

## 제 2 장 네트워크보안

### 1. 네트워크 일반

#### 1.1 OSI 7 layer

##### 1.1.1 각 레이어의 의미와 역할

###### o 핵심가이드

- 물리층의 기능, 인터페이스와 전송매체의 물리적 특성, 프로토콜과 물리층에 해당하는 장비들에 대한 이해
- 데이터 링크층의 데이터 전송 기능과 물리적 주소지정 방식, 네트워크 토폴로지와 해당하는 장비들에 대한 이해
- 네트워크층은 두 시스템 간에 연결성과 경로 선택 기능 이해(논리적 주소지정)와 PC의 라우팅 프로토콜, 해당하는 장비들에 대한 이해
- 전송층은 서비스 지점 주소지정 이해, 신뢰성 있는 데이터 전송을 위한 기능 이해
- 세션층은 애플리케이션간에 세션을 구축하고 관리하며 종료 기능 이해
- 표현층은 데이터 변환, 암호화, 압축 등의 기능 이해
- 애플리케이션층의 기능 및 서비스들의 특징 이해

##### (1) 물리층(Physical Layer)

- o 물리계층은 네트워크 케이블과 신호에 관한 규칙을 다루고 있는 계층으로 상위 계층에서 보내는 데이터를 케이블에 맞게 변환하여 전송하고, 수신된 정보에 대해서는 반대의 일을 수행한다. 다시 말해서 물리계층은 케이블의 종류와 그 케이블에 흐르는 신호의 규격 및 신호를 송수신하는 DTE/DCE 인터페이스 회로와 제어순서, 커넥터 형태 등의 규격을 정하고 있다. 이 계층은 정보의 최소 단위인 비트 정보를 전송매체를 통하여 효율적으로 전송하는 기능을 담당한다.
- o 전송매체는 송신자와 수신자간에 데이터 흐름의 물리적 경로를 의미하며, 트위스트페어케이블, 동축케이블, 광섬유케이블, 마이크로파 등을 사용할 수 있다.

- 네트워크장비로는 허브, 리피터가 있다.
- 물리계층 프로토콜로는 X.21, RS-232C, RS-449/422-A/423-A 등

## (2) 데이터 링크층(데이터-link Layer)

- 데이터 링크층은 통신 경로상의 지점간 (link-to-link)의 오류없는 데이터 전송에 관한 프로토콜이다. 전송되는 비트의 열을 일정 크기 단위의 프레임으로 잘라 전송하고, 전송 도중 잡음으로 인한 오류 여부를 검사하며, 수신측 버퍼의 용량 및 양측의 속도 차이로 인한 데이터 손실이 발생하지 않도록 하는 흐름제어 등을 한다.
- 네트워크 토폴로지는 기본적으로 버스 토폴로지, 스타 토폴로지, 링 토폴로지, 메쉬 토폴로지, 혼성토폴로지 등이 있으며 네트워크를 구성하는 방법이 된다.
- 데이터 통신시스템에서 데이터를 송수신하기 위해서는 통신의 의사에 따른 상대방의 확인, 전송조건 및 오류에 대한 처리 등 다양한 전송링크 상에서 발생하는 문제들을 제어할 수 있는 기능이 필요하며 데이터전송 제어방식이라고도 하며 ISO/OSI 기본 모델에서 데이터링크 계층(Data link layer)의 기능에서 적용된다.
  - 회선제어 : 회선구성방식은 점대점 또는 멀티포인트회선 구성방식과 단방향, 반이중 및 양방향 등의 통신방식에 따라 사용되는 전송링크에 대한 제어 규범(line discipline)이다.
    - 점대점 회선 제어 : 스테이션 A에서 B로 데이터를 보내려고 할 때, 우선 A는 B의 수신가능 여부를 알기 위한 신호를 전송하여 질의한다. B에서는 이에 대한 응답이 준비되었으면, ACK(Acknowledgement)를 보내고, 준비가 되지 않았거나, 오류발생시, NAK(Non-Acknowledgement)를 전송한다. A에서 ACK를 받을 때 "회선의 설정"라고 한다. 회선이 설정되면 A는 데이터를 프레임의 형태로 전송하며, 이에 대한 응답으로 B는 ACK신호를 수신한 프레임의 번호와 함께 전송한다. 마지막으로, A가 데이터를 모두 보내고 B로부터 ACK를 받은 후, A는 시스템을 초기 상태로 복귀하고 회선을 양도하기 위해서 EOT(End Of Transfer)신호를 전송한다. 전송제어의 회선 제어의 단계는 회선설정단계, 데이터 전송 단계, 회선양도 단계 이다.
    - 멀티포인트 회선 제어 : 주스테이션(Master)과 부스테이션(Slave)간이 데이터 교환시 사용되는 회선 제어 규범이며 폴-선택(Poll-select)방식을 이용하여 설명하며, 폴(Poll)은 주스테이션이 부스테이션에게 전송할 데이터가 있는지의 여부를 묻는 것이고 선택트는 주스테이션이 부스테이션에게 보낼

데이터를 준비하고 난 후, 부스태이션에게 데이터를 전송할 것이라는 것을 알려 주는 것을 의미한다. 이 방식의 데이터 전송은 주스태이션에 의해서 폴과 선택 방식에 따라 주도적으로 이루어지는 방식이다.

- 흐름제어 (Flow Control) : 회선제어는 수신장치의 용량 이상으로 데이터가 넘치지 않도록 송신장치를 제어하는 기술이다. 즉, 수신장치가 이전에 받은 데이터를 자신의 버퍼에서 처리하기 전에 송신장치로부터 다른 데이터가 전송되지 않도록 하는 제어방식으로 정지-대기(Stop and Wait)기법, 윈도우 슬라이딩(Window Sliding)기법이 있다.

- 정지-대기 흐름제어기법 : 흐름 제어의 가장 간단한 방식으로, 송신장치에서 하나의 프레임을 한 번에 전송하는 방식으로 송신장치의 프레임 전송 후 수신장치로부터 ACK신호를 받을 때까지 다음 프레임을 보낼 수 없는 방식이다. 이것은 보통 한 개의 연속적인 블록 또는 프레임을 한 번에 사용되며 커다란 연속적인 프레임을 작은 구간으로 분리해서 전송해야 한다.

- 슬라이딩 윈도우기법 : 한 번에 여러 개의 프레임을 보낼 수 있는 방식으로, 수신측에 n개의 프레임에 대한 버퍼를 할당하고, 송신측에서 수신측의 ACK를 기다리지 않고 n개의 프레임을 보낼 수 있도록 하는 방식으로 이 방식에서는 송수신의 흐름을 위해서 각 프레임에 순서번호(Sequence Number)를 부여한다. 이것은 수신측에서 기대하는 다음 프레임의 순서번호를 포함하는 ACK를 송신측으로 보내줌으로서 계속 받을 수 있는 프레임들의 번호를 알려준다(Acknowledge).

- 오류제어 : 여러 가지 원인(전원, 주파수혼란, 감쇠, 잠음등)으로 인해 전송된 데이터의 발생할 수 있는 오류에 대한 해결을 위한 제어방식이다.

- 후진 오류 수정방식(Backward error Correction) : 오류 발생시 재전송이 요구하는 방식으로 송신측에서 데이터 전송 시 오류를 검출할 수 있는 정도의 부가정보를 함께 전송하고 수신측에서 이를 이용하여 오류를 검출하여 오류의 발생여부를 알고 송신측에게 데이터의 재전송을 요구하는 방식이다. 이를 위해서 후진 오류 수정방식에서는 오류의 검출방식과 재전송 기법이 필요하다. 오류 검출 방식은 패리티 검사, 블록합 검사, 순환잉여 검사등이 있으며, 오류 검출 후 재전송 방식(ARQ : Automatic Repeat Request)으로는 정지-대기(Stop and Wait) ARQ방식, 연속 ARQ 방식 등이 있다.

- 전진 오류수정(Forward error Correction)방식 : 오류발생시 재전송이 불필요한 방식으로 송신측에서 데이터 송신 전송할 문자 또는 프레임에 부가정보를 함께 전송하고, 수신측에서 오류발생시 이 부가정보를 이용하여 오류

의 검출 및 정확한 정보로의 유출이 가능한 방식이다.

- HDLC, CSMA/CD, ADCCP, LAP-B 등이 데이터 링크 계층 프로토콜의 예이다.
- CSMA/CD 방식은 데이터를 송신하려는 클라이언트가 네트워크상에 다른 컴퓨터가 통신하고 있는지를 조사해 신호가 송출되고 있지 않을 시 데이터를 전송하는 구조다. 동시에 여러 노드에서 데이터를 전송할 경우 충돌이 발생한다. CSMA/CD는 이 충돌을 감시하는데, 충돌이 발생한 경우에는 일정 시간 갖고 있다가 다시 신호를 보내 통신을 제어한다.
- 네트워크장비로는 브리지, 스위치가 있다.

### (3) 네트워크층(Network Layer)

- 네트워크층은 패킷이 송신측으로부터 수신측에 이르기까지의 경로를 설정해주는 기능과 너무 많은 패킷이 한쪽 노드에 집중되는 병목 현상을 방지하기 위한 밀집제어 (Congest control) 기능을 수행한다. 또한 이질적인 네트워크를 연결하는 데서 발생하는 프레임의 크기나 주소 지정방식이 다른 데서 발생하는 문제를 극복해 주는 기능을 수행한다.
- 네트워크층은 IP 프로토콜이 동작하면서 IP헤더를 삽입하여 패킷을 생성하며 송신자와 수신자간에 연결을 수행하고 수신자까지 전달되기 위해서는 IP헤더 정보를 이용하여 라우터에서 라우팅이 된다.
- IP, X.25 등이 네트워크 계층 프로토콜의 예이다.
- 네트워크장비로는 라우터가 있다.

### (4) 전송층(Transport Layer)

- 전송층은 수신측에 전달되는 데이터에 오류가 없고 데이터의 순서가 수신측에 그대로 보존되도록 보장하는 연결 서비스의 역할을 하는 종단간(end-to-end) 서비스 계층이다. 한편, 패킷의 순서에 무관하게 수신되며, 에러 처리도 하지 않는 비연결 서비스 (Connectionless service)와 다중 목적지에 메시지를 전송하는 서비스도 있다. TCP 와 UDP 는 각각 연결지향 및 비연결지향 트랜스포트 프로토콜의 예이다.
- 전송층은 TCP 헤더를 삽입하여 패킷을 만들고 이 정보를 이용하여 서비스간에 통신을 가능하게 한다.

(5) 세션층(Session Layer)

- o Session Layer는 두 응용프로그램(Applications) 간의 연결설정, 이용 및 연결해제 등 대화를 유지하기 위한 구조를 제공한다. 또한 분실 데이터의 복원을 위한 동기화 지점(sync point) 을 두어 상위 계층의 오류로 인한 데이터 손실을 회복할 수 있도록 한다.

(6) 표현층(Presentation Layer)

- o Presentation Layer전송되는 정보의 구문 (syntax) 및 의미 (semantics)에 관여하는 계층으로, 부호화 (encoding), 데이터 압축 (compression), 암호화 (cryptography) 등 3가지 주요 동작을 수행한다. ANSI.1, XDR 등이 프로토콜의 예이다.

(7) 애플리케이션층(Application Layer)

- o Application Layer네트워크 이용자의 상위 레벨 영역으로, 화면배치, escape sequence 등을 정의하는 네트워크 가상 터미널 (network virtual terminal), 파일전송, 전자우편, 디렉토리 서비스 등 하나의 유용한 작업을 할 수 있도록 한다.

1.1.2 각 계층별 네트워크 장비의 정의 등

o 핵심가이드

- 네트워크층에 해당하는 장비로는 라우터와 멀티 레이어 스위치가 해당되며 기능 및 동작원리 이해
- 데이터링크층에 해당하는 장비로는 브리지와 스위치가 있으며 기능 및 동작원리 이해
- 물리층에 해당하는 장비로는 허브와 케이블과 커넥터 등이 있으며 허브에 대한 기능 및 동작원리 이해
- 케이블과 커넥터에 대한 주요 사항 이해

(1) 각 계층의 기능을 수행하는 장비들에 대해 학습

- o 라우터는 리피터와 브릿지, 허브가 비교적 근거리에서 네트워크(LAN)를 통합하

거나 분리하기 위해서 사용하는 반면, 라우터는 원거리에서 네트워크간 통합을 위해서 사용되는 장비이다. 라우터를 이용해서 거미줄처럼 얽혀있는 인터넷상에서 원하는 목적지로 데이터를 보낼 수 있으며, 원하는 곳의 데이터를 가져올 수도 있다.

○ 멀티 레이어 스위치

- 멀티 레이어 스위치는 스위치 자체가 레이어2 장비이었는데 비하여 상위 계층으로 점점 올라가면서 TCP, UDP 등의 프로토콜에 대한 컨트롤 역할을 수행하게 되면서 트래픽 제어 등의 기능이 추가되었다.
- L2(Layer 2) 스위치를 그냥 스위치라고 부르며, L3 스위치는 허브와 라우터의 역할, 즉 스위칭허브에 라우팅 기능을 추가한 장비이고 L4 스위치는 서버나 네트워크의 트래픽을 로드밸런싱하는 기능을 포함한 장비이다.

○ 브리지

- 브리지는 하나의 네트워크 세그먼트를 2개 이상으로 나누어서 관리하기 위해서 만들어진 장비이다. 하나로 통합해서 관리하기 위한 허브와 비교될 수 있다. 동일한 지역 네트워크에 있는 부서에서 호스트들을 2개로 분리하여 상호 영향을 미치지 않도록 하기 위해서 사용된다.

○ 스위치

- 스위치는 일반적으로 스위칭 허브를 말하며, 더미 허브의 가장 큰 문제점인 LAN을 하나의 세그먼트로 묶어버린다는 점을 해결하기 위해서 세그먼트를 여러 개로 나누어준다. A 호스트에서 B 호스트로 패킷을 보내려고 할 때, 더미허브는 허브에 연결된 모든 호스트에 패킷을 복사해서 보내지만 스위칭 허브는 B 호스트에게만 패킷을 보낸다. 스위칭 허브는 MAC주소를 이용해서 어느 세그먼트로 패킷을 보내야할지를 결정할 수 있으며 이를 위해서 맥 테이블(MAC table)을 메모리에 저장하여 기능을 수행한다.

○ 허브

- 허브는 일반적으로 더미 허브(dummy hub) 말하며, 허브 본래의 목적에 충실한 허브이다. A 호스트가 B 호스트에게 메시지를 보내고자 할때, 메시지는 허브로 전달되고, 허브는 허브에 연결된 모든 호스트에게 메시지를 전달한다. 만일 수신자가 아닌 호스트가 메시지를 받은 경우 자신에게 보내어진 패킷이 아니라면 이 패킷은 버려지게 되고, 그렇지 않을 경우 최종적으로 애플리케이션 계층까지 전달되게 될 것이다.

○ 리피터

- LAN 영역에서 다른 LAN 영역을 서로 연결하기 위한 목적으로 사용된다. 2

개의 LAN 영역을 하나의 LAN 영역으로 통합하고자 할 때 발생하는 문제는 데이터가 전달되어야 하는 망이 길어진다는 문제가 있는데 이에 따라서 데이터 전송매체인 전기적 신호가 감쇠되거나 잡음이 생길 수 있으므로 신호감쇠와 잡음을 처리하기 위한 장치를 필요로 하게 된다. 이러한 일을 해주는 네트워크 세그먼트간 연결장치가 리피터이다.

## 1.2 TCP/IP 일반

### 1.2.1 IP Addressing

#### o 핵심가이드

- TCP/IP 프로토콜 개념 이해 및 IP 어드레싱 이해
- IP 주소할당 방식, 구조 클래스 개념 이해
- IPv6의 특징과 유니캐스트, 애니캐스트, 멀티캐스트 이해

#### (1) IP 주소의 기본 개념

- o TCP/IP 프로토콜은 1960년대 후반 이기종 컴퓨터간의 원활한 데이터통신을 위해 미 국방성에서 개발한 통신 프로토콜이다. TCP/IP는 취약한 보안 기능 및 IP주소 부족은 제한성에도 불구하고 전세계적으로 가장 널리 사용하는 업계 표준 프로토콜이며 현재는 거의 모든 컴퓨터가 이 프로토콜을 기본으로 제공되는 인터넷 표준 프로토콜이다.

OSI 7 계층	TCP/IP 프로토콜	계층별 프로토콜
애플리케이션 계층	애플리케이션 계층	Telnet, FTP, SMTP, DNS, SNMP
프로젠테이션 계층		
세션 계층	트랜스포트 계층	TCP, UDP
트랜스포트 계층	인터넷 계층	IP, ICMP, ARP, RARP, IGMP
네트워크 계층	네트워크 인터페이스 계층	Ethernet    Token Ring    Frame Relay    ATM
데이터링크 계층		
물리적 계층		

(그림 2-1) OSI 7계층과 TCP/IP 프로토콜

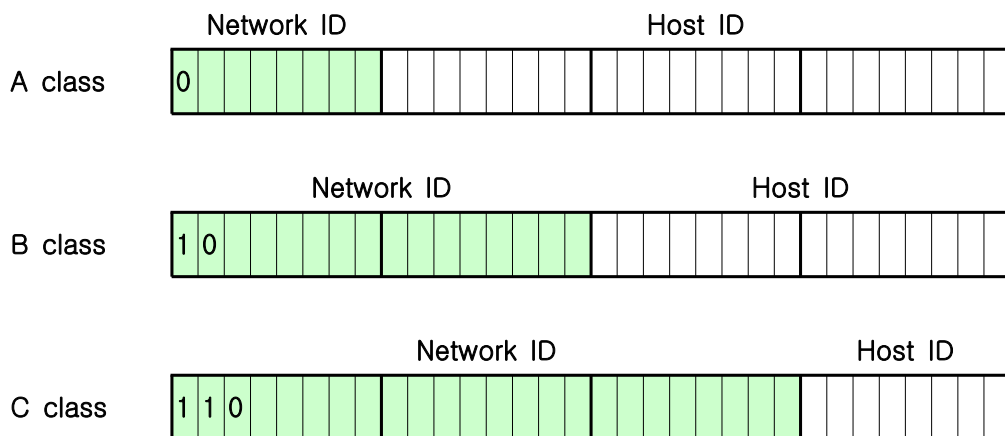
- o IP 주소는 네트워크 계층의 주소로써 유일한 IP 주소는 각 호스트와 TCP/IP를 이용하여 통신을 수행하는 모든 네트워크 컴퍼넌트에 필요하다. IP 주소는 마치 집주소를 이용하여 집을 찾는 것과 같은 방식으로 네트워크 상에서 특정 시스템의 위치를 찾는다. IP 주소는 32bit로 구성되고 네트워크 ID와 호스트 ID로 구성되며 네트워크 ID는 IP 라우터에 의해 묶여져 있는 동일한 물리적 네트워크에 존재하는 시스템을 구분한다. 동일한 물리적 네트워크상에 존재하는 모든 시스템은 반드시 동일한 네트워크 ID를 가져야 한다. 그리고, 외부망에서는 네트워크 ID는 반드시 유일해야 한다. 호스트 ID는 네트워크내에서 워크스테이션, 서버, 라우터, 기타 TCP/IP 호스트를 구분한다. 각 호스트의 주소는 반드시 네트워크 ID에 대해 유일해야 한다.
- o IP 어드레싱은 컴퓨터가 LAN을 통하여 연결된 상태에서 네트워크와 다른 네트워크 사이의 호스트간 통신이 용이하도록 설정하는 것으로 말할 수 있으며, 여기에는 IP, 넷마스크 등의 정보를 논리적으로 지정하여 부여하는 것도 포함하고 있다.

## (2) IP 주소지정

- o IANA는 전체 IP Address를 관리하며 ISP들에게 ISP(Internet Service Provider)를 발급하고, 일반 사용자들은 그러한 ISP로부터 IP를 할당받아서 호스트에게 할당하고 인터넷에 액세스하게 되는 것이다. 이 IP Address는 Class 라는 개념에 근거하여 관리되고 32비트를 4개의 8비트 영역(octet)으로 나누어 사용된다. 각 octet은 0-255의 범위를 가지는 10진수로 변경되고 마침표(".") 기호로 나누어져 있다.
- o 인터넷 공동체는 초기에 네트워크의 크기 별로 5개의 주소 클래스를 정의하였다. 주소의 클래스는 어떤 비트가 네트워크 ID로 사용되는지, 어떤 비트가 호스트 ID로 사용되는지를 정의하며 가능한 네트워크의 개수와 네트워크당 가능한 호스트의 개수를 정의 한다.
  - 클래스 A는 아주 많은 수의 호스트를 가지는 네트워크에 지정된다. 클래스 A 주소의 최상위 비트는 언제나 0으로 값이 지정된다. 나머지 7비트(첫번째 octet을 이루고 있는 7비트)는 네트워크 ID를 결정하게 된다. 나머지 24비트(마지막 3개의 octet)는 호스트 ID를 나타낸다. 결과적으로 클래스 A 주소는 126개의 네트워크와 각 네트워크마다 16,777,214개의 호스트를 지정할 수 있게 된다.



- 클래스 B는 중간 정도의 규모에서 대규모의 네트워크에 적용된다. 클래스 B의 주소 최상위 2 비트의 값은 언제나 이진수 1 0 로 지정된다. 그 다음 14비트는 네트워크 ID를 지정한다. 나머지 16비트는 호스트 ID를 나타낸다. 클래스 B는 16,384 개의 네트워크와 각 네트워크 별로 65,534 개의 호스트를 지정할 수 있다.
- 클래스 C는 소규모의 네트워크에 사용된다. 클래스 C 주소 최상의 3 비트는 언제나 이진수 1 1 0 로 값이 설정된다. 다음 21 비트는 네트워크 ID를 나타냅니다. 나머지 8비트 값은 호스트 ID를 나타냅니다. 클래스 C는 2,097,152개의 네트워크와 각 네트워크 별로 254개의 호스트를 지정할 수 있다.
- 클래스 D는 IP 멀티캐스트를 위해 사용되어 집니다. 클래스 D 주소의 최상위 4비트는 언제나 이진수 1 1 1 0으로 값이 지정된다. 나머지 비트는 관심 있는 호스트가 인식할 주소 값을 위해 사용된다. Microsoft 는 인터넷워크 상에서 데이터를 멀티캐스트 하는 애플리케이션을 위하여 클래스 D 주소를 지원한다.
- 클래스 E 앞으로 사용하기 위해 남겨둔 실험적인 영역이다 클래스 E 주소의 최상위 비트는 언제나 이진수 1 1 1 1로 지정되어 있다.



(그림 2-2) 클래스 구조

### (3) 차세대 인터넷 프로토콜(IPv6)

- o IPv6는 128 bit 주소체계를 사용하는 것으로 다음과 같은 배경에서 개발되었다.
  - IP 주소공간의 부족
  - IPv4 헤더 영역의 비효율적 사용 : 현재의 IPv4의 헤더의 경우 총 12개의 필

드로 구성되어져 있는데, 이중에서 Header Length, Identification, Flags, Fragment Offset, Header Checksum 총 5개의 필드가 IPv6에서는 삭제되어져 총 8개의 필드로 구성된다.

- 라우팅의 위기 : 라우터가 라우팅을 위해서는 송신자와 수신자간 데이터 전달을 하고 있지만 네트워크가 증가함에 따라서 효율성이 급격히 떨어지고 있으므로 현재에는 임시방편으로 CLIP(Class Less Interdomain Routing) 기술(클래스 개념이 아닌 도메인간의 라우팅 기술)을 사용하고 있다.

#### o IPv6의 특징

- 확장된 IP 주소공간 : IPv6는 128 비트 주소체계를 사용하므로 기존의 IPv4에 비해서 4배 이상 커졌다.
- 규모 조정이 가능한 라우팅 : IPv4의 문제점 중에 하나인 규모조정이 불가능한 라우팅 방법을 획기적으로 개선하는 것으로 사용하지 않는 IP에 대해 통제를 할 수 있다.
- 간략화된 헤더 포맷과 확장 헤더의 사용 : IPv6는 8개 필드로 구성된 헤더와 가변 길이 변수로 이루어진 확장 헤더 필드를 사용한다.
- 보안 : 보안과 인증 확장 헤더를 사용함으로써 인터넷 계층의 보안기능을 강화한다.

#### o IPv6의 주소형식 및 주소배정

- IPv6 주소는 총 128비트로 이루어져 있으며 상위 64비트는 네트워크 측면의 주소를, 하위 64비트는 호스트 측면의 주소를 나타낸다. IPv6 주소 형식은 기본적으로 TLA, NLA ID, SLA ID 그리고 인터페이스 ID 등의 네 개의 필드로 구성되어 있다. 주소 표현 방법은 128 비트를 16비트씩 8부분으로 나누어 각 부분을 ':'로 구분하고 실제 주소 값은 16진수로 표현할 수 있다.
- 애니캐스트(AnyCast) : 애니캐스트는 단일 송신자와 그룹 내에서 가장 가까운 곳에 있는 일부 수신자들 사이의 통신을 말한다. 이것은 단일 송신자와 다중 수신자 사이의 통신인 멀티캐스트, 그리고 단일 송신자와 네트워크 내의 단일 수신자 사이의 통신인 유니캐스트와 대비하여 존재한다. 애니캐스트는 한 호스트가 호스트 그룹을 위해 라우팅 테이블을 효과적으로 갱신할 수 있도록 하기 위해 설계되었다. IPv6는 어떤 게이트웨이 호스트가 가장 가까이 있는지를 결정할 수 있으며, 마치 유니캐스트 통신인 것처럼 그 호스트에 패킷을 보낼 수 있다. 그 호스트는 모든 라우팅 테이블이 갱신될 때까지, 그룹 내의 다른 호스트에게 차례로 애니캐스트할 수 있다. 애니캐스트 주소는 네트워크상에서 동시에 복수의 인터페이스에 주소 부여가 가능한 형태를 의미한다. 애니

캐스트 주소는 유니캐스트 주소와 동일한 포맷이다. 단 한가지 차이점은 여러 인터페이스가 특정 애니캐스트 주소에 할당될 수 있다는 것이며 그 인터페이스는 자신이 하나의 애니캐스트 주소를 가졌다는 것을 알도록 구성될 수 있다. 때문에 복수의 인터페이스에 애니캐스트 주소를 부여할 수 있는 것이다.

- 멀티캐스트(MultiCast) : 주소의 상위 Octet이 FF(11111111)값을 가짐으로써 유니캐스트 주소와 구별된다. 만약 패킷이 멀티캐스트 주소의 수신지로 보내지면 이 패킷은 라우팅을 통해 멀티캐스트 그룹의 모두에게 멀티캐스팅(Multicasting)된다. 멀티캐스트의 경우 멀티캐스트 주소공간의 어느 부분이 사용되느냐에 따라서 멀티캐스트 그룹은 서로 다른 범위를 지니게 된다.

## 1.2.2 서브네팅

### o 핵심가이드

- 서브네팅 개념 이해
- 서브네팅 마스크의 개념 및 장단점
- 각 클래스의 서브네팅 방법 이해

### (1) 서브네팅(subnet)의 개념

- o 서브네팅은 네트워크를 네트워크 세그먼트로 나눈 개별 네트워크를 말한다. 서브네트워크라고 해서 일반적인 네트워크 보다 미약한 기능을 제공한다는 의미는 아니며, 각각의 서브네팅들이 모여 하나의 논리적인 네트워크를 이루어 망간 상호접속을 위한 완전한 동작을 수행한다.

### (2) 서브네팅 마스크 활용 및 장단점

- o 서브네팅은 동일한 네트워크에 16,777,214개의 호스트를 가질 수 있는 클래스 A의 경우에서 IP 라우터에 의해 묶여진 동일 물리적 네트워크상의 모든 호스트들은 같은 브로드캐스트 트래픽을 공유하게 되며 16,777,214개의 호스트 주소의 대부분을 지정할 수 없고 낭비하게 되므로 좀 더 작은 브로드캐스트 도메인을 만들고 호스트 ID의 비트를 잘 이용할 수 있도록 하기 위해 IP 네트워크는 IP 라우터로 경계가 지어지는 작은 네트워크로 분리하여 네트워크에 새로운 서브네팅 네트워크 ID를 지정하여 기존의 클래스 기반의 네트워크 ID에 서브네팅으로

포함시키는 것을 말한다. 이렇게 하여 고유한 서브넷 네트워크 ID를 가진 IP 네트워크의 분할 네트워크인 서브넷을 만들 수 있다.

- o 서브넷 마스크는 32비트의 값으로 네트워크 ID와 호스트 ID를 IP 주소에서 구분하는 역할로 사용되며 서브넷 마스크의 비트는 다음과 같이 정의된다.
  - 네트워크 ID에 해당하는 모든 비트는 1로 설정
  - 호스트 ID에 해당하는 모든 비트는 0으로 설정

### (3) 각 클래스(A,B,C)의 서브네팅 방법

- o 서브네팅은 서브넷을 만드는 작업으로 130.80.20.0이 8비트 서브넷으로 구성된 클래스 B 네트워크 ID라고 하면 클래스 기반 호스트 ID의 8비트는 서브넷 네트워크 ID를 표현하기 위해 사용되며 서브넷 마스크는 총 24비트가 서브넷 네트워크 ID를 정의하기 위해 사용된다. 서브넷으로 구성된 네트워크 ID와 그에 해당하는 서브넷 마스크는 10진수로 표현할 수 있다.(255.255.255.0) 클래스 A와 C의 경우에도 동일한 방법으로 가능하다.
- o 네트워크 ID는 여러 가지 서브넷 마스크를 사용하는 여러 네트워크 ID에서 네트워크 ID를 정확히 찾아내기 위해서는 IP를 논리적 AND 비교라는 수학적 방법을 사용한다. AND 비교에서 비교되는 두 값은 양측 모두 true이어야 결과 값이 true가 된다. 이 연산은 bit-wise 논리적 AND 라고 하며 이러한 IP 주소와 서브넷 마스크간의 논리적 AND 연산의 결과 값은 네트워크 ID가 된다.

