

시스코 L4/L7 스위치 ACE의 알아두면 재미있는 가상화 기술

June 18, 2009

Cisco Korea, Systems Engineer

최성열, sungchoi@cisco.com



Agenda

Cisco ACE는?

가상화와 IT

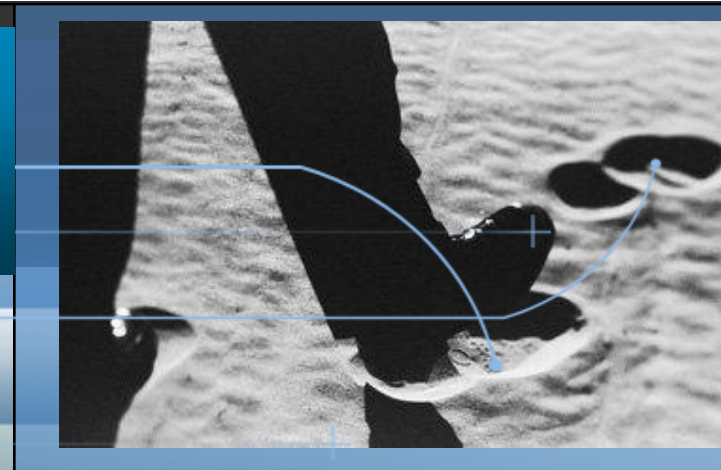
생각의 전환, 가상화

ACE 가상화와 네트워크 디자인

ACE의 진화

Q & A

ANS의 핵심, ACE

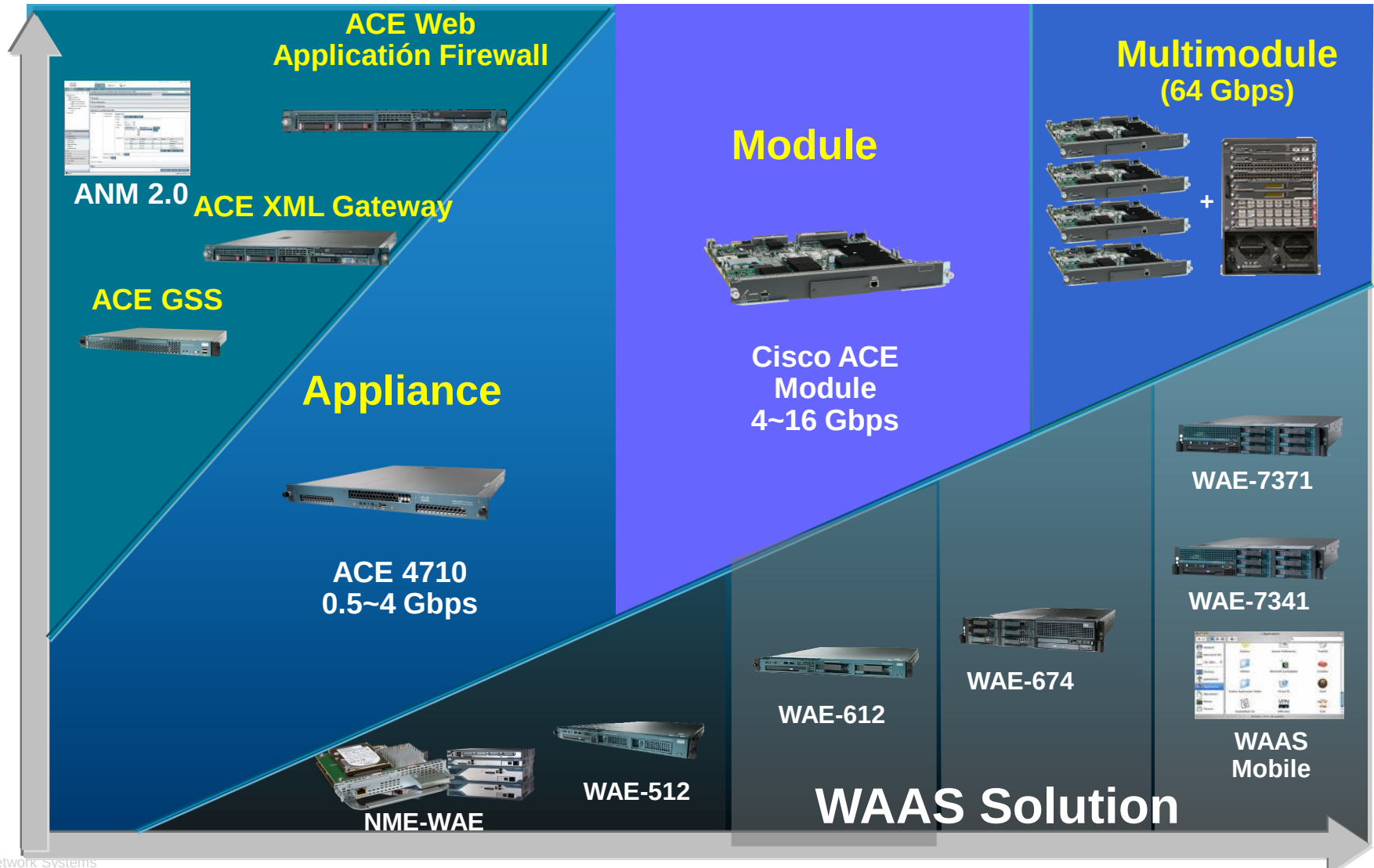


ACE Module

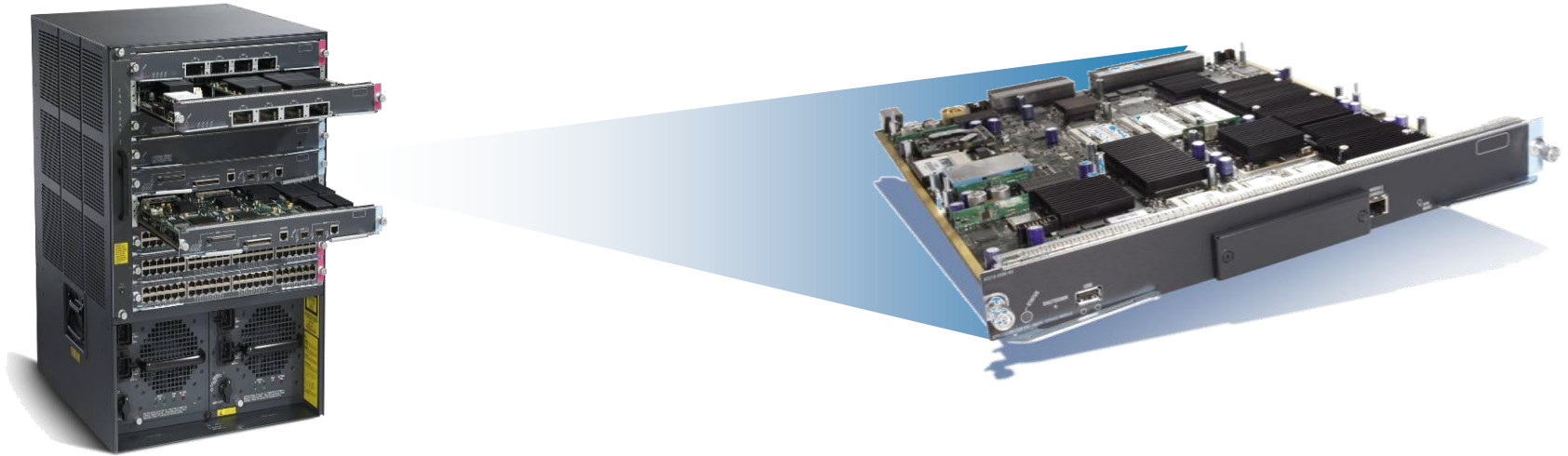


ACE 4710

Cisco Application Networking Services



ACE Module



Catalyst 6500 Switches, 7600 Routers에 장착되는 서비스 모듈

최대 4장의 Module을 장착하여 대형 서비스 구성

처리량: 4 Gbps** ~ 16 Gbps (라이선스 기반: 8, 16Gbps)

하드웨어 **SSL** 처리: 1,000 TPS** ~ 15,000 TPS (라이선스 기반: 5,000, 10,000, 15,000 TPS)

가상화: 5 Context** (라이선스 기반: 20, 50, 100, 250 Contexts)

CLI/GUI (by ANM)기반 편리한 관리

(** 기본 사양)

ACE 4710 Appliance

앞면



후면



1U 사이즈의 날씬한 어플라이언스, 4 x 10/100/1000 Copper Ethernet Ports

처리량: [0.5 Mbps**](#) ~ 4 Gbps (라이선스 기반: 1, 2, 4 Gbps)

하드웨어 기반 압축: [100 Mbps**](#) ~ 2 Gbps (라이선스 기반: 0.5, 1, 2 Gbps)

하드웨어 **SSL** 처리: [100 TPS**](#) ~ 7500 TPS (라이선스 기반: 1000, 5000, 7500 TPS)

웹 가속: 200Mbps, [5세션**](#) (라이선스 기반: 100 세션)

가상화: [5 Context**](#) (라이선스 기반: 20 Contexts)

CLI/GUI 기반 편리한 관리

(** 기본 사양)

Cisco ACE – 주요 특징

가용성



다양한 로드 밸런싱 지원

- SIP
- Extended RTSP
- Radius
- RDP
- Generic Protocol Parsing

확장된 알고리즘들

- Adaptive Algorithms
- Least Loaded (***)
- Least Bandwidth (***)

일반적인 SLB

- KAL-AP
- HTTP Header Rewrite
- Partial Serverfarm Failover
- Application-based Probes
- SNMP-based Probes
- UDP Fast Age

속도



SSL Enhancements

- Session ID Stickiness
- Client Authentication
- SSL Queue Delay

Fast DNS LB

- UDP “booster”

관리 기능

- ANM 1.2
- XML Tagged Config
- Real-time “TCP Dump”
- Mgmt Traffic Protection
- HA Sync Improvements
- Source NAT Changes

보안



Protocol Inspection

- SIP
- ILS/LDAP
- SCCP (Skinny)

ACL Improvements

- Object Grouping

DoS Protection

- SYN Cookie per Interface

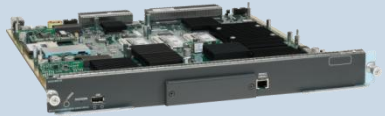
Rate-Limiting

- Connection-rate
- Bandwidth-rate

HTTP 방화벽 기능

- Inspect HTTP POST Body
- Inspect HTTP “Secondary cookies”

ACE4710 vs ACE Module

구 분	ACE4710	ACE Module
실물		
사이즈	1U	1 Slot (Cat6500, Cisco 7600)
포트	4Giga Copper	샤시 형태에 따라
처리량	0.5G ~ 4G	4G ~ 16G
L4 CPS	120,000	325,000
L7 CPS	40,000	133,000
동시 커넥션	1,000,000	4,000,000
DDoS/sec with Syn Cookie	1,000,000	4,000,000
HTTP 압축/가속	O/O	예정
IPv6	예정	예정

이제는 CSS/CSM에서 ACE로

3~4배의
성능 향상

Before:

CSS/CSM Family

로드 밸런싱 스위치



500Mbps to 6Gbps
7,000~44,000CPS

Content Services Switch
(CSS) Appliances –
CSS11501, 11503 11506



4Gbps max
150,000 CPS

Content Switching Module
(CSM) for Cat6K



Future:

ACE Family

가상화가 되는 어플리케이션 스위치



0.5Gbps to 4Gbps
120,000CPS

Application Control Engine
Appliance (ACE 4710)



4Gbps to 16Gbps
325,000CPS

Application Control Engine
Module for Cat6K

CSS/CSM에서 쉽게 ACE로 Conversion Tool

The image shows two overlapping browser windows. The background window is the 'Cisco ACE Module' interface, and the foreground window is the 'CSS to ACE Conversion Tool'.

Cisco ACE Module Interface:

- Header: Cisco ACE Module
- Left Sidebar: TOOLS
 - CSM2ACE conversion tool
 - CSS2ACE conversion tool
- System Info Table:

System Info	
Host_Name	ACE_Admin
Host_Info	10.72.83.182
Uptime	23:50:25 up 21 days, 12:30, 1 user, load average: 0.10, 0.09, 0.09
- Right Sidebar: LINKS
 - Cisco ACE Module Documentation
 - Cisco ACE Module MIB Support List

CSS to ACE Conversion Tool Interface:

- Header: CSS to ACE Conversion Tool
- readme link
- Paste CSS commands: [Text Area]
- User context Name: [Text Field]
- ☐ Include Domain Commands
- Get ACE Commands [Button] Clear CSS Commands [Button]
- Upload CSS command file: [Form with file selection and 'Get ACE Commands' button]
- OR
- Please specify a file: [Form with file selection and 'Get ACE Commands' button]
- Upload the CSS command file to be converted to ACE commands
- © 1992-2006 Cisco Systems, Inc. All rights reserved.

