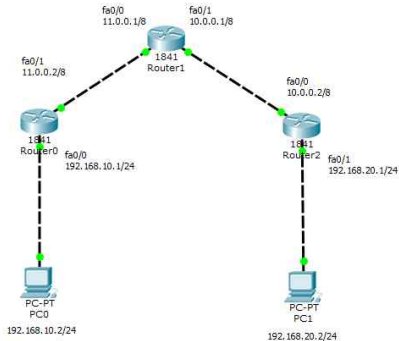
IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 128			
ID: 0x17		0x0	0x0			
TTL: 127		PRO: 0x1	CHKSUM			
		SRC IP: 8.8.8.1				
		DST IP: 8.8.8.8				
OPT: 0x0					0x0	
DATA (VARIABLE LENGTH)						

네트워크 장비 운영 및 보안 설정

VPN 설정 (1/8)

- VPN(Virtual Private Network) : 가상 사설 통신망
- 아래와 같이 네트워크 기본 토폴로지 구성
- ip주소, 서브넷 마스크, 기본 게이트웨이 주소까지 다음과 같이 설정



네트워크 장비 운영 및 보안 설정

VPN 설정 (2/8)

- 왼쪽 라우터에 다음과 같이 입력하여 라우팅을 설정

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 11.0.0.1
```

- 오른쪽 라우터에 다음과 같이 입력하여 라우팅

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.1
```

※ ip route : 라우팅(최적의 경로 설정) 명령어

VPN 설정 (3/8)

- 양쪽 라우터 모두 서로간에 ping 확인

```
Router#ping 10.0.0.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

```
Router#ping 11.0.0.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 11.0.0.2, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

네트워크 장비 운영 및 보안 설정

VPN 설정 (4/8)

- 왼쪽 라우터에 가상 ip가 172.16.1.1/16인 터널을 설정

```
Router#conf t
Enter configuration commands one per line. End with CNTL/Z.
Router(config)#int tunnel 10

Router(config-if)#
%LINK-5-CHANGED: Interface Tunnel10, changed state to up

Router(config-if)#ip add 172.16.1.1 255.255.0.0
Router(config-if)#tunnel source fa0/1
Router(config-if)#tunnel destination 10.0.0.2
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel10, changed state to up

Router(config-if)#no sh
```


네트워크 장비 운영 및 보안 설정

VPN 설정 (5/8)

- 오른쪽 라우터에 가상 ip가 172.16.1.2/16인 터널을 설정

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config) int tunnel 10

Router(config-if)#
%LINK-5-CHANGED: Interface Tunnel10, changed state to up

Router(config-if) ip addr 172.16.1.2 255.255.0.0
Router(config-if) tunnel source fa0/0
Router(config-if) tunnel destination 11.0.0.2
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel10, changed state to up

Router(config-if)#no sh
```

네트워크 장비 운영 및 보안 설정

VPN 설정 (6/8)

- 양쪽 라우터 모두 서로간에 가상 ip로 ping 확인

```
Router#ping 172.16.1.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/7 ms
```

```
Router#ping 172.16.1.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

네트워크 장비 운영 및 보안 설정

VPN 설정 (7/8)

- 왼쪽 라우터에 다음과 같이 입력하여 라우팅을 설정 (가상ip를 중간경로로 설정)

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 192.168.20.0 255.255.255.0 172.16.1.2
```

- 오른쪽 라우터에 다음과 같이 입력하여 라우팅을 설정 (가상ip를 중간경로로 설정)

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 192.168.10.0 255.255.255.0 172.16.1.1
```

네트워크 장비 운영 및 보안 설정

VPN 설정 (8/8)