## 1.2.3 CIDR 및 VLSM

- o 핵심가이드
  - CIDR와 VLSM의 개요
  - CIDR의 VLSM의 장단점 이해

### (1) CIDR와 VLSM의 개요

- o CIDR은 부족한 IP주소를 해결하기 위해 CIDR 이라는 새로운 주소 지정시스템이 만들어 지게되었는데 이는 IP 주소와 서브넷 마스크를 이진 표기법으로 표현하여 기존의 고정크기 네트워크를 다양하고 세부적으로 분할한다. 따라서 CIDR는 클래스형 방법보다 더 효율적으로 IP 주소를 지정할 수 있다. 클래스형

방법은 10진 표기법을 사용한 반면, CIDR은 이진 표기법을 사용한다. 모든 IP 주소와 서브넷 마스크를 이진 표기법으로 변환하다. 이렇게 분할하면 네트워크 크기를 더 다양하게 선택할 수 있고 IP주소 지정을 최적화 할 수 있다.

o CIDR 표기법 및 CIDR에서 네트워크 ID 호스트 ID 식별하기

- CIDR 표기법에서는 비트마스크를 사용하여 점으로 구분된 10진 표기법을 지정한다. 비트마스크는 IP주소에서 이진으로 표시된 서브넷 마스크에서 연속된 1의 수가 몇 개인지를 지정한다. 연속된 1은 서브넷 마스크의 맨 왼쪽 비트부터 시작된다.
- 예를 들어, CIDR 표기법으로 10.217.123.7/20인 IP주소는 그 서브넷 마스크에 연속된 1이 20개 있다는 것을 의미한다. 따라서 32비트 중에 총 나머지 12비트는 0이 되어야 한다. CIDR 표기법의 IP주소는 IP주소에서 네트워크ID를 구성하고 /x로 표현되는 비트 수를 통해 알 수 있다.
- 네트워크 ID의 계산은 IP주소가 CIDR 표기법으로 지정된 경우
  - IP주소를 이진 형식으로 변환한다.
  - 서브넷 마스크를 이진형식으로 변환한다.
  - 서브넷 마스크의 연속된 1의 개수를 사용하여 IP주소 중 네트워크 ID를 구성하는 비트수를 결정한다.
- 로컬 및 원격 호스트 결정은 네트워크 ID를 확인하고 나면 컴퓨터에서 자신의 네트워크 ID를 목적지 호스트의 것과 비교하여 목적지 호스트가 로컬네트워크에(네트워크 ID가 일치) 있는지 원격 네트워크(네트워크ID가 불일치)에 있는지 네트워크ID의 비교로 판단이 가능하다.

o VLSM (Variable Length Subnet Mask)

- VLSM은 IP를 효율적으로 할당하여 활용하기 위한 방법으로 서로 다른 크기의 서브넷을 지원하기 위한 구조이다. 만일 C class IP주소를 가진 회사에서 100개의 주소를 필요로 하는 부서가 있고 25개의 주소를 필요로 하는 4개의 부서를 서브네팅을 하는 경우에 적용이 가능하다.(예로, 192.168.120.0의 경우) 이때, 필요한 네트워크ID를 지원하기 위해 필요한 비트수를 계산하는 것이 아니라 필요한 호스트ID를 지원하기 위해 필요한 비트수를 먼저 계산해야하며 호스트의 수가 많이 필요한 서브넷부터 먼저 계산해 나간다.
- 100개의 IP 주소 할당
  - 필요한 호스트 bit : 7비트
  - 서브넷마스크 : 255.255.255.128
  - 서브넷 IP 대역 : 192.168.120.1~128, 192.168.120.129~255

- 사용할 IP 대역 : 192.168.120.1~128
- 25개의 IP 주소 할당(상위에서 할당된 서브넷 IP 대역에서 남은 대역을 사용)
  - 필요한 호스트 bit : 5비트
  - 서브넷마스크 : 255.255.255.224
  - 서브넷 IP 대역 : 192.168.120.128~159, 192.168.120.160~191, 192.168.120.192~223, 192.168.120.224~255

## (2) CIDR의 VLSM의 활용 및 장단점

### o CIDR의 장점

- CIDR는 기존의 클래스 A, B, C 네트워크 주소의 개념을 무시한다. 이로 인해 IPv4의 주소 공간을 효율적으로 할당할 수 있게 된다. ISP는 자신이 할당받은 주소 공간 중에서 clients의 요구하는 양 만큼만 잘라서 공급할 수 있게 되어 귀한 자원인 주소 공간의 낭비를 막을 수 있다.
- 인터넷 라우팅테이블의 비대화를 막아준다는 점이다. 즉, 인터넷을 여러 개의 addressing domain으로 나눔으로써 라우팅 정보량을 줄여준다. 한 도메인내에서는 그 도메인내의 모든 라우팅 정보가 공유된다.

### o VLSM의 장점

- CIDR와 VLSM은 둘다 IP주소 공간의 일부를 잘라서 사용한다는 점에서 근본적으로 동일하지만 VLSM은 한 기관에 이미 할당된 주소 공간상에서 recursion이 수행되며 global Internet에서는 이 관계가 보이지 않는다.(VLSM은 intranet domain) 그러나 CIDR는 주소 블록을 a high-level ISP에게, mid-level ISP에게, low-level ISP에게 그리고 마지막으로private organization network에게 recursive allocation한다는 점에서 서로 다르다.(CIDR는 Internet domain)

## 1.2.4 Client-Server Model

### o 핵심가이드

- Client/Server 모델 동작원리
- 반복/병렬 서버의 특징 이해

## (1) Client/Server 모델 개요

o 클라이언트(client)는 서비스를 요청하는 프로세스를 가지며, 서버(server)는 요청을 처리하고 결과를 반환하는 프로세스를 가진다.

- 클라이언트에서의 동작 순서

- 1단계 : 클라이언트와 서버간 통신 채널을 연다.(active open)
- 2단계 : 서비스를 요청하는 메시지를 서버에게 보낸다.
- 3단계 : 서버로부터 요청에 대한 결과를 받는다.
- 4단계 : 통신 채널을 닫고(close) 실행을 종료한다.

## (2) 반복/병렬 서버의 특징 등을 학습

o 서버는 크게 2개의 클래스로 구분할 수 있는데 반복서버와 병렬서버로 구분할 수 있다.

- 반복서버(Iterative server)는 다음과 같은 단계를 반복한다. 반복서버의 문제점은 2단계를 처리하는 시간에 다른 클라이언트에게 서비스를 제공하지 않는 것이다.

- 클라이언트의 요구가 오기를 기다린다.
- 클라이언트의 요구를 처리한다.
- 요구를 송신한 클라이언트에게 응답을 보낸다.
- 단계 1로 돌아간다.

- 병렬서버의 장점으로는 클라이언트의 요구를 처리하기 위한 별도의 새로운 서버를 가동할 수 있다는 것으로 클라이언트들은 자신의 전용 서버를 갖게 되는 셈이다.

- 클라이언트의 요구가 오기를 기다린다.
- 클라이언트의 요구를 처리하기 위한 새로운 서버를 시작한다. 이것은 사용하는 운영체제의 지원이 다르더라도 서버는 새로운 프로세스, 업무(task), 또는 스레드(thread)를 생성한다. 이 새로운 서버가 클라이언트의 모든 요구를 처리한다. 처리를 마치면 이 새로운 서버는 종료를 하게 된다.
- 단계 1로 돌아간다.

## 1.2.5 데이터 캡슐화

o 핵심가이드

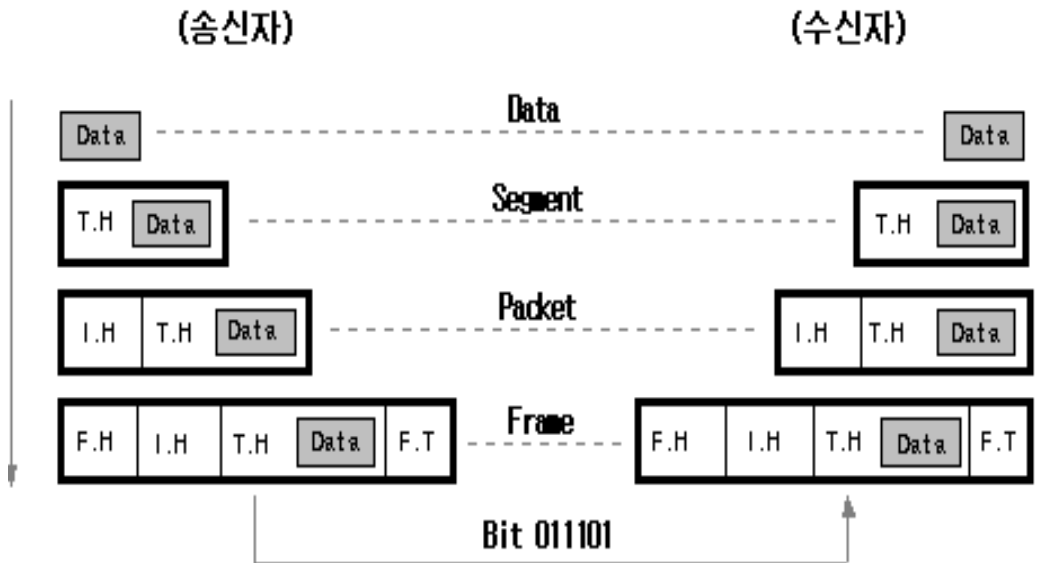
- 전송장비에서 데이터를 캡슐화하는 방법 이해

- 각 레이어는 수신 장비의 대응되는 레이어와 통신 이해
- PDU(Protocol Data Unit) 이해

(1) OSI 모델의 각 레이어에서 프로토콜 정보와 함께 데이터가 캡슐화

o TCP/IP를 이용한 통신 원리

- 송신자는 송신하려는 데이터에 레이어별로 헤더정보를 삽입한 후 수신자에게 전송하며, 수신자는 수신한 패킷의 헤더를 확인하면서 최종적으로 데이터를 확인할 수 있다. 송신자는 송신 데이터를 데이터로 변환하여 아래층 레이어로 전달하면 데이터를 세그먼트로 변경하고 연결은 전송 및 수신 호스트에서 이루어진다. 다시 아래층 레이어로 전달하면 세그먼트를 패킷이나 데이터그램으로 변경되고 아래층 레이어로 전달하면 패킷 또는 데이터그램은 로컬 네트워크에 전송하기 위한 프레임으로 변환된다. 하드웨어 주소를 사용하여 로컬 네트워크 세그먼트에서 호스트의 어드레스를 식별하는데 사용된다.



\* T.H : TCP Header, I.H : IP Header, F.H : Frame Header, F.T : Frame Trailer

(그림 2-3) TCP/IP 프로토콜 통신 방식

- o PDU는 각 계층에서 헤더 정보를 삽입하여 송신 데이터 형태로 생성하므로 이 계층마다 부르는 명칭을 말한다. 일반적으로는 패킷이라고 말하기도 한다.



## 1.2.6 포트주소의 의미와 할당원칙

### o 핵심가이드

- 포트의 개념 이해
- 포트 사용 규칙 및 번호체계와 주요 서비스 포트 이해

### (1) 포트의 개요

- o 포트번호는 인터넷이나 기타 다른 네트워크 메시지가 서버에 도착하였을 때, 전달되어야 할 특정 프로세스(응용 프로그램)를 인식하기 위한 방법으로 TCP와 UDP에서 포트번호는 단위 메시지에 추가되는 헤더 내에 들어지는 16 비트 정수의 형태를 갖는다. 이 포트번호는 논리적으로는 클라이언트와 서버의 전달계층 사이를, 그리고 물리적으로는 전달계층과 인터넷계층 사이를 통과하여, 계속 전달된다.

### (2) 포트번호와 소켓

- o 클라이언트가 서버에 접속을 하기 위해서 패킷을 만들어야 하는데 이때 TCP 헤더에 송신자 포트와 수신자 포트 번호 정보를 삽입하여 패킷을 만들게 된다. 이 패킷을 서버로 전달하여 프로세스(응용프로그램)과 연결이 되고 서비스를 이용할 수 있다. 원격지의 서버 내에 있는 FTP 프로세스에 사용자의 요청을 전달하기 위해 사용자 컴퓨터에 있는 TCP 프로토콜은 요청에 추가되어지는 16 비트 정수의 포트번호 내에 21이라는 포트번호를 삽입하여 전송하고 서버는 이 정보를 확인하여 21이라는 포트번호를 읽고 사용자의 요청을 FTP 프로그램에 전달할 것이다.
- o 포트번호에는 소스포트번호와 데스틴네이션포트번호가 있다. 우리가 보통 서비스포트라고 하는 것은 클라이언트를 기준으로 데스틴네이션 포트번호를 말하는 것이다.
- o 포트번호는 16비트이며 0번에서 65535번까지 있다. 1~1023번까지를 흔히 Well Known Port라고 해서 응용프로그램 개발자가 사용할 수 없는 영역으로 정의하고 있다. 그러므로 1023번까지는 메이저 벤더들이 이미 약속해서 사용하는 것이라고 생각하면 되고 1024~65535는 지정되지 않은 영역이라고 보면 된다.

[표 2-1] 주요 서비스 포트번호

- o 21번: FTP
- o 22번: 보안 텔넷(SSH)
- o 23번: 텔넷
- o 25번: SMTP(메일 발송)
- o 42번: 호스트 네임 서버
- o 53번: 도메인 메인 서버
- o 70번: 고퍼(Gopher)
- o 79번: 핑거(Finger)
- o 80번: 웹(HTTP)
- o 88번: 커베로스 보안 규격
- o 110번: POP3(메일 수신)
- o 118, 156번: SQL 서비스
- o 137~139번: NetBIOS(파일 서버)
- o 161번: SNMP(네트워크 관리)

### 1.2.7 IP, ARP, IGMP, UDP, TCP 등 각 프로토콜의 원리 및 이해

#### o 핵심가이드

- ARP의 동작원리 및 물리적 네트워크 주소 이해
- IGMP의 기능, IP 멀티캐스트의 개념 및 활용 이해
- UDP의 특징과 활용
- TCP 서비스 및 TCP 3-way 핸드셰이크, 그리고 UDP와 비교
- ICMP 기능 및 활용 이해

#### (1) ARP(Address Resolution Protocol)

- o ARP 프로토콜은 IP 패킷이 이더넷이나 토큰링과 같이 공유 액세스, 브로드캐스트 기반의 네트워크 기술로 전달된다면, IP 주소에 해당하는 48 bit의 MAC 주소를 반드시 알아야 TCP/IP의 경우 이더넷헤더를 포함한 프로토콜 헤더를 완성하여 수신자에게 데이터를 전송할 수 있다. 이때, ARP는 상대방의 IP 주소

를 알고있지만 MAC 어드레스를 알지 못하는 경우 ARP 프로토콜에 의해서 수신자 MAC 어드레스를 가져올 수 있는 프로토콜이며, MAC-레벨 브로드캐스트를 사용한다.

- o 이더넷 어드레스는 48bit 주소로 되어있으며, 물리적 어드레스, MAC 어드레스라는 용어로도 혼용되며, 랜카드의 고유번호이다.
- o IP 패킷이 이더넷이나 토큰링과 같이 공유 액세스, 브로드캐스트 기반의 네트워크 기술로 전달된다면, IP 주소에 해당하는 48 bit의 MAC 주소를 반드시 알아야 한다. ARP는 IP 주소를 그에 해당하는 MAC 주소로 변환하기 위해 MAC-레벨 브로드캐스트를 사용한다.

## (2) IGMP(Internet Group-Membership Protocol)

- o IGMP(Internet Group Management Protocol)은 IP 멀티캐스트 그룹에서 호스트 멤버를 관리하는 프로토콜로써 IP 멀티캐스트 그룹은 특정 멀티캐스트 IP 주소로 전달되는 IP 트래픽을 감시하는 호스트들의 집합이다. 멀티캐스트 IP 트래픽은 하나의 MAC 주소로 보내지지만 여러 개의 IP 호스트에 의해 처리된다. 지정된 호스트가 특정 IP 멀티캐스트 주소를 감시하고 그 IP 주소로 오는 모든 패킷을 받는다.
- o 호스트 그룹 멤버들은 어느 때나 그룹에 추가되거나 삭제될 수 있는 동적(dynamic)이며 호스트 그룹의 멤버는 IP 라우터를 여러 네트워크로 확장할 수 있다.

## (3) UDP(User Datagram Protocol)

- o UDP는 신뢰할 수 없는 비연결 지향 데이터그램 서비스를 제공한다. 데이터는 메시지 형태로 전달되며 전달하기 위한 최대한의 노력을 다한다. 즉, UDP는 데이터그램의 전송을 100% 보장하지 않으며, 전송된 패킷의 순서가 정확하다는 것을 보장하지 못한다는 것하며 손실된 데이터를 재전송을 통해 복구하지 않는다.
- o UDP는 데이터 전달을 확인할 필요가 없거나 한번에 작은 양의 데이터를 전송하는 애플리케이션에 주로 사용된다. NetBIOS 네임 서비스, NetBIOS 데이터그램 서비스, SNMP(Simple Network Management Protocol), DNS등이 UDP를 사용하는 서비스, 애플리케이션의 대표적인 예이다

(4) TCP(Transmission Control Protocol)

- o TCP는 신뢰할 수 있고, 연결 지향의 전달 서비스이다. 데이터는 세그먼트 단위로 전송된다. 연결 지향(Connection-oriented)이란 호스트가 데이터를 교환하기 이전에 연결이 반드시 이루어져야 함을 말하며 전송되는 모든 세그먼트에 순번을 지정하여 신뢰성을 확신할 수 있게 된다. 다른 호스트에 의해 데이터가 받아졌는지를 조사하기 위해 확인 방법이 사용된다. 각 세그먼트에 대해 전달 받은 호스트는 반드시 ACK(acknowledgment)를 정해진 시간 안에 리턴해야 한다. 만일 ACK를 받지 못하면, 데이터는 다시 전송된다.

[표 2-2] TCP 헤더의 주요 필드

필드	기능
Source Port	데이터를 보내는 호스트의 TCP 포트.
Destination Port	데이터를 받는 호스트의 TCP 포트.
Sequence Number	TCP 세그먼트에 있는 데이터의 첫번째 바이트에 대한 순번.
Acknowledgment Number	바이트에 대한 순번, 데이터를 보내는 측은 연결된 다른 측 호스트에서 이 값을 전달 받을 것을 기대한다.
Window	TCP 세그먼트를 보내는 호스트의 현재 TCP 버퍼 크기.
TCP Checksum	TCP 데이터와 TCP 헤더의 정확성 확인

- o TCP 3-way 핸드셰이크(Handshake) : 핸드셰이크의 목적은 순번을 동기화하고 연결의 양측에서 순번을 확인하고 TCP 윈도우의 크기를 교환하고 최대 세그먼트 크기와 같은 기타 TCP 옵션을 교환하는 것이다.
  - 클라이언트는 TCP 세그먼트에 연결을 위한 초기 순번과 서버로부터 전송 받은 세그먼트를 저장하기 위한 클라이언트측 버퍼크기를 나타내는 윈도우 크기를 저장하여 보낸다.
  - 서버는 자신이 선택한 초기 순번, 클라이언트의 순번에 대한 확인, 클라이언트로 전달 받을 세그먼트를 저장할 버퍼의 크기를 나타내는 윈도우 크기들을 TCP 세그먼트에 담아 전달한다.
  - 클라이언트는 서버의 순번을 확인하는 정보를 TCP 세그먼트로 서버에 전달한다.

(5) ICMP

- o ICMP 프로토콜은 문제를 해결하는 기능과 전달할 수 없는 패킷에 대한 에러 정보를 알리기 위해 사용된다. 예를 들어, IP가 어떤 패킷을 목적 호스트로 전달할 수 없다면, ICMP는 "Destination Unreachable" 메시지를 소스 호스트로 보냅니다.

[표 2-3] 대표적인 ICMP 메시지

ICMP 메시지	기능
Echo Request	원하는 호스트로의 IP 연결을 확인하기 위해 사용되는 간단한 문제 해결 메시지.
Echo Reply	ICMP Echo Request에 대한 응답 메시지.
Redirect	데이터를 보내는 호스트에게 목적 IP 주소에 대한 좀 더 적합한 경로가 있음을 알리기 위해 라우터가 보내는 메시지.
Source Quench	데이터를 보내는 호스트에게 IP 데이터그램이 라우터의 집중 현상에 의해 손실되고 있음을 알리기 위해 라우터가 보내는 메시지. 그러면, 데이터를 보내는 호스트는 전송률을 낮추게 된다. Source Quench는 ICMP에서 선택적 메시지이고 대부분 구현되지 않습니다.
Destination Unreachable	라우터나 목적 호스트에 의해 보내지며 데이터그램이 전달되지 못한다는 것을 데이터를 보내는 호스트에 알려줍니다.

1.2.8 Broadcast 및 Multicast의 이해

- o 핵심가이드
  - 유니캐스트, 브로드캐스트, 멀티캐스트 방식 이해

(1) 인터넷의 전송 방식의 특징과 장단점 이해

- o 유니캐스트는 하나의 송신자가 다른 하나의 수신자로 데이터를 전송하는 방식이다. 유니캐스트는 네트워크상에서 단일 송신자와 단일 수신자간의 통신이다.

단일 송신자와 다중 수신자간의 통신인 멀티캐스트나, 또는 네트워크 상의 어떠한 송신자와 가장 가까이 있는 수신자 그룹간의 통신인 애니캐스트 등과 구별하기 위해 존재한다.

- 브로드캐스트(Broadcast)는 하나의 송신자가 같은 서브네트워크 상의 모든 수신자에게 데이터를 전송하는 방식이다.
  - 브로드 캐스트 IP 주소는 호스트 필드의 비트 값이 모두 1인 주소를 말하며, 이러한 값을 갖는 IP주소는 일반 호스트에 할당하여 사용할 수 없다. 예를 들어, 198.18.166.0인 네트워크의 브로드캐스트 IP주소는 호스트 필드 값이 모두 1이 되는 주소가 198,18,166,255로, 이 주소는 일반 호스트에 할당할 수 없다. 목적지 IP 주소가 198.18.166.255인 데이터는 해당 네트워크에 접속 되어 있는 호스트로 전송된다. 이러한 브로드캐스트 IP주소는 라우팅 프로토콜이나 ARP 등의 특수한 목적으로 사용되며, 링크 레벨의 브로드 캐스트 주소와는 구분된다.
- 멀티캐스트(Multicast) : 하나 이상의 송신자들이 특정한 하나 이상의 수신자들에게 데이터를 전송하는 방식
  - 멀티캐스트 전송이 지원되면 송신자는 여러 수신자에게 한 번에 메시지가 전송되도록 하여 데이터의 중복전송으로 인한 네트워크 자원 낭비를 최소화할 수 있게 된다. 멀티캐스트 전송을 위해서는 헤더에 수신자의 주소 대신 수신자들이 참여하고 있는 그룹 주소를 표시하여 패킷을 전송한다. 멀티캐스트 전송을 위한 그룹 주소는 D-class IP 주소 (224.0.0.0~239.255.255.255)로 전 세계 개개의 인터넷 호스트를 나타내는 A, B, C-class IP 주소와는 달리 실제의 호스트를 나타내는 주소가 아니며, 그룹 주소를 갖는 멀티캐스트 패킷을 전송받은 수신자는 자신이 패킷의 그룹에 속해있는가를 판단해 패킷의 수용여부를 결정하게 된다.

### 1.3 Unix/Windows 네트워크 서비스

#### 1.3.1 DNS, DHCP, SNMP, telnet, ftp, smtp 등 각종 서비스의 원리 및 이해

##### (1) DNS 서비스

- 핵심가이드
  - DNS 제공하는 서비스 이해

- DNS의 동작 원리 이해
- DNS 레코드 구성 이해
- DNS 메시지 등 이해
- o DNS는 도메인 네임을 IP address로 매핑해주는 서비스이다. DNS 서비스는 다수의 네임서버들의 원활한 동작을 위해 계층적인 구조를 지닌다. DNS의 계층 구조는 Root Name Server에서 시작하는데, 전 세계를 통틀어 Root Name Server는 13개 정도가 존재한다. 이 Root Name Server 아래에 com, edu, net, org 국가별 접미사(kr, ch, jp)들의 목록을 지니는 DNS 서버들이 존재하고 그 아래에 각 기업 혹은 비영리 단체의 DNS 서버가 존재한다.
- o DNS의 동작방식
  - 클라이언트가 최초로 www.kisec.com에 접속하기 위해서 웹브라우저에 입력하고 접속 요청을 수행하면 컴퓨터의 캐시정보를 확인하고 hosts 파일을 확인한 후 해당하는 정보가 없으면 DNS 서버를 이용한다.
  - 로컬 네임서버에 질의를 보내고 해당정보가 없는 경우 루트 네임서버에 질의한다.
  - 루트 네임서버에 정보가 없는 경우 com을 관리하는 네임서버의 정보를 로컬 네임서버에 전달한다.
  - 로컬 네임서버는 다시 com 네임서버에 www.kisec.com 질의를 보내면 kisec.com에게 질의하도록 로컬 네임서버에 보낸다.
  - 루트 네임서버는 최종적으로 kisec.com에 질의하고 kisec.com의 DNS 서버로부터 www.kisec.com에 대한 IP 주소를 얻어 클라이언트에게 전달한다.
  - 클라이언트는 www.kisec.com의 IP를 이용하여 웹서버에 접속한다.

## (2) DHCP 서비스

- o 핵심가이드
  - BOOTP를 대체하는 프로토콜
  - DHCP 동작 절차 이해
  - 패킷 형식 등 이해
- o DHCP(Dynamic Host Configuration Protocol)는 호스트 IP 구성 관리를 단순화하는 IP 표준이다. DHCP 표준에서는 DHCP 서버를 사용하여 IP 주소 및 관련된 기타 구성 세부 정보를 네트워크의 DHCP 사용 클라이언트에게 동적으로 할당하는 방법을 제공한다. TCP/IP 기반 네트워크에서 DHCP를 사용하면 컴퓨터

터틀 다시 구성하는 관리자의 작업이 간단해지고 줄어든다.

- o DHCP는 클라이언트-서버 모델을 사용한다. 네트워크 관리자는 TCP/IP 구성 정보를 관리하는 DHCP 서버를 하나 이상 만들고 클라이언트에 TCP/IP 구성 정보를 제공한다. 네트워크에서 DHCP 서버를 설치하고 구성하면 DHCP 사용 클라이언트는 작동을 시작하여 네트워크에 참가할 때마다 IP 주소 및 관련 구성 매개 변수를 동적으로 받을 수 있다. DHCP 서버는 이 구성 정보를 요청하는 클라이언트에 주소 임대 제안의 형태로 제공한다.
- o BOOTP(Bootstrap Protocol)는 DHCP보다 먼저 개발된 호스트 구성 프로토콜이다. DHCP는 BOOTP를 향상시키고 BOOTP가 호스트 구성 서비스로서 가지는 제한을 해결하였다.

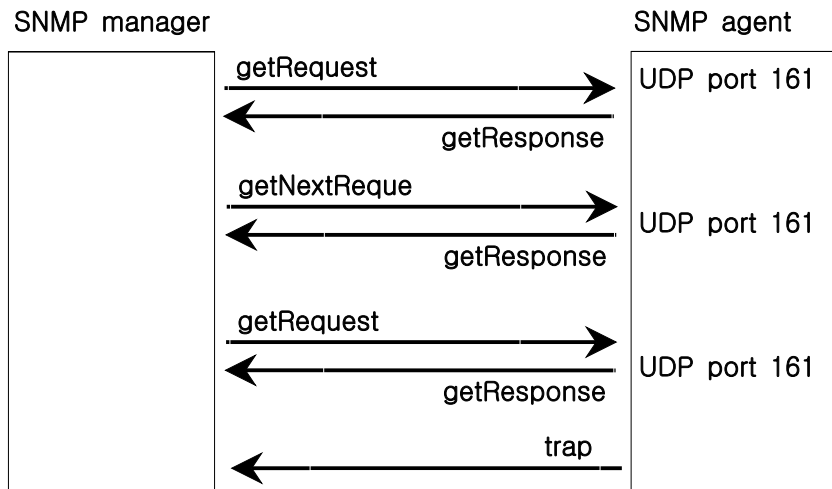
[표 2-4] BOOTP와 DHCP의 비교

BOOTP	DHCP
DHCP 앞서서 개발	BOOTP 이후에 개발
제한된 부팅 기능이 있고 디스크가 없는 워크스테이션을 구성하기 위한 프로토콜	로컬 하드 드라이브와 완전한 부팅 기능이 있으며 위치가 자주 바뀌는 네트워크 컴퓨터
동적 BOOTP의 IP 주소 임대 만료일은 30일	DHCP의 IP 주소 임대 만료일은 8일
공급업체 확장이라고 하는 제한된 수의 클라이언트 구성 매개 변수를 지원	옵션이라고 하는 크고 확장 가능한 클라이언트 구성 매개 변수 집합을 지원
2 단계 bootstrap 구성 프로세스를 설명 -클라이언트는 BOOTP 서버에 연결하여 주소를 결정하고 부팅 파일 이름을 선택 -클라이언트는 TFTP서버에 연결하여 부팅 이미지의 파일을 전송	DHCP 클라이언트가 그 IP 주소를 결정하고 네트워크 작업에 필요한 모든 초기 구성 세부 사항을 얻기 위해 DHCP 서버와 협상하는 단일 단계 부팅 구성 프로세스를 설명. DHCP 클라이언트는 DHCP 서버로 구성을 다시 바인딩하거나 갱신할 때 시스템을 다시 시작하지 않음.



