

IT 인프라 아키텍처 설계

# 네트워크 기초

## OSI L1~L7 + 장비·토폴로지

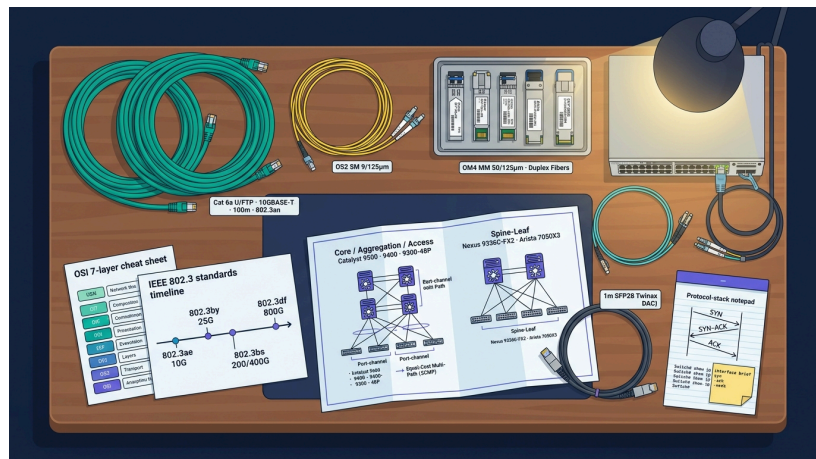
Session 4 · Day 1 — TA가 알아야 할 네트워크 전 계층 한 권

본문 108 슬라이드 · 강의 시간 약 150분 · TA(Technical Architect) 양성 과정

강사 박수현 ·  젠아이랩스(GenAI Labs)

데이터센터 · 서버·OS·DB·GPU · 가상화·컨테이너 · 네트워크 L1~L7 · 스토리지 · 백업·DR · 보안 6대 도메인 · HA · 용량·성능·관찰성 · 설계 워크숍 · RFP · 5종 실전 케이스

IT 인프라 아키텍처 설계 · Session 4 · 네트워크 기초 · OSI L1~L7 + 장비·토폴로지



Session 4 · Day 1 — TA가 알아야 할 네트워크 전 계층 한 권

## 세션 4 — 회차 메타데이터

### 📋 세션 정보

- **회차:** 4 / 15 — Day 1 · 네트워크 기초
- **소속:** Day 1 — IT 인프라 큰 그림 + 서버·NW 기초
- **카테고리:** is-technical (인프라 기초)
- **예상 분량:** 본문 108 슬라이드 + 이미지 18장
- **강의 시간:** 약 150분
- **강사:** 박수현 — 젠아이랩스(GenAI Labs) **CEO / CTO**

### 🎯 핵심 메시지

네트워크는 **7계층 · 100+ 프로토콜 · 수십 가지 장비**의 약속 집합. TA는 이 약속을 **다이어그램·표·결정 매트릭스**로 풀어낸다.

### 🎯 학습 목표 (Learning Objectives)

1. **OSI 7 / TCP/IP 4 계층** — 캡슐화·데이터 단위·장비 매핑
2. **L1 물리** — Cat 5e~8·SM/MM 광·SFP~OSFP 비교
3. **WiFi** — 802.11 a~be·2.4/5/6 GHz·WPA3·AP 설계
4. **L2** — Ethernet·MAC·ARP·STP·LACP·VLAN·L2 보안
5. **L3** — IP·CIDR·ICMP·라우팅(Static·OSPF·BGP·IS-IS)
6. **L4** — TCP/UDP/QUIC·3-Way·혼잡제어
7. **L5~L7** — DNS·DHCP·HTTP·TLS·SSH·SNMP·LDAP
8. **장비·토폴로지** — 3-Tier vs Spine-Leaf·ToR·OOB

## 강의 지도 — 세션 4 본문 10개 PART

### A. OSI / TCP/IP 모델

- 7 / 4 계층 + 매핑
- 캡슐화·디캡슐화
- 데이터 단위 (Frame·Packet·Segment)
- 계층별 장비 매핑

### B. L1 물리 계층

- Cat 5e~8 동선
- 광 SM/MM, 커넥터
- SFP~OSFP 모듈
- 거리·100G/400G/800G

### C. WiFi

- 802.11 a/b/g/n/ac/ax/be
- 2.4·5·6 GHz · 채널 폭
- MIMO·OFDMA·Beamforming
- WPA3·EAP·AP 배치

### D. L2 데이터링크

- Ethernet·MAC·ARP
- STP / RSTP / MSTP
- LACP·LLDP
- VLAN·L2 보안

### E. L3 네트워크

- IP·CIDR·VLSM·ICMP
- 라우팅 기본
- OSPF·BGP·IS-IS·EIGRP
- ECMP·PBR

### F. L4 전송

- TCP·UDP·SCTP·QUIC
- 3-Way / 4-Way
- 혼잡제어 (Reno·CUBIC·BBR)
- 포트 분류

### G. L5~L7 응용

- DNS·DHCP·NTP·LDAP
- HTTP/1.1·2·3·TLS
- SMTP/POP3/IMAP·FTP/SFTP·SSH·SNMP

### H. 장비 · I. 토폴로지 · J. 실전

- Hub~LB·WAF·FW
- 3-Tier vs Spine-Leaf
- 산출물·결정 10가지



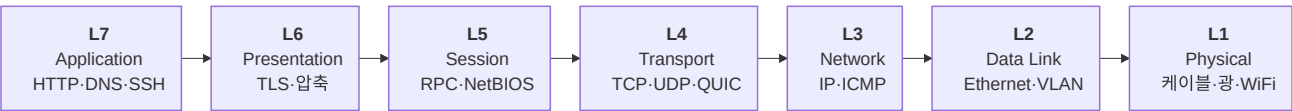
# PART A

## OSI 7 Layer + TCP/IP — 모든 네트워크의 공통 어휘

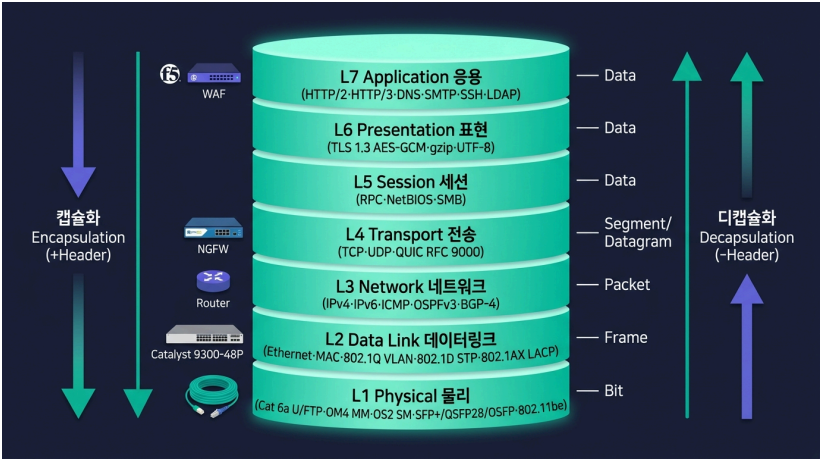
7개 계층의 약속이 모여 우리가 보는 모든 통신이 된다.

IT 인프라 아키텍처 설계 · Session 4 · 네트워크 기초 · OSI L1~L7 + 장비·토폴로지

## OSI 7 Layer — 7개 계층의 책임



**암기 트릭:** "All People Seem To Need Data Processing" (위→아래) — **Please Do Not Touch Steve's Pet Alligator** (아래→위).



OSI 7 Layer 스택 (상화)

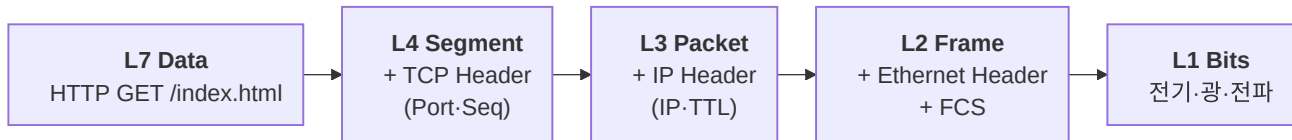
# TCP/IP 4 Layer — 실제 구현 모델

| TCP/IP 계층      | OSI 매핑   | 대표 프로토콜                                    | 대표 장비                    |
|----------------|----------|--------------------------------------------|--------------------------|
| Application    | L5+L6+L7 | HTTP-HTTPS-DNS-DHCP-SMTP-SSH-FTP-LDAP-SNMP | LB(L7)-WAF-Proxy         |
| Transport      | L4       | TCP-UDP-SCTP-QUIC                          | LB(L4)-Firewall          |
| Internet       | L3       | IP-ICMP-ARP*-OSPF-BGP                      | Router-L3 Switch         |
| Network Access | L1+L2    | Ethernet-WiFi-PPP-VLAN(802.1Q)-MAC         | L2 Switch-Hub-AP-케이블-SFP |

현장에서는 TCP/IP 4 계층이 실제 표준. OSI 7 계층은 개념·교육·트러블슈팅 용어. ARP는 L2와 L3의 경계.

IT 인프라 아키텍처 설계 · Session 4 · 네트워크 기초 · OSI L1~L7 + 장비·토폴로지

## 패킷 캡슐화 (Encapsulation) — 송신 시 위→아래



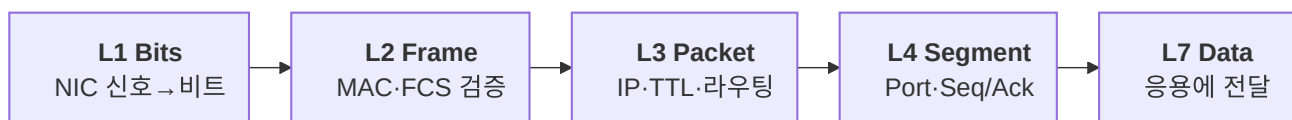
| 계층    | 추가되는 헤더                                   | 데이터 단위                         |
|-------|-------------------------------------------|--------------------------------|
| L7~L5 | Application 헤더                            | Data                           |
| L4    | TCP/UDP 헤더 (Src/Dst Port)                 | Segment (TCP) / Datagram (UDP) |
| L3    | IP 헤더 (Src/Dst IP·TTL·Protocol)           | Packet                         |
| L2    | Ethernet 헤더 (Src/Dst MAC·EtherType) + FCS | Frame                          |
| L1    | (헤더 없음)                                   | Bit (전기·광·전파)                  |

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

9 / 108

IT 인프라 아키텍처 설계 · Session 4 · 네트워크 기초 · OSI L1~L7 + 장비·토폴로지

## 디캡슐화 (Decapsulation) — 수신 시 아래→위



### 🔍 각 계층 검증

- **L2:** 목적지 MAC == 내 MAC? FCS 무결성?
- **L3:** TTL > 0? IP Header Checksum?
- **L4:** Port가 LISTEN 중인가? Seq 정상?
- **L7:** 응용이 받을 수 있는 형식?

### 🎤 TA의 관점

- 장애 발생 시 **Bottom-up**: 케이블 → Link → IP → Port → 응용 순서로 격리
- MTU 불일치 → **L3 Fragmentation** → 성능 폭락
- **L4 Reset(RST)** 폭주 → 응용/방화벽 의심
- **L7 Slow Response** → APM으로 절단점 추적

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

10 / 108

## 계층별 장비 매핑 — 어느 계층에서 일하는가

| OSI 계층 | 데이터 단위  | 주요 장비                                       | 핵심 결정                    |
|--------|---------|---------------------------------------------|--------------------------|
| L7     | Data    | WAF · L7 LB · API Gateway · Reverse Proxy   | URL/Header 라우팅·SSL Term  |
| L6     | Data    | TLS Offloader · HSM                         | 인증서·암호 스위트               |
| L5     | Data    | (특수)                                        | RPC·SMB 세션               |
| L4     | Segment | L4 LB · Firewall · NAT GW                   | 5-Tuple·Connection Track |
| L3     | Packet  | Router · L3 Switch · IPS · VPN GW           | 라우팅 테이블·ACL              |
| L2     | Frame   | L2 Switch · Bridge · Wireless AP            | MAC 테이블·VLAN             |
| L1     | Bit     | Hub · Repeater · Media Converter · 케이블·광 모듈 | 거리·속도·물리 표준              |

현장 단순화: L1 = 케이블/광, L2 = 스위치, L3 = 라우터, L4 = 방화벽/L4 LB, L7 = WAF/L7 LB. **장비 격리도 이 5개 축으로 나눠 본다.**

# PART B

## L1 물리 계층 — 케이블·광·SFP의 세계

물리 표준이 잘못되면 그 위의 모든 계층이 무너진다.

동선 표준 — Cat 5e · 6 · 6a · 7 · 8 비교

| 표준       | 최대 속도                         | 최대 거리      | 주파수      | 차폐               | 주 용도                   |
|----------|-------------------------------|------------|----------|------------------|------------------------|
| Cat 5e   | 1 Gbps                        | 100m       | 100 MHz  | UTP              | 일반 사무 (구식)             |
| Cat 6    | 1 Gbps (100m) / 10 Gbps (55m) | 100m / 55m | 250 MHz  | UTP/STP          | 표준 사무실                 |
| Cat 6a ★ | 10 Gbps                       | 100m       | 500 MHz  | F/UTP-STP        | 데이터센터 ToR 표준           |
| Cat 7    | 10 Gbps                       | 100m       | 600 MHz  | S/FTP (개별·전체 차폐) | 산업·고간섭 환경              |
| Cat 7a   | 10 Gbps                       | 100m       | 1000 MHz | S/FTP            | 특수 (드물게 사용)            |
| Cat 8    | 25/40 Gbps                    | 30m        | 2000 MHz | S/FTP            | 데이터센터 단거리 (Server↔ToR) |

현장 표준 결정: 사무 = Cat 6, 데이터센터 ToR = Cat 6a, 단거리 25/40G = Cat 8 또는 DAC, 25G 이상 장거리 = 광 (Fiber).

차폐 구조 — UTP · FTP · STP · S/FTP



차폐 종류

- UTP (Unshielded Twisted Pair) — 차폐 없음, 가장 저렴, 일반 사무
- FTP / F/UTP (Foiled) — 전체 외부 알루미늄 호일, 중간 가격
- STP / S/UTP (Shielded, 편조망) — 외부 편조망 차폐
- S/FTP / SF/FTP — 페어 개별 호일 + 외부 편조망 (최고 등급)



차폐 도입 시 부담

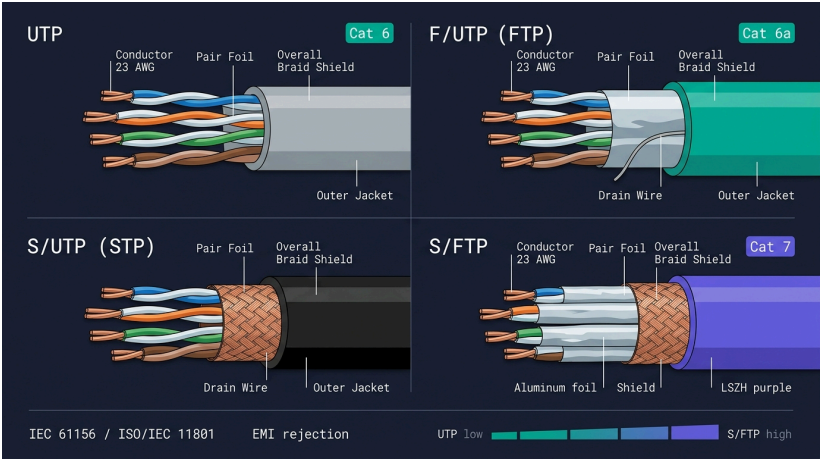
- 가격 1.5~3배 ↑
- 케이블 굵기 ↑ (Bend Radius 큼)
- 반드시 양 끝 접지 — 안 하면 오히려 안테나
- 굵어서 트레이 점유율 증가



TA의 선택 기준

| 환경               | 추천                 |
|------------------|--------------------|
| 일반 사무실           | UTP Cat 6          |
| 데이터센터 일반         | F/UTP Cat 6a       |
| 산업·공장·송전소 인근     | S/FTP Cat 6a/7     |
| 의료 영상·고감도 측정실    | S/FTP Cat 7        |
| 데이터센터 25/40G 단거리 | S/FTP Cat 8 또는 DAC |

현장 메모: 한국 공공 사업은 화재·차폐 등급 (CMP·CMR·LSZH) 도 함께 명시되는 경우가 많음.



차폐 구조 — UTP · FTP · STP · S/FTP

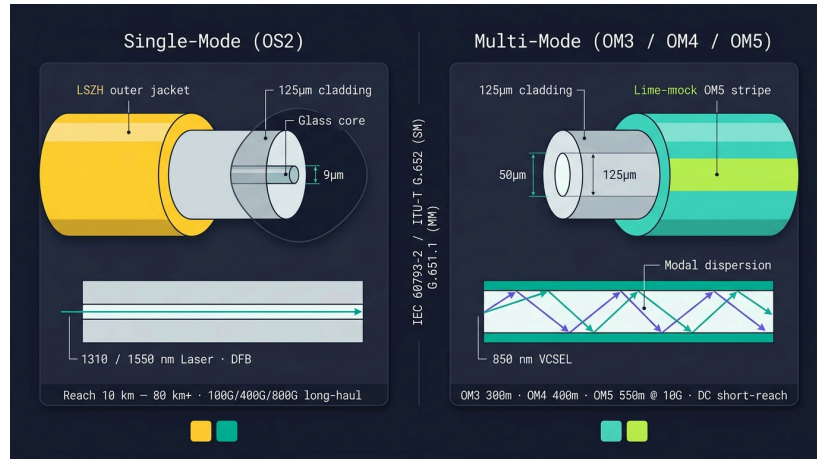
## 광 케이블 — Single-Mode vs Multi-Mode

| 구분       | Single-Mode (SM)     | Multi-Mode (MM)          |
|----------|----------------------|--------------------------|
| 코어 / 클래드 | 9 / 125 μm           | 50 / 125 μm (또는 62.5)    |
| 광원       | Laser (1310/1550 nm) | LED/VCSEL (850/1300 nm)  |
| 최대 거리    | 10 km ~ 80 km+       | 100m ~ 550m              |
| 대역폭·속도   | 100G/400G/800G 장거리   | 10G/40G/100G 단거리         |
| 케이블 색상   | 노란색                  | OM3 아쿠아·OM4 아쿠아·OM5 라임그린 |
| 단가       | 광원 비싸지만 케이블 저렴       | 광원 저렴, 케이블 약간 비쌈         |
| 용도       | DC 간·캠퍼스·WAN         | 데이터센터 내 단거리              |

## MM 등급 — OM1 · OM2 · OM3 · OM4 · OM5

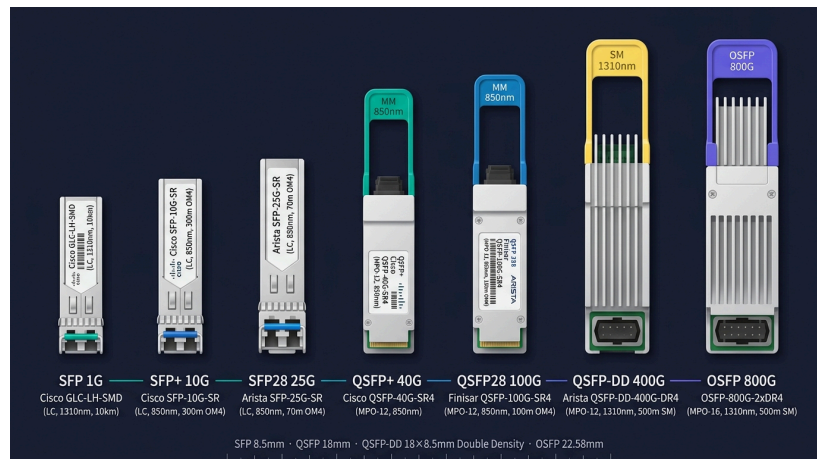
| 등급             | 색상         | 10G  | 40G  | 100G | 비고           |
|----------------|------------|------|------|------|--------------|
| OM1 (62.5/125) | Orange     | 33m  | —    | —    | 구식           |
| OM2 (50/125)   | Orange     | 82m  | —    | —    | 구식           |
| OM3            | Aqua       | 300m | 100m | 70m  | 표준           |
| OM4            | Aqua       | 400m | 150m | 100m | DC 표준        |
| OM5            | Lime Green | 550m | 440m | 150m | SWDM 지원 (신규) |

## IT 인프라 아키텍처 설계 · Session 4 · 네트워크 기초 · OSI L1~L7 + 장비·토폴로지



광 케이블 — Single-Mode vs Multi-Mode

## IT 인프라 아키텍처 설계 · Session 4 · 네트워크 기초 · OSI L1~L7 + 장비·토폴로지



광 모듈 라인업 (삼화)



광 모듈 — SFP · SFP+ · SFP28 · QSFP 계열 · OSFP

| 모듈      | 속도               | 포맷             | 커넥터         | 등장 시기 | 주 용도           |
|---------|------------------|----------------|-------------|-------|----------------|
| SFP     | 1 Gbps           | Small          | LC          | 2001  | 1G 액세스         |
| SFP+    | 10 Gbps          | Small          | LC          | 2009  | 현장 가장 흔함       |
| SFP28   | 25 Gbps          | Small          | LC          | 2014  | 서버 NIC ↔ ToR   |
| SFP56   | 50 Gbps          | Small          | LC          | 2018  | 신규·드물게         |
| QSFP+   | 40 Gbps (4×10G)  | Quad           | MPO 또는 LC×4 | 2010  | DC Aggregation |
| QSFP28  | 100 Gbps (4×25G) | Quad           | MPO 또는 LC   | 2015  | DC Spine 표준    |
| QSFP56  | 200 Gbps         | Quad           | MPO         | 2018  | 고밀도 DC         |
| QSFP-DD | 400 Gbps (8×50G) | Double Density | MPO-16      | 2019  | 차세대 Spine      |
| OSFP    | 800 Gbps         | Octal SFP      | MPO-16      | 2022  | AI/GPU 클러스터    |
| OSFP-XD | 1.6 Tbps         | XD             | MPO         | 2025+ | 초대형 AI         |

모듈 = NIC와 스위치의 약속. 같은 SFP+ 슬롯이라도 벤더 정품/호환 코드가 다르면 작동 안 함 — BOM에 벤더 PN(Part Number) 정확히 명시.

광 거리 표준 — SR · LR · ER · ZR

| 약자  | 풀네임            | 거리                     | 광 종류 | 파장       | 비고       |
|-----|----------------|------------------------|------|----------|----------|
| SR  | Short Reach    | 100m (OM4) / 70m (OM3) | MM   | 850 nm   | DC 내부 표준 |
| LR  | Long Reach     | 10 km                  | SM   | 1310 nm  | 캠퍼스·DC 간 |
| ER  | Extended Reach | 40 km                  | SM   | 1550 nm  | WAN      |
| ZR  | Z Reach        | 80 km                  | SM   | 1550 nm  | 광역 WAN   |
| ZR+ | 확장 ZR          | 120 km+                | SM   | Coherent | 차세대 광역   |

100G/400G 표준 (IEEE 802.3) 예시

| 표준           | 속도   | 매체            | 거리       |
|--------------|------|---------------|----------|
| 100GBASE-SR4 | 100G | MM (MPO)      | 100m     |
| 100GBASE-LR4 | 100G | SM (LC)       | 10km     |
| 100GBASE-ER4 | 100G | SM (LC)       | 40km     |
| 400GBASE-SR8 | 400G | MM (MPO-16)   | 100m     |
| 400GBASE-LR4 | 400G | SM (LC)       | 10km     |
| 400GBASE-ZR  | 400G | SM (Coherent) | 80~120km |

## 케이블 결정 매트릭스 — Cat 6a · Cat 8 · 광 SR·LR

| 시나리오               | 거리        | 속도        | 권고 매체                      | 이유          |
|--------------------|-----------|-----------|----------------------------|-------------|
| 사무실 ↔ 액세스 SW       | <100m     | 1G        | Cat 6                      | 가성비, 1G가 충분 |
| 사무실 ↔ 액세스 SW (신규)  | <100m     | 10G       | Cat 6a                     | 미래 대비       |
| 데이터센터 Server ↔ ToR | <3m       | 10/25G    | DAC (Direct Attach Copper) | 저전력·저지연·저비용 |
| Server ↔ ToR (랙 내) | <5m       | 25G       | Cat 8 또는 DAC               | 단거리 표준      |
| ToR ↔ Spine (랙 간)  | <100m     | 100G      | OM4 MPO + SR4              | 데이터센터 표준    |
| DC 동·충간            | 100m~10km | 100G      | SM LC + LR4                | 거리 확장       |
| DC ↔ DC (50km)     | 10~80km   | 100G      | SM + ER4                   | 캠퍼스         |
| WAN 광역 (서울↔부산)     | 80km+     | 100G/400G | SM + ZR 또는 통신사 회선          | 장거리         |
| AP ↔ 단말 (무선)       | 실내        | WiFi 6E/7 | 무선                         | 모빌리티        |

# PART C

## WiFi — 802.11 표준의 진화

무선은 유선의 보조가 아니라, 사무실·캠퍼스의 1차 액세스 매체다.

## 802.11 진화 — *a/b/g/n/ac/ax/be*

| 표준       | 브랜드            | 연도   | 주파수         | 최대 속도 (이론) | 채널 폭                 |
|----------|----------------|------|-------------|------------|----------------------|
| 802.11a  | (Wi-Fi 1/2 없음) | 1999 | 5 GHz       | 54 Mbps    | 20 MHz               |
| 802.11b  | (구식)           | 1999 | 2.4 GHz     | 11 Mbps    | 22 MHz               |
| 802.11g  | (구식)           | 2003 | 2.4 GHz     | 54 Mbps    | 20 MHz               |
| 802.11n  | Wi-Fi 4        | 2009 | 2.4 / 5 GHz | 600 Mbps   | 20/40 MHz            |
| 802.11ac | Wi-Fi 5        | 2014 | 5 GHz       | ~3.5 Gbps  | 20/40/80/160 MHz     |
| 802.11ax | Wi-Fi 6        | 2019 | 2.4 / 5 GHz | ~9.6 Gbps  | 20/40/80/160 MHz     |
| 802.11ax | Wi-Fi 6E       | 2021 | + 6 GHz     | ~9.6 Gbps  | 20~160 MHz           |
| 802.11be | Wi-Fi 7        | 2024 | 2.4/5/6 GHz | ~46 Gbps   | 320 MHz, 4K-QAM, MLO |

현재 기업 표준: 신규 = **Wi-Fi 6/6E**, 2026~ = **Wi-Fi 7**. 단말이 지원해야 의미 있음 (iPhone 16·Galaxy S24 부터 Wi-Fi 7).

## 주파수 대역 — *2.4 · 5 · 6 GHz 비교*

| 대역      | 채널 수        | 거리·관통성   | 간섭                  | 속도 | 비고         |
|---------|-------------|----------|---------------------|----|------------|
| 2.4 GHz | 3개 (1·6·11) | 멀리·잘 통과  | 심함 (BT·전자레인지·이웃 AP) | 낮음 | IoT·구식 단말  |
| 5 GHz   | 25개+        | 중간       | 중간 (DFS 채널 일부)      | 높음 | 사무·기업 표준   |
| 6 GHz ★ | 59개 (20MHz) | 짧음·관통 약함 | 거의 없음 (신규 대역)       | 최고 | Wi-Fi 6E/7 |

### 채널 폭 — 20·40·80·160·320 MHz

| 채널 폭    | 처리량 (이론) | 단점               |
|---------|----------|------------------|
| 20 MHz  | 기준       | 가장 안정, 좁음        |
| 40 MHz  | 2배       | 채널 절반 소모         |
| 80 MHz  | 4배       | 간섭 심해짐           |
| 160 MHz | 8배       | 5/6 GHz 만 가능     |
| 320 MHz | 16배      | 6 GHz Wi-Fi 7 전용 |



WiFi 주파수·채널 (삽화)

# WiFi 보안 — WEP · WPA · WPA2 · WPA3 + EAP

## 1. 암호 표준 4세대

| 표준     | 연도   | 암호               | 키 길이    | 취약점         | 현재 권고         |
|--------|------|------------------|---------|-------------|---------------|
| WEP    | 1997 | RC4              | 64/128  | 수분 내 해독     | 즉시 폐기         |
| WPA    | 2003 | TKIP             | 128     | 알려진 취약점     | 사용 금지         |
| WPA2   | 2004 | AES-CCMP         | 128     | KRACK(2017) | 폐지 시 가능, 권고 X |
| WPA3 ★ | 2018 | AES-GCMP-256-SAE | 128/192 | (현재 안전)     | 신규 표준         |

## 2. 인증 모드 — Personal vs Enterprise

| 모드                         | 키 방식                 | 적합        |
|----------------------------|----------------------|-----------|
| WPA2/3-Personal (PSK)      | 사전 공유 키 (Wi-Fi 비밀번호) | 가정·소규모    |
| WPA2/3-Enterprise (802.1X) | EAP + RADIUS         | 기업·캠퍼스 표준 |

## 3. EAP 방식 비교

| 방식        | 인증 요소              | 비고     |
|-----------|--------------------|--------|
| EAP-TLS   | 클라이언트·서버 인증서 양방향   | 가장 안전  |
| PEAP (MS) | 사용자명/비밀번호 + 서버 인증서 | 일반 기업  |
| EAP-TTLS  | PEAP 변형            | 유닉스 진영 |
| EAP-FAST  | Cisco PAC          | 레거시    |

# AP 배치 원칙 — 간격·간섭·채널 계획

 배치 원칙

- **AP 간 간격:** 10~15m (사무실), 6~10m (고밀도)
- **천장 중앙 설치** — 벽 부착보다 신호 균일
- **층간 간섭:** 위/아래층 AP와 채널 분리
- **AP 1대당 동시 단말** — Wi-Fi 6: 100~150, Wi-Fi 7: 200+
- **롤링 RF 측정** (사전 Site Survey)
- **PoE+/PoE++ 전원** — Wi-Fi 6/7은 30W+

 채널 계획

- 2.4 GHz: 1~6·11 만 사용 (Non-Overlap)
- 5 GHz: 자동 채널 할당 (DFS 제외)
- 6 GHz: 새 대역, 간섭 적음 → 자유롭게

 가정용 vs 엔터프라이즈

| 항목      | 가정용          | 엔터프라이즈                                                                              |
|---------|--------------|-------------------------------------------------------------------------------------|
| 가격      | 5~20만 원      | 80~300만 원/대                                                                         |
| 단말 수용   | ~50          | 200+                                                                                |
| 802.1X  | X            |  |
| Roaming | 단순           | 802.11k/v/r 표준                                                                      |
| 컨트롤러    | (없음)         | WLC 또는 Cloud Controller                                                             |
| 관리      | GUI          | SNMP-CLI-API-NMS                                                                    |
| 보안      | WPA2         | WPA2/3-Enterprise + RADIUS                                                          |
| 대표      | TP-Link/ASUS | Cisco · Aruba · Juniper Mist · Ruckus · 다산                                          |

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

27 / 108

#28

IT 인프라 아키텍처 설계 · Session 4 · 네트워크 기초 · OSI L1~L7 + 장비·토폴로지

AP 배치 원칙 — 간격·간섭·채널 계획

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

28 / 108

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

page 14 / 160

# PART D

## L2 데이터링크 — *Ethernet · MAC · ARP · STP · VLAN*

L2는 같은 브로드캐스트 도메인 안의 약속. 여기서 사고는 곧 폭풍이 된다.

IT 인프라 아키텍처 설계 · Session 4 · 네트워크 기초 · OSI L1~L7 + 장비·토폴로지

## Ethernet 프레임 구조 — 바이트 단위

|          |     |     |      |           |     |
|----------|-----|-----|------|-----------|-----|
| Preamble | Dst | Src | Type | Payload   | FCS |
| + SFD    | MAC | MAC |      |           |     |
| 8 B      | 6 B | 6 B | 2 B  | 46~1500 B | 4B  |

| 필드             | 크기        | 용도                                              |
|----------------|-----------|-------------------------------------------------|
| Preamble + SFD | 8 B       | 동기화 비트                                          |
| Dst MAC        | 6 B       | 목적지 MAC 주소                                      |
| Src MAC        | 6 B       | 발신 MAC 주소                                       |
| EtherType      | 2 B       | 상위 프로토콜 (0x0800=IPv4, 0x86DD=IPv6, 0x8100=VLAN) |
| Payload        | 46~1500 B | 실제 데이터 (기본 MTU 1500)                            |
| FCS (CRC32)    | 4 B       | 무결성 검사                                          |

MTU 1500 vs Jumbo Frame 9000 — 데이터센터 내부(스토리지·백업)는 Jumbo Frame 9000 으로 처리량 ↑. 단, 경로 전체가 동일 MTU 여야 함 (불일치 = 단편화).

MAC 주소 — 48bit + OUI

00:50:56:AB:CD:EF

OUI

NIC

24bit

24bit

|                |                    |
|----------------|--------------------|
| 비트 구조          |                    |
| 비트             | 용도                 |
| 48bit 전체       | MAC 주소 (16진수 12자리) |
| 상위 24bit = OUI | IEEE 할당 제조사 식별자    |
| 하위 24bit       | 제조사가 부여한 NIC 시리얼   |

|           |          |          |                     |
|-----------|----------|----------|---------------------|
| 대표 OUI 예시 |          |          |                     |
| OUI       | 제조사      | OUI      | 제조사                 |
| 00:50:56  | VMware   | 00:15:5D | Microsoft (Hyper-V) |
| 00:0C:29  | VMware   | F0:18:98 | Apple               |
| 52:54:00  | QEMU/KVM | 00:1B:21 | Intel               |
| 00:24:E8  | Dell     | B8:27:EB | Raspberry Pi        |

**MAC 특수 비트**

- I/G (8번째 비트)** — 0: 유니캐스트, 1: 멀티캐스트/브로드캐스트
- U/L (7번째 비트)** — 0: 글로벌(IEEE 할당), 1: 로컬 관리
- 브로드캐스트** = **FF:FF:FF:FF:FF:FF**

**TA의 활용**

- DHCP 예약** — MAC 기반
- L2 보안** — Port Security MAC 제한
- 자산 관리** — MAC ↔ 사용자/장비 매핑
- 장애편 분석** — OUI로 제조사 즉시 식별

L2 스위치 동작 — 학습 · 플러딩 · 포워딩

**1 Learning (학습)**

- 프레임 도착 시 **Src MAC + 수신 포트**를 MAC Table에 등록
- 기본 Aging Time = **300초**
- 학습 = 자동-하드웨어 (ASIC)

**2 Flooding (플러딩)**

- Dst MAC이 MAC Table에 **없으면** → 수신 포트 제외 **모든 포트**로 전송
- 브로드캐스트 (FF:FF...)도 동일
- 초기 통신 시 매번 발생

**3 Forwarding (포워딩)**

- Dst MAC이 MAC Table에 **있으면** → 해당 포트로만 전송
- ASIC 와이어 스피드 처리
- L2 통신의 정상 상태

충돌 도메인 vs 브로드캐스트 도메인

| 구분               | 정의           | 분할 장비                    |
|------------------|--------------|--------------------------|
| Collision Domain | 충돌 가능한 영역    | Switch 포트마다 분리 (Hub는 1개) |
| Broadcast Domain | 브로드캐스트 전파 영역 | VLAN 또는 L3 라우터로 분리       |

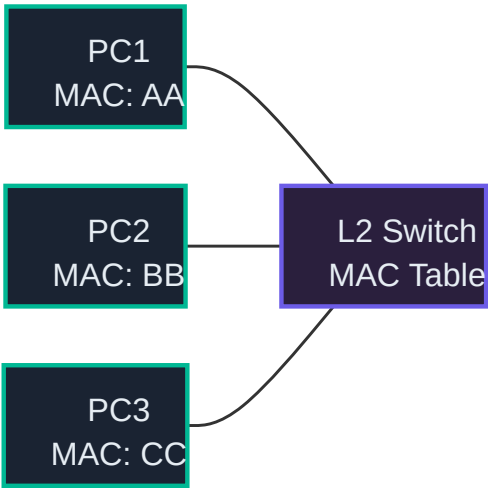
© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

32 / 108

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

page 16 / 160

L2 스위치 토폴로지 — *MAC Table* 학습 흐름



| MAC | 학습 포트  | Aging |
|-----|--------|-------|
| AA  | Port 1 | 300s  |
| BB  | Port 2 | 300s  |
| CC  | Port 3 | 300s  |

ARP 패밀리 — *ARP · RARP · GARP · Proxy ARP*

| 종류                    | 방향          | 용도                                |
|-----------------------|-------------|-----------------------------------|
| ARP                   | IP → MAC    | "이 IP의 MAC은?" — 브로드캐스트 질의         |
| RARP                  | MAC → IP    | 디스크리스 부팅 (거의 안 씀, BOOTP/DHCP로 대체) |
| GARP (Gratuitous ARP) | Self → Self | "나 이 IP-MAC 쓴다" — HA 절체-중복 IP 탐지  |
| Proxy ARP             | 라우터가 대리 응답  | 같은 서브넷처럼 통신 (구식·문제 소지)            |

ARP 동작 흐름

```
PC1 (10.0.0.1) → 브로드캐스트: "Who has 10.0.0.5?"
↓
PC2 (10.0.0.5) → 유니캐스트 응답: "I am 10.0.0.5, MAC=BB:..."
↓
PC1 ARP 캐시에 (10.0.0.5, BB:...) 저장 (TTL 약 4시간)
```

**보안 위협 — ARP Spoofing:** 공격자가 GARP 위조 발송 → 트래픽 중간 가로채기. 대응: **Dynamic ARP Inspection (DAI)** + DHCP Snooping 바인딩 테이블 + L3 ARP Inspection ACL.



# STP (Spanning Tree Protocol) — 802.1D · 루프 방지

 STP의 역할

- L2 토폴로지에 루프 = 브로드캐스트 스톰 (단 1~2초만에 NW 마비)
- STP가 자동으로 한 포트를 **Blocking** → 논리적 트리 형성
- 장애 시 Blocking 포트가 Forwarding으로 자동 전환

 BPDU (Bridge Protocol Data Unit)

- 스위치가끼리 매 2초마다 교환
- Root Bridge ID, Path Cost, Sender ID 등 포함

 Root Bridge 선출

- 가장 낮은 Bridge ID 가 Root
- Bridge ID = **Priority (2B)** + **MAC (6B)**
- 기본 Priority 32768 → 운영자가 Root로 만들 SW의 Priority 낮춤
- Root 선출은 자동, 운영자의 강제 지정 권장

 Path Cost

| 속도       | Cost (Long) |
|----------|-------------|
| 10 Mbps  | 2,000,000   |
| 100 Mbps | 200,000     |
| 1 Gbps   | 20,000      |
| 10 Gbps  | 2,000       |
| 100 Gbps | 200         |

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

35 / 108

# STP — Port Role · State · 수렴 시간

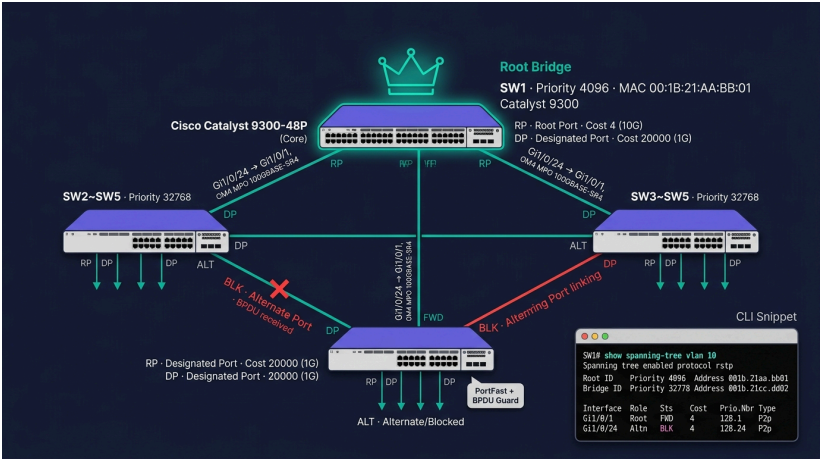
## Port Role (역할)

| 역할                       | 설명                             |
|--------------------------|--------------------------------|
| Root Port (RP)           | Root로 가는 최단 경로 포트 (스위치당 1개)    |
| Designated Port (DP)     | 한 세그먼트(케이블)당 1개의 Forwarding 포트 |
| Blocked / Non-Designated | 루프 방지를 위해 차단된 포트               |

## Port State (802.1D 기준 — 느낌)



802.1D STP 수렴 = 30~50초 → 사용자 입장에선 "끊김". 그래서 등장한 것이 RSTP·MSTP.



STP 토폴로지 (삽화)

# LACP (Link Aggregation) — 802.3ad

## LACP 개념

- 여러 물리 링크를 하나의 논리 링크로 묶음
- 대역폭 = 멤버 합 (4개 × 10G = 40G)
- 한 링크 장애 시 나머지로 계속 통신
- 로드밸런싱 알고리즘 — Src/Dst MAC/IP-Port 해시

## 모드

- Active** — LACP 패킷 능동 송신
- Passive** — 상대가 Active일 때만 응답
- On / Static** — LACP 없이 정적 묶음 (권고 X)

## LAG / Port-Channel / EtherChannel

| 벤더            | 명칭                           |
|---------------|------------------------------|
| 표준 (IEEE)     | LAG (Link Aggregation Group) |
| Cisco         | Port-Channel / EtherChannel  |
| Juniper       | AE (Aggregated Ethernet)     |
| Linux Bonding | mode=4 (802.3ad)             |

## TA의 결정

- Active-Active 대역 확장** 시 LACP 표준
- 다중 스위치 LACP** = MLAG / vPC / Stack (Cisco vPC-Arista MLAG-HPE IRF)
- 단일 SW LAG → 멀티세시 MLAG 로 진화

## VLAN — 802.1Q 태깅

일반 Ethernet 프레임 ·



### VLAN ID 범위

- 0 — 예약 (Priority 전용)
- 1 — 기본 VLAN (Native, 운영 권고 X)
- 2~1001 — 일반 사용
- 1002~1005 — Token Ring/FDDI (구식 예약)
- 1006~4094 — Extended VLAN
- 4095 — 예약
- 실용 = 약 4,000개



### PCP (Priority Code Point)

- 3bit = 0~7 우선순위
- L2 QoS (CoS)
- VoIP·영상은 보통 5~6



### Trunk vs Access Port

| 포트 종류       | 특징                                     |
|-------------|----------------------------------------|
| Access Port | 단일 VLAN, 태그 제거하고 단말에 전달                |
| Trunk Port  | 다중 VLAN, 태그 유지하고 다음 SW로 전달             |
| Native VLAN | Trunk 포트에서 태그 없이 전달되는 VLAN (기본 VLAN 1) |
| Voice VLAN  | IP 전화 전용 자동 할당 VLAN                    |



### 보안 위험

- VLAN Hopping — Double Tag로 우회 → 대응: Native VLAN을 사용 안 하는 ID로
- Trunk Auto-Negotiation — 비활성, 명시적 Trunk만

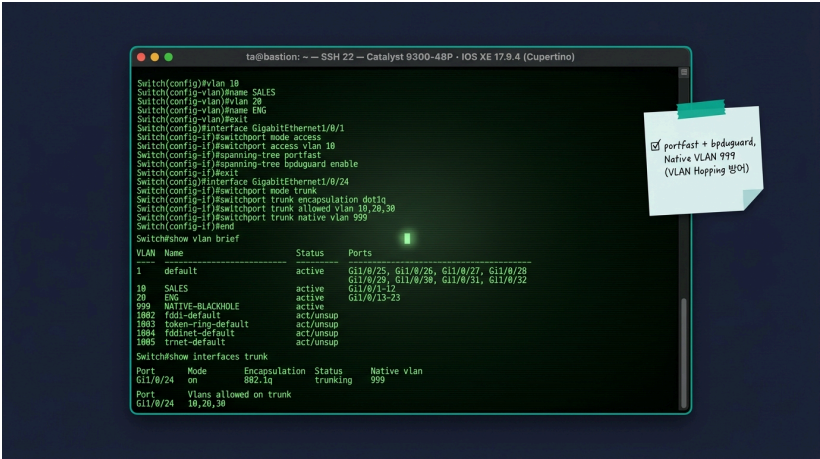
## Cisco IOS CLI — VLAN·Trunk 실제 명령

```
! — 액세스 SW: VLAN 10 (Sales) / VLAN 20 (Engineer) 생성 —
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name SALES
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name ENG
Switch(config-vlan)# exit
```

```
! — 단말 포트 (Gi1/0/1) 를 VLAN 10 액세스 포트로 —
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# spanning-tree portfast
Switch(config-if)# spanning-tree bpduguard enable
Switch(config-if)# exit
```

```
! — 업링크 (Gi1/0/24) Trunk + Native VLAN 999 —
Switch(config)# interface GigabitEthernet1/0/24
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport trunk allowed vlan 10,20,30
Switch(config-if)# switchport trunk native vlan 999
```

현장 팁: `spanning-tree portfast` + `bpduguard enable` 은 액세스 포트의 표준 세트, `switchport trunk native vlan 999` 로 Native VLAN 을 사용 안 하는 ID 로 옮겨 VLAN Hopping 방어.



