스위치 인프라 보안 차별화 기능 및 구현

조태진 (taecho@cisco.com)

Cisco Systems Korea

목 차

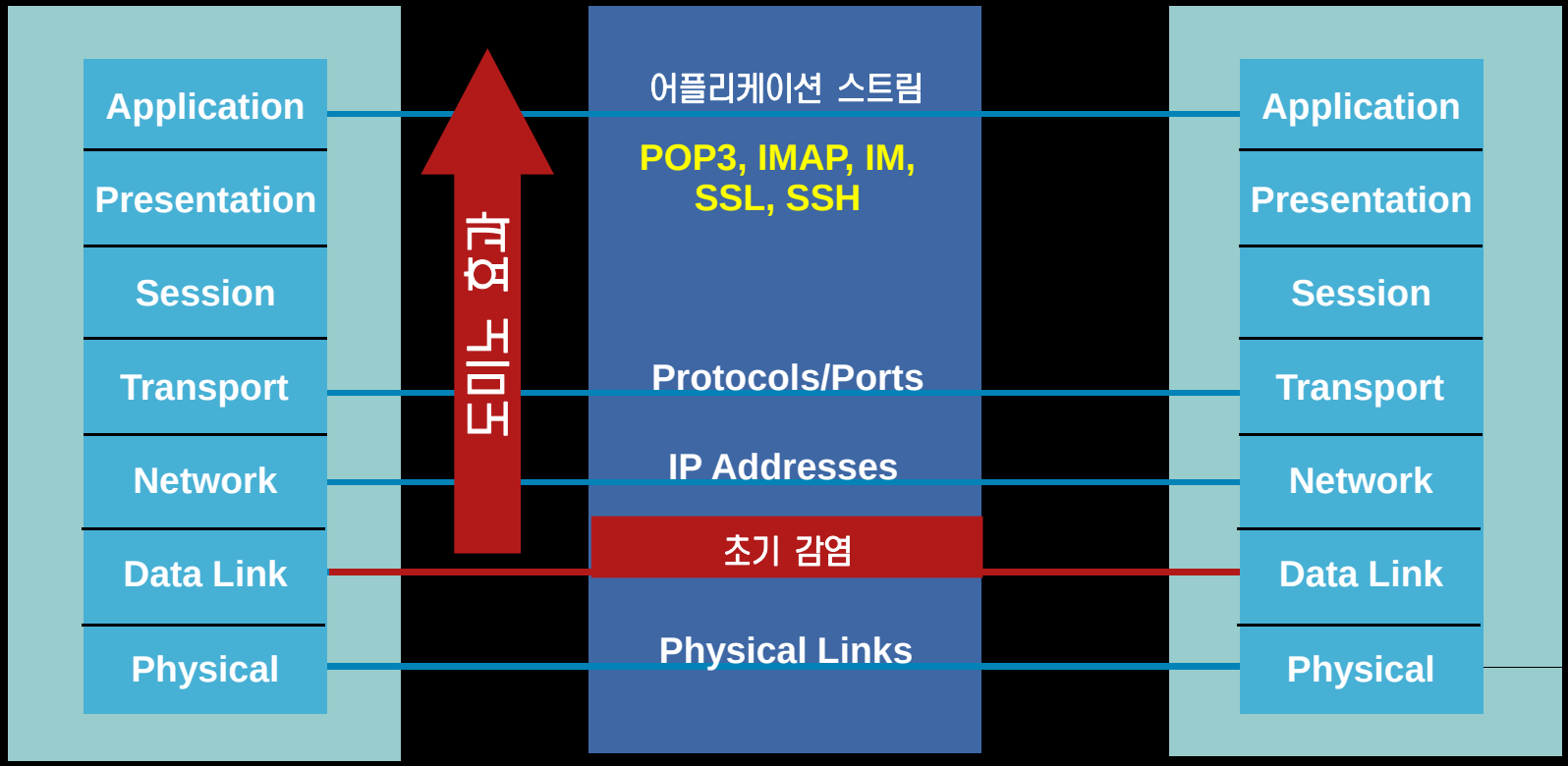
- 스위치 인프라 보안의 필요성
- 시스코 통합 스위치 보안 기능 (Cisco Integrated Security Features)
  - Port Security
  - DHCP Snooping
  - Dynamic ARP Inspection
  - IP Source Guard
  - Traffic Storm Control
- 스위치 장비 리소스 보호 기법 - CoPP
- Cisco TrustSec (CTS) 아키텍처
- 결론; Why Cisco

스위치 인프라 보안의 필요성

하위 계층의 보안 취약점 = 상위 계층의 보안 취약점

- 한 계층에서의 보안 취약점은, 다른 계층에서 인지하지 못하는 사이 연쇄적으로 해당 위험 요소를 전파 시킬 수 있는 위험 요소를 내포

- 네트워크를 보안 관점으로 바라봤을 때, '2계층'은 매우 취약한 구조에 노출



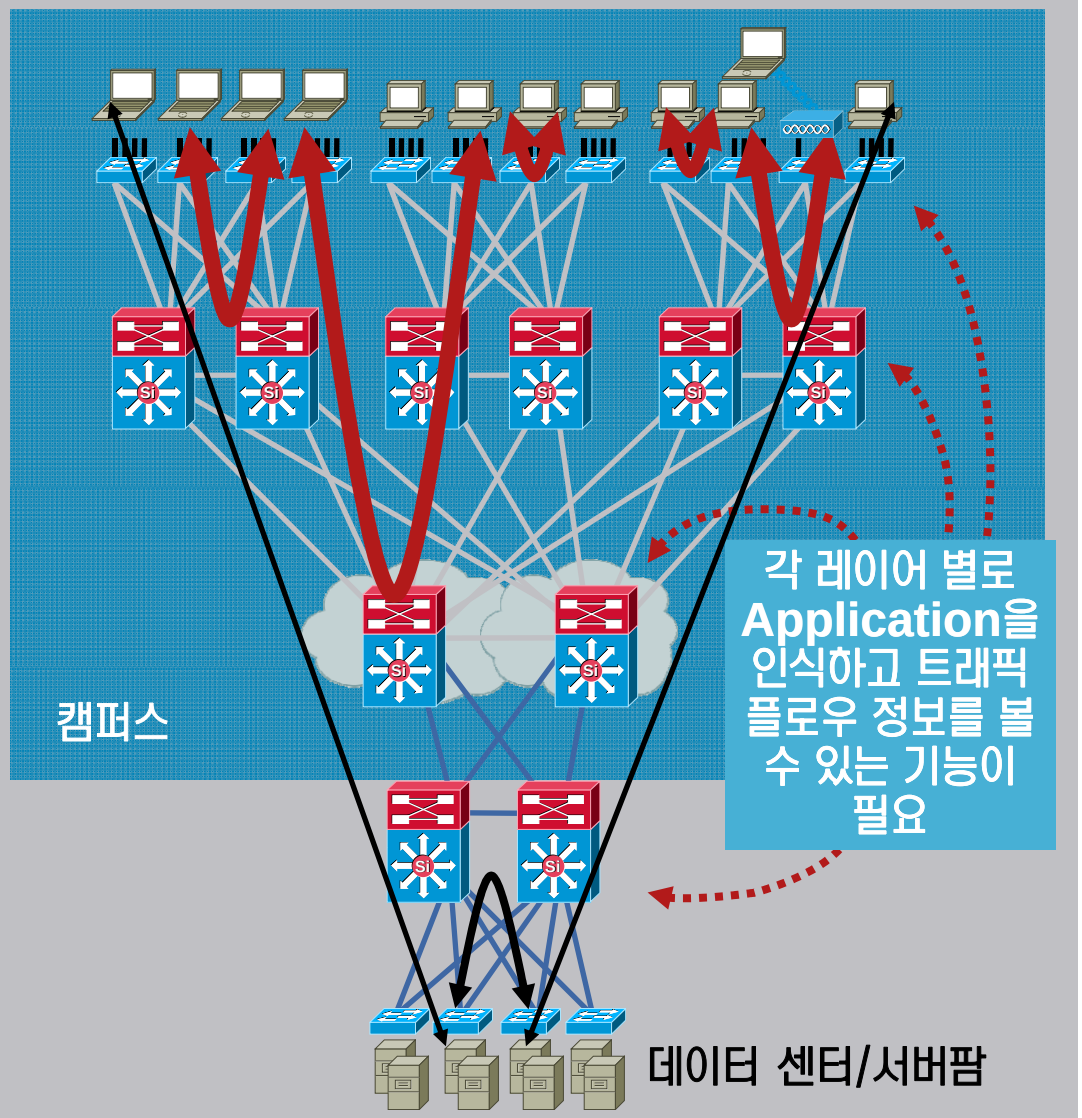
2계층이 보안에 취약한 이유는?