### (3) SNMP 서비스

- 핵심가이드
  - SNMP의 개념 이해
  - SMI와 MIB 프로토콜과의 관계 이해
  - SNMP의 메시지 이해 등
- 네트워크 관리 프로토콜인 SNMP는 시스템이나 네트워크 관리자로 하여금 원격으로 네트워크 장비를 모니터링하고 환경설정 등의 운영을 할 수 있게 한다. 이러한 SNMP의 편의성에 반해 여러 가지 취약점이 존재한다. 이 취약점들로 인해 서비스거부 공격, 버퍼 오버플로우, 비인가 접속 등 여러 가지 문제들이 야기될 수 있다.
- TCP/IP를 기반으로 하는 네트워크의 관리는 네트워크 관리 스테이션과 호스트, 라우터, 프린터 등과 같은 네트워크 구성요소에 설치된 에이전트라는 소프트웨어간의 통신에 의해 이루어지며, 다음 3개의 구성요소를 가진다.
  - Management Information Base(MIB) : 네트워크 구성요소에 의해 유지되는 변수값
  - Structure of Management Information(SMI) : MIB의 변수값 조회 시 사용되는 공통정책과 구조
  - Simple Network Management Protocol(SNMP) : manager와 agent간의 통신 프로토콜
- SNMP의 원리
  - SNMP는 OSI 7계층의 7번째 계층인 애플리케이션 계층의 프로토콜이며 에이전트의 MIB에 저장되어 있는 변수 값을 조회하거나 변경하기 위해 사용된다. 매니저와 에이전트 간의 통신은 메시지의 교환에 의해 이루어지며, 메시지는 UDP 데이터그램의 데이터부분으로 구성되어 전송된다. SNMP에서 매니저와 에이전트 간의 통신에 사용되는 메시지는 PDU 타입에 따라 5가지이다.



(그림 2-4) SNMP 동작

- getRequest : 매니저가 하나 또는 그 이상의 특정 변수 값을 읽어 올 수 있다.
  - getNextRequest : 매니저가 이미 요청한 변수 다음의 변수 값을 요청한다.
  - setRequest : 매니저가 하나 또는 그 이상의 변수 값 변경을 요청한다.
  - getResponse : 에이전트가 매니저의 요청에 해당하는 변수 값을 전송한다.
  - trap : agent 의 특정 상황 발생을 매니저에게 알린다.
- SNMP 에서 사용되는 메시지 5가지 중 4가지가 단순히 요청과 응답이라는 프로토콜에 의해 교환되기 때문에 SNMP는 UDP를 사용한다. 매니저는 161 UDP 프로토콜, 에이전트는 162 UDP 포트에 메시지를 전송한다.
- SNMP 통신이 가능하려면 다음의 3가지 사항이 반드시 필요하다.
- version : 매니저와 에이전트 시스템간의 SNMP버전이 일치해야 한다.
  - community : 양 시스템간의 커뮤니티가 일치해야 하고, 일반적인 값은 public이다.
  - PDU type : 값의 범위는 0과 4사이이며, 매니저가 요청하는 경우 get-(Next)Request 와 setRequest이외의 PDU 타입이 설정되면 응답이 없다. 마찬가지로 get-(Next)Request에 대한 응답 시에 getResponse 가 아닌 PDU타입으로 메시지가 오면 해석이 불가능하다.

#### (4) Telnet 서비스

- 핵심가이드
  - 네트워크 가상 터미널 이해
  - 운영 모드 이해
  - rlogin과 비교
- 텔넷은 클라이언트가 서버에 접속하여 그 서버에 연결/구동된 것처럼 상호 작용하도록 하는 서비스이다. 텔넷 서버는 23번 포트를 사용한다.
- 텔넷 프로토콜은 네트워크 가상 단말기(NVT)라고 하는 표준 포맷으로 코드화된 하나의 문자나 문자열로 구성된 명령어들을 사용하여 서로 통신한다. 네트워크 가상 단말기는 클라이언트와 서버의 커넥션 양측에 있는 실제 터미널에 매핑시켜주고 키보드와 프린터로 구성된 양방향 문자 디바이스 클라이언트가 먼저 터미널 형식을 계획하고 다음에 서버가 지원하는 형태이다. 명령을 위해 사용되는 문자 집합은 ASCII 형태이며, 상호작용에 관련된 모든 입출력 데이터는 ASCII로 전송된다. NVT 포맷의 모든 명령어들과 데이터들은 8비트를 사용하여 코드화되어 있다.
- 텔넷의 운영모드 : 리모트 호스트에 연결이 되면 라인모드 옵션을 사용가능 상태로 하려고 시도한다. 만약 이것이 실패하면 character at a time 모드 또는 old line by line 모드를 선택하여 사용한다.
  - character at a time 모드 : 사용자가 자판을 입력한 내용들 대부분이 처리를 위해 즉시 리모트 시스템으로 보내진다.
  - old line by line 모드 : 모든 텍스트가 지역적으로 반향(echo)된다. 그리고 보통 완벽한 한 줄만이 리모트 시스템에 보내진다.
  - 명령모드 : 라인모드 옵션이 사용가능 상태가 되거나, localchars 토클이 참값을 가지면(old line by line의 초기값), 사용자의 quit, intr, flush 문자가 지역적으로 trap되어지고, 텔넷 프로토콜 처리로 리모트 시스템에 보내진다. 라인모드 옵션이 사용불가 상태이면, 사용자의 susp(보류-suspend) eof(파일끝) 신호가 텔넷 프로토콜 처리로 리모트 시스템에 보내질 수 있으며, quit 신호는 break 대신에 telnet abort로 보내진다. 리모트 호스트에 연결되어 있을 때는, telnet "escape 문자"(초기값 : "^]")를 사용해서 telnet 프롬프트 상태로 진입할 수 있다. 이때를 명령 모드라 한다. 명령 모드일 때는 일반 터미널 편집 방식이 사용가능 상태가 된다.

[표 2-5] rlogin과 telnet 비교

구분	Rlogin	Telnet
Transport	하나의 TCP 연결	하나의 TCP 연결
프로토콜	긴급(urgent)모드	긴급(urgent)모드
패킷모드	항상 character at a time 원격 에코	명령 디폴트(character at a time, 원격 에코) 클라이언트 에코(kludge line mode) 서버상의 애플리케이션이 필요한 경우 항상 character at a time
흐름제어	일반적으로 클라이언트 수행 서버에 의해 무효 가능	일반적으로 서버 수행 클라이언트가 수행하는 옵션 사용 가능
터미널유형	항상 제공	옵션
터미널속도	항상 제공	옵션
윈도우크기	대부분 서버에 의해 지원되는 옵션	옵션
자동로그인	디폴트 패스워드 입력이 요구 가능 평문으로 전송 최근에 커버로스 로그인 지원	디폴트로 로그인 이름과 패스워드 입력 패스워드는 평문으로 전송 최근에 새로운 인증 옵션 제공

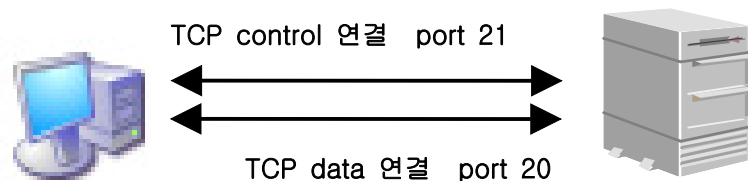
(5) 기타 Rlogin, FTP, TFTP, SMTP 등 유닉스 /Windows에서 제공하는 각종 네트워크 서비스에 대한 기본 개념과 기능에 대한 이해

o 핵심가이드

- Rlogin, FTP, TFTP, SMTP 등 네트워크 서비스에 대한 기본 개념과 주요 특징, 기능에 대한 이해

o ftp

- 인터넷 상에서 파일을 교환하는 기능을 하는 파일전송 프로토콜을 말하며, FTP는 인터넷의 한 호스트에서 다른 호스트로 파일을 복사하는 서비스를 제공한다.



(그림 2-5) FTP 동작

- 파일전송 프로토콜은 제어포트와 데이터포트를 사용한다. 21번 제어포트를 이용하여 인증과정과 파일 송수신 제어신호를 주고받은 후 20번 데이터포트를 사용하여 실제 파일을 송수신한다.
- o tftp
  - TFTP는 LAN 응용에서 주로 사용하기 위해서 만들어 졌다. 기본 FTP가 가지고 있는 기능을 대폭 줄여 구현 하였으며 TCP 대신 UDP를 사용한다. TFTP는 메시지 오류 체크를 위하여 RQ(stop-and wait)에러 제어 프로시저를 포함한다. 일반적으로 라우터의 설정 정보 백업을 위한 목적으로 사용되고 있다.
- o SMTP
  - SMTP는 인터넷에서 이메일을 보내고 받기 위해 이용되는 프로토콜이다. 사용하는 TCP 포트번호는 25번이다. 상대 서버를 지시하기 위해서 DNS의 MX레코드가 사용된다. 메일 서버간의 송수신뿐만 아니라, 메일 클라이언트에서 메일 서버로 메일을 보낼 때에도 사용되는 경우가 많은데 smtp는 텍스트 기반의 프로토콜로서 요구/응답 메시지만 아니라 모든 문자가 7bit 아스키로 되어 있어야 한다고 규정되어 있다. 이 때문에 문자 표현에 8bit 이상의 코드를 사용하는 언어나 첨부파일과 자주 사용되는 각종 바이너리는 MIME이라고 불리는 방식으로 7bit로 변환되어 전달된다.

### 1.3.2 Workgroup과 DOMAIN

#### (1) 디렉토리 데이터베이스(Directory database)

- o 핵심가이드
  - 디렉토리 데이터베이스의 역할 이해
  - domain controller의 역할 이해
  - Active Directory의 역할 이해
- o Active Directory는 네트워크상의 개체에 대한 정보를 저장하며 관리자와 사용자가 이 정보를 쉽게 찾아 사용할 수 있도록 한다. Active Directory는 체계적인 데이터 저장소를 사용하여 디렉터리 정보를 논리적인 계층 구조로 조직하고 디렉터리라고도 하는 이 데이터 저장소는 Active Directory 개체에 대한 정보를 포함하고 있다. 일반적으로 이러한 개체에는 서버, 볼륨, 프린터 등의 공유 리소스와 네트워크 사용자 및 컴퓨터 계정이 포함된다.
- o Active Directory 서버는 도메인 내에서 서버로 동작하는 컴퓨터는 구성원 서버

나 도메인 컨트롤러의 역할 중 하나를 수행할 수 있다. 도메인 내에 있지 않은 서버는 독립 실행형 서버가 된다.

- 구성원 서버는 다음과 같은 컴퓨터가 구성원 서버이다

- Windows 2000 Server 제품군 또는 Windows Server 2003 제품군의 운영 체제를 실행하는 컴퓨터
- 도메인에 속한 컴퓨터
- 도메인 컨트롤러가 아닌 컴퓨터

- 구성원 서버는 계정 로그온을 처리하지 않고 Active Directory 복제에 참여하지 않거나 도메인 보안 정책 정보를 저장하지 않습니다. 일반적으로 구성원 서버는 파일 서버, 응용 프로그램 서버, 데이터베이스 서버, 웹 서버, 인증 서버, 방화벽 및 원격 액세스 서버 같은 서버 종류로 동작한다.

o Active Directory 클라이언트는 Active Directory 클라이언트를 사용하면 Windows 2000 Professional 또는 Windows XP Professional에서 사용할 수 있는 많은 Active Directory 기능을 Windows 95, Windows 98 및 Windows NT 4.0을 실행하는 컴퓨터에서도 사용할 수 있다.

o 도메인 컨트롤러는 디렉터리 데이터를 저장하고 사용자 로그온 프로세스, 인증 및 디렉터리 검색과 같은 사용자와 도메인 간의 통신을 관리한다. 도메인 컨트롤러는 멀티마스터 복제를 사용하여 디렉터리 데이터를 동기화하여 시간이 지나도 정보의 일관성을 보장한다.

o 디렉터리 데이터 저장소는 Active Directory 디렉터리 서비스에서 모든 디렉터리 정보를 저장하는 곳이다. 이 데이터 저장소를 흔히 디렉터리라고 한다. 디렉터리에는 사용자, 그룹, 컴퓨터, 도메인, 조직 구성 단위 및 보안 정책과 같은 개체에 대한 정보가 들어 있다. 사용자 및 관리자가 사용할 수 있도록 이 정보를 게시할 수 있다.

## (2) Windows 2000 Workgroup 방식

o 핵심가이드

- 컴퓨터의 논리적 그룹 이해
- 컴퓨터는 전용서버(Dedicated Server)와 Client의 교번 가능 이해
- 보안 관리의 분산 이해

o Windows 2000의 네트워크 방식은 다음과 같이 2개로 구분할 수 있다.

- 워크그룹(Workgroup) 방식

- 각각의 계정과 자원을 시스템별로 관리하는 방식으로 소규모 네트워크에 적합하다.
  - '피어 투 피어'라고도 하며 전용 서버 없이 모든 시스템이 서버이면서 클라이언트 기능을 가지며 서로 동등하다.
  - 서버 관리자가 필요없으며 보안은 각 시스템의 로컬 디렉토리 데이터베이스(SAM DB)에 의해 제공된다.
  - Active Directory가 구축되지 않은 상태로서 다른 시스템에 접근할 때 수시로 액세스에 필요한 사용자 계정과 암호를 요구한다.
- 도메인(Domain) 방식
- 모든 계정과 자원을 특정 서버에서 관리하는 중앙 집중식 방식이다.
  - 사용자에게 적절한 사용 권한을 설정하면 사용자는 다른 컴퓨터에 자원을 지정한 권한대로 접근할 수 있다.
  - Active Directory가 구축된 상태에서 가능하며 기존의 Windows NT 기반의 도메인보다 확장된 기능을 제공한다.

### 1.3.3 터미널서비스 등 각종 원격관리 서비스

#### (1) 터미널 서비스 구성 요소

- 핵심가이드
  - 가상 데스크톱 컴퓨터 사용 장치의 활용 이해
  - Windows 2000 기반 서버의 원격 관리의 원리 이해
  - 터미널 서비스 클라이언트 소프트웨어의 특징 이해
- 관리자가 원격지의 컴퓨터에 접속하여 다양한 작업을 하는 경우 원격지의 컴퓨터를 관리하는데 지원하는 툴을 Windows 2000에서는 터미널 서비스라는 툴로 제공하고 있다.
- 터미널 서비스는 터미널 에뮬레이터 역할을 하는 소프트웨어를 통해 서버 데스크톱에 대한 원격 접속을 제공하는 툴이다. 터미널 서비스는 원격지의 컴퓨터에 접속하여 프로그램의 사용자 인터페이스만을 클라이언트로 전송한다. 그러면 클라이언트에서 키보드 및 마우스 입력을 다시 서버로 보내고 서버에서 그 입력을 처리한다. 각 사용자는 자신의 개별 세션에만 로그인하고 그 세션에 대한 결과화면만 보게 됨으로 독자적으로 제어하는 모습을 갖게 된다.
- 터미널 서비스는 응용 프로그램 서버모드 또는 원격 관리모드로 서버에 배포될

수 있다. 응용 프로그램 서버 모드의 터미널 서비스는 네트워크 서버를 통한 효과적이고 신뢰도 높은 Windows 기반 프로그램 배포 방법을 제공한다.

o 터미널서비스의 장점

- 원격지의 컴퓨터를 나의 컴퓨터처럼 사용할 수 있다.
- 집중된 프로그램 배포 Windows 2000 Server에서 터미널 서비스를 실행하면 모든 프로그램 실행, 데이터 처리 및 데이터 저장이 서버에서 수행되어 프로그램 배포가 집중화된다.
- 원격 관리 터미널 서비스는 Windows 2000 Server에 대한 원격 관리 기능을 제공하므로 시스템 관리자는 WAN 연결 또는 전화 접속 연결을 통해 어느 클라이언트에서나 서버를 원격 관리할 수 있다.
- 관리자가 원격 관리를 통해 데이터센터등에 존재하는 원격 서버들을 재부팅, 설치 등 다양한 원격 관리가 가능하다.

o 터미널 서비스 라이선스는 Windows 2000 Server의 라이선스와 별개로 터미널 서버에 로그인하는 클라이언트에 사용권을 허가하는 라이선스가 필요하다. 특히 터미널 서비스를 응용프로그램 서버로 활용할 경우에는 복잡한 라이선스 정책을 수용해야만 터미널 서비스를 자유로이 이용할 수 있다. 터미널 서비스를 응용 프로그램 서버 모드로 사용할 때는 라이선스 서버가 필요하며 라이선스 서버는 클라이언트 라이선스를 설치하고 터미널 서비스 클라이언트에 라이선스를 발급하게 된다. 클라이언트가 터미널 서버에 처음 로그인을 시도할 때 터미널 서버는 라이선스 서버에 연결하여 클라이언트를 위한 라이선스를 요청한다. 클라이언트에게 라이선스를 발급하려면 먼저 네트워크에 라이선스 서버를 설치하고, 클라이언트 라이선스 키팩을 라이선스 서버에 설치해야 한다.

### 1.3.4 인터넷 공유 및 NAT 원리, 활용

#### (1) NAT 원리

o 핵심가이드

- IP 주소 변환과 장단점 이해

o NAT는 사설 주소를 인터넷으로 라우팅할 수 있게 하는 라우팅 정책중 하나가 NAT(Network Address Translation)이다. 또한 NAT는 IANA주소를 절약하는데 아주 유용하게 이용될 수 있는데 인터넷으로 라우팅할 수 없는 사설 주소를 유일한 인터넷 주소로 전환하여 라우팅이 가능하게 한다.



- o NAT에 대한 가장 기본적인 정의는 public outside address와 private inside address의 사이에서 border router로서의 역할을 한다는 것이다. 이러한 border router로서의 역할은 inside address와 outside address가 서로 전환되는 동작을 말한다.
- o NAT의 동작 원리에서 NAT는 1:1의 주소 매핑을 수행하기 때문에 NAT라우터로 들어온 inside->outside 패킷(또는 그 반대)만이 주소 전환의 대상이 된다. 간단히 설명하자면 IP의 헤더 부분을 체크하여 NAT 테이블에 의해 해당 주소로 바꾼 다음 checksum을 다시 계산하여 IP의 헤더를 바꾸는 방법으로 동작한다. Application layer에서 까지 NAT의 주소 전환이 반영이 되려면 NAT는 IP 주소의 참조내용을 담고 있는 application 데이터 부분을 새로운 주소로 변환해야 한다.
- o NAT의 장점
  - 호스트는 사설 IP를 사용하면서 인터넷 및 통신을 할 수 있으므로 공인 IP 주소의 낭비 방지
  - 외부 컴퓨터에서 사설 IP를 사용하는 호스트 접근 어려움(보안 측면)
  - 기타

## (2) NAT의 활용

- o 핵심가이드
  - NAT 테이블의 구성요소와 역할 이해
  - IP 주소 정의 방법 이해
- o 일반적인 NAT에서 주소변환을 위해서는 IP 헤더의 IP 주소, TCP 헤더의 포트 번호, UDP 헤더의 포트번호의 3가지 사항에 의존하며 NAT 변환 테이블에 정책을 설정하여 NAT 기능을 수행할 수 있다. 시스코에서 만든 NAT 버전은 관리자가 다음과 같은 것들의 사상을 위한 표를 만들게 되어있다.
  - 사설 IP 주소를 정적인 하나의 공인 IP 주소 변환하기 위한 주소 설정
  - 사설 IP 주소를 회사가 가질 수 있는 공인 IP 주소들 중에서 어떤 하나와 사상되도록 설정
  - 사설 IP 주소에 특정 TCP 포트를 더한 것을 하나의 공인 IP 주소로 변환하기 위한 설정
  - 공인 IP 주소를 사설 IP 주소 중의 하나로(순서는 라운드 로빈 방식을 사용) 변환하기 위한 설정

## 2. 네트워크 활용

### 2.1 IP Routing

#### 2.1.1 IP 라우팅의 종류 [1급]

##### (1) Static Route 및 Dynamic Route

###### o 핵심가이드

- 라우팅 테이블의 역할 이해
- 가상회선의 이해

###### o 라우터는 네트워크들을 연결해 한 통신망에서 다른 통신망으로 통신할 수 있도록 도와주는 하드웨어와 소프트웨어 장치로 전송을 전담하는 장비이다.

###### - 라우터 동작 원리

- 인터넷은 라우터를 중심으로 하는 하나의 네트워크들의 연결 고리로 되어 있으며 특정 네트워크의 A라는 사람이 다른 네트워크의 B라는 사람에게 데이터를 보내고자 한다면, A라는 사람이 송신한 데이터를 A의 라우터로 전송된다.
- 라우터는 들어온 패킷이 주위에 있는 여러대의 라우터중 어느 라우터로 패킷을 보내야할 지를 결정할 수 있어야만 한다. 라우터의 입장에서 패킷에 적혀있는 목적지 주소(IP)와 라우팅 테이블을 이용하여 라우팅을 수행할 수 있으며, 라우팅 테이블은 패키지가 목적지 주소로 올바르게 전달되기 위해서는 어느 인터페이스를 통해서 다음 라우터로 전달되어야 하는지에 대한 정보를 가진 테이블이다.

[표 2-6] 라우팅테이블 예시

목적지 주소	마스크	인터페이스
222.110.3.0	255.255.255.0	eth0
222.110.4.0	255.255.255.0	eth1
222.120.0.0	255.255.0.0	eth2

- 라우팅 테이블의 구조는 목적지IP를 가지는 패킷이 라우터의 어느 인터페이

스를 사용해야 하는지에 대한 정보 테이블이며, 만약 패킷이 들어왔는데, 패킷의 IP헤더에 포함된 목적지 주소가 222.110.3.1에서 222.110.3.254 사이의 값을 가진다면 라면 라우팅 테이블의 정보에 의해서 인터페이스 eth0으로 보내진다. 이와 같은 방식으로 라우터간에 라우팅이 되어 수신자 네트워크의 라우터까지 전달된다.

- 라우팅 테이블을 구축하는 방법은 일반적으로 동적으로 구현하는 동적 라우팅과 정적으로 구현하는 정적 라우팅으로 분류한다.
  - 동적 라우팅 : 동적 라우팅 프로토콜을 사용하여 라우터가 스스로 이웃한 라우터와 라우팅 테이블을 서로 교환하면서 라우팅 테이블을 구축하는 방법이다. 만약 사용할 경로가 삭제 또는 변경되면 라우터는 즉시 이웃한 라우터에 자동으로 삭제된 경로 정보 또는 변경된 경로 정보를 전송한다. 따라서 초기 설정이외 별도의 관리가 필요없는 라우팅 테이블 구축 방법이다. 이와 같은 라우팅 프로토콜로는 RIP v1, RIP v2, OSPF와 같은 프로토콜이 있다.
  - 정적 라우팅 : 관리자가 직접 라우터가 사용할 경로를 라우팅 테이블에 입력함으로 라우팅 테이블을 구축하는 방법이다. 만약 사용할 경로가 삭제 또는 변경되면 그때마다 번거롭지만 관리자가 라우팅 테이블에 경로 정보를 삭제 또는 변경해주어야 한다. 따라서 라우팅 경로가 고정되어있는 네트워크 또는 라우팅 경로가 적은 네트워크에서 사용할 수 있는 라우팅 테이블 구축 방법이다
- 가상회선은 패킷교환망의 경우 가입자에게 물리적인 경로를 단독으로 사용하도록 허용하지 않는다. 즉 물리적인 경로를 타 가입자와 공유하면서 전송할 데이터가 있을 때에만 일정 대역폭을 사용하여 상대방에게 데이터를 전송하도록 한다. 호출 성립 이후 양측의 단말기는 회선 교환망의 경우처럼 물리적인 경로를 단독 사용할 수는 없지만 논리적인 통신경로를 호출 해제시까지 유지하는데 이 논리적인 통신경로를 가상회선(Virtual Circuit)이라고 하며, 두 라우터간의 데이터는 가상회선(Virtual Circuit)을 성립한 후 전송된다. 전송이 완결되면 사용한 가상회선은 다운된다. 추후 데이터를 다시 전송할 경우가 발생되면, 새로운 가상회선이 생성된다. 이러한 형태를 SVC(Switched Virtual Circuit)라고 한다. 반면에, 가상회선을ダイナミック하게 성립, 삭제를 반복하지 않고, 서비스제공자는 자신에게 등록된 고객에게 지속적으로 가상회선을 제공하기도 한다. 이를 PVC(Permanent Virtual Circuit)이라고 한다.

## (2) 라우팅 알고리즘

- 핵심가이드
  - 링크상태 라우팅 알고리즘 개념 이해
  - 거리벡터 라우팅 알고리즘 개념 이해
  - 기타 라우팅 알고리즘 개념 이해
- 링크상태 라우팅 알고리즘은 자신을 중심으로 전체 네트워크의 토폴로지를 그릴 수 있는 복잡한 토폴로지 정보 DB를 가진다. 이 정보 DB를 이용하여 SPF 알고리즘을 통해 SPF 트리를 만들어 내고, 이 트리를 가지고 라우팅 테이블을 유지 관리하며 패킷에 대한 스위칭을 수행한다. 이 알고리즘은 복잡한 전체 네트워크 구성을 모두 가지고 있어야 되므로 상당히 메모리를 많이 사용하게 되는 부담도 있다. 그러나 네트워크의 변화가 생겼을 때 상당히 빨리 전체 네트워크에 정보가 전달된다. 또한 네트워크의 모든 정보를 가지고 있기 때문에 복잡하고 정교한 네트워크 제어가 가능하다
- 거리벡터 라우팅 알고리즘은 네트워크 토폴로지 정보 데이터베이스의 유지 관리하고 특정 링크에 대한 방향(vector)과 거리(distance)를 결정하는 알고리즘이다. 라우터는 연결된 라우터들에 대한 거리벡터값과 인터페이스 정보를 데이터베이스로 유지하면서 이 정보를 이용하여 패킷을 전달한다.

## (3) default route

- 핵심가이드
  - IP Network Address에 대한 route가 없을 때의 라우팅
- 디폴트 라우트(Default Route)는 라우터에서 패킷을 수신하면 라우팅 테이블상에 상대방 네트워크 IP 어드레스를 검색하여 패킷을 어디로 보낼 것인가를 결정하는데, 라우터에 Default Route가 설정이 되어 있으면, 라우팅 테이블상에서 등록되어 있지 않는 모든 정보들이 지정된 경로로 전송하게 된다.

## 2.2 네트워크 장비 이해

### 2.2.1 랜카드

- 핵심가이드

- 랜카드의 동작원리 이해
- Half/Full-duplex 개념 이해
- 커넥터 및 케이블링 이해

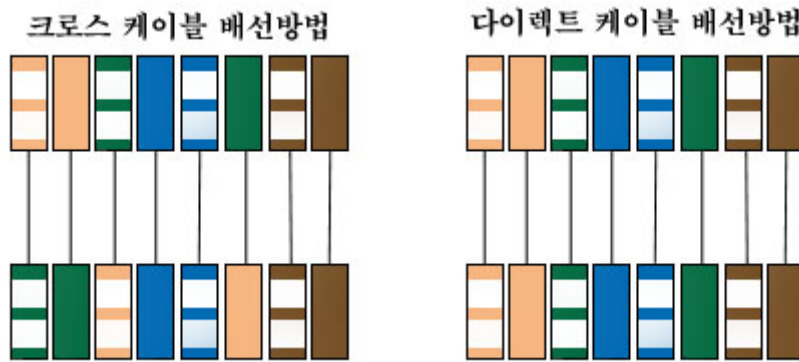
### (1) Half/Full-duplex 이해

- o 랜카드는 단순히 PC 혹은 네트워크에서 전달되어오는 정보를 상호 교환할 수 있도록 만들어 준다. PC에서 전송 요구가 발생 하면 랜카드로 정보를 일정한 형태로 만들어 보내고 랜카드에서는 이 정보를 일단 버퍼에 저장한 다음 네트워크에 맞는 형태로 보낸다. 여기서 PC와 랜카드사이에서 논리적으로 묶어주는 소프트웨어가 필요한데, 이 소프트웨어를 네트워크 드라이버라고 한다.
- o 랜카드 종류
  - Full Duplex
    - 송신 스테이션과 수신 스테이션이 동시에 양방향으로 데이터를 전송할 수 있는 방식으로 이 기능을 사용하기 위해서는 Server에 Full Duplex 기능을 지원하는 NIC를 사용해야 한다.
  - Half Duplex :
    - 송신 스테이션과 수신 스테이션간에 한 번에 한 방향으로만 데이터를 전송할 수 있는 방식으로 Hub의 경우는 CSMA/CD방식으로 동작하므로 Half Duplex만 지원한다.

### (2) 커넥터 및 케이블링 이해

- o 랜을 구성하는 케이블은 네트워크를 구성할 때 가장 많이 사용하는 케이블이 UTP 케이블이다 UTP 케이블의 구조는 4쌍의 전선(총 8가닥)이 서로 꼬여져있는 형태이며, 현재 가장 많이 사용되는 것은 Category 5이며 안정적인 전송거리는 100m 이내이다. 케이블 배선방법에 의해 다이렉트(Direct)케이블과 크로스(Cross)케이블로 나누어집니다.
  - 다이렉트 케이블의 경우는 케이블 양단이 똑 같은 순서에 의해 동일하게 구성된다. 다시말해 케이블 양단의 각 배선들이 1-1로 연결되는 형태이다. 컴퓨터와 허브간을 연결할 때는 다이렉트 케이블을 사용한다.
  - 크로스케이블은 케이블 양단의 송신, 수신선이 서로 교차(1-3, 2-6번선 교차)되도록 구성된다. 크로스케이블은 케이블 자체내에서 수신이 송신으로, 송신이

수신으로 연결되도록 하는 형태이다. 컴퓨터와 컴퓨터간을 1-1로 연결할 때는 크로스케이블을 사용한다.



(그림 2-6) 케이블링 방식

o 케이블링을 위한 툴

- 케이블링 툴은 UTP케이블의 끝에 RJ-45 커넥터를 연결해주는 도구로 대개 피복을 벗겨내는 스트리퍼의 기능도 함께 가지고 있다.
- 피복절단기는 UTP 케이블의 내선이 잘리지 않도록 피복부분만을 잘라주는 도구이다
- 테스터는 케이블을 제작한 후에 정상적인 송수신이 이루어지는지 여부를 확인하는 도구이다.
- RJ-45 커넥터는 랜카드나 허브의 포트에 연결하게 해주는 커넥터이며, 커넥터와 전선사이의 연결부분을 보호해주는 것을 보호부트라고 한다.