Cisco IOS CLI — VLAN·Trunk 실제 명령

## L2 보안 — Port Security · DHCP Snooping · DAI



### Port Security

- 포트당 허용 MAC 수 제한 (보통 1~2)
- 위반 시 Shutdown / Restrict / Protect
- 무단 SW 연결 차단
- Sticky MAC = 자동 학습 후 저장



### DHCP Snooping

- 신뢰(Trusted) = 진짜 DHCP 서버 포트만
- 그 외 포트는 DHCP Server 응답 차단
- 악성 DHCP 공격 방어
- 바인딩 테이블 (MAC-IP-포트-VLAN) 생성



### Dynamic ARP Inspection (DAI)

- DHCP Snooping 바인딩 테이블 기반
- 위조 ARP 차단 → ARP Spoofing 방어
- MITM 방지



### IP Source Guard

- DHCP Snooping 바인딩과 다른 Src IP 차단
- IP Spoofing 방어



### Storm Control

- 브로드캐스트/멀티캐스트/유니캐스트 폭주 임계 초과 시 차단
- L2 폭풍 방어



### 802.1X (Port-Based Auth)

- 단말 인증 후 포트 개방
- RADIUS 서버 + EAP
- NAC의 기반



### Private VLAN

- 같은 VLAN 내 단말 간 격리
- Isolated-Community-Promiscuous
- 호스팅·DMZ에 유용



### MACsec (802.1AE)

- L2 암호화 (AES-GCM)
- 스위치 간 또는 호스트 ↔ SW 암호화
- 군·금융 일부 도입

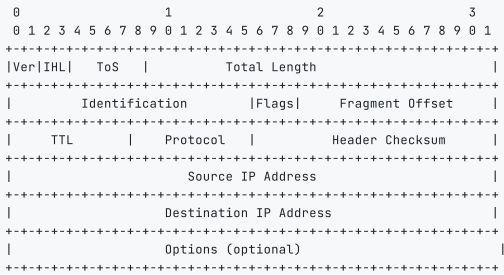
# PART E

## L3 네트워크 — IP · CIDR · 라우팅의 세계

L3는 다른 네트워크를 잇는 약속. TA의 가장 큰 설계 결정이 여기 모인다.

IT 인프라 아키텍처 설계 · Session 4 · 네트워크 기초 · OSI L1~L7 + 장비·토폴로지

## IPv4 패킷 헤더 — 20 bytes



| 필드           | 의미                                              |
|--------------|-------------------------------------------------|
| Version      | 4 또는 6                                          |
| TTL          | 라우터 통과 시 -1, 0이면 폐기 (Loop 방지)                   |
| Protocol     | 상위 프로토콜 (1=ICMP, 6=TCP, 17=UDP, 47=GRE, 50=ESP) |
| Src/Dst IP   | 발신·목적지 IP (각 4 bytes = 32bit)                   |
| Total Length | 최대 65535                                        |

# IPv4 — 클래스풀 → CIDR / VLSM

## 옛 클래스풀 (참고)

| 클래스 | 범위                          | 기본 마스크 | 호스트 수      |
|-----|-----------------------------|--------|------------|
| A   | 0.0.0.0 ~ 127.255.255.255   | /8     | 16,777,214 |
| B   | 128.0.0.0 ~ 191.255.255.255 | /16    | 65,534     |
| C   | 192.0.0.0 ~ 223.255.255.255 | /24    | 254        |
| D   | 224.0.0.0 ~ 239.255.255.255 | —      | 멀티캐스트      |
| E   | 240.0.0.0 ~ 255.255.255.255 | —      | 예약/실험      |

## 현재 = CIDR (Classless Inter-Domain Routing)

- 마스크를 /8 ~ /32 자유롭게 사용
- 예: 10.0.0.0/22 = 4개 /24 = 1024 IP

## VLSM (Variable Length Subnet Mask)

- 같은 큰 블록 안에서 서브넷마다 다른 크기
- 효율적 IP 분배 — /24·/26·/30 혼합 가능

# 사설 IP + 특수 주소 — RFC 1918 외

| 대역              | 표기                            | 호스트 수      | 용도        |
|-----------------|-------------------------------|------------|-----------|
| 10.0.0.0/8      | 10.0.0.0 ~ 10.255.255.255     | 16,777,216 | 대규모 사설    |
| 172.16.0.0/12   | 172.16.0.0 ~ 172.31.255.255   | 1,048,576  | 중규모 사설    |
| 192.168.0.0/16  | 192.168.0.0 ~ 192.168.255.255 | 65,536     | 소규모·가정    |
| 100.64.0.0/10   | CGNAT 전용                      | 4,194,304  | 통신사 CGNAT |
| 169.254.0.0/16  | Link-Local (APIPA)            | —          | DHCP 실패 시 |
| 127.0.0.0/8     | Loopback                      | —          | 자기 자신     |
| 224.0.0.0/4     | Multicast                     | —          | D 클래스     |
| 255.255.255.255 | Broadcast                     | —          | 한정 브로드캐스트 |

## 특수 주소 예시

| 주소              | 의미                     |
|-----------------|------------------------|
| 0.0.0.0         | Default Route, "모든 IP" |
| 127.0.0.1       | localhost              |
| 169.254.169.254 | (클라우드) 메타데이터 서비스       |
| 224.0.0.5       | OSPF AllSPFRouters     |
| 224.0.0.18      | VRRP                   |

# 서브넷 계산 — 분할 · 집약

## 표기 변환

| CIDR | 서브넷 마스크         | 호스트 (가용) | 예시               |
|------|-----------------|----------|------------------|
| /24  | 255.255.255.0   | 254      | 192.168.1.0/24   |
| /25  | 255.255.255.128 | 126      | /24 → 2개 분할      |
| /26  | 255.255.255.192 | 62       | /24 → 4개         |
| /27  | 255.255.255.224 | 30       | /24 → 8개         |
| /28  | 255.255.255.240 | 14       | DMZ 소규모          |
| /29  | 255.255.255.248 | 6        | P2P 링크           |
| /30  | 255.255.255.252 | 2        | <b>P2P 라우터 간</b> |
| /31  | 255.255.255.254 | 2        | P2P (RFC 3021)   |
| /32  | 255.255.255.255 | 1        | Loopback-VIP     |

## 분할 예시

```
10.0.0.0/22 (1024 IP) → 4개 /24
10.0.0.0/24
10.0.1.0/24
10.0.2.0/24
```

# 라우팅 기본 — Static vs Dynamic · 라우팅 테이블



## Static Routing

- 운영자가 수동으로 경로 입력
- 변경 없는 소규모·DMZ·Default Route
- 장점: 단순, 예측 가능, 보안적
- 단점: 확장성 X, 장애 시 수동 변경



## Dynamic Routing

- 라우터끼리 자동으로 경로 교환
- 대규모·다중 사이트
- 장점: 자동 우회, 확장
- 단점: 복잡, CPU 사용, 잘못된 설정 = 광역 사고



## Routing Table 구성

| Destination   | Next Hop   | Interface | Metric | Protocol         |
|---------------|------------|-----------|--------|------------------|
| 10.0.0.0/24   | Connected  | eth0      | 0      | Direct           |
| 10.0.1.0/24   | 10.0.0.254 | eth0      | 1      | Static           |
| 172.16.0.0/16 | 10.0.0.254 | eth0      | 110    | OSPF             |
| 0.0.0.0/0     | 10.0.0.254 | eth0      | 1      | Static (Default) |



## Longest Prefix Match

- 가장 긴 prefix(좁은 범위) 가 우선
- /24 가 /16 보다 우선
- Default 0.0.0.0/0 은 최후의 선택

## 라우팅 프로토콜 — *Distance Vector vs Link State*

| 분류              | 동작 원리                            | 대표           | 현장 위상               |
|-----------------|----------------------------------|--------------|---------------------|
| Distance Vector | 이웃에 자기 라우팅 테이블을 통째로 보냄, 홑 수 기반   | RIP          | 소규모·교육용 (운영 거의 안 함) |
| Link State ★    | 전체 토폴로지 DB 공유, SPF (Dijkstra) 계산 | OSPF · IS-IS | 사실상 IGP 표준          |

### IGP vs EGP

| 분류             | 범위               | 대표                           |
|----------------|------------------|------------------------------|
| IGP (Interior) | AS 내부 — 사내·캠퍼스   | OSPF · IS-IS (Link State 2종) |
| EGP (Exterior) | AS 간 — ISP 간 라우팅 | BGP-4 (Path Vector, 사실상 유일)  |

### Administrative Distance (Cisco 기준)

| 프로토콜      | AD  | 비고         |
|-----------|-----|------------|
| Connected | 0   | 직접 연결      |
| Static    | 1   | 수동         |
| eBGP      | 20  | AS 간 외부 광고 |
| OSPF      | 110 | IGP 1순위    |
| IS-IS     | 115 | ISP-통신사    |
| iBGP      | 200 | AS 내부 동기화  |

## OSPF — *Open Shortest Path First (RFC 2328)*



### OSPF 특징

- Link State 알고리즘
- 전체 토폴로지 DB 공유 → 각자 SPF (Dijkstra) 계산
- 빠른 수렴 (수초)
- VLSM·CIDR 완벽 지원
- 인증 (MD5-SHA)
- AS 내부 표준 (IGP)



### 패킷 종류

1. Hello — 이웃 발견·유지
2. DBD (DB Description) — DB 요약
3. LSR (Link State Request)
4. LSU (Link State Update) — LSA 운반
5. LSAck — ACK



### Area 구조

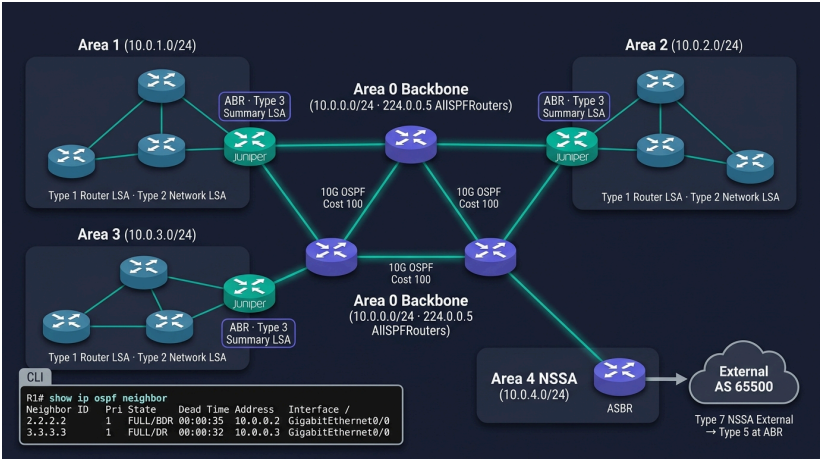
- Area 0 (Backbone) — 모든 Area 가 연결되어야 함
- Area 1, 2, ... — Non-Backbone
- ABR (Area Border Router) — Area 간 경계
- ASBR (Autonomous System Border Router) — 외부 AS 연결



### LSA Type

| Type | 이름            | 광고 범위     |
|------|---------------|-----------|
| 1    | Router LSA    | Area 내    |
| 2    | Network LSA   | Area 내    |
| 3    | Summary LSA   | Area 간    |
| 4    | ASBR Summary  | Area 간    |
| 5    | External LSA  | AS 전체     |
| 7    | NSSA External | NSSA Area |





OSPF Area 다이어그램 (삽화)

## OSPF·BGP 콘솔 — Cisco IOS 실제 명령

```
! ----- OSPF 설정 (Area 0 Backbone) -----
R1# configure terminal
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 10.0.0.0 0.0.0.255 area 0
R1(config-router)# network 10.0.1.0 0.0.0.255 area 0
R1(config-router)# passive-interface default
R1(config-router)# no passive-interface GigabitEthernet0/0
R1(config-router)# auto-cost reference-bandwidth 100000
R1(config-router)# exit

! 확인
R1# show ip ospf neighbor
R1# show ip ospf interface brief
R1# show ip route ospf

! ----- BGP 설정 (eBGP + iBGP) -----
R1(config)# router bgp 65001
R1(config-router)# bgp router-id 1.1.1.1
R1(config-router)# neighbor 1.1.1.2 remote-as 65002 ! eBGP (KT)
R1(config-router)# neighbor 1.1.1.2 description "KT-Edge"
R1(config-router)# neighbor 10.0.0.2 remote-as 65001 ! iBGP
R1(config-router)# neighbor 10.0.0.2 update-source Loopback0
R1(config-router)# address-family ipv4 unicast
R1(config-router-af)# network 203.0.113.0 mask 255.255.255.0
R1(config-router-af)# neighbor 1.1.1.2 route-map IN-FROM-KT in
```

**TA 팀:** **network** 구문은 OSPF에서 **광고 인터페이스** 선택 (Wildcard Mask), BGP에서 **광고할 prefix** 지정 (Subnet Mask). 두 문법이 의미가 다를 것을 주의.

```
ta@bastion → R1 — SSH 22 — Cisco ASR 9000 - IOS XR 7.10.2' (no vendor logo)

RP/0/RSP0/CPU0:R1(config-router)#
router ospf 1
router-id 1.1.1.1
network 10.0.0.0 0.0.0.255
area 0
passive-interface default
no passive-interface GigabitEthernet0/0/0
auto-cost reference-bandwidth 100000

BGP-4 + MP-BGP
router bgp 65001
bgp router-id 1.1.1.1
neighbor 1.1.1.2 remote-as 4766
description "KT-EDGE"
neighbor 10.0.0.2 remote-as 65001
update-source Loopback0
address-family ipv4 unicast
network 203.0.113.0/24
maximum-paths 4

R1# show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
2.2.2.2 1 FULL/BDR 00:00:35 10.0.0.2 Gi0/0/0

R1# show ip bgp summary
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
1.1.1.2 4 4766 1842 1851 47 0 0 02:14:01 Established 943125
10.0.0.2 4 65001 412 415 47 0 0 01:08:33 Established 27

R1# show ip route bgp
B* 0.0.0.0/0 [20/0] via 1.1.1.2 (eBGP)
```

OSPF-BGP 콘솔 — Cisco IOS 실제 명령

# BGP — Border Gateway Protocol (RFC 4271)



## BGP 정체

- 인터넷을 잇는 사실상 유일한 EGP
- **Path Vector** — 목적지까지의 **AS 경로 전체** 광고
- TCP 179 포트 사용 (UDP X)
- **신뢰성·정책 기반**
- 빠른 수렴 X, 안정성과 정책 우선



## AS (Autonomous System)

- 통일된 라우팅 정책 도메인
- AS 번호 16bit (~65535) / 32bit (확장)
- **사실 AS** = 64512~65534
- 예: KT=4766, SKT=9318, AWS=16509, Cloudflare=13335



## iBGP vs eBGP

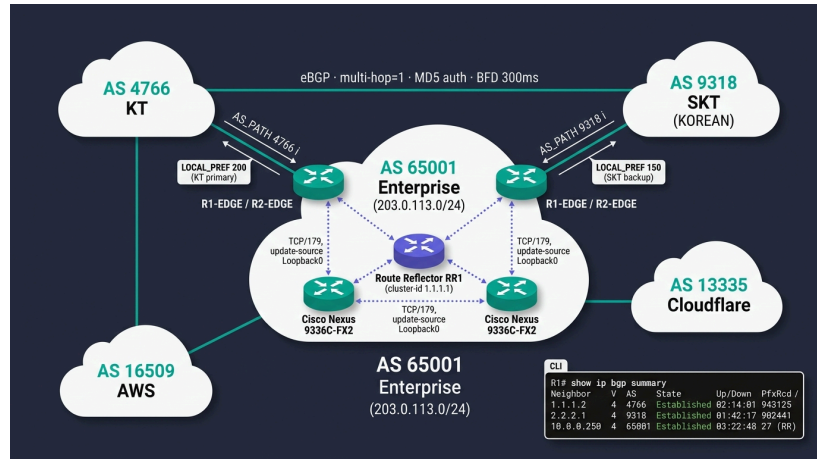
| 구분        | iBGP                  | eBGP      |
|-----------|-----------------------|-----------|
| 대상        | 같은 AS 내               | 다른 AS 간   |
| TTL       | 보통 multi-hop 사용       | 기본 1 (인접) |
| 광고 정책     | iBGP 받은 건 iBGP에 재광고 X | 자유        |
| Full Mesh | 필요 → Route Reflector  | —         |



## Route Reflector·Confederation

- **RR** — iBGP Full Mesh 회피, Reflector가 대신 광고
- **Confederation** — AS 내부를 작은 sub-AS로 분할

IT 인프라 아키텍처 설계 · Session 4 · 네트워크 기초 · OSI L1~L7 + 장비·토폴로지



BGP AS 토폴로지 (삽화)

IT 인프라 아키텍처 설계 · Session 4 · 네트워크 기초 · OSI L1~L7 + 장비·토폴로지

## ECMP · PBR — 경로 다중화·정책 라우팅

### ECMP (Equal-Cost Multi-Path)

- 동일 메트릭 경로 여러 개를 동시에 사용
- L3 로드밸런싱
- OSPF-BGP-EIGRP 모두 지원
- 해시 기반 — Src/Dst IP:Port (Per-Flow)
- Spine-Leaf의 핵심 (Leaf ↔ Spine 다중 경로)

### TA의 활용

- Active-Active 대역 확장
- 한 경로 장애 시 즉시 우회
- 64개 경로까지 일반적 (벤더별 상한 다름)

### PBR (Policy-Based Routing)

- 기본 라우팅 테이블을 무시하고 정책으로 경로 결정
- 기준: 출발지 IP·포트·DSCP·시간·VLAN 등
- 예: 백업 트래픽은 별도 화선으로

### ⚠ PBR 주의

- CPU 부하 ↑ (ASIC 지원 안 되면 느낌)
- 운영 복잡, 도면화 어려움

- 꼭 필요한 곳에만 적용

### 🚦 VRF·MPLS와의 연결

- L3 다중 테넌트 분리는 VRF·MPLS L3VPN 으로 확장 가능

# 라우팅 결정 매트릭스 — 언제 무엇을 쓸 것인가

| 규모·환경              | 권고 프로토콜                       | 이유                    |
|--------------------|-------------------------------|-----------------------|
| 지점 1~3개, 변경 없음     | Static                        | 단순·안정·예측 가능           |
| 단일 캠퍼스 (소규모)       | OSPF Single Area              | 자동 수렴·표준              |
| 다중 캠퍼스             | OSPF Multi-Area               | 확장성·요약·트래픽 격리         |
| Cisco 100% 환경 (중소) | EIGRP                         | 빠른 수렴·운영 편의           |
| ISP·통신사 백본         | IS-IS                         | 안정성·확장성               |
| 인터넷 연결·멀티홈         | BGP (eBGP)                    | 유일한 EGP               |
| DC 내부 (Spine-Leaf) | BGP (iBGP/eBGP unnumbered)    | Cumulus-SONIC·EVPN 표준 |
| 클라우드 VPC↔온프레미스     | BGP over IPSec/Direct Connect | 표준 연결                 |
| WAN 광역 (지점↔본사)     | MPLS L3VPN (BGP) 또는 SD-WAN    | 통신사 의존도에 따라           |

현장 메모: 데이터센터 내부 라우팅도 BGP 로 통일하는 흐름이 강해지고 있음 (RFC 7938 BGP in DC). EVPN-VXLAN의 컨트롤 플레인도 MP-BGP.

# PART F

## L4 전송 — TCP · UDP · QUIC

신뢰의 약속(TCP)과 속도의 선택(UDP), 그리고 차세대(QUIC).

## TCP · UDP — 두 가지 전송 약속

| 항목    | TCP                 | UDP                   |
|-------|---------------------|-----------------------|
| 연결    | Connection-Oriented | Connectionless        |
| 신뢰성   | 보장 (재전송·Ack)        | X                     |
| 순서 보장 | ○                   | X                     |
| 흐름 제어 | ○                   | X                     |
| 혼잡 제어 | ○                   | X                     |
| 헤더 크기 | 20 B+               | 8 B                   |
| 속도    | 느림                  | 빠름                    |
| 용도    | HTTP·SSH·DB·메일      | DNS·DHCP·VoIP·게임·스트리밍 |

현장 결정 기준: 데이터 손실이 치명적 = TCP, 일부 손실 허용·실시간 = UDP.

## TCP 3-Way Handshake — 연결 수립

### 📖 단계 설명

| # | 방향              | 플래그                             | 의미      |
|---|-----------------|---------------------------------|---------|
| 1 | Client → Server | <b>SYN</b> (Seq=x)              | "연결 요청" |
| 2 | Server → Client | <b>SYN+ACK</b> (Seq=y, Ack=x+1) | "수락"    |
| 3 | Client → Server | <b>ACK</b> (Seq=x+1, Ack=y+1)   | "시작"    |

3단계 완료 후 **ESTABLISHED** — 데이터 송수신 가능.

### ⚠️ SYN Flood 공격

- 1단계 SYN 만 대량 송신, 3단계 ACK 안 보냄
- 서버 백로그 큐 고갈로 정상 연결 거부
- 대응: SYN Cookies, Anti-DDoS, 방화벽 SYN Proxy

### 🔑 외움 포인트

- "악수 3번 = 연결 시작"
- Seq·Ack 번호는 +1씩 증가 (페이로드 없는 제어 패킷)

# TCP 3-Way Handshake — Sequence Diagram (시간 흐름)

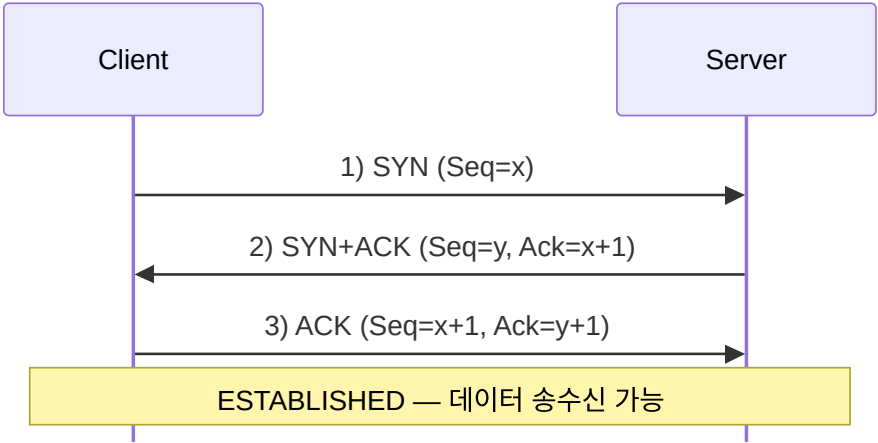
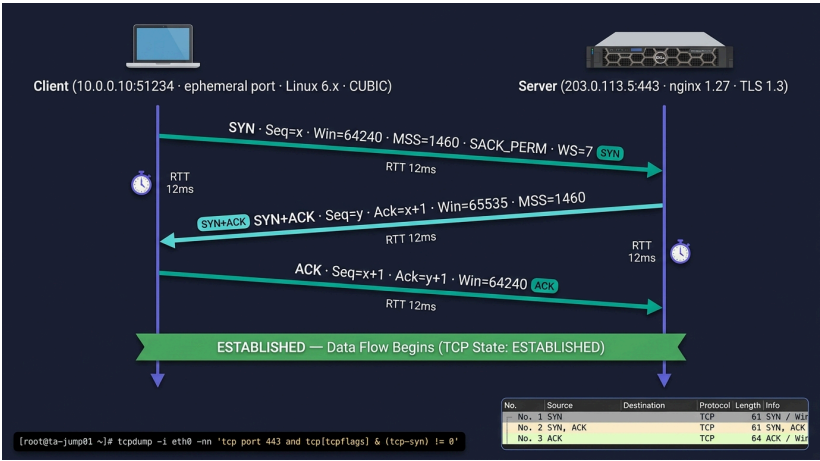
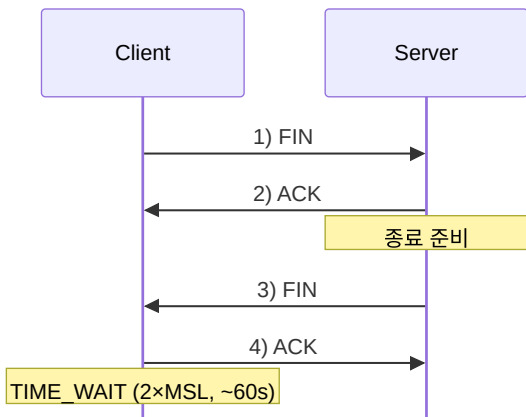


그림 읽는 법 — 위에서 아래로 시간이 흐른다. 화살표는 패킷 방향, 괄호 안은 Seq/Ack 번호. **3번째 ACK가 도착하는 순간** 양쪽이 동시에 ESTABLISHED 상태로 진입한다.



TCP 3-Way Handshake (삽화)

## TCP 4-Way Termination — 연결 종료



| 단계 | 동작                                 |
|----|------------------------------------|
| 1  | Client → <b>FIN</b> (종료 요청)        |
| 2  | Server → <b>ACK</b> (잘 받음, 처리 마저)  |
| 3  | Server → <b>FIN</b> (이제 나도 종료)     |
| 4  | Client → <b>ACK</b> + TIME_WAIT 대기 |

**TIME\_WAIT의 함정** — 짧은 연결을 대량 발생시키면 클라이언트 측 TIME\_WAIT가 쌓여 **포트 고갈** 발생. 대응: Connection Pool·Keep-Alive·`tcp_tw_reuse`.

## Sliding Window · Congestion Control



### Sliding Window

- 송신측이 **Ack 없이 보낼 수 있는 최대 바이트** = Window Size
- 수신측이 Ack에 다음 Window 크기 알림 → **Flow Control**
- BDP (Bandwidth-Delay Product) 기반 튜닝
- 큰 RTT × 큰 BW = 윈도우 키워야 처리량 ↑ ( `tcp_window_scaling` )



### Congestion Window (cwnd)

- 네트워크 혼잡에 따라 동적 조정
- 송신 가능 =  $\min(rwnd, cwnd)$



### 혼잡 제어 알고리즘

| 알고리즘         | 등장    | 동작                           |
|--------------|-------|------------------------------|
| Tahoe / Reno | 1988~ | Slow Start + AIMD            |
| NewReno      | 1996  | Fast Recovery 개선             |
| CUBIC        | 2008  | <b>Linux 기본</b> (3차 함수)      |
| BBR          | 2016  | Google 개발, <b>대역폭·RTT 기반</b> |
| BBRv3        | 2023  | YouTube·QUIC 표준              |



### TA의 활용

- 장거리·고대역 = BBR 권고
- 단거리 LAN = CUBIC 충분
- `sysctl net.ipv4.tcp_congestion_control`

## UDP — 비연결·저지연 표준

### 🎯 UDP 헤더 (8 bytes)

| [ | Src Port |  | Dst Port |  | Length |  | Checksum | ] |
|---|----------|--|----------|--|--------|--|----------|---|
|   | 2 B      |  | 2 B      |  | 2 B    |  | 2 B      |   |

### 📋 UDP 대표 용도

- **DNS** (53) — 짧은 질의·응답
- **DHCP** (67/68) — 부팅 시
- **NTP** (123) — 시간 동기화
- **SNMP** (161/162) — 모니터링
- **Syslog** (514) — 로그
- **RADIUS** (1812/1813)
- **VoIP / RTP** (실시간 음성·영상)
- 온라인 게임
- **VPN (IPSec ESP / WireGuard)**

### 🎤 TA의 운영 포인트

- DNS UDP 응답 > 512B = TCP fallback (DNSSEC·큰 응답)
- VoIP는 패킷 손실보다 **지터(Jitter)** 가 더 치명적 → QoS 최우선
- UDP Flood 공격 다수 → 방화벽 Rate Limit
- 일부 LB는 UDP를 잘 처리 못 함 (UDP 5-tuple 세션 분배)

### 🎮 QUIC = UDP 위의 신뢰성

- HTTP/3의 기반
- TCP의 신뢰성 + UDP의 자유
- 0-RTT 핸드셰이크
- 다음 슬라이드 참고

## QUIC — Quick UDP Internet Connections (RFC 9000)

### 🚀 QUIC 특징

- **UDP 위에서 동작** (포트 443)
- 자체적으로 신뢰성·재전송·암호화 (TLS 1.3 내장)
- **HTTP/3의 전송 계층**
- Google 개발 (2012) → IETF 표준 (2021)
- **0-RTT / 1-RTT 핸드셰이크** (TCP+TLS는 2~3 RTT)
- **HoL (Head-of-Line) Blocking 없음** — 스트림 독립
- 연결 마이그레이션 (Wi-Fi↔셀룰러 절체 시 연결 유지)

### 🎤 TA의 고려

- 방화벽이 **UDP 443 차단**하면 **HTTP/3 불가** → HTTP/2로 폴백
- L4 LB는 UDP 5-tuple 분배 잘 안 맞을 수 있음
- **CDN 표준 트래픽 점유율 30%+ (2026)**
- 운영자가 직접 만질 일은 적으나, 알아두면 트러블슈팅에 유리

### 🌐 차세대

- **HTTP/3 (RFC 9114)** = QUIC + HTTP 의미론
- **MASQUE** — QUIC 위의 프록시 (CONNECT-UDP)



포트 분류 — *Well-Known · Registered · Dynamic*

| 분류                  | 범위          | 용도                            |
|---------------------|-------------|-------------------------------|
| Well-Known          | 0~1023      | OS-root 권한 필요, 표준 서비스         |
| Registered          | 1024~49151  | IANA 등록 응용                    |
| Dynamic / Ephemeral | 49152~65535 | 클라이언트 임시 (Linux는 32768~60999) |

자주 보는 포트 (Well-Known + 운영)

| 포트      | 프로토콜    | 서비스                  |
|---------|---------|----------------------|
| 20/21   | TCP     | FTP (Data / Control) |
| 22      | TCP     | SSH                  |
| 23      | TCP     | Telnet (사용 금지)       |
| 25      | TCP     | SMTP                 |
| 53      | TCP/UDP | DNS                  |
| 67/68   | UDP     | DHCP (Server/Client) |
| 80      | TCP     | HTTP                 |
| 110     | TCP     | POP3                 |
| 123     | UDP     | NTP                  |
| 143     | TCP     | IMAP                 |
| 161/162 | UDP     | SNMP / SNMP Trap     |
| 389/636 | TCP     | LDAP / LDAPS         |

| 포트   | 프로토콜    | 서비스             |
|------|---------|-----------------|
| 443  | TCP/UDP | HTTPS / HTTP/3  |
| 445  | TCP     | SMB             |
| 514  | UDP     | Syslog          |
| 587  | TCP     | SMTP Submission |
| 993  | TCP     | IMAPS           |
| 1433 | TCP     | MS SQL          |
| 1521 | TCP     | Oracle DB       |
| 3306 | TCP     | MySQL           |
| 3389 | TCP     | RDP             |
| 5432 | TCP     | PostgreSQL      |
| 5900 | TCP     | VNC             |
| 8080 | TCP     | HTTP Alt        |

PART G

L5~L7 응용 프로토콜 — *DNS · HTTP · TLS · 그 외*

사용자가 직접 만나는 모든 서비스는 여기서 산다.

## DNS — Domain Name System (RFC 1034/1035)

### 🌳 DNS 계층

- Root (.) — 13개 글로벌 서버군
- TLD — .com · .kr · .org · .net · .gov ...
- 2LD — naver.com · google.co.kr
- Sub — mail.naver.com

### 🛡️ DNS 서버 역할

| 역할                 | 설명                                     |
|--------------------|----------------------------------------|
| Authoritative      | 특정 도메인의 정답 서버                          |
| Recursive Resolver | 사용자 대신 끝까지 질의 (보통 ISP 8.8.8.8-1.1.1.1) |
| Forwarder          | 사내 → 외부 DNS로 위임                        |
| Caching            | 응답 임시 저장 (TTL)                         |

### 📖 주요 레코드 타입

| Type  | 용도                                 |
|-------|------------------------------------|
| A     | 호스트명 → IPv4                        |
| AAAA  | 호스트명 → IPv6                        |
| CNAME | 별칭 (다른 이름으로 redirect)              |
| MX    | 메일 서버 (Priority)                   |
| TXT   | 임의 텍스트 (SPF·DKIM·도메인 인증)           |
| SRV   | 서비스 위치 (예: _ldap._tcp.example.com) |
| NS    | 권한 네임서버                            |
| PTR   | 역방향 (IP → 이름)                      |
| SOA   | Zone 메타 정보                         |
| CAA   | 발급 가능한 CA 제한                       |

### 🗣️ TA의 운영

- TTL 관리 (전환 직전 짧게 설정)
- 사내 / 외부 DNS 분리 (Split-Horizon)
- DNSSEC·DoH·DoT 도입 검토

## DHCP — Relay + Option (DORA 개요)

### 🔄 DORA 4단계 요약

| # | 단계       | 패킷                      |
|---|----------|-------------------------|
| 1 | Discover | 클라이언트 브로드캐스트 — "IP 줘"   |
| 2 | Offer    | 서버 → 클라이언트 — "이 IP 어때?" |
| 3 | Request  | 클라이언트 → 서버 — "그걸로 줘"    |
| 4 | ACK      | 서버 확정 + 옵션 전달           |

### 🔄 DHCP Relay

- 클라이언트는 브로드캐스트로 DHCP 검색
- 라우터는 브로드캐스트를 건너뛴다
- → DHCP Relay (IP Helper) 가 다른 서브넷의 DHCP 서버로 유니캐스트 전달
- L3 SW-라우터에 ip helper-address X.X.X.X

### 📦 DHCP Options

| Option | 용도                     |
|--------|------------------------|
| 3      | Default Gateway        |
| 6      | DNS Server             |
| 15     | Domain Name            |
| 42     | NTP Server             |
| 43     | 벤더 옵션 (AP·IP폰 컨트롤러 IP) |
| 60     | 벤더 클래스 식별              |
| 66/67  | PXE 부팅 서버·파일           |
| 82     | Relay Agent 정보 (위치·포트) |

### ⚠️ 보안

- DHCP Snooping 으로 악성 DHCP 차단
- IP Source Guard 결합

DHCP DORA — 시간 흐름



그림 읽는 법 — Discover-Request는 **브로드캐스트**(클라이언트 IP 미보유 단계), Offer-ACK는 **유니캐스트**. 4번째 ACK 수신 즉시 클라이언트는 받은 IP·게이트웨이·DNS·기타 Option(43·82 등)을 적용한다.

HTTP — 1.1 · 2 · 3 진화

| 항목           | HTTP/1.1           | HTTP/2         | HTTP/3          |
|--------------|--------------------|----------------|-----------------|
| 연도           | 1997               | 2015           | 2022            |
| 전송 계층        | TCP                | TCP + TLS      | UDP (QUIC)      |
| 다중화          | X (Pipelining 불완전) | 🔴 (Stream)     | 🔴 (Stream)      |
| 헤더 압축        | X                  | HPACK          | QPACK           |
| HoL Blocking | 있음                 | TCP 레벨에 있음     | 없음              |
| 암호화          | 옵션                 | 사실상 필수 (HTTPS) | 필수 (TLS 1.3 내장) |
| Server Push  | X                  | 🔴 (사실상 사용 X)   | (HTTP/3 X)      |
| 포트           | 80 / 443           | 443            | 443 (UDP)       |



HTTP/2 핵심

- 바이너리 프로토콜
- Stream 다중화 (한 TCP 연결에 여러 요청)
- 헤더 압축으로 모바일 성능 ↑



HTTP/3 핵심

- QUIC 기반 → **0-RTT 재연결**
- 모바일 환경 절체에 강함
- 방화벽 UDP 443 차단 주의

# HTTPS / TLS — 1.2 vs 1.3 핸드셰이크

## TLS 1.2 — 2-RTT 핸드셰이크

| 순서 | 방향              | 메시지                                        | 내용            |
|----|-----------------|--------------------------------------------|---------------|
| 1  | Client → Server | ClientHello                                | 지원 암호 스위트 랜덤  |
| 2  | Server → Client | ServerHello + 인증서 + Key Exchange           | 선택 암호·서버 공개키  |
| 3  | Client → Server | Key Exchange + ChangeCipherSpec + Finished | 프리마스터 키 암호 전환 |
| 4  | Server → Client | ChangeCipherSpec + Finished                | 암호 전환 확인      |
| ✓  | C ↔ S           | Encrypted Application Data                 | 본 통신 시작       |



### TLS 1.3 (RFC 8446)

- **1-RTT 핸드셰이크** (TLS 1.2의 절반)
- **0-RTT 재연결 가능** (PSK)
- 구식 약한 암호 제거 (RC4-SHA1-CBC)
- **AEAD 암호 스위트만**: AES-GCM, ChaCha20-Poly1305
- Perfect Forward Secrecy 필수



### TLS 운영 함정

- 인증서 **만료 알람** — Let's Encrypt 90일·EV 1년
- **약한 암호 비활성** — TLS 1.0/1.1 폐기 (2020+)
- 와일드카드 vs SAN 인증서
- HSTS-HPKP-CT (Certificate Transparency)
- TLS Offload — LB가 복호화, 내부는 평문 (관계 편의 vs 보안)

# 이메일 — SMTP · POP3 · IMAP



### SMTP (송신)

- **포트 25** — Server ↔ Server
- **포트 587** — Submission (Client → Server, AUTH 필수)
- **포트 465** — SMTPS (TLS implicit)
- 인증 암호화: STARTTLS



### 메일 보안 3종

- **SPF** — 허용 발신 IP 목록 (TXT 레코드)
- **DKIM** — 발신 도메인의 디지털 서명
- **DMARC** — SPF/DKIM 실패 시 처리 정책



### POP3 (수신 — 다운로드)

- **포트 110** (TLS = 995)
- 서버에서 다운로드 후 보통 삭제
- 단일 1대 기준 (모바일 시대에 부적합)
- 단순·가벼움



### IMAP (수신 — 서버 보관)

- **포트 143** (TLS = 993)
- 서버에 그대로 보관 → 다중 단말 동기화
- 폴다-플래그 서버 관리
- **현재 표준** (Gmail-M365-Yahoo)



### TA의 결정

- 사내 메일 = M365-Google Workspace-HCL Domino-메일 플러그
- 수신 = IMAPS-POP3S, 송신 = SMTP Submission
- DMARC 정책 (none → quarantine → reject)

파일 전송 — *FTP · SFTP · FTPS · NFS · SMB*

| 프로토콜                | 포트            | 보안            | 특징                            |
|---------------------|---------------|---------------|-------------------------------|
| FTP                 | 20/21         | 평문            | 구식, 보안 위협                     |
| FTPS                | 21-990        | TLS           | FTP + TLS (Explicit/Implicit) |
| SFTP                | 22 (SSH)      | SSH           | FTP 대체 표준                     |
| TFTP                | 69 (UDP)      | 없음            | 부팅-이미지 전송                     |
| SCP                 | 22 (SSH)      | SSH           | 단순 복사                         |
| rsync               | 873 / SSH     | SSH           | 증분 동기화                        |
| NFS v3/v4/v4.1/pNFS | 2049          | Kerberos 옵션   | Linux 파일 공유 표준                |
| SMB / CIFS          | 445           | NTLM/Kerberos | Windows 파일 공유 표준              |
| WebDAV              | 80/443 (HTTP) | TLS           | 웹 기반                          |
| S3 API              | 443 (HTTP)    | TLS           | 오브젝트 스토리지 표준                  |

현장 표준: 운영자 작업 = **SFTP**, Linux 파일 공유 = **NFS**, Windows 파일 공유 = **SMB**, 오브젝트 = **S3 API**.

SSH — *Secure Shell (RFC 4251)*

🔑 SSH 동작

- 포트 22
- 키 교환 (Diffie-Hellman) + 호스트 인증 + 사용자 인증
- 채널 다중화 (한 연결에 여러 세션)
- 흐름: TCP 연결 → 키 교환 → 인증 → 채널

🔒 인증 방식

- **Password** — 약함, brute force 위험
- **PubKey (Key-Based)** — 표준
- **Certificate-Based** — Bastion / CA 서명 키
- **MFA (2FA)** — Google Authenticator·FIDO2

🏠 포트 포워딩

- **Local Forward (-L)** — 클라 포트 → 원격 서비스
- **Remote Forward (-R)** — 원격 포트 → 클라 서비스
- **Dynamic (-D)** — SOCKS5 프록시
- 운영자가 **Bastion** → 내부 자원 접근 시 표준

🎤 TA의 표준

- root 직접 로그인 금지
- 키 기반만 허용 ( `PasswordAuthentication no` )
- Bastion-점프 호스트 도입
- 세션 기록 (Teleport·Strongdm·차체 PAM)

운영 프로토콜 — *SNMP · NTP · Syslog · LDAP*

 **SNMP**

| 버전  | 보안                    | 비고     |
|-----|-----------------------|--------|
| v1  | Community String (평문) | 폐기     |
| v2c | Community String      | 여전히 혼용 |
| v3  | 인증 + 암호화 (USM)        | 권고     |

- 포트 161 (Get/Set) · 162 (Trap)
- MIB·OID 트리 구조
- NMS (Zabbix·PRTG·SolarWinds) 의 기본

 **NTP (Network Time Protocol)**

- 포트 123 (UDP)
- Stratum 0 (원자시계) → 1 → 2 → ...
- 모든 보안·감사 로그의 전제
- chrony / ntpd

 **Syslog**

- 포트 514 (UDP) / 6514 (TLS)
- Facility (kern·auth·mail·local0~7)
- Severity (0 Emergency ~ 7 Debug)
- SIEM 입력의 기본 형식
- rsyslog·syslog-ng

 **LDAP / AD**

- 포트 389 (LDAP) / 636 (LDAPS)
- 디렉터리 서비스 — 사용자·그룹·자산
- Active Directory = LDAP + Kerberos + DNS + GPO
- 사내 인증 통합의 표준
- 응용 SSO·이메일·VPN·SSH 인증의 백엔드

PART H

네트워크 장비 — *Hub부터 WAF까지*

계층별로 살펴본 장비들을 한 번에 정리.

# L1·L2 장비 — Hub · Bridge · L2 Switch

 Hub (L1)

- 단순 전기 신호 증폭·재전송
- 모든 포트 플러딩 = 공유 매체
- 충돌 도메인 1개
- 현재는 박물관 — 사용 X

 Repeater (L1)

- 신호 재생·증폭
- 동선·광 거리 연장
- Media Converter = 동선↔광 변환

 Bridge (L2)

- 초기 L2 분할 장비
- 충돌 도메인 분리
- 현대엔 Switch에 흡수됨

 L2 Switch

- 포트마다 충돌 도메인 분리
- MAC 학습/플러딩/포워딩
- VLAN-STP-LACP 지원
- 종류:
  - Unmanaged — 가장 소규모, 설정 불가
  - Managed — 기업용, VLAN-STP 등 모두 가능
  - Smart / Lite-Managed — 중간

 Stackable Switch

- 여러 대를 하나의 논리 SW로
- 통합 관리-LACP 가능
- Cisco StackWise, Aruba Stack, HPE IRF

 Modular / Chassis SW

- 라인카드·SF-전원 모듈러
- 데이터센터 코어급
- Cisco Nexus 9500-Catalyst 9600, Juniper QFX-EX, Arista 7500

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

79 / 108

#80

IT 인프라 아키텍처 설계 · Session 4 · 네트워크 기초 · OSI L1~L7 + 장비·토폴로지

L2 Switch · HPE Aruba 6300M  
(1RU 48×1G + 4×SFP+)

“Switch# show mac address-table”

| Vlan | Mac Address    | Type    | Ports            |
|------|----------------|---------|------------------|
| 10   | 0050.56aa.bb01 | DYNAMIC | Gi1/0/1 (VMware) |
| 10   | 0050.56aa.bb02 | DYNAMIC | Gi1/0/2          |
| 20   | f018.99cc.dd03 | DYNAMIC | Gi1/0/3 (Apple)  |



ASIC wire-speed · MAC-table aging 300s · 802.1Q VLAN

L3 Switch / Router · Cisco Nexus 9336C-FX2  
(1RU 36×100G QSFP28)

“Switch# show ip route”

```
O 10.0.1.0/24 [110/2] via 10.0.0.1, 00:32:11, Vlan10
B 0.0.0.0/0 [20/0] via 1.1.1.2, 04:11:54 (eBGP AS 4766)
C 10.0.0.0/24 is directly connected, Vlan100
S 192.168.1.0/24 [1/0] via 10.0.0.254
```



ASIC wire-speed routing · OSPF/BGP/VRF · ACL

L2 = MAC 기반 포워딩 (Frame · 같은 브로드캐스트 도메인) / L3 = IP 기반 라우팅 (Packet · 서브넷 간 + AS 간 BGP)

L2 vs L3 스위치 (삽화)

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

80 / 108

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

page 40 / 160

## L3 Switch vs Router — 언제 무엇을 쓸 것인가

| 항목           | L3 Switch                             | Router                        |
|--------------|---------------------------------------|-------------------------------|
| 주 용도         | LAN 내부 VLAN 간 라우팅                     | LAN↔WAN, AS↔AS                |
| 포트 종류        | 대부분 Ethernet (Cu/Fiber)               | Ethernet + Serial + WAN 인터페이스 |
| 포트 밀도        | 24~96+ 포트                             | 보통 4~16 포트                    |
| 하드웨어 ASIC    | 라우팅도 ASIC → 와이어 스피드                   | CPU 또는 NPU 처리 (느릴 수 있음)       |
| 기능 깊이        | 기본 OSPF/BGP 정책                        | 풍부: NAT-VPN-MPLS-QoS-BGP 정책   |
| NAT-VPN-MPLS | 제한적                                   | 표준                            |
| 단가           | 상대적으로 저렴                              | 비쌈                            |
| 예시           | Cisco Catalyst 9300-9500, Arista 7050 | Cisco ASR-ISR, Juniper MX-SRX |

현장 결정: LAN/DC 내부 라우팅 = **L3 Switch**, WAN/Edge/복잡한 NAT-VPN = **Router**. 두 역할이 점차 겹치는 추세 (Universal Routers).