질문	네트워크팀	보안팀
• VLAN에 대한 보안 정책은?	• Layer 2 보안이 이슈가 있나요?	• Layer 3 이상의 보안 정책만 있음
• 얼마나 자주 VLAN을 사용하는지?	• 항상 사용합니다	• 글쎄요???
• 동일 스위치 내에서 VLAN을 사용시 VLAN별로 서로 다른 보안 레벨을 적용하나요?	• 동일 스위치 내에서 VLAN간 라우팅을 수행하는데 전혀 문제가 없습니다	• 그건 스위치의 역할이고 네트워크팀의 롤인데… 저희가 신경 써야 하나요?
• VLAN별로 할당되어지는 주소는 어떻게 관리하죠?	• 보안팀의 세그먼트 할당 요청에 따라 그때 그때 주소를 할당 해 줍니다	• 네트워크 팀에 요청하면 포트와 주소를 할당 해 줍니다

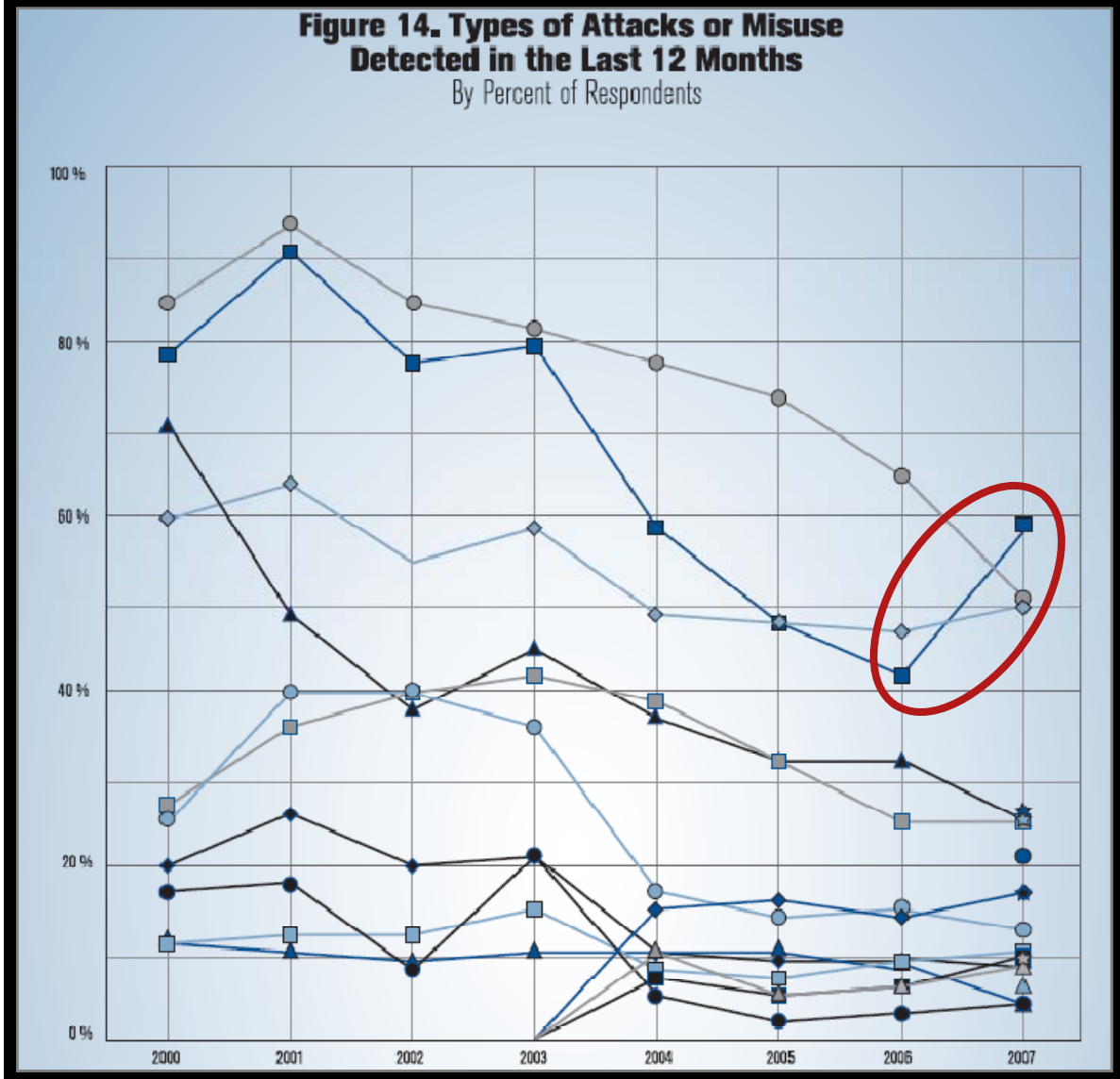
캠퍼스 네트워크 동향

- 기업 어플리케이션 진화
- UC 통합
- 협업 모델 (Web 2.0)
- 비디오 트래픽 증가
- Peer-to-Peer 통신 증가
- 모빌리티 환경

"네트워크 보안의 필요성 증대"



CSI Computer Crime & Security 설문 - 2007



TYPE OF ATTACK	2007
Insider abuse of Net access	59%
Virus	52%
Laptop / mobile device theft	50%
Phishing where your organization was fraudulently represented as sender**	26%
Instant messaging misuse**	25%
Denial of service	25%

*** CSI Survey—2007**
http://www.gocsi.com

시스코 통합 스위치 보안 기능
(Cisco Integrated Security Features)

- Port Security
- DHCP Snooping
- Dynamic ARP Inspection
- IP Source Guard
- Traffic Storm Control