- 왼쪽 PC에서 오른쪽 PC로 ping과 tracert 명령어 실행

```
PC>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time=1ms TTL=126
Reply from 192.168.20.2: bytes=32 time=0ms TTL=126
Reply from 192.168.20.2: bytes=32 time=0ms TTL=126
Reply from 192.168.20.2: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>tracert 192.168.20.2

Tracing route to 192.168.20.2 over a maximum of 30 hops:

  0  1 ms    1 ms    0 ms    192.168.10.1
  1  0 ms    0 ms    0 ms    172.16.1.2
  2  1 ms    1 ms    0 ms    192.168.20.2

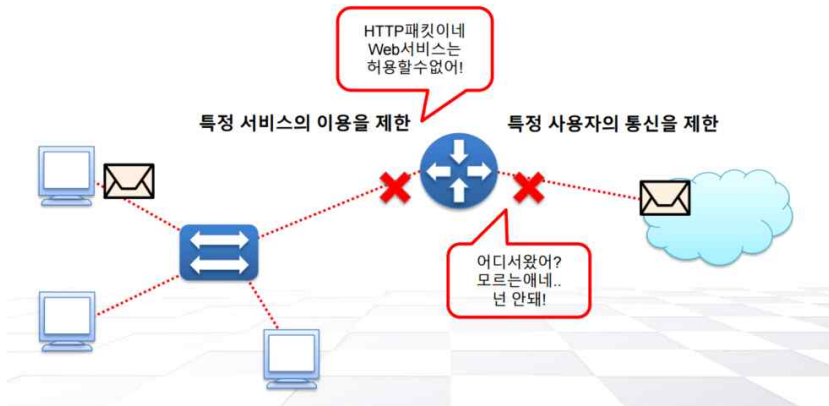
Trace complete.
```

ACL 설정 (1/15)

- ACL(Access Control List) : 접근 제어 목록
- 네트워크 트래픽 및 보안을 제공하기 위한 목적
- IP주소 or 특정 프로토콜 기반의 패킷 전달 여부를 통제 가능(패킷 필터링)
- 라우터를 통과하는 모든 패킷을 검사하여 ACL 부합 여부를 판단한 다음 패킷을 처리
- 네트워크 트래픽은 **들어오는(Inbound)** 트래픽과 **나가는(Outbound)** 트래픽이 있음

네트워크 장비 운영 및 보안 설정

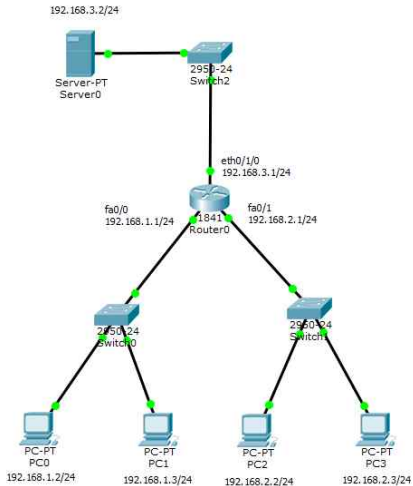
ACL 설정 (2/15)



네트워크 장비 운영 및 보안 설정

ACL 설정 (3/15)

- 아래와 같이 네트워크 토폴로지 구성



네트워크 장비 운영 및 보안 설정

ACL 설정 (4/15)

- 연결할 인터페이스가 부족할 경우 전원을 종료 한 후 상황에 맞는(WIC-1ENET) 추가 장비를 드래그 앤 드롭



네트워크 장비 운영 및 보안 설정

ACL 설정 (5/15)

- 와일드카드(Wildcard) 마스크
- ACL은 호스트의 범위를 결정하기 위해 IP 주소와 와일드카드 마스크를 사용
- 와일드카드 마스크는 서브넷 마스크의 반대
= 255.255.255.255 - 서브넷 마스크 = 와일드카드 마스크

Subnet Mask	Wildcard Mask
255.255.255.0	0.0.0.255
255.255.0.0	0.0.255.255
255.255.252.0	0.0.3.255
255.240.0.0	0.15.255.255

네트워크 장비 운영 및 보안 설정

ACL 설정 (6/15)