## 보안 장비 — FW · NGFW · WAF · IPS · VPN · Anti-DDoS



### Firewall · NGFW · UTM

| 종류           | 동작                                 |
|--------------|------------------------------------|
| Stateless FW | 패킷 단위, 세션 인식 X (구식)                |
| Stateful FW  | 세션 추적, 표준                          |
| NGFW         | 응용 인식 (App-ID)·IPS·URL 필터링         |
| UTM          | FW + AV + IPS + URL + Mail 통합 (중소) |



### WAF (Web App Firewall)

- HTTP 페이로드 검사
- OWASP Top 10 대응 (SQLi-XSS-CSRF)
- 시그니처 + 행위 분석
- F5 ASM-Imperva-Cloudflare-Akamai-Wapples (국산)



### IPS / IDS

- IPS = 인라인 차단
- IDS = 미러링 탐지만
- 시그니처·이상행위·머신러닝
- McAfee-Trellix-SecureSky (국산: 펜타시큐리티·시큐브)



### VPN Gateway

- IPSec (Site-to-Site-Client)
- SSL VPN (Pulse-Cisco AnyConnect-Fortinet-Penta-VPN)
- WireGuard-OpenVPN (오픈소스)



### Anti-DDoS

- L3/L4 볼륨 + L7 응용 공격 방어
- Arbor (NETSCOUT)·Radware-Cloudflare-Akamai



# LB / ADC — L4 vs L7 한 줄, 본문은 Session 5

LB = L4(5-Tuple로 IP/Port 분배) · L7(URL/Cookie/Header 분배), ADC = LB + SSL 중단 + WAF + Caching. 보안 장비(WAF·NGFW) 바로 옆 — 트래픽의 마지막 분기점이다.

 본문은 Session 5 PART F · G 로 이동 — 본 회차는 L1~L7 여휘 정리가 목표라 LB는 위치만 표시. 다음 항목은 모두 Session 5 로드 밸런싱 Part 에서 전개:

- L4 vs L7 결정 트리 · SSL Termination·Bridging·Passthrough — [s5 ## L4 vs L7](#)
- 분배 알고리즘 8종 (RR·WRR·Least Conn·IP/URL Hash ...) — [s5 ## L4 LB 알고리즘](#)
- 헬스 체크 Active/Passive · [/health](#) 설계 — [s5 ## 헬스 체크](#)
- Session Persistence (Cookie Insert·Source IP ...) — [s5 ## Session Persistence](#)
- 솔루션 카탈로그 F5·Citrix·A10·HAProxy·NGINX·KEMP·Radware·K8s Ingress — [s5 ## LB 솔루션 비교](#)
- GSLB 사이트 간 분산·DR Failover — [s5 ## GSLB](#)

# PART I

## 토폴로지 — Star · Mesh · 3-Tier · Spine-Leaf

토폴로지는 곧 가용성·확장성·비용을 결정한다.

# 기본 토폴로지 — Bus · Ring · Star · Mesh · Tree · Hybrid

 **Bus**

- 단일 케이블에 모든 노드
- 1980s 이더넷 초기
- **현재 사용 X**
- 단일 장애 = 전체 마비

 **Star**

- 중앙 허브 스위치
- **LAN의 표준**
- 단순·관리 용이
- 중앙 SW 장애 = 전체 마비 → 이중화

 **Tree**

- 계층적 (Star x 다중)
- 3-Tier 의 기반
- 캠퍼스 표준

 **Ring**

- 노드를 원형으로 연결
- Token Ring-FDDI-SONET
- **레거시·통신사 백본 잔존**
- 자동 우회 (Dual Ring)

 **Mesh**

- **Full Mesh** = 모든 노드 직접
- **Partial Mesh** = 핵심 노드만
- WAN-캐리어·고가용
- $N(N-1)/2$  회선 = 비싸짐

 **Hybrid**

- 여러 토폴로지 조합
- 현실의 거의 모든 NW
- 코어 = Mesh, 액세스 = Star

# 기본 토폴로지 6종 — 형태 비교

### 3-Tier 아키텍처 — Core · Aggregation · Access

**Core**

- 백본 라우팅
- 초고속·이중화
- 단일 도메인 통합

**Aggregation**

- VLAN 종단·L3 경계
- 정책 적용 (ACL·QoS)
- L2/L3 경계



**Access**

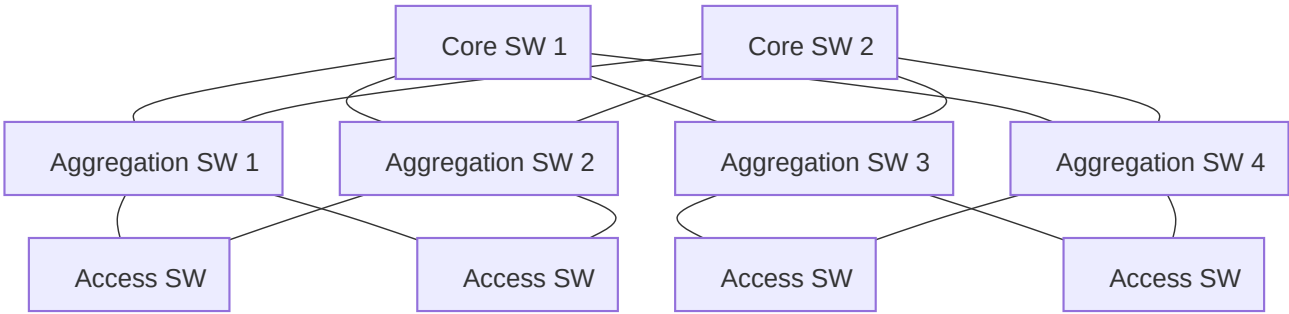
- 사용자·서버 직결
- PoE·VoIP 지원
- VLAN 할당

#### 3-Tier 사용 위상

- 현장 표준:** 캠퍼스 LAN·엔터프라이즈 빌딩 (사용자 → 액세스 → 어그리게이션 → 코어)
- 트래픽 패턴:** North-South 중심 (사용자 ↔ 서버·인터넷)
- 한계:** 데이터센터 East-West 트래픽 폭증 → Spine-Leaf로 대체

### 3-Tier 아키텍처 — Tier 배치 일러스트

### 3-Tier 토폴로지 — Core · Aggregation · Access 연결 도식



### Spine-Leaf (Clos) — 현대 데이터센터 표준

#### 🎯 핵심 특성

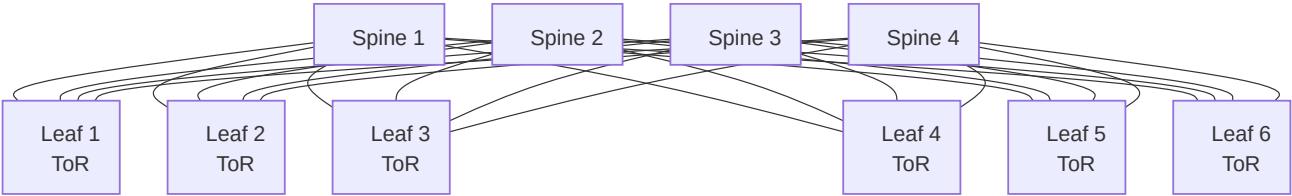
- 모든 Leaf가 모든 Spine과 연결 (Full Mesh)
- 동등 비용 경로 (ECMP)
- East-West 트래픽 최적화 (서버 ↔ 서버)
- 스케일 아웃 — Spine-Leaf 추가만으로 확장
- STP 없음 → BGP-EVPN-VXLAN 사용

#### 🎤 TA의 운영

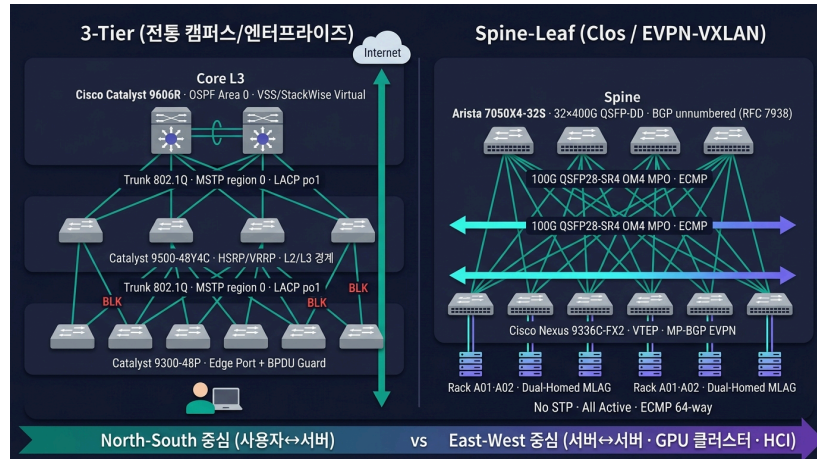
- Underlay = BGP unnumbered (RFC 7938)
- Overlay = VXLAN-EVPN (테넌트 격리)
- Spine은 라우팅만, Leaf가 액세스
- 50% 트래픽이 East-West인 현대 DC에 최적

# Spine-Leaf (Clos) — Full Mesh 패브릭 일러스트

# Spine-Leaf 토폴로지 — Full Mesh 연결 도식



IT 인프라 아키텍처 설계 · Session 4 · 네트워크 기초 · OSI L1~L7 + 장비·토폴로지



3-Tier vs Spine-Leaf (삽화)

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

93 / 108

IT 인프라 아키텍처 설계 · Session 4 · 네트워크 기초 · OSI L1~L7 + 장비·토폴로지

## WAN 토폴로지 — Hub-and-Spoke · Full-Mesh · SD-WAN

### Hub-and-Spoke

- 본사 = Hub, 지점 = Spoke
- 모든 지점 → 본사 경유
- **단순·저렴·관리 용이**
- 본사 회선 병목-SPOF

### Full-Mesh

- 모든 지점 간 직접 연결
- 지연 최소·이중화 ↑
- 회선 수 =  $N(N-1)/2$  = **매우 비쌈**
- 소수 핵심 지점만 적용

### Partial-Mesh

- 일부만 직결 (트래픽 많은 곳)
- Hub-and-Spoke + 선별적 직결
- **현실 표준**

### SD-WAN

- 컨트롤러가 정책 자동 적용
- 다중 통신사 자동 절제·로드밸런싱
- 응용 인지 라우팅
- 클라우드 우회 (Local Internet Breakout)

### DMVPN (Cisco)

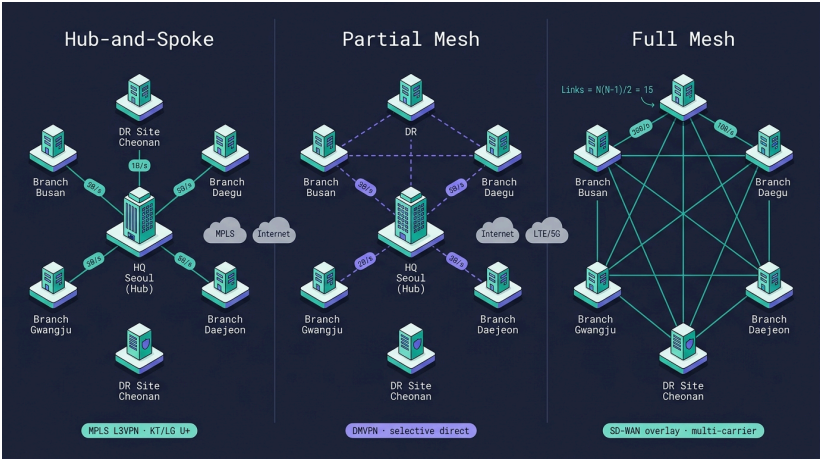
- 동적 Mesh — Hub로 시작, Spoke 간 직접 연결 동적 생성
- 회선 절감 + Mesh 효과

### MPLS L3VPN

- 통신사가 L3 분리 제공
- KT VPN-SKB VPN-LG U+ VPN
- 안정적이지만 비쌈
- VRF + MP-BGP 기반

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

94 / 108



WAN 토폴로지 — Hub-and-Spoke · Full-Mesh · SD-WAN

## 토폴로지 비교 매트릭스 — 장단점·비용·확장성

| 토폴로지           | 비용    | 가용성 | 확장성 | 관리  | 적합 환경         |
|----------------|-------|-----|-----|-----|---------------|
| Star           | 낮음    | 중간  | 중간  | 쉬움  | LAN 액세스       |
| Mesh (Full)    | 매우 높음 | 최고  | 낮음  | 어려움 | 코어·핵심 P2P     |
| Mesh (Partial) | 중간    | 높음  | 중간  | 중간  | 캠퍼스 코어        |
| Tree           | 중간    | 중간  | 중간  | 중간  | 캠퍼스           |
| 3-Tier         | 중간~높음 | 높음  | 중간  | 중간  | 전통 엔터프라이즈     |
| Spine-Leaf     | 중간    | 높음  | 최고  | 중간  | 현대 DC·AI 클러스터 |
| Hub-and-Spoke  | 저렴    | 낮음  | 낮음  | 쉬움  | WAN 다지점       |
| SD-WAN         | 중간    | 높음  | 높음  | 중간  | WAN 글로벌       |

# Out-of-Band (OOB) 관리 — 별도 NW로 장비 관리



## OOB 개념

- 운영 트래픽과 물리적으로 분리된 관리망
- 평시·장애 시 모두 항상 접근 가능
- 운영 NW가 죽어도 장비 관리 가능



## OOB 구성요소

- 각 장비의 관리 포트 (MGMT)
- iLO·iDRAC·BMC (서버)
- Console Server (RS-232·Serial-over-IP)
- KVM-over-IP
- 별도 PDU·UPS



## OOB 토폴로지

- 별도 관리 VLAN + 관리 SW
- 별도 라우터 + 별도 회선 (LTE 등) 백업
- 관리망용 작은 SW를 ToR과 별도로 배치
- Bastion / Jump Host 를 통한 접근



## TA의 표준

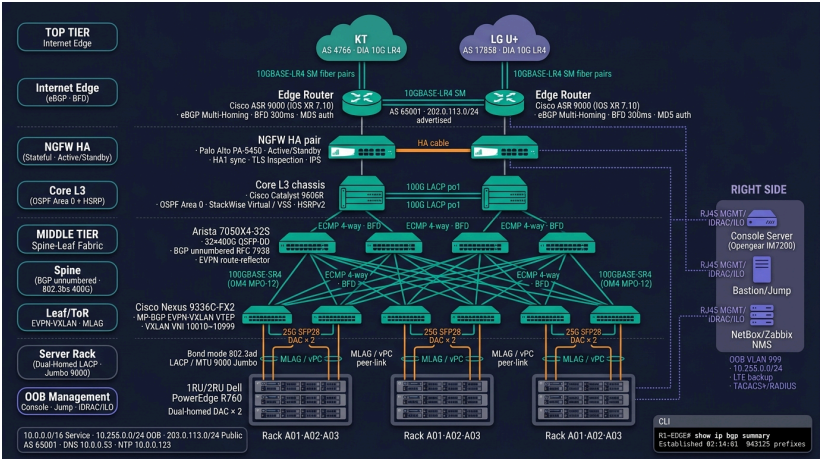
- 운영망 / 관리망 / DMZ 3망 분리
- 모든 관리는 OOB 통해서만
- 비밀번호·키·인증서 별도 관리
- 점프호스트 세션 기록 도입

# PART J

## TA의 네트워크 결정 · 산출물 · 정리

7계층·100+ 프로토콜·수십 가지 장비를 결정의 언어로 옮긴다.





데이터센터 NW 구성도 (삽화)

# TA가 네트워크 설계에서 결정해야 할 10가지

1 ~ 5

1. 물리 매체 — Cat 6a / 광 (SR/LR/ER) / DAC
2. 장비 벤더 표준 — Cisco·Juniper·Arista·국산
3. 토폴로지 — 3-Tier · Spine-Leaf · Hybrid
4. L2 도메인 범위 — VLAN 설계·STP 영역
5. L3 라우팅 프로토콜 — Static·OSPF·BGP·IS-IS

6 ~ 10

6. 이중화 패턴 — VRRP·MLAG·ECMP
7. IP 주소 체계 — CIDR·VLSM·사실 IP 대역 선정
8. MTU 정책 — 1500 / Jumbo 9000
9. 관리망 분리 — OOB·Bastion·3망 분리
10. WAN 연결 방식 — MPLS L3VPN·SD-WAN·인터넷 VPN

모든 결정은 산출물에 정량적으로 기록 — 단가·EOL·라이선스·유지보수 비용까지 BOM에 명시.

## TA의 네트워크 산출물 — 6종 표준

| 산출물    | 형식                | 핵심 내용                             | 작성 시점        |
|--------|-------------------|-----------------------------------|--------------|
| 논리 구성도 | Visio-draw.io     | L2/L3 토폴로지·VLAN-라우팅 영역            | 초기 설계        |
| 물리 구성도 | Visio-CAD         | 랙 배치·케이블 경로·포트 매핑                 | 시공 직전        |
| VLAN 표 | Excel             | VLAN ID-이름·서브넷·게이트웨이·사용처          | 설계 + 운영 갱신   |
| IP 할당표 | Excel-NetBox-IPAM | 호스트·VIP-DHCP 범위·예약                | 설계 + 매 변경    |
| 라우팅 표  | Excel-Markdown    | OSPF Area-BGP Peer-MED-LOCAL_PREF | 설계 + 트러블슈팅 시 |
| 포트 매핑표 | Excel-NetBox      | 장비 포트 ↔ 단말·서버·VLAN                | 시공 + 운영      |

### 추가 보조 산출물

- 방화벽 정책표 — Src/Dst/Port/Action/Justification
- 케이블 라벨링 표준 — 양 끝 라벨·도면 ID
- 점검 체크리스트 — 일/주/월/분기
- 변경관리 (CR) — 변경 영향·롤백 절차

## 결정 의사결정 트리 — 케이블·라우팅·토폴로지



### 케이블 선택 트리

거리 < 5m, 25G+  
→ DAC (저렴·저전력)  
거리 < 30m, 25/40G  
→ Cat 8 또는 SFP28 DAC  
거리 < 100m, 1G/10G  
→ Cat 6a  
거리 100m~500m, 10/40/100G  
→ MM (OM4) + SR  
거리 > 500m, 100G+  
→ SM + LR  
거리 > 10km  
→ SM + ER/ZR 또는 통신사 회선



### 라우팅 선택 트리

지점 1~3개·변경 없음  
→ Static  
단일 캠퍼스·동일 벤더  
→ OSPF Single Area  
다중 캠퍼스  
→ OSPF Multi-Area  
Cisco 단일·중소  
→ EIGRP (선택)  
인터넷 연결·멀티 ISP  
→ BGP (필수)  
DC 내부 Spine-Leaf  
→ BGP (RFC 7938)  
ISP·캐리어 백본  
→ IS-IS

# Linux 네트워크 CLI — ip · ss · tcpdump · dig

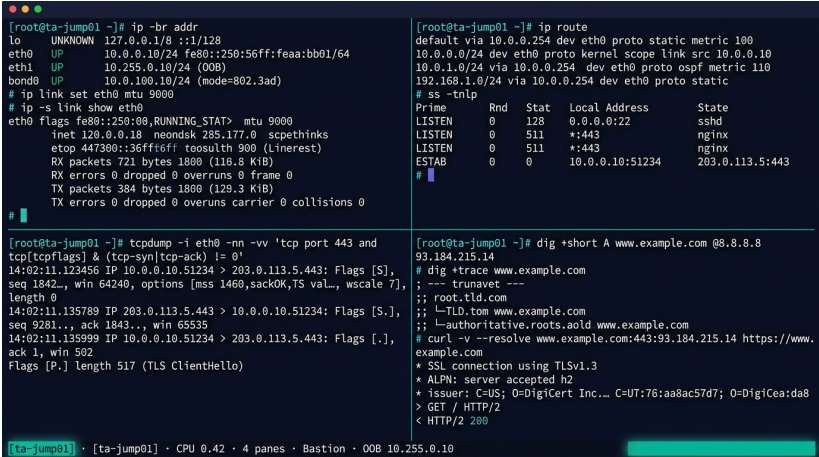
```
# ----- ip 명령 (iproute2 - net-tools 대체) -----
$ ip -br addr                # 인터페이스 + IP 요약
$ ip addr add 10.0.0.10/24 dev eth0      # IP 추가
$ ip link set eth0 mtu 9000              # Jumbo MTU
$ ip link set eth0 up                  # 인터페이스 UP
$ ip route                      # 라우팅 테이블
$ ip route add 192.168.1.0/24 via 10.0.0.1 # Static Route 추가
$ ip route add default via 10.0.0.254
$ ip neigh                      # ARP 테이블 (ip neighbour)
$ ip -s link show eth0          # 인터페이스 통계

# ----- ss - netstat 대체 -----
$ ss -tnp                    # TCP LISTEN+ESTABLISHED + 프로세스
$ ss -tan state established
$ ss -s                      # 요약 (TCP/UDP/Total)

# ----- tcpdump - 패킷 캡처 -----
$ sudo tcpdump -i eth0 -nn host 10.0.0.5 and port 443
$ sudo tcpdump -i any -nn 'tcp[tcpflags] & (tcp-syn|tcp-rst) != 0'
$ sudo tcpdump -i eth0 -w /tmp/capture.pcap port 53
$ sudo tcpdump -r /tmp/capture.pcap -nn -A | less

# ----- DNS-TLS-HTTP 디버그 -----
$ dig +short A www.example.com @8.8.8.8
```

현장 표준: `ifconfig` · `netstat` · `route` · `arp` · `nslookup` 은 모두 **deprecated**. RHEL 9·Ubuntu 24.04 기본 이미지는 빠져 있음 → `ip` · `ss` · `dig` · `mtr` 4종 세트를 외워야 함.



Linux 네트워크 CLI — ip · ss · tcpdump · dig

트러블슈팅 체크리스트 — *Bottom-up 7단계*

| 단계    | 점검 항목              | 명령·도구                                                                                           |
|-------|--------------------|-------------------------------------------------------------------------------------------------|
| L1    | 케이블·SFP·Link LED   | 물리 점검 · <code>ethtool eth0</code>                                                               |
| L2    | MAC 학습·VLAN·STP 상태 | <code>show mac address-table</code> · <code>show spanning-tree</code>                           |
| L3    | IP·게이트웨이·라우팅       | <code>ip addr</code> · <code>ip route</code> · <code>show ip route</code>                       |
| L3    | 도달성                | <code>ping</code> · <code>tracert</code> · <code>mtr</code>                                     |
| L4    | 포트 LISTEN·TCP 상태   | <code>netstat -an</code> · <code>ss -tnp</code>                                                 |
| L5~L7 | DNS·TLS·응용         | <code>dig</code> · <code>nslookup</code> · <code>openssl s_client</code> · <code>curl -v</code> |
| 패킷    | 실제 트래픽             | <code>tcpdump</code> · <code>Wireshark</code> · <code>tshark</code>                             |

기본 원칙: **Bottom-up** 으로 격리 → 각 계층에서 정상 동작 확인 → 한 계층씩 위로. **상위에서 시작하면 시간 낭비.**

세션 4 핵심 키워드 — *암기 카탈로그*

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>● <b>OSI / TCP/IP</b></p> <ul style="list-style-type: none"><li>7 Layer / 4 Layer</li><li>캡슐화·디캡슐화</li><li>Frame·Packet·Segment·Data</li><li>L1=Hub, L2=Switch, L3=Router, L4=FW/L4 LB, L7=WAF</li></ul> <p>● <b>L1 물리</b></p> <ul style="list-style-type: none"><li>Cat 5e·6·6a·7·8</li><li>SM (9/125)-MM (50/125-OM3/4/5)</li><li>LC-SC-MTP/MPO</li><li>SFP·SFP+·QSFP28·QSFP+·QSFP28-QSFP-DD·OSFP</li><li>SR (100m)·LR (10km)·ER (40km)·ZR (80km)</li></ul> <p>● <b>WiFi</b></p> <ul style="list-style-type: none"><li>802.11 a/b/g/n/ac/ax/be</li><li>2.4·5·6 GHz · 20~320 MHz</li><li>WPA3·EAP-TLS·802.1X</li></ul> | <p>● <b>L2</b></p> <ul style="list-style-type: none"><li>Ethernet-MAC OUI·ARP</li><li>STP·BPDU Guard·Root Guard</li><li>LACP·LAG·EtherChannel</li><li>LLDP·CDP·LLDP-MED</li><li>VLAN 802.1Q·Trunk·Native·Voice</li><li>Port Security·DHCP Snooping·DAI</li></ul> <p>● <b>L3</b></p> <ul style="list-style-type: none"><li>IPv4·TTL·Protocol</li><li>RFC 1918 사설 IP</li><li>CIDR·VLSM·Longest Prefix</li><li>ICMP·Ping·Traceroute</li><li>OSPF·BGP</li><li>iBGP·eBGP</li><li>AS_PATH·LOCAL_PREF</li><li>ECMP·PBR</li></ul> | <p>● <b>L4</b></p> <ul style="list-style-type: none"><li>TCP·UDP·QUIC</li><li>3-Way·4-Way·TIME_WAIT</li><li>Sliding Window·cwnd</li><li>CUBIC·BBR</li><li>Well-Known 포트</li></ul> <p>● <b>L5~L7</b></p> <ul style="list-style-type: none"><li>DNS (A·CNAME·MX·TXT·SRV·NS)</li><li>DHCP DORA·Option 43/60/82</li><li>HTTP/1.1·2·3·TLS 1.2/1.3</li><li>SMTP·POP3·iMAP·SPF·DKIM·DMARC</li><li>FTP/SFTP·NFS·SMB·S3</li><li>SSH·Bastion</li><li>SNMP·NTP·Syslog·LDAP/AD</li></ul> <p>● <b>장비·토폴로지</b></p> <ul style="list-style-type: none"><li>Hub·Bridge·L2/L3 SW·Router·LB·WAF·FW</li><li>Fixed·Modular·Stackable·ToR·EoR</li><li>3-Tier·Spine·Leaf·Hub·Spoke·SD-WAN</li><li>OOB 관리</li></ul> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

IT 인프라 아키텍처 설계 · Session 4 · 네트워크 기초 · OSI L1~L7 + 장비·토폴로지

## Q&A — 세션 4 자주 묻는 질문

### ? Q1. Cat 6와 6a 중 어느 것?

신규 = Cat 6a. Cat 6는 10G가 55m까지만 보장. 데이터센터·신축 표준은 Cat 6a.

### ? Q2. OSPF와 BGP 중 어느 것?

AS 내부 = OSPF, AS 간(인터넷) = BGP. DC 내부도 BGP로 통일하는 추세 (RFC 7938).

### ? Q3. TCP CUBIC과 BBR 중 어느 것?

LAN·단거리 = CUBIC 충분. WAN·고대역·장거리 = BBR 권고.

### ? Q4. HTTP/3로 바뀌어야 하나?

자동 협상되므로 강제 전환 불필요. CDN 사용 시 자동 적용. 사내는 HTTP/2가 표준.

### ? Q5. VLAN은 몇 개까지?

802.1Q = 4094개. 데이터센터 멀티 테넌트는 VXLAN(24bit·1600만) 같은 Overlay 로 확장.

### ? Q6. WiFi 7 도입 시점?

2026년 단말 보급 시작. AP는 미리, 단말은 자연 교체 권고.

### ? Q7. 관리망 분리는 꼭?

공공·금융 사실상 의무. 일반 기업도 보안 표준상 권고. OOB + Bastion 조합.

IT 인프라 아키텍처 설계 · Session 4 · 네트워크 기초 · OSI L1~L7 + 장비·토폴로지

## 마무리 — 7계층, 한 권의 통일

네트워크는 7개 계층의 약속, 100여 개의 프로토콜, 수십 가지 장비의 종합 예술.

TA는 이 약속을 도면·표·결정 매트릭스·산출물로 풀어낸다.

### 🏆 오늘의 성취

- OSI 7 / TCP/IP 4 계층 — 완전한 어휘 확보
- L1 케이블·광·모뎀·WiFi — 매체 결정 가능
- L2 Ethernet·VLAN·STP·LACP — 스위칭 이해
- L3 IP·CIDR·OSPF·BGP — 라우팅 결정 가능
- L4 TCP/UDP/QUIC — 전송 성능 진단 가능
- L5~L7 DNS·HTTP·TLS·SSH·SNMP — 응용 운영 가능
- 장비·토폴로지 — BOM·도면 설계 가능

### 🛒 가져갈 산출물 카탈로그

- TA의 NW 결정 10가지
- 표준 산출물 6종 (논리·물리 구성도·VLAN·IP·라우팅·포트)
- 케이블·라우팅·토폴로지 결정 트리
- Bottom-up 트러블슈팅 7단계 체크리스트
- 핵심 키워드 카탈로그 (시험·면접·산출물 공용)

### 💡 자기 학습 과제

- VLAN 표·IP 할당표 양식 한 번씩 작성해보기
- 사내 NW 도면을 OSI 7 계층 기준으로 분해해보기
- tcpdump · ip route · show interface trunk 명령 익혀 두기

IT 인프라 아키텍처 설계

# 네트워크 고급 VLAN·HA·NAT·LB·GSLB·망분리·NMS

Session 5 · Day 2 — TA의 기업 네트워크 운영 설계 한 권

본문 65 슬라이드 · 강의 시간 약 90분 · TA(Technical Architect) 양성 과정

강사 박수현 ·  젠아이랩스(GenAI Labs)

데이터센터 · 서버·OS·DB·GPU · 가상화·컨테이너 · 네트워크 L1~L7 · 스토리지 · 백업·DR · 보안 6대 도메인 · HA · 용량·성능·관찰성 · 설계 워크숍 · RFP · 5종 실전 케이스

IT 인프라 아키텍처 설계 · Session 5 · 네트워크 고급 · VLAN·HA·NAT·LB·GSLB·망분리·NMS

## 왜 네트워크 고급인가 — 국내 통신·NW 장애 3선

### ① KT 이동통신 장애

2021.10.25 (월)

라우터 설정 변경 중 BGP 오설정 → 전국 KT 유·무선 인터넷 약 89분 마비.

- 점심 시간 직격 (11:20~12:49)
- 카드결제·증권 거래 전부 영향
- 정부 '통신 장애 보상' 가이드라인 강화

💡 교훈 — 변경관리(CAB)·롤백 절차·점검 시간대 + 라우팅 검증

참고: 「2021 KT 통신장애」 검색

### ② 카카오 5일 장애 (NW 측면)

2022.10.15~10.20

판교 DC 화재 → DNS·LB-세션 동기화 다중 장애 연쇄. 메시지·결제·인증 모두.

- DNS TTL 길이 절체 지연
- LB Health Check 미흡
- 세션 복구 → 본인인증·로그인 연쇄 폭주

💡 교훈 — GSLB·Anycast DNS·LB Health Check·세션 외부화

참고: 「카카오 장애 보고서 과방위」 검색

### ③ 서울 행정망 마비

2023.11.17 (금)

행정안전부 「서울」 인증 인프라 장애 → 전국 민원 시스템 마비 (24시간+).

- L4 LB·인증 서버 NW 경로 문제
- 주민등록·인감 등 발급 불가
- 「공공 NW 이중화 의무」 강화 추진

💡 교훈 — 공공 NW 이중화·우회 경로·인증 NW 분리

참고: 「2023 서울 행정망 장애」 검색

🚩 이번 세션의 시각 — 위 3건은 모두 「VRRP/GSLB 미적용」「라우팅 변경 관리 부실」「NW 이중화 부재」가 핵심. 본 세션의 VLAN·HA(VRRP)·LB·GSLB·망분리가 직접 해법.



Session 5 · Day 2 — TA의 기업 네트워크 운영 설계 한 권

## 세션 5 — 회차 메타데이터

### 📋 세션 정보

- **회차:** 5 / 18 — Day 2 · 네트워크 고급
- **소속:** Day 2 — NW 고급 + 스토리지·백업 + 보안 + HA·운영
- **카테고리:** 인프라 고급
- **강의 시간:** 약 90분
- **강사:** 박수현 — 젠아이랩스(GenAI Labs) CEO / CTO

### 🎯 핵심 메시지

기초 위에 쌓는 **고급 도구 7종** — **VLAN**으로 분리, **HA/LB**로 살리고, **NAT/QoS**로 다듬고, **망분리/NMS**로 지킨다.

### 🎯 학습 목표 (Learning Objectives)

1. **VLAN 심화** — Private VLAN·Voice VLAN·VLAN 보안을 설계할 수 있다
2. **STP 보호·스위치 클러스터링** — Stack·VPC·MLAG을 비교 선택한다
3. **HA 프로토콜** — VRRP·HSRP·GLBP·ECMP를 결정 매트릭스로 본다
4. **NAT-QoS** — NAT 8종·DSCP·CoS·Policing·Shaping을 안다
5. **LB-GSLB** — L4/L7 알고리즘·헬스체크·Persistence·사이트 분산을 설계한다
6. **DHCP-IPv6** — DORA·Option 82·IPv6 주소 체계를 운영자 시각으로 다룬다
7. **망분리-SDN-Overlay-SD-WAN-NMS** — 기업·캠퍼스·WAN을 통째로 본다

# PART A

## VLAN 심화 — *QinQ · Private VLAN · Voice · VTP · 보안*

VLAN은 단순히 "방을 나누는 것"을 넘어, QinQ로 ISP·Private VLAN으로 호텔·Voice로 IP전화까지 확장된다.

IT 인프라 아키텍처 설계 · Session 5 · 네트워크 고급 · VLAN-HA·NAT·LB·GSLB·망분리·NMS

## VLAN 복습 — *Session 4* ↩ 참조 + 심화 진입

 **본문 참조** — VLAN 802.1Q 태그·Trunk·Access·Native VLAN 본문은 **Session 4** **## VLAN - 802.1Q 태그** 슬라이드에서 다뤘다. 여기서는 한 줄로 환기만 하고, QinQ·Private VLAN·Voice VLAN·VTP·VLAN 보안으로 곧장 들어간다.

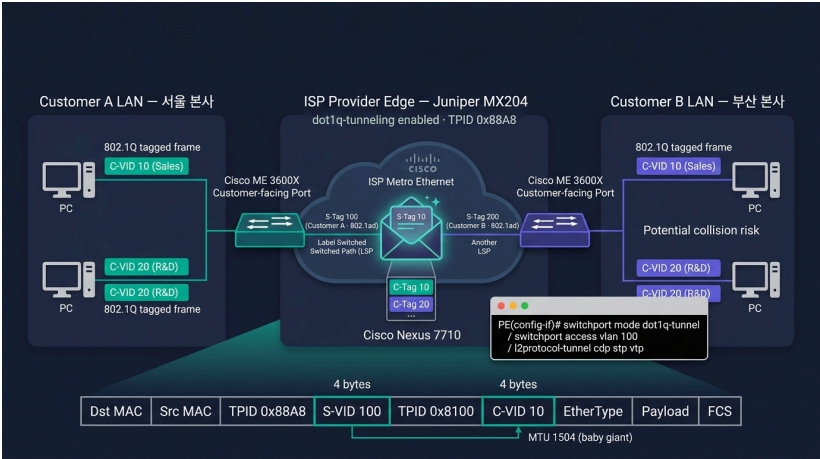
### 한 줄 환기

- **VLAN** = L2 broadcast 도메인 격리, 12bit VID = 0~4095 (실용 4,000개)
- **802.1Q 태그** = Ethernet 프레임 안에 4byte 삽입 (TPID: **0x8100** + TCI: PCP 3bit / DEI 1bit / **VID 12bit**)
- **Trunk** = 태그 유지하며 SW 간 다중 VLAN 전달, **Access** = 태그 제거 후 단말 전달, **Native VLAN** = Trunk 위의 무태그 1개 (보안상 1번 회피)

### 본 세션에서 새로 다루는 것 — Part A의 5장

- **QinQ** (802.1ad) — ISP가 고객 VLAN을 자기 VLAN으로 한 번 더 감싸기
- **Private VLAN** — Primary / Isolated / Community, 같은 서브넷 안에서 단말 격리 (호텔·아파트 패턴)
- **Voice VLAN** — IP 전화 자동 분류, LLDP-MED + CDP 연동
- **VTP** (VLAN Trunking Protocol) — Cisco VLAN DB 자동 동기화, 운영 사고 회피
- **VLAN 보안** — Port Security / DHCP Snooping / DAI / IP Source Guard 액세스 SW 표준 세트





QinQ 다이어그램 (삽화)

# Private VLAN — *Primary·Isolated·Community*



## Private VLAN의 동기

- "같은 서브넷 안에서도 단말끼리 통신을 막고 싶다"
- 4094 VLAN을 잡아먹지 않고 격리 — VLAN 1개 안에서 sub-격리



## 3종 VLAN

| 종류              | 통신 가능 대상                                    |
|-----------------|---------------------------------------------|
| Primary         | 모든 Secondary와 + 외부                          |
| Isolated (격리)   | Primary와만 — 동일 Isolated끼리도 차단               |
| Community (공동체) | 같은 Community 내부 + Primary — 다른 Community 차단 |



## Port Type

- **Promiscuous Port** — Primary VLAN에 연결, 모든 단말과 통신 (라우터 ·GW용)
- **Isolated Port** — Isolated VLAN, 다른 단말과 단절
- **Community Port** — 같은 Community 내부만 가능



## 활용 시나리오

- **호텔 객실** — 객실끼리 차단(Isolated), 공용 GW로만
- **공공 와이파이** — 사용자 간 격리
- **DC 멀티테넌트** — 고객 그룹 분리
- **DMZ 서버 분리** — 서로 침투 차단

# PART C

## STP·스위치 클러스터링 — *Stack·vPC·MLAG*

STP는 보호되어야 한다. 그리고 STP를 우회해서 진짜 Active-Active를 만드는 도구가 클러스터링이다.

IT 인프라 아키텍처 설계 · Session 5 · 네트워크 고급 · VLAN-HA-NAT-LB-GSLB-망분리-NMS

## BPDUGuard / Root Guard / Loop Guard



### BPDUGuard

- Edge (PortFast) 포트에 BPDU 수신 시 → 즉시 Err-Disable
- 사용자가 무단으로 스위치를 액세스 포트에 꽂는 사고 차단
- 모든 액세스 포트의 표준 설정

```
spanning-tree portfast edge default
spanning-tree portfast bpduguard default
```



### Root Guard

- "이 포트는 절대 Root 방향이 아니다"
- 이 포트에서 Superior BPDU 수신 → Root Inconsistent 상태 (Forwarding 중단)
- 운영자 의도 외의 Root 선출 차단 — 코어 SW의 다운링크에 적용



### Loop Guard

- 단방향 링크 또는 BPDU 손실로 인한 잘못된 Forwarding 차단
- BPDU 안 받으면 → Loop Inconsistent 상태로 차단
- Trunk 포트에 적용



### TA 매트릭스

| 위치      | 권장                                   |
|---------|--------------------------------------|
| 액세스 포트  | PortFast + BPDUGuard + Port Security |
| 코어 다운링크 | Root Guard                           |
| 광 Trunk | Loop Guard                           |

# 스위치 Stacking — Cisco StackWise · HPE IRF · Aruba VSF

## Stacking이란

- 여러 물리 스위치를 하나의 논리 SW 로 묶음
- 백플레인급 Stack Cable로 연결
- 단일 IP·단일 설정·단일 관리 평면
- LAG/LACP을 여러 SW 멤버에 걸쳐 구성 가능 (실질적 MLAG)

## 벤더별 명칭

| 벤더      | 명칭                                    |
|---------|---------------------------------------|
| Cisco   | StackWise / StackWise Virtual         |
| HPE     | IRF (Intelligent Resilient Framework) |
| Aruba   | VSF (Virtual Switching Framework)     |
| Juniper | Virtual Chassis (VC)                  |
| Arista  | (별도 — MLAG 선호)                        |

## 장점·단점

| 장점             | 단점                            |
|----------------|-------------------------------|
| 단일 관리          | 펌웨어 업그레이드 시 전체 영향 가능          |
| LAG/MLAG 자연스러움 | Stack Cable 장애 = 분할(Split) 위험 |
| 구성 단순          | Stack 멤버 수 한계 (보통 4~9대)       |
| 액세스 SW에 인기     | 코어/Spine에는 부적합                |

## TA 권고

- 액세스/집선 = Stacking 권고
- 코어/Spine = vPC/MLAG 권고 (편입 시 분리 가능)
- Stack 멤버는 동일 모델 + 동일 IOS 권고

# PART D

## HA 프로토콜 — VRRP · HSRP · GLBP · ECMP

게이트웨이 한 대만 죽어도 전체가 멈춘다. 표준 답은 가상 IP를 둘이서 나눠 갖는 것.

# VRRP (Virtual Router Redundancy Protocol) — RFC 5798

## VRRP 동작

- 2~N대의 라우터가 가상 IP/MAC 을 공유
- Master 1대가 가상 IP를 응답 — 나머지는 Backup
- Master가 1초마다 Advertisement 보냄
- Backup이 3.6초간 못 받으면 → 새 Master 선출
- 단말은 가상 IP만 게이트웨이로 알면 됨

## Master 선출

- 가장 높은 Priority (0~255, 기본 100)
- Owner (실IP=가상IP) = Priority 255 (자동 Master)
- 동물이면 IP 큰 쪽

## Virtual MAC

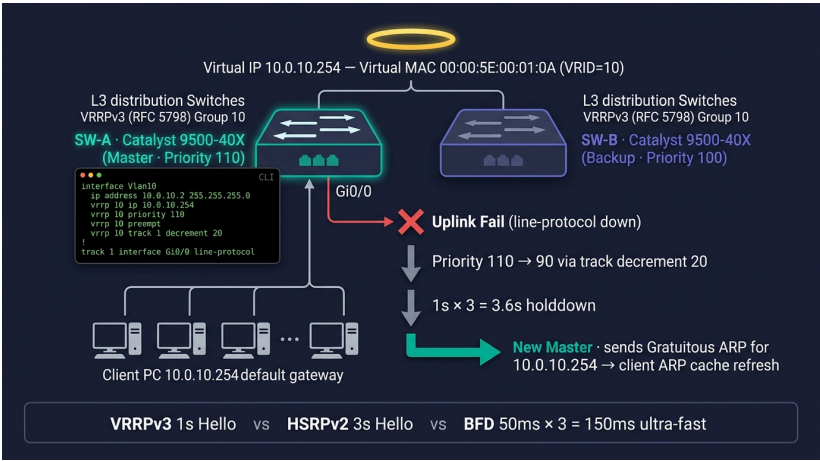
- IPv4: 00:00:5E:00:01:VRID
- VRID = VRRP Group ID (1~255)
- 절체 시 새 Master가 Gratuitous ARP 발송 → 단말 ARP 캐시 갱신

## Tracking

- 업링크 인터페이스 또는 라우트가 down 되면 Priority 자동 감소
- → 자동 절체 유발
- 예: 업링크 다운 → Priority 110 → 100 → 다른 SW가 Master

## TA 메모

- VRRPv3 (RFC 5798) = IPv4 + IPv6 동시 지원
- VRRPv2 = IPv4 only
- 벤더 중립 — Cisco·Juniper·Arista·HPE 모두 지원



VRRP 동작 (삽화)

HSRP · GLBP · CARP — VRRP의 변종

| 프로토콜 | 표준              | 벤더       | 특징                                  |
|------|-----------------|----------|-------------------------------------|
| VRRP | RFC 5798        | 표준       | Master 1대, Active-Standby           |
| HSRP | RFC 2281 (info) | Cisco 독자 | Active 1대 + Standby 1대, Hello 3초    |
| GLBP | (Cisco 독자)      | Cisco    | Active-Active — 가상 MAC 여러 개를 단말에 분배 |
| CARP | OpenBSD         | BSD 진영   | VRRP 호환, BSD/pfSense                |

HSRP 핵심

- Group: 0~255 (v1) / 0~4095 (v2)
- Virtual MAC: 00:00:0C:07:AC:00
- States: Init → Listen → Speak → Standby → Active
- Hello 3초, Hold 10초 (기본)
- Tracking 지원

GLBP 핵심

- AVG (Active Virtual Gateway) — 가상 IP의 ARP 응답 담당
- AVF (Active Virtual Forwarder) — 가상 MAC별 포워딩
- 단말 그룹별로 다른 MAC 반환 → Active-Active 부하 분산
- Cisco 독자

결정 매트릭스 — VRRP vs HSRP

| 항목      | VRRP     | HSRP           |
|---------|----------|----------------|
| 표준      | IETF RFC | Cisco 독자       |
| 멀티벤더    | ○        | △ (Cisco only) |
| IPv6    | v3 지원    | 가능             |
| Hello   | 1초       | 3초             |
| 절체 시간   | 3.6초     | 10초            |
| 운영자 인지도 | 신규 표준    | 한국 외 현장 압도적    |

권고

- 신규 사업 = VRRP
- 기존 Cisco 단독 사이트 = HSRP 잔존 OK
- Active-Active = GLBP 또는 MLAG

VRRP·HSRP 콘솔 — Cisco IOS 실제 설정

```
! ----- VRRP (RFC 5798) - SW-A: Master -----
SW-A# configure terminal
SW-A(config)# interface Vlan10
SW-A(config-if)# ip address 10.0.10.2 255.255.255.0
SW-A(config-if)# vrrp 10 ip 10.0.10.1          ! Virtual IP
SW-A(config-if)# vrrp 10 priority 110          ! 더 큼 = Master
SW-A(config-if)# vrrp 10 preempt
SW-A(config-if)# vrrp 10 authentication md5 key-string Sup3rS3cret
SW-A(config-if)# vrrp 10 timers advertise 1    ! Hello 1s
SW-A(config-if)# vrrp 10 track 1 decrement 20  ! 업링크 다운 시 -20
SW-A(config-if)# exit

SW-A(config)# track 1 interface GigabitEthernet0/0 line-protocol
SW-A(config)# end

! ----- VRRP - SW-B: Backup (priority 100) -----
SW-B(config-if)# vrrp 10 ip 10.0.10.1
SW-B(config-if)# vrrp 10 priority 100

! ----- HSRP (Cisco 독자) -----
SW-A(config-if)# standby version 2
SW-A(config-if)# standby 10 ip 10.0.10.1
SW-A(config-if)# standby 10 priority 110
SW-A(config-if)# standby 10 preempt
SW-A(config-if)# standby 10 timers msec 200 msec 750 ! 빠른 절체
SW-A(config-if)# standby 10 track 1 decrement 20
```

TA 표준 세트: preempt + track + timers msec + 인증. 절체 시 GARP가 흐름. 신규 = VRRP, 잔존 Cisco-only = HSRP.