스위치 보안 피해 사례

레이어 2 MAC 공격 사례

- Macof/dsniff 공격툴

- 단말 NIC 오 / 불안정한 광신호

DHCP 피해 사례

- Gobbler 공격툴

어가 DHCP 서버

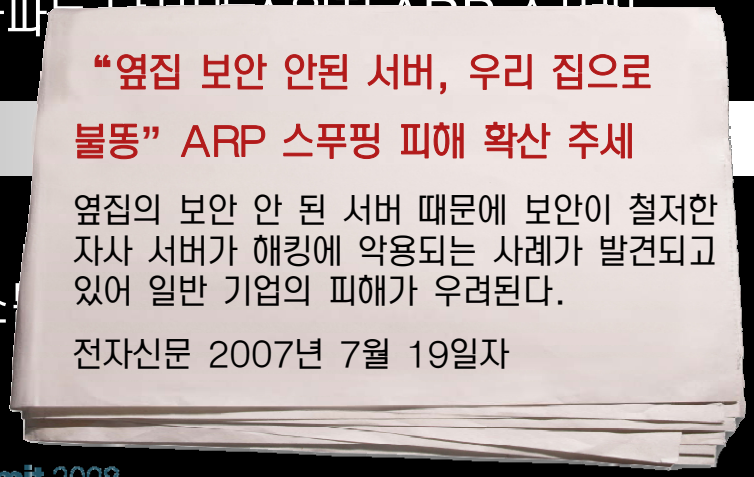
ARP 스푸핑 피해 사례

- IDC 스위치 / 기업 앱 / 초고속 아파

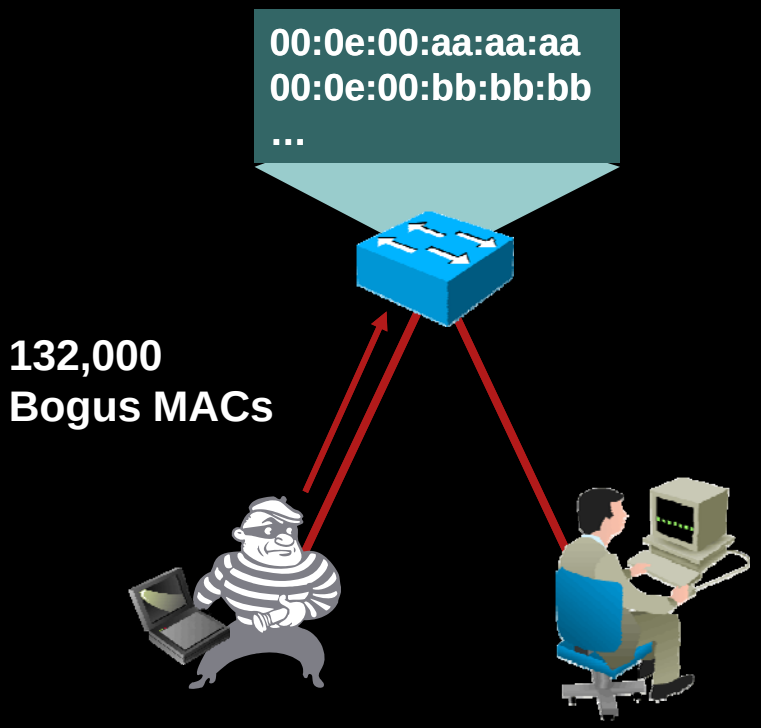
트래픽 flooding 사례

- STP 루프
- 서버 오동작으로 인한 다량의 브로드캐스트 스

"의도된 vs. 의도되지 않은"



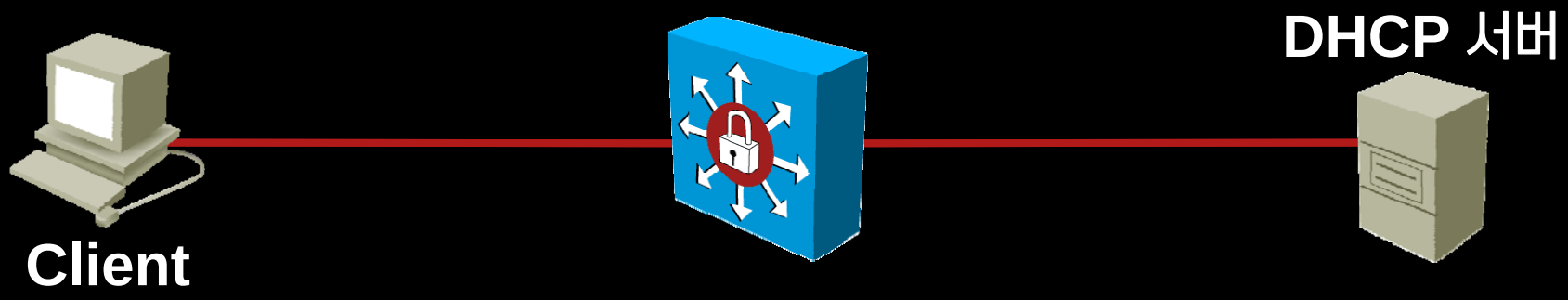
MAC 테이블 고갈 공격 = Port Security



솔루션:

- 허용된 MAC 주소보다 많은 수의 MAC 주소가 들어오면, 해당 포트를 셧다운 시키고 SNMP 트랩을 NMS로 보냄

DHCP의 이해



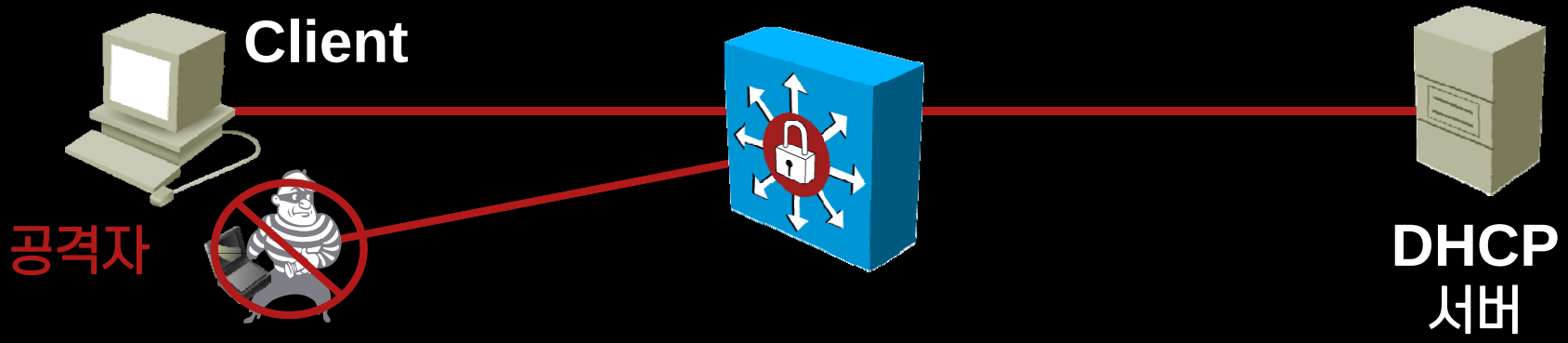
DHCP Discover (Broadcast)

DHCP Offer (Unicast)

DHCP Request (Broadcast)

DHCP Ack (Unicast)

DHCP 고갈 공격 방지 = Port Security



- 한 번의 새로운 DHCP lease 요청 시마다 한 개의 MAC 주소를 사용함
- 포트당 MAC 주소 허용치를 제한
- 오른쪽 예제의 경우, 공격자는 1개의 주소만 DHCP에서 할당 받을 수 있음

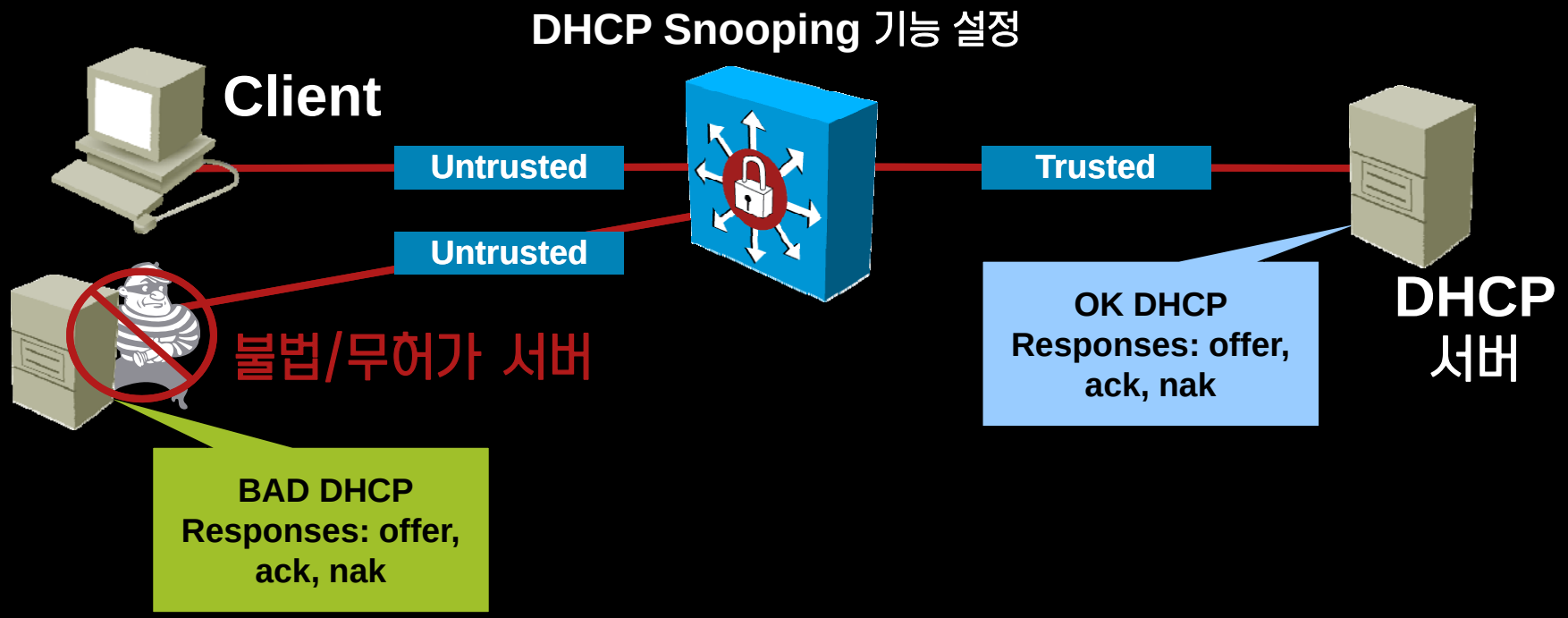
CatOS

```
set port security 5/1 enable
set port security 5/1 port max 1
set port security 5/1 violation restrict
set port security 5/1 age 2
set port security 5/1 timer-type inactivity
```