가상화(Virtualization)와 IT



가상화?

Terminal Output:

```

root@localhost/windows/Ani_Movie
Games System V
[root@localhost windows]# cd .
[root@localhost Ani_Movie_Back]# ls
LAST EXILE 건담시드 더파이팅
[root@localhost Ani_Movie_Back]# sl
-bash: sl: command not found
[root@localhost 건담시드]# ls
G-seed08.avi G-seed23.avi G-seed24.avi G-seed25.avi G-seed26.avi G-seed27.avi G-seed28.avi G-seed29.avi G-seed30.avi G-seed31.avi G-seed32.avi G-seed33.avi G-seed34.avi G-seed35.avi G-seed36.avi G-seed37.avi
[root@localhost 건담시드]#
[영어][완성][두벌식]
  
```

Web Browser (Naver Linux Cafe):

NAVER | 메일 | 카페 홈 | 블로그

내 블로그 ▼ 카페 지름길 ----- 로그인

Linux 유져 그룹
cafe.naver.com/linuxcare

Best cafe | 카페매니저: 토모노스 | 카페설립일: 2003.12.15 | 카페멤버: 644 명

초대 | 채팅 | 관리하기

전체보기 (570)

오른 마인드

- 알림 게시판
- 가입인사

리눅스 커뮤니티

- 새 소식/정보
- 자유 게시판
- 질문/답변
- 팁/기술정보
- 컬럼/인터뷰
- 장터/구입구직
- 마이 리눅스박스

스터디 그룹

- 배워서 남주자

공유 자료실

- 문서자료
- 갤러리/스크린샷

RELATED SITE

- 데비안 사용자 모임
- 그놈 한국 사용자 모임

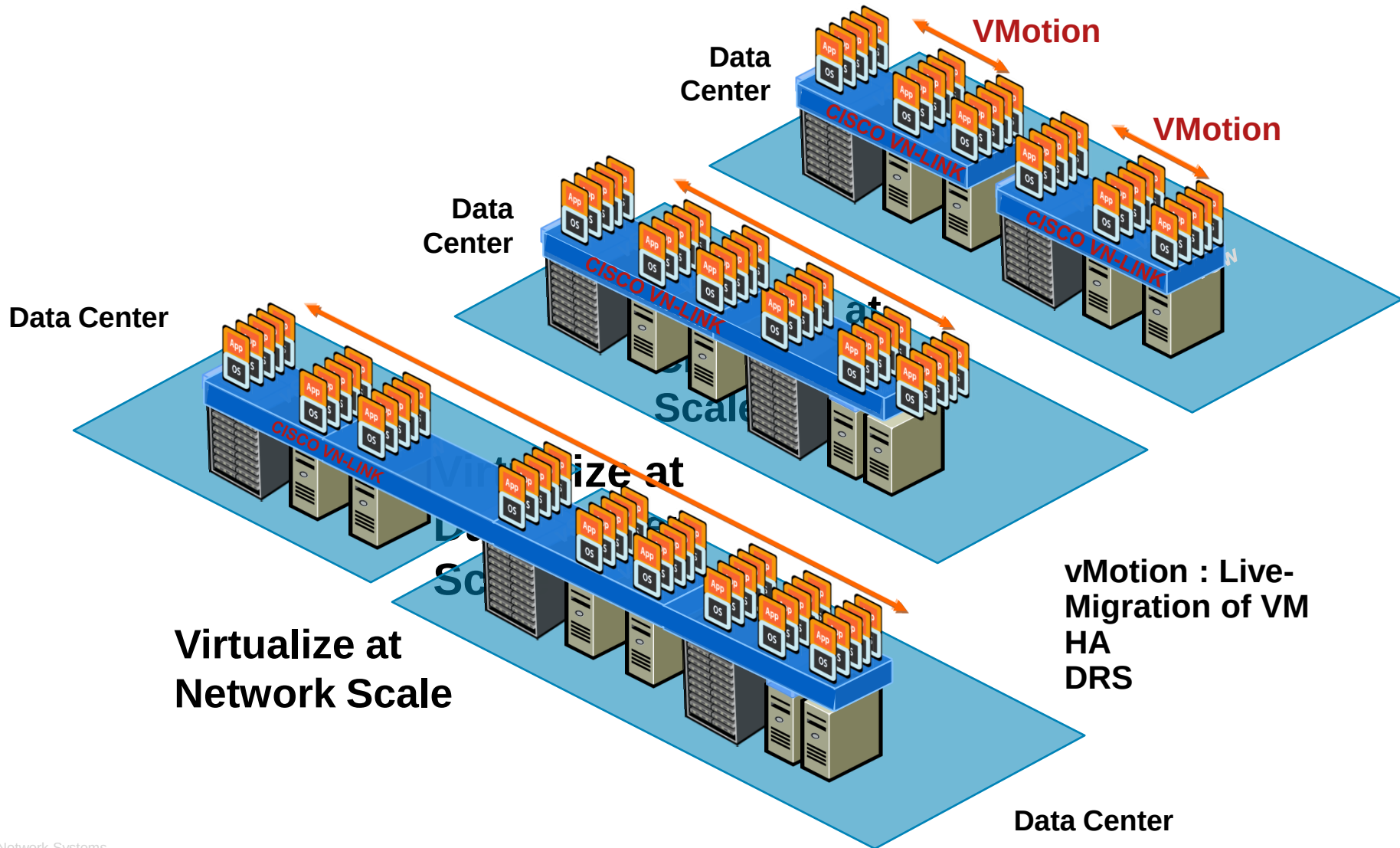
전체보기

NOTICE	제목	작성일	답변
NOTICE	'배워서 남주자' 프로젝트(?)에 동참해 주세요! :) [6]	2004/02/28	
NOTICE	축! '네이버 대표카페 선정, 디렉토리 대표카페로 등록!' ^^ [11]	2004/01/20	
NOTICE	"네이버 리눅스 유져 그룹(NLUG)" 이란? [1]	2003/12/15	
	639 산 [질문]리눅스에 VMware설치후 Win2000 에서...	2004/03/04	0
	638 groomy78 enlightenment 설치 할줄아시는분??	2004/03/04	1
	637 산 리눅스 프로그래머 73% "로열티 법적 공세 부당"	2004/03/03	0
	636 식풍 드라이버 설정이 궁금해요...	2004/03/03	5
	635 송규호 LVSL NFS에 관한 질문입니다.....	2004/03/03	3
	634 hope4179 오늘 가입했어요!!	2004/03/03	9
	633 byulrim [스샷] 엑스윈도.. windowmaker ^^	2004/03/03	14
	632 jara3 가입인사 드려요~~~~	2004/03/03	3
	631 junanyoo [질문] 윈도우에서 리눅스 접속하기	2004/03/03	21
	630 우리누리 리눅스 초보자 질문입니다...고수님들의 조언좀..	2004/03/03	11
	629 jacob427 안녕하세요~~~ 첨 가입했어요..	2004/03/03	3
	627 댄디짱 협력요청합니다.★국제 IT 자격증 쉽게 따기 카페입니다.	2004/03/03	10
	625 jerryjiang 가입했습니다.!!!	2004/03/03	3

출처: http://cafe.naver.com/linuxcare-cafe?iframe_url=/ArticleRead.nhn%3FarticleId=640

서버 가상화

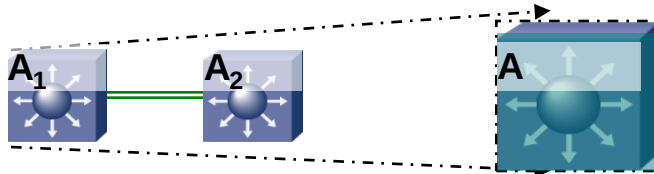
Vmware, Hyper-V, OVM, KVM, Xen, VirtualBox.....



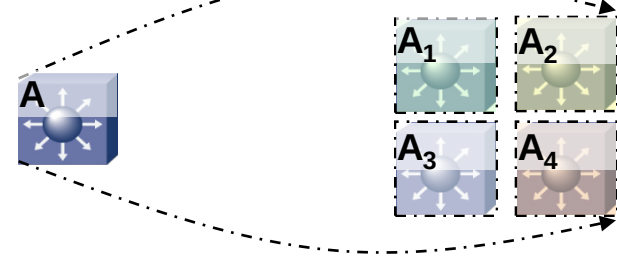
스위치 가상화

Cisco Catalyst 6500 VSS / Nexus 7000 VDC

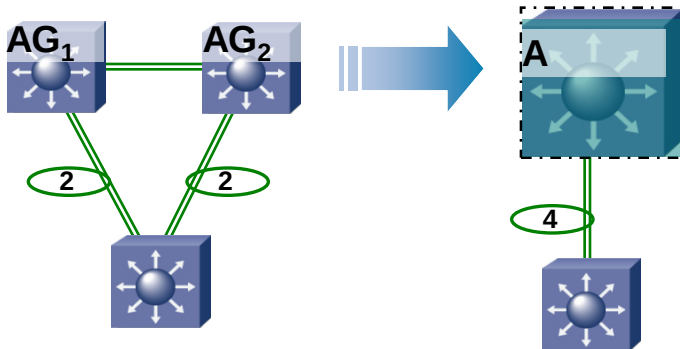
Catalyst 6500 VSS (2 → 1)



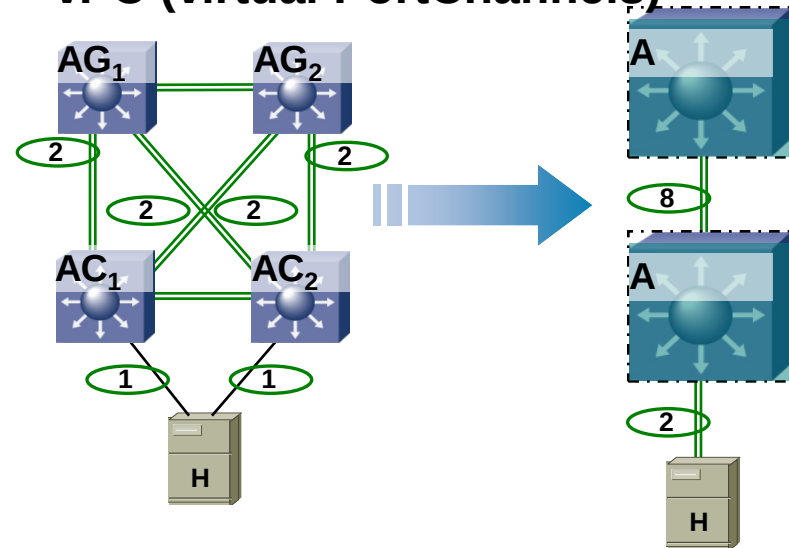
Nexus 7000 VDC (1 → upto 4)



Catalyst 6500 VSS



Nexus 7000/5000 vPC (virtual PortChannels)



(Note) Ethernet Evolution : STP+ → vPC → L2MP

통합을 위한 가상화

Physical Infrastructure



Server

Virtual Infrastructure



Virtual Servers



Network



Virtual Networks



Storage



Virtual Storage

Shared Infrastructure 'Stack'

VMotion App1

Application 2

Virtual Machines



Virtual LANs



Virtual Firewalls



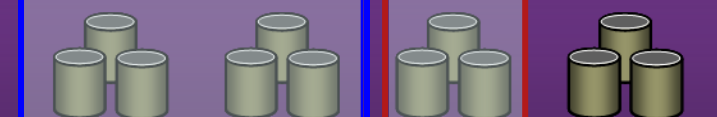
Virtual Load Balancers



Virtual SANs



Virtual LUNS



Policy, Security, QoS

그런데 왜 가상화?