# ECMP (Equal-Cost Multi-Path) — 동일 비용 다중 경로

## ECMP 개념

- 같은 목적지로 비용이 동일한 N개 경로가 있을 때
  - 라우터가 N개 모두에 트래픽을 분산
  - Active-Active 라우팅
  - Spine-Leaf DC의 표준 동작
- ### 해시 알고리즘
- L3 Hash: Src IP + Dst IP
  - L4 Hash: + Src/Dst Port (Per-Flow)
  - Polarization 회피 — 동일 해시 키 사용 시 분기점마다 같은 경로 선택 → 일부 링크 과부하

## Per-Packet vs Per-Flow

| 모드         | 장점            | 단점              |
|------------|---------------|-----------------|
| Per-Packet | 균등 분산         | 재정렬 → TCP 성능 ↓  |
| Per-Flow ★ | 같은 플로우는 같은 경로 | 큰 플로우는 한 링크에 집중 |

## 라우팅 프로토콜 지원

- OSPF/IS-IS — 동일 cost 자동 ECMP
- BGP — maximum-paths 설정 + AS-PATH 동일 조건
- 일반 라우터 = 최대 4·8·16·32·64 경로

## TA 메모

- DC Spine 대역폭 확장의 표준 도구
- BGP EVPN-VXLAN과 결합

# PART E

## NAT·QoS — 주소 변환 8종 · 큐잉 정책

외부와 내부의 경계에서는 주소를 바꾸고, 트래픽의 종류에 따라 줄을 세운다.

# NAT 종류 — 8가지 변형

| 종류                         | 동작                          | 주 용도                |
|----------------------------|-----------------------------|---------------------|
| Static NAT (1:1)           | 내부 IP ↔ 외부 IP 고정            | 서버 공개 (웹-메일)        |
| Dynamic NAT                | 내부 IP → 풀의 외부 IP 임시 매핑      | 다수 내부 사용자           |
| PAT (NAPT) ★               | 다수 내부 IP → 1개 외부 IP + 포트 변환 | 가정·기업 인터넷 표준        |
| Hairpin NAT (NAT Loopback) | 내부 → 외부 공인IP로 접근 시 다시 내부로   | 내부에서 자사 웹 접속        |
| Twice NAT (Bidirectional)  | Src-Dst 모두 변환               | 사이트 간 IP 충돌 해결      |
| NAT64                      | IPv6 ↔ IPv4 양방향             | IPv6 단말이 IPv4 서버 접근 |
| NAT46                      | IPv4 → IPv6                 | 드물게                 |
| CGN (LSN)                  | 통신사 대규모 PAT                 | IPv4 고갈 대응          |

현장 단순화: 가정/사무실 = PAT, 서버 공개 = Static, IPv6 전환 = NAT64, 통신사 = CGN.

# NAT 보안 · NAT-Traversal — STUN · TURN · ICE



## NAT의 보안 효과 (부수적)

- 내부 사설 IP가 외부에 노출 안 됨
- 외부에서 직접 connect 불가 (Static 제외)
- 단, NAT 자체는 보안 솔루션이 아님 — FW가 별도 필요



## NAT의 부작용

- End-to-End 깨짐 — IPsec AH 호환 안 됨 (ESP는 NAT-T 필요)
- VoIP·P2P 어려움
- 로그·감사 추적 복잡 (외부에서 보면 1 IP)
- Active FTP·SIP·H.323 → ALG (Application Layer Gateway) 필요



## NAT-Traversal 기술

- STUN (RFC 5389) — 자신의 공인 IP·포트 발견
- TURN (RFC 8656) — 중계 서버 경유 (STUN 실패 시)
- ICE (RFC 8445) — STUN+TURN 후보 자동 선정
- WebRTC 의 표준 백본



## 운영 관점

- VoIP·화상회의·게임·원격제어 = STUN/TURN
- IPsec NAT-T (UDP 4500) — VPN을 NAT 너머로
- 기업 FW는 SIP·H.323 ALG 동작 정책 점검 필수

## QoS 큐잉 — *DSCP · CoS · 우선순위 표시*

### 표시 (Marking)

- **CoS (802.1p)** — L2, VLAN 태그의 PCP 3bit (0~7)
- **DSCP** — L3, IP TOS의 6bit (0~63), 64개 클래스
- **MPLS EXP** — MPLS 라벨의 3bit

### DSCP 클래스

| 클래스                       | DSCP | 용도                |
|---------------------------|------|-------------------|
| EF (Expedited Forwarding) | 46   | 음성 (VoIP)         |
| AF41                      | 34   | 영상 회의             |
| AF31                      | 26   | 영상 스트리밍           |
| AF21                      | 18   | 트랜잭션              |
| CS6                       | 48   | 라우팅 제어 (OSPF-BGP) |
| CS0 (BE)                  | 0    | Best Effort (기본)  |

### 분류 (Classification)

- DSCP-CoS 신뢰 (Trust) — Edge가 이미 표시했다면 신뢰
- ACL 매칭 — 출발/도착 IP/Port로 분류
- NBAR (Cisco) — 응용 시그니처로 분류

### 큐잉 알고리즘

| 알고리즘                      | 특징                          |
|---------------------------|-----------------------------|
| FIFO                      | 단일 큐, 우선순위 없음               |
| WFQ (Weighted Fair Queue) | 플로우별 공평 분배                  |
| CBWFQ (Clos6-Based)       | 클래스별 대역폭 보장                 |
| LLQ (Low Latency Queue) ★ | CBWFQ + PQ → <b>VoIP 표준</b> |

### TA 메모

- VoIP·영상 = LLQ + 명시적 대역폭
- 데이터는 CBWFQ 클래스로 분배

## Policing vs Shaping — *드롭 vs 지연*

### Policing

- 정해진 속도 초과분을 **즉시 드롭** (또는 Remark)
- **Inbound** 적용이 일반
- Token Bucket 알고리즘
- 빠르고 단순, 저메모리

### 단점

- TCP 재전송 폭주 가능
- 사용자 체감 품질 저하

### Shaping

- 초과분을 **버퍼에 저장**했다가 천천히 보냄
- **Outbound** 적용이 일반
- Leaky Bucket / Token Bucket
- 메모리·지연 증가

### 장점

- 평활한 트래픽
- TCP 친화적

### 결정

| 상황              | 권고                  |
|-----------------|---------------------|
| ISP 가입자 초과 단속   | Policing            |
| WAN 회선 한계 맞출 송출 | <b>Shaping</b>      |
| QoS Marking     | Policing의 Remark 활용 |



# VoIP·영상회의 QoS 정책 — 현장 표준 설정



## VoIP 요구사항

- **One-way Latency** < 150ms
- **Jitter** < 30ms
- **Loss** < 1%
- 대역 = G.711(80kbps) / G.729(24kbps) per call
- BFCP-SIP 시그널링은 별도 우선순위



## 영상회의 요구사항

- HD = 2~4 Mbps
- 4K = 8~15 Mbps
- Loss < 0.5%
- 같은 LLQ 그룹 또는 별도 AF41



## 표준 정책 (예)

| 트래픽                   | 표시        | 큐             | 대역              |
|-----------------------|-----------|---------------|-----------------|
| Voice RTP             | EF (46)   | <b>LLQ</b>    | 회선의 10~33% (한도) |
| Voice 시그널링 (SIP)      | CS3 (24)  | CBWFQ         | 작게              |
| Video                 | AF41 (34) | CBWFQ         | 25%             |
| Mission Critical Data | AF31 (26) | CBWFQ         | 25%             |
| Best Effort           | CS0 (0)   | CBWFQ default | 나머지             |
| Scavenger (백업-P2P)    | CS1 (8)   | WRED 일찍 드롭    | 잔여              |



## TA 메모

- LLQ 한도는 회선의 **33% 이하** 권고
- WAN 회선 = Shaping으로 ISP 약정 속도에 맞춤

# PART F

## 로드 밸런싱 — L4 · L7 · 알고리즘 · 솔루션

단일 서버는 한계가 있다. 여러 서버 앞에 LB를 두면 가용성·확장성·보안 모두 얻는다.

IT 인프라 아키텍처 설계 · Session 5 · 네트워크 고급 · VLAN-HA-NAT-LB-GSLB-망분리-NMS

## L4 vs L7 — 결정의 첫 갈래길

### ⚙️ L4 LB (Transport)

- **5-Tuple** 보고 분배 (Src IP·Src Port·Dst IP·Dst Port·Protocol)
- 페이로드 무관 — HTTP·HTTPS·DB·SMTP 등 모든 TCP/UDP
- **빠름·저오버헤드** — 수십만 cps
- DSR(Direct Server Return) 가능
- L4 표준 솔루션 = LVS · HAProxy(TCP 모드) · F5(LTM L4)

### 🎯 사용 사례

- DB 클러스터 (3306·5432·1521)
- TCP 응용 (SMTP·LDAP·RDP)
- 단순 HTTP 부하 분산

### 🌐 L7 LB (Application)

- HTTP/HTTPS/gRPC 등 **응용 페이로드** 분석
- **URL·Header·Cookie·Method** 보고 분배
- SSL Termination → 백엔드는 평문
- WAF·Rate Limit·인증·Caching 부가 기능
- L7 표준 = NGINX · HAProxy · F5 LTM(L7) · Citrix NetScaler

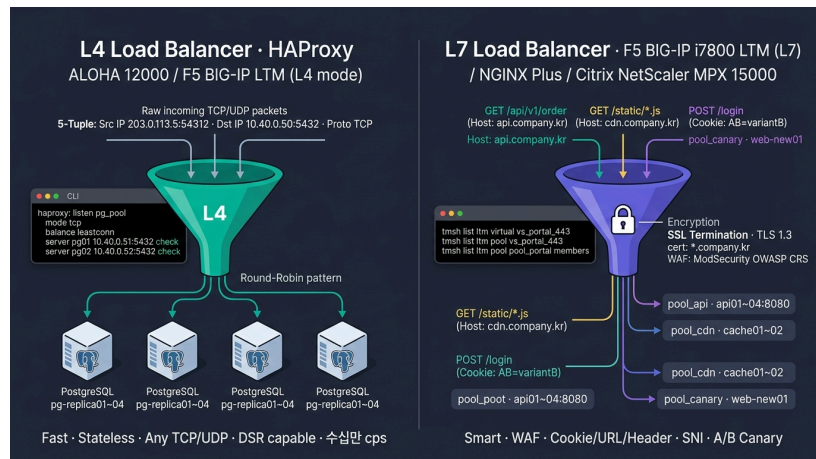
### 🎯 사용 사례

- `/api` → API 서버, `/static` → 캐시
- **A/B 테스트** (Header·Cookie 기반)
- **Canary 배포** (가중치)
- 다중 도메인 → 단일 IP

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

25 / 64

IT 인프라 아키텍처 설계 · Session 5 · 네트워크 고급 · VLAN-HA-NAT-LB-GSLB-망분리-NMS



L4 vs L7 (삼화)

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

26 / 64

# L4 LB 알고리즘 — 분배 방식

| 알고리즘                  | 동작               | 적합                      |
|-----------------------|------------------|-------------------------|
| Round Robin (RR)      | 순서대로 1→2→3→1     | 균등한 서버                  |
| Weighted RR           | 가중치 비율 (2:1:1)   | 사양 다른 서버                |
| Least Connections ★   | 현재 활성 연결 최소 서버   | 세션 긴 서비스 (DB·WebSocket) |
| Weighted Least Conn   | 가중치 + 연결 수       | 세션 + 사양 차이              |
| IP Hash (Source Hash) | Src IP 해시로 고정 매핑 | Session Persistence 대안  |
| URL Hash (L7)         | URL 해시           | 캐시 친화                   |
| Random                | 임의               | 단순                      |
| Least Response Time   | 응답시간 가장 빠른 서버    | 가용성 보장 안되면 위험           |

한 줄 결정: 짧은 요청 = RR/WRR, 긴 세션 = Least Conn, 캐시 = URL/IP Hash.

# L7 LB — URL·Header·Cookie·SSL Termination



## L7 콘텐츠 스위칭

- Path 기반: /api/\* → API 백엔드, /static/\* → CDN
- Host Header: www.a.com → A 풀, www.b.com → B 풀
- HTTP Method: GET → 캐시, POST → 직접 백엔드
- Cookie: A/B 테스트 그룹 분기
- User-Agent: 모바일 vs 데스크톱
- Geo IP: 국가별 다른 풀



## SSL Termination

- LB에서 TLS 종단 → 백엔드는 평문 HTTP
- 인증서 관리 1곳 (LB)
- 백엔드 CPU 절감
- 단점: 내부 평문 → DC 내부망 보안 신뢰 필요



## SSL Bridging (Re-encrypt)

- LB가 TLS 종단 → 백엔드 TLS 재암호화
- WAF·정책 적용 + 내부 암호 유지
- 더 안전, CPU 더 씀



## SSL Pas6-through

- LB가 SNI만 보고 라우팅 → TLS 그대로 백엔드
- WAF·L7 정책 불가
- 가장 단순



## TA 메모

- 일반: SSL Termination + WAF
- 금융·의료: SSL Bridging
- gRPC mTLS 또는 SSH = Pas6-through

## 헬스 체크 — *Active vs Passive*

### Active Health Check

- LB가 주기적으로 **테스트 요청** (HTTP GET /health)
- 응답 시간·상태 코드·콘텐츠 검증
- 실패 N회 → 풀에서 제외 (Drain)
- 복구 M회 → 다시 투입
- 간격: 보통 5~30초

### Passive Health Check

- 실제 클라이언트 요청 응답을 모니터링
- 5xx·Timeout 발생 시 풀에서 제외
- 즉시성 ↑, 가짜 양성 ↑

### 헬스 체크 종류

| 레벨                      | 검사             | 비고             |
|-------------------------|----------------|----------------|
| ICMP Ping               | L3 응답          | 가장 단순, 응용 무관   |
| TCP Connect             | 3-way 성공       | L4 표준          |
| HTTP GET /health        | 200 OK + 응답 본문 | <b>L7 표준</b> ★ |
| TLS Handshake           | 인증서 유효성        | HTTPS 서비스      |
| Script (gRPC-DB-Custom) | 응용 종속          | 정확도 ↑          |

### TA 메모

- **/health 엔드포인트는 응용 + DB까지 점검**해야 의미
- 단순 200 OK는 "프로세스 살았다" 만 의미

## Session Persistence — *Sticky Session*

### 왜 필요한가

- 세션 정보가 서버 메모리에 있을 때 — 다른 서버로 가면 로그아웃
- 장바구니·로그인 상태·WebSocket
- 외부 세션 스토어(Redis)를 쓰지 않는 응용

### Persistence 방식

| 방식                   | 동작            | 단점                   |
|----------------------|---------------|----------------------|
| Source IP            | 클라이언트 IP 해시   | NAT 뒤 다수 사용자 한 서버 집중 |
| Cookie Insert ★      | LB가 쿠키 발급     | HTTP/HTTPS 한정        |
| App Cookie Learn     | 서버가 발급한 쿠키 학습 | 응용 의존                |
| SSL Session ID       | TLS 재사용 키     | TLS 1.3에서 변경         |
| Header (X-Forwarded) | 임의 헤더         | 응용 협조 필요             |

### Persistence의 부작용

- **부하 불균형** — 일부 서버에 트래픽 집중
- **장애 시 세션 손실** — 그 서버만 죽으면 그 세션도 끝
- 외부 세션 스토어(Redis·DB)가 진짜 해법

### TA 권고

- **무상태 응용 + Redis 세션 스토어** = 최고
- 어쩔 수 없으면 Cookie Insert
- Source IP는 모바일 캐리어 NAT 환경 부적합

LB 솔루션 비교 — *F5 · Citrix · A10 · HAProxy · NGINX · KEMP · Radware*

| 솔루션                              | 형태          | 강점                                        | 일반 사용        |
|----------------------------------|-------------|-------------------------------------------|--------------|
| F5 BIG-IP LTM                    | 하드웨어/가상     | 시장 1위, iRules 강력, WAF(ASM)-DNS(GTM) 연계    | 국내 대기업·금융 표준 |
| Citrix NetScaler (NetScaler ADC) | 하드웨어/가상     | App Delivery + AAA-WAF, Citrix VDI 연계     | VDI 환경       |
| A10 Thunder                      | 하드웨어/가상     | 가성비, CGN-DDoS 우수                          | 통신사·증권기업     |
| Radware Alteon                   | 하드웨어/가상     | DDoS-SSL 강점                               | 보안 강조        |
| HAProxy                          | SW (OSS+상용) | 고성능·경량·세밀 제어                              | MSA·DC 내부    |
| NGINX / NGINX Plus               | SW (OSS+상용) | 웹서버 + LB + Caching                        | 웹·API GW     |
| KEMP LoadMaster                  | SW/하드웨어     | 중소규모 가성비, Exchange 친화                     | 중소·MS 스택     |
| AVI Networks (VMware NSX ALB)    | SW Defined  | DC SDN 통합                                 | NSX 환경       |
| 클라우드 LB                          | 관리형         | AWS ALB/NLB·Azure LB·GCP LB·NCP LB        | 클라우드         |
| K8s Ingress / Service Mesh       | SW (OSS)    | NGINX·Traefik·Istio·Contour·HAProxy·Envoy | MSA·컨테이너     |

한국 현장 단순화 — 금융·공공 대기업 = F5, 통신사 = A10/Radware, 신규 MSA = HAProxy/NGINX, VDI = NetScaler, K8s = NGINX Ingress-Istio.

🔧 실제 장비·UI 참조 (벤더 공식) - [F5 BIG-IP rSeries Hardware](#) — F5 공식 - [F5 BIG-IP Configuration Utility \(TMUI\)](#) / [iControl REST](#) — F5 TechDocs (관리 UI) - [Citrix NetScaler ADC](#) — NetScaler 공식 - [A10 Thunder ADC](#) — A10 공식 - [Radware Alteon](#) — Radware 공식 - [HAProxy Enterprise Console](#) — HAProxy 공식

PART G

GSLB — *Global Server Load Balancing · 사이트 간 분산*

한 LB로 단일 사이트, GSLB로 여러 사이트·국가 분산이 가능해진다.

# GSLB — 왜 필요한가

 **GSLB가 푸는 문제**

- 단일 LB로는 **단일 DC** 만 보호 — DC 통째 장애 시 모두 마비
- 글로벌 서비스에서 **사용자 가까운 사이트** 로 자동 라우팅 필요
- DR 시 **자동 DNS 절체** 필요 — 수동 변경 = 24~48시간 TTL

 **GSLB의 3가지 결정**

1. **헬스** — 어느 사이트가 살아있나
2. **위치** — 사용자에게 가까운 사이트
3. **부하** — 어느 사이트의 LB가 여유 있나 → 종합해서 **DNS 응답으로 IP를 다르게 반환**

 **구현 방식**

- **DNS 기반** (가장 흔함) — 도메인 질의에 위치/헬스에 따라 다른 A 레코드 반환
- **Anycast 기반** — 같은 IP를 여러 사이트가 BGP 광고, 라우팅이 최단 사이트로
- **HTTP Redirect** — L7에서 302로 위치 변경 (구식)

 **TA 메모**

- 한국 공공 단일국가 서비스도 **DR 자동 절체**용으로 GSLB 도입 일반화
- TTL을 짧게 (30~60초) 유지하는 것이 절체 시간 단축

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

33 / 64

#142

IT 인프라 아키텍처 설계 · Session 5 · 네트워크 고급 · VLAN-HA-NAT-LB-GSLB-망분리-NMS

F5 BIG-IP DNS (v17.1)

Authoritative DNS

portal.company.com IN A?

Seoul DC (KR · 203.0.113.10)

Tokyo DC (JP · 198.51.100.10)

Singapore DC (SG · 192.0.2.10)

Mumbai user

Sydney user

Health Check Probe Status

|                                      |                    |            |   |
|--------------------------------------|--------------------|------------|---|
| Seoul:                               | HTTPS GET /healthz | 32ms       | ✓ |
| 200 OK:                              |                    |            |   |
| Tokyo:                               | HTTPS GET /healthz | 41ms       | ✓ |
| 200 OK:                              |                    |            |   |
| Singapore:                           | HTTPS GET /healthz | timeout 3s | ✗ |
| (Failed 3/3 → Removed from DNS pool) |                    |            |   |

Topology LB → Fallback

Geo DNS (this diagram) vs Anycast BGP (8.8.8.8 / 1.1.1.1 style — same IP advertised from all sites via AS65000)

GSLB 다이어그램 (삼화)

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

34 / 64

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

page 71 / 160

## 헬스체크 · Active-Active · DR Failover

 **GSLB 헬스 체크**

- **ICMP Ping** — 가장 단순, 응용 무관
- **TCP Connect** — 포트 열림 여부
- **HTTP GET /health** — 응용 레벨
- **Scripted** — 특정 응답·DB 쿼리
- 보통 사이트당 여러종류 동시 검사
- 주기 30초·실패 3회 = 90초 절체

 **사이트 모드**

| 모드             | 특징                        |
|----------------|---------------------------|
| Active-Active  | 모든 사이트 동시 가동, 사용자 분산      |
| Active-Standby | 메인 사이트 우선, 장애 시만 보조       |
| Weighted       | 가중치로 비율 분배 (Canary·신규 DC) |

 **DR Failover 시나리오**

1. 메인 DC HTTP 헬스체크 실패
2. GSLB가 DR DC IP 반환 시작
3. 짧은 TTL(30~60초)에 따라 단말 DNS 캐시 만료
4. 새 요청은 DR DC로 → **2~5분 내 90% 절체**

 **TA 권고**

- **DR 사이트 사전 가동** (Warm/Hot) 권고 — Cold면 부팅 시간 추가
- 데이터 복제 RPO와 GSLB TTL 정합 확인
- **반기 1회 GSLB Failover 훈련** (Tabletop or 실제)

## GSLB 솔루션 — *F5 DNS · Citrix ITM · Akamai · Route 53*

| 솔루션                         | 형태        | 강점                                 | 일반 사용     |
|-----------------------------|-----------|------------------------------------|-----------|
| F5 DNS (구 GTM)              | 어플라이언스/가상 | LTM과 통합·iQuery로 LB 부하 인지           | 국내 대기업 표준 |
| Citrix ITM (NetScaler GSLB) | 어플라이언스    | NetScaler 환경                       | VDI 사이트   |
| A10 Thunder GSLB            | 어플라이언스    | 가성비                                | 통신사       |
| Infoblox NIOS DTC           | DDI 통합    | IPAM·DHCP·DNS 통합                   | 대기업       |
| Akamai GTM                  | 글로벌 SaaS  | 글로벌 PoP, 분석                        | 글로벌 서비스   |
| AWS Route 53                | 클라우드      | Health Check·Geo-Weighted-Failover | 클라우드      |
| Azure Traffic Manager       | 클라우드      | Performance·Priority-Weighted      | Azure     |
| Cloudflare Load Balancing   | 글로벌 SaaS  | 빠른 절체·Anycast                      | 글로벌 SaaS  |
| NS1 / NS-One                | 글로벌 SaaS  | 데이터 기반 라우팅                         | 핀테크       |

# PART H

## DHCP · Multicast · IPv6 — 주소·그룹·전환

자동 주소 할당, 그룹 통신, 차세대 주소 — 세 가지 핵심 인프라.

IT 인프라 아키텍처 설계 · Session 5 · 네트워크 고급 · VLAN-HA-NAT-LB-GSLB-망분리-NMS

## DHCP 복습 — Session 4 ↩ 참조 (DORA · Option · Snooping)

 **본문 참조** — DHCP DORA 4단계 흐름·Relay·Option 표·Snooping 보안은 **Session 4** **## DHCP - DORA 4단계** 슬라이드에서 본문급으로 다뤘다. 여기서는 한 줄 환기만 하고 망분리·DNS·QoS 로 진입한다.

### 한 줄 환기

- **DHCP** = IP·서브넷·GW·DNS·NTP 를 단말에 자동 분배 (수동 정적 IP 의 표준 대안)
- **DORA 4단계** = **D**iscover (Broadcast) → **O**ffer → **R**equest (Broadcast) → **A**ck, 같은 서브넷 한정 — 다른 서브넷은 **Relay (Option 82)**
- **자주 쓰는 옵션** = 1 (Mask) · 3 (GW) · 6 (DNS) · 15 (Domain) · 42 (NTP) · 43 (Vendor, AP Controller 자동 발견) · 51 (Lease) · 82 (Relay 정보) · 150 (IP Phone TFTP)
- **Lease 갱신** = T1 (50%) Unicast → T2 (87.5%) Broadcast → 만료 시 DORA 재시작
- **액세스 SW 보안 표준 세트** = **DHCP Snooping** (위조 서버 차단) + **DAI** (ARP 위조 차단) + **IP Source Guard** (Snooping 바인딩 외 차단)



# PART I

## 망분리 · DMZ — 물리·논리 분리, KISA 가이드

한국 공공·금융의 핵심 보안 요건. 인터넷망·업무망을 어떻게 나누는가가 설계의 절반.

IT 인프라 아키텍처 설계 · Session 5 · 네트워크 고급 · VLAN-HA-NAT-LB-GSLB-망분리-NMS

## 망분리 개요 — 왜·무엇을 분리하는가



### 망분리의 목적

- 인터넷 위협 차단 — 악성코드·랜섬웨어
- 개인정보 유출 방지 — 업무망 데이터가 인터넷으로 못 가게
- 법령 준수 — 정보통신망법·개인정보보호법·금융업 감독규정
- KISA 망분리 가이드(2013~) — 공공·금융 의무



### 분리 대상

- 인터넷망 — 외부 통신, 웹 브라우징, 메일 일부
- 업무망 (내부망) — 사내 시스템, 개인정보, 핵심 자료
- 일부는 개발망·운영망·DMZ 까지 추가 분리



### 2가지 큰 방식

| 방식      | 특징                             |
|---------|--------------------------------|
| 물리적 망분리 | 별도 PC·별도 NIC·별도 케이블·별도 SW      |
| 논리적 망분리 | 1대 PC·1대 SW + 가상화·VLAN·VDI로 격리 |



### TA 메모

- 금융권 = 물리적 망분리 기본 (전자금융감독규정)
- 공공 = 물리 또는 논리 (조직별)
- 일반 기업 = 논리 + DLP·EDR

## 물리적 망분리 — 2PC · 공용 PC · 전용 NIC

### 2 PC 방식

- 인터넷용 PC + 업무용 PC를 각각 별도
- 사용자 책상에 2대
- KVM 스위치로 모니터·키보드 공유 가능
- 가장 강한 분리, 가장 비싼 구축

### 공용 PC + 2 NIC

- 1대 PC, NIC 2장
- 사용자가 부팅 시 또는 SW로 모드 전환
- 동시 사용 불가
- 중간 보안 수준

### 전용 NIC + VLAN

- 1대 PC, NIC 2장 동시 운영 (인터넷 + 업무)
- 각 NIC가 다른 VLAN·다른 SW에 연결
- OS 라우팅 정책으로 트래픽 분리
- 편의성 ↑, 보안 ↓ (악성코드 한 OS에서 양쪽 접근 가능)

### TA 결정

- 금융 = 2PC 또는 가상화 망분리(VDI)
- 공공 = 2PC 또는 SBC(Server-Based VDI)
- 일반 기업 = 1PC + VDI 가상 환경

## 논리적 망분리 — SBC · CBC · VDI

### SBC (Server-Based Computing)

- 응용/세션을 서버에서 실행, 화면만 사용자 PC로 (RDP/ICA/HDX)
- 인터넷 영역을 서버 팜에 격리
- 사용자 PC = 단순 뷰어
- Citrix Virtual Apps and Desktops, Microsoft RDS

### CBC (Client-Based Computing)

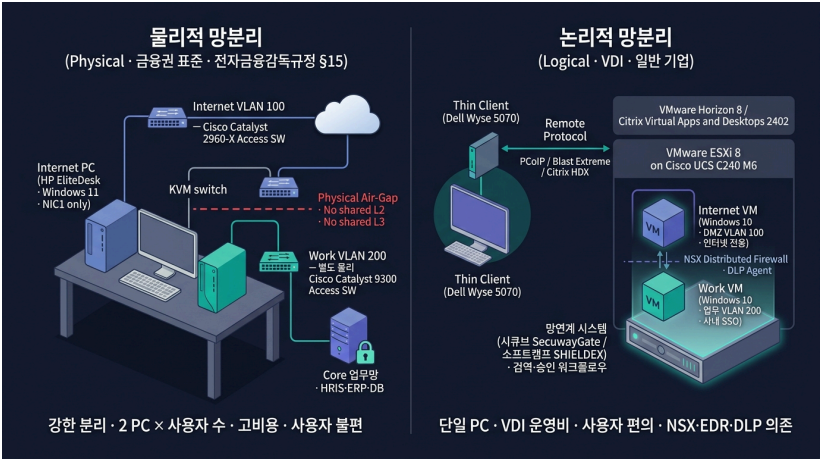
- 사용자 PC의 로컬 가상머신(VM/컨테이너) 으로 분리
- 한 PC 안에 인터넷용 가상 OS 별도
- 망간 자료 전송 제어
- 사례: 안랩, 시큐브 등 국내 솔루션

### VDI (Virtual Desktop Infrastructure)

- 사용자별 개인 가상 데스크톱을 DC에서 운영
- 사용자 PC는 Thin Client 또는 일반 PC + 클라이언트
- VMware Horizon · Citrix Virtual Desktops · Azure Virtual Desktop
- 인터넷용 VDI + 업무용 PC 조합으로 망분리

### TA 메모

- 신규 사업 = VDI 기반 논리 망분리 증가
- 5G/재택근무로 DaaS (Desktop as a Service) 도 검토



망분리 비교 (삽화)

## KISA 망분리 가이드 — 한국의 표준

### 📖 근거 법령·고시

- 개인정보보호법 제29조 (안전성 확보 조치 기준)
- 개인정보의 안전성 확보조치 기준 고시 — 100만명 이상 처리자, 망분리 의무
- 전자금융감독규정 제15조 — 금융회사 망분리 의무
- 정보통신기반보호법 — 주요정보통신기반시설
- 공공기관 망분리 가이드라인 (KISA)

### 🎯 KISA 권고 망분리 5단계

1. 외부 인터넷 차단
2. 외부 메일 서버 분리
3. 업무망 ↔ 인터넷망 물리/논리 분리
4. 망간 자료 전송 통제 시스템 도입
5. 운영·감사 로그 보존

### 📦 망간 자료 전송 시스템 (Data Diode-SecureUSB-NWStat)

- 망간 자료 이동 시 별도 검역망(Sandbox) 거쳐 악성코드 차단
- 일방향 게이트웨이 (Data Diode) — 하드웨어 강제 단방향
- 승인 기반 워크플로우
- 국내: 시큐브·소프트캠프·안랩·이니텍·이글로벌시스템

### 🗨️ TA 메모

- 망분리 설계 = 자료 전송 설계가 절반
- 모든 자료 이동 = 로그 + 감사관 승인

📖 참조 자료 (공식 가이드·국내 솔루션) - [KISA 정보보호 가이드](#) — KISA 공식 - [개인정보의 안전성 확보조치 기준 \(개인정보보호위원회\)](#) — 개인정보위 공식 - [전자금융감독규정 \(금융위·금감원\)](#) — 금융위 공식 - [시큐브 망연계 솔루션](#) — 시큐브 공식 - [소프트캠프 망간자료전송](#) — 소프트캠프 공식 - [Owl Cyber Defense Data Diode](#) — Owl 공식

DMZ 토폴로지 — *Single · Dual · 3-Tier*



Single Firewall DMZ

Internet - FW (3-leg) — DMZ (Web)  
└ Internal

- FW 1대에 인터넷·DMZ·내부 3개 인터페이스
- 가장 단순·저렴
- FW 1대 침해 = 전체 위험



Dual Firewall DMZ

Internet - FW1 - DMZ - FW2 - Internal

- 인터넷↔DMZ는 FW1, DMZ↔내부는 FW2
- 다른 벤더 FW 권고 — 동일 취약점 회피
- 한국 표준 구성



3-Tier DMZ

Internet - FW1 - Web Tier - FW2 - App Tier - FW3 - DB Tier

- 웹·앱·DB 3계층 분리
- 각 계층 사이 FW
- 대형 서비스·금융권



TA 결정

- 중소 = Single FW + L7 LB (HTTPS 중단)
- 일반 기업 = **Dual FW** (다른 벤더)
- 금융·대형 공공 = **3-Tier + WAF + IPS**
- DMZ 서버는 **NTP·DNS·로그**만 외부 허용

망간 자료 전송 — *NWStat · SecureUSB · 망연계*

| 솔루션 종류           | 동작                       | 사례                                               |
|------------------|--------------------------|--------------------------------------------------|
| 망연계 시스템          | 두 망 사이 게이트웨이로 파일 전송 + 검사 | 시큐브 SecuwayGate, 소프트캠프 SHIELDEX, 안랩 SafeTransfer |
| 검역망 (Sandbox)    | 외부에서 들어온 파일 자동 분석        | FireEye, Cisco AMP, 안랩 MDS                       |
| SecureUSB·세큐어디스크 | 인가 USB만 사용, 자동 암호화       | 마크애니, Cyberone                                   |
| DRM 전송           | 문서를 DRM으로 포장 전송          | 마크애니, Fasoo, 소프트캠프                               |
| 데이터 다이오드         | 하드웨어 단방향                 | Owl, Waterfall, 시큐레터                             |
| 메일 망연계           | 메일을 망간 전송 전용으로           | 별도 메일 SMTP 게이트웨이                                 |

한국 SI 현장의 통념: 망분리 도입 시 **망연계 시스템이 핵심 SW**. 자료 흐름 통제 + 감사 로그 + 백신 검역 + 승인 워크플로우를 한 솔루션에서.

# PART J

## SDN · Overlay · SD-WAN · MPLS — 현대 네트워크의 4가지 큰 그림

컨트롤 평면을 분리하고, 가상 네트워크를 오버레이로 띄우고, WAN을 소프트웨어로 제어한다.

IT 인프라 아키텍처 설계 · Session 5 · 네트워크 고급 · VLAN-HA-NAT-LB-GSLB-망분리-NMS

## SDN — *Software Defined Networking*



### SDN의 핵심

- **Control Plane** (라우팅 결정)과 **Data Plane** (패킷 포워딩) 분리
- 중앙 컨트롤러가 모든 SW에 **일관 정책** 푸시
- 네트워크를 **API로 제어**



### 표준 프로토콜

- **OpenFlow** (ONF) — 컨트롤러 ↔ 스위치 표준
- **NETCONF / YANG** — 설정 모델링
- **OpFlex** (Cisco) — ACI 표준
- **OVSDB** — Open vSwitch 관리



### SDN의 장점

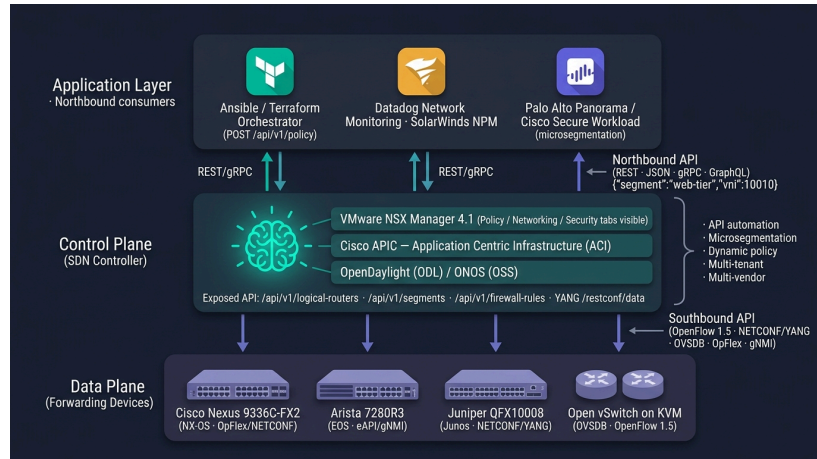
- **자동화** — API-CI/CD로 NW 변경
- **마이크로세그멘테이션** — 워크로드 단위 정책
- **동적 변경** — 트래픽·테넌트·앱별 최적화
- 멀티벤더 호환 (이론)



### 컨트롤러 솔루션

- **VMware NSX** (Network Virtualization) — DC SDN 1위
- **Cisco ACI** (Application Centric Infrastructure)
- **OpenDaylight (ODL)** — OSS 컨트롤러
- **ONOS** — OSS, 통신사 지향
- **Tungsten Fabric** (구 OpenContrail)

IT 인프라 아키텍처 설계 · Session 5 · 네트워크 고급 · VLAN-HA-NAT-LB-GSLB-망분리-NMS



SDN 아키텍처 (삽화)

# PART K

## NMS · 관찰성 — *SNMP · MIB · NetFlow* · 솔루션

측정되지 않는 것은 관리되지 않는다. NMS는 NW 운영의 시계·청진기·CCTV.

# SNMP — v1 · v2c · v3 비교

| 항목     | SNMPv1                | SNMPv2c               | SNMPv3 ★                       |
|--------|-----------------------|-----------------------|--------------------------------|
| 표준     | RFC 1157 (1990)       | RFC 1901~ (1993)      | RFC 3411~ (2002)               |
| 인증     | Community String (평문) | Community String (평문) | User-Based (USM) — Auth + Priv |
| 암호화    | ✗                     | ✗                     | AES-128/192/256                |
| 데이터 타입 | 기본                    | + Counter64 (대역폭)     | v2c + 보안                       |
| 메시지    | Get-GetNext-Set-Trap  | + GetBulk-Inform      | 동일 + 보안                        |
| 보안 등급  | 매우 낮음                 | 낮음                    | 고                              |
| 현재 권고  | 폐기                    | 폐기                    | 신규 표준                          |

SNMP v3 보안 모드 — - noAuthNoPriv: 인증·암호 모두 없음 - authNoPriv: 인증(MD5/SHA) 있고 암호 없음 - authPriv: 인증 + 암호 (AES) — 권장

# MIB · OID — SNMP 데이터 모델



## MIB (Management Information Base)

- 장비가 노출하는 관리 데이터 구조
- 트리 구조 — 각 노드에 OID 부여
- 표준 MIB + 벤더 MIB



## OID (Object Identifier)

- 점으로 구분된 숫자 시퀀스 (또는 이름)
- 예: 1.3.6.1.2.1.2.2.1.10 = ifInOctets (인터페이스 입력 바이트)
- 예: 1.3.6.1.2.1.2.2.1.16 = ifOutOctets (출력 바이트)



## OID 트리 주요 가지

```
1.3.6.1 iso.org.dod.internet
.1 directory
.2 mgmt
.1 mib-2 (표준 MIB)
.1 system
.2 interfaces
.4 ip
.6 tcp
.7 udp
.25 host
.4 private
.1 enterprises
.9 Cisco
.2636 Juniper
.12356 Fortinet
```



## TA 메모

- 표준 MIB-II로 거의 모든 NMS가 동작
- 벤더 MIB는 CPU·Temp·전원·팬 등 상세 정보

SNMP 동작 — *Get · GetNext · Set · Trap · Inform*



Polling (NMS → 장비)

- **Get** — 특정 OID 1개 조회
- **GetNext** — 트리 다음 OID
- **GetBulk (v2c+)** — 한 번에 다수 조회 (성능 ↑)
- **Set** — 값 변경 (예: 인터페이스 down)
- 보통 5~15분 주기 폴링



Push (장비 → NMS)

- **Trap (v1·v2c·v3)** — 비동기 이벤트 알림
- **Inform (v2c+)** — Trap + ACK (재전송 보장)
- 포트: NMS = **UDP 162**, 폴링은 **UDP 161**



자주 보는 Trap 종류

- coldStart · warmStart — 장비 부팅
- linkDown · linkUp — 인터페이스 상태
- authenticationFailure — 인증 실패
- 벤더 특정 — Fan·Temp·전원·HA 절체



TA 메모

- **Trap은 신뢰성 낮음 (UDP)** — 중요한 이벤트는 Inform 또는 Syslog 병행
- 폴링 주기는 **5분 표준** — 1분은 부하·30분은 너무 늦음
- v3 + Trap 함께 — 보안 + 이벤트

트래픽 분석 — *NetFlow · sFlow · IPFIX 비교*

| 프로토콜       | 표준               | 동작              | 정확도        |
|------------|------------------|-----------------|------------|
| NetFlow v5 | Cisco 독자 (1996)  | 전수 측정 (모든 패킷)   | 정확, CPU 부담 |
| NetFlow v9 | Cisco            | 샘플링 기반 가변       | 정확         |
| IPFIX      | IETF RFC 7011    | v9 표준화          | 정확, 벤더 중립  |
| sFlow      | InMon Foundation | 샘플링 (예: 1/1024) | 통계적, 저부하   |
| NetStream  | Huawei           | v5/v9 호환        | Cisco 호환   |



수집되는 정보 (Flow Record)

- 5-Tuple (Src/Dst IP·Port·Protocol)
- 입·출력 인터페이스 · TCP Flags · DSCP·ToS
- 시작·종료 시간 · 바이트·패킷 수 · AS 번호 (BGP)

한 줄 정리 — IPFIX는 NetFlow v9의 IETF 표준화 버전, sFlow는 샘플링 기반 저부하 솔루션. 운영 활용·샘플링 권고는 다음 페이지에서.



Flow 운영 활용 — 분석 도구 · TA 활용 · 결정 매트릭스



분석 도구

- SolarWinds NTA, PRTG, ManageEngine NetFlow Analyzer
- OSS: ntopng, Akvorado, GoFlow + ClickHouse
- 통신사: 자체 백엔드 (Kafka + Druid·ClickHouse)



TA 활용

- Top Talkers — 트래픽 점유 상위
- 이상 트래픽 탐지 — DDoS·내부 봇
- 회선 사용률 — 증설 결정
- 응용별 트래픽 — Office365·SAP·Backup
- 포렌식 — 침해 시 누가 어디로



결정 매트릭스

| 구간                | 권고 프로토콜            | 샘플링            |
|-------------------|--------------------|----------------|
| 엑세스·캠퍼스 (≤10G)    | NetFlow v9 / IPFIX | 전수             |
| DC 코어 (40G)       | IPFIX              | 1:100~1:1000   |
| DC 스파인·백본 (100G+) | sFlow 또는 IPFIX 샘플링 | 1:1000~1:10000 |
| WAN·인터넷 인입        | IPFIX + 자체 백엔드     | 전수 또는 1:100    |



운영 권고

- 단일 컬렉터 보다 NetFlow + sFlow 병행 — 정확도와 처리량의 균형
- TTL 단위로 보관(7일 원본 · 90일 집계 · 1년 KPI) 정책 합의



NMS 대시보드 (삽화)

# PART L

## 산출물·결정·정리 — 오늘 배운 것을 문서로

오늘 다룬 12개 PART를 산출물·결정 매트릭스로 묶는다.