2.2.2 허브, 스위치 및 브리지

o 핵심가이드

- 허브의 기능 및 종류별 특징
- 스위치의 기능 및 종류별 특징
- 브리지의 기능

(1) 허브(Hub)

- o 허브는 집중화 장비(Concentrator)라고 부르기도 하며, 각 Node들을 연결시켜주

는 역할을 한다. 허브는 공유방식(CSMA/CD)을 사용하며, 각 Node들은 주로 UTP Cable을 통해 연결된다.

o 허브의 종류

- 더미허브는 단순히 여러 대의 컴퓨터를 연결할 수 있는 기능만을 가진 허브이다. 이 허브는 회선의 속도를 여러 대의 컴퓨터가 나누어 쓰므로 접속되는 컴퓨터의 개수대로 속도가 나뉘어 진다.
- 스택터블 허브는 더미 허브들을 여러 개 쌓아 놓을 수 있는 허브들을 말한다. 대부분의 네트워크에서 이 더미 허브 들을 여러 개 쌓아 놓고 있다.
- 스위칭허브는 더미 허브가 하나의 회선을 여러 대의 컴퓨터들이 나누어 쓰면서 속도의 저하가 발생하는 것을 개선하여 여러 대의 컴퓨터들을 연결하여도 원래의 속도를 사용할 수 있는 허브를 말한다. 이를 위해서 맥테이블을 메모리에 저장한다.
- 인텔리전트 허브는 더미 허브의 기능을 가진 컴퓨터에 네트워크 관리 기능이 추가된 허브를 말한다.
- 엔터프라이즈 허브는 이더넷과 토큰링, FDDI와 같은 다중 매체를 지원하는 허브이다. 그러므로 하나의 허브에 여러 종류의 네트워크를 연결할 수 있는 허브를 말한다.

(2) 스위치(Switch)

o 스위치는 스위칭허브이라고도 불리지만 허브보다 훨씬 더 나은 기능을 제공한다. 스위치는 호스트 A와 B가 통신하는 순간에도 호스트 C와 D는 통신할 수 있다. 스위치는 허브와는 달리 공유방식을 사용하지 않고, 포트별로 Dedicate한 대역폭을 할당해 준다.

o 스위치의 종류

- L2 스위치 : Mac Address 기반 스위칭
- L3 스위치 : IP Address 기반의 트래픽 조절 가능
- L4 ~ L7스위치 : Port Number 또는 Packet 내용을 분석 및 판단하여 Packet 의 경로 설정, 변환, 필터링 동작을 수행할 수 있는 장비

o L4스위치와 L7스위치의 차이점

- 구조적 차이점
  - L4스위치 : TCP/UDP 포트 정보를 분석해 해당 패킷이 현재 사용하는 서비스 종류(HTTP, FTP, 텔넷, SMTP, POP3, SSL등)별로 패킷을 처리

- L7스위치 : 트래픽의 내용(e-mail의 문자열, HTTP URL, FTP 파일 및 제목 등)패턴 등을 분석해 패킷을 처리
- 기능적 차이점
  - 높은 수준의 Intelligence를 갖춘 스위치일수록 더 정교한 패킷의 부하분산 (Load Ballancing)및 QoS기능 구현이 가능함.

### (3) 브리지(Bridge)

- o 브리지는 OSI 7 계층 모델에서 2 계층인 데이터 링크 계층에서 동작한다. 데이터 링크는 LLC(Logical Link Control) 계층과 MAC 계층으로 나뉘어지는데 그 중 MAC 계층에서 브리지가 동작한다. 그래서 MAC 계층 브리지라고도 한다. 브리지가 동작하려면 라우팅 테이블이 필요하다. 이 테이블은 브리지의 램에 만들어지는데 처음에는 비어있다가 처음으로 브리지가 패킷을 받으면 그 정보를 라우팅 테이블에 저장하게 된다. 여기 들어가는 주소는 MAC 주소가 들어간다.
- o 전송되는 데이터 패킷을 라우팅 테이블과 비교해서 같은 세그먼트에 있다고 판단되면 브리지는 상대방 세그먼트로 패킷을 전달하지 않고 아니면 전송을 실행한다.

### 2.2.3 VLAN [1급]

- o 핵심가이드
  - VLAM의 개념
  - VLAM의 표준 이해

#### (1) VLAN(virtual LAN)

- o VLAN이란 브로드캐스팅 트래픽을 제한하여 불필요한 트래픽을 차단하기 위한 논리적인 LAN이다. VLAN은 물리적으로 LAN을 분리하는 것이 아니라 논리적으로 한 장비 내에서 브로드캐스팅 도메인을 나누는 것이다. 스위치에 연결된 호스트들을 그룹으로 나누어서 VLAN 1 과 VLAN 2으로 그룹을 설정할 수 있으며 호스트는 각자의 VLAN 내에 속한 호스트들 간에 통신은 가능하지만 다른 VLAN에 속한 호스트들과의 통신은 불가능하다. 또한 VLAN 1내의 브로드캐스팅 트래픽은 VLAN 2로 전달되지 않는다.



o VLAN 종류

- 포트기반 VLAN : 포트기반 VLAN은 스위치 포트를 각 VLAN에 할당하는 것으로 같은 VLAN에 속한 포트에 연결된 호스트들 간에만 통신이 가능하다. 이 VLAN은 가장 일반적이고 많이 사용되는 VLAN이다
- 맥어드레스기반 VLAN : 맥어드레스 VLAN은 각 호스트들의 맥어드레스를 VLAN에 등록하여 같은 VLAN에 속한 맥어드레스들 간에만 통신이 되도록 하는 방법이다. 이 VLAN은 호스트들의 맥어드레스들을 전부 등록해야 하기 때문에 자주 사용되지는 않는다.
- 네트워크주소기반 VLAN : 네트워크주소별로 VLAN을 구성하여 같은 네트워크에 속한 호스트들 간에만 통신이 가능하도록 구성한 VLAN이다. 주로 IP 네트워크 VLAN을 사용한다.
- 프로토콜기반 VLAN : 같은 통신 프로토콜(TCP/IP, IPX/SPX, NETVIEW 등)을 가진 호스트들 간에만 통신을 가능하도록 구성된 VLAN이다

o Port Mirroring

- 스위치는 허브처럼 한 포트에서 발생한 데이터를 전 포트에 전달하지 않기 때문에 스위치에 흐르는 데이터를 분석하려면 허브와는 달리 Port Mirroring기능을 사용해야 한다. 스위치 1번 포트에 흐르는 트래픽을 Analyzer로 조사하려면 1번 포트에 흐르는 트래픽을 트래픽 분석장비가 설치된 포트에 복사하여 보내야 한다. 이것을 Port Mirroring이라고 한다.

2.2.4 라우터 구성 명령어의 이해

o 핵심가이드

- 시스코라우터 구성모드 이해
- 시스코라우터 기본 명령어 이해
- 라우터에서 각종 암호를 설정하는 방법 이해

(1) CISCO 라우터 구성 모드

- o 라우터는 동일한 전송 프로토콜을 사용하는 분리된 네트워크를 연결하는 장치로 네트워크 계층간을 서로 연결한다. 라우터는 브리지가 가지는 기능에 추가하여 경로 배정표에 따라 다른 네트워크 또는 자신의 네트워크 내의 노드를 결정한다. 그리고 여러 경로 중 가장 효율적인 경로를 선택하여 패킷을 보낸다. 라

라우터는 흐름제어를 하며, 인터넷워크 내부에서 여러 서브네트워크를 구성하고, 다양한 네트워크 관리 기능을 수행한다. 브리지와 라우터의 차이점을 간단히 살펴보면, 라우터는 네트워크 계층까지의 기능을 담당하고 있으면서 경로 설정을 해준다.

o 라우터 모드

- privileged mode에서 global configuration mode로 전환할 수 있으며, global configuration mode에서 하위 configuration mode로 전환할 수 있다.
- setup mode도 privileged mode에서 전환 가능하다.
- global configuration mode로 전환하려면 privileged mode prompt에서 다음과 같이 명령 입력해야 한다.
  - Router# configuration terminal
- 하위 configuration mode로 전환하려면 global configuration mode prompt에서 다음과 같이 명령을 입력해야 한다. 여기에서는 interface configuration mode로 가기 위한 것을 보인다.
- 각 하위 configuration mode의 prompt가 다른 것을 주목하자.
  - Router(config)# interface serial 0
  - Router(config-if)#

User Mode Router> 제한된 명령어만을 이용	Priviledged mode Router# 모든 명령어를 이용할 수 있고 configuration file 조정할 수 있음.
Setup Mode 초기 환경설정 Priviledged mode 에서 명령어 setup을 입력	RXBOOT mode 비밀번호를 잃어버렸거나 Flash의 OS가 지워지는 등의 경우 이용
Global configuration mode Router(config)# 라우터 운영 전체에 영향을 미치는 요소들을 조정할 수 있음. 하위 configuration mode로 전환할 수 있음.	하위 configuration mode Router(config-???)# 영역별 환경 설정

(그림 2-7) 라우터 모드

## (2) CISCO 라우터 명령어 이해

### o 모드변환

- router>enable <-- 사용자 모드에서 특권 모드로 변경
- router#diabile <-- 특권 모드에서 사용자 모드로 변경
- router#configure terminal <-- config 모드로 변경
- router(config)#CTRL+Z 또는 exit <-- config 모드에서 빠져나올 때
- router#

### o 도움말

- 프롬프트 상에서 도움말 보기 : ?
- 명령어의 활용법 : 명령어 ?

### o 환경설정

- hostname 변경
  - router(config)#hostname Router-A
  - router-A(config)#^z
  - router-A#write memory
- 배너 설정
  - router(config)#banner motd \$
  - This is MOTD banner 이라고 배너 내용 입력하고 \$로 메시지 끝을 알린 후 라우터 재접속하면 배너를 확인 가능
- 시간 설정
  - router(config)#ntp server 시간서버IP
- 셋팅값을 NVRAM에 저장해서 리부팅시에도 적용
  - router#Copy runn-config startup-config

### o interface ip address변경

- router(config)# interface serial 0
- router(config-if)# no ip address <- 기존 ip address를 삭제
- router(config-if)# ip address 172.16.4.1 255.255.255.0
  - 명령 형식 : ip address {ip address} {net mask}

### o telnet으로 접근할 수 있게 설정

- router(config)#interface ethernet0
- router(config-if)#ip address 192.168.0.1 255.255.255.0
- router(config-if)#no shutdown

- Telnet session 활성화
- router(config)#line vty 0 4 -> 동시에 5명까지 telnet 접속 허용
- router(config-line)#login
- router(config-line)#password \*\*\*\*

(3) 라우터에서 각종 암호를 설정하는 방법 이해

o 라우터에 로그인하기 위해서는 username 없이 초기 암호를 입력하여 로그인해야 하는데 이때 프롬프트가 Router>와 같이 되며 이때의 모드를 User exec 모드라고 한다. 이후 enable 또는 en 명령어를 실행하여 다시 암호를 입력하면 프롬프트가 Router#와 같이 되며 이때의 모드를 Privileged exec 모드 또는 enable 모드라고 한다. 여기에서 초기에 User exec 모드로 들어가기 위해 입력하는 암호를 일반사용자, Privileged exec 모드 또는 enable 모드는 관리자 암호라고 생각하면 된다.

o 라우터 암호설정

- 콘솔 패스워드 설정 : 로그인후 enable을 실행하여 Privileged EXEC 모드로 들어가도록 한다. 이후 설정을 변경하기 위해 "conf t"를 실행하여 Global Configuration 모드로 들어간 후 콘솔을 지정하여 암호를 재설정하면 된다.

- Router#configure terminal
- Router(config)#line console 0
- Router(config-line)#password \*\*\*\*\*
- Router(config-line)#^Z

- 터미널 패스워드 설정 : 원격 관리를 위한 로그인에 필요한 암호를 Terminal password 또는 Virtual password 라고 한다.

- Router#configure terminal
- Router(config)#line vty 0 4 <=== 터미널 수
- Router(config-line)#password \*\*\*\*\*
- Router(config-line)#^Z

- Enable 패스워드 및 Enable Secret 패스워드 설정 : Privileged EXEC 모드로 접근하기 위해서는 enable 명령어를 실행하여 암호를 입력하여야 하는데, 이때의 암호는 아래와 같이 enable password 또는 enable secret를 이용할 수 있는데, 각각은 지정한 암호가 평문으로 저장되는지 아니면 암호화되어 저장되는지의 여부에 차이가 있다.

- Router#configure terminal
- Router(config)#enable password \*\*\*\*\*
- Router(config)#^Z
  
- Router#configure terminal
- Router(config)#enable secret \*\*\*\*\*
- Router(config)#^Z

## 2.2.5 네트워크 장비를 이용한 네트워크 구성 [1급]

### o 핵심가이드

- 각각의 인터페이스에 적당한 IP 주소를 설정 이해
- 네트워크를 구성 이해
- 라우팅 프로토콜이 선택 방법 이해

### (1) 각각의 인터페이스에 적당한 IP 주소를 설정

#### o IP 할당

- 기본적인 네트워크 구성에서는 네트워크의 호스트 수에 따라서 IP주소를 할당 받고 조직체계에 따라서 그룹별로 분류하여 IP 주소를 할당하여 관리한다.
- 공인 IP 주소가 부족한 경우에는 사설 IP주소를 사용할 수 있다.

### (2) 네트워크를 구성

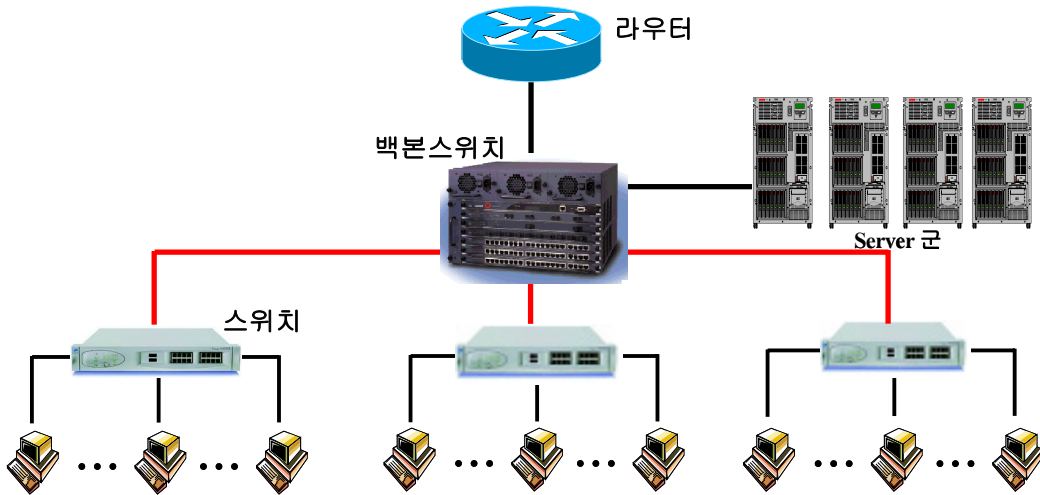
#### o 네트워크 구성 절차 이해

- 조직의 업무상황 파악
- 네트워크를 설계
- 네트워크를 구축
- 구축된 네트워크 테스트

#### o 소규모 네트워크 구성

- 그룹별로 스위치 또는 허브를 설치하고 각각의 호스트와 연결
- 스위치를 백본스위치에 연결
- 백본스위치에서 라우터로 연결하여 외부망과 연결

- 서버들이 있는 경우 백본스위치에 직접 연결하여 서버 운용



(그림 2-8) 소규모 네트워크 구성

### (3) 어떠한 라우팅 프로토콜이 필요한지 이해

- o 라우팅 프로토콜은 라우터에서 라우팅을 위해서 인접한 라우터의 정보를 유지 및 관리를 하여야하는데 이때 네트워크 정보 생성 후 네트워크 정보를 교환 및 제어하는 프로토콜을 말한다.
- o 라우팅 프로토콜 선택 기준
  - 네트워크 그룹의 범위 기준
    - Interior Gateway Protocol(IGP) : RIP, OSPF, IGRP 등(Autonomous System(AS) 내에서의 라우팅 프로토콜)
    - Exterior Gateway Protocol(EGP) : EGP, BGP 등(Autonomous System(AS) 사이에서의 라우팅 프로토콜)
  - 라우팅 알고리즘 기준
    - 거리벡터 알고리즘
    - 링크상태 알고리즘
- o 라우팅 프로토콜 이해
  - RIP는 인테리어 라우팅 프로토콜로서, 전통적인 DISTANCE VECTOR ALGORITHM 을 사용한다. 현재 널리 사용하고 있는 프로토콜 중 하나로서

소규모 네트워크에 적합한 라우팅 프로토콜이다.

- OSPF 프로토콜은 계층적 구조로 네트워크 구성이 가능하다. OSPF에는 라우팅 도메인이며, 대규모 네트워크에 적합하다.
- IGRP 프로토콜은 시스코(Cisco)사에서 독자적으로 개발한 프로토콜로, 독립적 네트워크 내에서만 사용하기 위해 개발되었다. 네트워크의 규모가 크고 복잡하더라도 안정적으로 움직일 수 있도록 되어 있다.

## 2.2.6 네트워크 토폴로지 이해 [1급]

### o 핵심가이드











- 토폴로지 이해
- 네트워크의 배열이나 구성 표현 방법 이해
- 네트워크 토폴로지를 종류별로 이해

#### (1) 토폴로지의 일반적인 의미 이해

- o 토폴로지(Topology: 위상) : 네트워크 토폴로지는 네트워크에 있는 컴퓨터, 케이블 및 다른 구성요소의 배치로 일종의 네트워크 지도와 같다. 사용하는 토폴로지 종류는 네트워크 하드웨어의 종류와 기능, 그 관리, 미래의 확장 가능성에 영향을 미치므로 각자 자신의 환경에 맞는 선택을 하는 것이 중요하다.

#### (2) 네트워크의 배열이나 구성을 개념적인 그림으로 표현

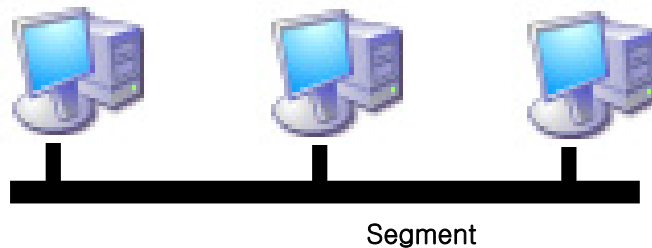
- o 네트워크 배열 및 구성 그림으로 표현하기 위해서는 네트워크 설계시에 사용하는 기호 및 표현법을 이해하여야 한다.

<b>LAN</b>	 Bridge	 Hub	 Ethernet Switch	 Router	 ATM Switch
<b>WAN</b>	 Router	 X.25 or FrameRelay Switch	 Modem DSU/CSU NT1/TA	 Comm Server	 ATM Switch

(그림 2-9) 네트워크장비 심볼

(3) 네트워크 토폴로지들 이해 (star형, 망형, 버스형, 환형, 나무형 등)

- o 네트워크 구성에 사용되는 다섯 가지 기본 토폴로지가 있다.
- o 버스 토폴로지(Bus Topology) : 네트워크의 모든 컴퓨터들이 연속된 케이블 또는 세그먼트에 접속되어 직선으로 연결된다.
  - 장점 : 저렴한 비용. 네트워크 구성이 간단
  - 단점 : 어느 한 부분이 끊어지거나 한 끝이 중단되지 않으면 신호가 네트워크를 통해 왕복하여 모든 통신이 중지된다. 또 버스에 접속된 컴퓨터수에 따라 네트워크 성능 크게 저하되는 단점이 있다.



(그림 2-10) 버스 토폴로지

- o 스타 토폴로지(Star Topology) : 네트워크의 각 컴퓨터에서 나온 케이블 세그먼트가 허브라는 중앙 구성요소에 연결된다. 컴퓨터는 허브를 거쳐 네트워크의 모든 컴퓨터로 신호가 전송된다.
  - 장점 : 한 컴퓨터가 고장나도 고장난 컴퓨터만이 데이터를 송신, 수신할 수 없고 나머지 부분은 정상작동이 가능
  - 단점 : 각 컴퓨터가 허브에 연결되기 때문에 허브가 고장나면 전체네트워크가 고장난다는 것이고, 네트워크에서 노이즈가 많이 발생한다는 것이다.
- o 링 토폴로지(Ring Topology) : 링 토폴로지에서는 컴퓨터들이 하나의 케이블 원에 연결된다. 신호는 루프를 이루며 한 방향으로 주행하며 신호를 강화하여 다음 컴퓨터에 보내는 리피터 역할을 하는 각 컴퓨터를 통과한다. 더 큰 규모에서는 TickNet 동축케이블 또는 광섬유 케이블을 사용하여 여러 랜을 링 토폴로지로 연결할 수 있다.
  - 장점 : 트래픽이 많은 환경을 버스 네트워크보다 잘 처리할 수 있고 노이즈의 영향이 작다.
  - 단점 : 이것 역시 회선 단절 시 데이터 전송의 두절을 초래하는데 이것을 방



지하기 위해 이중 링 구조를 더 선호한다. 단일 토크링에서 한번에 한 대만이 데이터를 보낼 수 있고, 대개 버스 기술보다 비용이 많이 든다.

- 메쉬 토폴로지(Mesh Topology) : 각 컴퓨터가 별도의 케이블을 통해 모든 다른 컴퓨터에 연결된다. 이 연결은 네트워크를 통해 중복 경로를 제공하므로 한 케이블이 고장나면 또 다른 케이블이 트래픽을 전달하고 네트워크가 계속 작동한다.

- 장점 : 네트워크를 통해 여러 경로를 제공하는 백업기능이 강하다.

- 단점 : 중복 경로에는 케이블이 다른 토폴로지에 필요한 것보다 더 많이 필요하므로 비용이 많이 들어 실제 사용은 드물다.

- 혼성 토폴로지(Hybrid Topology) : 둘 이상의 토폴로지를 결합하여 전체 네트워크 디자인을 구성하는 것이다. 실제 한 종류의 토폴로지를 사용하여 네트워크를 디자인하는 경우는 드물다. 일반적으로 스타-버스 토폴로지와 스타-링 토폴로지 두 종류의 혼성기술이 많이 사용된다.

- 스타-버스형 : 여러 스타 토폴로지 네트워크를 버스 연결장치에 연결한다. 스타구성이 채워지고 나면 두 번째 스타를 추가하고 버스 연결을 사용하여 두 스타 토폴로지를 연결할 수 있다. 한 컴퓨터가 고장나도 네트워크의 나머지 부분에 영향이 미치지 않는다(스타구조의 단점이 보완됨)

- 스타-링형 : 스타-링 토폴로지에서는 스타 네트워크에서와 같이 컴퓨터들이 중앙 구성요소에 연결된다. 그러나 이러한 구성요소들이 연결되어 링 네트워크를 형성한다. 이는 한 컴퓨터가 고장나도 네트워크의 나머지 부분에는 영향이 없다. 토큰 전달을 사용하면 스타-링 토폴로지의 각 컴퓨터는 같은 통신 기회를 가진다. 따라서 스타-버스 토폴로지의 경우보다 세그먼트사이에 더 많은 네트워크 트래픽이 허용된다.

## 2.2.7 각종 네트워크 응용 프로그램의 작동 원리와 활용 [1급]

- 핵심가이드

- 기타 다른 네트워크 응용 프로그램의 작동원리 및 활용방안에 대해 이해

(1) 기타 다른 네트워크 응용 프로그램의 작동원리 및 활용방안에 대해 이해

## 2.3 무선통신

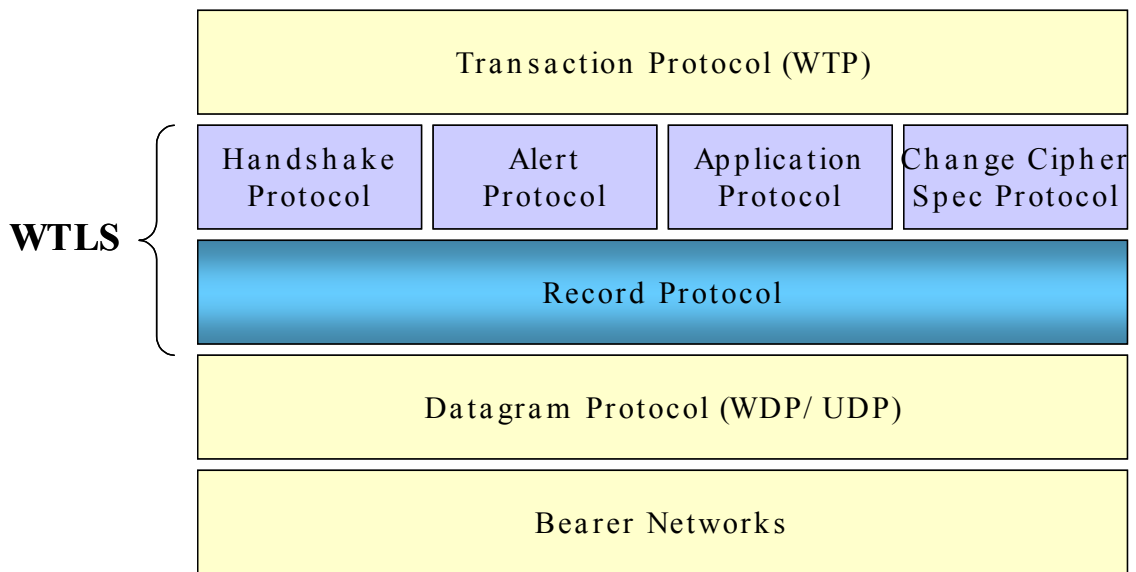
### 2.3.1 이동통신(PDA, WAP) 등

#### ○ 핵심가이드

- Wireless Application Environment(WAE) 이해
- Wireless Session Layer(WSL) 이해
- Wireless Transport Layer Security(WTLS) 이해

#### (1) Wireless Application Environment(WAE) 이해

- WAP은 무선망과 WWW(World Wide Web)의 연동을 위하여 Proxy기능을 이용한다. WAP의 Proxy는 다음의 역할을 한다.
  - 프로토콜 게이트웨이 : WAP의 게이트웨이는 WAP 프로토콜 스택(WSP, WTP, WTLS, WDP)을 WWW프로토콜 스택(HTTP, TCP/IP)으로 변환한다.
  - 콘텐츠 인코딩과 디코딩 : 콘텐츠 인코더는 네트워크의 부하를 줄이기 위하여 WAP콘텐츠에서 작게 인코딩된다.
- 인프라 구조는 사용자가 무선 단말기를 이용하여 WAP 콘텐츠와 애플리케이션을 이용할 수 있도록 하며, 애플리케이션 제작자들이 광대한 무선 통신망에서 사용되는 서비스와 애플리케이션을 제작할 수 있도록 한다. WAP Proxy는 콘텐츠와 애플리케이션이 표준 WWW서버 위에서 호스팅되게 하며 CGI 프로그래밍과 같은 검증된 WWW의 기술을 바탕으로 발전하고 있다.
- WAP은 휴대폰, 호출기, PDA 등의 무선 단말기를 위한 응용 구조와 프로토콜을 정의한다. GSM(Global Standard for Mobiles), TDMA(Time Division Multiple Access), CDMA(Code Division Multiple Access) 등의 서로 다른 망에서 쓰일 수 있는 프로토콜을 정의하고 개발자들이 빠르고 유연하게 더 나은 서비스와 응용 기술을 개발할 수 있도록 한다.



(그림 2-11) WAP 레이어

o WAE(Wireless Application Environment)

- WAE는 WWW와 이동통신에 기반한 애플리케이션 환경이며 주 목적이 서비스 공급자들과 개발자들이 다양한 무선 환경에서 효율적으로 애플리케이션과 서비스를 개발하도록 호환적인 환경을 제공하는 것을 목적으로 하기 때문에 무선인터넷 서비스를 개발하기 위해서는 반드시 필요하다.
- WAE는 다음과 같은 포맷을 인식할 수 있는 환경을 제공한다.
  - WAP 게이트웨이에서의 WAE
  - WAP 클라이언트에서의 WAE
  - WML : HTML 과 유사한 가벼운(light-weight) 언어, 무선 단말기를 위해 최적화 되어야 한다.
  - WML Script : Java Script 언어와 유사한 가벼운 스크립트 언어.

(2) Wireless Session Layer(WSL) 이해

- o WSP(Wireless Session Protocol)는 2개의 session 서비스에 대한 일관적인 인터페이스로 WAP의 애플리케이션 레이어를 제공한다. 이러한 세션 서비스는 연결기반 서비스와 비연결기반 서비스로 연결기반 서비스는 WTP 상에서 동작하고 비연결기반 서비스는 WDP위에서 동작한다.

### (3) Wireless Transport Layer Security(WTLS) 이해

- WTLS(Wireless Transport Layer Security)는 SSL(Secure Socket Layer)로 알려진 산업 표준인 TLS 프로토콜에 기반한다. WTLS는 WAP을 위해 설계되었으며 좁은 밴드의 통신 채널에 맞도록 최적화되었다. WTLS의 특징은 다음과 같다.
  - Data integrity
  - Privacy
  - Authentication
  - Denial of service protection
- WDP( Wireless Datagram Protocol ) layer는 다양한 네트워크에 의해 지원되는 bearer 서비스를 이용하는 데이터 위에서 작동한다. 일반적인 통신 서비스로써 WDP는 상위레이어로 일관적인 서비스를 제공하며 bearer 서비스위에서 작동한다. WDP 프로토콜이 상위 레이어 프로토콜에 대하여 통상의 인터페이스를 제공하기 때문에 Security, Session, Application 레이어는 무선망에 대하여 독립적으로 작동할수 있다.