데이터센터 공간 활용 극대화



서비스간의 보안



새로운 서비스 도입시간 단축

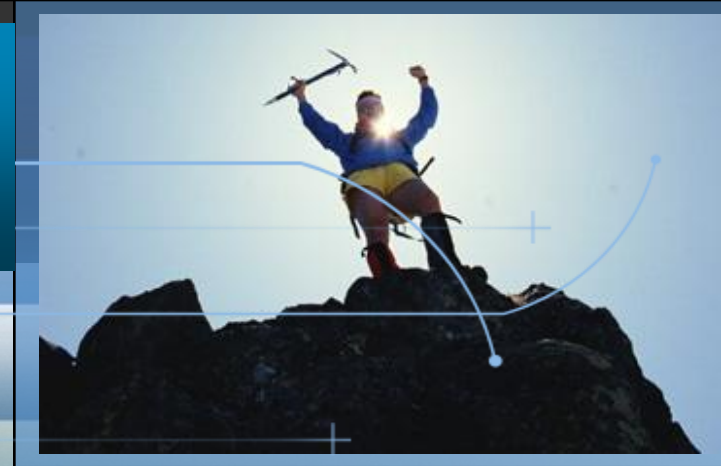


전력/쿨링 비용 감소-그린IT



서비스 연속성/가용성

생각의 전환, 가상화



불황의 시대, 네트워크 가상화를 주목하라

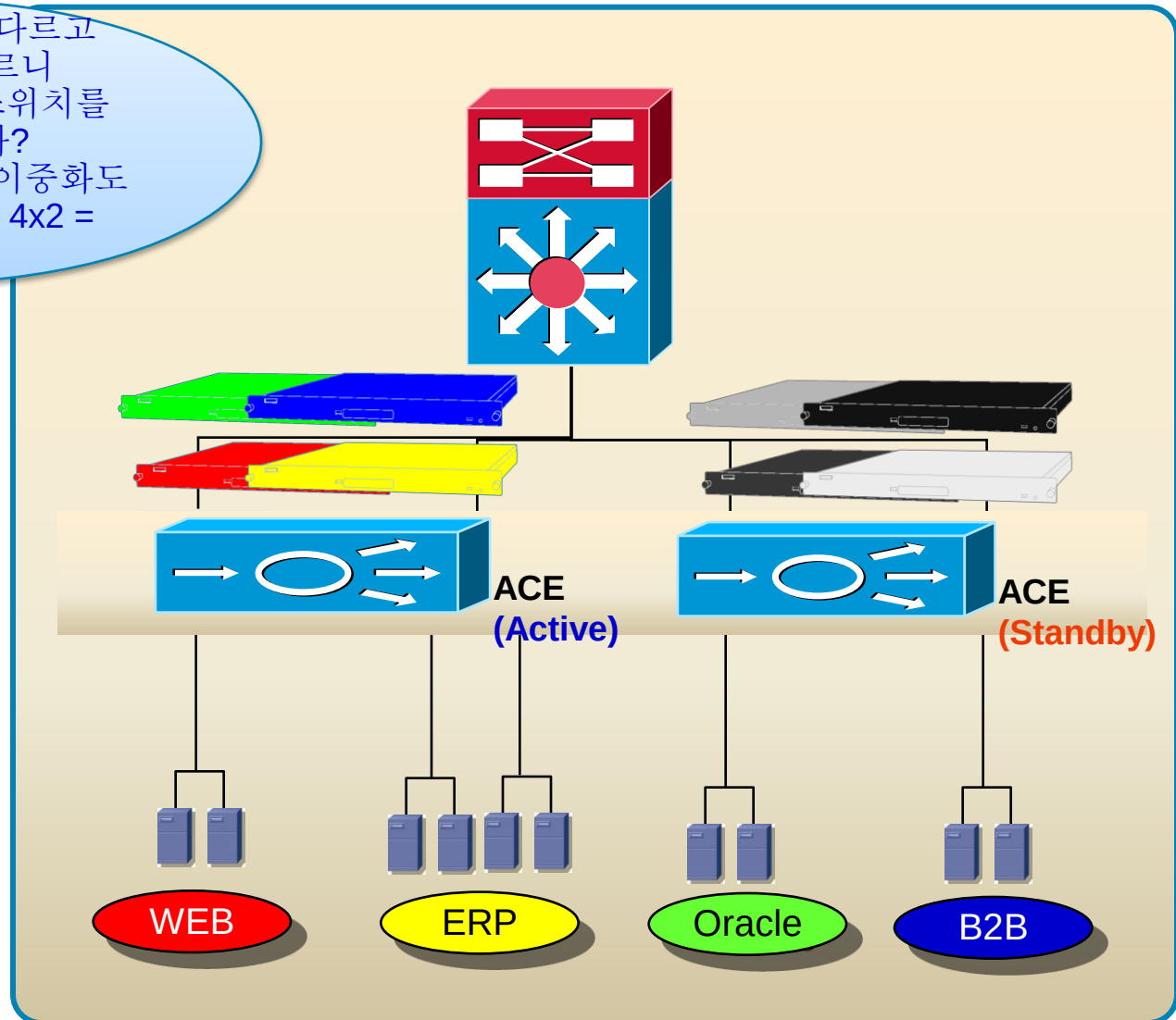
가상화 기술로 대형 네트워크 운영효율성 높이는 방안 속속 등장

2009년 02월 24일 11:33:38 / 김재철 기자 mykoreaone@ddaily.co.kr

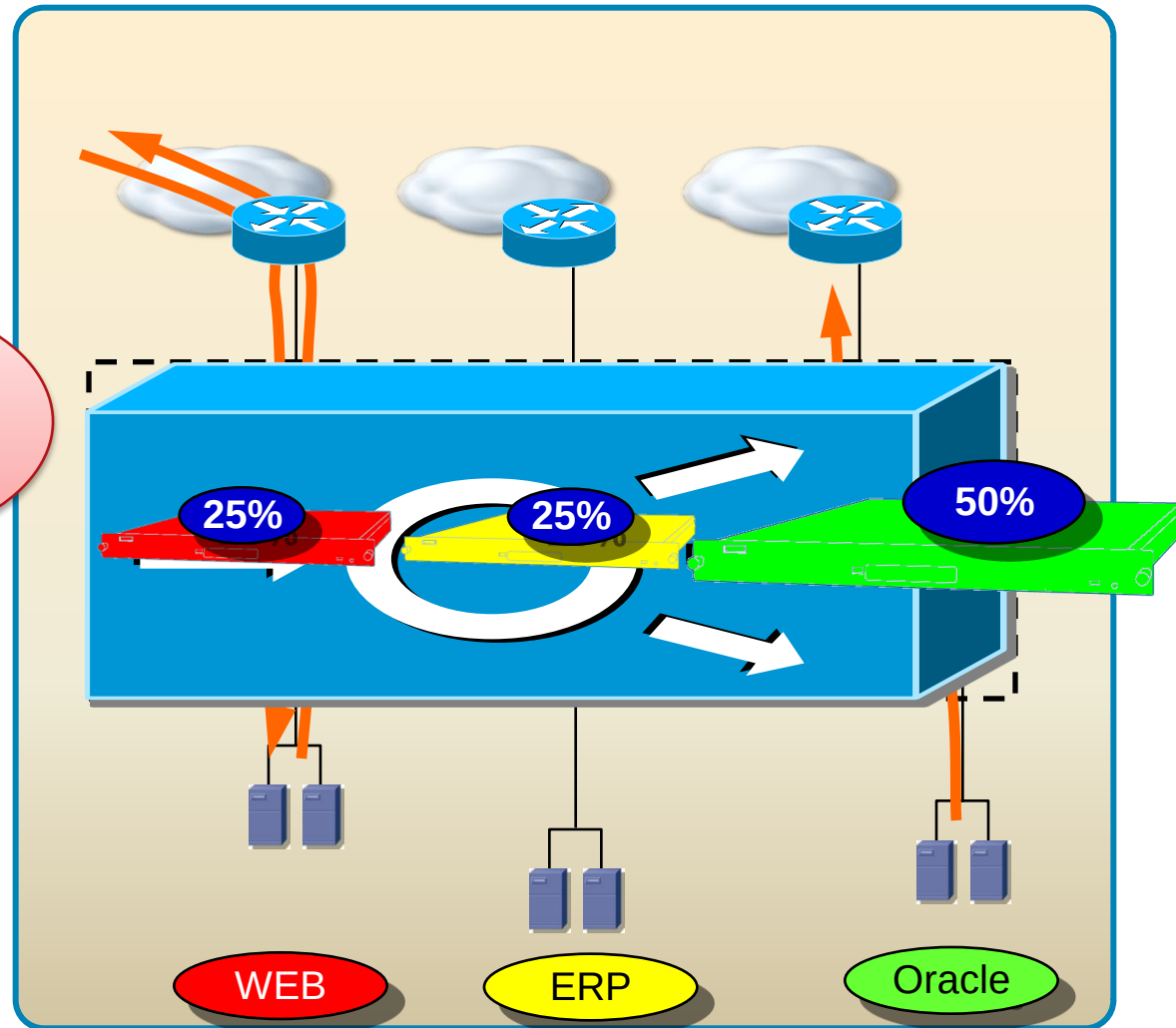
네트워크 장비 업체들, 가상화 지원 팔 걷고 나선다

가상화?

“음.. 관리자 들도 다르고
네트워크도 다르니
서비스마다 L4/7 스위치를
도입해야 하나?
안정성을 위해서는 이중화도
해야하고 그러면? $4 \times 2 = 8$ 대네?”

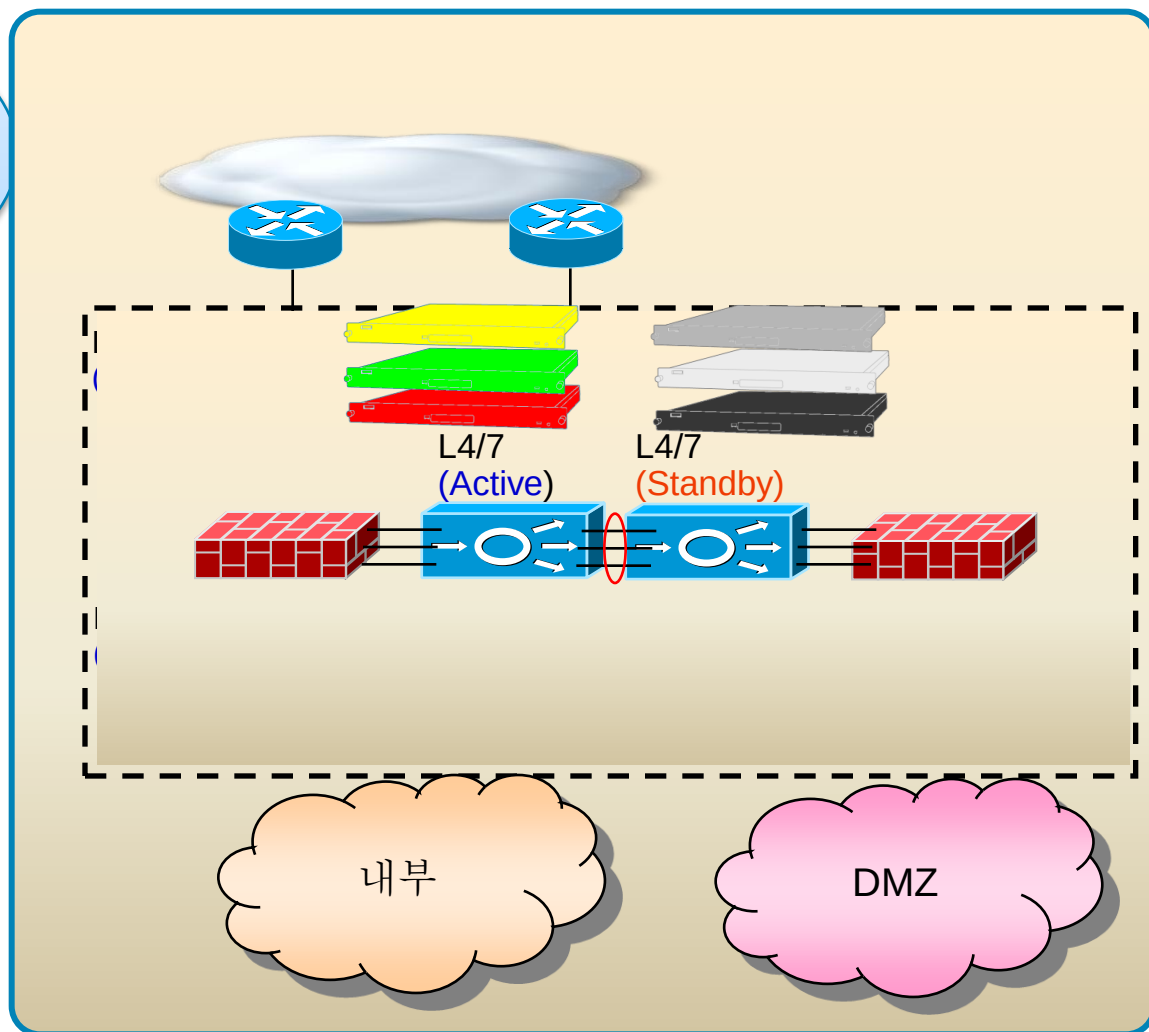


그럼 이럴 때도 될까?