IT 인프라 아키텍처 설계 · Session 5 · 네트워크 고급 · VLAN-HA-NAT-LB-GSLB-망분리-NMS

## TA의 NW 고급 설계 결정 10가지

| #  | 결정         | 후보                         | 권고 (전형)                              |
|----|------------|----------------------------|--------------------------------------|
| 1  | 게이트웨이 HA   | VRRP-HSRP-GLBP             | <b>VRRP (벤더 중립)</b>                  |
| 2  | 스위치 클러스터링  | Stack-vPC/MLAG             | 액세스 = Stack, DC = <b>vPC/MLAG</b>    |
| 3  | DC 백본 토폴로지 | 3-Tier vs Spine-Leaf       | <b>Spine-Leaf + EVPN-VXLAN</b>       |
| 4  | 멀티테넌트 격리   | VLAN vs VXLAN/EVPN         | 캠퍼스 = VLAN, DC = <b>VXLAN (EVPN)</b> |
| 5  | 로드 밸런서     | F5 vs HAProxy/NGINX vs A10 | 금융 = <b>F5</b> , MSA = HAProxy       |
| 6  | SSL 처리     | Term · Bridge · Pass       | 일반 = <b>Term + WAF</b>               |
| 7  | DR 자동화     | DNS 변경-GSLB                | <b>GSLB (TTL 30s)</b>                |
| 8  | 망분리 방식     | 물리 2PC vs VDI              | 금융 = 물리, 일반 = <b>VDI</b>             |
| 9  | DMZ 토폴로지   | Single vs Dual vs 3-Tier   | <b>Dual FW (다른 벤더)</b>               |
| 10 | NMS-트래픽 분석 | SNMP + NetFlow/sFlow       | SNMP v3 + <b>IPFIX</b>               |

## 네트워크 고급 산출물 — TA 8종



### 도면·표

1. **L2/L3 토폴로지 도면** — Visio/Lucidchart
2. **VLAN 표** — VID·이름·서브넷·GW·용도·담당
3. **IP 주소 계획 (IPAM)** — Subnet·할당·예약
4. **MLAG-VRRP 도메인 표** — 페어·Peer Link·VIP
5. **LB 정책서** — Pool·Member·Health·Persistence
6. **QoS 정책서** — DSCP·CoS·큐 매핑
7. **방화벽·DMZ 도면** + 정책 매트릭스
8. **망분리 도면** + 자료전송 SOP



### 정책·설계서



### 운영 산출물

9. **NMS 설계서** — 폴링·임계·알람 매트릭스
10. **장애 대응 SOP** — 시나리오별 절차
11. **변경관리 표준** — 변경 분류·검토·승인·롤백
12. **백업 설정 SOP** — 장비 설정 자동 백업



### TA 산출물 원칙

- 모든 도면 = **As-Is + To-Be + 마이그레이션** 3장
- 모든 정책 = **신청자·승인자·롤백 책임자** 명시
- **버전 관리** — Git or CMDB
- **반기 정기 갱신**

## VLAN 표 산출물 — 예시 템플릿

| VID | 이름          | 서브넷              | GW | 용도         | 담당 부서 | 비고             |
|-----|-------------|------------------|----|------------|-------|----------------|
| 10  | MGT-OOB     | 10.10.0.0/24     | .1 | 관리망 (OOB)  | NW팀   | SSH-NMS 전용     |
| 20  | SVR-WEB     | 10.20.0.0/24     | .1 | 웹 서비스      | 운영팀   | DMZ            |
| 30  | SVR-APP     | 10.30.0.0/24     | .1 | 응용 서비스     | 운영팀   | 내부             |
| 40  | SVR-DB      | 10.40.0.0/24     | .1 | DB         | DBA팀  | 내부, 제한 ACL     |
| 50  | BACKUP      | 10.50.0.0/24     | .1 | 백업망        | 운영팀   | Jumbo MTU 9000 |
| 100 | OFFICE-N    | 192.168.100.0/24 | .1 | 사무 (복관)    | 인사    | 사용자망           |
| 200 | VOICE       | 192.168.200.0/24 | .1 | IP 전화      | 통신팀   | LLDP-MED 자동    |
| 999 | NATIVE-NULL | (사용 안 함)         | -  | 보안용 Native | NW팀   | 운영 사용 금지       |

산출물 품질의 척도 — VID·서브넷·게이트웨이만 적힌 표는 "지도", **담당·용도·비고**까지 적힌 표가 "운영 매뉴얼".

LB 정책 산출물 — 예시 템플릿

| 서비스               | VS IP-Port       | Pool 멤버            | 알고리즘       | Health          | Persistence      | SSL        |
|-------------------|------------------|--------------------|------------|-----------------|------------------|------------|
| portal.company.kr | 203.0.113.10:443 | web01~web04:8080   | Least Conn | HTTP /health 5s | Cookie Insert    | Term + WAF |
| api.company.kr    | 203.0.113.11:443 | api01~api04:8080   | RR         | HTTP /health 5s | None (Stateless) | Term       |
| db-rw.internal    | 10.40.0.50:5432  | pg-master:5432     | (단일)       | TCP 10s         | -                | Pass       |
| db-ro.internal    | 10.40.0.51:5432  | pg-replica1~3:5432 | Least Conn | TCP 10s         | Source IP        | Pass       |
| mail.company.kr   | 203.0.113.20:25  | smtp01~smtp02      | RR         | TCP 30s         | None             | Pass       |



정책 추가 항목

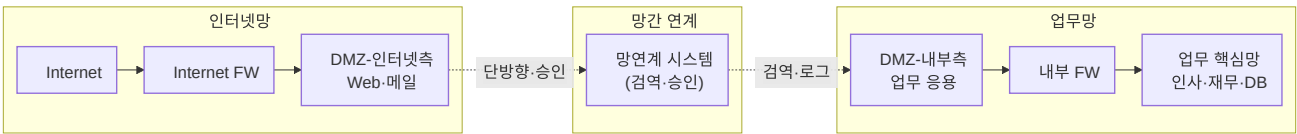
- 연결 한도 (Connection Limit)
- 세션 타임아웃 (Idle/Long)
- Rate Limit (DDoS 완화)
- 로깅 레벨
- 장애 시 동작 (Drop / Send 503)



TA 메모

- Pool 멤버 수 = N+1 이상
- 가중치는 사양 비율
- 헬스 체크는 **응용 + DB 점검** 엔드포인트
- SSL 인증서 만료 알람은 NMS·SIEM 연동

망분리 도면·산출물 — 예시 구성



산출물 5종

- 망분리 도면 (As-Is·To-Be)
- 자료 전송 SOP — 신청·검토·승인·기록
- 검역 정책 — 백신·샌드박스·콘텐츠 검사
- 사용자 가이드 — 메일·파일 전송 절차
- 감사 로그 보존 정책 — 3년 이상



TA 메모

- 망연계는 **단방향 + 승인 + 로그** 3종 세트
- 사용자 경험 = 절차 단순화 + 자동화
- 모의 침투·정기 감사 필수

## 한국 현장 토픽 — 체크리스트

### 한국 SI 특수성

- 망분리 의무 — KISA·금감원·개정법 매년 점검
- 공인 인증서·KISA 인증 솔루션 우선
- 이중화·HA 강조 — N+1 기본
- 국산 솔루션 가산점 — NMS·LB·망연계
- 공공 = 단방향 게이트웨이 사례 다수
- 금융 = 물리 2PC + DRM 표준

### 벤더 매트릭스 (현장 친숙도)

- LB = F5 압도적, A10·HAProxy 증가
- NMS = SolarWinds + 국산 (다산데이타·VCNC·다인스)
- 망연계 = 시큐브·소프트캡프·안랩·이니텍

### RFP·제안 시 자주 묻는 표준

- ISMS-P 적합성
- CC 인증 / 보안기능 확인서
- KCMVP 암호 모듈
- IPv6 지원 (의무화)
- BGP·OSPF 라우팅 자격
- GSLB 동시 다중 사이트
- 망분리·DMZ 도면 + 자료 전송 정책

### TA 메모

- 한국 사업의 90%는 위 체크리스트 안에서 답을 찾는다
- 신규 사업도 레거시 호환을 함께 다룬다 (혼합 운영 가이드)

## 핵심 키워드 — 시험·면접 대비

### A·C·D

- 802.1Q · Native VLAN
- Trunk · Access
- Private VLAN (Isolated-Community)
- Voice VLAN
- VLAN Hopping · DTP
- STP · RSTP · MSTP
- BPDU/Root/Loop Guard
- Stack · vPC · MLAG
- VRRP · HSRP · GLBP · CARP
- ECMP · Per-Flow Hash

### E·F·G·H

- Static NAT · PAT · Hairpin
- NAT64 · DNS64
- STUN · TURN · ICE
- DSCP · CoS · EF · AF
- LLQ · CBWFQ
- Policing vs Shaping
- L4 vs L7 LB
- Least Conn · Source Hash
- SSL Termination · Bridging · Pass-through
- Active vs Passive Health
- Cookie Persistence
- GSLB · Active-Active · DR Failover
- DHCP DORA · Option 82
- IPv6 SLAAC · Dual-Stack

### I·J·K

- 물리 망분리 · 논리 망분리
- VDI · SBC · CBC
- KISA 가이드
- DMZ Single/Dual/3-Tier
- 망연계 시스템
- SDN · OpenFlow · NETCONF
- VMware NSX · Cisco ACI
- VXLAN · VNI · VTEP
- EVPN-VXLAN
- SD-WAN
- SNMP v3 · MIB · OID
- NetFlow · sFlow · IPFIX
- Trap · Inform

IT 인프라 아키텍처 설계

# Session 6

## 스토리지 · 백업 · DR

Day 2 오후 · 약 180분

6대 스토리지 유형 · SAN 패브릭 · RAID · Snapshot · Tape · 백업 정책 · 랜섬웨어 대응 · DR 4단계

강사 박수현 ·  젠아이랩스(GenAI Labs)

데이터센터 · 서버·OS·DB·GPU · 가상화·컨테이너 · 네트워크 L1~L7 · 스토리지 · 백업·DR · 보안 6대 도메인 · HA · 용량·성능·관찰성 · 설계 워크숍 · RFP · 5종 실전 케이스

IT 인프라 아키텍처 설계 · Session 6 · 스토리지 · 백업 · DR

## 왜 스토리지·백업·DR인가 — 국내 백업 실패·랜섬웨어 3선



### ① 서울대병원 환자정보 83만건 유출

2021.06 (북한 해킹조직)

서울대병원 서버 해킹 → 환자 81만 명 + 직원 1만 7천명 정보 유출 (북한 해킹조직 소행 확정).

- 의료 업종 보안 투자 8개 산업군 중 최저
- 진료정보·주민번호·진단명
- 의료데이터는 다크웹 고가 거래

💡 교훈 — Air-Gap-Immutable Backup-SIEM-SAC + 의료 망 분리

참고: 「서울대병원 환자정보 유출 2021」 검색



### ② SK C&C 화재 → DR 미흡

2022.10.15 (재인용)

판교 DC 화재 + 카카오의 DR 사이트 동기화 지연 → 복구가 5일 걸린 핵심 원인.

- DR 안 시 데이터 동기화 미흡
- BCP 시험 부족
- RPO-RTO 사전 정의 부재

💡 교훈 — 3-2-1-1-0 백업 + DR 분기 시험 + Sync/Async 복 제 설계

참고: 「카카오 IDC 이중화 보고서」 검색



### ③ 2025 국가정보자원관리원 화재

2025.09.26 (금)

대전 본원 화재 → 정부 시스템 709개 마비 · 4주+ 복구. DR 사이트 미흡으로 96개 시스템을 대구 센터로 「긴급 이전 복구」.

- 정부 IT의 DR-이중화 부재 노출
- 운영-DR 동시 영향 (단일 사이트 의존)
- 복구 시험 미실시
- 「공공 IT BCP 점검」 의무화 추진

💡 교훈 — 3-2-1-1-0 + Sync/Async 복제 설계 + 분기 1회 복구 시험

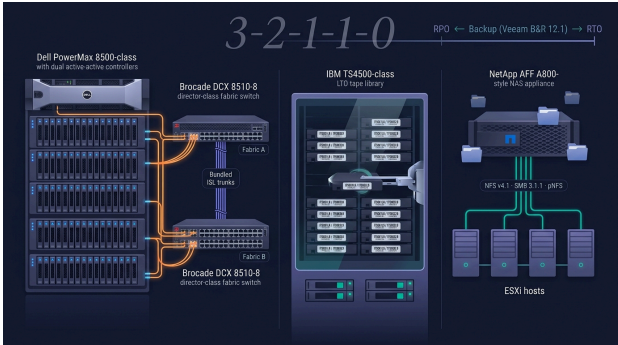
참고: 위키백과 「2025년 국가정보자원관리원 화재」

🔥 이번 세션의 시각 — 위 3건은 「랜섬웨어 → 백업까지 같이 암호화」「DR 동기화 미흡」「복구 시험 누락」 패턴. 3-2-1-1-0 + Immutable Backup + RPO/RTO 정량화가 본 세션의 핵심.

3-2-1-1-0 — 백업 황금 원칙(2024+)

- 3 — 데이터 사본 3벌 (운영 1 + 백업 2)
- 2 — 서로 다른 저장 매체 2종 (Disk + Tape·Cloud 등)
- 1 — 1벌은 사외 (Offsite·다른 사이트·Cloud)
- +1 — 1벌은 Offline / Air-Gap / Immutable (랜섬웨어 무력화 방지)
- +0 — 검증 오류 0건 (SureBackup·이상탐지로 무결성 확인)

"검증되지 않은 백업은 존재하지 않는 백업" — Veeam·Rubrik·Cohesity가 사실상의 표준으로 만든 확장판.



Day 2 오후 · 약 180분

회차 메타데이터 — Session 6 한눈에

세션 정보

- 회차: 7 / 18 — Day 2 오후
- 소속: 스토리지·백업·DR 통합 도메인
- 카테고리: 인프라 / 데이터 보호
- 예상 분량: 본문 70 슬라이드 + 일러스트 11장
- 강의 시간: 약 90분
- 강사: 박수현 — 젠아이랩스(GenAI Labs) CEO / CTO

핵심 메시지

"데이터는 어디에·어떻게 저장되며, 어떻게 보호하고, 사라졌을 때 어떻게 되살리는가" — 스토리지·백업·DR 의사결정의 압축 정리.

학습 목표 (Learning Objectives)

1. 6대 스토리지 유형 — DAS·NAS·SAN·Object·HCI·SDS를 워크로드별로 매핑한다
2. SAN 패브릭 — Director·Edge·Zoning·NPV·WWN의 동작 원리를 설명한다
3. RAID·Snapshot·Replication — 안전망 3중 구조를 설계한다
4. Tape·LTO·LTFS·VTL — 장기 보존·랜섬웨어 대응의 마지막 방어선을 안다
5. 백업 정책 6종 — Full·Inc·Diff·Synthetic·Forever·Reverse를 비교한다
6. 3-2-1-3-2-1-1-0-Immutable — 랜섬웨어 시대 백업 황금 원칙을 설계한다
7. DR 4단계·RPO/RTO — 사이트 등급과 비용·가용성을 산정한다

# PART A

## 스토리지 6대 유형 — *DAS · NAS · SAN · Object · HCI · SDS*

한 줄로 정리: 블록은 **SAN·HCI**, 파일은 **NAS**, 객체는 **Object**, 단일서버는 **DAS**, 소프트웨어 정의는 **SDS**.

IT 인프라 아키텍처 설계 · Session 6 · 스토리지 · 백업 · DR

## 스토리지 6대 유형 — *전체 조망 wheel*

### 1 DAS

- **Direct Attached**
- SAS/SATA 케이블 직결
- 단일 서버 전용
- 가장 단순·빠름·저렴

### 2 NAS

- **Network Attached**
- Ethernet + NFS-SMB
- 다수 클라이언트 파일 공유
- 홀디랙·미디어·백업타겟

### 3 SAN

- **Storage Area Network**
- FC-iSCSI-NVMe-oF
- 블록 단위 공유
- DB-VM-미션크리티컬

### 4 Object

- **HTTP REST + S3 API**
- 무한 확장·메타데이터
- WORM·버저닝·Object Lock
- 백업·아카이브·CDN 오리진

### 5 HCI

- **Hyper-Converged**
- Compute + Storage + NW 통합
- vSAN-Nutanix-VxRail
- VDI·중규모 가상화

### 6 SDS

- **Software-Defined Storage**
- 범용 HW + 소프트웨어
- Ceph-GlusterFS-Lustre
- 비용·확장성 우선

**결정 한 줄 요약:** 워크로드의 **공유 단위**(블록·파일·객체)와 **운영 모델**(어플라이언스·HCI·SDS·Object)가 6대 유형을 가른다.





스토리지 6대 유형 — 전체 조망 wheel

## ① DAS — 서버 안의 디스크, 가장 단순한 형태

### 🔧 구성

- 서버 내장 디스크 베이 (2.5"/3.5")
- **RAID 컨트롤러** + 캐시 + BBU/Flash 백업 모듈
- **JBOD** (Just a Bunch Of Disks) 외장 enclosure 연결
- 연결: **SAS** (12Gbps-24Gbps) · **SATA** (6Gbps) · **NVMe** (PCIe Gen4/5)

### 🔌 SCSI 계보

- **SCSI** (전통 Parallel SCSI)
- **SAS** (Serial Attached SCSI) — 12G-24G
- **SATA** (Serial ATA) — 6G
- **NVMe** (Non-Volatile Memory express) — PCIe 직결

### ✅ 적합한 용도

- 단일 서버 워크로드 (Web-WAS)
- 부팅 디스크·로컬 캐시
- 가성비·단순 운영 우선
- 공유가 불필요한 데이터
- AI 학습 데이터 로컬 캐싱 (NVMe)

### ⚠️ 한계

- 공유·이중화 어려움
- Live Migration 불가 (단일 노드 종속)
- 디스크 장애 = 서버 장애
- 확장성 낮음

**TA 시각:** DAS는 "없으면 안 되지만, 거기서 멈춰서는 안 되는" 가장 기본 옵션. **부팅 디스크 = DAS RAID 1**이 표준 패턴.

② NAS — 파일 단위 공유 · NFS와 SMB의 두 축



NFS (Network File System)

- **Unix·Linux** 표준 파일 공유
- **v3** — 무상태, UDP/TCP, 가장 보편
- **v4** — 상태 유지, TCP만, 보안 강화 (Kerberos), ACL
- **v4.1** — pNFS (병렬 액세스), 세션 multipathing
- **v4.2** — Server-side copy, sparse file



SMB / CIFS (Server Message Block)

- **Windows** 표준 파일 공유
- **SMB 1.0 / CIFS** — 구식, 보안 취약 (비활성화 권장)
- **SMB 2.x** — Win Vista·2008, 효율 개선
- **SMB 3.x** — Win 2012+, 암호화·Multichannel·Direct (RDMA)



비교 매트릭스

| 항목           | NFS v4.1      | SMB 3.x          |
|--------------|---------------|------------------|
| 주 OS         | Unix·Linux    | Windows          |
| 인증           | Kerberos-sys  | NTLM·Kerberos-AD |
| 암호화          | TLS·Kerberos  | 내장 AES-128/256   |
| Multichannel | pNFS          | SMB Multichannel |
| RDMA         | NFS over RDMA | SMB Direct       |
| 잠금           | byte-range    | 강력한 oplock       |



선택 기준

- 운영 서버군 = **NFS** (홀디렉·App 데이터)
- 사무용 PC 공유 = **SMB** (AD 통합)
- 혼용 환경 = **NetApp·TrueNAS** 멀티프로토콜

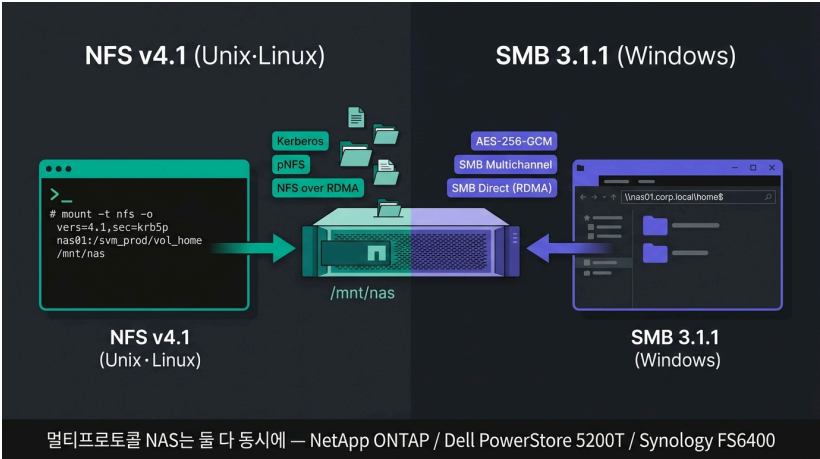
NAS 솔루션 — 2026 현장 표준

| 솔루션                         | 분류            | 강점                               | 주 사용자      |
|-----------------------------|---------------|----------------------------------|------------|
| NetApp ONTAP                | 엔터프라이즈        | SnapMirror·SnapVault·멀티프로토콜·중복제거 | 금융·공공·대기업  |
| Dell EMC Unity / PowerStore | 엔터프라이즈        | 통합 SAN+NAS·Tiering·Inline Dedup  | 대기업·공공     |
| Dell PowerScale (Isilon)    | Scale-Out NAS | 단일 네임스페이스·수십 PB                  | 미디어·HPC·AI |
| IBM Storage Scale (GPFS)    | 분산 파일시스템      | 초고성능·병렬                          | HPC·연구소    |
| Hitachi (HNAS)              | 엔터프라이즈        | FPGA 가속·고성능                      | 통신·제조      |
| Synology DSM                | SOHO·중소       | 가성비·DSM UI·앱 생태                  | 중소·연구실·홈   |
| QNAP QTS                    | SOHO·중소       | 확장 모듈·가상화                        | 중소·콘텐츠     |
| TrueNAS (iXsystems)         | 오픈소스+상용       | ZFS 기반·OpenZFS                   | 미디어·중소     |
| OpenZFS                     | 오픈소스          | CoW·Snapshot·Send/Receive        | 자가 구축      |

국내 도입 패턴: 금융·공공 핵심 = NetApp / Dell, 대용량 분석·미디어 = Isilon, 중소 = Synology·QNAP.



실제 장비·UI 참조 (벤더 공식) - [NetApp AFF / FAS 시리즈](#) — NetApp 공식 - [NetApp ONTAP System Manager](#) — NetApp Docs (관리 UI) - [Dell PowerStore](#) — Dell 공식 - [Dell PowerScale \(Isilon\)](#) — Dell 공식 - [Synology DiskStation](#) — Synology 공식



NAS 삽화

### ③ SAN — 블록 단위 · FC와 IP SAN의 진화

#### FC (Fibre Channel)

- 전용 광 패브릭, 가장 안정적
- 세대별 속도:
  - 4 Gbps (2003)
  - 8 Gbps (2008)
  - 16 Gbps (2011)
  - 32 Gbps (2016)
  - 64 Gbps (Gen 7, 2019)
  - 128 Gbps (Gen 8, 2025+)
- BB Credit-CRC-In-Order Delivery 보장
- WWN-WWPN 식별자

#### iSCSI

- IP 위에 SCSI 캡슐화
- 이더넷 + TCP 사용 (저비용)
- IQN 식별자 ( `iqn.YYYY-MM.com.example:host` )
- 10G-25G-100G NIC + DCB/PFC

#### FCoE (Fibre Channel over Ethernet)

- FC 프레임을 이더넷에 캡슐화
- Lossless DCB 필요 (PFC-ETS)
- 2010년대 중반 → 2020년대 쇠퇴
- NVMe/TCP-NVMe/RoCE로 대체

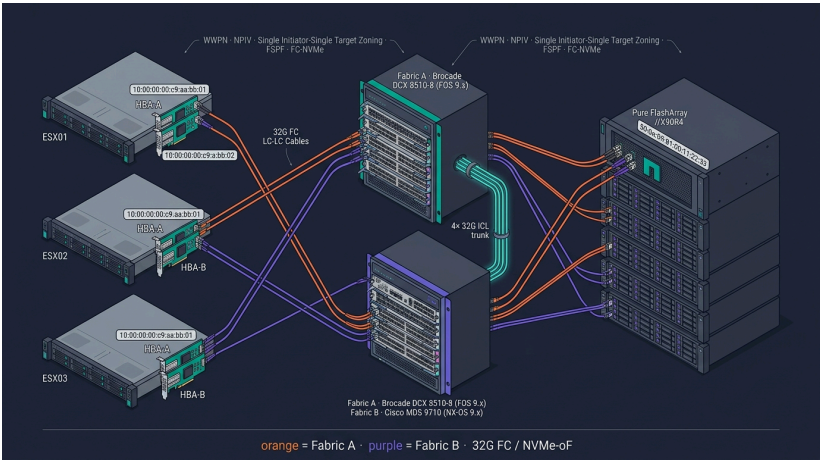
#### NVMe-oF (NVMe over Fabrics)

- 차세대 SAN 표준
- 변종:
  - NVMe/FC — 기존 FC 패브릭 활용
  - NVMe/TCP — TCP 위 (저비용)
  - NVMe/RoCE — RDMA over Ethernet
  - NVMe/IB — InfiniBand (HPC)
- 지연 < 100μs, IOPS 수백만

#### 비교 한 줄

- FC = 안정·고가, iSCSI = 저비용, NVMe-oF = 차세대

 실제 장비 참조 (벤더 공식) - [Brocade \(Broadcom\) X7 Director](#) — Broadcom 공식 - [Brocade G730 / G720 Edge Switch](#) — Broadcom 공식 - [Cisco MDS 9710 / 9706 Director](#) — Cisco 공식 - [Cisco MDS 9148T / 9396V](#) — Cisco 공식 - [Fibre Channel 표준 개요](#) — Wikipedia



SAN 패브릭 토폴로지 삽화

④ Object Storage — S3 API의 세계

📦 Object Storage 특징

- 버킷 → 객체 2단 구조 (디렉터리 없음)
- HTTP REST API (S3-Swift)
- 메타데이터 풍부 — 사용자 정의 가능
- 무한 확장 — 수십 PB-수십 억 객체
- WORM-버저닝-Object Lock — 랜섬웨어 대응
- Erasure Coding 일반적 (RAID 대체)

🏠 적합한 워크로드

- 백업-아카이브 (장기 보존)
- 로그-이벤트 저장
- 미디어 (이미지-동영상)
- CDN 오리진
- 데이터 레이크-AI 학습 데이터셋
- 정적 웹 콘텐츠

🏆 주요 솔루션

| 솔루션                 | 분류      | 특징               |
|---------------------|---------|------------------|
| AWS S3              | 퍼블릭     | de facto 표준 API  |
| Azure Blob          | 퍼블릭     | 호환 SDK           |
| OpenStack Swift     | 오픈소스    | OpenStack 생태     |
| Ceph RGW            | 오픈소스    | S3-Swift 둘 다     |
| MinIO               | 오픈소스+상용 | 경량-고성능 S3        |
| Cloudian HyperStore | 상용      | 엔터프라이즈 S3 어플라이언스 |
| Scality RING        | 상용      | 대용량-SDS          |
| NetApp StorageGRID  | 상용      | 멀티사이트-메타 강력      |

🔒 핵심 기능

- Object Lock (Compliance-Governance 모드)
- 버저닝 — 이전 버전 보존
- 수명 주기 정책 — Hot→Cold→삭제

🏠 실제 솔루션-UI 참조 (벤더 공식) - [AWS S3](#) — AWS 공식 - [NetApp StorageGRID](#) — NetApp 공식 - [Dell EMC ECS \(Elastic Cloud Storage\)](#) — Dell 공식 - [MinIO Enterprise Object Store](#) — MinIO 공식 - [Ceph](#) — Ceph 공식 - [Cloudian HyperStore](#) — Cloudian 공식

⑤ HCI — Hyper-Converged Infrastructure

🏠 HCI란

- Compute + Storage + Network을 한 노드에 통합
- 노드 추가만으로 수평 확장
- 전용 SAN 패브릭 없음 (이더넷만)
- 단일 UI로 통합 관리
- VDI-중소 가상화의 사실상 표준

🔧 핵심 아이디어

- 각 노드의 로컬 디스크를 분산 스토리지 풀로 묶음
- 데이터 복제 (Replica 2-3) 또는 Erasure Coding
- 메타데이터-캐시는 SSD-NVMe

🏆 주요 솔루션 비교

| 제품                  | 분류          | 특징                         |
|---------------------|-------------|----------------------------|
| VMware vSAN         | SW + 인종 HW  | vSphere 통합-시장 1위           |
| Nutanix             | SW + 어플라이언스 | Prism UI-AHV 자체 hypervisor |
| Dell VxRail         | 어플라이언스      | vSAN 기반 검증 HW              |
| HPE SimpliVity      | 어플라이언스      | Dedup 가속 카드 내장             |
| Cisco HyperFlex     | 어플라이언스      | UCS 통합                     |
| Azure Stack HCI     | SW (MS)     | S2D + Hyper-V              |
| Scale Computing HC3 | 어플라이언스      | 중소-엣지                      |

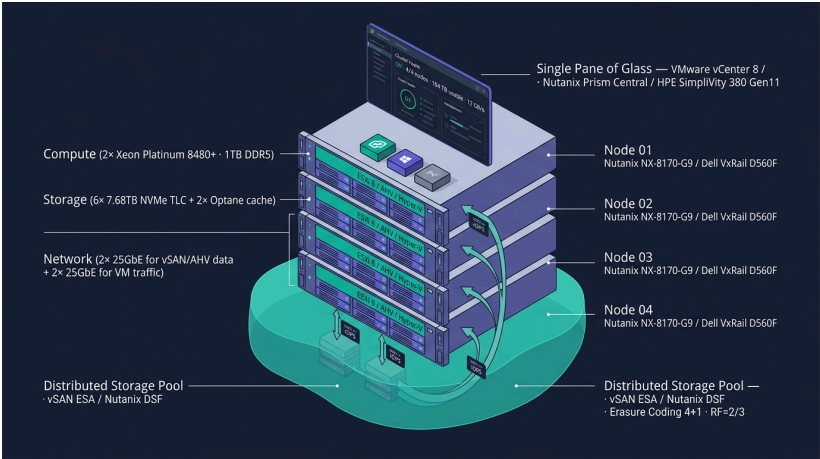
✅ 장점

- 운영 단순화 (단일 UI)
- 빠른 도입 (수일~수주)
- 노드 단위 확장
- 백업-DR 통합 솔루션 풍부

⚠️ 한계

- 대규모 분리 확장(컴퓨트만/스토리지만) 어려움
- 라이선스 비용 (vSAN-Nutanix)
- 특정 워크로드(초대용량 DB)에서는 SAN 우위

🏠 실제 솔루션-UI 참조 (벤더 공식) - [VMware vSAN](#) — VMware 공식 - [Nutanix Prism \(관리 UI\)](#) — Nutanix 공식 - [Dell VxRail](#) — Dell 공식 - [Cisco HyperFlex](#) — Cisco 공식 - [Microsoft Azure Stack HCI](#) — Microsoft 공식



HCI 아키텍처 삽화

## ⑥ SDS — *Software-Defined Storage*

### 💡 SDS란

- 범용 x86 서버 + 디스크 위에 **소프트웨어**가 스토리지 기능 제공
- 벤더 종속 탈파·비용 절감
- 블록·파일·객체 통합 가능
- 클러스터로 확장

### 🏆 주요 솔루션

- Ceph** — 블록(RBD)·파일(CephFS)·객체(RGW) 통합, 오픈소스 최강
- GlusterFS** — 분산 파일시스템, Red Hat 인수
- Lustre** — HPC 병렬 파일시스템, 슈퍼컴퓨터 표준
- BeeGFS** — HPC·AI 학습용
- DRBD** — 블록 레벨 복제 (HA Pair)
- Storage Spaces Direct (S2D)** — MS Windows Server

### vs SDS vs 어플라이언스

| 항목    | SDS         | 어플라이언스 |
|-------|-------------|--------|
| HW    | 범용 (선택 자유)  | 인종 모델  |
| 비용    | 낮음 (HW만)    | 높음     |
| 운영    | 자체 책임       | 벤더 지원  |
| 성능 튜닝 | 자유롭게        | 벤더 한정  |
| 적합 규모 | 중대형 (전담 인력) | 전 규모   |

### 🎯 SDS가 빛나는 곳

- HPC·AI 학습 (Lustre·BeeGFS)
- 대용량 백업·아카이브 (Ceph RGW)
- 클라우드 오픈소스 인프라 (Ceph + OpenStack)
- 비용 절감 정책이 강한 공공·연구

### ⚠️ 운영 부담

- 노드 장애·재구축·확장이 전부 자체 책임
- 사고 시 벤더 책임 한정적

## 6대 유형 비교 매트릭스 — 한 페이지 결정표

| 항목      | DAS           | NAS             | SAN              | Object                 | HCI          | SDS                |
|---------|---------------|-----------------|------------------|------------------------|--------------|--------------------|
| 공유 단위   | 블록            | 파일              | 블록               | 객체                     | 블록           | 블록·파일·객체           |
| 프로토콜    | SAS·SATA·NVMe | NFS·SMB         | FC·iSCSI·NVMe-oF | S3·Swift               | 자체 분산        | 자체 + 표준            |
| 성능      | 최고 (직결)       | 중               | 매우 높음            | 중~높음                   | 높음           | 가변                 |
| 확장성     | 낮음            | 중               | 높음               | 최고                     | 높음 (노드 단위)   | 최고                 |
| 공유 범위   | 1대            | 다수 클라이언트        | 다수 호스트           | 무제한 (HTTP)             | 클러스터 내       | 클러스터 내             |
| 비용      | 낮음            | 중               | 높음               | 낮음~중                   | 중~높음         | 낮음 (HW만)           |
| 운영 난도   | 낮음            | 낮음              | 높음               | 중                      | 중 (단일 UI)    | 높음                 |
| 대표 워크로드 | 부팅·캐시         | 홈랙·미디어·백업       | DB·VM            | 백업·아카이브·AI             | VDI·중소 가상화   | HPC·대용량            |
| 대표 솔루션  | 서버 내장         | NetApp·Synology | EMC·NetApp·HDS   | MinIO·Ceph·StorageGRID | vSAN·Nutanix | Ceph·Lustre·BeeGFS |

**결정 한 줄:** "어떤 공유 단위·어떤 운영 모델인가" 두 축이 6대 유형을 가른다.

# PART B

## RAID + 데이터 경로 — 디스크 묶음과 경로 이중화

RAID는 디스크 결함의 안전망, Multipath는 경로 결함의 안전망.

## RAID 0·1·5·6·10·50·60·DP — 비교 매트릭스

| RAID             | 최소 디스크 | 용량 손실 | 결합 허용    | 읽기 | 쓰기   | Rebuild | 용도        |
|------------------|--------|-------|----------|----|------|---------|-----------|
| 0 Stripe         | 2      | 없음    | 0        | 최고 | 최고   | 불가      | 캐시·임시     |
| 1 Mirror         | 2      | 50%   | 1        | 빠름 | 보통   | 빠름      | OS·소용량 중요 |
| 5 Parity         | 3      | 1 디스크 | 1        | 보통 | 느림   | 매우 느림   | 구식·소용량    |
| 6 Dual Parity    | 4      | 2 디스크 | 2        | 보통 | 더 느림 | 느림      | 대용량 표준    |
| 10 Mirror+Stripe | 4      | 50%   | 1 디스크/그룹 | 최고 | 빠름   | 빠름      | DB·고성능    |
| 50               | 6      | 그룹별 1 | 그룹별 1    | 빠름 | 중    | 중       | 대용량 + 성능  |
| 60               | 8      | 그룹별 2 | 그룹별 2    | 빠름 | 중    | 중       | 대용량 + 내결함 |
| DP (NetApp)      | 4      | 2 디스크 | 2        | 보통 | 보통   | 빠름      | NetApp 전용 |

### RAID 5가 사라지는 이유 (URE 문제)

- HDD 용량 증가 (수 TB~수십 TB)
- Rebuild 중 다른 디스크 URE(Unrecoverable Read Error) 확률 ↑
- 8TB HDD 4개 RAID 5 → Rebuild 중 실패 확률 비현실적으로 높음
- → **RAID 6** 또는 **RAID 60** 권장

"RAID는 백업이 아니다" — 디스크 고장에는 강하지만 사용자 실수·랜섬웨어에는 무력.

## Hot Spare · Rebuild — 재구성의 시간 싸움

### Hot Spare

- 정상 동작 중인 대기 디스크
- 장애 발생 시 즉시 자동 재구축 투입
- **Global Hot Spare** — 전 그룹 공유
- **Dedicated Hot Spare** — 특정 그룹 전용
- 권고: **그룹당 1개 + Global 1개**

### Rebuild Time 예시

- 1TB SAS HDD RAID 6 → 수 시간
- 8TB SATA HDD RAID 6 → **24~48시간**
- 18TB HDD RAID 6 → **수 일** ⚠️
- SSD/NVMe → 빠름 (수십 분)
- 운영 IO 부하 + Rebuild = 성능 저하

### Drive Failure Rate

- AFR (Annualized Failure Rate)
- Backblaze 공개 데이터:
- Enterprise HDD: 0.5~1.5%/년
- Consumer HDD: 1.5~3%/년
- Enterprise SSD: 0.2~0.7%/년
- 디스크 100개 운영 시 = 연 1~3개 교체 필요

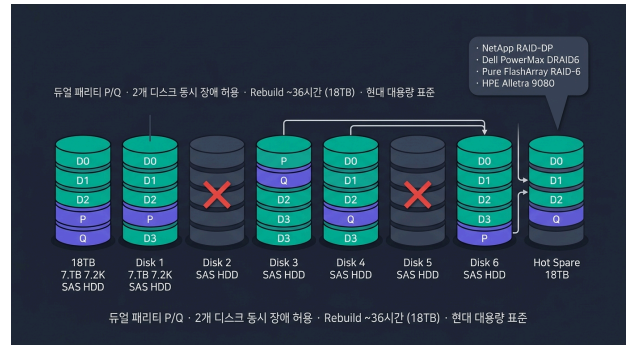
### Rebuild 위험 완화

- **RAID 6** 또는 **Triple Parity** 적용
- **Erase Coding** 도입 (Object-SDS)
- **Rebuild 우선순위 정책** — 운영 부하 시간 회피
- Hot Spare 사전 확보
- 정기 **Scrub** (Patrol Read) — 잠재 오류 사전 발견



## RAID 6 — 듀얼 패리티 P/Q

- **N+2 디스크** 구성 (데이터 N + 패리티 2)
- 두 패리티 **P (XOR) + Q (Reed-Solomon)** 를 디스크 전체에 **분산** 저장
- **2개 디스크 동시 장애**까지 데이터 보존
- Rebuild 중 추가 1개 장애도 견딤 → **대용량 HDD 시대 표준**
- 쓰기 페널티 6배(읽기 2+쓰기 2 = 패리티 갱신)
- 적합: 18TB+ HDD·대용량 NAS·아카이브
- 벤더: NetApp RAID-DP · Dell PowerMax DRAID6 · Pure RAID-6 · HPE Alletra 9080



RAID 6 단면도 — 분산 P/Q 패리티 + Hot Spare Rebuild

# PART C

## 고급 스토리지 기능 — *Snapshot · Replication · Dedup · Tiering · QoS*

디스크 박스가 아니라 **소프트웨어 기능**이 곧 엔터프라이즈 스토리지의 가치.

## Snapshot — CoW와 RoW 두 가지 방식

### CoW (Copy-on-Write)

- Snapshot 시점에 **원본 데이터 위치 그대로 유지**
- 변경 발생 시: **이전 데이터를 별도 영역에 복사** → 그 후 원본 덮어쓰기
- 읽기 성능 우수, **쓰기 성능 저하** (1회 쓰기 = 1읽기 + 1쓰기 + 1쓰기)
- 채택: 전통 SAN (Dell EMC·HPE·일부 IBM)

### RoW (Redirect-on-Write)

- Snapshot 시점부터 **새 쓰기를 새 위치에 기록**
- 원본 블록은 변경되지 않음
- **쓰기 성능 우수** (1회 쓰기 = 1쓰기)
- 메타데이터 관리 복잡 (가비지 컬렉션)
- 채택: NetApp WAFL·ZFS·대부분 현대 시스템

### Clone

- Snapshot을 **읽기·쓰기 가능한 새 볼륨**으로 노출
- 처음엔 원본 공유, 변경분만 별도
- DB 테스트·개발 환경 신속 복제에 활용

### Snapshot의 한계

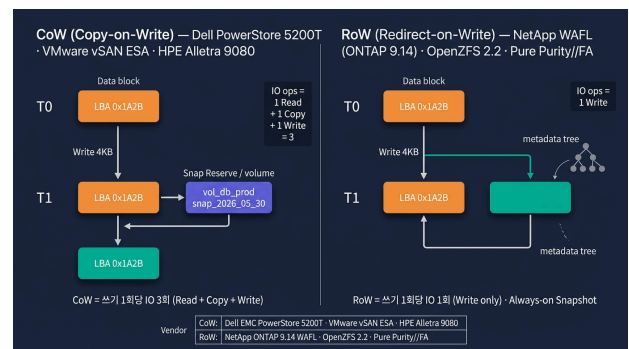
- **백업이 아니다** — 동일 어레이에 종속
- 어레이 자체 장애 시 Snapshot도 함께 손실
- 원본 데이터 부분 손상이면 Snapshot도 영향
- 메타데이터 의존 → 파일시스템 손상 시 무력

### 활용 패턴

- 패치·업그레이드 전 안전장치
- 시간별 정기 (RPO 단축 수단)
- Clone으로 테스트 DB 신속 생성
- **백업의 보조 수단**으로 위치 잡기

### CoW vs RoW — Snapshot 두 갈래

- **CoW (Copy-on-Write)** — 쓰기 발생 시 **원본을 복사 후 덮어쓰기**
- 쓰기 1회 = **IO 3회** (Read + Copy + Write)
- Dell PowerStore · vSAN ESA · HPE Alletra
- **RoW (Redirect-on-Write)** — 쓰기를 신규 위치로 리다이렉트, 원본은 유지
- 쓰기 1회 = **IO 1회** (Write only)
- NetApp WAFL · OpenZFS · Pure Purity//FA
- 핵심: **Snapshot ≠ 백업** — 어레이가 죽으면 Snapshot도 죽는다



Snapshot CoW vs RoW — IO 경로 차이

Replication — 동기 vs 비동기

 **Synchronous Replication**

- 원본·복제본 동시 쓰기 후 응답
- RPO = 0** (데이터 손실 0)
- 거리 한계 ~ **100km** (지연 < 5ms 권고)
- 비용 높음 (전용 회선·동등 사양)
- 사이트 간 응답시간 지연이 운영에 영향
- 미션크리티컬 (금융 코어·결재)

 **Asynchronous Replication**

- 원본 쓰기 응답 → 일정 주기로 복제본에 적용
- RPO 수 초 ~ 수 분**
- 거리 무제한 (대륙 간 가능)
- 운영 성능 영향 최소화
- 일반 기업 DR의 표준

 **주요 솔루션**

| 솔루션              | 벤더       | 모드                   |
|------------------|----------|----------------------|
| SnapMirror       | NetApp   | Sync-Async (본 단위)    |
| SnapVault        | NetApp   | 백업 복제                |
| SRDF             | Dell EMC | Sync-Async-SRDF/Star |
| HyperSwap        | IBM      | Sync (Active-Active) |
| MetroCluster     | NetApp   | Sync (Stretched)     |
| PowerStore Metro | Dell     | Sync                 |
| Hitachi GAD      | Hitachi  | Sync (Active-Active) |
| VPLEX            | Dell EMC | Sync (Active-Active) |

 **Stretched Cluster**

- 두 사이트가 **단일 클러스터**로 동작
- LUN이 양쪽에서 동시 활성화 (Active-Active)
- VMware vMSC-Hyper-V Stretch
- 거리·지연 제약 엄격

 **NetApp** ONTAP 9.14.1 · cluster1 · AFF A800

SSH

NetApp AFF A800 · cluster1 (2-node HA pair) · ONTAP 9.14.1 · RAID-DP

```
cluster1> cluster show
cluster1-01 / cluster1-02 — Health: true · Eligibility: true
cluster1> storage aggregate show
aggr_ssd_01 · 92TB · 38TB Available · 59% Used · online · cluster1-01

cluster1> volume create -vserver svm_prod -volume vol_db_prod -aggregate aggr_ssd_01
-size 4TB -junction-path /db_prod -security-style unix
cluster1> snapshot show -vserver svm_prod -volume vol_db_prod
Vserver · Volume · Snapshot · State · Size
-----
hourly.2026-05-30_0905 · valid · 812MB
daily.2026-05-30_0010 · valid · 4.2GB
before_patch.2026_05_30 · valid · 0B

cluster1> snapmirror create -source-path cluster1://svm_prod:vol_db_prod -destination-path
cluster_dr://svm_dr:vol_db_prod_dr -type XDP -policy MirrorAllSnapshots -schedule hourly
cluster1> snapmirror show
svm_prod:vol_db_prod → svm_dr:vol_db_prod_dr · Snapmirrored · Idle
Last Transfer 2026-05-30 09:00:12 · Lag 00:05:48
cluster1>
```

XDP =  
Extended Data  
Protection ·  
Async DR ·  
RPO ≈ 1h

NetApp ONTAP CLI — Volume-Snapshot:SnapMirror 실제 명령

Dedup · Compression — 공간 효율의 두 축



Deduplication (중복제거)

- 동일한 블록을 1번만 저장, 나머지는 참조
- **Inline** — 쓰기 시점에 즉시 처리 (성능 영향 ↑)
- **Post-Process** — 일단 기록 후 백그라운드 처리



Compression (압축)

- LZ4-Snappy-Zstd-Deflate 알고리즘
- Inline-Post-Process 동일 구분
- 텍스트·로그에서 효과 큼, 영상·암호화 파일은 효과 적음



효과가 큰 곳

- **VDI** (동일 OS 이미지 수십~수백) — 10:1 이상
- **백업 데이터** — 5:1 ~ 30:1
- **DB 로그·텍스트** — 2:1 ~ 5:1



트레이드오프

| 항목     | Inline             | Post-Process  |
|--------|--------------------|---------------|
| 쓰기 성능  | 낮음 (CPU 부하)        | 높음            |
| 디스크 사용 | 즉시 절감              | 일시 점유 후 절감    |
| 운영 단순성 | 단순                 | 복잡 (스케줄)      |
| 대표     | 현대 All-Flash·Veeam | 전통 SAN·일부 NAS |



실효 절감률 측정

- Veeam 백업: 5~10:1 일반적
- VDI 부팅 이미지: 10~20:1
- DB: 2~3:1
- 영상·암호화 파일: 1.1:1 (효과 미미)



주의

- **암호화 후 Dedup-Compression 불가** — 순서 중요
- 메타데이터 손상 = 전체 데이터 손실 가능
- CPU·메모리 사양 충분히 확보

Tiering · Thin Provisioning — 공간과 성능의 자동 분배



Tiering (자동 계층화)

- 데이터 접근 빈도에 따라 자동 이동
- 일반 계층:

Tier 0: NVMe (Hot)  
Tier 1: SSD  
Tier 2: SAS HDD  
Tier 3: SATA HDD  
Tier 4: Cloud Cold (S3 Glacier·Deep Archive)

- **Cloud Tier** — 자동 클라우드 오프로드 (NetApp FabricPool·Pure Cloud Block Store)
- 정책: 30일·90일·1년 미사용 → 다음 Tier로 이동



Thin vs Thick Provisioning

| 항목 | Thick      | Thin        |
|----|------------|-------------|
| 할당 | 즉시 전체 점유   | 사용분만 점유     |
| 성능 | 일정 (예측 가능) | 가변          |
| 효율 | 낮음         | 높음          |
| 위험 | 없음         | 과할당 시 일제 중단 |
| 적합 | DB·미션크리티컬  | 일반·VDI      |



Thin Provisioning 과할당

- 가상 1TB 할당 × 100개 = 100TB 가상
- 실제 디스크 50TB → 사용량 50TB 도달 시 **모든 LUN 일제 정지**
- 실사용량 모니터링 + 알람(70%·80%·90%) 필수
- 정기 회수 (UNMAP) 운영



운영 권고

- DB·미션크리티컬 = **Thick**
- VDI·일반 = **Thin** + 강한 모니터링

# PART D

## Tape · 아카이브 — 랜섬웨어 시대에 다시 빛나는 매체

Tape는 과거 기술이 아니다 — 오프라인의 마지막 방어선이자 장기 보존의 최저 비용 수단.