### (4) Wireless Transport Layer(WTP) 이해

- 핵심가이드
  - Wireless Transport Layer(WTP) 이해
- WTP는 datagram 서비스의 위에서 동작한다. client(mobile station)에 구현하기에 적합한 가벼운 트랜잭션 기반의 프로토콜을 제공한다. WTP는 안전성이 보장되거나 보장되지 않는 무선 데이터그램 망에서 효과적으로 동작한다.
- WTP의 특징은 3 종류의 트랜잭션 서비스를 제공
  - 신뢰성이 없는 단방향 요구
  - 신뢰성 있는 단방향 요구
  - 신뢰성 있는 양방향 요구 응답

## 2.3.2 이동/무선통신 보안 [1급]

### (1) 보안정책

- 핵심가이드

- 조직이나 업체가 무선랜을 도입하여 강화된 보안 정책 수립
- 무선랜 이해
  - 무선랜은 기존 네트워크는 전화선이나 통신케이블 등의 유선으로 연결된 호스트간의 통신 방식을 이용하는데 이것을 대신하여 전파를 이용하여 통신을 수행하는 것으로 크게 두 가지 컴포넌트로 구성된다.
    - 액세스 포인트(Access Point)
    - 무선랜 네트워크 어댑터(Wireless Network Interface Card)
  - AP는 유선 네트워크에 접속되어 무선 사용자들의 트래픽을 중계하는 역할을 담당하는 장비이고 무선랜 네트워크 어댑터는 무선랜 터미널(STA)에서 AP로 접속하기 위한 네트워크인터페이스를 담당하는 장비이다. 기존의 사내 네트워크 혹은 인터넷 접속은 모두 유선으로만 이뤄져 있어 물리적으로 침투 위치를 확보해야만 하지만 무선랜의 경우에는 전파가 도달 가능한 거리에 있는 경우 어디에서든지 스니핑과 같은 공격이 가능하다. 또한 무선랜은 사내망이므로 기존 인터넷 접속 망에 적용되는 보안 정책을 적용하기가 쉽지 않다
- 무선랜 보안정책 수립 방법
  - 무선랜 보안정책을 수립하기 위해서는 무선랜에 대한 네트워크 구성 및 특성을 이해하고 무선랜의 보안 취약점을 고려하여 보안정책을 수립하여야 한다.
- 무선랜 보안 취약점
  - 무선환경의 물리적 특성에 의한 취약점
    - AP의 전파가 강하게 설정되어 건물 외부에까지 출력될 경우 건물 외부에서도 내부 네트워크에 접속 가능
    - 무선랜은 유선처럼 물리적으로 랜케이블을 연결할 필요가 없기 때문에 관리자의 눈을 피해 불법침입자가 접속하기 용이
    - 기존의 AP를 제거하고 불법으로 AP를 교체하거나, 임의의 장소에 불법으로 AP를 설치하는 방법으로 내부 네트워크를 해킹
    - 사용자 인증이 없는 경우 장비를 도난하여 네트워크에 손쉽게 접속-무선은 유선에 비해 장비 이동이 용이해 장비 도난 가능성 높음
  - 인증 및 암호화 매커니즘의 취약점
    - 단말기 인증과 무선 구간의 암호화를 위해 AP와 단말기에 설정하는 WEP 프로토콜이 있으나 보안기능이 미약(WEP 인증방법은 상호인증 기능을 제공하지 않기 때문에 AP는 단말기를 인증할 수 있지만 단말기는 AP를 인증할 수 없어 단말기 입장에서 정당한 AP와 통신하는지 확인이 곤란. WEP 키를 주기적으로 변경하지 않고 사용할 경우 도청에 의한 복호화의 위험.

64비트 이하의 WEP키를 사용할 경우 전문가에 의해 30분 이내에 복호화 가능)

o 소규모 무선랜 환경에서의 보안정책 수립 예시

- AP 보호를 위한 조치

- AP의 전파가 건물 내로 한정되도록 전파 출력을 조정하고, 외부에 접한 벽이나 창 쪽에서 먼 건물 안쪽에 설치
- AP 관리용 S/W의 ID, 비밀번호 변경-AP 관리용 S/ W의 ID, 패스워드를 출고상태로 사용하지 말고, 관리자 이외의 사람(불법침입자 등)이 추측하기 어렵게 변경
- AP 설치 장소 관리 유의-외부인이 발견하거나 접근하기 어려운 곳에 설치

- 인증 및 데이터 보호를 위한 조치

- 출고 시 제조회사에서 설정한 SSID는 ANY인 경우가 대부분이므로, AP와 단말기의 SSID를 변경-공중 무선랜 사업자가 사용하는 SSID 사용 지양
- AP에 MAC 주소 필터링 기능을 설정하고 무선랜 카드의 주소를 AP에 등록
- AP가 제공하는 WEP키 중 제일 긴 키를 사용하고 WEP키를 주기적으로 변경

- 기 타

- 유선구간에서 적용되는 보안수칙 실천을 강화(네트워크 공유시 비밀번호 설정 등 유선구간의 보안수칙을 준수. PC용 침입탐지시스템이나 침입차단시스템을 설치하여 불법접근 탐지 및 차단)

(2) 보안 기능 제공 여부

o 핵심가이드

- 하드웨어의 분실, 부적절한 액세스포인트의 활용 이해
- 해커의 공격에 보안 위협을 최소화할 수 있는 보안기능 방안 이해
- 상호인증을 위한 WEP키 활용 이해
- 중앙집중 제어방식의 보안을 관리하는 방안 이해 등

o 무선랜의 보안기술 이해

- SSID 설정을 통한 접속 제한
  - 기본적인 사항으로 AP와 Client는 SSID 가 일치해야 통신이 가능하게 되는데 SSID는 AP장비에서 브로드캐스팅되는 것이 기본설정이다. 보안을 위해

서는 AP장비에서 SSID를 브로드캐스팅하지 않게 설정하면 SSID를 알고 있는 사람만이 AP를 이용하여 무선랜을 사용할 수 있으므로 기본적인 보안 기능을 수행할 수 있다.

- 폐쇄시스템 운영

- 무선랜 단말기가 SSID 숨김기능으로 SSID값을 브로드캐스팅하지 않는 AP 장비에 접속하기 위해서는 무선랜 단말기가 SSID를 이용하여 AP장비에 인증을 받아야 한다. 이때, SSID 값을 NULL로 하여 인증을 요청하는 사용자를 차단하도록 AP를 설정하여 운영하는 것을 폐쇄시스템 운영이라 한다.

- MAC 주소 인증

- 무선랜카드에 부여된 MAC 주소값을 이용하여 무선랜 단말기와 AP를 인증하는 방식으로 사전에 단말기의 MAC 주소를 이용하여 등록 리스트를 만들어 놓고 접속 요청하는 단말기를 존재여부에 의해서 필터링하는 방식을 MAC 주소 필터링이라 한다. 이런 방식을 AP, 라우터, 인증서버 등에 적용할 수 있다.

- WEP 인증

- WEP은 데이터 암호화와 사용자 인증 기능을 제공하며, 사용자 인증 기능은 서로 같은 공유키를 갖는 사용자들을 정상적인 사용자로 인증하여 통신하는 방법을 제공한다. 그러나, WEP 인증방식은 단방향 인증 방식으로 인한 취약성, 고정된 공유키 사용으로 인한 취약성 등이 있다.

- 동적 WEP 인증

- 동적 WEP 인증은 WEP 인증방식이 고정된 공유키 값을 사용하게 되는 보안상의 문제점을 줄이기 위해서 동적 WEP을 적용하였다. 동적 WEP을 사용하기 위해서는 인증서버가 필요하고 AP에서 동적 WEP를 지원하여야 한다.

- EAP 인증

- WEP 인증은 단방향 인증이고 고정된 공유키값을 사용하는 문제점이 있고, 동적 WEP도 단방향 인증방식이며, 공격자에 의해 패킷을 도청당한 후 크랙되는 문제점이 있다. EAP는 모든 링크에 적용될 수 있으며, 다양한 인증 방법을 사용할 수 있다. EAP 동작은 무선랜 클라이언트가 AP에 네트워크 접속을 요구하고 AP는 인증이 수행되어 연결이 설정될때까지 AP를 차단하고 무선랜 클라이언트는 인증서버와 인증절차를 수행하게 되며, 이때 패스워드 방식의 인증을 사용할 수도 있으며, 데이터 암호화 기능도 수행할 수 있다.

- 공격자의 패킷 도청 방지 대책

- WEP나 EAP 기능을 이용한 데이터 암호화 수행
- AP장비 물리적 접근 차단
  - AP 장비가 공격자에게 접근이 가능하면 물리적인 공격 및 파손 등이 가능하므로 AP장비의 접근을 차단하여야 한다.
- 무선랜 단말기의 관리 강화
  - 무선랜 단말기를 분실하였을 경우에는 무선랜 단말기를 이용하여 비 인가자의 네트워크 접속 등의 공격이 가능하므로 무선랜 단말기 관리를 강화하여야 한다.
- AP 장비의 전파 출력 조정
  - AP 장비의 전파 출력 조정을 하지 않아서 전파가 불필요한 지역까지 나간다면 그에 따른 공격이 증가될 수 있으므로 적절한 전파 출력의 조정이 필요하다.
- 암호화키 길이 증가
  - 암호화키 길이가 작으면 공격자에 의해서 패킷 도청을 통하여 크랙될 수 있으므로 키 길이를 길게 사용한다.

## 2.4 네트워크 기반 프로그램 이해 및 활용

### 2.4.1 Ping, Traceroute 등 네트워크 기반 프로그램의 활용

- o 핵심가이드
  - Ping의 기능 및 동작원리
  - Traceroute의 기능 및 동작원리

#### (1) Ping

- o Ping의 동작 원리 이해
  - Ping은 상대방 컴퓨터, 네트워크 장비, 서버 장비까지 통신이 잘 되는지를 확인하는 명령이다. 대상컴퓨터에 ICMP 에코 패킷을 보낸 후 에코 응답 패킷을 수신하여 대상 컴퓨터와의 연결의 확인이 가능하며 송신한 패킷의 수를 되돌려준다.
  - ping 명령의 TTL(Time To Live)값은 어떤 OS를 사용하는지도 유추가 가능한



데 유닉스 계열은 255, 윈도우 계열은 128부터 TTL 값이 라우터를 지날 때마다 1씩 감소하므로 TTL이 대략 200번 정도이면 유닉스이고, 100번 정도이면 윈도우 계열이라고 확인할 수 있다.

o Ping의 옵션 활용(Windows NT 계열)

- -n, -t, -l 등

## (2) Traceroute

o Traceroute의 동작원리 이해

- Traceroute는 목적지까지의 데이터 도달여부를 확인하는 도구이다. 네트워크와 라우팅의 문제점을 찾아내는 목적으로 많이 사용된다. Traceroute는 UDP 패킷을 이용해 진행경로를 추적한다. 그리고 그 패킷이 지나가는 router의 IP 주소나 이름을 출력한다.
- Traceroute는 패킷의TTL( Time to Live)을 하나씩 증가시켜 보낸다. 그러면 1의 ttl을 갖는 패킷은 도착한 라우터에서 ttl 이 감소하고 ICMP 메시지가 출발지로 보내진다. 다음 2의 ttl을 갖는 UDP 패킷이 두 번째 라우터에 도달하여 소멸된다. 목적지에 도달할 때까지 계속 패킷을 보내는데 이 패킷은 사용 불가능한 포트번호(33434)를 붙여서 간다. Unreachable Port 라는 ICMP 메시지를 받으면 trace 는 목적지에 도달했음을 알 수 있게 된다. traceroute 는 유연히 도달하는 것을 방지하기 위해 정확히 3개의 UDP 패킷을 보낸다.

o Traceroute의 활용

- Traceroute 결과에서 응답시간이 \* 로 표시되는 경우 침입차단시스템 등의 접근통제리스트에 의해 Traceroute의 UDP 패킷이 차단되었음을 확인할 수 있다.
- Traceroute를 통한 네트워크 Troubleshooting 방법은 다음과 같다.
  - 지정한 주소가 실제로 존재하는 지 체크하고, 없다면 패킷이 멈춘 곳을 알려준다.
  - 수행속도가 느리면 어느 지점에서 시간을 많이 잡아먹는지 확인한다.
  - 패킷이 적당한 곳을 통해서 라우트되고 있는지 확인한다.
  - \* 모양이 생기는 곳이 있는지 확인한다.

## 2.4.2 Netstat, Tcpdump 등 활용

o 핵심가이드

- Netstat의 기능 이해
- Netstat의 동작 원리와 옵션 활용 이해

(1) Netstat

o Netstat는 자신의 컴퓨터의 네트워크 상태를 다양하게 보여주는 명령어로서 연결 상태, 라우팅테이블, 패킷 통계, 프로토콜별 통계 등의 정보를 활용할 수 있는 명령어이다.

o Netstat의 주요 보안 기능

- 네트워크 연결 상태 확인
- 컴퓨터의 열린 포트 상태 확인
- 네트워크 연결 상태에서 외부에서 접속해온 호스트 유추 가능

o Netstat의 결과 분석

- Proto : 현재 사용한 프로토콜
- Local Address : 현재 열려 있는 사용자 컴퓨터의 IP/호스트 네임과 사용 중인 포트
- Foreign Address : 현재 사용자의 컴퓨터에 접속되어 있는 IP/호스트 네임과 사용 중인 포트
- State : 연결 상태
  - ESTABLISHED : 현재 연결
  - LISTENING : 연결을 위하여 접속을 기다리는 상태
  - TIME\_WAIT : 이미 해당 사이트와 연결이 종료되었거나 다음 연결을 위해 기다리는 상태
  - SYN\_SENT : 접속하기 위해 패킷을 송신 상태

o Netstat의 옵션 활용 이해

- -a : 현재의 모든 네트워크 연결 정보와 Listening Port 정보를 보여준다.
- -e : Ethernet 패킷의 통계를 보여준다.
- -n : IP 주소와 포트 정보를 10진 표기한다.
- -p proto : 지정된 포트와 관련된 네트워크 연결 정보를 보여준다.
- -r : 라우팅 테이블을 보여준다.
- -s : 프로토콜 별 통계정보를 보여준다.

o Netstat -an 결과 이해

- 자신의 컴퓨터에서 서비스하고 있는 포트 정보와 TCP와 UDP를 이용하여 현재 접속하고 있는 원격 호스트를 확인할 수 있다.
- 현재 연결된 상태의 세션에서 일반적으로 접속 방향을 유추할 수 있는 데 포트 1024번 이상의 포트에서 1024번 이하의 서비스 포트에 접속하게 되는 원리를 이용

### 2.4.3 네트워크 패킷/로그분석 및 이해 [1급]

#### o 핵심가이드

- Tcpdump의 기능
- Tcpdump의 동작 원리 및 패킷분석

#### (1) Tcpdump

o Tcpdump는 네트워크 인터페이스를 거치는 패킷의 내용을 출력해 주는 프로그램이다. 즉, 스니핑 도구의 일종으로 자신의 컴퓨터로 들어오는 모든 패킷의 내용을 도청할 수 있으며, 공격자를 추적 및 공격 유형 분석을 위한 패킷 분석 시에 활용할 수 있는 도구이다. tcpdump는 유닉스 계열에서 설치, 활용이 가능하며 윈도우용으로는 windump가 있으며 활용 방법은 유사하다.

#### o 사용 예제

- tcpdump dst host 000.000.000.000 : 패킷의 IP 목적지가 특정 IP인 패킷 보기
- tcpdump -vv -X host 000.000.000.000 : 특정 IP와 통신하는 패킷들을 자세한 내용의 hex값으로 보기

#### o IP Fragmentation의 패킷 분석

- ping을 이용하여 4000 바이트를 보낸 경우에 Ethernet 네트워크를 통하여 전송되기 전의 데이터그램은 20바이트의 IP헤더와 8바이트의 ICMP 헤더, 그리고 4000바이트의 ICMP 데이터를 가진 총 4028바이트의 데이터그램을 송신하여야 하는데 Ethernet을 통하여 전송되기 위해서는 Ethernet의 MTU, 즉 1500 바이트를 넘을 수 없으므로 1500바이트 또는 그보다 작은 fragment로 쪼개어져서 전송되게 된다.

- 첫번째 패킷 : IP헤더(20바이트)+ICMP헤더(8바이트)+데이터(1472바이트)
- 두번째 패킷 : IP헤더(20바이트)+데이터(1480바이트)

- 세번째 패킷 : IP헤더(20바이트)+데이터(나머지 데이터인 1048바이트)

```
11:55:56.548630 xshield.com > test.korean.com: (frag 30338:1048@2960)
11:55:56.558095 xshield.com > test.korean.com: (frag 30338:1480@1480+)
11:55:56.565466 xshield.com > test.korean.com: icmp: echo request (frag 30338:1480@0+)
```

- o 보안 기능 활용

- IP Fragmentation 이해 및 데이터크기 계산 방법
- ICMP 및 ack backdoor 탐지 이해

#### 2.4.4. 네트워크 문제의 원인분석과 장애처리 방안 [1급]

- o 핵심가이드

- 다양한 네트워크 구조에서의 문제발생시 문제 발생 원인 분석
- 어떻게 장애처리를 하여야 하는지 다양한 해결 방안 이해

##### (1) 다양한 네트워크 구조에서의 문제발생시 문제 발생 원인 분석

- o 네트워크 문제 발생시 장애가 발생했을 때부터 그 원인을 규명하고 장애를 복구하기 위해서는 많은 장애 요인을 고려하고 넓은 각도에서 접근해야 한다.
- 장애를 처리하기 위해서는 문제 정의, 사실 수집, 원인 추론, 조치 방안 작성, 구현 단계로 나눌수 있다.

##### (2) 어떻게 장애처리를 하여야 하는지 다양한 해결 방안 이해

- o 네트워크 문제에 대한 문제인식 및 사실수집을 통하여 얻은 정보를 이용하여 원인을 판단하고 이에 대한 조치를 취하여야 한다.

### 3. 네트워크 기반 공격의 이해

#### 3.1 서비스 거부(DoS)공격

##### 3.1.1 Land Attack 등 각종 DoS의 원리와 대처요령

- o 핵심가이드

- Land Attack의 원리 및 대응 방안
- Targa/NewTear/Nestea 공격의 원리 및 대응 방안
- Ping of Death 공격의 원리 및 대응 방안
- Inconsistent Fragmentation 공격의 원리 및 대응 방안

##### (1) Land Attack

- o Land Attack의 원리 이해

- 출발지와 목적지의 IP 주소를 공격자의 IP로 동일하게 만들어서 공격대상에게 보내는 공격으로 패킷을 받은 호스트는 응답을 위해서 수신한 패킷에서 출발지 IP를 이용하여 패킷을 만들어 전송하더라도 자신의 IP이므로 외부로 전송하지 못하고 자신의 컴퓨터에서 부하를 발생하게 된다. 즉, 루프 상태에 빠지게 되어 IP 프로토콜 스택에 심각한 장애를 유발시킨다.

- o Land Attack의 대응 방안

- 라우터나 패킷필터링 도구를 이용하여 네트워크로 유입되는 패킷 중에서 source 주소가 내부 IP인 패킷 차단

##### (2) Targa/NewTear/Nestea 공격

- o Teardrop 공격

- 헤더가 조작된 일련의 IP 패킷조각(IP fragments)들을 전송함으로써 공격이 이루어진다. 공격자가 패킷을 프래그먼트할 때 정상적으로 하지 않고 데이터 일부가 겹치거나 일부 데이터를 포함하지 않고 다음 패킷으로 프래그먼트하여 전송하면 수신자는 패킷 재조합을 수행할 때 부하를 발생하게 된다. 공격당한 시스템은 네트워크 연결이 끊어지거나 일명 “죽음의 푸른 화면(Blue Screen of Death)”이라 불리는 오류 화면을 표시하면서 중단된다. 시스템이 정지될

경우, 사용자는 시스템을 재부팅하여야 하며, 이 경우, 시스템에 직접적인 피해는 없으나 시스템이 정지될 때 저장하지 못한 데이터 등을 잃게 된다. 이 공격이 성공할 수 있는 원인은 윈도우 및 Linux 시스템의 IP 패킷 재조합 코드의 버그에 있었으나 현재 대부분의 시스템에서는 IP 패킷의 재조합 시 0보다 작은 패킷에 대한 처리 루틴이 포함되어 있어 이러한 teardrop 공격에 대해서 방어하고 있다.

#### o Targa 공격

- Targa는 여러 종류의 서비스 거부 공격을 실행할 수 있도록 만든 공격 도구로서 Mixer에 의해 만들어졌다. 즉, 이미 나와 있는 여러 DoS 공격 소스들을 사용하여 통합된 공격도구를 만든 것이다. targa에서 지원하는 공격 기법은 bonk, jolt, land, nestea, newtear, syndrop, teardrop, winnuke 등이 있다.

### (3) Ping of Death 공격

#### o Ping of Death 공격의 원리 이해

- Ping을 이용하여 ICMP 패킷을 정상적인 크기보다 아주 크게 만들어 진 패킷을 전송하면 네트워크를 통해 라우팅(Routing)되어 공격 네트워크에 도달하는 동안 아주 작은 조각(Fragment)이 되어 공격대상 시스템은 이렇게 작게 조각화된 패킷을 모두 처리해야 하므로 정상적인 Ping의 경우보다 훨씬 많은 부하가 걸리게 되므로 시스템의 성능을 떨어뜨리는 공격이다.

### (4) Inconsistent Fragmentation 공격

#### o Bonk

- 패킷을 프래그먼트하여 전송할 때 패킷 조작을 하여 결과적으로 공격대상자에게 시스템 부하를 증가시키는 공격이다.
- 처음 패킷을 1번으로 보낸후 다음 패킷의 보낼때 순서번호를 모두 1번으로 조작하여 전송하는 DoS 공격

#### o Boink

- Bonk를 수정한 DoS 공격도구로써 처음 패킷을 1번으로 보낸 후 다음 패킷을 100번, 다음 패킷을 200번 등 정상적으로 보내다가 20번째 패킷을 2002, 21번째 패킷을 100, 22번째 패킷을 다시 2002 등으로 중간에 패킷 시퀀스 번호를 비정상적인 상태로 보내는 공격기술이다.

### 3.1.2 Syn Flooding, Smurf 등 각종 Flooding 공격의 원리와 대응 방안

#### o 핵심가이드

- Syn Flooding 공격의 원리 및 대응 방안
- 스머프 공격의 원리 및 대응 방안
- UDP Flood 공격의 원리 및 대응 방안

#### (1) Syn Flooding 공격

##### o Syn Flooding 공격의 원리 이해

- Syn flooding 공격은 TCP 연결 설정 과정 중에 3-Way Handshaking 과정에서 Half-Open 연결 시도가 가능하다는 취약성을 이용한 공격으로 공격대상 시스템은 외부로부터 접속 요청을 더 이상 받아들일 수가 없게 되어 정상적인 서비스를 제공할 수 없게 된다. 즉, 공격자가 다수의 syn 신호를 공격대상자에게 전송하면 공격대상자는 ack/syn 신호를 공격자에게 전달하게 되는데 이때 공격자가 ack 신호를 반송하지 않으면 공격대상자의 시스템은 일정 시간동안 신호를 기다리게 된다. 이 공격은 윈도우시스템 뿐만 아니라 인터넷에 연결되어 TCP 기반의 서비스(예를 들면, 웹서버, FTP서버, 또는 메일서버 등)를 제공하는 모든 시스템들에 대해 피해를 줄 수 있다. 그러나 이 문제에 대한 완벽한 해결책은 없으며 단지 영향을 감소시키는 방법들만이 알려져 있다.

##### o Syn Flooding 공격 대응 방안

- SYN Flooding 공격은 TCP 프로토콜의 연결설정 절차의 설계상의 취약성으로 인해 발생하는 것으로서 이에 대한 완전한 해결책은 마련되지 않았으며, 공격의 가능성을 줄이거나 피해를 최소화하기 위한 방법 또는 패치들만 제공되고 있을 뿐이다.

#### (2) 스머프 공격

##### o 스머프 공격의 원리 이해

- 스머프(smurf)공격은 네트워크 수준에서 어떤 호스트의 서비스를 방해하는 서비스거부 공격방법으로 공격자는 공격대상 호스트의 IP주소로 위장하여 ICMP 에코 요청을 특정 IP 브로드캐스트 주소로 보내게 된다. 공격대상 주소로 소스 IP주소를 만들고 임의의 브로드캐스트 주소로 ICMP echo packet을

보내면 스푸핑된 IP를 가진 호스트는 ICMP reply 패킷들을 동시 다발적으로 수신하여 시스템 부하가 증가하게 된다.

o 스머프 공격 대응 방안

- 중간매개지로 쓰이는 것을 막기 위해서 라우터에서 다른 네트워크로부터 자신의 네트워크로 들어오는 IP broadcast 패킷을 막도록 설정한다.
- 호스트는 IP broadcast address로 전송된 ICMP 패킷에 대해 응답하지 않도록 시스템을 설정할 수 있다.

(3) UDP Flood 공격

o UDP Flood 공격

- UDP는 비연결성 프로토콜로써 데이터를 전달하기 위한 연결 셋팅 절차가 필요없는 프로토콜이다. UDP Flood 공격은 공격대상자 시스템에 UDP 패킷을 전송하면 목적지 포트가 어떤 애플리케이션이 서비스하고 있는지 조사하고 그 포트를 이용하여 서비스하고 있는 애플리케이션이 없다고 파악되면 소스 어드레스에 ICMP Unreachable 패킷을 전송하는데, 이때 너무 많은 UDP 패킷이 공격대상자에게 전송되면 시스템에 부하가 걸리게 된다.

o 공격 대응 방안

- 사용하지 않는 UDP 서비스를 중지
- 방화벽 등을 이용하여 패킷 필터링
- 리눅스 시스템의 경우 chargen 또는 echo 서비스를 중지

3.2 분산 서비스 거부 공격

3.2.1 Trinoo, TFN, Stacheldraht 등

o 핵심가이드

- 트리누 공격의 원리 및 대응 방안
- TFN 공격의 원리 및 대응 방안
- Stacheldraht 공격의 원리 및 대응 방안
- TFN2K 공격의 원리 및 대응 방안



## (1) 트리누 공격

### o 트리누 공격의 원리 이해

- 트리누(Trinoo)는 많은 호스트로부터 통합된 UDP flood 서비스거부 공격을 유발하는데 사용되는 도구로 몇 개의 서버들(혹은 마스터들)과 많은 수의 클라이언트들(데몬)로 이루어진다. 공격자는 트리누 마스터에 접속하여 마스터에게 하나 혹은 여러개의 IP 주소를 대상으로 서비스 거부공격을 수행하라고 명령을 내린다. 그러면 트리누 마스터는 특정한 시간에 하나 혹은 여러 개의 IP 주소를 대상으로 공격하도록 데몬들에게 명령을 내리게 되어 공격대상자에게 DoS 공격을 수행한다.

- 공격자 -----> 마스터 : 27665/tcp 포트
- 마스터 -----> 데몬들 : 27444/udp 포트
- 데몬들 -----> 희생 시스템 : 임의의 포트를 통한 UDP flood

- 트리누에 의해 생성된 UDP flood 공격의 소스 IP 주소는 위장되지 않았지만 앞으로 위장된 IP 주소를 사용하는 도구가 나올 수도 있다.

### o 트리누 공격 대응 방안

- 라우터에서의 access-list 설정
  - access-list 171 deny tcp any any eq 27665
  - access-list 171 deny udp any any eq 27444

## (2) TFN 공격

### o TNF 공격의 원리 이해

- TFN은 트리누와 거의 유사한 분산 서비스 거부 도구로 많은 소스에서 하나 혹은 여러 개의 목표 시스템에 대해 서비스거부 공격을 수행한다. TFN은 UDP flood 공격을 할 수 있을 뿐만 아니라 TCP SYN flood 공격, ICMP echo 요청 공격, ICMP 브로드캐스트 공격(smurf 공격)을 할 수도 있다. TFN 서비스 거부 공격은 공격자가 클라이언트(혹은 마스터) 프로그램이 공격명령을 일련의 TFN 서버들(혹은 데몬들)에게 보냄으로써 이루어진다. 그러면 데몬은 특정 형태의 서비스거부 공격을 하나 혹은 여러 개의 목표 IP 주소를 대상으로 수행한다. 소스 IP 주소와 소스 포트는 임의로 주어지고, 패킷의 사이즈도 바꿀 수 있다.
- TFN 마스터는 명령어라인에서 TFN 데몬에 명령을 보낸다. TFN 마스터는 ID

필드와 패킷의 위치 인수를 가진 16비트 바이너리 값의 ICMP echo reply 패킷을 사용하여 데몬과 통신을 한다. TFN 마스터는 공격자가 제공한 데몬들의 IP 주소목록이 필요하다. 또한 어떤 TFN은 rcp와 같은 원격파일복사 기능을 가지고 있어 자동으로 새로운 TFN 데몬을 생성하거나 기존의 TFN을 업데이트하는데 사용하고 있다.

### (3) Stacheldraht 공격

#### o Stacheldraht 공격의 원리 이해

- stacheldraht는 트리누와 TFN을 참고하여 제작된 도구로써 이들이 갖고 있는 특성을 대부분 가지고 있는 공격도구로 stacheldraht의 마스터시스템 및 자동적으로 업데이트되는 에이전트 데몬과의 사이에 통신을 할 때 암호화하는 기능이 추가되었다.
- stacheldraht는 TFN이나 TFN2K처럼 ICMP flood, SYN flood, UDP flood와 Smurf 등의 공격에 의해서 DDoS 공격을 할 수 있는 기능을 가지고 있다.
  - 침입하여 클라이언트(handler)와 데몬 프로그램 설치 단계 : 해킹으로 마스터와 에이전트로 이용할 수천 개의 시스템에 침입하여 root권한을 획득한 후 그곳에 클라이언트와 데몬 프로그램을 설치한다. 이 작업을 위해서는 단 시간 내 많은 시스템을 연달아 원격 해킹할 수 있는 자동화된 최신 해킹툴이 이용된다.
  - DDoS공격 단계 : 공격자 시스템에서 마스터 시스템과의 암호통신용 프로그램을 실행시켜서 마스터를 통해 에이전트 시스템의 데몬으로 공격대상 시스템/네트워크에 DDoS공격을 하도록 한다.

#### o Stacheldraht 공격 대응 방안

- 라우터에서의 공격주소에 의한 차단 : 대규모 데이터를 보내는 DDoS 공격을 막기 위해서는 네트워크 차원에서의 접근통제가 필요하다. DDOS 공격의 특성상 공격자 주소는 하나가 아닌 수십 수백개가 될 수도 있으며 위장된 주소일 가능성도 있고, 공격이 시작된 후에 네트워크 이상을 사람이 인지하는데는 얼마 시간이 걸리지 않기 때문에 주소단위로 차단하는 것은 쉽지 않다.
  - 라우터의 egress 필터링 기능 : egress는 외부 인터넷으로부터 들어오는 packet을 의미하며, ingress는 내부 네트워크에서 외부로 나가는 패킷을 말한다. egress 필터링이란 지정한 IP(도메인)로부터의 패킷만이 라우터를 통과하게 만들어 패킷 필터링을 하는 것이며, 지정되지 않은 IP로부터의 패킷

은 모두 drop된다.