- 192.168.1.2에서 들어오는 패킷을 다음과 같은 방법으로 거부할 수 있음
- access-list 1 : 1번 ACL 생성
- ip access-group 1 in : 1번 ACL을 해당 인터페이스에 추가

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 1 deny 192.168.1.2 0.0.0.0
Router(config)#access-list 1 permit any
Router(config)#int fa0/0
Router(config-if)#ip access-group 1 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

ACL 설정 (7/15)

- 라우터에 설정된 ACL 리스트 확인
- 관리자 모드에서 show access-list 실행

```
Router#show access-list
Standard IP access list 1
    10 deny host 192.168.1.2
    20 permit any
Router#
```

네트워크 장비 운영 및 보안 설정

ACL 설정 (8/15)

- PC0(192.168.1.2)에서 다른 PC로 ping 테스트

```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=3ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

네트워크 장비 운영 및 보안 설정

ACL 설정 (9/15)

- 라우터에 설정된 ACL 삭제
- no access-list 삭제할 번호

```
Router#show access-list
Standard IP access list 1
  10 deny host 192.168.1.2
  20 permit any
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no access-list 1
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-list
Router#
```

네트워크 장비 운영 및 보안 설정

ACL 설정 (10/15)

- 192.168.1.2에서 서버로 FTP 프로토콜 요청을 거부 하도록 설정하는 방법
- 서버 - Services - FTP에서 Service가 On인지 확인
- On이라면 Username, Password 확인



ACL 설정 (11/15)

- PC0(192.168.1.2)에서 서버로 FTP 접속 테스트

```
PC>ftp 192.168.3.2
Trying to connect...192.168.3.2
Connected to 192.168.3.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

ACL 설정 (12/15)

- 라우터에서 100번 ACL로 FTP 프로토콜 요청을 차단하도록 설정
- access-list 100 deny tcp 출발지ip 목적지 ip eq 포트번호
- access-list 100 permit ip any any

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 100 deny tcp 192.168.1.2 0.0.0.0 192.168.3.2 0.0.0.0 eq
21
Router(config)#access-list 100 permit ip any any
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-list
Extended IP access list 100
  10 deny tcp host 192.168.1.2 host 192.168.3.2 eq ftp
  20 permit ip any any
Router#
```


ACL 설정 (13/15)

- fa0/0에 ACL 100번 적용

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

네트워크 장비 운영 및 보안 설정

ACL 설정 (14/15)

- PC0(192.168.1.2)에서 서버로 ping과 FTP 테스트

```
PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=7ms TTL=127
Reply from 192.168.3.2: bytes=32 time=0ms TTL=127
Reply from 192.168.3.2: bytes=32 time=1ms TTL=127
Reply from 192.168.3.2: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 2ms
```

```
PC>ftp 192.168.3.2
Trying to connect...192.168.3.2

%Error opening ftp://192.168.3.2/ (Timed out)