IT 인프라 아키텍처 설계 · Session 6 · 스토리지 · 백업 · DR

### LTO (Linear Tape-Open) — 9세대·10세대로 가는 진화

| 세대     | 출시           | Native     | Compressed | 전송속도           |
|--------|--------------|------------|------------|----------------|
| LTO-1  | 2000         | 100 GB     | 200 GB     | 20 MB/s        |
| LTO-2  | 2003         | 200 GB     | 400 GB     | 40 MB/s        |
| LTO-3  | 2005         | 400 GB     | 800 GB     | 80 MB/s        |
| LTO-4  | 2007         | 800 GB     | 1.6 TB     | 120 MB/s       |
| LTO-5  | 2010         | 1.5 TB     | 3 TB       | 140 MB/s       |
| LTO-6  | 2012         | 2.5 TB     | 6.25 TB    | 160 MB/s       |
| LTO-7  | 2015         | 6 TB       | 15 TB      | 300 MB/s       |
| LTO-8  | 2017         | 12 TB      | 30 TB      | 360 MB/s       |
| LTO-9  | 2021         | 18 TB      | 45 TB      | 400 MB/s       |
| LTO-10 | 2025~2026 예정 | 36 TB (예정) | 90 TB (예정) | 1100 MB/s (예정) |
| LTO-11 | 미래           | 72 TB (계획) | 180 TB     | —              |

#### 🔑 핵심 특징

- WORM 매체 옵션 (LTO-3+) — Write Once Read Many
- AES-256 하드웨어 암호화 (LTO-4+)
- 30년+ 보존 (적정 환경)
- 호환성: n세대 드라이브는 n-1 읽기·쓰기, n-2 읽기 가능

# LTFS (Linear Tape File System) — Tape을 디스크처럼 사용

 LTFS란

- Tape에 파일시스템 메타데이터를 별도 파티션으로 저장
- 일반 OS 마운트 가능 (Linux·Windows·macOS)
- 파일 단위 접근 — `cp`, `mv` 로 직접 다룸
- LTO-5+ 지원, 산업 표준 (ISO/IEC 20919)

 활용 패턴

- 방송·미디어 — 영상 마스터 보관
- 연구·과학 — 측정 데이터 장기 보존
- 공공·아카이브 — 법정 보관
- 클라우드 백업 — AWS S3 Glacier 기반

 LTFS vs 전통 Tape

| 항목    | 전통 Tape    | LTFS        |
|-------|------------|-------------|
| 접근    | 백업 SW 필수   | OS 마운트로 직접  |
| 메타데이터 | 백업 SW 카탈로그 | Tape 자체에 보관 |
| 호환    | 백업 SW 종속   | 표준          |
| 용도    | 백업         | 아카이브        |

 주의

- 순차 매체 — 임의 접근 느림 (수십 초~수 분 탐색)
- 헤드 위치 이동 비용 큼
- 쓰기 후 자주 수정하는 데이터에는 부적합

# Tape의 현대적 가치 — 랜섬웨어 시대에 다시 부상

 Tape의 본질적 강점

- 오프라인 매체 — 네트워크에서 분리되면 사이버 공격 불가
- WORM — 본질적으로 한 번 쓰면 변경 불가
- 장기 보존 — 30년+ (적정 환경)
- 저비용 — GB당 단가 가장 낮음
- 에너지 효율 — 보관 중 전력 소모 0

 비용 비교 (대략, GB 당)

- HDD: \$0.02 / GB / 월 (전력 포함)
- Object Cold: \$0.004 / GB / 월
- Tape: **\$0.001 / GB / 월** + 초기 HW

 랜섬웨어 대응 가치

- 운영망·관리망·백업망 다 침해되어도
- 오프라인 Tape은 격리되어 살아남음
- 실제 사건: 2020+ 다수 기업이 백업까지 암호화당해 몸값 지불
- 이후 Tape 복구가 보안 권고로 부상

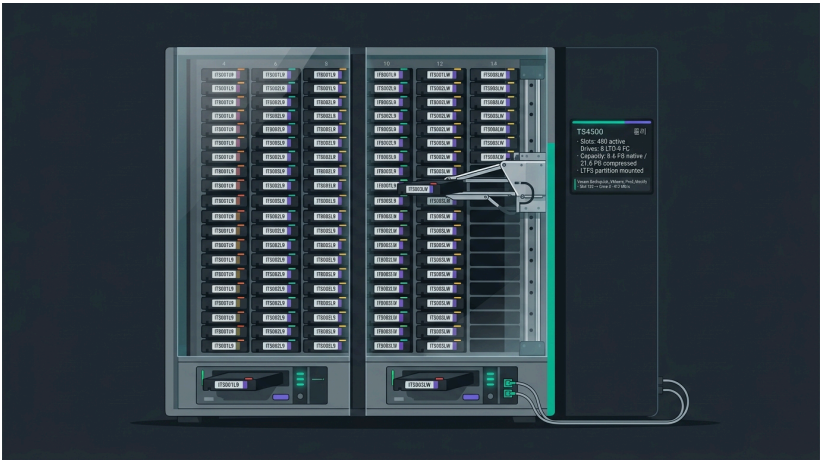
 Tape의 한계

- 복구 시간 길다 — 수 시간~수 일
- 순차 매체 — 부분 복구 비효율
- 물리 보관·운반 비용
- 카트리지·드라이브 노후화 관리

 권장 운영

- 일별 Inc → 디스크, 주별 Full → Tape
- Tape는 오프사이트 보관 (사외 보관소)
- 분기 1회 복구 시험

 **실제 장비 참조** (벤더 공식·Wikipedia) - [IBM TS4500 Tape Library](#) — IBM 공식 - [IBM TS1170 / LTO-9 Drive](#) — IBM 공식 - [Dell PowerVault ML3](#) — Dell 공식 - [HPE StoreEver MSL Series](#) — HPE 공식 - [Quantum Scalar i6 / i6000](#) — Quantum 공식 - [LTO Ultrium 표준](#) — LTO Program 공식 (로드맵·사양서)



Tape Library 삽화

# PART E

## 백업 정책 · 솔루션 — 6종 정책 · GFS · 7대 솔루션

"검증되지 않은 백업은 백업이 아니다."

IT 인프라 아키텍처 설계 · Session 6 · 스토리지 · 백업 · DR

## 백업 정책 6종 — 비교 매트릭스

| 정책                  | 첫 백업 | 이후                           | 복구 시 필요            | 용량 | 백업 속도       | 복구 속도         |
|---------------------|------|------------------------------|--------------------|----|-------------|---------------|
| Full                | 전체   | 전체                           | 마지막 Full 1개        | 큼  | 느림          | 빠름            |
| Incremental         | Full | 변경분 (이전 Inc 이후)              | Full + 모든 Inc      | 적음 | 빠름          | 느림            |
| Differential        | Full | 변경분 (마지막 Full 이후)            | Full + 마지막 Diff    | 중간 | 중간          | 중간            |
| Synthetic Full      | Full | Inc + 가상 합성                  | 마지막 Synthetic Full | 큼  | 빠름 (Inc 백업) | 빠름            |
| Forever Incremental | Full | Inc만 지속                      | Forever Inc 체인     | 적음 | 빠름          | 중간            |
| Reverse Incremental | Full | 직전 백업이 Full, 이전이 Reverse Inc | 최근 Full만           | 중간 | 중간          | 매우 빠름 (최근 우선) |

### 📋 정책 선택 가이드

- 일반 환경: **Synthetic Full** (Inc로 빠르게, 복구는 Full처럼)
- 대용량·고빈도: **Forever Incremental** (Veeam 표준)
- 오프사이트 Tape: **Weekly Full + Daily Inc** (전통)
- 빠른 최근 복구: **Reverse Incremental**



# Hot · Cold · Warm Backup — 서비스 상태별 백업

 Hot Backup

- 서비스 운영 중 백업
- DB Online Backup (Oracle RMAN-MS SQL VSS)
- Snapshot + 백업 SW 통합
- 응용 일관성 (Application-Consistent)
- 무중단 필수 환경

 Cold Backup

- 서비스 중단 후 백업
- 가장 안정적 (정합성 100%)
- 야간 점검 원도 활용
- 현대 거의 사용 안 함

 Warm Backup

- 단시간 일시 정지 후 백업
- 짧은 점검 원도 활용
- 일부 DB-중요도 중간

 일관성 수준

- Crash-Consistent — 디스크 상태만 (응용 미인지)
- File-System-Consistent — FS sync
- Application-Consistent — DB-App 협력 (VSS-Agent)

 VSS (Volume Shadow Copy Service)

- Windows 표준 Snapshot 프레임워크
- Exchange-SQL-SharePoint-AD 응용 일관성

 권장 패턴

- Hot Backup + Application-Consistent = 현대 표준
- DB는 Native Backup Tool + 백업 SW 연계
- Oracle RMAN
- MS SQL Native Backup
- PostgreSQL pg\_basebackup
- MongoDB mongodump
- 트랜잭션 로그 별도 백업 → 시점 복구

 흔한 실수

- DB 파일을 일반 파일 백업하면 깨질 위험
- VSS Writer 비정상 → 백업 실패
- 트랜잭션 로그 백업 누락

# 백업 검증 · 복원 테스트 — 검증 없는 백업은 백업이 아니다

 검증 단계

- Job 성공 확인 — 백업 SW의 status (기본)
- 체크섬 검증 — SHA-256-CRC
- 샘플 복구 시험 — 정기 무작위
- 전체 복구 시험 — 분기·반기
- 자동화된 검증 — 백업 후 자동 부팅·테스트

 자동 검증 솔루션

- Veeam SureBackup — 격리 샌드박스에서 자동 부팅·테스트
- Commvault DASH — 자동 복구 시험
- Rubrik Live Mount — 즉시 마운트 검증
- Cohesity TestDev — 격리 환경 자동 생성

 정기 점검 체크리스트

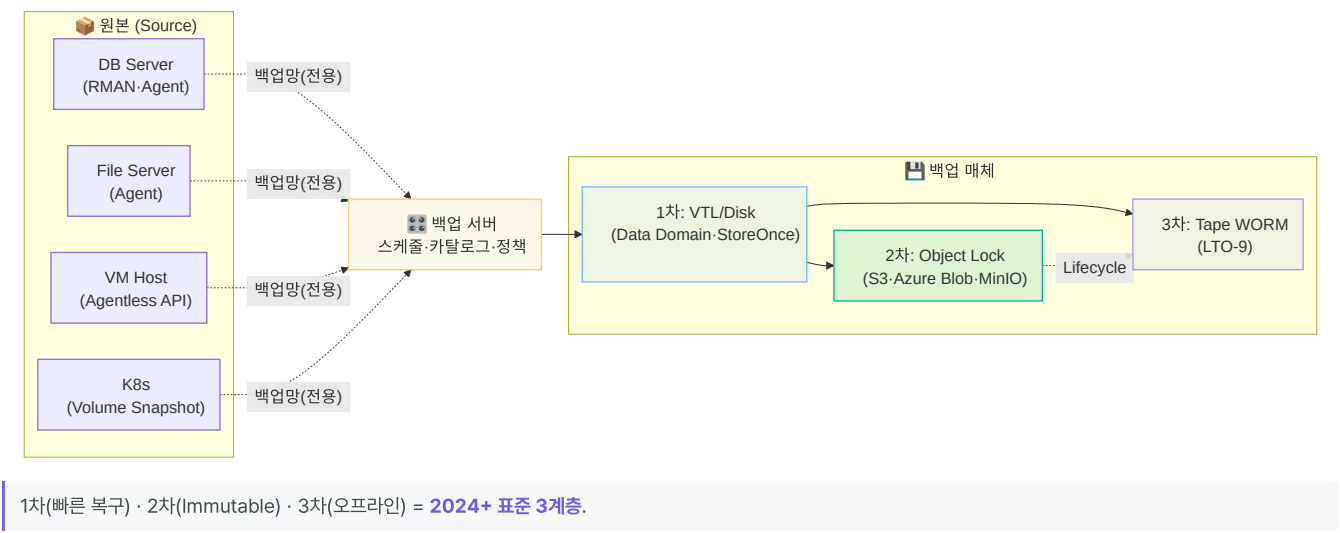
- [ ] 일별: Job 성공률 100%인가
- [ ] 주별: 무작위 1건 복구 시험
- [ ] 월별: 보고서 + 실측 RTO 기록
- [ ] 분기별: 전체 DR 전환 시뮬레이션
- [ ] 반기별: Live DR 훈련
- [ ] 연: 정책·매체·솔루션 재검토

 흔한 실패 패턴

- 백업 Job은 성공인데 데이터는 실제 백업되지 않은 경우 (Agent 오류)
- Tape 카트리지 자체 불량
- 복구 시 의존 라이브러리·DB 누락
- 비밀번호·인증서 정보가 없어 복구 불가

"백업이 정상 수행되고 있습니다"는 의미 없는 보고. "복구 시험 분기 1회 + 최근 실측 RTO + 검증된 복구 절차서"가 실질적 답.

# 백업 시스템 아키텍처 — 전형적 구조



1차(빠른 복구) · 2차(Immutable) · 3차(오프라인) = 2024+ 표준 3계층.

# PART F

## 데이터 무결성 · 랜섬웨어 대응 — 3-2-1-1-0과 Immutable

모든 백업은 결국 "복구할 수 있는가 + 변경되지 않는가" 두 질문에 답해야 한다.

# Air-Gapped · Immutable Backup — 공격자가 접근할 수 없는 백업

 **Air-Gapped (에어갭)**

- 물리적·논리적으로 운영망과 분리된 백업
- 평시 분리 → 백업 시점에만 연결 → 다시 분리
- 종류:
  - 물리 에어갭 — Tape 카트리지 오프라인 보관
  - 논리 에어갭 — VLAN 분리 + 일시 활성화
  - 시간 에어갭 — 백업 원도 외 차단
  - 자동화: 백업 SW + NW 자동화 연동

 **Immutable Backup**

- 한 번 기록되면 변경·삭제 불가
- 보존 기간 동안 그대로 보존
- 시스템 관리자도 삭제 불가 (Compliance 모드)
- 랜섬웨어가 접근해도 데이터 보존

 구현 방법

| 매체                              | 메커니즘                       |
|---------------------------------|----------------------------|
| S3 Object Lock                  | Compliance / Governance 모드 |
| Azure Blob Immutable            | Time-based / Legal Hold    |
| Veeam Hardened Linux Repository | 변경 불가 OS 설정                |
| Dell PowerProtect Cyber Vault   | 격리·Immutable 통합            |
| Linux WORM (XFS:ZFS)            | 파일시스템 옵션                   |
| LTO WORM 카트리지                   | 물리적 WORM                   |

 권장 조합

- 1차: Veeam Hardened Repository (즉시 복구)
- 2차: S3 Object Lock (Immutable 클라우드)
- 3차: LTO WORM (오프라인 최종 방어)
- 3중 Immutable

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

43 / 70

#216

IT 인프라 아키텍처 설계 · Session 6 · 스토리지 · 백업 · DR

# WORM · S3 Object Lock — 법적·물리적 변경 불가

 **WORM (Write Once Read Many)**

- 물리적 또는 논리적으로 한 번만 쓰기 가능
- 금융·의료·공공 법정 보관에 사용
- 매체별 구현:
  - CD-R·DVD-R·BD-R — 광 매체 (구식)
  - LTO WORM 카트리지 — 별도 모델
  - WORM Disk — 어플라이언스
  - WORM Object Storage — S3 Object Lock

 S3 Object Lock 모드

**Governance 모드** - 일반 사용자는 삭제 불가 - 특별 권한(`s3:BypassGovernanceRetention`) 보유자는 가능 - 운영 유연성 + 보안

**Compliance 모드** - 누구도 삭제 불가 (Root 계정조차) - 보존 기간 동안 100% 보존 - 법정 요건·랜섬웨어 최고 방어

 Object Lock 설정 예시

```
Retention:
  Mode: COMPLIANCE
  RetainUntilDate: 2027-12-31
LegalHold:
  Status: ON
```

- Retention** — 시간 기반 (만료 후 삭제 가능)
- Legal Hold** — 무기한 (수동 해제 전까지)
- 동시 적용 가능

 활용 패턴

- 금융: **Compliance 모드** + 5~10년 보관
- 공공: **Compliance** + 법정 보관 기간
- 일반 기업: **Governance** + 90일~1년
- 의료: **Compliance** + 10년+

 주의

- 보존 기간 동안 **저장 비용 청구 지속**
- 잘못 설정하면 **수정 불가** — 신중히 적용
- 버킷 단위·객체 단위 모두 가능

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

44 / 70

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

page 108 / 160

### 3-2-1 원칙 — 백업의 황금 규칙

3

사본 3개 보유  
(원본 + 백업 2개)

2

서로 다른 매체 2종  
(Disk + Tape · Disk + Cloud)

1

오프사이트 1부  
(다른 건물·다른 도시·클라우드)

#### 🏠 적용 예시 (일반 기업)

- 원본: 운영 서버 (DAS·SAN·NAS)
- 백업 ☉: 1차 디스크 (VTL·Backup Appliance) — 사내
- 백업 ☉: Tape WORM — 사외 보관 (오프사이트)

#### 🎯 매체 다양화의 이유

- 동일 매체는 동일 결함을 공유 (펌웨어 버그·환경 영향)
- 디스크 어레이가 전부 죽어도 Tape이 살아 있어야 함

### 3-2-1-1-0 — 랜섬웨어 시대의 확장판

1  
2  
3  
4

추가된 1과 0

+ 1 (Offline) - 오프라인·에어갭 1부 - Tape 카트리지 오프라인 보관 - 또는 Immutable Object Lock - 랜섬웨어 격리의 최종 방어선

+ 0 (Zero Errors) - 백업 후 검증 시 오류 0 - 자동화된 복구 시험 통과 - 체크섬 무결성 확인 - "검증된 백업만 백업"

🛡️ 시각화

3 - Copies (원본+2)  
2 - Different Media (Disk+Tape·Disk+Cloud)  
1 - Offsite (다른 건물·도시·클라우드)  
1 - Offline (Tape WORM·Immutable)  
0 - Errors (검증 통과)

🎯 실무 매핑

- 3-2-1-1-0 충족 = ISMS-P·금융 점검 통과 수준
- 핵심 시스템은 모두 이 수준 필수
- 일반 시스템은 3-2-1 만으로 충분할 수 있음

📋 점검 질문 (TA 면접 단골)

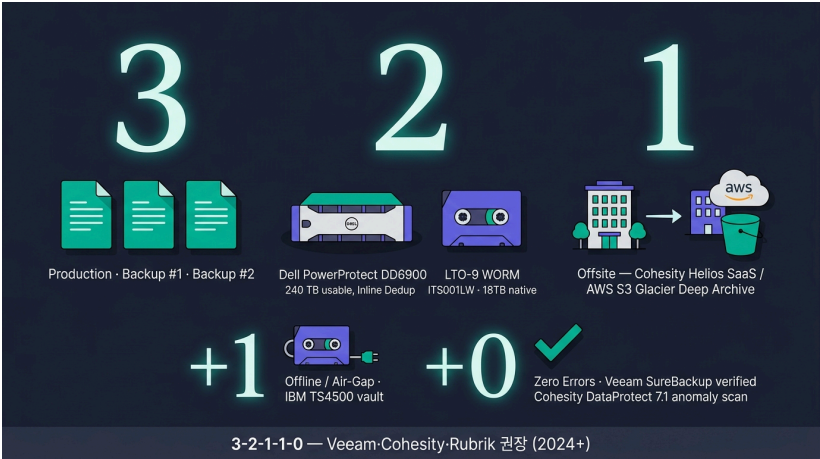
- "당신 환경의 3-2-1-1-0 수준은?"
- "마지막 검증 복구 시험 일자는?"
- "Immutable 백업 보유 여부?"

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

46 / 70

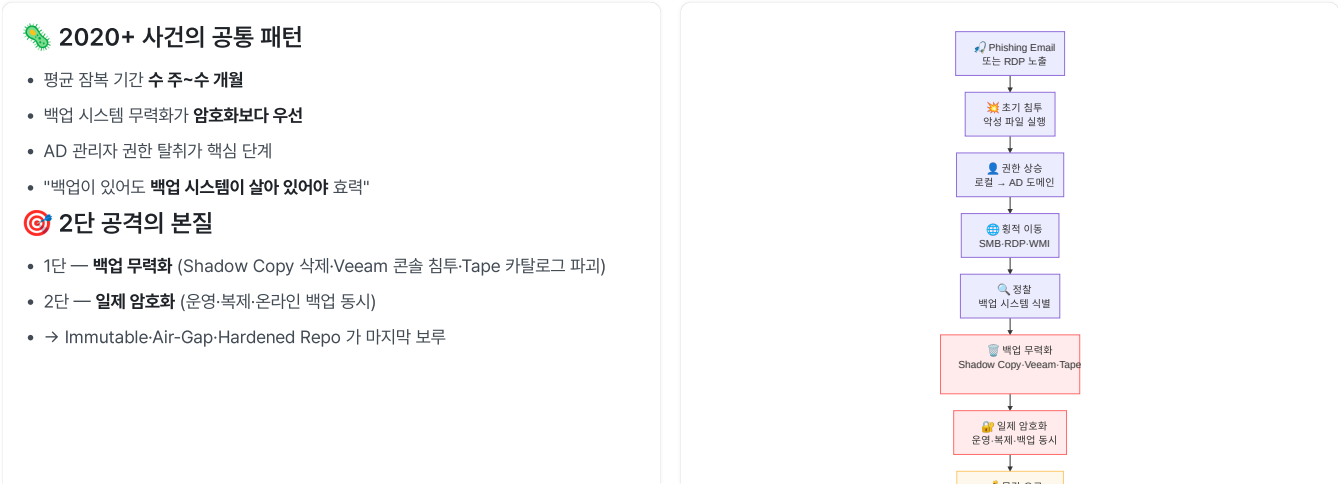
© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

page 109 / 160



3-2-1 삽화

## 랜섬웨어 공격 시나리오 — 전형적 침투 흐름



랜섬웨어 대응 SOP — 발견 시 5단계

 1단계 — Detection (탐지)

- EDR-SIEM-NDR 경보
- 사용자 신고 (파일 열리지 않음)
- 백업 Job 비정상

 2단계 — Containment (격리)

- 감염 호스트 즉시 **네트워크 분리**
- AD 관리자 계정 비활성화
- 백업망 **물리 차단** (운영 영향 격리)
- 외부 인터넷 차단 (C2 통신 차단)

 3단계 — Investigation (조사)

- 침투 경로·시점·범위 식별
- 감염 시점 이전 백업 확보
- 포렌식 (디스크 이미지·메모리)
- 법적 절차 (경찰·KISA 신고)

 4단계 — Recovery (복구)

- **Immutable-Offline 백업** 확보 확인
- 깨끗한 환경(새 서버) 준비
- 백업 시점 이전으로 복구
- 시스템 단계적 재구축
- 응용 검증 후 서비스 재개

 5단계 — Lessons Learned

- 사고 보고서 작성
- 침투 경로 차단 (패치·정책)
- 백업 정책 강화
- 직원 보안 교육
- 모의 침투 정기화

 절대 하지 말아야 할 것

- 몸값 지불 → 복호화 보장 없음
- 백업 검증 없이 운영 망 재연결
- 사건 미보고 (법적 의무)

PART G

DR (재해 복구) — 4단계 · RPO/RTO · BCP · 훈련

"데이터를 잃지 않는 것"이 백업이라면, "**서비스를 잃지 않는 것**"이 DR.

DR 4단계 — Backup&Restore부터 Multi-Site Active-Active까지

| 단계 | 명칭                       | 핵심                         | RTO  | RPO   | 비용  |
|----|--------------------------|----------------------------|------|-------|-----|
| 1  | Backup & Restore         | 백업 데이터만 사외 보관, 사이트 0       | 시간~일 | 시간~일  | 저   |
| 2  | Pilot Light              | DR 사이트에 핵심 인프라만 가동, 데이터 복제 | 시간   | 분~시간  | 중   |
| 3  | Warm Standby             | 축소된 운영 사이트 가동, 데이터 비동기 복제  | 분~시간 | 분     | 중~고 |
| 4  | Hot Standby              | 운영과 동일 사양, 동기 복제           | 분 단위 | 0~수 초 | 고   |
| 5  | Multi-Site Active-Active | 두 사이트가 동시 운영 (트래픽 분산)      | 0    | 0     | 최고  |

🎯 등급별 채택 패턴

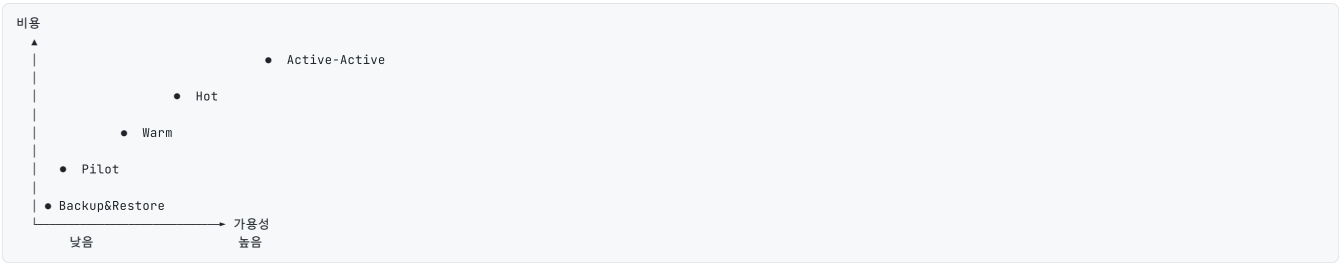
- 일반 기업: 1~2단계 (Backup+Restore 또는 Pilot Light)
- 중요 시스템: 3단계 (Warm)
- 금융 코어·통신: 4단계 (Hot)
- 결제·119·재난·국방: 5단계 (Active-Active)

AWS 백서가 정리한 4단계 + Active-Active를 더한 5단계 모델이 현재 표준.

RPO · RTO 매트릭스 — 비용과 가용성의 결정표

| 등급     | RTO    | RPO   | 일반 수단                           | 추가 비용 (대략) |
|--------|--------|-------|---------------------------------|------------|
| 일반     | 4~24시간 | 24시간  | 일 1회 백업 (Backup&Restore)        | 기본         |
| 중요     | 1~4시간  | 1~4시간 | 백업 + 시간별 Snapshot (Pilot Light) | +30%       |
| 준 미션   | 15~60분 | 분 단위  | 비동기 복제 + 백업 (Warm Standby)      | +100%      |
| 미션크리티컬 | 분 단위   | 0~수 초 | 동기 복제 + HA (Hot Standby)        | +200~400%  |
| 무중단    | 0      | 0     | 사이트 이중화 + Active/Active         | +400%+     |

💰 비용 vs 가용성 그래프 (개념)



BCP · DR 사이트 위치 — *지리적 거리의 의미*

 BCP (Business Continuity Plan)

- DR은 IT 인프라 영역
- BCP는 업무 연속성** — 사람·프로세스·외부 통신·물리 공간 포함
- BCP > DR > 백업·복구

 BIA (Business Impact Analysis)

- 업무별 중단 시 영향도 분석
- MTPD (Maximum Tolerable Period of Disruption)
- 등급별 우선순위
- DR 등급 결정의 출발점

 DR 사이트 위치 결정 변수

- 거리** — 동일 재해 영향 회피
- 네트워크 비용** — 거리 ∝ 회선료
- 법규** — 금융 30km+ (전자금융감독규정)
- 인력 가용성** — 원격 운영 가능 여부

 한국 DR 사이트 표준

| 등급     | 거리 권고  | 예시           |
|--------|--------|--------------|
| 일반     | 도시 내   | 서울 강남 ↔ 강서   |
| 중요     | 30km+  | 서울 ↔ 일산·분당   |
| 미션크리티컬 | 수도권 분산 | 서울 ↔ 진안·대전   |
| 국가 핵심  | 전국 분산  | 서울 ↔ 부산·광주   |
| 글로벌    | 국가 간   | 한국 ↔ 일본·싱가포르 |

 거리의 트레이드오프

- 동기 복제 가능 한계 = ~100km (지연 5ms 이내)
- 100km+ → 비동기 복제 필수
- 1000km+ → 회선 비용 폭증

 권고

- 동일 지진대·동일 전력망·동일 통신망 회피
- 통신 회선 **물리적 이중화** (2개 통신사·2개 경로)

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

53 / 70

#226

IT 인프라 아키텍처 설계 · Session 6 · 스토리지 · 백업 · DR

DR 훈련 5단계 — *Tabletop부터 Full Interruption까지*

| 훈련                   | 정의                      | 운영 영향 | 비용    | 주기 권고          |
|----------------------|-------------------------|-------|-------|----------------|
| 1. Tabletop          | 회의실에서 시나리오 토론·점검        | 없음    | 매우 낮음 | 분기 1회          |
| 2. Walkthrough       | 절차서 따라 단계별 시뮬레이션 (실형 X) | 없음    | 낮음    | 반기 1회          |
| 3. Simulation        | 격리 환경에서 일부 시스템 실제 시뮬레이션 | 낮음    | 중     | 반기~연 1회        |
| 4. Parallel          | DR 사이트 동시 운영, 트래픽은 운영에만 | 낮음    | 중~높   | <b>연 1회+</b>   |
| 5. Full Interruption | 운영 중단 + DR로 완전 절제       | 있음    | 매우 높음 | <b>2~5년 1회</b> |

 **권장 운영**

- 분기: **Tabletop** (가벼운 검토)
- 반기: **Walkthrough** + 부분 **Simulation**
- 연: **Parallel** + 산출물 갱신
- 2~5년: **Full Interruption** (대형 변경 시)

 **훈련 시 점검 항목**

- 실측 RTO·RPO (vs 목표)
- 절차서 일치도
- 인력 가용성 (휴가·교대)
- 통신·이해관계자 알림 절차

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

54 / 70

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

page 113 / 160



재해 시나리오 — 우리가 대비해야 할 7가지

 **화재**

- 가장 흔한 데이터센터 재해
- 진압 후에도 **수증기-연기-연쇄 누전**
- 화재진압 가스 (FM-200-Inergen-Novec-1230) 후 환기 필요
- 수 시간~수일** 복구 불가
- DR 사이트 절체 필요

 **침수**

- 1층-지하 데이터센터 위험
- 누수 감지기 필수
- 폭우-태풍-내부 배관 파열
- 한 번 침수되면 정비 거의 폐기

 **지진**

- 한국도 안전지대 아닌 (포항-경주)
- 진동 차단-내진 설계 필수
- 동일 지진대 회피 → **DR 거리 결정 요인**

 **정전 (장기)**

- UPS-발전기로 단기 대응
- 디젤 발전기 연료 = 보통 **8~24시간분**
- 장기 정전(수일+) = 운영 중단
- 한전 2회선-자가발전 + DR 필요

 **통신 케이블 단절**

- 광케이블 굴착 사고
- 통신사 1개 의존 = 리스크
- 2개 통신사-2개 물리 경로** 필수
- 수 시간~수일 복구

 **랜섬웨어**

- 21세기 가장 빈번한 "재해"
- 기술 사고가 아닌 **공격**
- Immutable-Air-Gap 필수
- BCP 시나리오 1순위

 **팬데믹-인력 불가**

- COVID-19 사례
- 원격 운영 체계 필수
- 출입 인력 격리-교대
- 데이터센터 운영 BCP 별도

 **건물·시설 재해**

- 천장 누수-에어컨 고장
- 전력 분전반 사고
- 시설 노후화

 **시나리오별 대응 매트릭스**

| 재해    | 백업 | 복제     | DR 사이트 |
|-------|----|--------|--------|
| 화재    | △  | ○      | ⊗      |
| 침수    | △  | ○      | ⊗      |
| 지진    | △  | △ (거리) | ⊗      |
| 정전    | △  | ○      | ⊗      |
| 통신 단절 | ×  | ×      | ⊗      |
| 랜섬웨어  | ⊗  | ×      | △      |
| 팬데믹   | ×  | ×      | △      |

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

55 / 70

#228

IT 인프라 아키텍처 설계 · Session 6 · 스토리지 · 백업 · DR

DR 비용 산정 사례 — 현실적 숫자로 보기

🎯 가상 사례: 중규모 SaaS 기업

- 운영 사이트: 서울 (자체 데이터센터)
- 핵심 워크로드: 웹 + DB(Oracle) + 파일 + 백업
- 목표 RTO 1시간 · RPO 5분 → **Warm Standby + Async 복제**

 **초기 구축 비용 (CapEx)**

| 항목                     | 비용 (대략)         |
|------------------------|-----------------|
| DR 사이트 임대 (코로케이션)      | 5,000만 원 (약 5개) |
| DR 서버 (운영의 60% 사양)     | 3억 원            |
| DR 스토리지 (운영의 70% 용량)   | 2억 원            |
| DR NW 장비 (FW-SW-LB)    | 1억 원            |
| 사이트 간 회선 (전용선 100Mbps) | 초기 3,000만 원     |
| DR 백업 (Immutable-Tape) | 1억 원            |
| DR 솔루션-라이선스            | 1억 원            |
| <b>합계</b>              | <b>약 8억 5천</b>  |

 **운영 비용 (OpEx, 연간)**

| 항목                | 비용 (대략)       |
|-------------------|---------------|
| 코로케이션 임대 + 전력     | 6,000만 원/년    |
| 회선료 (전용선 100Mbps) | 4,800만 원/년    |
| 유지보수 (HW-SW)      | 1.5억 원/년      |
| DR 훈련 비용          | 2,000만 원/년    |
| 인력 (DR 운영 0.5명)   | 5,000만 원/년    |
| <b>연 합계</b>       | <b>약 3.5억</b> |

 **5년 TCO**

- 초기 8.5억 + 운영 17.5억 = **약 26억**
- 동일 가용성 클라우드 DR = 약 20~25억 (지속)
- 비교: 자체 DR vs AWS DR vs DRaaS

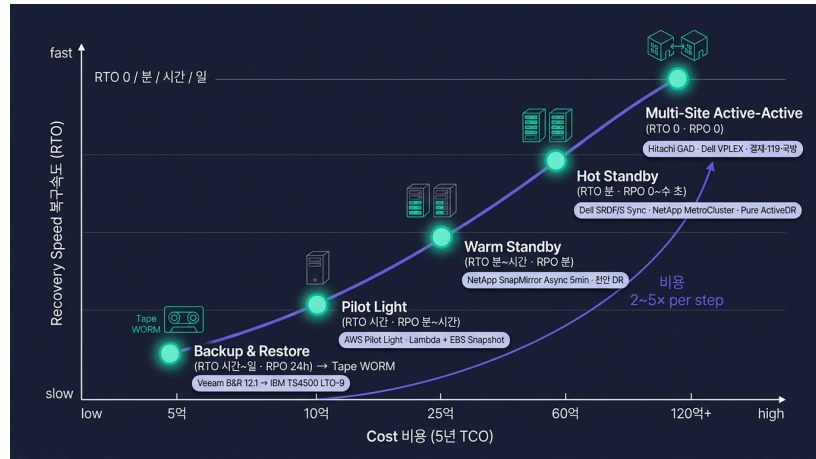
© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

56 / 70

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

page 114 / 160

IT 인프라 아키텍처 설계 · Session 6 · 스토리지 · 백업 · DR



DR 4단계 매트릭스 삽화

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

57 / 70

# PART H

## 산출물 · 결정 — TA가 만들고 결정하는 것

스토리지·백업·DR 설계는 결국 숫자와 정책의 문서화.

# TA가 스토리지·백업 설계에서 내리는 12가지 결정

1 스토리지 유형

- 워크로드별 6대 유형 매핑
- SAN vs HCI vs Object

2 프로토콜

- FC vs iSCSI vs NVMe-oF
- NFS vs SMB

3 RAID 레벨

- DB = RAID 10
- 대용량 = RAID 6 / EC

4 Snapshot 정책

- 추가·보관 기간
- CoW vs RoW (벤더 종속)

5 Replication 모드

- Sync vs Async
- 거리·RPO

6 Dedup·Compression

- Inline vs Post
- 실효 질감을 보수적 산정

7 Thin vs Thick

- 워크로드별
- 모니터링 정책

8 백업 정책

- Full·Inc·Synthetic·Forever
- GFS 보관 기간

9 백업 매체 3계층

- 1차 Disk/VTL · 2차 Object Lock · 3차 Tape WORM

10 Immutable·Air-Gap

- 매체별 구현
- Compliance vs Governance

1 1 DR 단계 결정

- 4단계 + Active-Active 중 선택
- BIA 기반

1 2 훈련 정책

- Tabletop·Walkthrough·Simulation·Parallel-Full
- 주기 + KPI

이 12가지가 곧 [스토리지·백업·DR 설계서의 목차](#).

# 산출물 ① — 스토리지 BOM (Bill of Materials)

| 분류                    | 모델                            | 수량 | 단가      | 합계     | 비고                |
|-----------------------|-------------------------------|----|---------|--------|-------------------|
| SAN 어레이               | Dell PowerStore 1200T         | 1  | 4억 원    | 4억     | 이중 컨트롤러           |
| 디스크 (NVMe SSD)        | 1.92TB NVMe TLC               | 24 | 200만    | 4,800만 | RAID 6 (22+2)     |
| 디스크 (SAS HDD)         | 8TB 7.2K SAS                  | 36 | 50만     | 1,800만 | RAID 6 (16+2) × 2 |
| SAN Switch (Director) | Brocade X7-4                  | 2  | 1.5억    | 3억     | Fabric A/B 이중화    |
| HBA                   | Emulex LPe35002 32G FC        | 16 | 80만     | 1,280만 | 호스트당 2개 × 8호스트    |
| 광 케이블·SFP+            | 32G FC LC-LC 5m               | 32 | 5만      | 160만   | 양단 결선             |
| VTL/백업 어레이            | Dell DD6900 (240TB usable)    | 1  | 2.5억    | 2.5억   | Inline Dedup      |
| Tape Library          | Dell TL4000 (LTO-9, 48슬롯)     | 1  | 8,000만  | 8,000만 | WORM 카트리지 24매     |
| 백업 SW 라이선스            | Veeam Universal License (VUL) | 50 | 100만/VM | 5,000만 | 5년                |
| 유지보수 (5년)             | HW-SW 통합                      | —  | —       | 4억     | 24×7 4hr 응대       |
| 합계                    |                               |    |         | 약 17억  | —                 |

-  BOM 작성 체크리스트
- 모델·세대·펌웨어 명시
  - 수량·단가·합계
  - 유지보수 기간·SLA 등급
  - 케이블·광 모듈 등 부속품 누락 방지
  - 라이선스 모델 (Per-Capacity·Per-VM·Per-Node)

산출물 ② — 백업 정책표

| 시스템            | 등급     | 정책                | 주기               | 보관         | 매체                   | RTO | RPO | 검증              |
|----------------|--------|-------------------|------------------|------------|----------------------|-----|-----|-----------------|
| 핵심 DB (Oracle) | Tier-1 | Hot+RMAN          | 일별 Inc, 주 1 Full | 30일/90일/연  | VTL+Object Lock+Tape | 1h  | 5m  | 일 1회 자동         |
| VM (운영)        | Tier-1 | Veeam Forever Inc | 매 4시간 Inc        | 30일/52주/7년 | VTL+Object Lock      | 30m | 4h  | 일 1회 SureBackup |
| 파일 서버          | Tier-2 | Full + Diff       | 주 1 Full, 일 Diff | 30일/12주/3년 | VTL+Tape             | 4h  | 24h | 주 1회            |
| 로그·아카이브        | Tier-3 | Inc               | 일별 Inc           | 90일/3년     | Object Cold          | 24h | 24h | 월 1회            |
| 개발·테스트         | Tier-4 | Full              | 주 1 Full         | 4주         | VTL only             | 24h | 7d  | 월 1회            |

📄 정책표 구성 요소

- 시스템·등급
- 백업 정책 (방식 + 솔루션)
- 주기 + 보관 기간 (GFS)
- 매체 (3계층 매핑)
- RTO/RPO (목표)
- 검증 주기·방법

🎯 권고

- 핵심 시스템은 3계층 매체 + 자동 검증
- 일반 시스템은 2계층 + 수동 분기 검증
- 정책표는 분기 1회 갱신

산출물 ③ — DR 설계서 (목차)

📄 DR 설계서 목차

1. 사업 개요·범위
2. BIA (Business Impact Analysis) - 핵심 업무 목록 - 중단 시 영향도 - MTPD·RTO·RPO 도출
3. DR 등급 결정 - 4단계 중 선택 근거 - 비용 산정
4. DR 사이트 위치·계약 - 거리·통신·접근성 - 코로케이션 vs 자체
5. DR 아키텍처 - 인프라 구성도 - 복제·동기화 방식 - 네트워크 토폴로지

6. 절체 절차 - Failover 절차 - Failback 절차 - 의사결정자·승인자
7. 데이터 동기화 모니터링 - 복제 지연·오류 알람 - RPO 실측
8. DR 훈련 계획 - 5단계 훈련 주기 - 실측 결과 기록
9. 이해관계자 통신 - 사고 시 알림 흐름 - 외부 통신 (고객·언론·당국)
10. 사후 검토·개선

- 훈련 결과 반영
- 설계서 갱신

🎯 산출물 권고 분량

- 본문: 80~150 페이지
- 별첨: 절차서·연락처·점검표

IT 인프라 아키텍처 설계 · Session 6 · 스토리지 · 백업 · DR

## 산출물 ④ — 랜섬웨어 대응 SOP

### SOP 구성

1. 목적·범위
2. 역할 정의 - CISO·CIO·TA·운영팀·홍보팀·법무팀 - 외부 연락처 (KISA·경찰·MSSP)
3. 탐지 기준 - EDR·SIEM 경보 조건 - 사용자 신고 채널
4. 초동 격리 절차 - 호스트 분리·계정 비활성화 - 백업망 차단 의사결정자
5. 조사·증거 보존 - 디스크 이미지·메모리 덤프 - 로그 보존

6. 복구 절차 - Immutable 백업 식별 - 복구 우선순위 - 단계별 시스템 복구촉
7. 외부 통신 - KISA 신고 (24시간 내) - 개인정보 유출 시 통지 - 고객·언론 응대
8. 사후 조치 - RCA 보고서 - 정책·인프라 강화 - 직원 교육
9. 체크리스트·점검표
10. 연락처·에스컬레이션 매트릭스

### SOP 권고

- 분기 1회 검토·갱신
- 모의 침해 훈련 시 SOP 따라가기
- 인쇄본도 비치 (NW 차단 시 디지털 접근 불가)

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

63 / 70

IT 인프라 아키텍처 설계 · Session 6 · 스토리지 · 백업 · DR

## 케이스 미니 ① — DB 데이터 손실 시나리오

### 상황

- 운영자 실수로 핵심 테이블 DELETE
- 동기 복제본도 함께 삭제 (사이트 B에도 적용됨)
- 백업: 전일 야간 Full (자정)
- 사고 시점: **당일 14:00**

### TA가 던지는 질문

1. RTO·RPO 등급은?
2. 시점 복구(PiTR) 가능한 DB인가?
3. 트랜잭션 로그 보관 여부
4. 백업 + 로그로 14:00 직전 복구 가능?
5. 전체 롤백 vs 부분 복구?

### 대응 절차

1. 격리 — 추가 변경 차단 (운영 일시 중지)
2. Snapshot 확보 (있다면)
3. 복구 결정 - Full + Archive Log → 13:59 시점 복구 - 별도 인스턴스에 복구 후 데이터만 추출 → 운영 인스턴스에 INSERT
4. 검증 — 데이터 정합성
5. 서비스 재개
6. 사후 보고 — 사용자 권한 재검토·감사 로그 강화

### 교훈

- 복제 ≠ 백업 — 본 시나리오가 정답
- 트랜잭션 로그 백업이 PiTR의 전제
- DB Native Backup이 일반 백업보다 우선

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

64 / 70

## 케이스 미니 ② — 랜섬웨어로 백업까지 암호화

### 상황

- 운영 서버·파일·NAS 일제 암호화
- 백업 디스크도 함께 암호화 (네트워크 마운트 상태)
- 동기 복제본도 암호화 상태로 복사됨
- → 일반 백업·복제 전부 무력화

### 보존된 자원

- 오프라인 Tape WORM (격리 보관)
- S3 Object Lock (Compliance) Immutable
- Veeam Hardened Linux Repository (변경 불가)
- → 3중 Immutable 중 일부 살아남음

### 대응 절차

1. 격리 — 전체 NW 차단, 외부 인터넷 차단
2. 조사 — 침투 시점 파악 (감염 이전 백업 확보)
3. 깨끗한 환경 준비 — 신규 서버·OS·NW 분리
4. 복구: - Tape 또는 Object Lock에서 마지막 정상 백업 복구 - 감염 시점 이전 데이터로 환원

5. 검증 — 악성코드 잔존 검사

6. 단계적 서비스 재개

7. KISA·경찰 신고 (의무)

### 교훈

- "복제 + 백업 디스크"만 있으면 무력
- Immutable + Offline 2중이 최종 방어선
- 사후 침투 경로 차단·직원 교육·정기 훈련

## 케이스 미니 ③ — 전력 장기 정전으로 DR 절체

### < 상황

- 강남 운영 사이트 인근 변전소 화재
- 한전 2회선 모두 동시 차단
- UPS 30분 + 자가발전기 가동
- 발전기 연료 12시간분 → **장기화 우려**
- 운영팀 DR 절체 결정

### RTO/RPO 목표

- 운영 RTO 1시간 / RPO 5분
- DR 사이트: 천안 (Warm Standby + 비동기 복제)

### 절체 절차

1. 결정 — CIO 승인 (사전 정의된 의사결정 매트릭스)
2. 고객 통지 — 점검 안내 (전화·SMS·홈페이지)
3. DB 비동기 복제 종료 — 마지막 복제분 적용
4. DR DB 활성화 — Read-Only → Read-Write 전환
5. DNS 변경 / GSLB 전환 — 트래픽 DR로
6. 응용 서비스 가동 — 미리 준비된 인스턴스
7. 검증 — 헬스체크·기본 트랜잭션
8. 서비스 재개 — 30분 내
9. 사후: - 실측 RTO/RPO 기록 - Failback 일정 수립 - 운영 사이트 복전·검증 후 Failback

### 교훈

- 절체 자체보다 **Failback**이 어려움
- 정기 훈련이 실측 시간 단축의 유일한 방법

## 워크로드별 권장 매핑 — 한 페이지 결정표

| 워크로드                          | 스토리지                        | RAID             | 백업                  | DR                        |
|-------------------------------|-----------------------------|------------------|---------------------|---------------------------|
| OS 부팅 디스크                     | DAS NVMe                    | RAID 1           | 이미지 백업 (월)          | DR 사이트 동일 구성              |
| Web/WAS 로컬                    | DAS SSD                     | RAID 10          | VM 백업 (일)           | Pilot Light               |
| <b>DB (Oracle/MSSQL) — 핵심</b> | <b>SAN FC</b>               | <b>RAID 10</b>   | RMAN + Veeam, 매 4시간 | <b>Hot Standby + Sync</b> |
| DB (NoSQL-Cassandra-Mongo)    | DAS NVMe-HCI                | RAID 10 / EC     | Native + Snapshot   | Multi-DC Replication      |
| VMware 데이터스토어                 | SAN / HCI                   | RAID 6/10        | Veeam VBR (일)       | Warm Standby              |
| 파일 공유 (홀디렉-문서)                | NAS NFS/SMB                 | RAID 6           | NDMP (일)            | Async Replication         |
| 미디어-영상 마스터                    | Scale-Out NAS-Object        | EC               | LTFS Tape (월)       | Backup&Restore            |
| 로그-이벤트                        | Object Cold                 | EC               | Lifecycle (자동)      | Object Replication        |
| 백업 1차 매체                      | VTL/Backup Appliance        | RAID 6           | —                   | Tape + Object Lock        |
| 백업 2차 매체                      | Object Lock                 | EC               | —                   | Cros6-Region Replication  |
| 백업 3차 매체                      | LTO WORM                    | —                | —                   | Offsite 보관                |
| 캐시-임시                         | DAS NVMe                    | RAID 0 (or none) | 백업 안 함              | 재생성                       |
| AI 학습 데이터                     | Scale-Out NAS-Lustre-BeeGFS | EC               | 데이터셋 백업 (Object)    | 별도 정책                     |

표 한 장이 곧 워크숍·면접·실무의 기준점.