IOS

```
switchport port-security
switchport port-security maximum 1
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

불법/무허가 DHCP 서버 공격 = DHCP Snooping

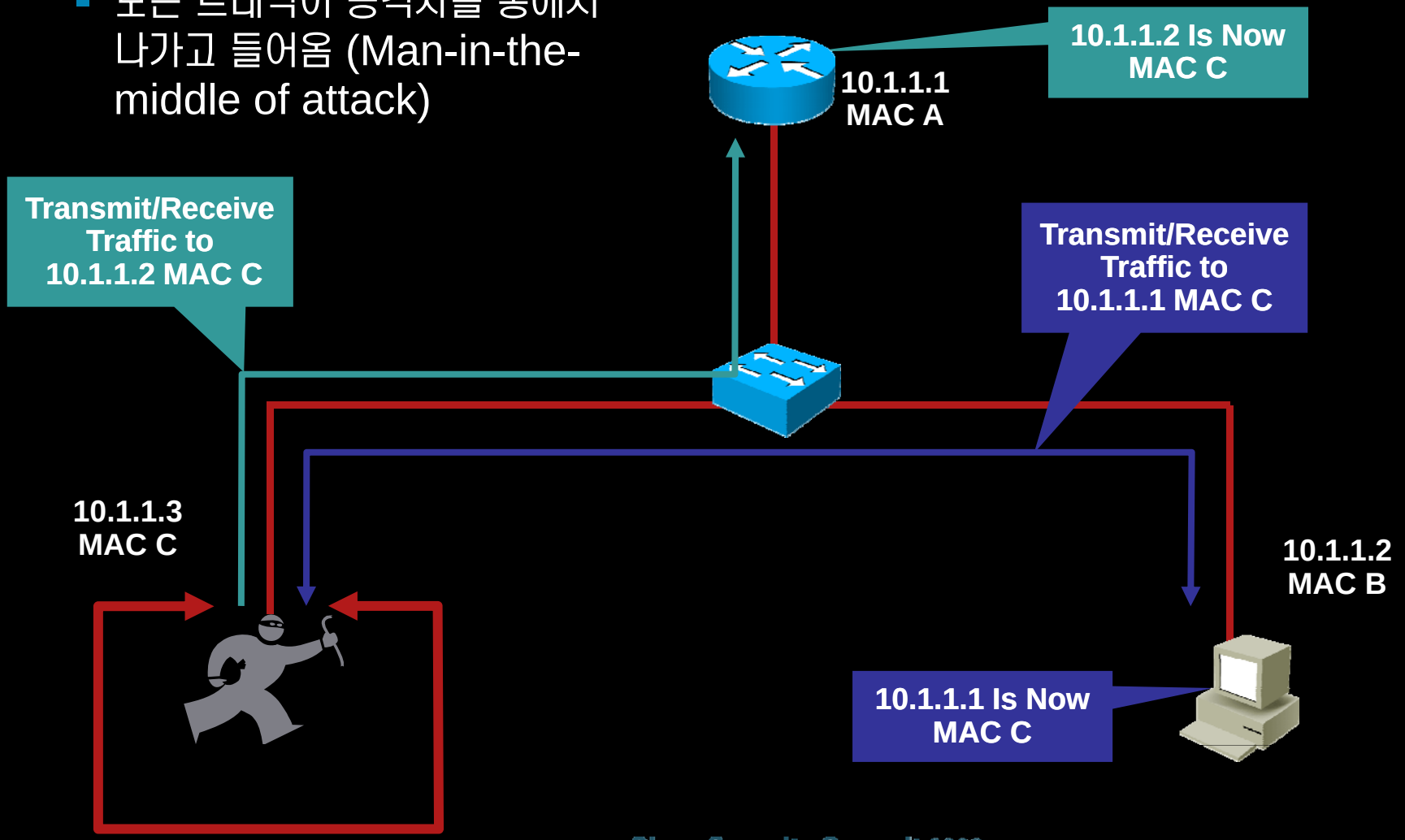


DHCP Snooping Binding 테이블 생성