Packet Tracer PC Command Line 1.0
PC>(Disconnecting from ftp server)
```

ACL 설정 (15/15)

- ACL 작성 연습

1. 출발지 13.13.10.1에서 172.16.1.1의 FTP 서버로 접근하는 것을 차단하고
나머지 출발지 IP에서는 모두 허용하는 ACL 규칙을 110번으로 정의하시오
2. 출발지 30.44.22.0/24가 172.16.1.1의 FTP 서버로 접근하는 것을 허용하고
나머지 출발지 IP에서는 모두 거부하는 ACL 규칙을 120번으로 정의하시오
3. 외부 사용자가 인터넷을 통하여 172.16.1.1 서버로 telnet 접속하는 것을 차단하는
ACL을 130번으로 정의하시오
4. 13.13.10.0/24 사용자들이 172.16.1.0/24로 접근하는 것을 차단하고 나머지는 모두
허용하는 ACL을 140번으로 정의하고 Fa0/6포트에 해당 ACL 규칙을 적용하시오

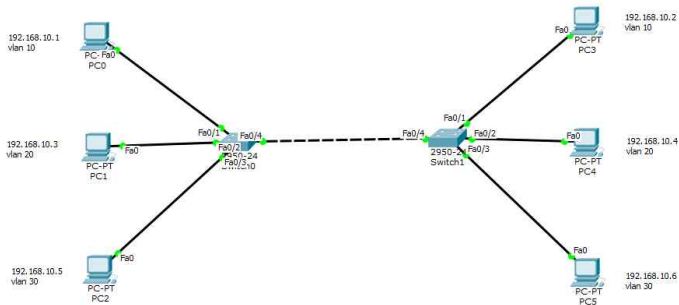
VLAN 설정 (1/7)

- VLAN(Virtual Local Area Network)
- 물리적 배치와 상관없이 **논리적으로** LAN을 구성할 수 있는 기술
- 주로 서버와 네트워크 트래픽에 대한 로드 밸런싱(Load Balancing)에 사용됨

네트워크 장비 운영 및 보안 설정

VLAN 설정 (2/7)

- 다음과 같이 네트워크 토폴로지 구성



VLAN 설정 (3/7)

- 양쪽 스위치에서 VLAN 생성
- vlan 번호 : vlan 생성
- name vlan이름 : vlan 이름 지정

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name vlan_10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name vlan_20
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name vlan_30
Switch(config-vlan)#exit
Switch(config)#
```

VLAN 설정 (4/7)

- 각 인터페이스에 해당하는 VLAN 설정
- 각 스위치 포트는 access모드로 사용 후 지정된 VLAN에 속한다고 선언해야함

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#
```

네트워크 장비 운영 및 보안 설정

VLAN 설정 (5/7)

- show vlan으로 VLAN이 제대로 만들어졌는지 확인

```
Switch#show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24
10 vlan_10	active	Fa0/1
20 vlan_20	active	Fa0/2
30 vlan_30	active	Fa0/3
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

--More-- |

네트워크 장비 운영 및 보안 설정

VLAN 설정 (6/7)

- 스위치를 통해 동일한 VLAN끼리 통신 설정
- conf t - switchport mode trunk 설정

Switch0

Physical Config CLI

IOS Command Line Interface

```
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/4
Switch(config-if)#switchport mode trunk

Switch(config-if)#
```

Switch1

Physical Config CLI

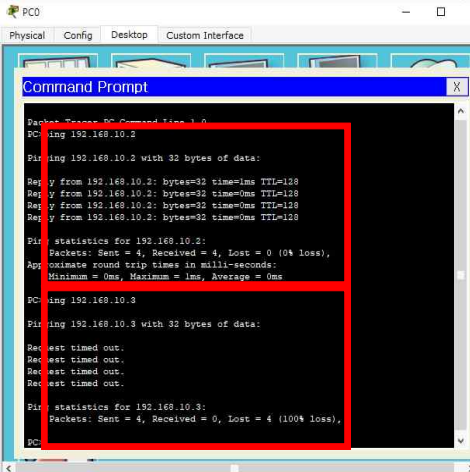
IOS Command Line Interface

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#
```

네트워크 장비 운영 및 보안 설정

VLAN 설정 (7/7)

- 동일한 VLAN으로 설정된 PC끼리 ping 테스트
(동일하지 않은 VLAN은 통신 불가)



The screenshot shows a Packet Tracer PC Command Prompt window for PC0. The window has tabs for Physical, Config, Desktop, and Custom Interface. The Command Prompt displays the following text:

```
PC>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time=0ms TTL=128
Reply from 192.168.10.2: bytes=32 time=0ms TTL=128
Reply from 192.168.10.2: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    PC>
```

A red rectangular box highlights the two ping test sections, indicating the successful communication with 192.168.10.2 and the failed communication with 192.168.10.3.

네트워크 장비 운영 및 보안 설정

라우터 설정 정보 저장 및 백업 (1/3)

- show running-config : RAM에 저장된 정보로서 현재 라우터에 설정된 값을 보여줌
- show startup-config : NVRAM에 저장된 정보로서 라우터에 초기 설정된 값을 보여줌