## 자주 보는 안티패턴 — 피해야 할 8가지

### ❌ 1. RAID = 백업

- RAID는 디스크 결함 대응만
- 사용자 실수·랜섬웨어 무력

### ❌ 2. 복제 = 백업

- 동기·비동기 모두 실수도 함께 복제
- 시점 복구 불가

### ❌ 3. Snapshot = 백업

- 어레이 자체 장애 시 함께 손실

### ❌ 4. 백업 = 복구 검증

- 백업 Job 성공 ≠ 실제 복구 가능
- 분기 1회 복구 시험 필수

### ❌ 5. Thin Provisioning 무한 과할당

- 실사용량 모니터링 누락
- 100% 도달 시 일제 정지

### ❌ 6. 모든 시스템 = 미션크리티컬

- 비용 비현실적
- BIA로 등급 분류 필수

### ❌ 7. 백업 디스크에만 의존

- 랜섬웨어가 NW 마운트 백업 같이 암호화
- Immutable + Offline 1종 이상 필수

### ❌ 8. DR 사이트 = 백업·복구의 끝

- 정기 훈련 없는 DR은 무용
- 절체 절차·인력 가용성 동반 필요

외부 규제 · 표준 — 백업·DR이 요구되는 근거

📄 국내 규제

- 전자금융감독규정 (금융위)
- 금융 DR 사이트 30km+
- 일 1회 이상 백업
- 분기 1회 모의 훈련
- 개인정보보호법
- 백업·복구 가능한 수단
- 안전한 보관·파기
- 정보통신망법
- 침해사고 24시간 내 신고
- 공공 SW 사업 데이터 요구사항
- 백업·보관 기간 명시

🏆 국내 인증

- ISMS-P — 정보보호·개인정보보호 관리체계
- 백업·복구 항목 점검
- CSAP — 클라우드 보안
- 백업·DR 요건

🌐 국제 표준

- ISO 27001 — 정보보호 관리체계
- 2.9.3 백업
- A.17 BCP
- ISO 22301 — BCM (사업연속성 관리)
- NIST SP 800-34 — Contingency Planning
- NIST CSF — Recover 기능
- PCI-DSS — 카드사 보안
- HIPAA — 의료 데이터 보안
- GDPR — 데이터 보호

🎯 TA의 점검 포인트

- 자사 적용 규제 목록 작성
- 규제별 백업·DR 요건 매트릭스
- 정기 점검 (분기·연)
- 인증 갱신 일정 관리

Session 6 정리 — 오늘 확보한 시야 7가지

① 스토리지 6대 유형

DAS·NAS·SAN·Object·HCI·SDS — 워크로드별 매핑

② SAN 패브릭

Director·Edge·Zoning·NPIV·WWN

③ RAID + 안전망

RAID 6/10·Hot Spare·Rebuild = 디스크 결함 안전망

④ 고급 기능

Snapshot·Replication·Dedup·Tiering·Thin Provisioning

⑤ Tape 르네상스

LTO-9·LTFS·VTL·WORM·D2D2T·D2D2C

⑥ 백업 정책 + 3-2-1-1-0

6중 정책·GFS·Immutable·Hardened·Air-Gap

⑦ DR 4단계 + 훈련 5단계

BIA → 등급 → 사이트 → 절체 → 훈련 → 사후

🎯 핵심 메시지

- RAID + 백업 + 복제 + Immutable + DR = 5중 안전망
- 검증되지 않은 백업은 존재하지 않는 백업
- RPO/RTO는 요건, 수단은 TA가 설계



IT 인프라 아키텍처 설계

# Session 7

## 보안 6대 도메인

Day 2 · 오후 후반 (약 180~200분)

네트워크 · 엔드포인트 · 데이터 · 최신 트렌드 · 거버넌스/인증 · 클라우드

강사 박수현 ·  젠아이랩스(GenAI Labs)

데이터센터 · 서버·OS·DB·GPU · 가상화·컨테이너 · 네트워크 L1~L7 · 스토리지 · 백업·DR · 보안 6대 도메인 · HA · 용량·성능·관찰성 · 설계 워크숍 · RFP · 5종 실전 케이스

IT 인프라 아키텍처 설계 · Session 7 · 보안 6대 도메인

## 왜 보안인가 — 국내 개인정보 유출 3선



### ① KB·NH·롯데카드 1억 건

2014.01 (공개)

KCB 내부 협력업체 직원이 카드 3사 고객정보 약 **1.04억 건** 유출. 역대 최대 규모.

- 주민번호·카드번호·연락처
- 외부 위탁 보안 통제 부재
- 신용카드사 「보안수칙·내부통제」 의무화

💡 **교훈** — 외부 위탁 보안 (SAC·DRM·로그 감시) + 개인정보 암호화 의무

참고: 「2014 카드 3사 정보유출」 검색



### ② LG U+ 18만 건

2023.01 (공개)

LG U+ 고객정보 약 **29만 건** (이후 추가 18만 건) 유출. 다크웹 판매 정황.

- 인증·DB 접근 통제 미흡
- DB 암호화·접근 로그 부족
- 과징금·CISO 책임 강화

💡 **교훈** — DB 보안(접근제어·암호화·감사) + ISMS-P 2.5.5 특수권한

참고: 「2023 LG유플러스 정보유출」 검색



### ③ SK텔레콤 USIM 해킹 (역대 최대)

2025.04.18 (금)

BPFdoor 악성코드로 SKT 핵심 시스템 침투 → **USIM 정보 2,695만건 + IMEI 29만건** 유출 (9.82GB).

- 국내 통신 사상 최대 개인정보 유출
- 신고 지연 → 기입 책임론
- 집단소송 3만명+ 참여
- 「통신사 보안 인프라 점검」 의무화

💡 **교훈** — EDR·XDR·BPFdoor 대응·KISA 신고 SOP·DRM·SIEM

참고: 위키백과 「2025년 SK텔레콤 유심 정보 유출 사고」

🚨 **이번 세션의 시각** — 위 3건은 모두 「위탁 보안 통제 부재」, 「DB 접근 감사 누락」, 「인증 통제 미흡」. 본 세션의 NGFW·SAC·DLP·DRM·FIDO·PKI·SIEM 6대 도메인 다층 방어가 직접 해법.

## Session 7 — 회차 메타데이터

### 📋 세션 정보

- **회차:** 8 / 15 — Day 2 오후 후반
- **소속:** Day 2 — 네트워크·스토리지·보안·HA
- **카테고리:** security (보안-거버넌스)
- **예상 분량:** 본문 78 슬라이드 + 이미지 14장
- **강의 시간:** 약 120~150분
- **강사:** 박수현 — 젠아이랩스(GenAI Labs) **CEO / CTO**

### 🎯 핵심 메시지

보안은 단일 솔루션이 아니라 **6대 도메인의 다층 방어**. TA는 모든 솔루션을 직접 구현하지 않더라도 **배치 위치·정책 흐름·인증 요구사항**을 설계한다.

### 🎯 학습 목표 (Learning Objectives)

1. **네트워크 보안** — Firewall 4세대, NGFW/UTM, WAF, IPS/IDS, Anti-DDoS, VPN 비교·선택
2. **엔드포인트 보안** — AV → EPP → EDR → XDR → MDR 진화, NAC·PMS·SIEM 역할
3. **데이터 보안** — DRM·DLP·DB보안·TDE·PKI·FIDO·HSM 배치와 운영 흐름 설계
4. **최신 보안** — CDR·SOAR·SASE·SDP·ZTNA·Zero-Trust·MITRE ATT&CK·TI·LLM 보안 조망
5. **거버넌스·인증** — ISMS·P·KCMVP·CC인증·ISO 27001·NIST CSF·PCI-DSS 인증 체계 비교

## 강의 지도 — 6 PART + 운영 보너스

### A. 네트워크 보안 (18 슬라이드)

- Firewall 4세대 진화
- NGFW · UTM · WAF
- IPS · IDS · Anti-DDoS
- APT · DPI · NDR
- VPN (IPSec·SSL·WireGuard)

### B. 엔드포인트 보안 (11 슬라이드)

- AV → EPP → EDR → XDR → MDR
- 솔루션 비교 (CrowdStrike·V3 등)
- PMS · NAC · SIEM
- SecureOS · 공급망 공격

### C. 데이터 보안 (12 슬라이드)

- DRM · DLP
- DB보안 3종 (NW·Plug-in·Kernel)
- TDE · DAM · Tokenization
- FIDO · MFA · 생체 인증
- PKI · KMS · HSM

### D. 최신 트렌드 (13 슬라이드)

- CDR · SOAR · SASE · SDP · ZTNA
- Zero-Trust · MITRE ATT&CK
- Threat Intelligence · LLM 보안

### E. 거버넌스·인증 (10 슬라이드)

- 정책 4계층 · SOP 4종
- 국내 — ISMS·P · KCMVP · CC
- 국제 — ISO 27001·NIST·PCI
- 국내 법령

### F. 보안 운영 + 실전 (12 슬라이드)

- SOC Tier 1·2·3
- VA · PT · BAS
- TA의 12대 결정

# 보안 6대 도메인 — 한눈에 보는 전체 지도

## 6대 도메인 + 횡축

- ① 네트워크 — 경계·내부 트래픽 통제
- ② 엔드포인트 — PC·서버·모바일 보호
- ③ 데이터 — 정보 자산 자체 보호
- ④ 최신 트렌드 — Zero-Trust·AI·자동화
- ⑤ 거버넌스·인증 — 정책·법규·인증
- ⑥ 클라우드 — IaaS/PaaS/SaaS 통제

## 횡으로 관통하는 축

- 사용자/계정 (Identity) — 모든 도메인의 기반
- 로그·관찰성 (SIEM) — 모든 이벤트 집중
- 거버넌스 (Policy) — 모든 통제의 근거
- 자동화 (SOAR·IaC) — 운영의 미래

6대 도메인은 독립이 아니라 다층 방어 — 한 곳이 뚫려도 다음이 막는다.



보안 6대 도메인 — 한눈에 보는 전체 지도

# 정보보안의 3대 원칙(CIA) — 다시 확인

**Confidentiality**  
기밀성 — *알아야 할 사람에게만* - 권한 없는 자 접근 금지 - 암호화·접근통제·물리 격리 - 망분리·DRM·KMS - 위반 = **유출 사고**

**Integrity**  
무결성 — *변조 없이 그대로* - 데이터 변조 차단 - 해시 (SHA-256-SM3)·전자서명 - WORM 백업·감사로그 - 위반 = **조작 사고**

**Availability**  
가용성 — *필요할 때 작동* - 서비스·데이터 사용 가능 - HA·DR·DDoS 대응 - Anti-DDoS·백업·이중화 - 위반 = **서비스 중단**

**확장 5원칙 (Parkerian Hexad):** CIA + **Authenticity(진본성)** · **Non-repudiation(부인방지)** · **Utility(유용성)** — 전자서명·PKI 시대에 추가된 축.

6대 도메인의 모든 솔루션은 CIA 중 어떤 축을 지키는가로 분류할 수 있다.

# PART A

## 네트워크 보안 — 경계와 내부 트래픽의 통제

Firewall 4세대 · NGFW · UTM · WAF · IPS · Anti-DDoS · VPN

# Firewall 4세대 진화 — Stateless → NGFW

### 1세대 — Packet Filter (Stateless)

- 헤더만 검사 (SRC/DST IP·Port·Protocol)
- 연결 상태 추적 없음
- ACL 기반 단순 통제
- 빠르지만 무지 — Spoof·반사 공격 취약

### 2세대 — Stateful Inspection (1995~)

- 연결 상태 테이블 유지
- TCP/UDP 흐름·세션 추적
- 응답 패킷 자동 허용
- Check Point FW-10이 대표

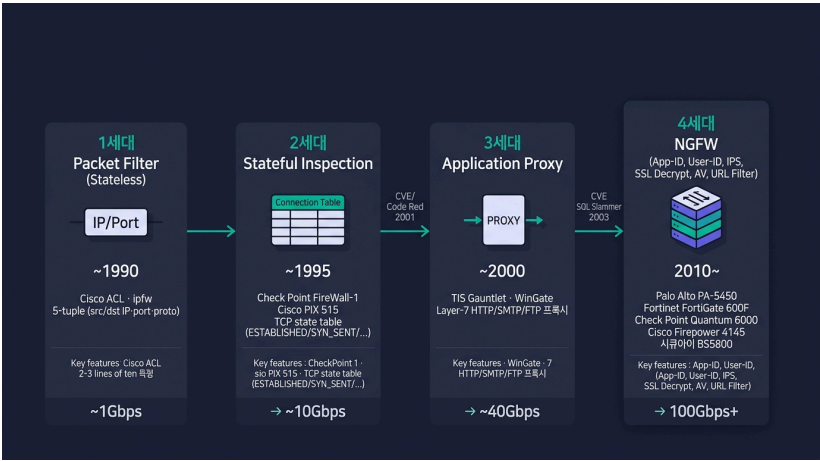
### 3세대 — Application Proxy

- L7 페이로드 검사
- 응용 계층까지 분해 (HTTP·FTP·SMTP)
- 클라이언트 ↔ Proxy ↔ 서버 (중계)
- 느리지만 강력 — 콘텐츠 통제 가능

### 4세대 — NGFW (2010~)

- Stateful + DPI + IPS + App-ID + User-ID
- SSL/TLS 인스펙션
- Threat Intelligence 연동
- Palo Alto·Fortinet·Check Point·Cisco

신규 도입은 4세대 NGFW가 표준 — 1·2세대는 백본·내부 분리용으로만 잔존.



Firewall 4세대 진화 — Stateless → NGFW

# Firewall 유형 비교 — 언제 무엇을 쓰나

| 세대        | 검사 깊이                | 성능    | 가시성 | 주 용도             |
|-----------|----------------------|-------|-----|------------------|
| Stateless | L3-L4 헤더만            | 최고    | 낮음  | 백본·라우터 ACL·간단 분리 |
| Stateful  | + 세션 추적              | 높음    | 중간  | 내부 망 경계·DMZ      |
| App Proxy | L7 페이로드              | 중간    | 높음  | 메일·FTP·웹 게이트웨이   |
| NGFW      | L3~L7 + IPS+TI       | 중간~높음 | 최고  | 외부 경계·표준         |
| UTM       | NGFW + AV/URL/VPN 통합 | 중간    | 높음  | 중소기업·지점          |

NGFW vs UTM의 차이: NGFW는 고성능 단일 기능 통합, UTM은 저비용 다기능 통합. 대기업·금융은 NGFW 다층, 중소기업·지점은 UTM 1대로 처리하는 것이 일반적.

# NGFW — 7대 핵심 기능

① Application Awareness

- L7 App-ID — 5,000+ 응용 인식
- 포트가 아닌 앱 단위 정책 (예: Facebook 차단 vs Messenger 허용)
- 모바일 앱·SaaS도 식별

② Identity Awareness

- 사용자·그룹 단위 정책
- AD/LDAP 연동
- "재무팀만 ERP 접근" 식 정책

③ IPS 통합

- 시그니처 + 휴리스틱 침입탐지
- 실시간 차단

④ SSL/TLS Inspection

- HTTPS 트래픽 복호화 → 검사 → 재암호화
- 인증서 체인 관리 필수
- 성능 부하 30~50%
- 개인정보·은행 사이트는 예외 정책

⑤ Threat Intelligence

- 외부 TI 피드 (Palo Alto WildFire·Fortinet FortiGuard)
- IoT·평판 기반 자동 차단
- 분 단위 업데이트

⑥ Sandbox 연동

- 의심 파일 가상 환경에서 실행
- APT 대응의 핵심
- WildFire·FortiSandbox

⑦ URL Filter

- 카테고리 기반 URL 차단 (도박·성인·뉴스)
- 업무 시간 통제

📊 주요 NGFW 솔루션

- Palo Alto PA-시리즈
- Fortinet FortiGate
- Check Point Quantum
- Cisco Firepower
- Sangfor · 수산INT · 시큐아이

🔗 NGFW 어플라이언스·관리 콘솔 reference - Fortinet FortiGate 600F / 3000F — fortinet.com/products/next-generation-firewall - Palo Alto PA-1410 / PA-3400 / PA-5400 — paloaltonetworks.com/network-security/next-generation-firewall - Check Point Quantum 6200 / 16200 — checkpoint.com/quantum - Cisco Firepower 9300 / 4100 — cisco.com/c/en/us/products/security/firewalls - F5 BIG-IP iSeries i7800 — f5.com/products/big-ip-services - 관리 콘솔 — FortiManager · Panorama (Palo Alto) · Cisco FMC · Check Point SmartConsole - 시큐아이·안랩 TrusGuard·수산INT — 국내 KCMVP 인증 NGFW - Linux 호스트 — iptables · nftables · firewalld (firewall-cmd) 매뉴얼

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

12 / 78

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

page 127 / 160

WAF — 웹 응용 전용 방화벽

🛡️ WAF가 막는 것 — OWASP Top 10

1. Broken Access Control

2. Cryptographic Failures

3. Injection (SQLi·XSS·Command)

4. Insecure Design

5. Security Misconfiguration

6. Vulnerable Components

7. Authentication Failures

8. Software/Data Integrity Failures

9. Logging Failures

10. SSRF (Server-Side Request Forgery)

NGFW가 막지 못하는 응용 계층 공격 전달.

🏢 WAF 솔루션 — 클라우드 vs 온프레미스

클라우드형 WAF - Cloudflare WAF · Akamai Kona - AWS WAF · Azure WAF · NCP WAF · KT Cloud WAF - 즉시 도입, 글로벌 분산 - 대규모 DDoS 흡수

온프레미스형 WAF - F5 Advanced WAF (ASM) - Imperva · Radware AppWall - Penta WafXpert · 이트원 WAF - 내부 응용 보호·법규 대응 (국정원 검증)

**TA 결정 포인트:** 외부 인터넷 노출 = 클라우드 WAF + 온프레미스 WAF 2단이 표준. 내부망 응용은 온프레미스 WAF만으로 충분.

🏠 WAF 어플라이언스·콘솔 reference - F5 BIG-IP Advanced WAF / ISeries i7800 — f5.com/products/big-ip-services/advanced-waf - Imperva SecureSphere WAF Gateway — imperva.com/products/web-application-firewall-waf - Cloudflare WAF Dashboard — cloudflare.com/application-services/products/waf - AWS WAF Console — aws.amazon.com/waf - Akamai Kona Site Defender — akamai.com/products/kona-site-defender - 국내 — 펜타시큐리티 WAPPLES · 이트원 WAF (KCMVP)

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

13 / 78

#256

IT 인프라 아키텍처 설계 · Session 7 · 보안 6대 도메인

WAF — 웹 응용 전용 방화벽

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

14 / 78

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

page 128 / 160

# UTM — *Unified Threat Management*



## UTM 1대에 들어가는 기능

- **Firewall** (Stateful·NGFW급)
- **IPS/IDS**
- **VPN** (IPSec·SSL VPN)
- **Anti-Virus** (Gateway AV)
- **Anti-Spam** (메일 필터)
- **URL Filter · Web Filter**
- **DLP** (간단한 키워드·패턴)
- **App Control**
- **SD-WAN** (최신형)



## 도입 패턴

- **본사** — NGFW 다층 + 별도 IPS·WAF
- **지점·소규모** — UTM 1대로 일괄 처리
- **사용자 수** — 50~500명 규모가 sweet spot
- **HA** — UTM 2대 Active-Passive



## 대표 솔루션

- **Fortinet FortiGate** (UTM 시장 1위)
- **Sophos XG · WatchGuard · SonicWall**
- **국내** — 안랩 TrusGuard · 이트론 · 수산INT
- **가격** — 동급 NGFW의 60~70%

UTM은 **AIO(AI-In-One)**의 편리함과 **단일 장애점**의 트레이드오프 — 지점·소규모에 적합.

# IPS vs IDS — 탐지냐 차단이냐



## IDS (Intrusion Detection System)

- **Tap 모드** — 트래픽 복사본만 감시
- 탐지만 (차단 불가)
- 오탐 영향 적음
- 분석·포렌식 중심
- **신호 + 알람**
- 대표: Snort·Suricata·국정원 인증 IDS

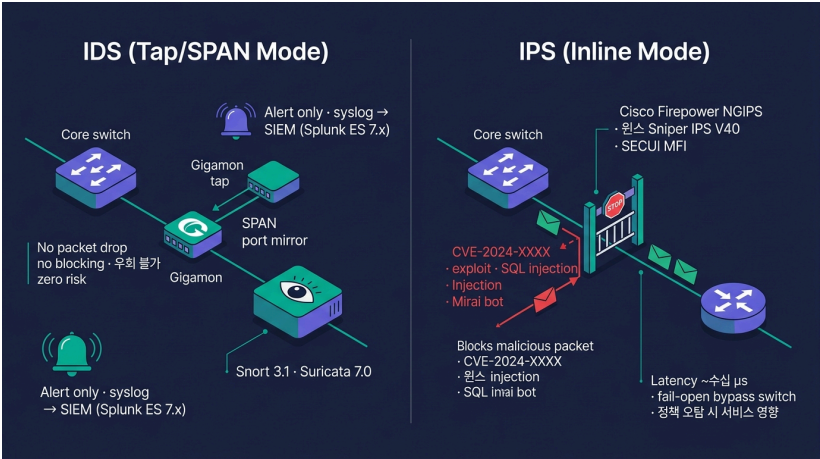


## IPS (Intrusion Prevention System)

- **Inline 모드** — 트래픽 경로상 위치
- 탐지 + **차단**
- 오탐 = 정상 트래픽 차단 사고
- 실시간 대응
- **신호 + 차단**
- 대표: Palo Alto·Fortinet·시큐아이 IPS

**현실의 운영:** 신규 도입은 99% IPS(NGFW 내장 또는 별도 어플라이언스). IDS는 **로그 수집·SIEM 연동 분석**용으로 잔존. **국내 보안기능 확인서 IPS 6종**이 공공 표준.





IPS vs IDS — 탐지냐 차단이냐

## Anti-DDoS — 대량 트래픽 차단



### DDoS 7대 유형

1. **Volumetric** — UDP Flood · ICMP Flood
2. **Reflection/Amplification** — DNS · NTP · Memcached
3. **TCP State Exhaustion** — SYN Flood
4. **Application Layer** — HTTP GET/POST Flood
5. **Slowloris · R-U-Dead-Yet** — 저속 고갈
6. **DNS Query Flood**
7. **Encrypted (SSL) Flood**



### 대응 방식 3단계

- **Scrubbing Center** — 트래픽 우회·정화 (Akamai Prolexic · Cloudflare Magic Transit)
- **BGP FlowSpec** — ISP에 차단 규칙 전파
- **RTBH** (Remotely Triggered Black Hole) — 공격 대상 IP 트래픽 폐기



### 솔루션·서비스

- **클라우드 흡수형** — Cloudflare · AWS Shield Advanced · Akamai · Cloudbric
- **온프레미스 어플라이언스** — Radware DefensePro · Arbor (NETSCOUT) · A10 Thunder · Genie Networks
- **국내** — KT · LG U+ · SK 통신사 Anti-DDoS 서비스
- **국정원 보안기능 확인서 DDoS 6종 인증 제품**



### TA 결정 포인트

- **회선 대역** > 공격 규모 → 자체 방어 가능
- **회선** < 공격 → **상위 ISP · 클라우드 흡수 필수**
- **하이브리드** — 평소 온프레, 임계 초과 시 클라우드 자동 우회

# APT — *Advanced Persistent Threat*



### APT의 특징

- 지속·은밀·표적
- 평균 잠복 기간 **200일+**
- 국가·산업 스파이·해커그룹
- 사례 — 농협·KBS·청와대·SK텔레콤
- 일반 시그니처로 탐지 불가



### APT Kill Chain (Lockheed Martin)

- Reconnaissance** (정찰)
- Weaponization** (무기화)
- Delivery** (전달)
- Exploitation** (취약점 악용)
- Installation** (설치)
- C2** (Command & Control)
- Actions on Objectives** (목적 달성)



### APT 대응 핵심

- Sandbox 기반 탐지** — 알려지지 않은 악성코드 실행 검사
- C&C 채널 차단** — 평판 기반 IP·도메인 차단
- 이메일 첨부 무해화 (CDR)**
- EDR + NDR 연동** — 호스트·네트워크 통합
- 위협 인텔리전스 (TI)** 연동



### APT 솔루션

- FireEye** (Trellix·NX/EX/HX)
- Palo Alto WildFire**
- Trend Micro Deep Discovery**
- 국내** — 안랩 MDS · 윈스 Sniper APT · 시큐레터

# DPI · NDR — *심층 패킷 검사와 네트워크 탐지*



### DPI (Deep Packet Inspection)

- 패킷 **페이로드까지** 분석
- 응용 식별·콘텐츠 검사
- NGFW·IPS·QoS의 기반 기술
- ISP 트래픽 분석에도 활용
- 암호화 트래픽**은 SSL Inspection 결합 필요



### 활용 영역

- 응용 인식 (App-ID)
- DLP (콘텐츠 검사)
- QoS (응용별 우선순위)
- 합법 감청 (CALEA·국내 통신비밀보호법)



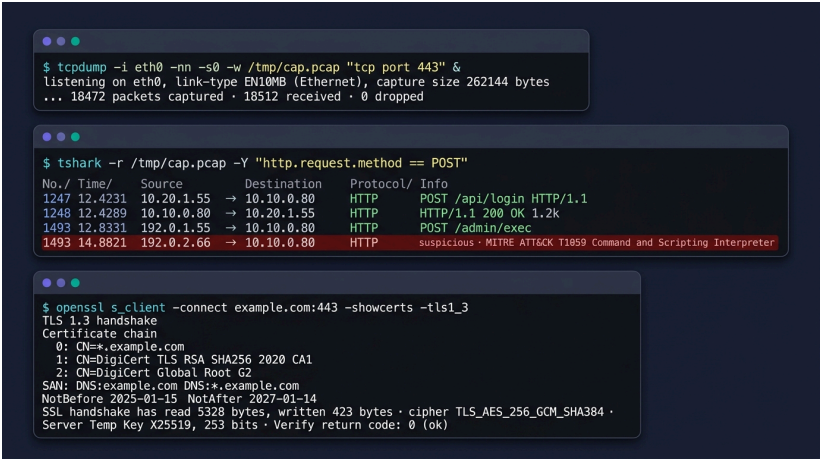
### NDR (Network Detection & Response)

- 네트워크 트래픽 메타데이터 + AI/ML**
- 시그니처가 없어도 이상 행위 탐지
- East-West (내부 횡 이동)** 가시성
- C&C 통신·데이터 유출 탐지
- EDR의 네트워크판



### NDR 솔루션

- Darktrace · ExtraHop Reveal(x)**
- Vectra AI · Corelight · Cisco Secure Network Analytics (Stealthwatch)**
- 국내** — 시큐레터·시큐아이 NDR



DPI · NDR — 심층 패킷 검사와 네트워크 탐지

# VPN — 네 가지 표준 + 신형 두 가지

### IPSec VPN

- 표준 RFC 4301 · 게이트웨이↔게이트웨이
- Site-to-Site (지사↔본사)·Client-to-Site
- IKE (키 교환)·ESP (암호+무결성)·AH (무결성만)
- Tunnel 모드 (전체 IP 캡슐화) vs Transport 모드 (페이로드만)
- DMVPN (Cisco) — IPSec + GRE + NHRP, Hub-Spoke 동적

### SSL VPN

- 브라우저 HTTPS 또는 클라이언트 SW
- 사용자 단위 원격 접속에 최적
- Pulse-Cisco AnyConnect·F5·Fortinet·NCP

### OpenVPN

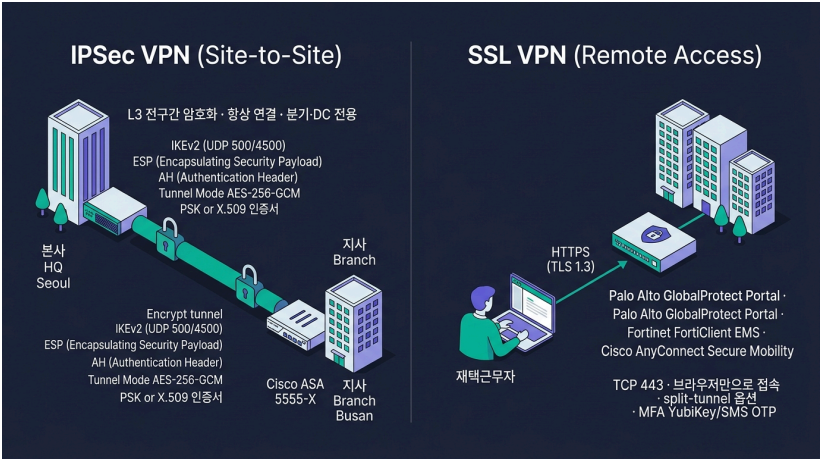
- 오픈소스·TLS 기반
- 포트 1194 (UDP/TCP)
- 중소기업·SMB 표준
- 라이선스 비용 0

### WireGuard

- 차세대 표준 (2020~)
- Linux 커널 내장
- 코드 4,000줄 (vs OpenVPN 600,000줄)
- 빠르고 단순·NAT 우회 강력
- Tailscale·Twingate가 활용

### 망분리 환경

- 망연계 솔루션 (한 방향) — 시큐웍스 SecuwayLink·소만사



VPN — 네 가지 표준 + 신흥 두 가지

# VPN 결정 매트릭스 — 언제 어느 것?

| 시나리오              | 권장 VPN               | 이유                |
|-------------------|----------------------|-------------------|
| 본사 ↔ 지사 상시        | IPSec Site-to-Site   | 안정·표준·대역 활용       |
| 재택근무 사용자          | SSL VPN 또는 WireGuard | 클라이언트 단순·HTTPS 통과 |
| 외부 협력사 한시적        | SSL VPN + MFA        | 사용자 단위·세분화        |
| 다수 지점 (Hub-Spoke) | DMVPN                | 동적 터널·관리 단순       |
| 오픈소스·저예산          | OpenVPN              | 무료·검증·널리 호환       |
| 차세대·고성능           | WireGuard            | 단순·빠름             |
| 공공·금융 망연계         | 단방향 게이트웨이            | 망분리 의무            |
| 클라우드 VPC 연결       | Cloud VPN (IPSec)    | AWS/Azure 표준      |

TA 결정 4축: ① 사용자 vs 사이트 단위, ② 클라이언트 SW 설치 가능 여부, ③ 인증·암호화 강도 요구, ④ 운영 인력 역량.

Part A 정리 — 네트워크 보안 9가지

경계 보안

- **NGFW** — 4세대 통합 방화벽
- **WAF** — OWASP Top 10 차단
- **UTM** — 중소·지점 통합형

트래픽 통제

- **IPS/IDS** — Inline vs Tap
- **Anti-DDoS** — Scrubbing·RTBH

위협 탐지

- **APT 대응** — Sandbox + Kill Chain
- **NDR** — 네트워크 이상행위 AI 탐지
- **DPI** — L7 페이로드 분석

원격 접속

- **IPSec/SSL/OpenVPN/WireGuard**
- **DMVPN** — Hub-Spoke
- **단방향 GW** — 망분리 필수

TA 결정 7가지

1. 외부 경계 방화벽 세대
2. WAF 위치 (클라우드 vs 온프레)
3. IPS 도입 (NGFW 내장 vs 별도)
4. Anti-DDoS 자체 vs 통신사
5. APT 솔루션 도입 여부
6. VPN 종류·이중화
7. 망분리 수준 (논리 vs 물리)

PART B

엔드포인트 보안 — PC·서버·모바일의 마지막 방어선

AV → EPP → EDR → XDR → MDR · NAC · PMS · SIEM · SecureOS

엔드포인트 보안 5세대 진화

1세대 — Anti-Virus (1990~)

- 시그니처 기반 — 알려진 악성코드만
- 매일 패턴 업데이트
- 한계: 신종·변종·Zero-day 대응 불가
- 대표: 안랩 V3·이스트시큐리티 알약·Symantec Endpoint Protection·McAfee

2세대 — EPP (Endpoint Protection Platform)

- AV + 방화벽 + 디바이스 통제
- 휴리스틱·행위 기반 추가
- 통합 콘솔
- 대표: Trend Micro Apex One (구 OfficeScan)·Symantec Endpoint Protection·McAfee EPS

3세대 — EDR (Endpoint Detection & Response)

- IoC·이상 행위·시계열 기반
- 모든 프로세스·파일·네트워크 행위 기록
- 사고 발생 후 포렌식·롤백 가능

4세대 — XDR (Extended Detection & Response)

- Endpoint + Network + Cloud + Identity 통합
- 다층 텔레메트리 상관 분석
- AI/ML 자동 분류·우선순위
- 대표: Palo Alto Cortex XDR·CrowdStrike Falcon·SentinelOne Singularity·Microsoft Defender XDR

5세대 — MDR (Managed Detection & Response)

- 외부 SOC 24/7 위탁 운영
- 자체 보안 인력 부족 기업용
- 솔루션 + 인력 패키지
- 대표: CrowdStrike Falcon Complete·SentinelOne Vigilance·Arctic Wolf-Expel

1세대 AV는 더 이상 충분하지 않다 — EDR/XDR + MDR이 2026 신규 도입 표준.

EDR — 동작 원리와 분석 흐름

🎯 수집 데이터

- 프로세스 생성·종료
- 파일 읽기·쓰기·삭제
- 네트워크 연결 (IP·포트·도메인)
- 레지스트리 변경 (Windows)
- PowerShell·CMD 명령
- DLL 로드·인젝션
- 사용자 로그인·권한 상승

🧠 분석 방법

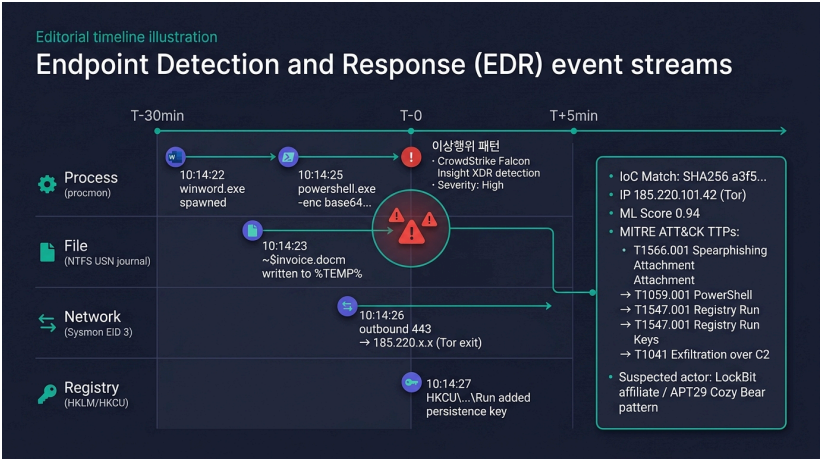
- IoC 매칭 (해시·도메인·IP)
- 행위 기반 (MITRE ATT&CK TTP)
- ML 이상 탐지·시계열 상관

🛡️ 대응 (Response)

- 격리 (Network Containment)
- 프로세스 강제 종료
- 파일 격리·삭제·롤백
- 레지스트리 복원
- 원격 셀·라이브 응답
- 자동 차단 Playbook

📊 운영 관점

- 튜닝 기간 3~6개월 · 오탐 최소화 핵심
- SOC Tier 1·2 인력 필수
- MDR 위탁 시 인력 부담 ↓



EDR — 동작 원리와 분석 흐름

## XDR — *Extended Detection & Response*

### XDR의 통합 범위

- **Endpoint** (EDR)
- **Network** (NDR-NGFW 로그)
- **Cloud** (CSPM-CASB-CloudTrail)
- **Identity** (AD-Okta-IAM)
- **Email** (Email Security)

### 핵심 차별점

- 다층 텔레메트리 **상관 분석**
- 단일 사건 → **공격 캠페인** 재구성
- AI/ML로 우선순위 자동화
- **MTTD/MTTR 단축**

### SIEM vs XDR

- **SIEM** — 로그 수집·검색·룰 기반 (범용)
- **XDR** — 보안 도메인 특화 통합 분석

둘은 대체가 아니라 **보완** — XDR이 1차 자동 분석, SIEM이 통합 보존·감사.