```
show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:03:47:B5:9F:AD   10.120.4.10      193185      dhcp-snooping  4     FastEthernet3/18
```

ARP 테이블 변조 공격

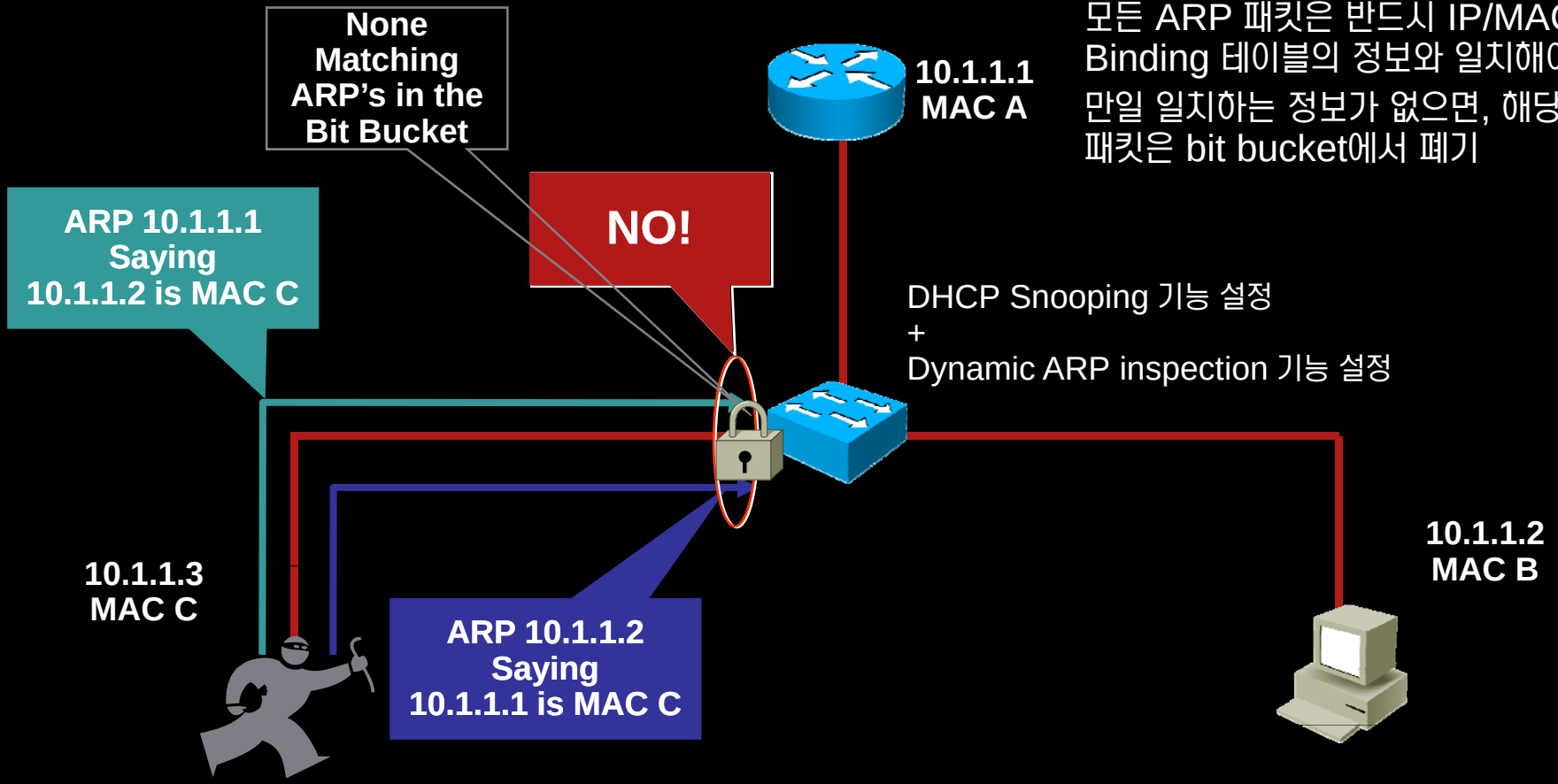
- 모든 트래픽이 공격자를 통해서 나가고 들어옴 (Man-in-the-middle of attack)



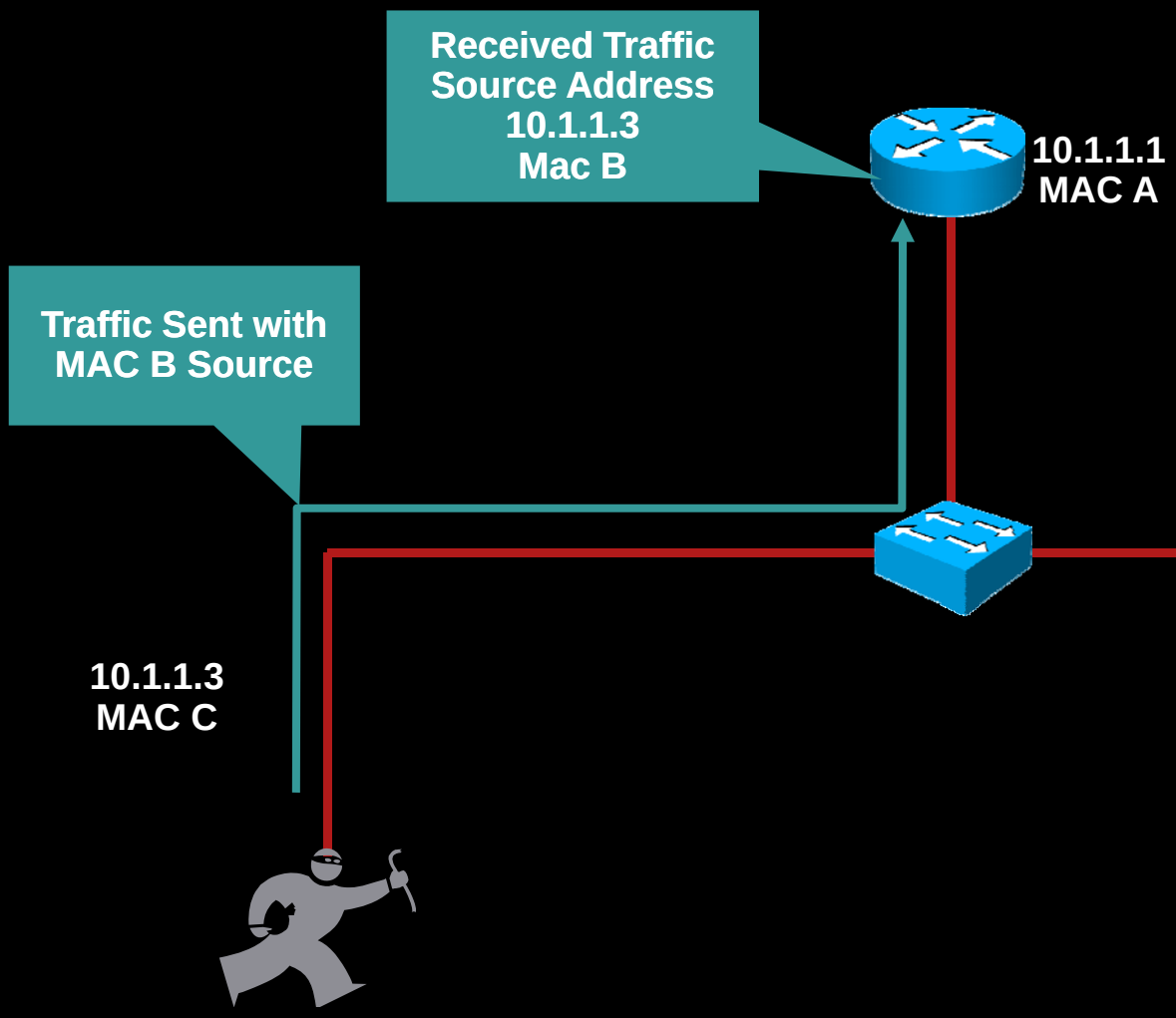
ARP 공격 방지: Dynamic ARP Inspection

- DHCP Snooping Binding 테이블 정보 참조
- Dynamic ARP Inspection

  모든 ARP 패킷은 반드시 IP/MAC Binding 테이블의 정보와 일치해야 만일 일치하는 정보가 없으면, 해당 패킷은 bit bucket에서 폐기

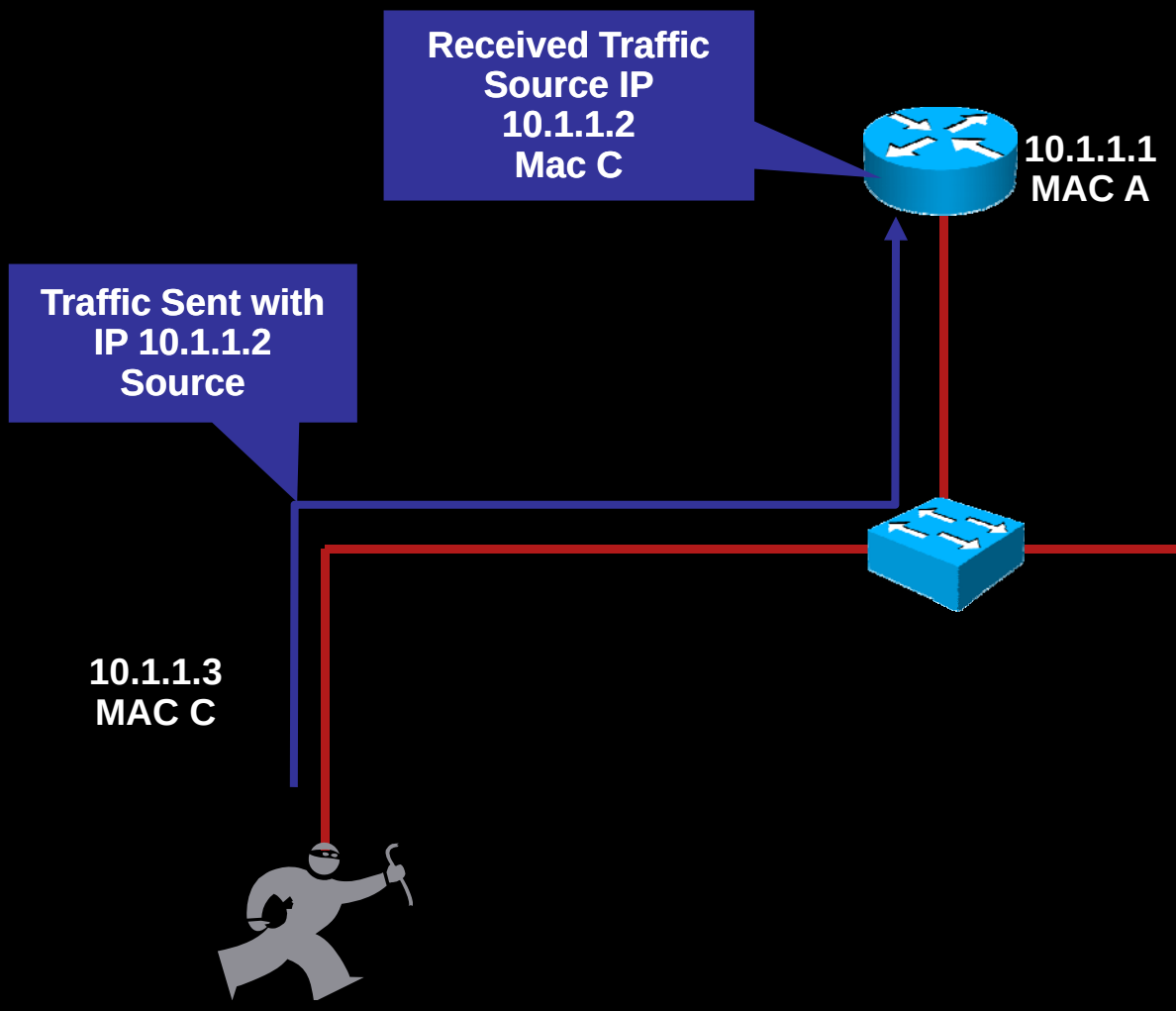


MAC 주소 변조 공격



- 공격자는 완전히 다른 소스 MAC 주소로 변조하여 패킷을 보냄
- MAC 주소 기반의 통신을 하는 Layer 2 장비에서는, 공격자를 10.1.1.2 장비처럼 인식

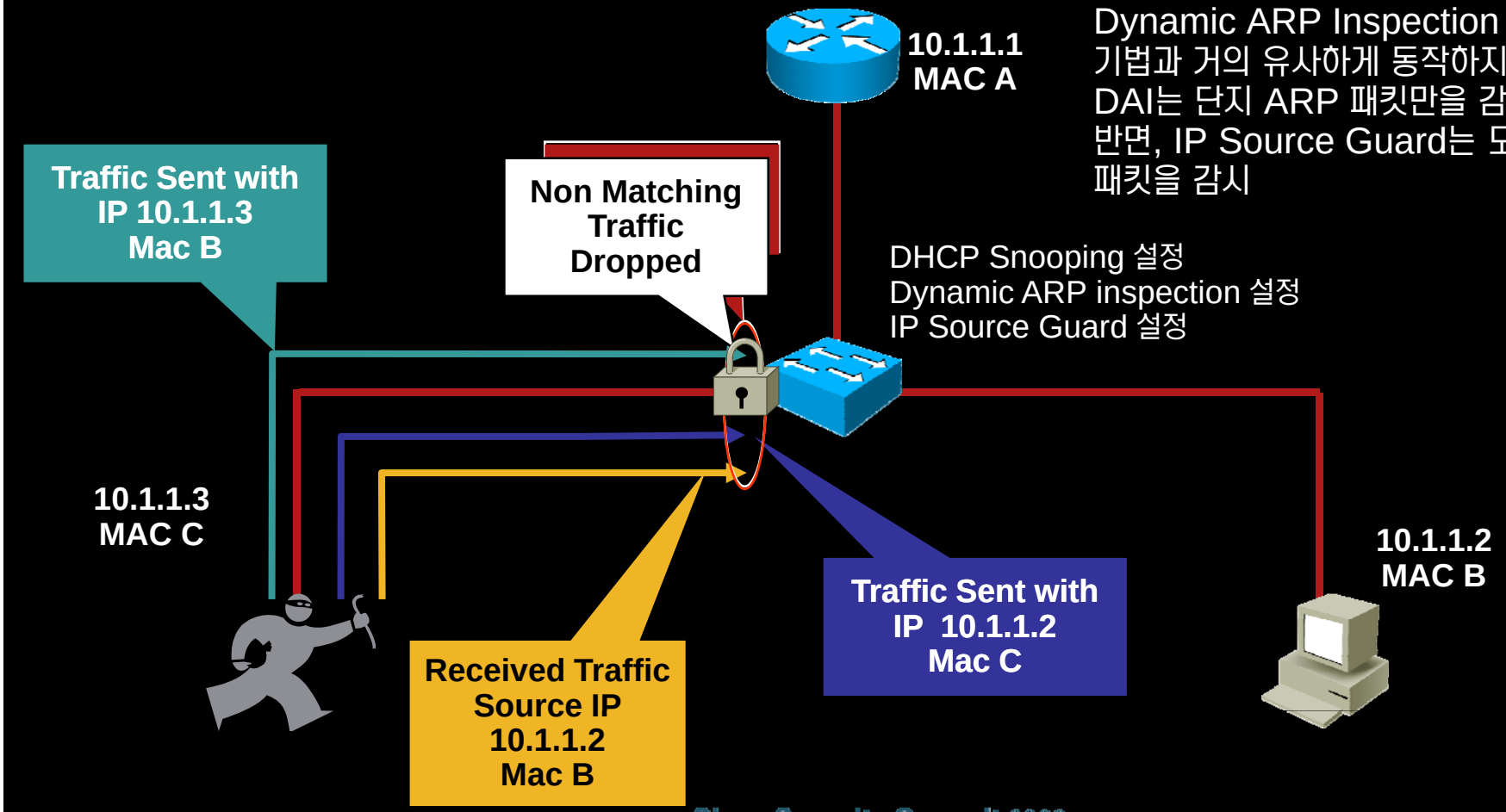