```
Router#show startup-config
startup-config is not present
Router#
```

※ NVRAM(non-volatile memory) : 비휘발성 메모리, 전원을꺼도 정보가 날아가지 않음

네트워크 장비 운영 및 보안 설정

라우터 설정 정보 저장 및 백업 (2/3)

- copy running-config startup-config로
running-config 정보를 NVRAM으로 저장
- 복사 후 show startup-config로 확인

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#show startup-config
Using 641 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKK7m0
enable password cisco
!
!
!
!
!
ip cef
no ipv6 cef
!
--More-- |
```

네트워크 장비 운영 및 보안 설정

라우터 설정 정보 저장 및 백업 (3/3)

- reload 명령 or 라우터 재부팅 후 설정값이 유지되는지 확인

```
R1#reload
Proceed with reload? [confirm]
System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Initializing memory for ECC
..
c2811 processor with 524288 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled

Readonly ROMMON initialized

Self decompressing the image :
#####
```

```
R1#show run
Building configuration...

Current configuration : 641 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbKX7m0
enable password cisco
!
!
!
!
!
ip cef
--More-- |
```

네트워크 취약점 진단

1. 네트워크 취약점 진단 개요 및 항목
2. 네트워크 취약점 진단 준비
3. 네트워크 취약점 진단 및 결과 분석

네트워크 취약점 진단 개요 및 항목

네트워크 취약점 진단 개요

- 라우터, 스위치 등 네트워크 장비를 통과하는 트래픽 처리 설정을 통해 공격을 당하지 않도록 보안 점검 항목을 정의하여 점검을 실시
- 취약점 점검 항목에 의해 현황을 파악하고 보안 기준에 부합하도록 설정을 유지하여 안정적인 서비스와 보안 위험을 사전 제거하는 것을 목적으로 함
- 장비 특성에 따라 점검방법 및 확인 사항이 달라질 수 있으나 사전 정의된 취약점 점검 항목을 바탕으로 점검이 이루어짐
- 취약점 점검은 계정관리, 접근관리, 패치관리, 기능관리 등으로 나누어 실시

네트워크 취약점 진단 개요 및 항목

네트워크 취약점 진단 항목 (1/5)

- 계정관리 : 시스템에 등록되어 있는 관리자 및 사용자 계정의 권한 오남용 여부, 패스워드의 안전한 설정 적용여부 등을 점검

분류	점검항목	항목 중요도	항목코드
1. 계정 관리	패스워드 설정	상	N-01
	패스워드 복잡성 설정	상	N-02
	암호화된 패스워드 사용	상	N-03
	사용자·명령어별 권한 수준 설정	중	N-15

네트워크 취약점 진단 개요 및 항목

네트워크 취약점 진단 항목 (2/5)

- 접근 관리 : 장비에 접근 IP 설정 등 장비 자체에 대한 접근통제 현황 점검

분류	점검항목	항목 중요도	항목코드
2. 접근 관리	VTY 접근(ACL) 설정	상	N-04
	Session Timeout 설정	상	N-05
	VTY 접속 시 안전한 프로토콜 사용	중	N-16
	불필요한 보조 입·출력 포트 사용 금지	중	N-17
	로그온 시 경고 메시지 설정	중	N-18

네트워크 취약점 진단 개요 및 항목

네트워크 취약점 진단 항목 (3/5)

- 패치 관리 : 장비별 최신 보안 패치 및 제조사 권고사항 적용 내역 점검

분류	점검항목	항목 중요도	항목코드
3. 패치 관리	최신 보안 패치 및 벤더 권고사항 적용	상	N-06

네트워크 취약점 진단 개요 및 항목

네트워크 취약점 진단 항목 (4/5)