방화벽 LB는 배보다 배꼽이 더 크다?

FLB 구성을 하고 L4도 이중화 하려니 적어도 4대, DMZ까지 있으면 6대? 고민이네.
외부 HA, 내부 HA, DMZ HA + SLB



가상화 구성

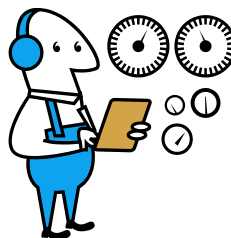
생각대로
ACE~

- 기본 5개의 Context, 라이선스로 20(ACE4710), 250(ACE-M)개로 업그레이드

Rates



- Bandwidth
- Data connections / sec
- Management connections / sec
- Ssl-bandwidth
- Syslogs / sec

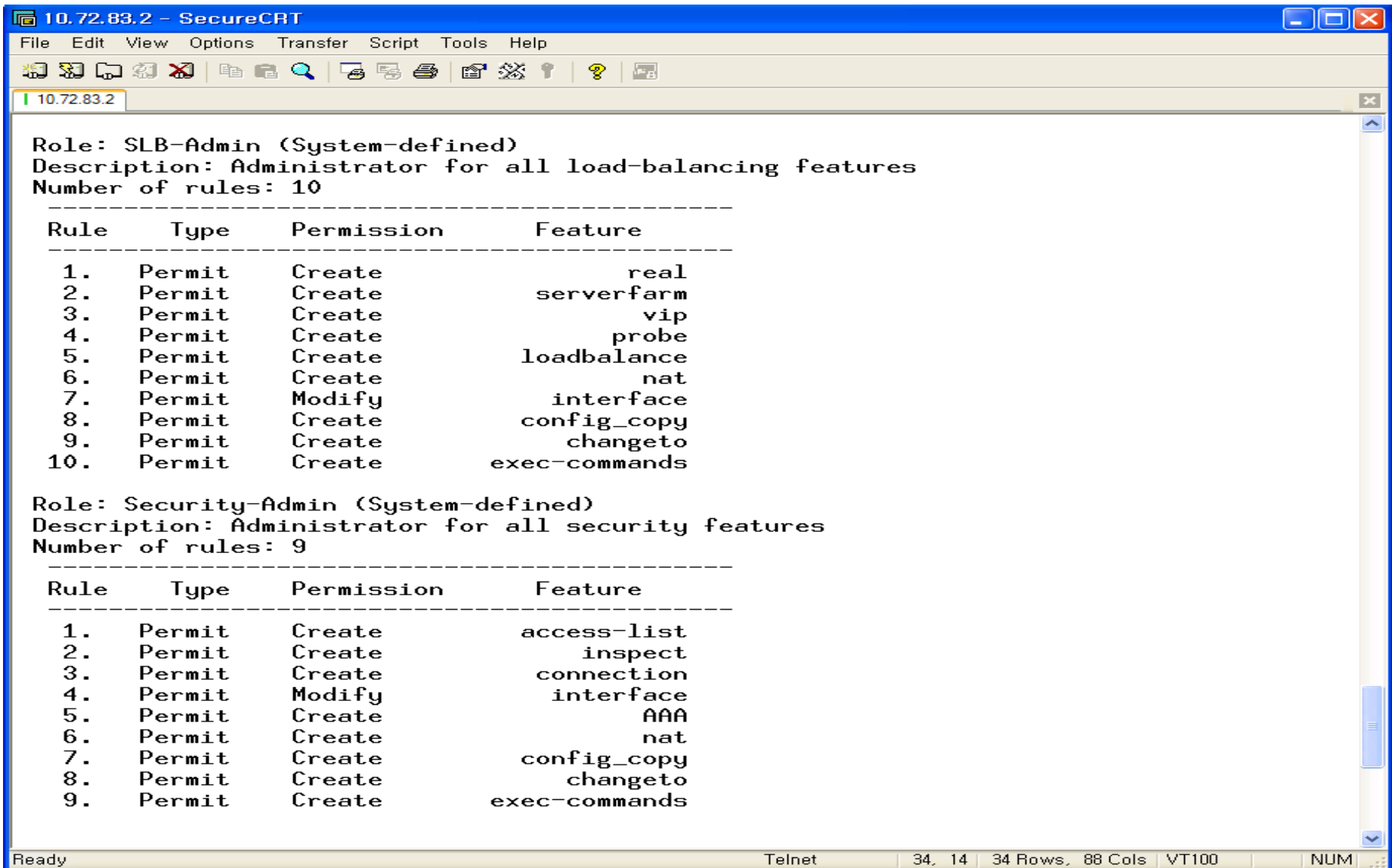


Memory



- Access Lists
- Regular Expressions
- Data connections
- Management connections
- SSL connections
- Xlates
- Sticky entries

가상화를 위한 Role 정의



10.72.83.2 - SecureCRT

File Edit View Options Transfer Script Tools Help

10.72.83.2

Role: SLB-Admin (System-defined)
Description: Administrator for all load-balancing features
Number of rules: 10

Rule	Type	Permission	Feature
1.	Permit	Create	real
2.	Permit	Create	serverfarm
3.	Permit	Create	vip
4.	Permit	Create	probe
5.	Permit	Create	loadbalance
6.	Permit	Create	nat
7.	Permit	Modify	interface
8.	Permit	Create	config_copy
9.	Permit	Create	changeto
10.	Permit	Create	exec-commands

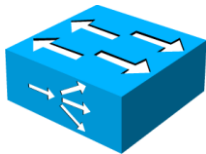
Role: Security-Admin (System-defined)
Description: Administrator for all security features
Number of rules: 9

Rule	Type	Permission	Feature
1.	Permit	Create	access-list
2.	Permit	Create	inspect
3.	Permit	Create	connection
4.	Permit	Modify	interface
5.	Permit	Create	AAA
6.	Permit	Create	nat
7.	Permit	Create	config_copy
8.	Permit	Create	changeto
9.	Permit	Create	exec-commands

Ready Telnet 34, 14 34 Rows, 88 Cols VT100 NUM

가상화를 정리하면

□ 전통적인 SLB Switch 문제점



복잡한 설정 파일

복잡한 라우팅 테이블

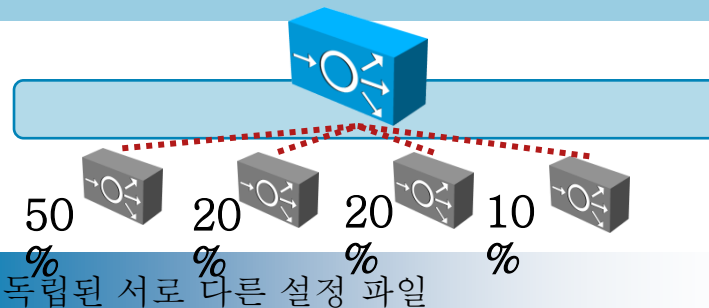
Roll 기반 접근 제어 불가능

Resource 할당 및 제어 불가능

단일 Box의 한계점과 단점들...



□ 가상 파티셔닝 기술 제공 장점

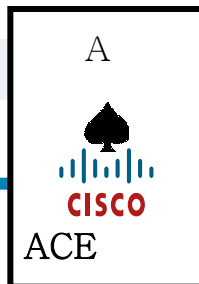


라우팅 테이블 분리

가상 파티셔닝별 접근 제한

가상 SLB 별 Resource 할당 및 제어

독립된 보안 기능 적용



최근 ACE 가상화 구성 현황

ACE Module

1,040 ACE Modules Sold

- 73% 4G
- 24% 8G
- 2% 16G

31% SSL attach

- 79% 5k tps
- 8% 10k tps
- 13% 15k tps

31% Virtualization attach

- 85% 20 contexts
- 9% 50 contexts
- 2% 100 contexts
- 2% 250 contexts

ACE Appliance

817 Appliances Sold

- 17% 0.5G
- 62% 1G
- 14% 2G
- 7% 4G

4% SSL attach

- 100% 5k tps

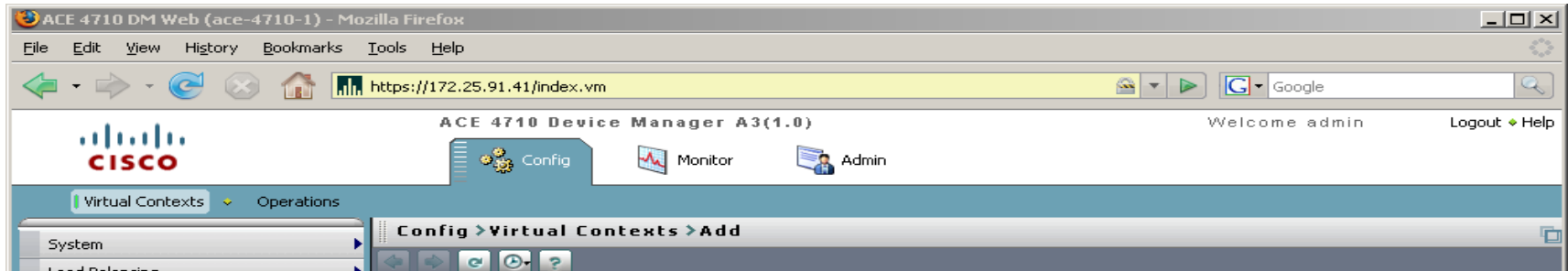
3% Virtualization attach

- 100% 20 contexts

2% Compression attach

- 58% 500Mbps
- 29% 1G
- 13% 2G

새로운 Load Balancer 똑딱 만들기



All Virtual Contexts

	Name	Resource Class	Management IPs	CLI Sync Status	ACE HA State	ACE HA Peer State	ACE HA Peer	ACE HA Autosync
1	☐ Admin	admin	10.1.20.2, 172.25.91.41	✓ OK	N/A	N/A		true
2	☐ IBM	silver_service	172.25.91.42	✓ OK	N/A	N/A		true
3	☐ Microsoft	default	172.25.91.43	✓ OK	N/A	N/A		true
4	☐ Shopping-Cart	gold_service	172.16.200.10	✓ OK	N/A	N/A		true
5	☒ SJC-WEB-Basic-0375Q	Web-Starter-Pack	10.0.33.15	✓ OK	N/A	N/A		true

Default Gateway IP: 10.0.33.15

SNMP v2c Community: public

Community string required for monitoring virtual contexts.

Deploy Now Cancel

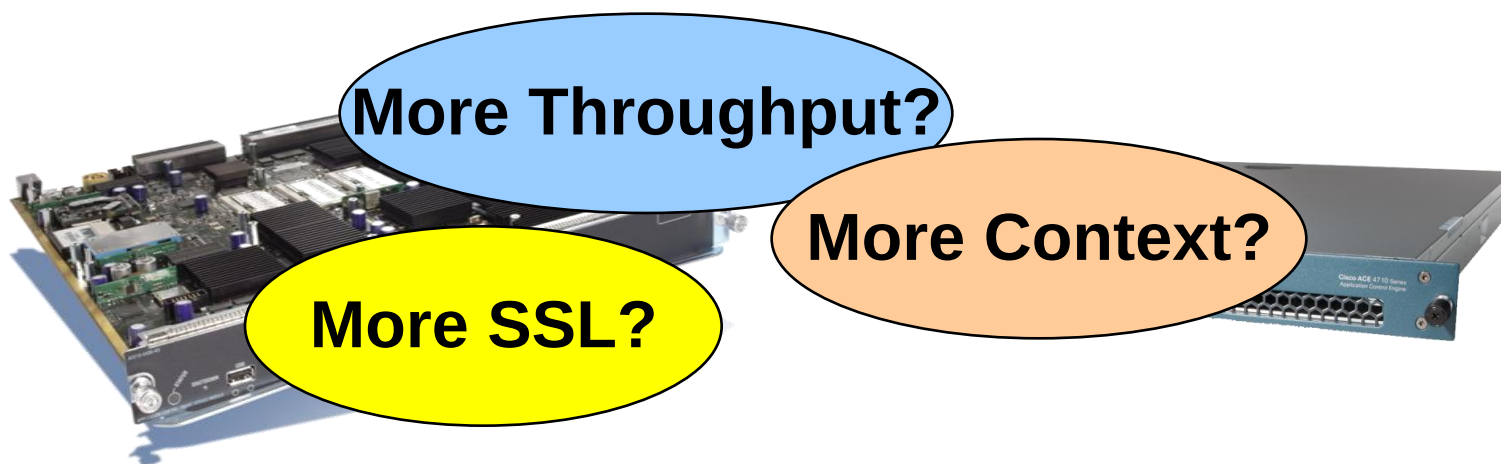
Ready ✓ DM in sync with CLI 13-Oct-2008 16:13:22

라이센스 기반?