IP 주소 변조 공격



- 공격자는 변조된 소스 IP로 패킷을 전송
- 변조된 IP를 수신한 장비의 응답 패킷은 다른 선의의 사용자로 송신 되게 됨

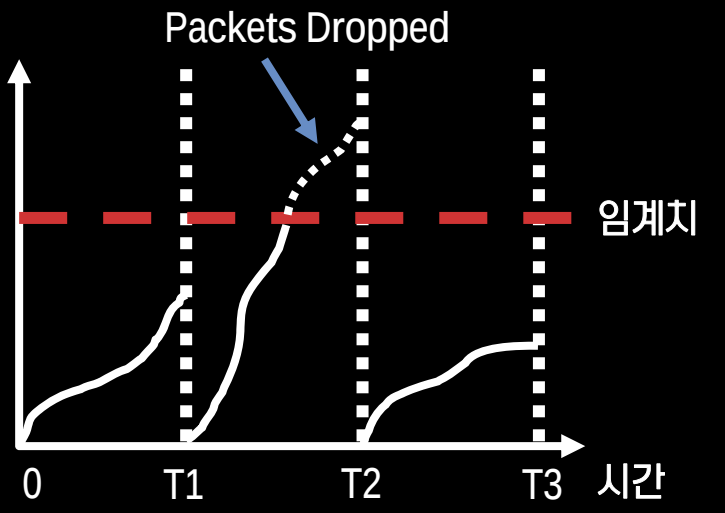
IP/MAC 변조 공격 방지 기법: IP Source Guard

- DHCP Snooping Binding 테이블 정보 참조
- IP Source Guard
  - Dynamic ARP Inspection (DAI) 기법과 거의 유사하게 동작하지만 DAI는 단지 ARP 패킷만을 감시 하는 반면, IP Source Guard는 모든 패킷을 감시



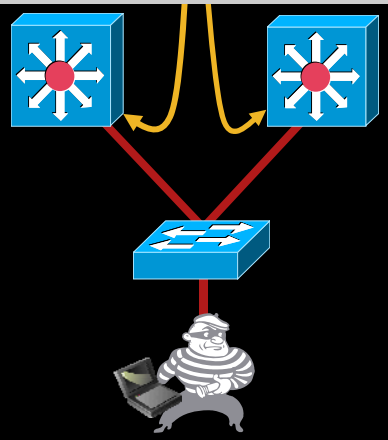
Traffic Storm Control
Flooding 형태의 DoS 공격 방지

- Traffic Storm = 다량의 트래픽이 포트를 통해 VLAN으로 flooding 되면서 전체 네트워크의 성능 저하를 유발시키는 일련의 행위
- Broadcast, multicast, unicast 트래픽에 대한 유입량을 제어
- 의도된 또는 의도되지 않은 다양한 네트워크 flooding 공격 방지
  예) STP 루프, 서버에서 발생되는 대량의 브로드캐스트 트래픽 등

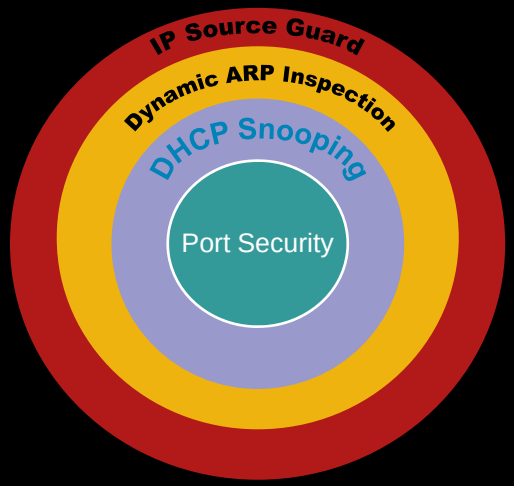