### 대표 XDR 솔루션

- Palo Alto Cortex XDR
- CrowdStrike Falcon XDR
- Microsoft Defender XDR
- Trend Vision One
- Cisco XDR (구 SecureX)

# PMS — Patch Management System



## 왜 PMS인가

- 취약점 = Zero-day의 99%는 패치 미적용
- 수동 패치 = 누락·지연·검증 불가
- 공공·금융은 30일 이내 보안 패치 의무
- 자산 대수 100대 넘으면 자동화 필수



## 주요 기능

- 취약점 스캐닝 (CVE 매칭)
- 패치 배포 스케줄
- 사전 검증 (Pilot Group)
- 롤백·강제 리부트
- 준수 보고서 (감사 대응)



## 솔루션

- Microsoft WSUS / SCCM (MECM) — Windows 표준
- Red Hat Satellite — RHEL
- Ivanti · ManageEngine Patch Manager
- 국내 — 안랩 APC·소만사 PMS·지란지교 PMS



## 한국 특수성

- 공공 보안 가이드 — 패치 30일 이내
- 분기별 모의 점검 — 미패치 0건 목표
- 1년 누적 미패치 발견 시 감사 지적



## 보안기능 확인서

- 국정원 인증 PMS 제품이 공공 표준

# 공급망 공격 — Supply Chain Attack



## 사례

- log4j (2021) — Apache 로깅 라이브러리 RCE, 전 세계 영향
- SolarWinds (2020) — Orion 패치에 백도어 삽입
- Kaseya VSA (2021) — RMM 솔루션 통한 랜섬웨어
- MOVEit (2023) — 파일 전송 SW RCE
- 3CX (2023) — VoIP 클라이언트 변조
- 국내 — 공공 SW 업데이트 채널 공격 시도



## 공격 경로

- 오픈소스 라이브러리 (npm·PyPI·Maven)
- 유료 SW 업데이트 채널
- DevOps 파이프라인 (Git·CI/CD)
- 하드웨어 펌웨어
- 외주·MSP



## 대응 7가지

1. SBOM (Software Bill of Materials) — 구성요소 목록화
2. 의존성 스캐닝 (Snyk·Dependabot·OWASP Dep-Check)
3. 이미지 서명 검증 (Sigstore·Cosign·Notary)
4. SLSA Framework (Supply-chain Levels for Software Artifacts)
5. CI/CD 파이프라인 보안 (인증·시크릿 관리)
6. 벤더 보안 점검 (SOC 2·ISO 27001 요구)
7. EDR/XDR이 변조 패치 탐지 (행위 기반)



## TA 인식

- 자체 보안만으로는 부족 — 공급사슬 전체 가시성이 필요
- 미국 EO 14028, 유럽 CRA, 한국도 가이드 강화 중



# NAC — Network Access Control

## NAC의 역할

- "누가 들어왔나" — 사용자·단말 인증
- "상태는?" — Posture Assessment (AV·패치·OS)
- "어디로?" — VLAN 자동 할당
- "격리" — 비인가·미준수 단말 격리망

## 인증 방식

- 802.1X — 표준 포트 단위 인증 (EAP-TLS·EAP-PEAP)
- MAC 인증 — MAC 화이트리스트
- Captive Portal — 웹 로그인 (Wi-Fi·게스트)
- Agentless — Fingerprinting 기반

## Posture Assessment

- AV 설치·최신화 확인
- OS 패치 수준
- 방화벽 활성화
- 인가 SW 외 차단
- 부적합 → 격리 VLAN → 자동 교정 → 재인증

## 솔루션

- Cisco ISE — 글로벌 1위
- Aruba ClearPass
- Forescout (CounterACT) — Agentless 강자
- 국내 — Genians NAC·시큐브 SecuwayNAC·원스 NAC
- 공공 KCMVP·보안기능 확인서 NAC 6종

# ESM vs SIEM — 통합 보안 관제의 두 세대

## ESM (Enterprise Security Management)

- 2000년대 통합 보안 관제 1세대
- 보안 장비 이벤트 통합·정규화
- 실시간 알람·대시보드
- 상관 분석 약함
- 국내 — 이글루시큐리티 SPiDER·안랩 TMS·LG CNS ESM

## SIEM (Security Information & Event Management)

- ESM + 빅데이터·상관 분석·룰 엔진
- 전 IT 로그 통합 (보안 + 시스템 + 응용)
- 컴플라이언스 보고서 자동화
- 장기 보존 6개월~1년+
- 머신러닝 이상 탐지 (UEBA)

## SIEM 솔루션

- Splunk Enterprise Security — 시장 1위·고가
- IBM QRadar — 금융권 강자
- Micro Focus ArcSight — 정부·통신
- Elastic SIEM — 오픈소스·비용 절감
- LogRhythm · Securonix · Exabeam
- 국내 — 이글루 SPiDER TM·안랩 TMS·LG U+ SecureNet

## TA 결정

- 로그량 (EPS) 기반 라이선스
- 보존 기간 (1년 vs 3년)
- 상관 룰 작성 인력 보유 여부
- MDR 위탁 가능성

📚 SIEM 콘솔 reference - Splunk Enterprise Security — [splunk.com/en\\_us/products/enterprise-security.html](https://splunk.com/en_us/products/enterprise-security.html) - IBM QRadar SIEM — [ibm.com/products/qradar-siem](https://ibm.com/products/qradar-siem) - Microsoft Sentinel — [azure.microsoft.com/products/microsoft-sentinel](https://azure.microsoft.com/products/microsoft-sentinel) - Elastic SIEM — [elastic.co/security/siem](https://elastic.co/security/siem) - 이글루코퍼레이션 SPiDER TM · 안랩 TMS — 국내 SIEM



ESM vs SIEM — 통합 보안 관제의 두 세대

Part B 정리 — 엔드포인트 보안 8가지

### 5세대 진화

- AV → EPP → EDR → XDR → MDR
- 한국 표준 = **EDR + MDR** 위탁

### 운영 솔루션

- PMS** — 30일 패치 의무
- NAC** — 단말 인증·격리
- SecureOS** — 커널 강화

### 통합 관제

- ESM → SIEM → XDR**
- EPS·보존기간 기준 라이선스
- MDR 위탁 옵션

### TA 결정 6가지

- EDR 솔루션 선택 (KCMVP 여부)
- MDR 자체 vs 위탁
- PMS 도입 시점
- NAC 802.1X vs MAC
- SIEM EPS·보존기간
- SecureOS 적용 범위

### 공급망 보안

- SBOM·의존성 스캔
- 이미지 서명·SLSA
- 벤더 SOC 2 요구

### 한국 공공 표준

- KCMVP 인증 EDR
- 패치 30일 의무
- NAC·SecureOS 점진 의무화

# PART C

## 데이터 보안 — 정보 자산 자체를 지키는 기술

DRM · DLP · DB보안 · TDE · PKI · FIDO · KMS/HSM

IT 인프라 아키텍처 설계 · Session 7 · 보안 6대 도메인

## DRM — Digital Rights Management



### DRM의 본질

- 문서·파일 자체에 암호화 + 권한 정책 결합
- 외부로 유출되어도 권한 없으면 열람 불가
- 한국 기업 보안의 트레이드마크 — 글로벌엔 거의 없음



### 통제 항목 — CRWDNO

- Copy — 복사
- Read — 읽기
- Write — 편집
- Delete — 삭제
- Net — 전송
- Output — 출력·캡처



### 핵심 기술

- AES-256 파일 암호화
- Watermarking — 인쇄·캡처 시 사용자 식별 워터마크
- 권한 서버 — 열람할 때마다 정책 확인
- 오프라인 정책 — 일정 시간 후 만료



### 솔루션 (한국 시장)

- Fasoo (파수) — 시장 1위·금융·공공
- 마크애니 (MarkAny) — 미디어·문서 워터마크
- 소프트캠프 (Softcamp) — 한컴 그룹
- 이니텍·세이프넷



### 운영 이슈

- 응용 호환성 항상 검증 필요 (Office·CAD 등)
- 권한 서버 장애 시 전사 업무 중단

# DLP — Data Loss Prevention

## DLP 3대 배치

- **Endpoint DLP** — PC·노트북 에이전트
- USB·프린트·캡처·메신저 통제
- **Network DLP** — 게이트웨이
- 이메일·웹·FTP 트래픽 검사
- **Storage DLP** (Data-at-Rest)
- 파일서버·DB 스캔·분류·암호화

## 검출 기법

- 키워드·정규식 (주민번호·카드번호)
- 데이터 식별자 (Document Fingerprint)
- 머신러닝 분류
- **OCR** — 이미지 내 문자

## DLP 정책 예

- 주민번호 10건+ 이메일 → 차단 + 알림
- 카드번호 외부 송신 → 암호화 강제
- 기밀 등급 문서 → 외부 전송 차단
- USB 복사 → 승인 후 허용

## 솔루션

- Symantec DLP (Broadcom) · Trellix DLP (구 McAfee)
- Forcepoint DLP · Digital Guardian
- Microsoft Purview DLP (M365 통합)
- 국내 — 소만사 i-DLP·지란지교 OfficeKeeper DLP·시큐브 DLP
- 공공 보안기능 확인서 DLP 인증 제품

# DB 보안 3종 — 접근·감사·암호화

## DB 접근제어 (DAC)

- 사용자 ↔ DB 사이에 Proxy
- 쿼리 단위 인증·인가
- 세션 녹화
- 마스킹 (응답 데이터 가리기)
- 대표 — 펜타시큐리티 D'Amo·신시웨이 Petra·이글루 SAS

## DB 감사 (DAM)

- 모든 쿼리 로그 수집
- 외부 분석·이상 행위 탐지
- 컴플라이언스 보고서
- 4가지 수집 방식:
- **Network Sniff** — 무영향
- **Plug-in / Agent** — DB 내 후크
- **API / Trigger** — 응용 변경
- **Kernel Hook** — OS 수준

## DB 암호화

- **TDE (Transparent Data Encryption)**
- DB 엔진 차원 자동 암호화
- Oracle Advanced Security-MSSQL TDE-MySQL Enterprise
- **Column-level**
- 특정 컬럼만 (주민번호·카드)
- **Tokenization**
- 원본 → 무의미한 토큰 치환
- PCI-DSS 표준 대응

## 결합 운영

- DAC + DAM + TDE = 3종 풀세트
- 공공·금융 표준

## 한국 솔루션

- 펜타시큐리티 D'Amo — 시장 1위
- 신시웨이 Petra
- 이글루코퍼레이션 SAS
- 이니텍·웨어밸리
- 글로벌 — Imperva SecureSphere·IBM Guardium

## TA 결정

- 운영 DB 부하 영향
- 응용 코드 수정 필요 여부
- KCMVP·보안기능 확인서 요구

## FIDO · MFA — 비밀번호 없는 인증

## FIDO 표준 진화

- **FIDO U2F** (2014) — USB 보안키 + 비밀번호
- **FIDO UAF** (2014) — 모바일 생체 인증
- **FIDO2 / WebAuthn** (2019) — 브라우저 표준-비밀번호 완전 대체

 **인증 요소 3가지**

- **소유 (Possession)** — 휴대폰·OTP·보안키
- **지식 (Knowledge)** — 비밀번호·PIN
- **고유 (Inherence)** — 지문·홍채·얼굴·정맥

MFA = 2개 이상 요소 결합

#### MFA 종류

- **OTP** — HOTP-TOTP (Google Authenticator)
- **SMS OTP** — 보안 약함 (SIM Swap)
- **Push 알림** — Duo-MS Authenticator
- **하드웨어 토큰** — YubiKey-Feitian
- **생체** — TouchID-FaceID-Windows Hello
- **카드 인증서** — 공동인증서·금융인증서

 한국 인증 시장

- 공동인증서 (구 공인인증서)
- 금융인증서
- 간편인증 — 카카오톡·네이버·PASS·토스
- FIDO 협회 (Korea FIDO Alliance)

[FIDO 보안키-생체인증 reference](#) — [YubiKey 5 Series](#) — [yubico.com/products/yubikey-5-overview](#) — [Google Titan Security Key](#) — [store.google.com/product/titan\\_security\\_key](#) — [Feitian FIDO2 키](#) — [ftsafe.com](#) - [지문/얼굴 단말](#) — [Suprema BioStation](#) · [iDemia MorphoWave](#) - [Apple Passkey](#) / [Windows Hello](#) — [FIDO2 OS 내장 인증](#)



FIDO · MFA — 비밀번호 없는 인증

PKI — *Public Key Infrastructure*

 PKI 구성 요소

- **CA (Certificate Authority)** — 인증서 발급·서명
- **RA (Registration Authority)** — 신청자 신원 확인
- **Subscriber** — 인증서 발급자
- **Relying Party** — 인증서 검증자
- **CRL (Certificate Revocation List)** — 폐기 목록
- **OCSP** — 실시간 폐기 조회

 X.509 인증서 항목

- 발급자(Issuer)·주체(Subject)
- 공개키·서명 알고리즘
- 유효기간·확장 필드
- CN·SAN

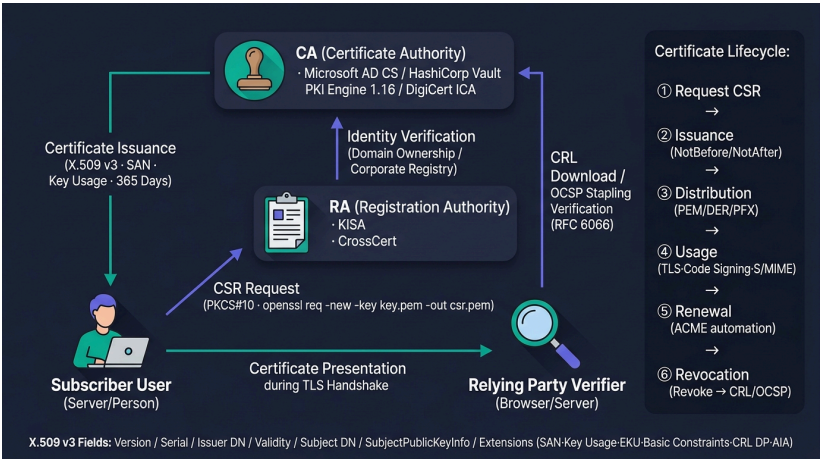
 인증서 수명주기

1. **CSR 생성** (개인키·공개키)
2. **신원 확인** (RA)
3. **발급** (CA 서명)
4. **배포·사용**
5. **갱신** (만료 전 30일)
6. **폐기** (탈취·이직 시)

 한국 CA

- **공인인증기관** (구) — 금융결제원·한국정보인증·코스콤·한국전자인증·한국무연정보통신
- **사설 CA** — 사내용 (AD CS·OpenSSL)
- **글로벌** — Let's Encrypt·DigiCert·Sectigo·GlobalSign

 **PKI-인증서 reference** - X.509 인증서 구조 — RFC 5280 / DigiCert blog - OpenSSL CLI 매뉴얼 — openssl.org/docs/man3.0 ( [openssl x509](#), [openssl s\\_client](#), [openssl req](#) ) - Microsoft Active Directory Certificate Services (AD CS) Console — learn.microsoft.com/windows-server/identity/ad-cs - 한국 공동인증서·금융인증서 — yesign.or.kr · 금융결제원 - Let's Encrypt / Certbot — letsencrypt.org · certbot.eff.org



PKI — *Public Key Infrastructure*

# 전자서명 vs 전자봉투 — PKI 두 가지 활용

## ✂ 전자서명 (Digital Signature)

- 목적: 무결성 + 부인방지
- 송신자의 **개인키**로 서명
- 수신자가 **송신자 공개키**로 검증
- 평문 + 서명 함께 전달
- 누구나 평문 열람 가능
- 예: PDF 서명·계약·API 서명

## ✉ 전자봉투 (Digital Envelope)

- 목적: 기밀성 + 무결성
- 평문을 **세션키(대칭키)**로 암호화
- 세션키를 **수신자 공개키**로 암호화
- 수신자만 개인키로 세션키 복호 → 평문 복호
- 외부에 노출되지 않는 비밀 전달
- 예: 암호화 메일·DRM

왜 세션키를 쓰냐: 공개키 암호는 느리고 큰 데이터 부적합. 빠른 대칭키로 본문 암호화 + 작은 세션키만 공개키로 → 속도+보안 동시 달성.

# KMS · HSM — 키 관리의 인프라

## 🔑 KMS (Key Management System)

- 암호 키 **생성·저장·회전·폐기**
- 응용은 키를 직접 보지 않고 **사용 API**만 호출
- 정책 기반 키 사용 제어
- 감사 로그 자동

### 🏢 솔루션

- **AWS KMS** · **Azure Key Vault** · **GCP KMS**
- **HashiCorp Vault** — 오픈소스
- **Thales CipherTrust Manager**
- **국내** — 펜타시큐리티 D'Amo KMS·시큐브·이니텍

## 🛡 HSM (Hardware Security Module)

- 물리 보안 칩 안에 **개인키 보관**
- **반출 불가** — 외부에서 키 추출 불가
- FIPS 140-2 / FIPS 140-3 인증
- **Level 2** — 변조 흔적 탐지
- **Level 3** — 변조 시 자동 삭제
- **Level 4** — 모든 변조 대응

### 📄 KCMVP

- 한국 **국정원 암호모듈 검증**
- 공공·금융은 KCMVP 필수
- **검증필 암호 모듈** 사용 의무

### 🏢 HSM 솔루션

- **Thales Luna** · **Entrust nShield** · **Utimaco**
- **국내** — 펜타시큐리티·시큐브·이니텍 HSM

📖 **HSM 어플라이언스 reference** - Thales Luna Network HSM 7 — [cpl.thalesgroup.com/encryption/hardware-security-modules](https://cpl.thalesgroup.com/encryption/hardware-security-modules) - Entrust nShield Connect XC (구 nCipher) — [entrust.com/products/hsm](https://entrust.com/products/hsm) - Utimaco SecurityServer CSe — [utimaco.com/products/general-purpose-hsm](https://utimaco.com/products/general-purpose-hsm) - AWS CloudHSM — [aws.amazon.com/cloudhsm](https://aws.amazon.com/cloudhsm) - 국내 — 펜타시큐리티 ISIGN+ HSM · 시큐브 SecuKMS (KCMVP 검증필 암호 모듈)



KMS · HSM — 키 관리의 인프라

## Part C 정리 — 데이터 보안 8가지

### 콘텐츠 보호

- **DRM** — CRWDNO 통제
- **DLP** — Endpoint-NW-Storage 3종

### DB 보안

- **DAC** — 접근제어 Proxy
- **DAM** — 감사 로그
- **TDE** — 컬럼-Tokenization

### 인증·신원

- **FIDO U2F/UAF/FIDO2**
- **MFA** — 3대 요소 조합
- 한국 — 공동/금융인증서-간편인증

### 키·서명

- **PKI** — CA-RA-CRL-OCSP
- 전자서명-전자봉투
- **KMS / HSM** — FIPS-KCMVP

### TA 결정 7가지

1. DRM 적용 범위 (전사·기밀만)
2. DLP 3종 중 우선 도입
3. DB 보안 3종 모두 vs 부분
4. FIDO2 도입 시점
5. PKI 자체 운영 vs 공인 CA
6. KMS SaaS vs 온프레
7. KCMVP HSM 필수성

### 한국 특수성

- **DRM·DB보안 3종** 강세
- KCMVP·보안기능 확인서



# PART D

## 최신 보안 트렌드 — *Zero-Trust* 시대

CDR · SOAR · SASE · SDP · ZTNA · Zero-Trust · MITRE ATT&CK · TI · LLM 보안

IT 인프라 아키텍처 설계 · Session 7 · 보안 6대 도메인

## CDR — *Content Disarm & Reconstruction*



### CDR이 하는 일

- 문서·파일에서 **위험 요소 제거 후 재구성**
- 매크로·스크립트·임베디드 OLE·JavaScript 제거
- **알려지지 않은 악성코드도 무력화** (Sandbox와 보완)
- 사용자에게는 **정상 콘텐츠만** 전달



### 대상 파일

- Office (DOC·XLS·PPT)
- PDF (JavaScript·Form)
- HWP (한컴) — 한국 특수
- ZIP·이미지·CAD



### 배치 위치

- **메일 게이트웨이** — 첨부 무해화
- **웹 다운로드** — 파일 다운로드 무해화
- **망 연계 솔루션** — 망 간 자료 이동 시 무해화
- **USB 키오스크** — 외부 매체 무해화



### 솔루션

- **OPSWAT MetaDefender** — 글로벌 1위
- **Sasa Software Gate Scanner**
- 국내 — 지란지교 **OfficeKeeper** / 한국 CDR, 소프트캡프 **SHIELDEX**, 시큐레터

# SOAR — Security Orchestration, Automation & Response



### SOAR가 하는 일

- 보안 이벤트 → **Playbook** 자동 실행
- SIEM·EDR·NGFW·TI 등 다수 도구 오케스트레이션
- 반복 작업 자동화
- SOC Tier 1 부담 70%+ 감소



### Playbook 예시

- 피싱 이메일 신고 → 자동 분석 → 격리 → 차단·통지
- 의심 IP 탐지 → TI 조회 → NGFW 차단 → 티켓 발행
- 사용자 계정 이상 → 잠금 → 알림 → 조사



### SOAR 솔루션

- Splunk SOAR** (구 Phantom)
- Palo Alto Cortex XSOAR** (구 Demisto)
- IBM Resilient** (QRadar SOAR)
- Microsoft Sentinel Playbook**
- Swimlane · Tines · Torq



### TA 결정

- SIEM과의 통합 호환성
- Playbook 작성 인력
- TI 피드 비용
- 자동 차단 vs 승인 후 실행

SOAR 도입 = SOC 자동화의 출발점.

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

51 / 78

#294

IT 인프라 아키텍처 설계 · Session 7 · 보안 6대 도메인

# SASE — Secure Access Service Edge



### SASE의 정의 (Gartner, 2019)

- SD-WAN + 보안 스택**의 클라우드 통합
- 사용자·디바이스가 어디 있든 **동일 정책**
- 본사 백홀 불필요 — SaaS 직접 통신



### 보안 스택 구성

- FWaaS** — Firewall as a Service
- SWG** — Secure Web Gateway
- CASB** — Cloud Access Security Broker
- ZTNA** — Zero Trust Network Access
- DLP·RBI** (Remote Browser Isolation)



### SASE 솔루션

- Zscaler** — SSE 시장 1위
- Netskope** · Cloudflare One
- Palo Alto Prisma Access**
- Cisco Umbrella + Meraki**
- Cato Networks** — 통합형 강자



### TA 관점

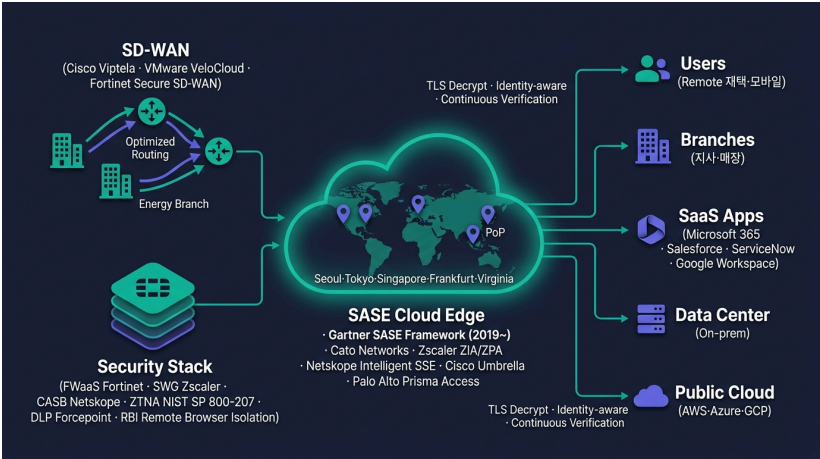
- 재택·다지점 시대의 **VPN 대체**
- 글로벌 사용자 latency 최소화
- 운영 부담 ↓ (클라우드 매니지드)
- 데이터 주권** 검토 필요 (Edge 위치)

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

52 / 78

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

page 147 / 160



SASE — Secure Access Service Edge

## SDP · ZTNA — VPN의 대체

### ● SDP (Software-Defined Perimeter)

- 일명 **Black Cloud** — 외부에서 자원이 "보이지 않음"
- 인증 전에는 **포트 응답 없음** (Single Packet Authorization)
- **Mutual TLS** 인증 후 1:1 마이크로 터널
- CSA (Cloud Security Alliance) 표준

### ■ ZTNA (Zero Trust Network Access)

- **"Never Trust, Always Verify"** 구현체
- 사용자·디바이스·컨텍스트 **매번 검증**
- 응용 단위 권한 (네트워크 단위 X)
- VPN의 사실상 후계자

### vs VPN vs ZTNA

| 항목    | VPN        | ZTNA  |
|-------|------------|-------|
| 접근 단위 | 네트워크       | 응용    |
| 신뢰 모델 | 1회 인증 후 신뢰 | 매번 검증 |
| 가시성   | 외부에 IP 노출  | 숨겨짐   |
| 횡 이동  | 가능         | 차단    |

### ☰ 솔루션

- **Zscaler Private Access**
- **Cloudflare Access · Netskope ZTNA**
- **Palo Alto Prisma Access**
- **Tailscale · Twingate**
- **Cisco Secure Access** (구 Duo Network Gateway)

# Zero-Trust — NIST SP 800-207 5대 축



### Zero-Trust 원칙

- **Never Trust, Always Verify**
- 경계 신뢰(perimeter trust) 폐기
- 모든 트래픽·요청을 **본질적으로 적대적으로** 가정
- **최소 권한·세밀한 통제·지속 검증**
- NIST SP 800-207 (2020 발간)



### 핵심 통제

- **Microsegmentation** — 응용·워크로드 단위 분리
- **Continuous Authorization** — 매 요청 검증
- **Risk-based Authentication** — 컨텍스트 기반
- **Encryption Everywhere**



### 5대 축 (NIST)

1. **Identity** — 사용자·서비스 정체성
2. **Device** — 단말 상태·신뢰도
3. **Network** — Micro-Segmentation
4. **Application / Workload** — 응용 단위 정책
5. **Data** — 분류·암호화·DLP



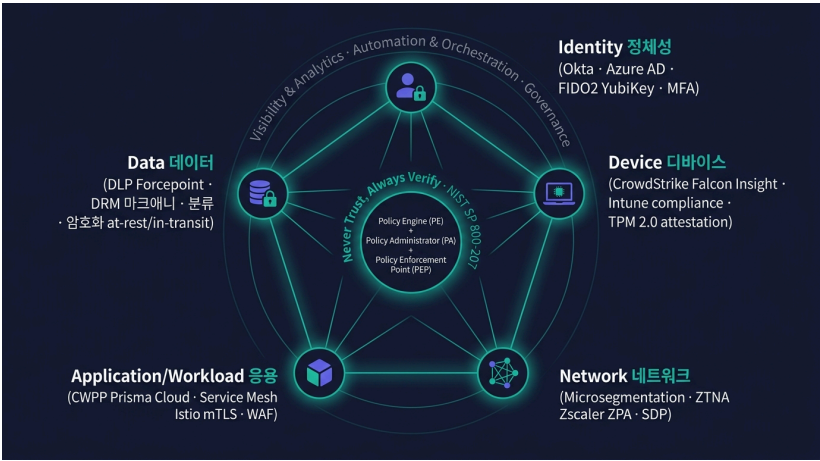
### 미국 정부 의무화

- **EO 14028 (2021)** — 연방 기관 ZT 의무
- **OMB M-22-09** — 2024년까지 ZT 적용



### 한국

- **국가정보원·KISA** ZT 가이드라인 작성 중
- 공공 부문 점진 도입



Zero-Trust — NIST SP 800-207 5대 축

# MITRE ATT&CK — 공격자의 TTPs 카탈로그

 **ATT&CK이란**

- MITRE가 운영하는 무료 프레임워크
- 실제 관측된 공격자 **TTP**(Tactic-Technique-Procedure) 정리
- 14개 Tactic (목적) → 200+ Technique (방법) → 수천 Procedure (구체적 사례)
- **공통 언어**로 위협을 표현

 **14개 Tactic**

- Reconnaissance-Resource Development
- Initial Access-Execution-Persistence
- Privilege Escalation-Defense Evasion
- Credential Access-Discovery-Lateral Movement
- Collection-C2-Exfiltration-Impact

 **Kill Chain vs ATT&CK**

- **Lockheed Kill Chain (2011)** — 7단계 선형
- **ATT&CK (2013~)** — 비선형·세밀·실증
- 현재 보안 업계 표준은 ATT&CK

 **활용처**

- EDR/XDR 룰 — Technique 단위 룰 작성
- SIEM 상관 분석 — 다단계 공격 탐지
- 레드팀·블루팀 공통 언어
- CTI — 위협 그룹 매핑 (APT28·Lazarus)
- Atomic Red Team — 검증 도구

# Threat Intelligence — 위협 정보의 활용

 **TI 4계층**

- **Strategic** — 경영진용 위협 동향
- **Operational** — 캠페인·공격자 그룹
- **Tactical** — TTP·도구
- **Technical** — IoC (IP·도메인·해시)

 **IoC vs IoA**

- **IoC (Indicator of Compromise)** — 침해 흔적 (사후)
- **IoA (Indicator of Attack)** — 공격 행위 패턴 (실시간)

 **TI 표준 포맷**

- **STIX 2.x** — 위협 정보 구조화 표준
- **TAXII** — STIX 교환 프로토콜
- **MISP** — 오픈소스 TI 플랫폼

 **TI 피드·플랫폼**

- VirusTotal · AlienVault OTX
- Recorded Future · Mandiant TI
- Microsoft Defender TI · CrowdStrike Intelligence
- Group-IB · 국가 사이버안보센터 (NCSC)
- KISA C-TAS — 한국 정부 운영

 **TA 결정**

- 무료 피드 (OTX·MISP) vs 유료 (Mandiant)
- SIEM·SOAR 자동 연동
- TI 평판 기준 자동 차단 임계
- CTI (Cyber Threat Intel) 분석가 보유 여부

AI·LLM 보안 — 2026년 신흥 도메인

 AI 시스템 위협

- **Prompt Injection** — 시스템 프롬프트 우회
- **Data Poisoning** — 학습 데이터 오염
- **Model Inversion** — 학습 데이터 추출
- **Model Extraction** — 모델 자체 탈취
- **Adversarial Examples** — 오분류 유도
- **Jailbreak** — 안전 가드 우회

 OWASP Top 10 for LLM

1. Prompt Injection
2. Insecure Output Handling
3. Training Data Poisoning
4. Model DoS
5. Supply Chain (모델-플러그인)
6. Sensitive Information Disclosure
7. Insecure Plugin Design
8. Excessive Agency
9. Overreliance
10. Model Theft

 대응 방향

- **Input/Output Guardrails** — NeMo Guardrails·LangChain Filters
- **PII 마스킹** — 입출력 식별자 가림
- **출력 제한 토큰·도메인 통제**
- **모델 모니터링** — drift·hallucination
- **RAG 보안** — 벡터 DB 권한·민감 문서 격리
- **에이전트 도구 권한 최소화**

 신흥 솔루션

- **HiddenLayer** · **Robust Intelligence** · **Lakera**
- **Cisco AI Defense** · **Palo Alto AI Security**
- **국내** — 스캐터랩·셀바스·시큐레터 AI 보안

 TA 시사점

- LLM 도입 시 **모델 + 데이터 + 도구** 3축 보안
- RAG에는 **벡터 DB 권한 모델** 필수

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

59 / 78

#302

IT 인프라 아키텍처 설계 · Session 7 · 보안 6대 도메인

Part D 정리 — 최신 보안 9가지

**운영 자동화**

- **CDR** — 콘텐츠 무해화
- **SOAR** — Playbook 자동화
- **TI** — STIX/TAXII

**네트워크 신모델**

- **SASE** — SD-WAN + Security
- **SDP** — Black Cloud
- **ZTNA** — VPN 대체

**거버넌스 모델**

- **Zero-Trust** — NIST 5대 축
- **MITRE ATT&CK** — TTPs 공통 언어
- 미국 EO 14028 의무화

**AI 시대**

- **LLM 보안** — OWASP Top 10 for LLM
- 모델·데이터·도구 3축
- Guardrails-RAG 권한

**TA 결정 6가지**

1. SOAR Playbook 자동화 범위
2. SASE 도입 시 VPN 교체
3. ZTNA 응용 단위 정책
4. Zero-Trust 로드맵
5. TI 무료 vs 유료
6. LLM 도입 시 보안 가이드라인

**핵심 메시지**

- 경계 신뢰 모델 종말
- 정체성 + 데이터 중심
- 자동화 + AI 결합

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

60 / 78

© 2026 젠아이랩스 (GenAI Labs) · 강사 박수현

page 151 / 160

# PART E

## 보안 거버넌스·인증 — 정책·법규·인증 체계

정책 4계층 · SOP 4종 · 국내·국제 인증 · 한국 법령

IT 인프라 아키텍처 설계 · Session 7 · 보안 6대 도메인

## 보안 정책 4계층 — *Policy* → *Guideline*



### 4계층 구조

1. **Policy (정책)** — 최상위 방침 - "회사는 ISMS-P 준수한다" - 이사회 승인·연 1회 갱신
2. **Standard (표준)** - "비밀번호는 12자·복잡도·90일" - CISO 승인·반기 갱신
3. **Procedure (절차)** - "신규 사용자 등록 단계" - 운영팀 작성·분기 갱신
4. **Guideline (지침)** — 권고·참조 - "안전한 비밀번호 작성 팁"



### 운영 원칙

- 상위가 하위를 **강제**
- 충돌 시 **상위 우선**
- 변경 이력 관리 의무
- **모든 단계가 문서화**돼야 인증·감사 통과
- **연 1회 검토**가 ISMS-P 통제 항목



### 누가 작성하나

- CISO·보안팀이 Policy·Standard
- 운영팀이 Procedure
- TA는 **Procedure 작성의 핵심 주체**
- 기술 표준의 합리적 근거 제공

## SOP 4종 — 운영 표준 절차

### ① 백업·복구 SOP

- 백업 정책·매체·보관
- 복구 시험 주기 (분기 1회 권고)
- 랜섬웨어 대응 시 Immutable 검증
- RPO·RTO 명시

### ② 변경 관리 SOP

- CR (Change Request) 양식
- CAB (Change Advisory Board) 회의
- 영향도 분석·롤백 계획
- 표준 변경·정기 변경·긴급 변경
- 변경 후 검증·종료 보고

### ③ 장애 대응 SOP

- 등급 분류 (Critical·Major·Minor)
- 에스컬레이션 (On-Call 명단)
- Detection → Containment → Investigation → Recovery → Postmortem
- 사후 Blameless Postmortem

### ④ 침해사고 대응 SOP

- 탐지 → 격리 → 조사 → 복구 → 보고
- KISA 신고 (72시간 내)
- 증거 보존·포렌식 체인
- 법무·홍보·고객 통지

이 4종 SOP는 ISMS-P·SOC 2·ISO 27001 핵심 통제 항목.

## ISMS-P — 정보보호 및 개인정보보호 관리체계

### 개요

- 운영: KISA (한국인터넷진흥원)
- 근거 법령: 정보통신망법·개인정보보호법
- 명칭: ISMS-P = ISMS + 개인정보(P)
- 기존: ISMS·PIMS 통합 (2018)
- 유효기간: 3년 + 매년 사후심사

### 통제 항목

- 관리체계 (16개) — 정책·조직·자산·위험
- 보호대책 (64개) — 인적·물리·기술·운영
- 개인정보 처리 (21개) — 수집·이용·제공·파기

### 대상

- 의무: 매출 1,500억+ ISP·일평균 100만+ 사용자
- 권장: 모든 대규모 기업·공공
- 공공기관: 점차 의무화 확대

### 비용·기간

- 인증 비용: 5천만 ~ 2억원 (규모 따라)
- 준비 기간: 12~18개월
- 컨설팅 비용 별도: 3천만 ~ 5천만원

### 효과

- 정보보호 수준 객관 평가
- 대고객·B2B 신뢰 확보
- 사고 시 책임 경감 (선관주의)



KCMVP · CC인증 · 보안기능 확인서

**KCMVP (암호모듈 검증)**

- **국정원 운영**
- 암호 알고리즘·모듈의 안전성 검증
- 등급: 검증필 암호 모듈 = KCMVP 인증
- 공공·금융 의무

**CC인증 (Common Criteria)**

- **국정원 IT보안인증사무국**
- 보안 기능 평가·국제 상호인증 (CCRA)
- EAL1~EAL7 (한국은 EAL1~EAL4+)
- 대상 — 운영체제·DB·방화벽·VPN 등 60+ 분야

**보안기능 확인서 (구 보안적합성 검증)**

- 공공기관 보안 솔루션 도입 시 의무
- **6종 카테고리:**
  - **FW** (방화벽)
  - **IPS** (침입방지)
  - **UTM** (통합위협관리)
  - **SAC** (시스템 접근 통제)
  - **NAC** (네트워크 접근 통제)
  - **DDoS** (DDoS 차단)
- 기타 카테고리 — DLP·PMS·NAC·EDR도 점차 추가

**TA 시사점**

- 공공 RFP = KCMVP + 보안기능 확인서가 사실상 필수
- 글로벌 제품 도입 시 가장 큰 장벽
- 국내 솔루션이 우선 검토 대상

국제 보안 인증 — 7대 표준

| 인증        | 영역               | 운영          | 주요 적용     |
|-----------|------------------|-------------|-----------|
| ISO 27001 | 정보보호 관리체계 (ISMS) | ISO/IEC     | 전 산업 표준   |
| ISO 27017 | 클라우드 보안 통제       | ISO/IEC     | CSP·SaaS  |
| ISO 27018 | 클라우드 개인정보        | ISO/IEC     | 글로벌 CSP   |
| ISO 22301 | 사업 연속성 (BCMS)    | ISO/IEC     | DR·BCP 대응 |
| NIST CSF  | 사이버보안 프레임워크      | NIST (미국)   | 정부·기간시설   |
| PCI-DSS   | 결제카드 데이터 보호      | PCI Council | 결제·카드사    |
| HIPAA     | 의료정보 보호          | 미국 HHS      | 의료 (미국법)  |
| SOC 2     | SaaS·서비스 통제 보고   | AICPA       | SaaS·아웃소싱 |
| GDPR      | EU 개인정보 보호 규정    | EU          | EU 시민 대상  |

한국 글로벌 진출: SaaS·B2B는 SOC 2 + ISO 27001, 결제는 PCI-DSS, EU 대상은 GDPR 추가. ISMS-P만으로는 글로벌 부족.

## 한국 보안·개인정보 법령 — 5대 축

### 📖 5대 법령

1. **개인정보보호법 (PIPA)** - 모든 개인정보 처리자 적용 - 2024 개정 — 과징금 매출 3%·국외이전
2. **정보통신망법 (정보망법)** - ICT 사업자 정보보호 의무 - ISMS-P 근거
3. **신용정보법** - 금융권 신용정보 보호
4. **정보통신기반보호법** - 주요정보통신기반시설 (CII) 보호
5. **전자정부법·전자정부 SW 개발보안 가이드** - 공공 시스템 개발 단계 보안

### 🏛️ 주관 기관

- **개인정보보호위원회 (PIPC)** — 개인정보 감독
- **방송통신위원회 (KCC)** — 정보망법 감독
- **금융위원회·금융감독원** — 금융 보안
- **국가정보원** — 국가·공공 보안
- **KISA** — 인증·정책 지원
- **과기부** — ICT 정책

### 📌 TA 관점

- 법령 → 정책 → SOP의 흐름
- RFP 보안 요구는 **법령 인용 매칭**
- 사고 시 **선관주의** 입증의 출발점

## 인증 절차·비용·기간 — 현실 가이드

| 인증              | 준비 기간   | 컨설팅비    | 인증 심사비  | 갱신 주기      |
|-----------------|---------|---------|---------|------------|
| ISMS-P          | 12~18개월 | 3~5천만원  | 5천만~2억원 | 3년 (사후 매년) |
| ISO 27001       | 6~12개월  | 2~4천만원  | 2~5천만원  | 3년 (사후 매년) |
| CC인증 EAL2~4     | 12~24개월 | 1~3억원   | 3~5천만원  | 5년         |
| KCMVP           | 6~12개월  | 5천만원~   | 별도      | 5년         |
| SOC 2 Type 2    | 12~18개월 | 1~3억원   | 5천만~1억원 | 매년         |
| PCI-DSS Level 1 | 6~12개월  | 5천만~1억원 | 5천만원    | 매년         |

### 🎯 인증 실패 흔한 사유

- 정책·SOP는 있는데 **실행 증거 부재**
- 위험평가 갱신 **누락**
- 백업 **복구 시험 미실시**
- 권한 검토·로그 검토 **누락**

### 💡 TA 인증 준비 팁

- **CMDB·자산 인벤토리** 먼저
- 변경관리 **티켓 흔적**
- 로그 보존·검색 **가능성**
- 분기 **모의 점검** 정착

Part E 정리 — 거버넌스·인증 8가지

정책 체계

- Policy → Standard → Procedure → Guideline
- SOP 4종 — 백업·변경·장애·침해

국내 인증

- ISMS-P — KISA
- KCMVP — 국정원
- CC인증·보안기능 확인서 6종

국제 인증

- ISO 27001/17/18·22301
- NIST CSF
- PCI-DSS·HIPAA·SOC 2·GDPR

한국 법령

- 개인정보보호법·정보통신망법
- 신용정보법·정보통신기반보호법
- 전자정부 SW 개발보안 가이드

TA 결정 7가지

1. ISMS-P 대상 여부
2. CC·KCMVP 필요 솔루션
3. 글로벌 진출 시 SOC 2 / ISO 27001
4. PCI 도입 결재 영역
5. 정책 4계층 작성·갱신
6. SOP 4종 정착
7. 인증 비용·기간 예산화

핵심 메시지

- 기술 + 운영 + 문서가 인증
- TA는 Procedure 작성 주체

PART G

보안 운영 + 실전 — SOC · 점검 · TA의 결정

SOC Tier 1·2·3 · VA · PT · BAS · TA의 12대 결정

# SOC — Security Operations Center 운영

 Tier 1 — Monitoring

- 24/7 모니터링-1차 트리이지
- 알람 분류-기본 대응
- Playbook 실행
- 에스컬레이션 판단
- 인력: 신입~주니어

 Tier 2 — Investigation

- 심층 분석-포렌식 초기
- IoC 확인-범위 산정
- Containment 수행
- Tier 1 멘토링
- 인력: 중급

 Tier 3 — Threat Hunting

- 능동 위협 헌팅
- 신규 룰 작성
- 포렌식-RCA
- TI 연구-APT 추적
- 인력: 시니어

 SOC Manager-CISO

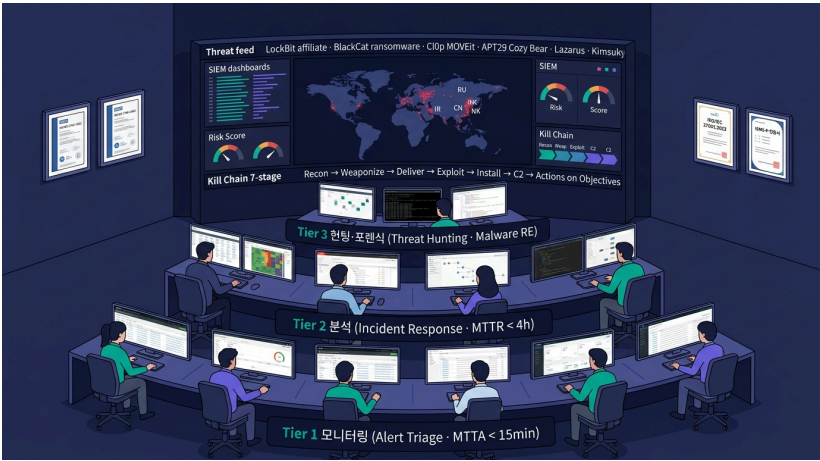
- KPI-보고-예산
- 사고 외부 공조 (KISA-국정원)

 SOC 운영 모델

- 자체 SOC — 24/7 인력 풀
- MSSP 위탁 — 운영 위탁
- MDR — EDR/XDR 통합 위탁
- 하이브리드 — 평시 자체-야간 MSSP

 TA 결정

- 인력 규모-시간대 분담
- 운영 시간 (8x5 vs 24x7)
- 위탁 시 SLA-KPI 정의
- 한국 — KT-LG U+·이글루·안랩 MSSP



SOC — Security Operations Center 운영

침해사고 대응 — KISA·NIST 표준 절차

 ① Preparation (사전 준비)

SOP·연락망·도구 사전 점검 / 정기 모의 훈련

 ② Detection (탐지)

SIEM·EDR·신고 채널 통합 / 초기 분류

 ③ Containment (격리)

영향 범위 격리 / 단기 vs 장기 격리 결정

 ④ Eradication (근절)

악성코드 제거·취약점 패치 / 백도어 제거

 ⑤ Recovery (복구)

정상 운영 복귀 / 점진적·검증 후 단계 확대

 ⑥ Lessons Learned (사후 분석)

Blameless Postmortem / RCA · 재발 방지 · 정책 갱신

KISA 신고 의무: 정보통신서비스 제공자 — 침해사고 인지 후 72시간 이내 KISA 신고, 개인정보 유출 — 5일 이내 정보주체·PIPC 통지.

TA의 보안 설계 — 12대 결정 카탈로그

네트워크 (4)

1. NGFW 다층 vs UTM 단일 — 규모·인력

2. WAF 클라우드 vs 온프레 — 외부 노출·법규

3. IPS Inline vs IDS Tap — 오탐 감내도

4. VPN 종류 — IPSec/SSL/ZTNA 조합

엔드포인트 (3)

5. EDR 솔루션 — KCMVP 여부·MDR 묶음

6. NAC 인증 방식 — 802.1X / MAC

7. SIEM EPS·보존 — Splunk vs Elastic vs 국내

데이터 (3)

8. DRM 적용 범위 — 전사 vs 부서·기밀

9. DB 보안 3중 풀세트 vs 부분

10. KMS/HSM — 클라우드 vs HSM 박스 (KCMVP 요구 시)

거버넌스 (1)

11. 인증 로드맵 — ISMS-P → ISO 27001 → SOC 2 시퀀스

클라우드·운영 (1)

12. SASE·ZTNA 도입 시점 — VPN 교체·SaaS 통제·재택 인구

 결정의 출발점 5가지

- 법규·인증 요구사항 — RFP 명문화
- 자산 가치·민감도 — DPIA 수행
- 인력 역량 — 자체 vs 위탁
- 예산 — CapEx vs OpEx
- 운영 부담 — 솔루션 수·통합도

## 시나리오 ① — 중견 제조 기업, 신규 보안 체계 구축

### 상황

- 직원 800명·서버 80대·사용자 PC 700대
- 매출 3,000억·해외 매출 30%
- 사내 ERP·MES·CRM 운영
- **개인정보 보유** (직원·고객사)
- 침해사고 1회 전력 (랜섬웨어)
- 보안 전담 2명 (CISO 겸직)

### 요구사항

- ISMS-P 인증
- 24/7 보안 모니터링
- 재택근무 보안 강화

### TA 설계안 (8축)

1. **경계** — NGFW 2대 HA + 클라우드 WAF + Anti-DDoS 통신사
2. **내부** — IPS · NAC (MAC 인증)
3. **엔드포인트** — EDR + MDR 위탁 (24/7)
4. **데이터** — DLP Endpoint + DB 보안 3종 (D'Amo)
5. **인증** — MFA + FIDO2 단계 도입
6. **백업** — Immutable + Air-Gap (랜섬웨어 대응)
7. **거버넌스** — ISMS-P 12개월 컨설팅 + SOP 4종
8. **운영** — MDR + 분기 VA · 연 1회 PT · BAS 도입

**예상 투자:** 초기 12억 + 연 운영 5억

## 시나리오 ② — 공공기관 클라우드 전환

### 상황

- 공공기관·대국민 서비스
- 기존 온프레미스 → **CSAP 클라우드** 이전
- 개인정보 다수 (수십만 건)
- 망분리 의무 (전자정부)
- 정기 보안 점검 의무

### 요구사항

- **CSAP 인증 사업자** 사용
- **국정원 보안기능 확인서** 솔루션
- **KCMVP 암호 모듈**
- ISMS-P + CC인증

### TA 설계안

1. **CSP 선택** — NCP·KT Cloud·NHN Cloud (CSAP 인증)
2. **경계** — 국정원 보안기능 확인서 NGFW·IPS·DDoS
3. **망분리** — VPC + 단방향 게이트웨이 (CDR)
4. **데이터** — TDE + KCMVP HSM + DLP
5. **계정** — SSO + MFA + PAM
6. **클라우드** — CSPM + CWPP (멀티 계정 통합)
7. **운영** — 자체 SOC + MSSP 야간 위탁
8. **인증** — ISMS-P + CC인증 + KCMVP

## 시나리오 ③ — AI 스타트업, 글로벌 진출

### 상황

- LLM 기반 AI 서비스 운영
- 직원 50명·AWS 멀티 리전
- 한국 + 미국 + EU 사용자
- 글로벌 진출 + 엔터프라이즈 B2B 영업
- 보안 전담 1명

### 요구사항

- **SOC 2 Type 2** (B2B 영업 필수)
- **ISO 27001**
- **GDPR** 대응
- AI 모델 보안

### TA 설계안

1. **인프라** — AWS Well-Architected + GuardDuty + Security Hub
2. **CSPM·CNAPP** — Wiz 또는 Prisma Cloud
3. **IAM** — Okta SSO + MFA + JIT
4. **데이터** — KMS + S3 암호화 + DynamoDB TDE + 백업 Immutable
5. **AI** — Guardrails + RAG 권한 모델 + PII 마스킹
6. **WAF·DDoS** — Cloudflare
7. **로그** — Datadog 또는 Elastic SIEM + AWS CloudTrail
8. **인증** — ISO 27001 (1년) → SOC 2 Type 2 (1년) → GDPR DPA

**TA 인사이트:** B2B는 SOC 2 없으면 영업 자체 불가능한 경우 다수.

## Session 7 학습 정리 — 5대 도메인 + 운영

### 5대 도메인 한 줄 요약

- **A. 네트워크** — NGFW 4세대 + WAF·IPS·DDoS·VPN
- **B. 엔드포인트** — EDR/XDR + MDR + NAC·SIEM
- **C. 데이터** — DRM·DLP·DB 3중·PKI·FIDO·HSM
- **D. 최신** — Zero-Trust·SASE·ZTNA·ATT&CK·LLM
- **E. 거버넌스** — ISMS·P·KCMVP·CC + ISO·SOC 2

### 본 회차에서 확보한 시야

- 보안 5대 도메인 + 운영을 한 번에 조망
- 솔루션 카테고리의 배치·역할
- 한국 인증 체계와 RFP 요구 매핑
- TA의 12대 보안 의사결정 카탈로그
- 시나리오 3종을 통한 결정 패턴 체험

### 본 회차의 카탈로그

- 5 PART의 솔루션 카탈로그
- 솔루션 × 한국·글로벌 매핑
- 3종 시나리오의 8축 설계안 템플릿