이젠 필요할 때 업그레이드 한다..

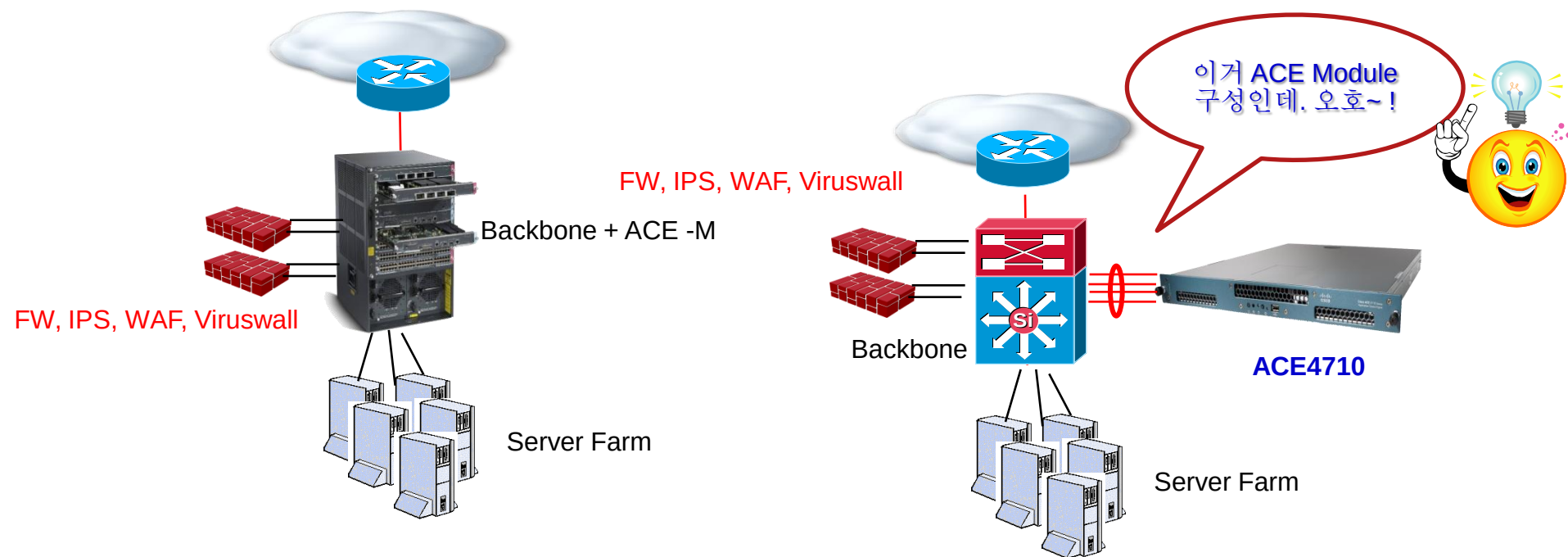
- 라이선스 만으로 원하는 성능 구현!
- 필요한 성능/기능을 자유롭게 선택
- 불투명한 미래를 위해 비싼 초기 비용은 이제 그만!!!!



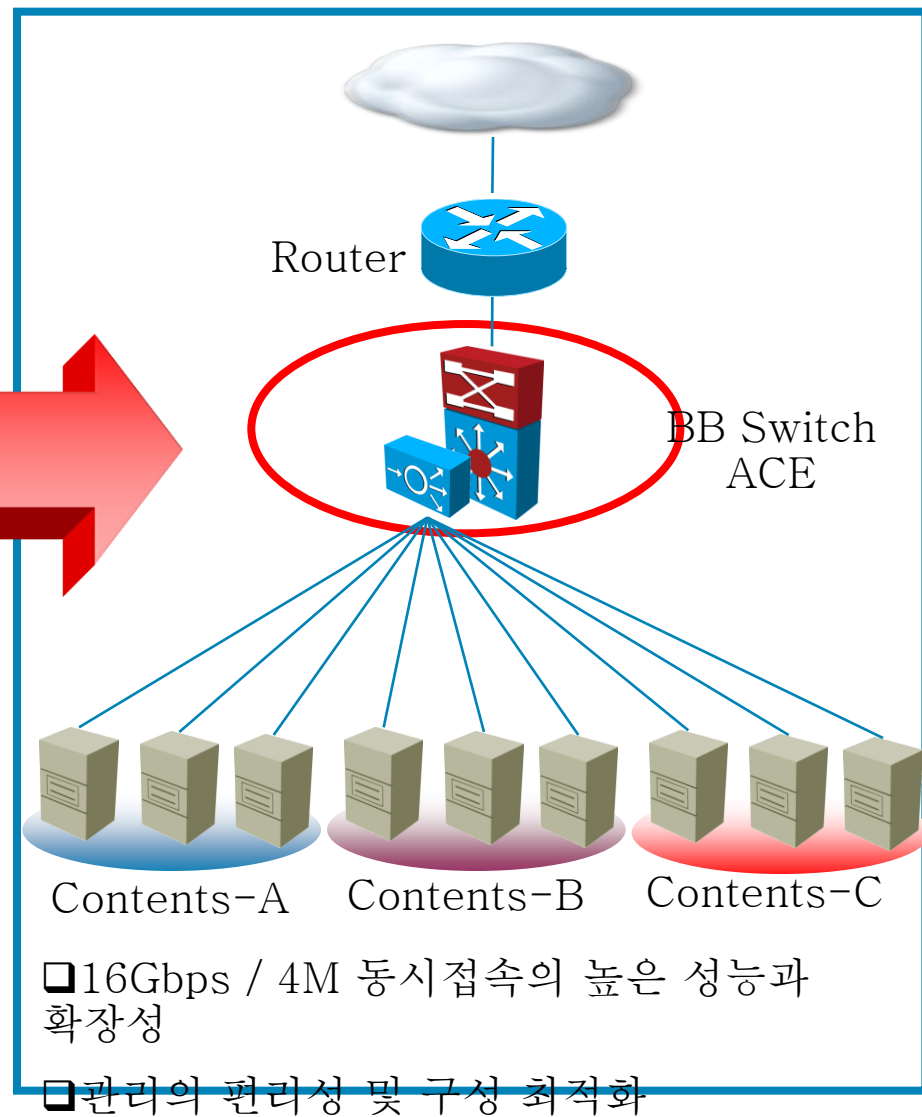
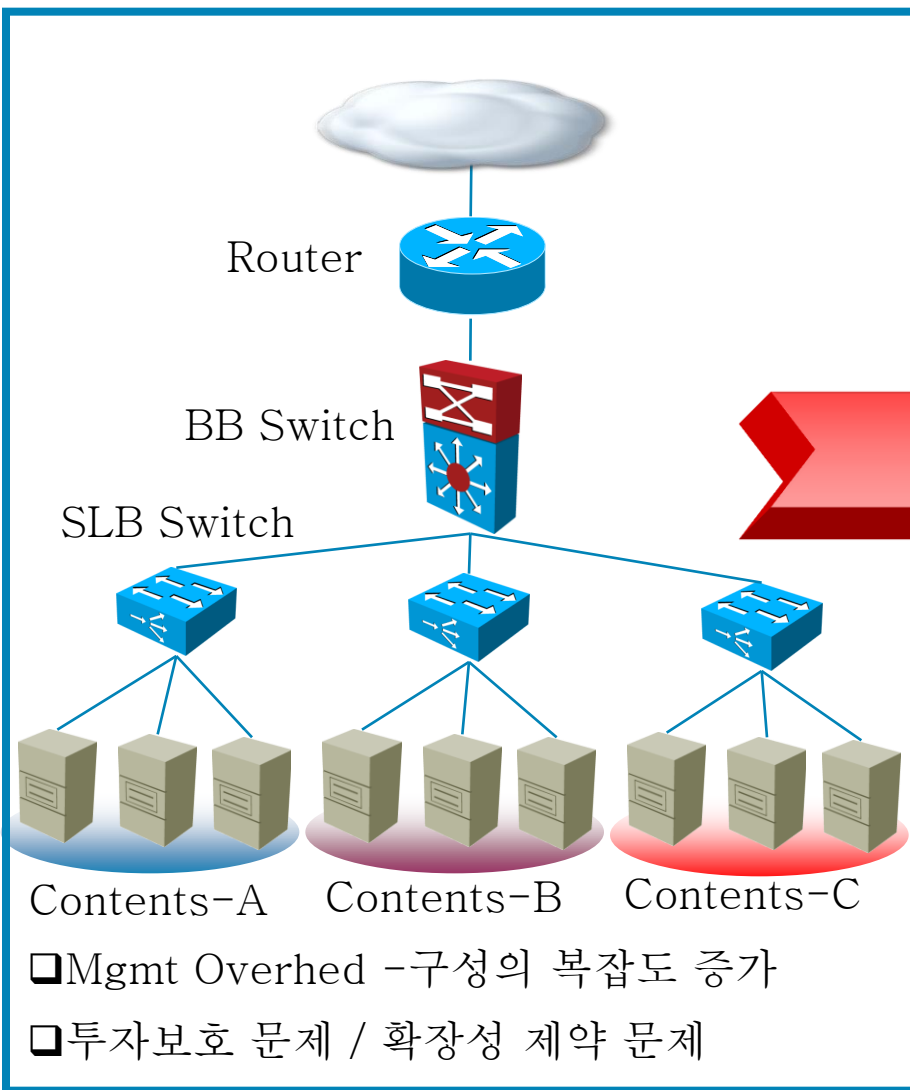


물리적인 포트 구성을 자유롭게!