- Unicast RPF를 이용한 차단 : 시스코 라우터에서 제공하는 Unicast Reverse Path Forwarding기능은 Source IP주소가 spoofing된 DoS공격을 하는 것을 막아주는데 사용될 수 있다. Unicast RPF는 라우터로 패킷이 들어올 때 패킷의 input interface로의 reverse path route가 존재하는지를 확인한다. 이는 packet이 source IP주소로부터 input interface로의 route path를 가지고 있는지를 CEF에서 주는 라우팅 정보(FIB)를 이용하여 확인하는 것이다.
- 라우터의 Committed Access Rate(CAR) 기능 : 단위시간 동안 일정량 이상의 패킷이 라우터로 들어올 경우, 일정량 이상의 패킷은 통과시키지 않도록 하는 기능을 CAR 기능이라 한다.

#### (4) TFN2K 공격

##### o TFN2K 공격의 원리 이해

- TFN2K는 TFN의 발전된 형태로써 다음과 같은 특징이 있다.
  - 통신에 특정 포트가 사용되지 않고 암호화되어 있으며, 프로그램에 의해 UDP, TCP, ICMP가 복합적으로 사용되며 포트도 임의로 결정된다.
  - TCP Syn Flooding, UDP Flooding, ICMP Flooding, Smurf 공격이 가능하다.
  - 모든 명령은 CAST-256 알고리즘으로 암호화된다.
  - 지정된 TCP 포트에 백도어를 실행시킬 수 있다.
  - 데몬은 인스톨 시 자신의 프로세스 이름을 변경함으로써 프로세스 모니터링을 회피한다.
  - UDP 패킷의 헤더가 실제 UDP 패킷보다 3바이트만큼 더 크다.
  - TCP 패킷의 헤더의 길이는 항상 0이다. 정상적인 패킷이라면 절대로 0일 수 없다.

### 3.3 네트워크 스캐닝

#### 3.3.1 Remote Finger Printing

##### o 핵심가이드

- TCP/IP Fingerprinting의 특성을 이용한 원리 이해

### (1) 원격지의 OS 등을 판별 방법 이해

- o 고전적인 방법으로 배너그래빙을 이용할 수 있다.
  - telnet ip port의 형태로 하여 port를 서버스 포트로 지정하여 명령어를 실행하면 OS 또는 서비스 프로그램의 정보를 얻을 수 있다.
- o TCP/IP Fingerprinting의 특성을 이용 원리 이해
  - TCP/IP 프로토콜의 특성을 이용한 Fingerprinting 방법은 RFC 문서를 이용하여 전송에 대한 응답 형태를 이용하는 방법이다.

### 3.3.2 IP 스캔, 포트스캔

- o 핵심가이드
  - PORT Scan Attack의 원리 이해
  - PORT Scan Attack 대응 방안

#### (1) PORT Scan Attack

- o PORT Scan은 공격대상 시스템의 포트가 열려있는지 확인하는 공격
  - TCP Open 스캔 : 포트가 열려있을 경우, 세션이 성립되며, 포트가 닫혀 있을 경우에는 RST/ACK 패킷을 받게 된다.
  - Stealth 스캔(TCP Half-Open 스캔) : 포트가 열려있을 경우, 서버로부터 SYN/ACK 패킷을 받은 후, RST 패킷을 보내어 연결을 끊는다. 포트가 닫혀 있을 경우에는 Open 스캔의 경우와 같다.
  - FIN, Xmas, Null 스캔 : 포트가 열려 있을 경우에는 응답이 없고, 포트가 닫혀 있는 경우에만 RST/ACK 패킷이 되 돌아온다.
  - UDP Open 스캔 : 포트가 열려있을 경우, 아무런 응답이 없으며, 포트가 닫혀 있을 경우에는 ICMP Unreachable 패킷을 받게 된다.

### 3.3.3 Third Party Effect 등 [1급]

- o 핵심가이드
  - Third Party Effect(제3자 현상)의 이해
  - Third Party Effect와 각종 DoS 공격과의 관계 이해

### (1) Third Party Effect(제3자 현상)의 이해

- 제3자 현상은 행위자가 대상자에게 어떤 행위를 했는데 그에 대한 반응이 행위자가 아닌 다른 사람에게 나타나므로 행위자는 제 3자가 되는 현상이다. 즉, DoS 공격에서 공격자가 공격대상자를 공격하기 위해서 제 2자(second party)에게 소스 IP를 공격대상자 IP로 속여서 보내면 제 2자는 공격대상자인 제 1자(first party)에게 응답을 보내는 형태로 공격대상자에게 부하를 발생시킬 수 있다.

### (2) Third Party Effect와 각종 DoS 공격과의 관계 이해

- 제3자 현상을 예를 보면 공격자(third party)가 희생자(second party)에게 소스 IP를 공격대상자(first party) IP로 변조하여 TCP syn 신호를 보내면 희생자는 공격대상자에게 ack/syn 신호를 응답할 것이며, 다수의 희생자를 이용한다면 공격대상자는 DoS 공격을 당하게 된다. 또한, 공격대상자는 공격자의 IP를 추적하기 어려울 것이다.

## 3.4 IP Spoofing, Session Hijacking

### 3.4.1 IP Spoofing과 Session Hijacking의 원리 및 실제

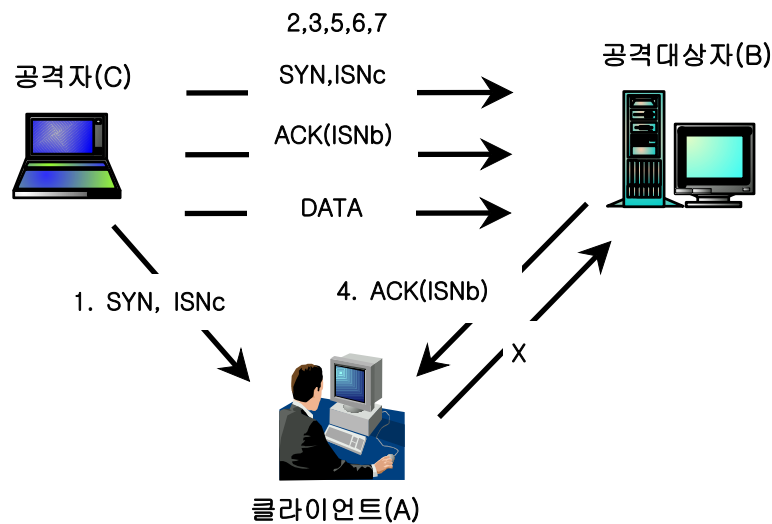
- 핵심가이드
  - IP Spoofing의 공격원리 이해
  - 공격종류와 특징 이해
  - 대응방안 이해
  - Session Hijacking의 공격 원리 및 대응 방안

#### (1) IP Spoofing의 공격원리 이해

- IP Spoofing은 그대로 자신의 ip를 속이는 행위를 말한다. IP스푸핑은 TCP/IP의 구조적인 결함에서 출발한 방법으로 TCP sequence number, source routing, 소스 ip 주소를 이용해서 상대방 호스트가 자신의 호스트를 트러스트 하게 만드는 방법이다.

## (2) 공격 종류와 특징 이해

- o IP spoofing은 IP를 속여서 공격하는 기법으로 TCP/IP 프로토콜의 약점을 이용한 IP spoofing은 순서제어번호 추측, 반(Half)접속시도 공격, 접속가로채기, RST를 이용한 접속끊기, FIN을 이용한 접속끊기, SYN/RST패킷 생성공격, 네트워크 데몬 정지, TCP 윈도우 위장 등이 있다. 그러나 일반적으로 IP spoofing은 케빈미트닉이 사용한 방법을 의미하며 순서제어번호추측 공격, 반(Half)접속시도 공격 등이 함께 사용되는 수법이다.
- o 공격원리



(그림 2-12) IP Spoofing 흐름도

- C는 A로 자신의 IP주소를 위장하여 SYN를 보내 접속요청을 한다.(1번 흐름도) 요청에 대한 응답으로 A가 C에 대해 ACK와 함께 자신의 SYN을 전송하지만 C가 이에 대해 ACK를 보내지 않으면 A는 자신이 보낸 ACK에 대한 C의 응답을 기다리게 된다. 이 과정을 연속적으로 반복하면 A는 외부의 접속요청에 응답할 수 없는 오버플로우 상태가 된다.
- C는 B로 정상적인 접속을 시도하여 순서제어번호의 변화를 패킷 모니터링을 이용하여 관측한다.(2번 흐름도)
- 순서제어번호의 변화를 관찰하여 추측한 순서제어번호를 이용하여 C는 자신의 IP주소를 A로 가장한 후 B에 접속요청(SYN)을 보낸다.(3번 흐름도)
- B는 수신된 SYN 패킷이 A에서 온 것으로 인식, A에게 ACK와 새로운 SYN

를 보내지만 이미 A는 외부와 통신 불능상태이므로 응답을 할 수 없게 된다.(4번 흐름도)

- C는 자신의 IP 주소를 A주소로 위장하여 추측된 순서제어번호를 이용하여 A로 보낸 SYN/ ACK에 대한 ACK를 B에 보낸다.(5번 흐름도)
- 결국 C와 B는 불법적 접속이 이루어지고, B는 A와 연결되어 있는 것으로 착각한다.(6번 흐름도)
- 이후 rsh를 이용하여 echo '+ +' >/.rhosts과 같은 데이터를 보내면 된다.(7번 흐름도)

### (3) 대응방안 이해

- o 외부에서 들어오는 패킷 중에서 출발지 IP주소(Source IP Address)에 내부망 IP 주소를 가지고 있는 패킷을 라우터 등에서 패킷 필터링을 사용하여 막아낼 수 있다. 그러나 내부 사용자에게 의한 공격은 막을 수 없으므로 각 시스템에서 TCP wrapper, ssh 등을 설치해서 운영하고, rlogin 등과 같이 패스워드의 인증 과정이 없는 서비스를 사용하지 않는 것이 바람직하다.

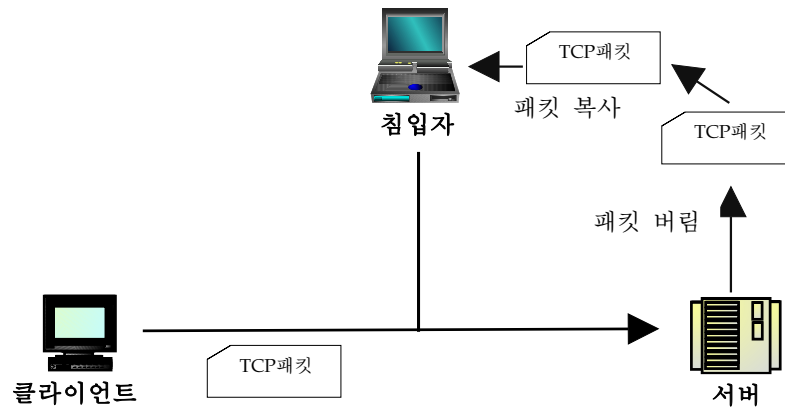
### (4) Session Hijacking

- o Session Hijacking의 공격 원리
  - TCP 세션 하이재킹은 연결의 신뢰성을 확보하기 위한 시퀀스 넘버를 이용한 공격으로 클라이언트와 서버간의 통신을 관찰할 수 있을 뿐만 아니라. 트러스트를 이용한 거의 모든 세션의 갈취가 가능하다.
  - TCP는 두 지점간의 신뢰성 있는 전이중 접속을 제공한다. 그리고 호스트에 의해서 송신되어지는 모든 바이트는 32비트 정수 값인 순차번호가 매겨지고 수신자도 이 순차 번호로 승인한다. 첫 번째 송신 바이트를 위한 순차 번호는 연결 설정시 계산되어지고 매번 TCP 연결이 될 때마다 다른 순차 번호를 사용하기 위하여 설계된 규칙에 근거하여 연결될 때마다 변화한다.
  - 기호정의
    - SVR\_SEQ : 서버에 의해서 송신되어질 다음 바이트의 순차 번호
    - SVR\_ACK : 서버에 의해 수신될 다음 바이트(수신된 바이트의 순차 번호+ 1)
    - SVR\_WIND : 서버의 수신 윈도우 크기

- CLT\_SEQ : 클라이언트에 의해서 송신되어질 다음 바이트의 순차 번호
  - CLT\_ACK : 클라이언트에 의해 수신될 다음 바이트 (마지막 수신된 바이트의 순차 번호 + 1)
  - SVR\_WIND : 클라이언트의 수신 윈도우 크기
  - SEG\_SEQ : 패킷의 순차 번호
  - SEG\_ACK : 패킷의 확인 번호
  - SEG\_FLAG : 제어 비트
- 데이터 교환이 이루어지지 않은 초기에는  $SVR\_SEQ = CLT\_ACK$ ,  $CLT\_SEQ = SVR\_ACK$  상태이다. 이런 상태는 접속 후 데이터의 전송이 이루어지지 않은 "quiet" 상태에서도 마찬가지이다. 이러한 상태는 데이터가 전송되어지는 상태에서는 성립하지 않는다.
  - 비동기 상태는 양쪽이 확립된(established) 상태일 경우의 아무런 데이터 전송이 없으면서 다음과 같이 서로의 순차 번호와 확인 번호가 일치하지 않는 접속 상태를 말한다.
    - $SVR\_SEQ \neq CLT\_ACK$
    - $CLT\_SEQ \neq SVR\_ACK$
  - 이 상태는 데이터가 전송되기 전까지는 안정적이다. 하지만 데이터가 전송된다면 다음 두 경우가 발생하게 된다.
    - $CLT\_SEQ < SVR\_ACK + SVR\_WIND$
    - $CLT\_SEQ > SVR\_ACK$
  - 이 상태에서 패킷 수신이 가능하며 데이터는 차후의 사용을 위해서 저장되지만 사용자에게 SVR\_ACK의 순차 번호는 전송하지는 않는다.
    - $CLT\_SEQ > SVR\_ACK + SVR\_WIND$
    - $CLT\_SEQ < SVR\_ACK$
  - 패킷 수신이 불가능한 상태이며 데이터도 버려진다. 두 가지 경우의 이러한 상태는 존재할 수 있지만 상호간의 데이터 교환은 불가능한 상태이다.
  - 후기(post) 비동기 하이재킹 공격
    - 하이재킹 공격은 TCP 접속 양단을 비동기 상태로 만들어 접속 쌍방이 더 이상 데이터 전송이 불가능하도록 하는데 있다. 그런 후 침입자는 실제 패킷을 흉내내어 양쪽에서 수신될 수 있는 패킷을 생성한다. 침입자가 TCP 세션을 비동기화 시키는 데 성공하고, 클라이언트가 패킷의 헤더에 다음의 코드가 포함된 패킷을 보냈다고 가정하자.
 
$$SEG\_SEQ = CLT\_SEQ$$



SEG\_ACK = CLT\_ACK



(그림 2-13) 침입자는 서버가 버린 패킷을 복사

- 패킷 헤더의 첫 번째 행, SEG\_SEQ = CLT\_SEQ는 패킷의 순차 번호가 클라이언트의 다음 순차 번호라는 것을 나타낸다. 두 번째 행, SEG\_ACK = CLT\_ACK은 패킷의 ACK값을 다음 ACK값으로 설정한다. 침입자가 TCP 연결을 비동기화 시켰기 때문에 클라이언트 패킷의 순차 번호(CLT\_SEQ)는 기대했던 순차 번호의 서버 ACK(SVR\_ACK)와 결코 같을 수 없어서 서버는 데이터를 받아들이지 않고 패킷을 버린다. 침입자는 서버가 버린 패킷을 복사한다. 그 후 침입자는 같은 패킷이지만 SEG\_SEQ와 SEG\_ACK(그리고 체크섬)을 바꾼 패킷을 다음과 같이 변경하여 서버에게 보낸다.

SEG\_SEQ = SVR\_ACK

SEG\_ACK = SVR\_SEQ

- 패킷 헤더의 순차 번호는 옳기 때문에 패킷을 받아들이고, 데이터를 처리한다. 그 동안 클라이언트가 보내고, 서버가 받아들이지 않은 패킷을 클라이언트는 계속 전송할 것이다.
- CLT\_TO\_SVR\_OFFSET의 값을 SVR\_ACK에서 CLT\_SEQ의 값을 뺀 값과 같게 설정하고, SVR\_TO\_CLT\_OFFSET의 값을 CLT\_ACK에서 SVR\_SEQ의 값을 뺀 값과 같게 설정하면 해커는 클라이언트가 서버에게 보내는 TCP 패킷의 값을 패킷이 SEG\_SEQ와 SEG\_ACK값을 나타낼 수 있도록 고쳐야만 한다.

CLT\_TO\_SVR\_OFFSET = SVR\_ACK - CLT\_SEQ

SVR\_TO\_CLT\_OFFSET = CLT\_ACK - SVR\_SEQ

- 공격자는 클라이언트에서 서버로 가는 TCP 패킷을 다음과 같이 고치게 된다.

$SEG\_SEQ \leftarrow SEG\_SEQ + CLT\_TO\_SVR\_OFFSET$

$SEG\_ACK \leftarrow SEG\_ACK - SVR\_TO\_CLT\_OFFSE$

- 공격자가 두 지점간에 교환되는 패킷을 감청 할 수 있고 IP 패킷을 가장할 수 있다면 모든 행동이 공격자의 컴퓨터를 통하게 된다. 이로써 데이터 흐름에 데이터를 추가 및 삭제가 가능하다. 예를 들어 접속이 텔넷을 이용한 원격접속이라고 하면 공격자는 사용자를 대신하여 어떠한 명령어(예: "echo merit.edu lpj >& ~/.rhosts"와 같은)를 포함할 수 있고, 이때 생길 수 있는 원치 않는 화면출력을 제거할 수도 있어 사용자는 침입자의 존재를 전혀 눈치채지 못한다.

### 3.5 스니핑 및 암호화 프로토콜

#### 3.5.1 스니핑 공격의 이해

##### o 핵심가이드

- 스니핑 공격의 동작 원리 이해
- 스니핑 공격 대응 방안

##### (1) 스니핑 공격의 동작 원리 이해

- o 스니핑은 네트워크 상에서 자신이 아닌 다른 상대방들의 패킷 교환을 엿듣는 것을 의미한다. 간단히 말하여 네트워크 트래픽을 도청(eavesdropping)하는 과정을 스니핑이라고 할 수 있다. TCP/IP 프로토콜을 이용한 통신에서는 통신매체를 통과하는 패킷들이 암호화가 되지 않은 상태이므로 이 패킷을 도청하여 메시지 내용을 볼 수 있다.

##### o 허브 환경에서의 스니핑

- 허브(Hub)는 기본적으로 들어온 패킷에 대해 패킷이 들어온 포트를 제외한 모든 포트에 대해 패킷을 보내는 장비이다. 따라서, 기업에서 허브를 사용하고 있다면 원하던 원치 않던 간에 계속하여 다른 사람의 패킷들을 받아보고 있었던 것이다. 물론 네트워크 드라이버, OS 커널 등의 수준에서 MAC 주소를 보아 자신이 아닌 다른 이들의 패킷은 버려지기 때문에 그것을 쉽게 느낄

수는 없었을 것이다. 하지만 여러분 시스템의 NIC를 promiscuous 모드로 동작하게 한다면 다른 이들의 패킷 또한 버리지 않고 받아볼 수 있다. 이때 스니핑 도구를 통해 해당 패킷을 저장하고 분석하는 것이 가능하다. 모든 패킷은 실제 수신 대상이 아닌 호스트에게도 전달되며 Promiscuous 모드로 동작하는 호스트는 다른 수신 대상의 패킷도 볼 수 있다

o 스위치 환경에서의 스니핑

- 일반적으로 스니핑을 방지하는 방법으로 스위칭 허브를 사용하는 방법이 있다. 스위칭 허브는 로컬 네트워크를 여러 개의 세그먼트로 나누어 쓸 수 있도록 하는데, 각 세그먼트내의 트래픽은 다른 세그먼트로 전달되지 않는다. 따라서 스위칭 허브를 이용하여 업무별로 또는 사이트별로 네트워크를 나누어 놓으면 원칙적으로는 다른 네트워크 세그먼트내의 네트워크 트래픽을 도청할 수 없게 된다. 하지만 이러한 스위칭 허브를 사용하는 방법으로 스니핑 공격을 완벽하게 막을 수는 없다. 다음과 같은 Switch Jamming, ARP Redirect나 ICMP Redirect 등의 기법을 이용하여 다른 네트워크 세그먼트의 데이터를 스니핑 할 수 있는 방법이 존재한다.

- 스위칭 환경에서의 스니핑 공격 방법

· Switch Jamming : 일반적으로 스위치 장치들은 MAC 주소 테이블이 가득 차게 되면(Full) 모든 네트워크 세그먼트로 트래픽을 브로드캐스팅하는 특성을 가지고 있다. 따라서 공격자는 위조된 MAC 주소를 지속적으로 네트워크에 흘림으로서 스위칭 허브의 주소 테이블을 오버플로우시켜 허브처럼 동작하게 하여 다른 네트워크 세그먼트의 데이터를 스니핑 할 수 있게 된다. 이는 일반적인 스위칭 장비가 보안 원리의 하나인 "Fail close(시스템에 이상이 있을 경우 보안기능이 무력화되는 것을 방지하는 원리)를 따르지 않기 때문에 발생한다. 결국, 공격자가 만들어낸 임의의 arp 패킷의 MAC 주소는 스위치의 주소 테이블을 오버플로우 시키게 되는 것이 공격 성공의 주요 요인이다.

· ARP Redirect 공격 : ARP Redirect 공격은 위조된 arp reply를 보내는 방법을 사용한다. 공격자가 "나의 MAC 주소가 라우터의 MAC 주소이다"라는 위조된 arp reply를 브로드캐스트로 네트워크에 주기적으로 보내어 스위칭 네트워크상의 다른 모든 호스트들이 공격자 호스트를 라우터로 믿게 한다. 결국 외부 네트워크와의 모든 트래픽은 공격자 호스트를 통하여 지나가게 되고 공격자는 스니퍼를 통하여 필요한 정보를 도청할 수 있게 된다. ARP Protocol specification에 의하면 이미 cache에 저장하고 있는 IP에 대한 ARP request를 받게 되면 호스트는 ARP request를 보낸 호스트의 MAC 주소를 cache에 업데이트 하게 된다고 나와 있다. 그리고 이러한 cache의 업데이트 기능은 arp reply에도 적용되는 것으로 보이며, 위의 공격이

성공할 수 있는 요인이 된다.

- ARP Spoofing 공격 : 공격자가 특정 공격대상자를 대상으로 ARP Redirect 공격처럼 arp 테이블을 조작하여 공격대상자의 패킷을 스니핑하는 공격이다.

## (2) 스니핑 공격 대응 방안

- 암호화 기능 및 보안 프로토콜을 사용한다.
  - SSL, IPSEC, PGP 등 여러 암호화 프로토콜 및 응용 프로그램을 통하여 인터넷 통신에 사용되는 모든 데이터를 암호화하여 사용한다.
- 스니핑 탐지 방안
  - 스니핑을 탐지하는 방안은 Ping이나 ARP를 이용하는 방법과 anti-sniff와 같은 전문 탐지 도구를 이용하는 방법이 있다.
  - Ping request를 이용하는 방법 : MAC 주소를 위조(로컬 네트워크에 존재하지 않는 MAC 주소 사용)하여 ping echo request 메시지를 다른 시스템에게 보낸다. 만약 이때 ping echo reply를 받게 되면, 해당 호스트가 스니핑하고 있는 것이다. 왜냐하면 존재하지 않는 MAC 주소를 사용했기 때문에 스니핑하지 않는 호스트는 누구도 ping request를 볼 수 없게 되기 때문에 reply를 보낼수 없다.
  - ARP를 이용한 방법 : ping과 유사한 방법으로 non-broadcast로 위조된 ARP request를 보냈을 때, ARP response가 오면 상대방 호스트가 스니핑하고 있다고 볼 수 있다.
  - Anti-sniffer 도구 : 로컬 네트워크에서 네트워크 카드의 promiscuous 유무를 체크하여 스니퍼가 돌고 있는가를 체크한다. 또한 Anti-Sniffer 프로그램은 DNS test, ICMP time test, Ether ping test, UDP echo test 등 여러 테스트를 지원한다.
  - Sentinel 등 도구 활용

## 3.6 각종 Remote Attack

### 3.6.1 각종 공격의 인지 및 이해

- 핵심가이드
  - Local Attack과 Remote Attack의 비교

- named, imapd, smbd, mountd 등의 버그를 이용한 공격 이해

(1) Local Attack과 Remote Attack의 비교

- o Local Attack는 시스템에 접속한 후에 공격자가 원하는 공격을 수행하는 것이고 Remote Attack는 원격 컴퓨터에서 공격대상으로 공격을 수행할 수 있는 공격이다. 공격자 입장에서는 공격대상에 대해서 실제적으로는 어떠한 접근 권한도 가지고 있지 않으므로 Remote Attack을 수행하여야 하며 이 공격으로 공격대상에 접근권한을 얻은 경우에 Local Attack을 연속하여 수행할 수 있다.

(2) named, imapd, smbd, mountd 등의 버그를 이용한 공격 이해

- o Mountd 버퍼 오버플로우 취약점 및 대책
  - NFS는 네트워크를 통하여 다른 컴퓨터 간에 파일 시스템을 공유하기 위한 클라이언트/서버 프로그램이다. NFS 클라이언트측 컴퓨터가 NFS 서버의 파일에 접근하기 위해서는 클라이언트가 먼저 파일 시스템에 마운트하겠다는 요청을 해야 한다.
  - NFS 마운트 요청을 처리하는 소프트웨어(Mountd 프로그램)에 취약점이 발견되었다. 공격자는 NFS에 대한 접근을 처리하기 위한 코드 영역에 버퍼 오버플로우를 일으킬 수 있는데, 리눅스 시스템에서는 기본적으로 NFS 서버가 Mountd를 구동한다. 이 취약점은 NFS 서버가 파일 시스템을 공유하고 있지 않더라도 공격당할 수 있다.
  - 클라이언트가 파일 시스템을 사용하기 위한 요청을 하게 되면 그 파일 시스템을 마치 지역 파일시스템처럼 사용할 수 있게 되는데 취약점은 NFS 서버가 파일 시스템 마운트 요청을 처리하는 소프트웨어에 존재한다. 이 소프트웨어는 일반적으로 mountd나 rpc.mountd라고 불린다. 이 취약점으로 인해 공격자는 취약한 NFS 파일 서버에 시스템 관리자 접근권한을 획득할 수 있다. 이 취약점은 원격지에서 공격당할 수도 있어서 공격목표 시스템에 계정이 필요 없다. 즉, 이 버퍼오버플로우 취약점으로 인해 원격지의 공격자는 시스템 관리자 권한으로 임의의 코드를 실행할 수 있다.
  - 대책 : 리눅스 시스템 제공업체로부터 패치를 설치한다. 해당 시스템이 반드시 NFS 서버 역할을 할 필요가 없을 경우에는 시스템에서 mountd 데몬을 사용 중지시켜야 한다.

## 3.7 각종 Trojan 및 Exploit 이해

### 3.7.1 Trojan, Exploit 등

#### o 핵심가이드

- Trojan, Exploit 식별 요령
- Trojan, Exploit 대처 요령

#### (1) Trojan, Exploit 식별 요령

o Trojan은 악의적인 프로그램을 건전한 프로그램처럼 포장하여 일반 사용자들이 의심 없이 자신의 컴퓨터 안에서 이를 실행시키고 실행된 Trojan은 특정 포트를 열어 공격자의 침입을 돕고 추가적으로 정보를 자동 유출하며 자신의 존재를 숨기는 기능 등을 수행하는 공격 프로그램이며, Exploit은 OS에서 버그를 이용하여 루트권한 획득 또는 특정 기능을 수행하기 위한 공격 코드 및 프로그램을 의미한다.

#### o Trojan 식별

- 안티바이러스 프로그램 등의 도구를 이용하여 탐지
- 네트워크의 연결상태 및 자신의 컴퓨터에 열려진 포트를 검사
- 자신이 설치하지 않은 프로그램이 동작하는 지 검사
- 레지스트리를 검사하여 자동실행 설정되어 있는 프로그램 검사
- 루트킷이 설치된 경우 프로세스 및 프로그램 등을 숨기므로 안티바이러스 프로그램 또는 전용 루트킷 탐지 도구를 이용하여 검사
- 무결성 점검도구를 활용

#### o Exploit 식별

- 안티바이러스 프로그램 등의 전용도구를 이용하여 탐지
- 자신이 저장하지 않은 파일이 저장되어있는 경우에 그 파일을 의심할 수 있으며 코드 분석을 수행하여 식별
- 자신의 컴퓨터에 저장된 파일이 Exploit 이름과 동일한 경우 의심
- 무결성 점검도구를 활용

#### (2) Trojan, Exploit 대처 요령

o Trojan 대처 요령

- Trojan 프로그램은 안티바이러스 프로그램 또는 전용 도구를 이용하여 제거할 수 있으며 직접 제거할 때는 프로그램을 삭제하고 레지스트리 등을 검사하여 자동실행 설정을 제거한다.

o Exploit 대처 요령

- 안티바이러스 프로그램 등의 전용 도구를 이용하여 탐지 및 제거할 수 있으며 Exploit라고 식별이 되면 파일을 삭제한다.

## 4. 각종 네트워크 장비를 이용한 보안기술

### 4.1 침입탐지시스템(IDS)의 이해

#### 4.1.1 원리, 종류, 작동방식, 특징, 구성, 실제 활용 등 [1급]

##### o 핵심가이드

- IDS(Intrusion Detection System)의 원리
- IDS의 종류 및 특징
- IDS의 작동 원리 이해
- IDS의 구성과 활용 이해

#### (1) IDS(Intrusion Detection System)의 원리

- o 침입탐지시스템은 대상 시스템(네트워크 세그먼트 탐지 영역)에 대한 인가되지 않은 행위와 비정상적인 행동을 탐지하고, 탐지된 불법 행위를 구별하여 실시간으로 침입을 차단하는 기능을 가진 보안시스템이다. 침입탐지시스템은 일반적인 보안시스템 구현 절차의 관점에서 침입차단시스템과 더불어 가장 우선적으로 구축되었으며, 침입탐지시스템의 구축 목적은 해킹 등의 불법 행위에 대한 실시간 탐지 및 차단과 침입차단시스템에서 허용한 패킷을 이용하는 해킹 공격의 방어 등의 목적으로 구축된다.