```
! Storm control 기능 설정

storm-control broadcast level 1.0
storm-control multicast level 1.0
```



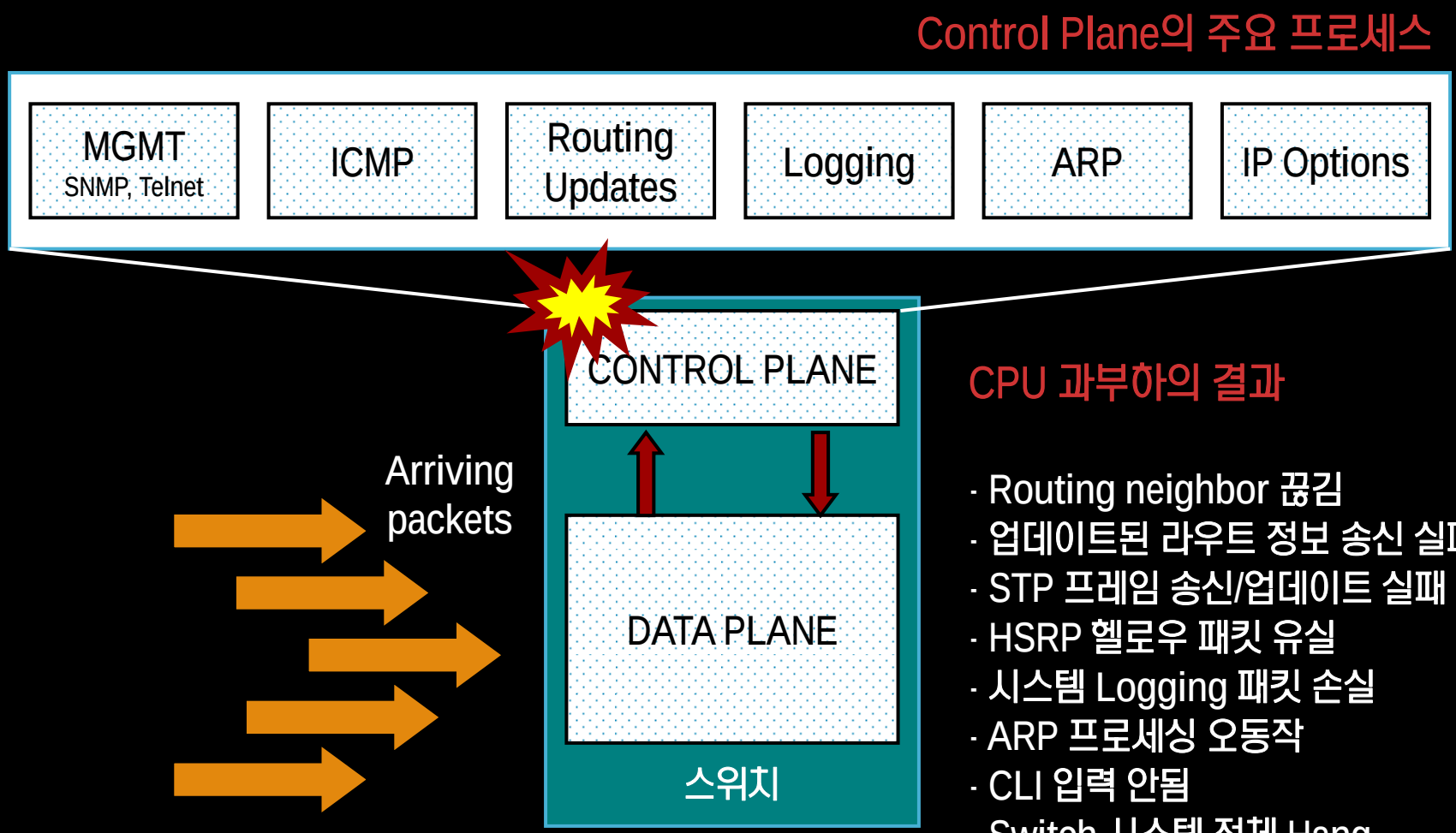
Building the Layers



- Port security: MAC flooding 공격과 DHCP 고갈 공격 방지
- DHCP Snooping: 불법/무허가 DHCP 서버 공격 방지
- Dynamic ARP Inspection: ARP 스푸핑 공격 방지
- IP source guard: IP/MAC 주소 변조 공격 방지
- Traffic Storm Control: Flooding 형태의 DoS 공격 방지

스위치 장비 리소스 보호 기법: CoPP (Control Plane Policing)

Control Plane 보호 기법의 이해

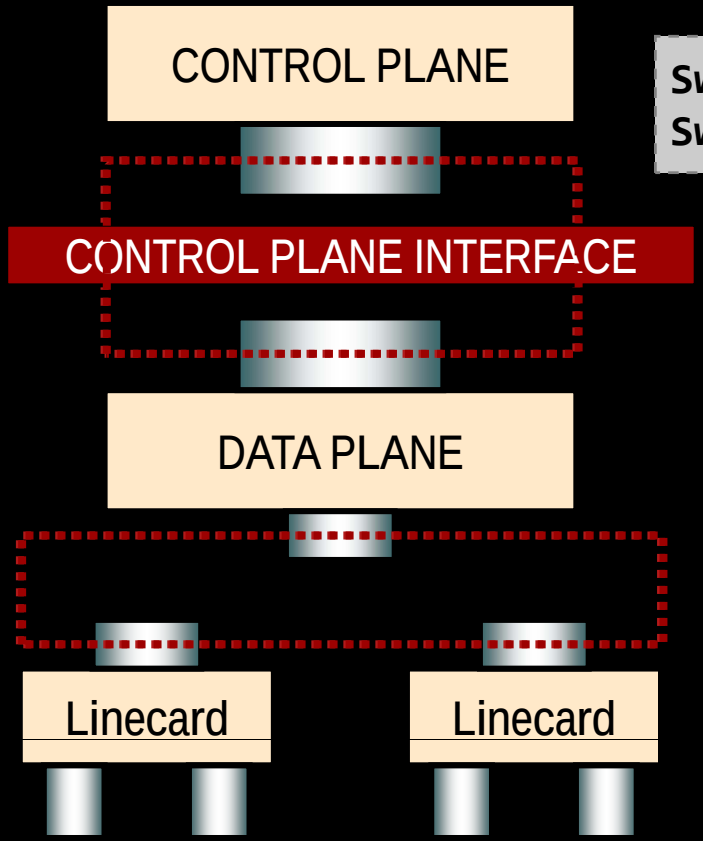


CPU 과부하의 결과

- Routing neighbor 끊김
- 업데이트된 라우트 정보 송신 실패
- STP 프레임 송신/업데이트 실패
- HSRP 헬로우 패킷 유실
- 시스템 Logging 패킷 손실
- ARP 프로세싱 오동작
- CLI 입력 안됨
- Switch 시스템 전체 Hang
- 기타 등등

CoPP 기법의 적용

- **Control Plane Policing (CoPP) 기법:**
  Data Plane과 Control Plane 사이에 논리적인 가상의 인터페이스를 제공하며, 이 가상의 인터페이스에 **Control Plane**을 향하는 트래픽 양을 제어하여 중요한 **Control Plane**의 자원을 보호