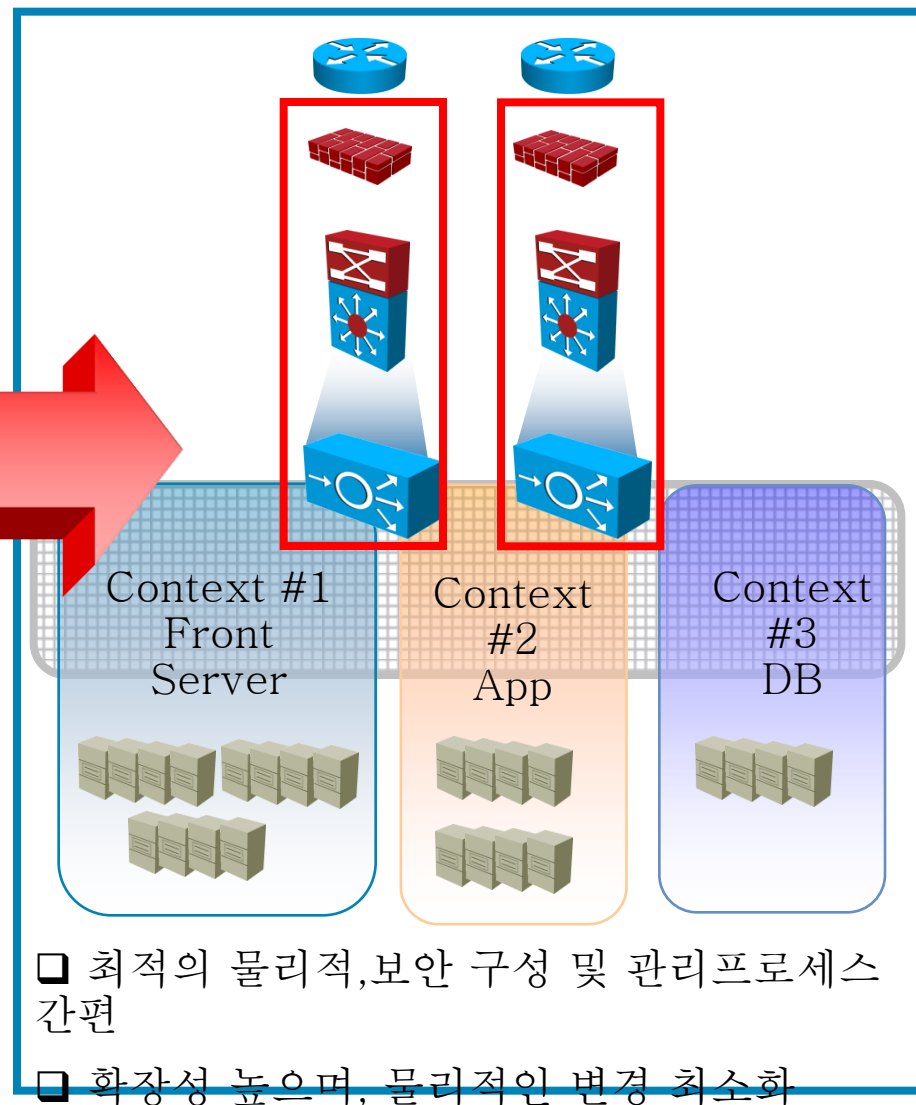
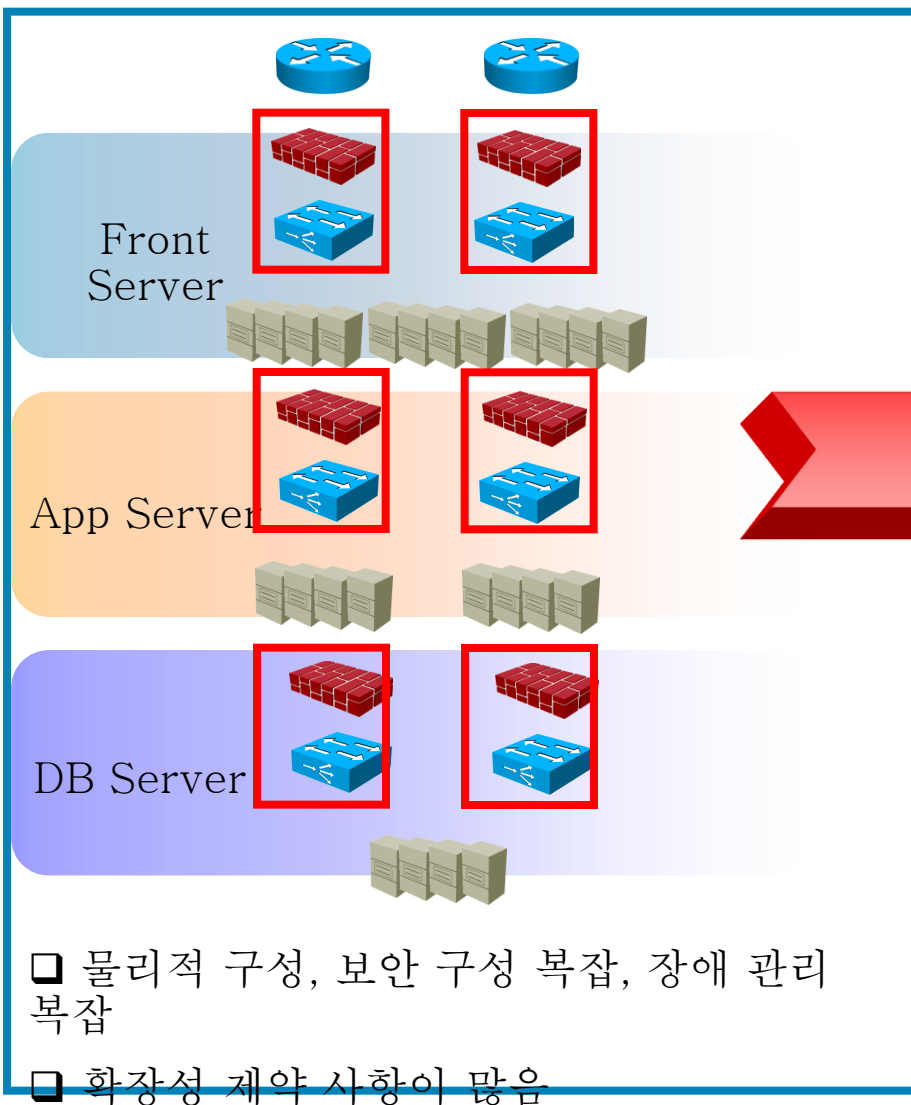
- C6500과 연계시 포트 구성에 대한 제약 탈피
- ACE4710의 경우 기존/신규 L2/L3 SW를 적용하여 ACE Module 과 동일 구성
- 브리지, 라우팅, DSR 모든 구성 가능



ACE Module의 가장 큰 효과는? *Simple*

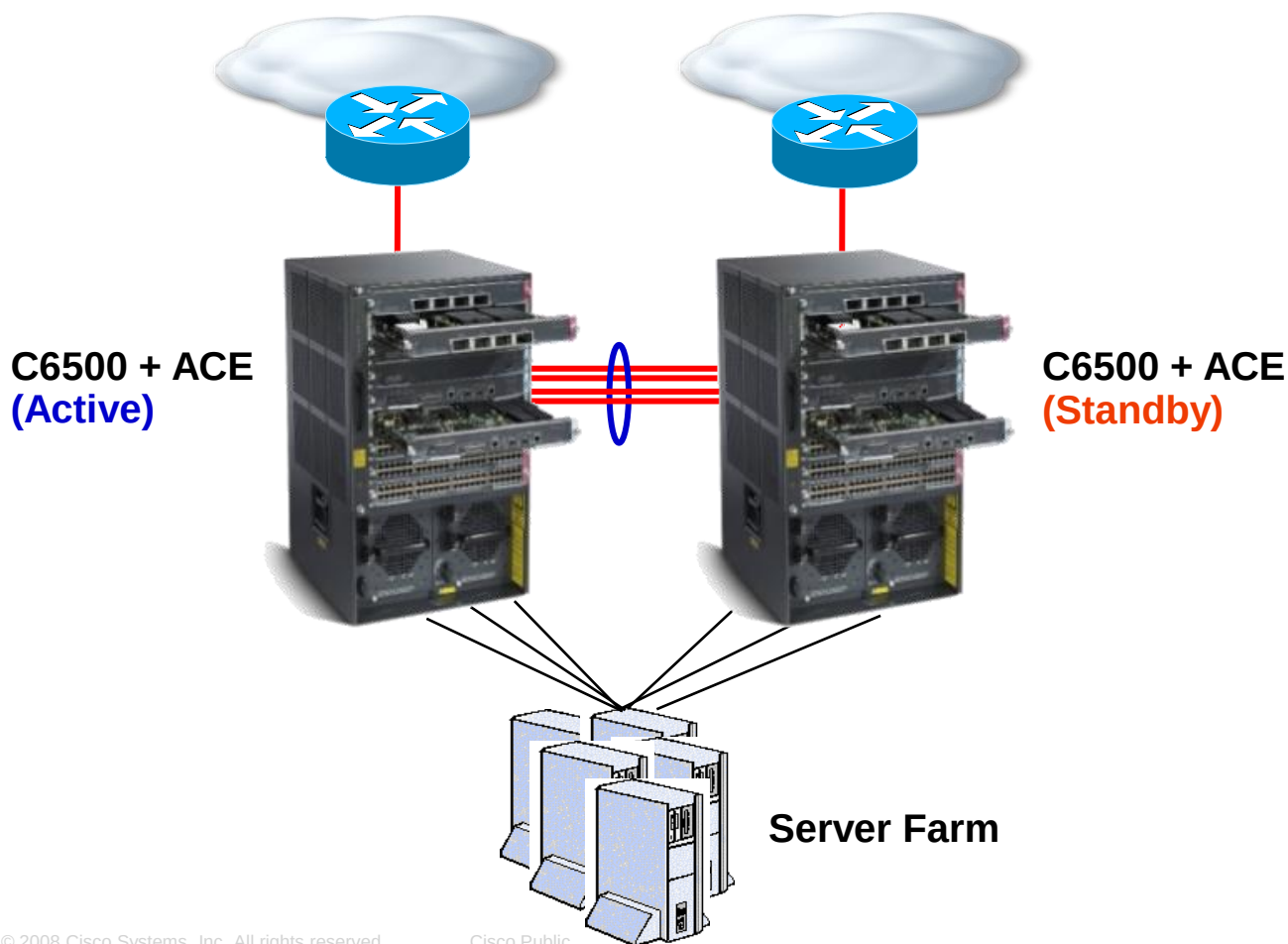


ACE Module의 가장 큰 효과는? *Simple*



이중화 구성(HA) – *ACE Module*

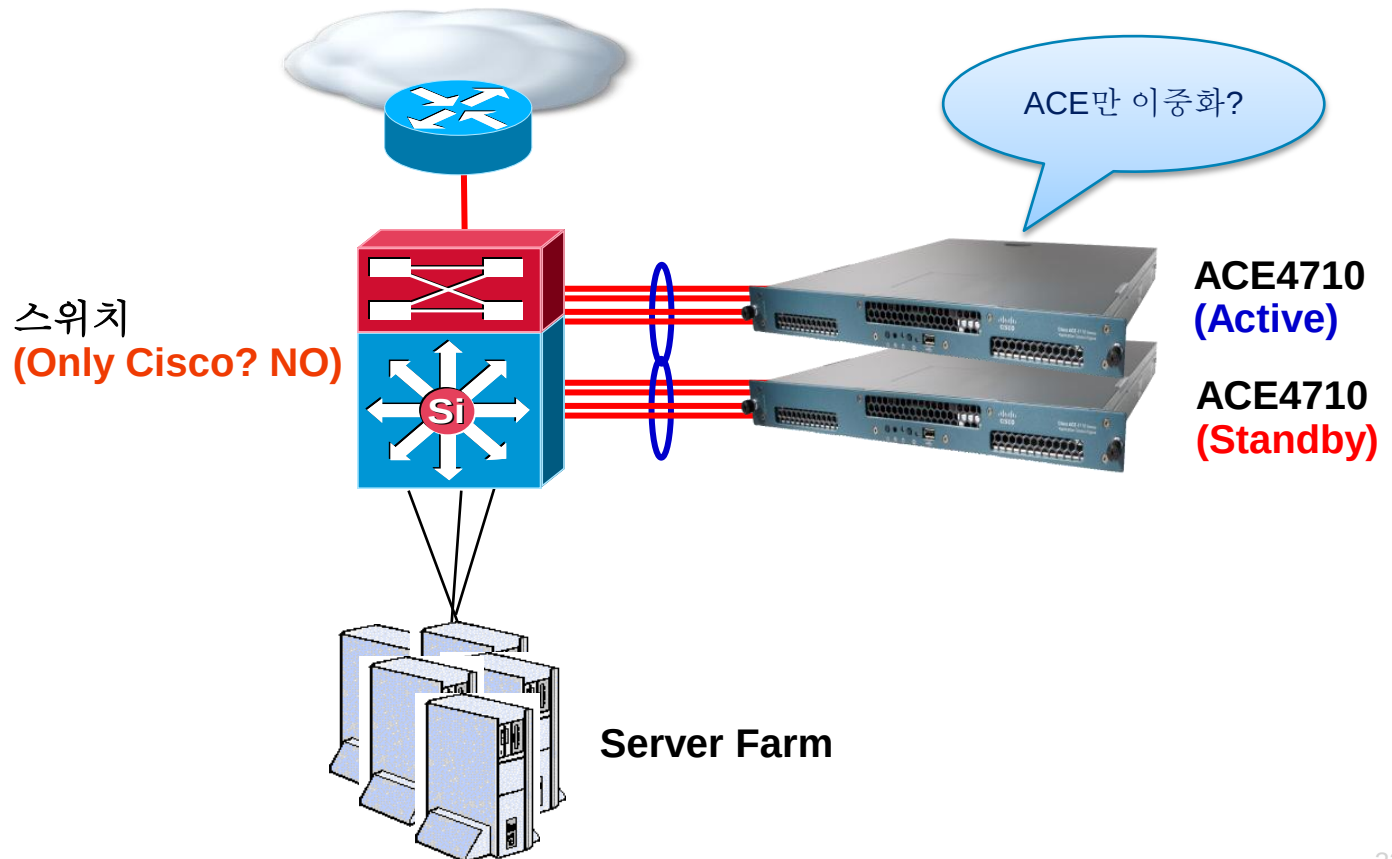
- 기존 C6500 고객이 모듈 추가도입으로 간단한 구현 가능
- C6500과는 별도로 ACE Module내에서의 이중화 구성