#### (2) IDS의 종류 및 특징

##### o 데이터 소스 기반 분류

- 네트워크 기반 IDS(Network-IDS) : 네트워크의 패킷 캡처링에 기반하여 네트워크를 지나다니는 패킷을 분석해서 침입을 탐지하고 네트워크 기반 IDS는 네트워크 단위에 하나만 설치하면 된다. 호스트 기반 IDS에 비하여 운영체제의 제약이 없고 네트워크 단에서 독립적인 작동을 하기 때문에 구현과 구축 비용이 저렴하다
- 호스트 기반 IDS(Host-IDS) : 시스템 내부에 설치되어 하나의 시스템 내부 사용자들의 활동을 감시하고 해킹 시도를 탐지해내는 시스템이다. 각종 로그파일 시스템콜 등을 감시한다. Host기반의 IDS는 시스템 감사를 위해서는 기술



적인 어려움이 크고, 비용 또한 비싸다, 그리고 로그분석 수준을 넘어 시스템 콜 레벨 감사까지 지원해야 하기 때문에 여러 운영체제를 위한 제품을 개발하는 것 또한 시간적, 기술적으로 어렵다

- Hybrid IDS : 두 종류를 통합한 형태의 IDS.

o 침입모델 기반 분류

- 오용탐지 : 알려진 공격법이나 보안정책을 위반하는 행위에 대한 패턴을 지식 데이터베이스로부터 찾아서 특정 공격들과 시스템 취약점에 기초한 계산된 지식을 적용하여 탐지해 내는 방법으로 지식 기반(Knowledge-Base)탐지라고도 한다. 자신이 가지고 있는 지식에 기반하여 취약점들에 대한 정보를 알아내고 해당 취약점을 이용하려는 시도를 찾기 때문에 비교적 탐지의 정확도가 높으나 알려진 공격에 대한 정보 수집이 어려우며 새로운 취약성에 대한 최신 정보를 유지하기가 어렵다.

- 비정상적인 행위탐지 : 시스템 사용자가 정상적이거나 예상된 행동으로부터 이탈하는지의 여부를 조사함으로써 탐지하는 방법을 말한다. 정상적인 혹은 유효한 행동 모델은 다양한 방법으로 수집된 참조 정보들로부터 생성되며 현재 활동과 행동 모델을 비교함으로써 탐지한다. 이탈이 발견되면 경보가 발생하며 모든 침입을 탐지할 수 있을 만큼 완벽하지만 높은 확률의 잘못된 경보(False alarm)로 정확성이 문제가 된다.

(3) IDS의 작동 원리 이해

o 침입탐지 시스템은 데이터수집 단계, 데이터의 가공 및 축약 단계, 침입 분석 및 탐지 단계, 그리고 보고 및 대응 단계의 4 단계 구성 요소를 갖는다.

- 데이터 수집(raw data collection) 단계는 침입탐지 시스템이 대상 시스템에서 제공하는 시스템 사용 내역, 컴퓨터 통신에 사용되는 패킷 등과 같은 탐지대상으로부터 생성되는 데이터를 수집하는 감사 데이터(audit data) 수집 단계이다.

- 데이터 가공 및 축약(data reduction and filtering) 단계는 수집된 감사데이터가 침입 판정이 가능할 수 있도록 의미 있는 정보로 전환시킨다.

- 분석 및 침입탐지 단계에서는 이를 분석하여 침입 여부를 판정하는데, 이 단계는 침입탐지 시스템의 핵심 단계이며, 시스템의 비정상적인 사용에 대한 탐지를 목적으로 하는지, 시스템의 취약점이나 응용 프로그램의 버그를 이용한 침입에 대한 탐지를 목적으로 하는지에 따라 비정상적 행위 탐지 기술과 오

용 탐지 기술로 나뉘어진다.

- 보고 및 대응(reporting and response) 단계에서는 침입탐지 시스템이 시스템의 침입 여부를 판정한 결과 침입으로 판단된 경우 이에 대한 적절한 대응을 자동으로 취하거나, 보안관리자에게 침입 사실을 보고하여 보안관리자에 의해 조치를 취하게 한다. 최근 들어서는 침입탐지 및 대응에 대한 요구가 증가되고 있으며, 특히, 침입을 추적하는 기능에 대한 연구가 시도되고 있다

#### (4) IDS의 구성과 활용 이해

- o Host 기반 IDS : 단일 호스트로부터 수집된 감사 자료를 침입 판정에 사용하며, 하나의 호스트만을 탐지 영역으로 하기 때문에 호스트에 설치
- o Network 기반 IDS : 네트워크의 패킷 자료를 침입 판정에 사용하며 네트워크 영역 전체를 탐지 영역으로 하기 때문에 스위치 등 네트워크 장비에 연결하여 설치

#### 4.1.2 False Positive, False Negative 등 [1급]

##### (1) IDS의 침입 판정 원리 이해

- o 핵심가이드
  - IDS의 침입 판정 원리 이해
- o 침입탐지에는 두 개의 상보적인 흐름이 있는데, 첫째는 공격에 관한 축적된 지식을 사용하여 어떤 공격을 사용하고 있다는 증거를 찾는 방식이며, 두 번째는 감시중인 시스템의 정상행위에 관한 참조모델을 생성한 후 정상행위에서 벗어나는 경우를 찾는 방식이다.
  - 지식기반 침입탐지(오용탐지) 방법은 알려진 침입행위를 이용하여 침입을 탐지하고, 정해진 모델과 일치하는 경우를 침입으로 간주한다. 이러한 방법에는 전문가시스템(Expert System), 시그너처 분석(Signature Analysis), 페트리넷(Petri-net), 상태전이분석(State Transition Analysis), 신경망(Neural Network), 유전 알고리즘(genetic algorithm) 등이 있다.
  - 행위기반 침입탐지(비정상행위 탐지) 방법은 사용자의 패턴을 분석한 후, 입력 패턴과 비교하여 침입을 탐지하는데, 이러한 방법에는 통계적(Statistical) 방법, 전문가시스템(Expert System), 신경망(Neural Network), 컴퓨터 번역학

(Computer Immunology), 데이터마이닝(Data Mining), HMM(Hidden Markov Model), 기계학습(machine learning) 방법 등이 있다.

- 침입탐지를 위한 분석을 수행하는 방식에 따라 정적 및 동적 침입탐지로 나눌 수 있다. 동적 침입탐지시스템은 시스템에 영향을 미치는 이벤트가 발생하는 즉시 획득함으로써 실시간 분석을 수행하며, 정적 침입탐지시스템은 시스템의 스냅샷을 잡아서 분석한 후 취약한 소프트웨어나 구성오류 등을 찾는다.

## (2) False Positive/False Negative 판정 이해

### o 핵심가이드

- False Positive/False Negative 판정 이해

o False Positive : 실제로 잘못된 정보를 옳다고 판단하는 오류

o False Negative : 실제로 옳은 정보를 틀린 정보로 인식하는 오류

## 4.2 침입차단시스템(Firewall)의 이해

### 4.2.1 원리, 종류, 작동방식, 특징, 구성, 실제 활용 등

#### (1) 방화벽의 종류 이해

### o 핵심가이드

- 스크린라우터
- 베스천호스트
- 프락시(proxy) 서버 등

o 방화벽이란 외부로부터 내부망을 보호하기 위한 네트워크 구성요소 중의 하나로써 외부의 불법 침입으로부터 내부의 정보자산을 보호하고 외부로부터 유해 정보 유입을 차단하기 위한 정책과 이를 지원하는 H/W 및 S/W를 말한다. 두 네트워크 간을 흐르는 패킷들을 미리 정해놓은 규칙에 따라 차단하거나 보내주는 간단한 패킷 필터를 해 주는 라우터라 할 수 있다

### o 방화벽의 기능

- 접근제어 : 정책에 의하여 허용/차단 결정하기 위한 검사
- 로깅 및 감사 추적
- 인증(Authentication) : 네트워크 스니핑 등의 공격에 대응하는 방법의 인증

- 무결성(Integrity)
- Traffic의 암호화
- 트래픽 로그
- o 방화벽 종류
  - 패킷필터링(packet filtering) 방식
    - 패킷필터링은 방화벽의 가장 기본적인 형태의 기능을 수행하는 방식이다. 패킷필터링은 설정된 규칙에 의해 패킷의 통과여부를 결정하는 것으로 외부 침입에 대한 1차적 방어수단으로 활용된다. 패킷필터링 방식의 방화벽은 OSI 모델에서 네트워크층(IP 프로토콜)과 전송층(TCP 프로토콜)층에서 패킷의 출발지 및 목적지 IP 주소 정보, 각 서비스에 port 번호, TCP Sync 비트를 이용한 접속제어를 한다.
  - 애플리케이션(Application) 방식
    - 애플리케이션 게이트웨이 방식은 사용자가 서비스를 요청하면 애플리케이션 게이트웨이를 통해 사용자의 요청을 원격시스템의 서비스에 요구하고 다시 요청된 파일 및 관련 정보를 애플리케이션 게이트웨이를 통해 사용자에게 전달하는 방식이다. 이때 접속관련 정보의 기록 및 활용이 애플리케이션 게이트웨이를 통해 이루어지게 된다. 애플리케이션 게이트웨이는 OSI 7계층 네트워크 모델의 애플리케이션 계층에 방화벽 기능이 들어있다. 이 게이트웨이는 각 서비스별로 Proxy Daemon이 있어 프락시 게이트웨이 또는 응용 게이트웨이라고도 한다. 애플리케이션 게이트웨이는 각 서비스별 프락시를 이용하여 패킷필터링 방식처럼 IP 주소 및 TCP port를 이용하여 네트워크 접근제어를 할 수 있으며 추가적으로 사용자 인증 및 파일전송시 바이러스 검색기능과 같은 기타 부가적인 서비스를 지원한다.
  - 서킷 게이트웨이(Circuit Gateway)
    - 서킷 게이트웨이는 OSI 네트워크 모델에서 5계층에서 7계층 사이에 존재하며 애플리케이션 게이트웨이와는 달리 각 서비스별로 프락시가 존재하는 것이 아니고, 어느 애플리케이션도 이용할 수 있는 일반적인 프락시가 존재한다. 방화벽을 통해서 내부 시스템으로 접속하기 위해서는 먼저 클라이언트 측에 서킷 프락시를 인식할 수 있는 수정된 클라이언트 프로그램이 필요하다. 따라서 수정된 클라이언트 프로그램이 설치되어있는 클라이언트만 circuit 형성이 가능하다.
  - 하이브리드(Hybrid) 방식
    - 여러 유형의 방화벽들을 경우에 따라 복합적으로 구성할 수 있는 방화벽이

다. 이 방화벽은 서비스의 종류에 따라서 사용자의 편의성, 보안성 등을 고려하여 방화벽 기능을 선택적으로 부여할 수 있지만 서비스의 종류에 따라서 다양한 보안정책을 부여함으로써 구축 및 관리하는데 어려움이 따를 수 있다. CheckPoint의 Firewall-1이 전형적인 패킷필터링 방식의 방화벽에서 패킷필터링과 애플리케이션 게이트웨이를 혼합한 형태의 방화벽시스템으로 변화되었다.

o 방화벽 구축 형태

- Dual Homed Host : Dual-Homed 게이트웨이는 두 개의 네트워크 인터페이스를 갖는 호스트이며 한 개는 외부, 한 개는 내부와 연결되어 있기 때문에 물리적으로 내부와 외부 네트워크를 연결하는 역할을 하며 이 두 인터페이스 사이에서 필터링을 한다.
- screening router : 패킷 필터링(스크리닝)라우터의 한 포트는 외부망에 연결되어 있고 다른 포트는 내부망에 연결되어 있고 베스천 호스트가 내부에 있는 형태의 방화벽을 뜻한다.
- Screened Subnet : Screened 호스트 방식의 보안상 문제점을 보완하기 위해서 외부 네트워크와 내부 네트워크 사이에 하나 이상의 경계 네트워크를 두어 내부 네트워크를 외부 네트워크로부터 분리하기 위한 구조이다. 비무장 지대(DMZ)라고 불리는 경계 네트워크에는 서비스를 위해 외부에서 접속이 많은 시스템을 구성하고 보호할 정보가 많은 시스템은 내부 네트워크 안에 구성한다.

(2) 패킷필터링 기능

o 핵심가이드

- 데이터의 흐름 필터링 원리 이해
- 통과 허용/차단 원리 이해
- 상태추적 등 최근 관련 기술 이해

o 방화벽에서 패킷필터링을 위해서는 들어오는 패킷과 나가는 패킷 방향, 포트번호, ip주소, TCP 헤더의 플래그 등을 이용하여 패킷을 필터링 할 수 있다. 데이터의 gm를 필터링 원리는 외부로 부터 들어오는 패킷과 내부에서 나가는 패킷의 흐름을 분석하여 정책에 따라서 필터링

o 통과 허용/차단 원리는 방화벽을 통과하는 패킷의 IP 헤더 및 TCP 헤더를 열어서 정책을 검사하여 필터링하게 된다.

## 4.3 가상사설망(VPN)의 이해

### 4.3.1 원리, 작동방식, 특징, 구성, 실제 활용 등 [1급]

#### o 핵심가이드

- VPN의 동작원리 이해
- VPN의 구성과 활용 이해

#### (1) VPN의 동작원리 이해

##### o 가상사설망(VPN: Virtual Private Network)

- 인터넷(Internet)과 같은 공중망을 이용하여 사설망과 같은 효과를 얻기 위한 기술로 기존의 전용선을 이용한 사설망에 비해 훨씬 저렴한 비용으로 보다 연결성이 뛰어나면서도 안전한 망을 구성할 수 있다. 또한 VPN은 Public Switched Network(인터넷) 상에서 물리적인 네트워크의 구성과는 무관하게 논리적인 회선을 설정하여, 별도의 사설망을 구축하지 않고도 사설망에서의 안정성을 보장하기 위한 가상 사설 통신망을 구축하는 기술이다.
- VPN을 구성하기 위한 핵심 기술로는 터널링(tunneling) 기술과 암호화 기술이 있다. VPN에 사용되는 터널링(tunneling) 기술은 인터넷 상에서 외부의 영향을 받지 않는 가상적인 터널을 형성해 정보를 주고받도록 하는 기술로서, 시작점에서 끝점까지 상호 약속된 프로토콜로 세션을 구성하게 된다.
- 암호화 혹은 인증 터널을 통해 전송되는 데이터는 기밀성, 무결성, 인증 과 같은 보안 서비스가 보장된다.

##### o VPN 동작원리

###### - 터널링 기술(tunneling)

- 터널링 기술은 VPN 의 기본이 되는 기술로서 터미널이 형성되는 양 호스트 사이에 전송되는 패킷을 추가 헤더 값으로 인캡슐화(Encapsulation)하는 기술이다. 이때 덧붙여지는 헤더는 각 터널링 프로토콜에 따라 다른 값을 지닌다.
- L2TP 터널링은 2계층 터널링 기술이기 때문에 데이터링크층 상위에서 L2TP 헤더를 덧붙이고 IPSec 터널링은 3계층 터널링 기술이기 때문에 인터넷층 상위에서 IPSec(AH, ESP) 헤더를 덧붙인다. 이러한 인캡슐화 과정은

인터넷망을 통한 데이터 전송의 경우에도 다른 네트워크를 통하지 않고 목적지까지 한 홉(Hop)으로 이동하는 것처럼 보이게 한다. 즉, 두 터널링 End to End 포인트에게 가상경로를 설정해준다.

- VPN 터널링(tunneling) 기술은 사용자에게 투명한 통신 서비스를 제공해 줄뿐 아니라 인터넷과 같은 안전하지 못한 네트워크 환경에서 강력한 보안을 제공한다.
- 데이터 암호화 및 인증 기술(Data Encryption/Data Authentication)
  - VPN을 통한 터널 내 보안 기능은 데이터의 암호화 기술 및 무결성 도구를 통한 데이터 인증 기술에 의해 이루어진다.
  - 데이터 암호화 기술의 경우 터널이 형성된 한 쪽 호스트에서 데이터를 암호화하여 보내면 반대편 호스트에서 암호화 데이터를 복호화하여 원본 데이터를 확인한다. 데이터 인증 기술은 터널을 통해 전송할 데이터의 해쉬값을 원본 데이터와 같이 전송함으로써 수신 호스트 측이 데이터의 무결성을 검증할 수 있도록 돕는다.
- 인증 기술(Source Authentication) 및 접근 제어 기술(Access Control)
  - VPN은 데이터의 출처(출발지 IP)가 확실한지의 대한 인증기술을 제공하고 내부 자원에 대해서 허가 받지 않은 사용자의 접속을 차단하는 접근제어 기능을 제공한다. 이러한 인증기술 및 접근제어기술은 VPN 게이트웨이를 통하여 터널이 생성되는 경우 게이트웨이의 정책에 따라 결정된다.

## (2) VPN의 구성과 활용 이해

### o 접속 지점에 따른 분류

- VPN은 터널이 생성되는 네트워크 영역에 따라 보통 다음의 세 가지 형태로 분류하며 각각의 경우에 서로 다른 보안 정책(Security Policy)이 필요하고 다른 구현 기술이 존재할 수 있다.
  - 지사 연결(branch office interconnection or Intranet)
  - 회사간 연결(inter-company connection or Extranet)
  - 원격 접근(Remote access)

### o 터널링(Tunneling) 기법에 의한 분류

- 가상사설망(VPN) 구현에 가장 널리 사용되는 터널링 프로토콜(Tunneling Protocol)로는 PPTP, L2TP, IPSEC, SOCKS V5 가 있다.

## 4.4 라우터의 이해

### 4.4.1 라우터 자체 보안설정

#### o 핵심가이드

- 라우터 자체 보안 설정 방법으로 기본적인 암호설정, 불필요한 서비스에 대한 제거 및 정책설정, 허가된 사용자만이 접근할 수 있도록 하는 접근통제 등에 대해서 이해

#### (1) 라우터 자체 보안 설정 이해

#### o 기본 접근통제

- 암호설정을 통한 접근통제
- 사용자마다 계정 및 패스워드 설정하여 원격에서 텔넷을 이용하여 라우터에 접속할 때 계정 및 패스워드를 이용하여 로그인하도록 설정
  - Router(config)#username XXXX password XXXX
  - Router(config)#line vty 0 4
  - Router(config-line)#login local
  - Router(config-line)#^Z
- IP 주소 필터링을 통한 텔넷 연결 제한을 하여 보안을 강화할 수 있다. 특정 IP의 접속을 허용하고 그 외 접속은 필터링을 하도록 ACL을 10번으로 생성하고 VTY에 적용한다.
  - Router(config)#access-list 10 permit 219.252.48.200
  - Router(config)#access-list 10 deny any
  - Router(config)#line vty 0 4
  - Router(config-line)#access-class 10 in
  - Router(config-line)#^Z
- 사용자별 권한 수준 지정 : 시스코 라우터에서는 0에서 15단계까지 권한 레벨이 있으므로 사용자별로 권한 수준을 지정하여 보안 강화 가능
  - Router(config)#username XXXX privilege 권한레벨 password XXXX

#### o 배너변경

#### o 불필요한 프로토콜과 서비스 제거

- ICMP 프로토콜을 ACL로 차단



- ICMP redirect 차단
- TCP/UDP Small Services 차단 : no service tcp-small-servers 등
- finger 차단
- http 차단
- CDP 차단
- Bootp
- DNS
- PAD 등
  - Router(config)# no service udp-small-servers
  - Router(config)# no service pad
  - Router(config)# no service finger
- o SNMP 보안 : 보안 기능이 강화된 버전 3을 사용하는 것을 권장
- o access-list를 이용한 접근제어에 대한 방법론 이해
- o 로깅

#### 4.4.2 라우터를 이용한 네트워크 보안설정

- o 핵심가이드
  - 라우터를 이용한 네트워크 보안 설정 방법으로 트래픽 제어 설정 등에 대해 이해한다.
  - 소스라우트 원리와 기능 이해
  - 라우팅 프로토콜 보안

##### (1) 라우터를 이용한 네트워크 보안 설정 이해

- o ingress 필터링 설정
  - ingress 필터링은 앞에서 살펴보았던 standard 또는 extended access-list를 활용하여 라우터 내부로 즉 사내 네트워크로 유입되는 패킷의 소스 ip나 목적지 포트 등을 체크하여 허용하거나 거부하도록 필터링하는 것을 뜻한다. 먼저 공통적으로 필터링하여야 할 소스ip 는 인터넷상에서 사용되지 않는 ip 대역이다. 대부분의 공격이 실제 존재하지 않는 위조된 ip 주소를 소스로 하여 진행되므로 이 ip 대역만 차단해도 일정정도의 비정상 패킷을 사전에 차단하는 효과가 있다.
    - Router#configure terminal

· Router(config)# access-list 102 deny ip 127.0.0.1 0.255.255.255 any

o egress 필터링 설정

- egress filtering 이란 내부에서 라우터 외부로 나가는 패킷의 소스 ip 를 체크하여 필터링하는 것이다. 만약 라우터 내부에서 220.1.2.0/24 의 C class 대역을 사용한다면 라우터를 통과하여 외부로 나가는 트래픽의 소스 ip 는 반드시 이 대역인 것이 정상이며 이외의 패킷은 모두 위조된 패킷일 것이다. 따라서 라우터를 통해 나가는 패킷의 소스 ip 중 사용 중인 ip 대역을 소스로 한 패킷은 허용하고 나머지는 거부하도록 access-list를 설정하면 내부 네트워크에서 소스 ip를 위조하여 외부로 나가는 트래픽을 차단할 수 있을 것이다.

o Null routing을 활용한 필터링

- access-list와 함께 유용하게 사용할 수 있는 필터링 기법으로는 blackhole 필터링이라는 것이 있다. 만약 시스템이나 네트워크를 모니터링하던 중 특정 ip 또는 특정 대역에서 비정상적인 시도가 감지되었을 경우 해당 ip를 차단하기 위해 매번 기존 access-list를 지우고 새롭게 ip를 추가하여 작성하는 것은 여간 번거로운 일이 아닐 수 없다. 이때 사용할 수 있는 것이 바로 black hole 필터링인데, 명령어 자체는 특정한 목적지 ip 또는 ip 대역에 대하여 routing 테이블을 생성하는 방식과 동일하다. 다만, 특정한 ip 또는 ip 대역에 대해서 Null 이라는 가상의 쓰레기 인터페이스로 보내도록 함으로써 패킷의 통신이 되지 않도록 하는 것이다. 이의 사용 형식은 다음과 같다.

· interface Null0

· no ip unreachable

· ip route <차단하고자하는목적지ip 또는 ip대역> <netmask> Null0

- 라우터에서는 패킷이 Null0 인터페이스로 보내어져 패킷이 필터링 될 때마다 패킷의 소스 ip 로 icmp unreachable이라는 에러 메시지를 발송하게 되는데, 만약 필터링하는 패킷이 많을 경우에는 라우터에 과부하를 유발할 수 있기 때문에 Null 인터페이스에서 이에 대해 icmp 에러 메시지로 응답하지 않도록 no ip unreachable 설정을 반드시 하도록 한다.

o Unicast RPF를 이용한 필터링

- Unicast RPF의 원리는 인터페이스를 통해 들어오는 패킷의 소스 ip 에 대해 라우팅 테이블을 확인하여 들어온 인터페이스로 다시 나가는지 확인하는 것이다. 즉, URPF가 enable 된 인터페이스에 1.1.1.1이라는 소스 ip를 달고 들어오는 패킷이 있다면 라우팅 테이블을 확인하여 만약 1.1.1.1이라는 목적지로 라우팅 될 때 같은 인터페이스를 통하여 나가는지 확인하여 같다면 정상적인

트래픽으로 간주하여 트래픽을 통과시키고, 다르다면 스푸핑된 패킷으로 간주하여 필터링하는 것이다. 만약 Unicast RPF를 serial 인터페이스에 설정한다면 라우팅 테이블에 없거나 소스 ip를 위조하는 형태의 패킷을 필터링할 수 있을 것이고, ethernet 인터페이스에 설정한다면 내부에서 패킷을 위조하여 나가는 패킷을 필터링 할 수 있을 것이다. 즉, serial 인터페이스에 설정할 경우 ingress 필터링의 효과를, ethernet 인터페이스에 설정할 경우 egress 필터링의 효과를 기대할 수 있을 것이다.

- Unicast RFP를 이용하면 앞에서 살펴본 access-list 나 blackhole 필터링을 이용하여 일일이 ip나 ip 대역을 지정하지 않고도 비정상 트래픽을 효율적으로 필터링할 수 있다.

## (2) 소스라우트 원리와 기능 이해

o 패킷을 수신 IP주소에 전송할 때 경로를 지정해서 패킷을 전송하는 방법으로 IP 패킷에 경유하는 경로 정보를 설정해 두고 그 경로상에 있는 라우터가 정보에 따라 수신측에 패킷을 보내는 방법이다. 즉, 패킷의 전송은 수신측 IP주소의 호스트에 도달하기 까지 목적 경로 상에 있는 라우터 등이 중계를 하여 실현되므로 이때 지정한 경로나 라우터에 따라 전송하기 위한 기술이다. IP 소스라우팅에는 대략적으로 경로를 지정하는 루즈 소스라우팅과 정확하게 경로를 지정하는 스트릭트 소스 라우팅이 있다.

- 루즈 소스라우팅(Loose Source and Record Route) : 송신측에서 패킷이 통과하는 라우터를 지정한다. 스트릭트 소스라우팅과 달리 지정된 라우터까지는 임의의 수의 라우터를 경유할 수 있다.

- 스트릭트 소스라우팅(Strict Source and Record Route) : 송신측에서 패킷이 통과하는 경로를 정확하게 지정한다. 소스 라우터에 지정되어 있는 경로대로 패킷을 전송할 수 없는 경우에는 ICMP 에러가 돌아온다.

o 라우터에서 소스라우팅은 패킷이 네트워크의 어떤 경로를 거쳐서 전달되는가를 보여주는데 특별한 이유 없이는 사용할 필요가 없으므로 차단한다.

- Router(config)#no ip source-route

- Router(config)#^Z

### (3) 라우팅 프로토콜 보안

#### o Static 라우팅

- 가장 안전한 라우팅 방법으로 라우팅 프로토콜을 사용하지 않기에 공격자가 임의로 라우팅 정보를 변경하거나 조작할 수 없다.

#### o Dynamic 라우팅 : 가장 안전하게 사용하는 방법은 라우팅 프로토콜에 인증 기능을 적용하는 것으로 인증을 구현하기 위해서는 라우팅 패스워드를 설정할 수 있다.

- RIPv2 : 인증 기능을 적용

- Router(config-if)#ip rip authentication key-chain 10
- Router(config-if)#ip rip authentication mode md5
- Router(config-if)#exit
- Router(config)#key chain 10
- Router(config-keychain)#key 1
- Router(config-keychain-key)#key-string UnguessableKey

- EIGRP : 인증 기능을 적용하는 방법은 RIPv2와 유사

- OSPF

- 각각의 인터페이스에 ip ospf message-digest-key 명령을 사용하여 key를 정의
- area 번호 authentication-digest 명령을 사용하여 OSPF 프로토콜 사용시에 인증을 하도록 설정

- BGP : 인증 설정은 neighbor 명령을 사용하여 password 키워드를 명령에 추가함으로써 단순하게 설정이 가능

### 4.4.3 Reflexive Access-list, NBAR를 통한 보안설정 [1급]

#### o 핵심가이드

- Reflexive Access-list를 이용하여 상태추적이 가능한 Access-list를 설정 이해
- 웹 형태의 공격을 라우터에서 차단할 수 있는 방법 이해
- NBAR의 분류기능 이해

### (1) Reflexive Access-list를 이용하여 상태추적이 가능한 Access-list를 설정 이해

- o Reflexive access list는 상위 레이어 세션 정보를 기반으로 IP 패킷을 필터링하는 것으로 Reflexive access list는 내부 네트워크에서 생성된 세션에 대한 IP 트래픽을 허용하고 외부 네트워크에서 생성된 세션에 대한 IP 트래픽은 거부하도록 하는데 이용할 수 있는 일종의 세션 필터이다. Reflexive access list는 확장된 네임(Extended named) IP 액세스 리스트로 정의되며 번호나 표준 네임 IP 액세스 리스트 또는 다른 프로토콜 액세스 리스트로 정의할 수 없다.
- o Reflexive access list는 다른 액세스 리스트와 비슷한데 IP 패킷을 허용하기 위한 규칙을 정의한 조건 엔트리를 포함한다. 이 엔트리는 순서대로 검사하고 조건에 맞았을 때 더이상 엔트리를 검사하지 않는다. 그러나, 다른 형식의 액세스 리스트와 큰 차이점이 있다. Reflexive access list는 새로운 IP 세션이 시작될 때 (예로 아웃바운드 패킷) 자동으로 생성되고 세션이 종료되었을 때 제거되는 임시 엔트리만을 가진다. Reflexive access list는 인터페이스에 직접적으로 적용하는 것이 아니고 인터페이스에 적용된 확장된 네임 IP 액세스 리스트를 이용한다.
- o 기본적인 액세스 리스트와의 차이점
  - 기본적인 방법과 고정된 확장 액세스 리스트를 가지고 'established'일 때 허용 명령어를 이용하여 세션 필터링을 유사하게 할 수 있다. 'established' 상태는 ACK 또는 RST 신호가(ACK or RST 비트는 패킷이 세션에서 시작이 아니라는 것을 의미하므로 패킷이 'established' 세션에 속한다는 것을 의미한다.) 설정되어있는 지에 따라서 TCP 패킷을 필터링할 수 있다. 이러한 필터링 방식은 인터페이스에 영구적으로 적용되는 액세스 리스트 중에 하나가 된다.
  - Reflexive access list는 패킷이 허용되어지기 전에 액세스 리스트의 검사가 수행되어지므로 스푸핑을 더 어렵게 하는 세션 필터링의 형태이다.(예로, ACK와 RST 비트만을 검사하는 것이 아니고 소스와 목적지 주소, 포트번호를 검사한다.) 세션 필터링은 세션이 종료될 때 제거되는 임시적인 필터를 사용한다. 또한, 아주 짧은 시간동안의 공격자의 공격 기회를 제한할 수 있다. 더욱이 'established' 상태를 가지고 필터링하는 방식은 TCP 상위 레이어 프로토콜에만 적용될 수 있으므로 다른 상위 프로토콜에(UDP, ICMP 등) 대해서 들어오는 트래픽들을 허용하거나 각각 프로토콜에 대해 모든 경우에 대해 가능한 소스/목적지 호스트/포트 주소쌍들을 정의해야 한다.
- o Reflexive access list는 네트워크 해커로부터 네트워크를 안전하게 보호하는데 중요하게 이용될 수 있다. Reflexive access list는 스푸핑과 여러 종류의 DoS 공격에 대응할 수 있다.