- 기능 관리 : 장비를 통과하는
트래픽에 대하여 보안 설정 점검

분류	점검항목	항목 중요도	항목코드
5. 기능 관리	SNMP 서비스 확인	상	N-07
	SNMP community string 복잡성 설정	상	N-08
	SNMP ACL 설정	상	N-09
	SNMP 커뮤니티 권한 설정	상	N-10
	TFTP 서비스 차단	상	N-11
	Spoofing 방지 필터링 적용 또는 보안장비 사용	상	N-12
	DDoS 공격 방어 설정 또는 DDoS 장비 사용	상	N-13
	사용하지 않는 인터페이스의 Shutdown 설정	상	N-14
	TCP keepalive 서비스 설정	중	N-24
	Finger 서비스 차단	중	N-25
	웹 서비스 차단	중	N-26
	TCP/UDP Small 서비스 차단	중	N-27
	Bootp 서비스 차단	중	N-28
	CDP 서비스 차단	중	N-29
	Directed-broadcast 차단	중	N-30
	Source 라우팅 차단	중	N-31
	Proxy ARP 차단	중	N-32
	ICMP unreachable, Redirect 차단	중	N-33
	identd 서비스 차단	중	N-34
	Domain lookup 차단	중	N-35
	pad 차단	중	N-36
	mask-rely 차단	중	N-37
	스위치, 허브 보안 강화	하	N-38

네트워크 취약점 진단 준비

네트워크 취약점 진단 항목 (5/5)

- 라우터, 스위치 등 네트워크 장비 각각에 대한 running-config 파일 필요
- 네트워크 장비 설정의 근간이 되는 전체적인 설정 파일을 가져와야함
- 네트워크 장비에서 TFTP 서비스를 이용해 가져올 수 있으나 취약하다고 알려져 있어
보통은 네트워크 장비 운영자가 원격(Telnet 등)으로 접속하여 show running-config 명령
실행결과를 복사, 붙여넣기 과정을 통해 메모장 파일로 가져옴(수동)
- 가져온 config 내용이 PC에 저장되는 파일명은 라우터 이름(hostname), 가져온 날짜 등으로
명명하여 구분함(기준 없음)

네트워크 진단 및 결과 분석

네트워크 취약점 진단 계획서 작성

- 목적, 기간, 범위, 일정, 세부 수행계획, 절차, 추진계획 등
점검을 의뢰한 고객 입장과 점검자의 입장을 고려하여 명확하게 작성
- 보고서 품질을 생각하여 모호한 단어, 문장 사용을 최대한 지양하며
특히 **오탈자**와 같은 신뢰가 저해될 수 있는 요인들은 반드시 제거하여 작성

네트워크 진단 및 결과 분석

네트워크 취약점 수동 점검 및 결과분석

- 주요정보통신기반시설 취약점 분석 평가 및 상세가이드를 참고하여 취약점 항목별 양호/취약 여부 확인
- 제공받은 running-config 파일에 양호/취약 여부가 불명확한 경우 해당 항목들을 취합
- 네트워크 운영 담당자(팀장 등)와 직접 인터뷰 과정을 통하여 양호/취약 여부 판단
- (네트워크 장비 운영 담당자 직접 수행) 각 항목별 보안권고 사항 확인하여 취약점 조치
- 점검 결과에 따라 취약점을 제거하여 알려진 공격에 대비
- 취약점에 대한 조치 시 서비스 영향을 주지 않도록 조치 전에 반드시 서비스 영향도 분석 및 검토가 필요

네트워크 진단 및 결과 분석

네트워크 취약점 진단 결과보고서 작성

- 취약점 점검 의뢰를 한 담당자의 눈높이에 최대한 맞춰서 일목요연하게 작성
- 각 네트워크 장비별로 취약점 점검 항목들에 대한 양호/취약 여부를 한눈에 파악할 수 있도록 엑셀 및 함수 등을 활용하여 양호율에 대한 데이터 집계
- 전체적인 네트워크 취약점 진단 결과에 대한 총평 기재
- 도출된 취약점에 대한 보안권고문 작성