ACE4710 으로 ACE Module 구성을 그대로

- HA 구성

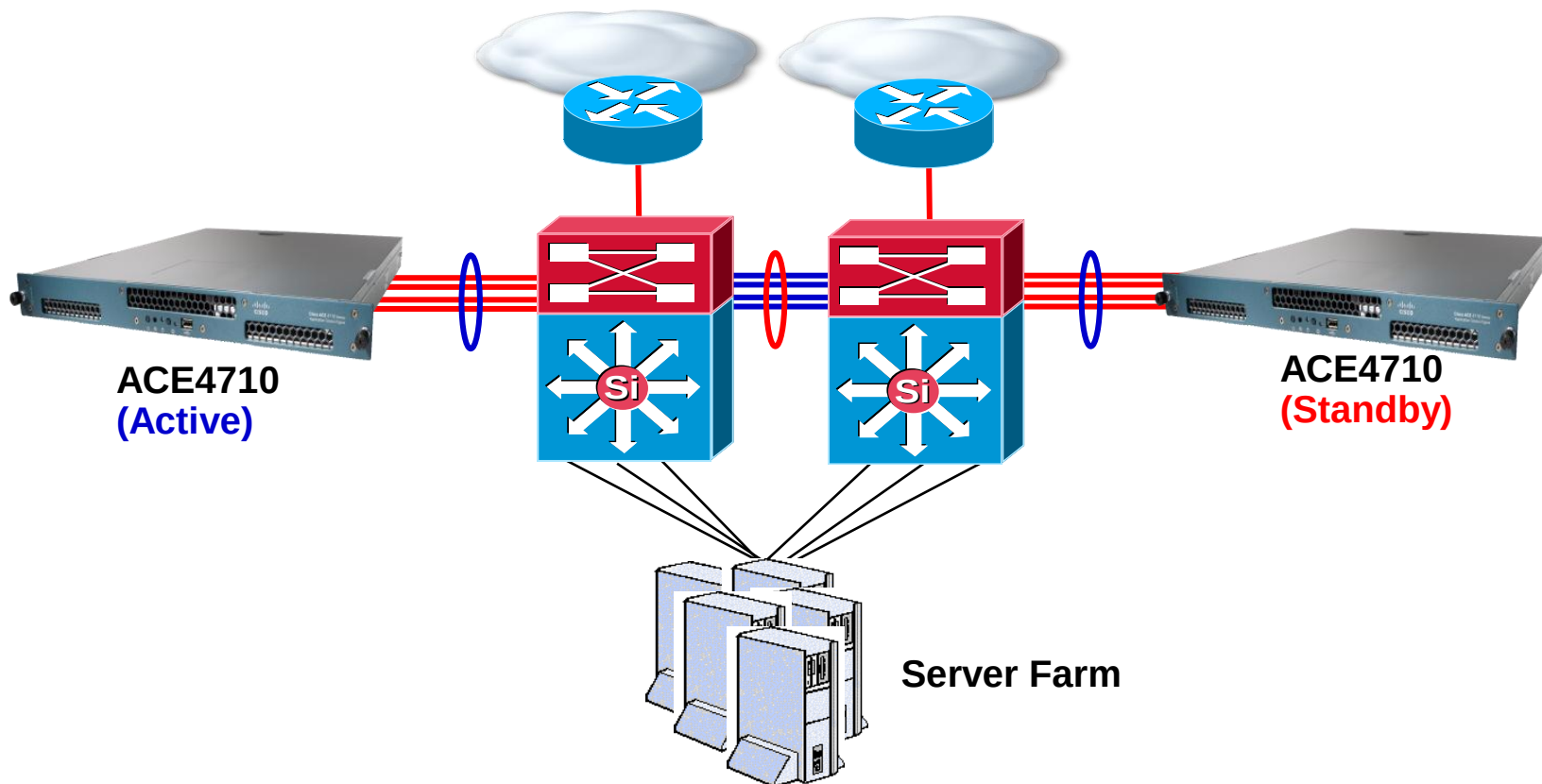
- 백본 또는 Server Farm용 스위치에 One Arm 형태 구성
- 네트워크 구성이 보다 간단하게 구성 될 수 있음.
- ACE Module을 사용하는 것과 동일한 구성/효과



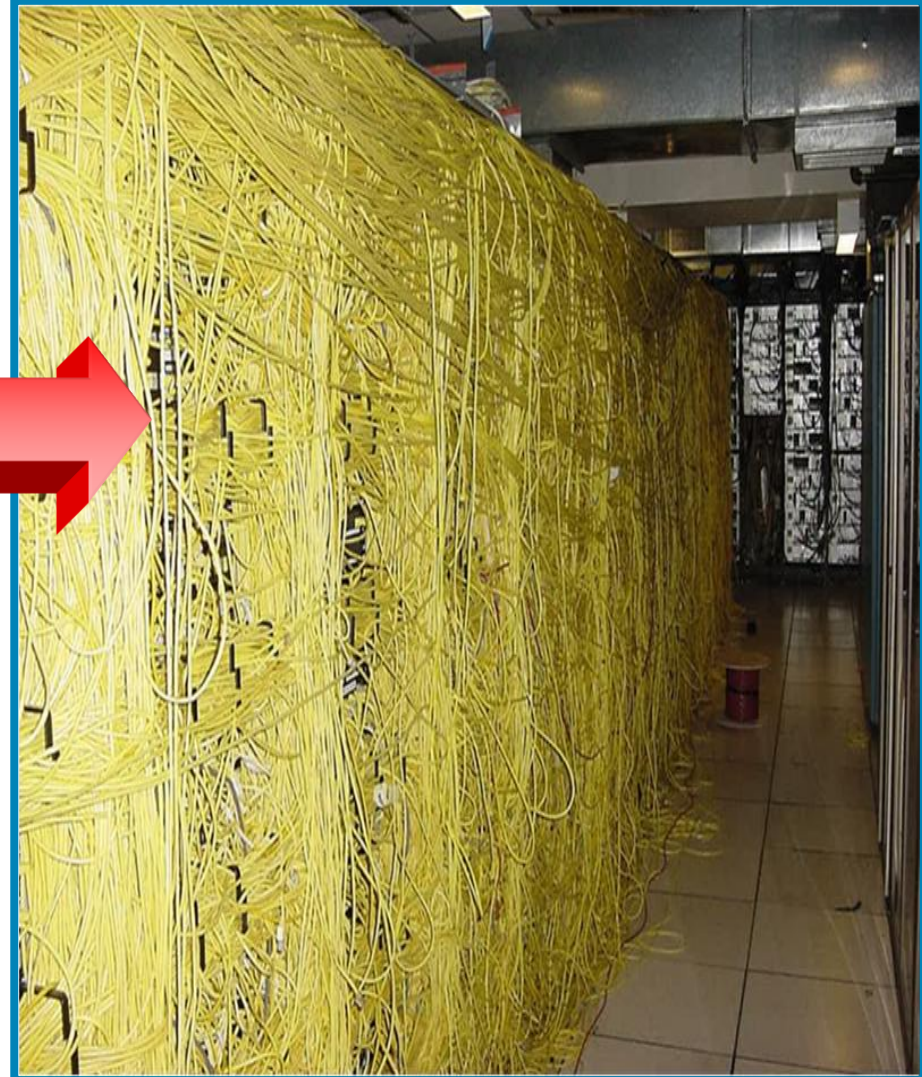
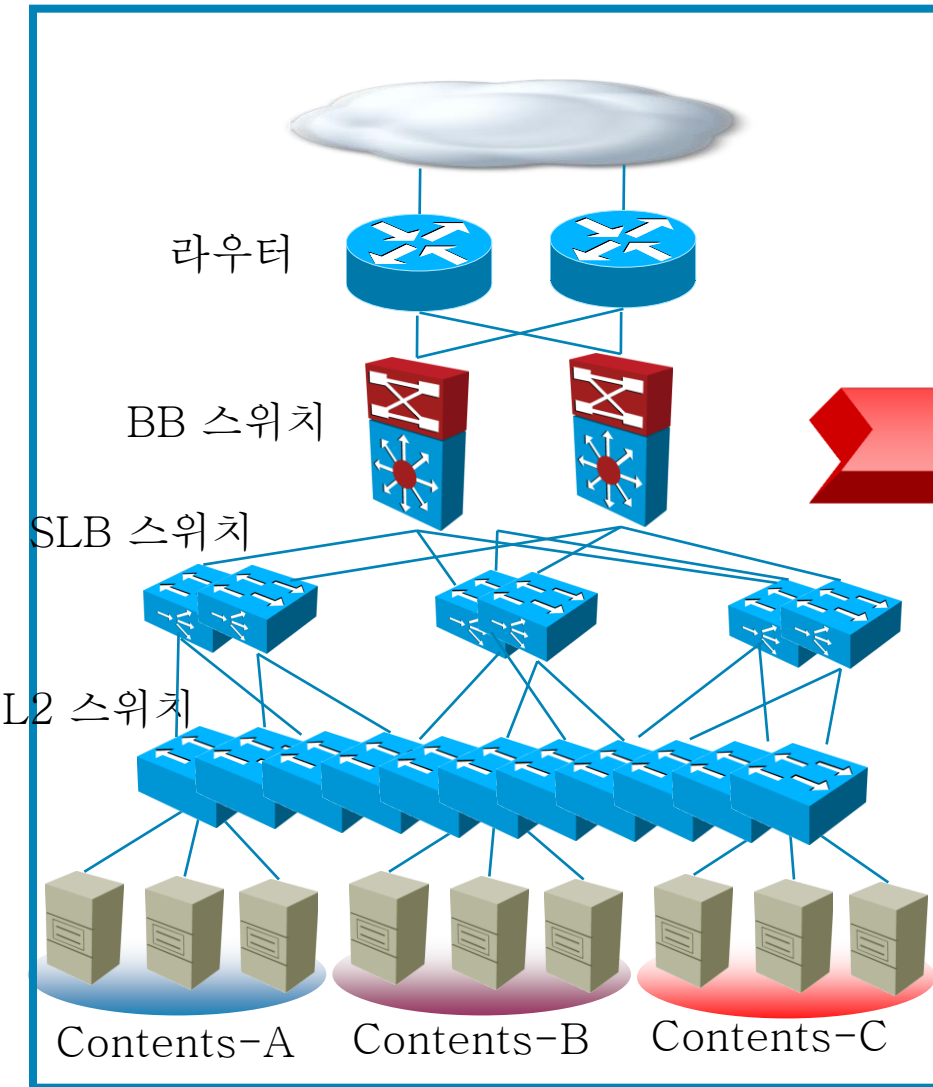
ACE4710 으로 ACE Module 구성을 그대로

- HA 구성

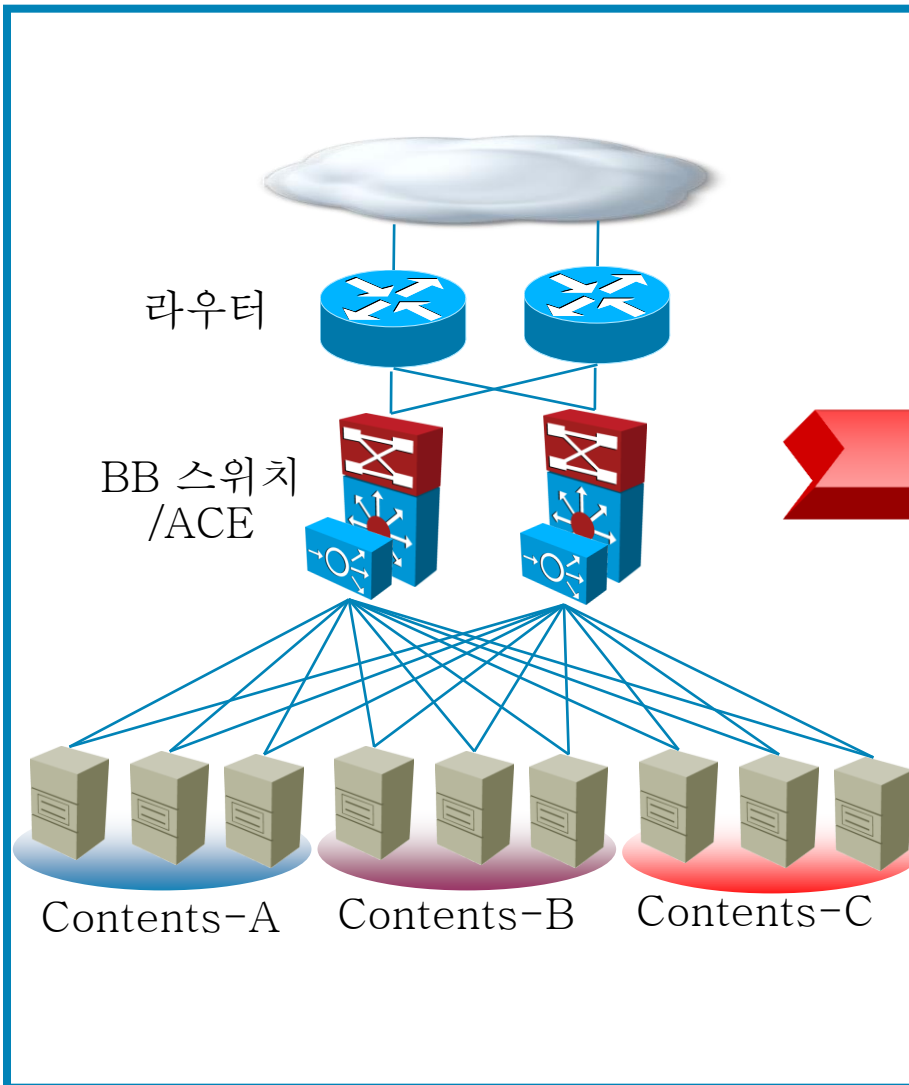
- 백본 또는 Server Farm용 스위치에 One Arm 형태 구성
- 네트워크 구성이 보다 간단하게 구성 될 수 있음.
- ACE Module을 사용하는 것과 동일한 구성/효과