## (2) 웹 형태의 공격을 라우터에서 차단할 수 있는 방법 이해

- 코드레드 웹은 IIS 취약점을 이용한 공격으로써 IIS 버그 보안 패치를 통하여 방어할 수 있지만 웹의 HTTP GET requests가 웹서버로 계속적으로 들어오게 되어 네트워크의 부하에 많은 영향을 미칠 수도 있다. 따라서, 시스코 라우터에서 제공되는 class-map, Policy Map, 접근 제어리스트(ACL)기능 등을 사용하여 네트워크 차원에서 차단할 수도 있다.

### - 공격패턴

```
o 최초의 Code Red의 패턴
2001-08-04 16:32:23 24.101.17.216 - 10.1.1.75 80 GET /default.ida NNNN.....
o Code Red II 의 패턴
2001-08-04 15:57:35 64.7.35.92 - 10.1.1.75 80 GET /default.ida XXXXX.....
```

### - 라우터 보안 설정

- Class-map을 사용하는 방법

```
Router(config)#class-map match-any http-hacks
Router(config-cmap)#match protocol http url "*default.ida*"
Router(config-cmap)#match protocol http url "*x.ida*"
Router(config-cmap)#match protocol http url "*.ida*"
Router(config-cmap)#match protocol http url "*cmd.exe*"
Router(config-cmap)#match protocol http url "*root.exe*" T
```

- Policy Map을 사용하는 방법

## (3) NBAR의 분류기능 이해

- NBAR은 다양한 유형의 애플리케이션을 인식하는 시스코 IOS 소프트웨어의 지능형 분류 엔진으로써 애플리케이션의 QOS 정책을 강화시켜준다. 인식할 수 있는 애플리케이션에는 TCP 또는 UDP 포트 번호를 동적으로 할당하는 웹 기반 애플리케이션, 클라이언트/서버 애플리케이션 등이 포함된다. 네트워크로 하여금 애플리케이션에 적절한 서비스를 제공하고 중요하지 않은 애플리케이션이 중요한 애플리케이션의 성능을 방해하지 않도록 한다.

- NBAR의 기능 이해

### - 프로토콜 발견

- NBAR에 신규 프로토콜 추가 기능
- 지능적 애플리케이션 분류
- QOS 서비스 지원

#### 4.4.4 라우터의 리소스 점검 [1급]

##### o 핵심가이드

- CLI에서의 show process cpu, show process mem으로 CPU나 메모리 상태를 모니터링 이해

(1) CLI에서의 show process cpu, show process mem으로 CPU나 메모리 상태를 모니터링 이해

##### o show 명령어를 이용한 라우터 상태를 파악할 수 있다.

- show controllers s 0 : 인터페이스의 DTE혹은 DCE상태를 보여줌
- show history : 디폴트로 지난 10번의 입력된 명령을 보여줌
- show interface s0 : 인터페이스 시리얼 0의 통계를 보여줌
- show run : show running config의 단축명령. 현재 라우터상에 구동중인 환경설정을 보여줌
- show start : show startup-config의 단축명령. NVRAM내에 저장된 백업환경 설정을 보여줌
- show terminal : 환경설정된 history size를 보여줌
- show version : 라우터의 시스템 정보를 보여줌 ( IOS의 버전, 부팅시간, 메모리종류/크기, H/W 구성정보 등등)

#### 4.4.5 인증 서버를 통한 보안 [1급]

##### o 핵심가이드

- Cisco에서 제공하는 AAA(Authentication, Authorization, Accounting) 모델에 대해 이해

(1) Cisco에서 제공하는 AAA(Authentication, Authorization, Accounting) 모델에 대해 이해

- o Cisco IOS Software AAA 네트워크 보안 서비스는 라우터 또는 액세스 서버에 대해 액세스 제어 설정을 위한 프레임워크를 제공하는데 AAA는 관리자가 특정 서비스 또는 인터페이스에 적용되는 방법 목록을 사용하여 회선(사용자 단위) 또는 서비스(예: IP, IPX, VPDN) 단위로 원하는 인증 및 인가 유형을 동적으로 구성할 수 있도록 한다.

#### 4.4.6 CAR를 이용한 보안설정 [1급]

- o 핵심가이드
  - CAR(Committed Access Rate) 기술 이해
  - ICMP나 SYN 패킷량을 제한하는 기능 이해

##### (1) CAR(Committed Access Rate) 기술 이해

- o CAR(Committed Access Rate)은 레이트 필터링(rate filtering)이라고도 하며, 일정 시간 동안 정의한 트래픽양을 초과해 라우터로 유입되는 패킷을 제한함으로써 부가적으로 필요한 대역폭을 어느 수준 이상으로 확보할 수 있다. 또한 CoS(Class of Service) 등을 적용해 패킷을 클래스별로 구분하고 이를 적절한 QoS에 적용할 수 있다. 이를 응용해 불필요한 트래픽을 제한하며 대표적으로 최근 문제가 되고 있는 UDP, ICMP 트래픽이나 SYN 패킷량을 제어할 수 있다. 이는 라우터의 해당 인터페이스에 rate-limit라는 명령어 형식을 이용한다.

##### (2) ICMP나 SYN 패킷량을 제한하는 기능 이해

- o rate-limit 설정 시 정책은 액세스 리스트와 같이 위에서부터 순서대로 조건에 매칭되는지를 체크하므로 설정 순서에 주의해야 한다. 첫 번째 매칭되는 조건이 있으면 이하의 조건은 적용되지 않는다는 점을 주의해야 한다.
  - 첫 번째는 들어오는 트래픽에 대한 액세스 리스트이므로 일단 인바운드되는 패킷 중 150번 액세스 리스트, 즉 UDP에만 해당하는 사항이므로 들어오는 모든 트래픽 중 UDP 패킷은 약 2.5Mbps (2000000+250000+250000) 정도로 제한하는 설정이며, 만약 2.5Mbps가 초과할 경우에는 더 이상의 패킷을 받지 않고 바로 끊어지게 된다.
  - 두 번째는 액세스 리스트 160번에 대한 설정인데, 160번의 의미는 ICMP 패킷



중 echo-reply만 해당하므로 인바운드되는 트래픽 중 echo-reply를 약 0.5Mbps로 제한했다는 것을 알 수 있다. 이는 외부의 브로드캐스트 주소를 증폭기로 악용해 대량의 echo-reply 패킷을 유발하는 대표적인 ICMP 기반의 DoS 공격인 Smurf에 대한 대응 방법이다.

- 세 번째 설정은 첫 번째 설정과 똑같지만, 단지 아웃바운드에 대한 제한이라는 것만 차이가 있다. 네 번째는 앞의 예제에서와 같이 간헐적으로 과도한 아웃바운드 트래픽을 유발하고 있는 서버의 트래픽을 제한하기 위한 설정인데, 해당 IP에서 TCP나 UDP, ICMP 등의 프로토콜에 관계없이 아웃바운드되는 패킷을 1.5Mbps 정도로 제한한 것이다. 물론 그 이상의 트래픽이 유발되면 나머지는 모두 끊어질 것이다.
- 마지막 설정은 액세스 리스트를 설정하지 않고 사용한 것인데, 아웃바운드되는 총 트래픽을 50Mbps로 제한해 더 이상의 트래픽이 유발되지 않도록 하는 것이다. 물론 이 값은 각자의 네트워크 환경에 따라 적절히 변경해야 한다. 이렇게 rate-limit로 트래픽 제한 설정을 끝낸 후에는 “show interface serial 0 rate-limit” 명령어를 사용해 rate-limiting에 대한 그간의 통계를 볼 수 있다
- 시리얼 0 인터페이스에 rate-limit를 설정하는 예를 살펴보도록 한다.
  - int serial 0
  - rate-limit input access-group 150 2000000 250000 250000 conform-action transmit exceed-action drop
  - rate-limit input access-group 160 512000 8000 8000 conform-action transmit exceed-action drop
  - rate-limit output access-group 150 2000000 250000 250000 conform-action transmit exceed-action drop
  - rate-limit output access-group 151 1000000 250000 250000 conform-action transmit exceed-action drop
  - rate-limit output 42000000 3562500 4750000 conform-action transmit exceed-action drop
  - access-list 150 permit udp any any
  - access-list 151 permit ip host 211.47.0.1 any
  - access-list 160 permit icmp any any echo-reply

#### 4.4.7 각종 응용 프로그램을 이용한 라우터 보안 [1급]

- 핵심가이드

- Solarwinds 등 라우터 관련 응용 프로그램을 이용하여 라우터의 보안을 강화하는 방안에 대해 이해

(1) Solarwinds 등 라우터 관련 응용 프로그램을 이용하여 라우터의 보안을 강화하는 방안에 대해 이해

- Solarwinds는 SNMP 스캔을 수행하여 정보 수집에 최적화된 도구이며, 'IP Browser'를 이용하여 지정한 특정 네트워크 영역에서 기본 커뮤니티 값으로 설정된 시스템의 계정 정보와 운영 서비스, 공유 자원, TCP/UDP 포트 정보와 같은 세부 정보를 쉽게 수집할 수 있다. 분산 네트워크 환경에서 SNMP와 MIB을 이용한 모니터링과 관리 작업은 매우 효율적인 작업이지만, 보안에 취약하거나 악용될 경우 심각한 사태를 초래할 수 있기 때문에 이 도구를 이용하여 취약점에 대한 보안강화를 수행할 수 있다.
- RAT는 Cisco IOS 라우터 환경설정에서 보안 설정상태를 점검하는 도구이다. RAT는 주어진 각각의 라우터에서 보안 문제점을 발견해서 이를 대략적인 보안 점수와 함께 리포트 한다. 또한 발견된 문제점에 대해서 hyper link를 통해 문제점에 대한 내용을 자세히 소개하고, 이를 fix할 수 있는 방법을 소개한다. RAT에서 점검하는 항목들은 NSA의 "Router Security Configuration Guide"에서 언급된 보안설정 Checklist에 적합하게 각 라우터의 설정이 정상적으로 취해졌는지를 자동화하여 점검할 수 있도록 구현하였다.

4.5 각종 네트워크 기반 보안 프로그램 활용 방안 이외 다른 네트워크 보안 관련 프로그램을 활용하여 어떻게 보안을 강화할 수 있는지에 대해 평가한다.

4.5.1 기타 네트워크 기반 보안 프로그램의 활용 각 프로그램의 작동원리 및 활용방안에 대해 이해한다.

- 핵심가이드

- 기타 네트워크 기반 보안 프로그램의 활용 각 프로그램의 작동원리 및 활용방안에 대해 이해한다.

4.6 각 장비의 로그 및 패킷 분석을 통한 공격방식의 이해 및 대처요령 로그 및 패킷분석은 문제 확인과 해결 등에 반드시 필요하다. 로그와 패킷 분석을 통해 공격을 인지하는 방법과 이러한 공격에 대해 어떻게 대처할 지에 대해 평가

#### 4.6.1 호스트 및 IDS, 방화벽, 라우터등 각종 네트워크장비의 로그 및 패킷분석 [1급]

##### o 핵심가이드

- 네트워크 기반의 장비 또는 프로그램의 로그나 패킷을 분석
- 라우터, 방화벽의 로그 분석 방법 및 TCPdump를 이용한 패킷 분석 방법

#### (1) 각종 네트워크 기반의 장비 또는 프로그램의 로그나 패킷을 분석

o IDS 중에서 snort는 경고와 경고관련 패킷 데이터 모두를 로그로 저장하며 이 데이터는 snort의 패킷 캡처 엔진에서 수집한 네트워크 트래픽이다. 리눅스에 설치된 경우 공격 로그는 snort 실행시 로그 디렉토리로 지정한 /var/log/snort 에 남게 된다. 로그 디렉토리에는 경고 메시지가 저장되는 alert 파일과 포트스캔 결과가 저장되는 portscan.log 파일 그리고, 각 IP 주소별로 좀 더 상세한 로그를 저장한다.

- FTP 데몬의 site exec 버그를 이용하여 원격에서 시스템 관리자 권한을 취득하려는 공격을 시도하였을 경우 snort에서 alert 파일에 남긴 공격 메시지

```
[**] EXPLOIT x86 NOOP [**]
```

```
03/27-01:38:25.743974 172.16.4.80:2561 -> 172.16.2.34:21
```

```
TCP TTL:63 TOS:0x0 ID:8846 IpLen:20 DgmLen:558 DF
```

```
***AP*** Seq: 0x76E783D2 Ack: 0x499461D5 Win: 0x7D78 TcpLen: 32
```

```
TCP Options (3) => NOP NOP TS: 242635123 77742672
```

```
[**] FTP site exec [**]
```

```
03/27-01:38:27.773483 172.16.4.80:2561 -> 172.16.2.34:21
```

```
TCP TTL:63 TOS:0x0 ID:8850 IpLen:20 DgmLen:478 DF
```

```
***AP*** Seq: 0x76E785CC Ack: 0x49946486 Win: 0x7D78 TcpLen: 32
```

```
TCP Options (3) => NOP NOP TS: 242635327 77742675
```

[참고] 이 결과 FTP 공격에 대해 정상적으로 탐지하고 있음을 알 수 있다. 그리고, 자세한 공격 메시지는 공격자 주소인 172.16.4.80이라는 디렉토리를 참조한다.

##### o TCPDump 패킷 분석

- MSCAN은 jsbach라는 해커가 만든 취약점 스캐닝 도구로써 MSCAN을

TCPDUMP를 이용하여 탐지할 수 있다.

```
14:38:19.459109 0:0:c:8d:24:df 0:0:c:8d:24:df loopback 60:
0000 0100 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000
14:38:21.969109 kitty.test.com.1192 > 210.116.239.255.sunrpc: udp 100
14:38:28.299109 kisa1.test.com.finger > alzza.test.com.6266: F 3185928987:3185928987(0) ack
3769291987 win 8760 (DF)
14:38:28.379109 alzza.test.com.1882 > ns.test.com.domain: 46628+ (45)
14:38:28.379109 ns.test.com.domain > alzza.test.com.1882: 46628* 1/1/0 (114)
14:38:29.459109 0:0:c:8d:24:df 0:0:c:8d:24:df loopback 60:
0000 0100 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000
14:38:30.879109 0:0:c:8d:24:df > 1:0:c:cc:cc:cc sap aa ui/C len=270
0c00 0100 0965 6167 6c65 0002 0011 0000
0001 0101 cc00 04d2 74ef fe00 0300 0d45
7468 6572 6e65 7431 0004 00
.....
```

- tcpdump 로그를 보면 네임서비스에 대한 요청이 엄청나게 증가했음을 볼 수 있으며, 그 외에 취약점 스캐닝을 위한 패킷정보가 나타나 있음을 볼 수 있다. mscan 공격이 인터넷상에서 이루어질 때에 네트워크에 상당히 많은 부하를 줄 수 있음을 알 수 있으며, 특히 네임서버에 대한 부하가 크다.

## (2) 네트워크의 activity 이해

- o 핵심가이드
  - 네트워크의 activity 이해
- o 내부와 외부 네트워크 간에 다양한 서비스를 제공하거나 이용하기 때문에 허용하는 정책을 설정하고 비정상적인 트래픽을 탐지 및 차단하여야 한다.

## (3) 공격여부를 감지하는 방법 이해

- o 핵심가이드
  - 공격여부를 감지하는 방법 이해
- o 라우터, 방화벽, IDS, TCPDUMP에 대한 로그 및 패킷 캡처를 통하여 다양한

공격에 대한 이해를 기반으로 비정상적인 상태 또는 공격 유형을 확인하여 공격을 감지한다.

(4) 이에 대해 대처할 수 있는 방법에 대해 이해

o 핵심가이드

- 이에 대해 대처할 수 있는 방법에 대해 이해

o 라우터 보안 설정

- 코드레드 웹을 공격을 방지하기 위한 라우터 설정 방법

· Class-map을 사용하는 방법

```
Router(config)#class-map match-any http-hacks
Router(config-cmap)#match protocol http url "*default.ida*"
Router(config-cmap)#match protocol http url "*x.ida*"
Router(config-cmap)#match protocol http url "*.ida*"
Router(config-cmap)#match protocol http url "*cmd.exe*"
Router(config-cmap)#match protocol http url "*root.exe*" T
```

· Policy Map을 사용하는 방법 : output 인터페이스가 E0/1이고 input 인터페이스가 E0/0이라고 가정하면 Ethernet 0/0에서 생성되는 트래픽을 통제하고 Ethernet 0/1로 유입되기 전에 필터링되도록 설정한다. inbound 트래픽에 대해 먼저 설정한 후에 outside 인터페이스에 대한 서비스 정책을 적용한다.

```
Router(config)#policy-map mark-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap)#set ip dscp 1
Router(config)#interface ethernet 0/0
Router(config-if)#service-policy input mark-inbound-http-hacks
```

## 5. 최근 경향 및 추세

### 5.1 최근 네트워크 기반 침해사고에 대한 이해

#### 5.1.1 분산반사 서비스 거부 공격(DRDoS), 기타 새로운 공격방식 [1급]

##### o 핵심가이드

- DRDoS 공격의 원리 이해
- DRDoS 공격 대응 방안 이해
- 기타 새로운 공격방식에 대한 이해

#### (1) DRDoS 공격의 원리 이해

- o DRDOS 공격은 DDoS 공격의 에이전트의 설치상의 어려움을 보완한 공격 기법으로 TCP 프로토콜 및 라우팅 테이블 운영상의 취약성을 이용한 공격으로 정상적인 서비스를 작동 중인 서버를 Agent 로 활용하는 공격기법이다.
- o DRDOS 공격원리
  - TCP 취약성 : 기존의 tcp 프로토콜의 대표적인 취약성인 TCP 3-Way Handshake 기법상의 취약성을 이용한다.
  - BGP 프로토콜 취약성 : 인접한 라우터의 라우터 테이블의 정보 교환상의 취약성을 이용한다.
  - Reflection Server 설정 방법 : 인터넷 명령어인 Tracerouter를 이용한 다수의 라우터 및 대용량의 대역폭을 가진 특정한 서비스를 제공하는 서버(예로 www.yahoo.com) 목록을 얻는다.
  - 공격 시스템에서 임의의 서비스를 제공하는 서버를 대상으로 공격 대상들을 대상으로 정해진 임의의 주소로 Spoofing 하여 전송함으로 인하여 기존 라우터들의 라우터 테이블의 자료 전송이 이루어지게 한다.
  - DDoS 와 DRDoS 비교
    - DDoS : Agent를 특정한 버그가 존재하는 시스템에 설치함으로써 관련 DDoS 공격에 사용될 일련의 네트워크 연결망을 형성한다. 이로 인하여 공격전 네트워크 관리자는 네트워크 모니터링 작업을 통하여 DDoS 공격의 탐지 및 제거가 가능하다.
    - DRDoS : 일반 서비스를 제공하는 서버가 Agent 역할을 대신 수행함으로

인하여 사전 연결망 구축과 같은 작업이 가벼워지며 또한 관리자에 의한 네트워크 모니터링 작업을 통하여 공격전 관련 도구의 탐지 작업이 불가능하게 된다.

## (2) DRDoS 공격 대응 방안

- 서버 측면에서는 포트 보통 1024 이상의 포트로 유입되는 Ack/Syn 플래그가 설정된 패킷을 차단함으로써 인하여 DRDoS 공격을 방지할 수 있으나 몇 가지 한계점이 있다. 첫째 IRC 서비스와 같은 예외의 포트의 경우 서비스를 제공하지 못한다. 두 번째 한계점은 웹 전용 SMTP 서비스인 경우 25 포트로부터 나오므로 DRDoS 관련 필터의 복잡성을 야기할 수 있다.
- 클라이언트 보호
  - 클라이언트의 특성상 외부 인터넷 서버의 접속이 잦음으로 인하여 클라이언트의 보호는 사실상 불가능하다.
- Reflection Server 에 대한 보호
  - 완전한 연결이 이루어지지 않은 Syn 패킷을 소스 IP를 인식함으로써 인하여 임의의 시간 안에 연결 실패를 야기할 경우 Reflection 공격 호스트로 단정함으로써 해당 네트워크망의 서버가 Reflection Server 로서 악용되는 것으로부터 보호할 수 있다.

## (3) 기타 새로운 공격방식에 대한 이해

- 최근 발생하는 라우터 스니핑 또는 무선랜 해킹기술 등에 대한 이해

## 5.2 최근 보안솔루션에 대한 이해

### 5.2.1 역추적 시스템, 보안관제, 취약성 점검, ESM 등 [1급]

#### (1) 역추적 시스템

- 핵심가이드
  - 원천지 주소 추적 기법 이해
  - 로그 분석 방법 이해

- 보안 장치간 연동 기법 이해
- o 역추적(traceback)이란 해킹을 시도하는 해커의 실제 위치를 실시간으로 추적하는 기술을 말한다. 역추적 기술은 일반적으로 크게 2가지 분야로 분류한다.
  - 해커의 실제 위치를 추적하는 기술 : TCP 연결 역추적(TCP connection traceback) 혹은 연결 역추적(connection traceback)
  - IP주소가 변경된 패킷의 실제 송신지를 추적하는 기술 : IP 패킷 역추적(IP packet traceback) 혹은 패킷 역추적(packet traceback)
- o 역추적 기술 이해
  - TCP 연결 역추적은 TCP 연결을 기반으로 우회 공격을 시도하는 해커의 실제 위치를 실시간으로 추적하는 기법으로 호스트 기반 연결 역추적 기술과 네트워크 기반 연결 역추적 기술로 분류한다.
    - 호스트 기반 연결 역추적 기술 : 역추적을 위한 모듈이 인터넷상의 호스트들에 설치되는 역추적 기법으로 호스트에서 발생하는 로그 기록 등의 다양한 정보를 바탕으로 역추적을 진행하는 기술이다.
    - 네트워크 기반 연결 역추적 기술 : 네트워크 상에 송수신되는 패킷들로부터 역추적을 수행할 수 있는 정보를 추출하여 역추적을 수행하는 것으로 역추적 모듈이 네트워크 상에 송수신되는 패킷을 확인할 수 있는 위치에 설치된다.
  - IP 패킷 역추적 기술은 IP주소가 변경된 패킷의 실제 송신지를 추적하기 위한 기술이다. IP 패킷 역추적 기법으로는 해커가 전송하는 패킷에 해당 패킷을 전달한 라우터를 표시함으로써 추적할 수 있게 하는 패킷 표시 기법을 이용한 기술이다.

## (2) ESM

- o 핵심가이드
  - ESM의 개념 이해
  - ESM 제품들의 특징
- o ESM은 침입차단시스템(firewall), 침입탐지시스템(IDS), 가상사설망(VPN) 등으로 다른 보안제품에서 발생하는 정보를 한곳에서 손쉽게 관리하여, 불법적인 행위에 대해서 대응할 수 있도록 하는 보안 관리시스템이다.
- o ESM구성요소내용
  - Agent Part : 보안 장비에 탑재. 수집된 데이터를 Manager서버에 전달하고 통



제를 받음

- Manager Part : Agent Part에서 받은 이벤트를 룰에 의해 분석, 저장. Console Part에 그 내용을 인공 지능적으로 통보
- Console Part : Manager Part에서 받은 데이터의 시각적 전달, 상황 판단 기능. Manager Server에게 룰을 설정하도록 지휘/통제

### (3) 취약성 점검 프로그램

#### o 핵심가이드

- 네트워크 기반 프로그램
- 호스트 기반 프로그램
  - 시스템 환경 설정 점검 : 시스템에서 중요한 환경 파일의 설정을 검사한다.
  - 사용자 환경설정 점검 : 사용자의 부주의로 잘못 설정된 환경설정에 대해 검사한다.
  - 파일 무결성 점검 : 시스템 내부의 중요한 파일에 대해 변조나 삭제 유무를 정확히 파악한다.
  - 파일 퍼미션 점검: 시스템 내부의 중요한 파일에 대해 퍼미션을 점검한다.
  - 패스워드 점검 : 각각의 사용자에게 대해 취약한 패스워드를 점검한다.
  - 데몬 버전 점검 : 취약한 프로그램이나 데몬의 버전을 점검한다.

#### o 시스템 취약점 점검 프로그램

- 시스템 취약점 점검도구는 로컬 시스템에 설치되어(취약점 점검 대상에 따른 분류), 시스템 운영체제의 수많은 부분을 자동 점검하여 호스트 내부의 취약점을 발견하거나 취약점에 대한 적절한 교정 방법까지도 제시하는 도구와 원격 서버에 접속하여 슈퍼유저(root) 권한으로 이들 서버의 운영체제 및 시스템 자체의 취약점을 점검하는 도구를 의미한다.
- 파일 무결성 점검도구
  - tripwire : 시스템의 무결성을 보장할 수 있는 데이터베이스를 만들어 시스템의 불법 변경을 점검. 대표적인 파일 무결성 점검도구
  - aide : tripwire를 대신할 수 있는 도구. message digest 알고리즘을 사용하여 파일의 변조를 점검
  - slipwire : 파일의 SHA-1 해쉬값을 비교하여 변경될 경우, 사용자에게 이를 통지하는 기능이 있음
  - fcheck : 유닉스 파일시스템의 변조유무를 점검하기 위한 perl script 도구. 관리

- 자에게 파일시스템의 변화를 통지하는 기능이 있음
- claymore : cron 데몬을 이용하여 주기적으로 파일시스템의 변조유무를 점검. 관리자에게 파일시스템의 변화를 통지하는 기능이 있음
- COPS
- 시스템 설정사항 점검
  - samhah : 각각의 호스트에서 실행되는 모니터링 에이전트와 이러한 에이전트로부터 정보를 수집하는 중앙 로그서버로 구성
  - sbscan : anonymous ftp 설정사항, 패스워드 없는 계정, 열려진 포트, 서브넷의 promiscuous 모드가 설정된 시스템의 탐지, 의심스러운 파일, .rhost 파일, sniffer 점검, rootkit 파일 흔적 검색, xhosts, NFS 설정 사항 등을 점검
  - swatch
  - stjude : 솔라리스 시스템 취약점 점검도구. 솔라리스 시스템에서 권한의 흐름을 감시하는 프로그램. 비정상적인 권한 변화 즉, stack smashing, local root exploits 등을 감시함
  - HFNetChk : 윈도우 시스템의 패치 점검도구. 최신 보안 패치의 설치 유무를 점검
  - MBSA : HFNetChk의 기능을 모두 포함하며, 최신의 윈도우 시스템의 버전별 핫픽스의 설치 유무나 패치 설치 유무를 점검
  - Vetescan local
- 패스워드점검
  - crack : 사용자별로 암호를 추측하여, 이를 /bin/passwd에 의하여 암호화 시킨 뒤 /etc/passwd 파일 내의 암호화 된 정보와 비교하여 암호를 추적하는 도구
  - NTCrack : 윈도우 NT 시스템의 패스워드 크랙 프로그램
- o 네트워크 취약점 점검 프로그램
  - 네트워크 취약점 점검도구는 진단시스템이 설치된 원격 시스템에서 특정 네트워크에 연결된 시스템이나 네트워크의 취약점을 알아내는 것이 목적이므로 특정 시스템이 내부적으로 가지고 있는 취약점을 모두 파악하는데는 한계가 있다. 하지만, 점검서버마다 에이전트를 운영하지 않으므로 네트워크 취약점 점검도구의 관리가 용이하다. 네트워크 취약점 점검도구는 네트워크 상의 알려지지 않은 혹은 비인가된 장비와 시스템을 발견할 수 있는 기능도 가지고 있으며, 알려지지 않은 네트워크의 비인가 된 원격 접근 서버를 발견할 수 있도록 도와준다.
    - nmap : Unix/Linux 기반 동작

- LANguard Network Scanner : Unix/Linux 기반 동작
- NetScanTools : NT/WIN95/98/ME/2000/XP 기반 동작
- Solarwinds : NT/WIN95/98/ME/2000/XP 기반 동작
- Nessus : NT/WIN95/98/2000/Linux/Unix 기반 동작
- SATAN : Unix/Linux 기반 동작
- SARA : Unix/Linux 기반 동작
- SAINT : Unix/Linux 기반 동작
- Internet Scanner : NT/WIN2000 기반 동작
- Shadow Security Scanner : NT/WIN2000 기반 동작
- N-Stealth HTTP Security Scanner : NT/WIN2000 기반 동작
- XScsn : NT/WIN2000 기반 동작
- Nikto : Linux/NT/WIN2000 기반 동작

## 참고문헌

- [1] 운영체제, 상조사, 2002
- [2] 리눅스 서버보안 관리 실무, (주)슈퍼유저코리아, 2005.4
- [3] Microsoft 홈페이지, <http://www.microsoft.com/korea/technet/>
- [4] 인터넷침해사고대응지원센터, [www.krcret.or.kr](http://www.krcret.or.kr)
- [5] 라우터를 활용한 네트워크 보안설정, KISA, 2005
- [6] 정보보안 개론과 실습:네트워크 해킹과 보안, 한빛미디어, 2003
- [7] 정보보안 개론과 실습:시스템해킹과 보안, 한빛미디어, 2004
- [8] 라우터 보안관리 가이드, KISA, 2003
- [9] Cisco 홈페이지, [www.cisco.com](http://www.cisco.com)