```
Switch(config)#control-plane
Switch(config-cp)#service policy input <name>
```

- 새로운 논리 인터페이스 제공: the control-plane interface
- 모듈러 QoS 명령체계 (MQC) 사용
- 계층 구조의 명확하고 손쉬운 config 환경 제공
- 네트워크 장비를 타깃으로 하는 DoS 공격 방어

Cisco TrustSec 아키텍처

변화하는 기업 비즈니스 요구사항

Driving Need for Increased Security with Pervasive Identity

Cisco TrustSec (CTS)

Cisco TrustSec (CTS) 아키텍처란?

"Topology-aware" 방식의 보안 정책 → **"Role-aware"** 방식의 네트워크 보안 정책 적용

1. **"Role-aware" 방식의 접근 제어**
2. **통합 정책 Framework**
3. 기밀성과 무결성

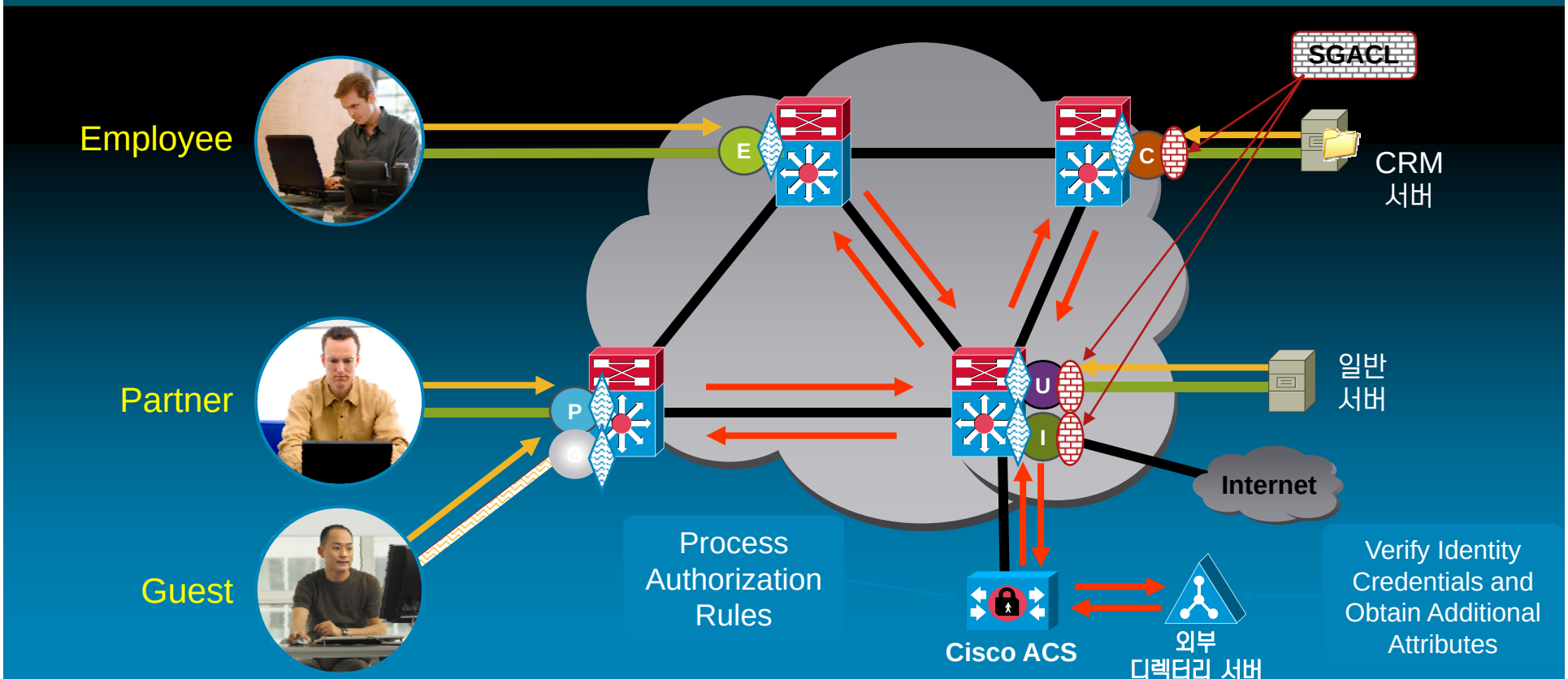
기대효과

운영의 복잡성 제거 & 비용 절감

사용자 접속 환경과 무관한 일관된 정책 적용

Hop-by-hop의 기밀성과 무결성 제공

CTS: 정책 적용 방식



Legend

Link/Port Status

- Unauthenticated
- Failed Authentication
- Authenticated
- Shutdown

- Ingress Tagging
- Egress Filtering

Security Group Classifications

- E Employee Group
- C Confidential Group
- P Partner Group
- U Unrestricted Group
- Guest Group
- I Internet Group

1.
2.
3.
4.
5.

Cisco TrustSec
기밀성과 무결성: Link Layer Encryption

- IEEE 802.1ae 기반의 Hop-by-Hop 패킷 기밀성 / 무결성 제공
- “Bump-in-the-wire” 모델
- 시스템 내에서 다양한 packet inspection 기법 (NetFlow, CISF, IDS) 적용 가능

시스템 내부에서는 Clear 데이터

결론; Why Cisco…

결론; Why Cisco…

모니터링
- 이벤트 검색
- Netflow

전세계 스위치 마켓 리더

전체 스위치 플랫폼에 대한 일관된 보안 솔루션 제공

새로운 Cisco TrustSec 아키텍처

고객 투자보호를 고려한 제품 개발

지속적인 End-To-End 솔루션 리더십

- QoS Scavenger Class
- RACL/PBACL
- Storm Control

Guard/uRPF
- 서비스 모듈

- NetFlow

CISCO

Layer 2 보안 Best Practices (1/2)

- 스위치의 관리는 최대한의 보안 기능을 가미하여 운영 할 것 (SSH, Out Of Band 관리, 리모트 접속에 대한 permit lists, 기타 등등.)
- 항상 trunk 포트를 위한 전용의 VLAN ID를 사용 할 것
- Be paranoid: 어떠한 경우라도 VLAN1은 사용하지 말 것!
- 모든 사용자 포트 설정은 non trunking 모드로
  (Cisco IPT 솔루션 적용의 경우 예외, Voice + Data VLAN)
- 가능한 모든 사용자 포트에 Port-Security를 적용 할 것
- SNMP의 community 설정은 서버의 루트 암호처럼 어렵게 설정
- ARP 보안 이슈에 대비할 수 있는 네트워크 기반 환경 마련 (ARP inspection, IDS/IPS, 기타 등등.)

Layer 2 보안 Best Practices (2/2)

- STP 공격 방지 기법 적용
  (BPDU Guard, Root Guard, Loop Guard 등등)
- DHCP 공격에 대비할 수 있는 솔루션 구현
  (DHCP Snooping, VACLs)
- VTP는 transparent 모드 권장; 사용할 경우 MD5 인증 사용 할 것
- 시스코의 CDP 프로토콜은 꼭 필요한 구간에만 enable 할 것 (IPT 연동 구간, 시스코 장비간의 연동 – 관리목적 – 구간, 등등)
- 사용하지 않는 포트는 셧 다운 시켜놓거나, 사용하지 않는 VLAN을 할당해 놓을 것

"이러한 Best Practice는 고객사의 보안 정책에 맞게끔 구성하여 사용하세요!!!"

Matrix for Security Features (1/3)

Feature/Platform	Nexus 7K NXOS	6500/ Catalyst OS	6500/Cisco IOS	4500/Cisco IOS
Dynamic Port Security	4.0	7.6(1)	12.1(13)E	12.1(13)EW
DHCP Snooping	4.0	8.3(1)	12.2(18)SXE	12.1(12c)EW **
DAI	4.0	8.3(1)	12.2(18)SXE	12.1(19)EW **
IP Source Guard	4.0	8.3(1)*	12.2(18)SXD2	12.1(19)EW **
CoPP	4.0	N/A	12.2(18)SXD1	12.2(31)SG

* Sup720의 경우

** Sup2+ 이상의 Supervisor 필요

Matrix for Security Features (2/3)

Feature/Platform	3750/3560 EMI	3550 EMI	2960 EI	2950 EI	2950 SI
Dynamic Port Security	12.1(25)SE	12.2(25)SEA	12.1(11)AX	12.0(5.2)WC1	12.0(5.2) WC1
DHCP Snooping	12.1(25)SE	12.2(25)SEA	12.1(19)EA1	12.1(19)EA1	N/A
DAI	12.2(25)SE	12.2(25)SEA	N/A	N/A	N/A
IP Source Guard	12.2(25)SE	12.2(25)SEA	N/A	N/A	N/A

Note: Old Names of the IOS for the 3000 Series Switches IOS Feature Finder—
http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

Matrix for Security Features (3/3)

Feature/ Platform	3750/3560 Advance IP	3550 Advanced IP	3750/3560 IP Base	3550 IP Base
Dynamic Port Security	12.1(25)SE	12.2(25)SEA	12.1(25)SE	12.2(25)SEA
DHCP Snooping	12.1(25)SE	12.1(25)SEA	12.1(25)SE	12.1(25)SEA
DAI	12.2(25)SE	12.2(25)SEA	12.2(25)SE	12.2(25)SEA
IP Source Guard	12.2(25)SE	12.2(25)SEA	12.1(25)SE	12.2(25)SEA

Note: Name Change of the IOS on the 3000 Series Switches IOS Feature Finder—
http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

CISCO