일반적인 L4 구성의 경우

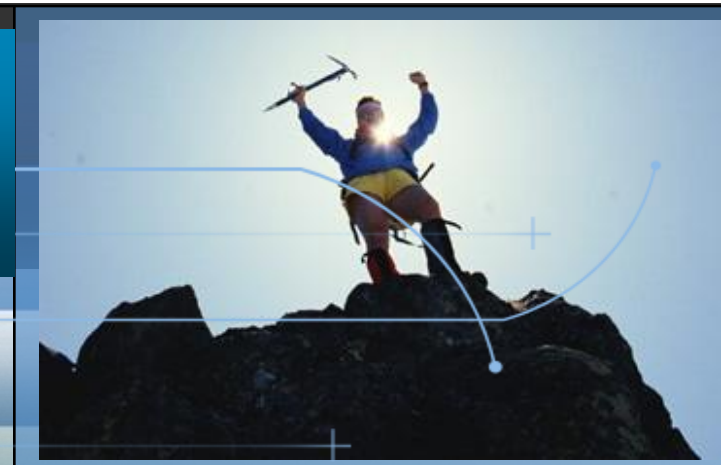


ACE를 이용한 구성 시



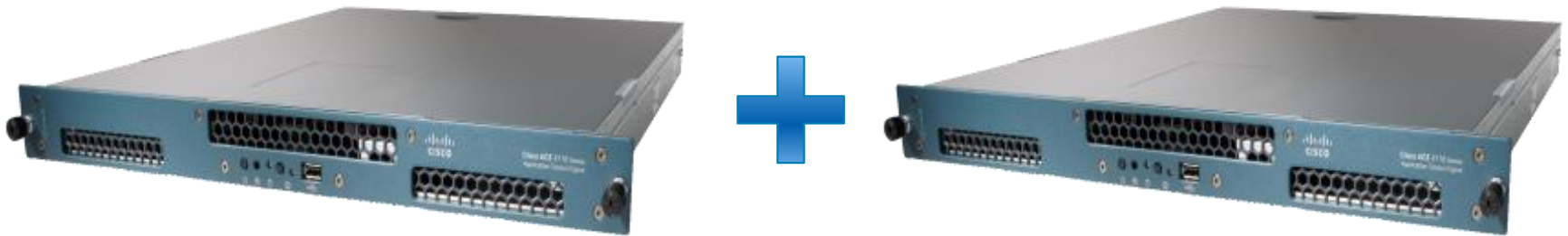


누구와 경쟁 할 것인가?



1~2G 시장에서의 경쟁

ACE4710 2PAK Bundle



**이중화 구성(HA)을 기본 적으로 할 때.
2PAK의 경우 경쟁력 있음.**



Nortel 2216/2424E



PIOLINK 4009/4509



Big-IP 3400/6400

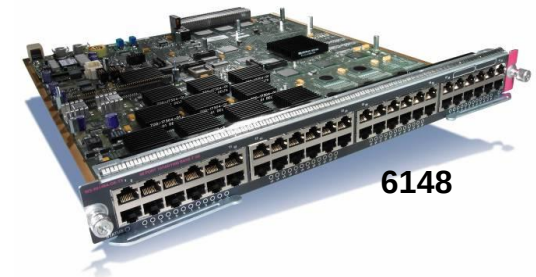
3~4G 시장에서의 경쟁 **C6504** 번들



SUP720



ACE Module



6148

720G Backplane, ACE 4Gbps, 48Port Line Card
그리고 여분 Slot 까지
(10G 필요한가?, FWSM을 꽂을까?)



Nortel 3408E



PIOLINK 5016/8016



Big-IP 8400/8800

10G 또는 그 이상에서의 경쟁

**C6504 번들 Upgrade
또는 6509 8G 번들
또는 다양한 조합**



720G Backplane, ACE 4~16Gbps 에 다양한 Line card 와 Service Module 조합



Nortel VSS5000



PIOLINK 10020

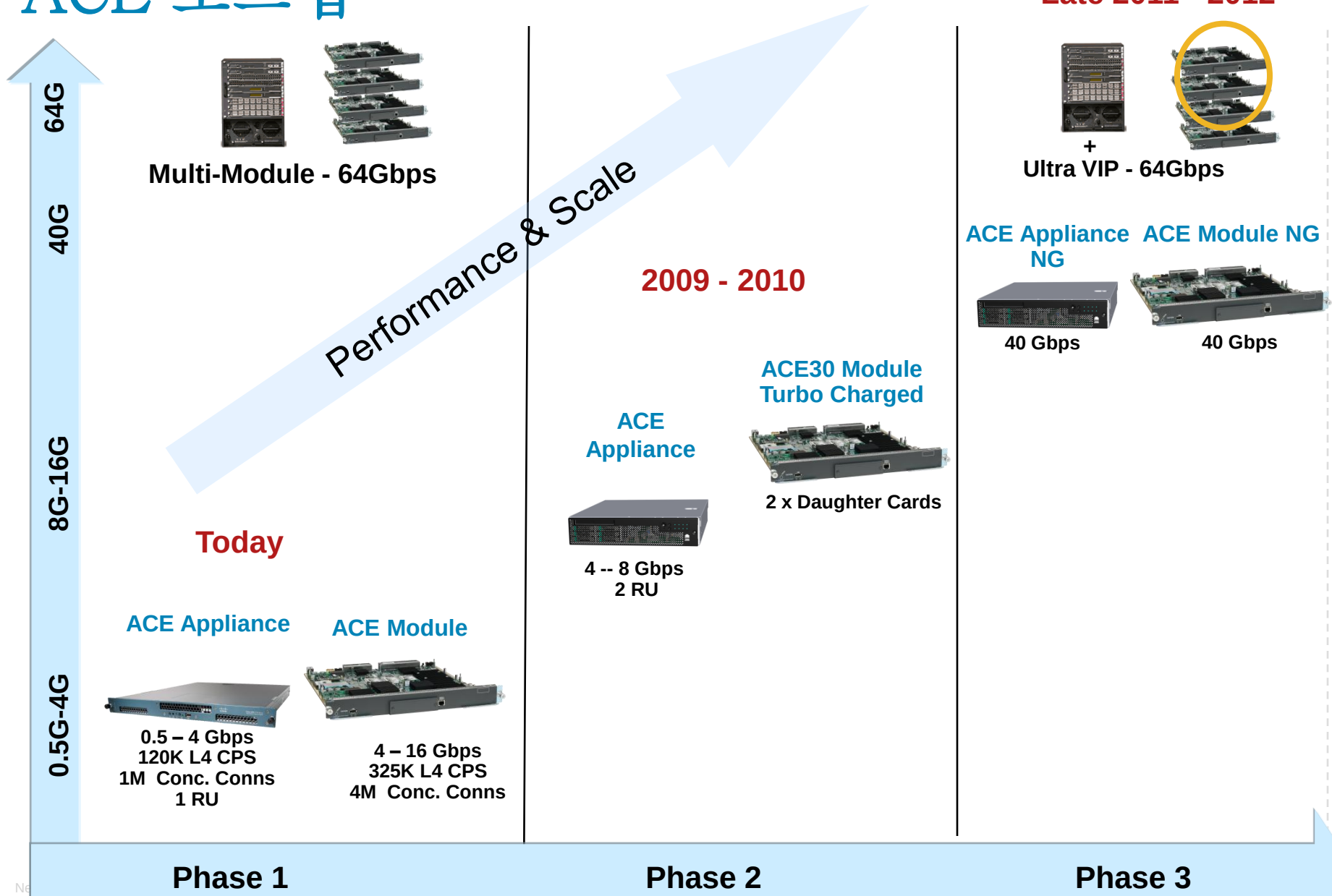


**Big-IP 8800
& Viprion**

ACE는 어떻게 진화 할까?

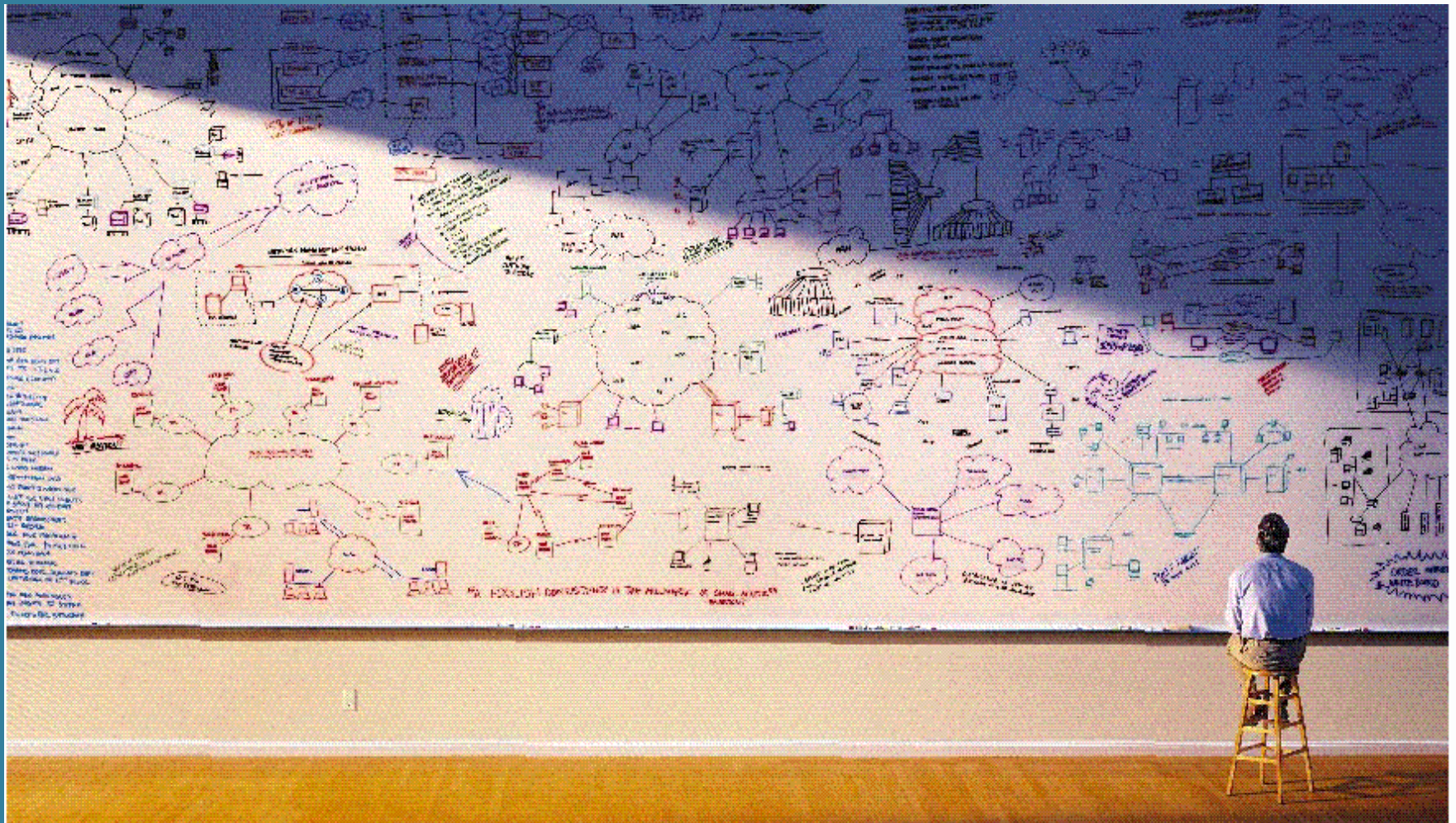


ACE 로드맵





Q&A





CISCO