



Cisco *START!*
Strategic Transformation
Revolutionary Technology 2008

SP 데이터 센터 설계 방안

2008년 3월 11일

김재한 / jaehakim@cisco.com

Cisco Korea



목차

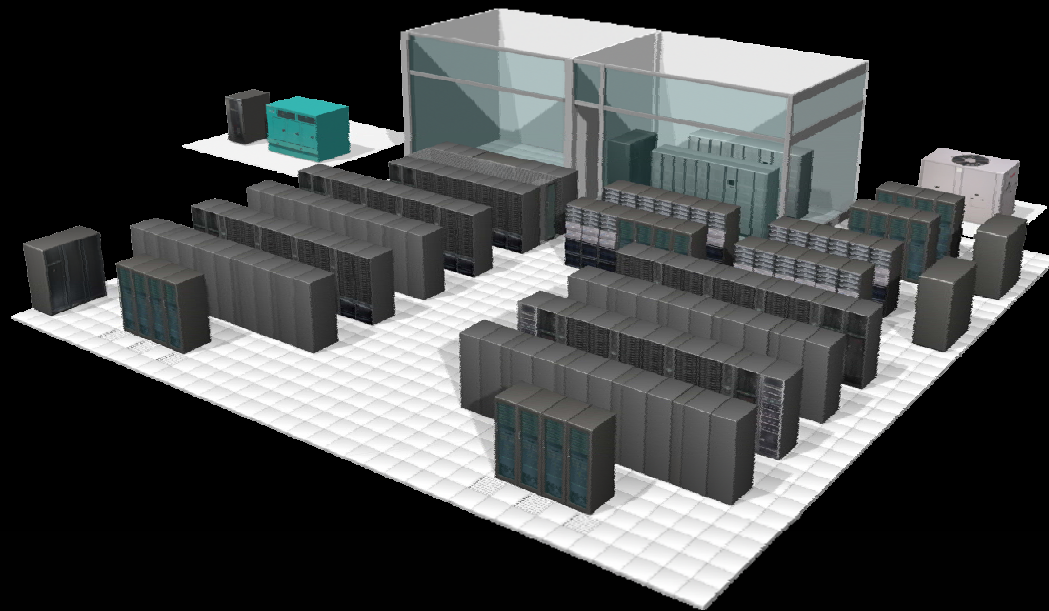
- SP 데이터 센터의 특징
- SP 데이터 센터 구현 시 고려 사항
 - 확장성
 - 고가용성
 - 가상화를 통한 유연성
- 시스코 SP 데이터 센터 비전 및 전략

SP 데이터 센터의 특징

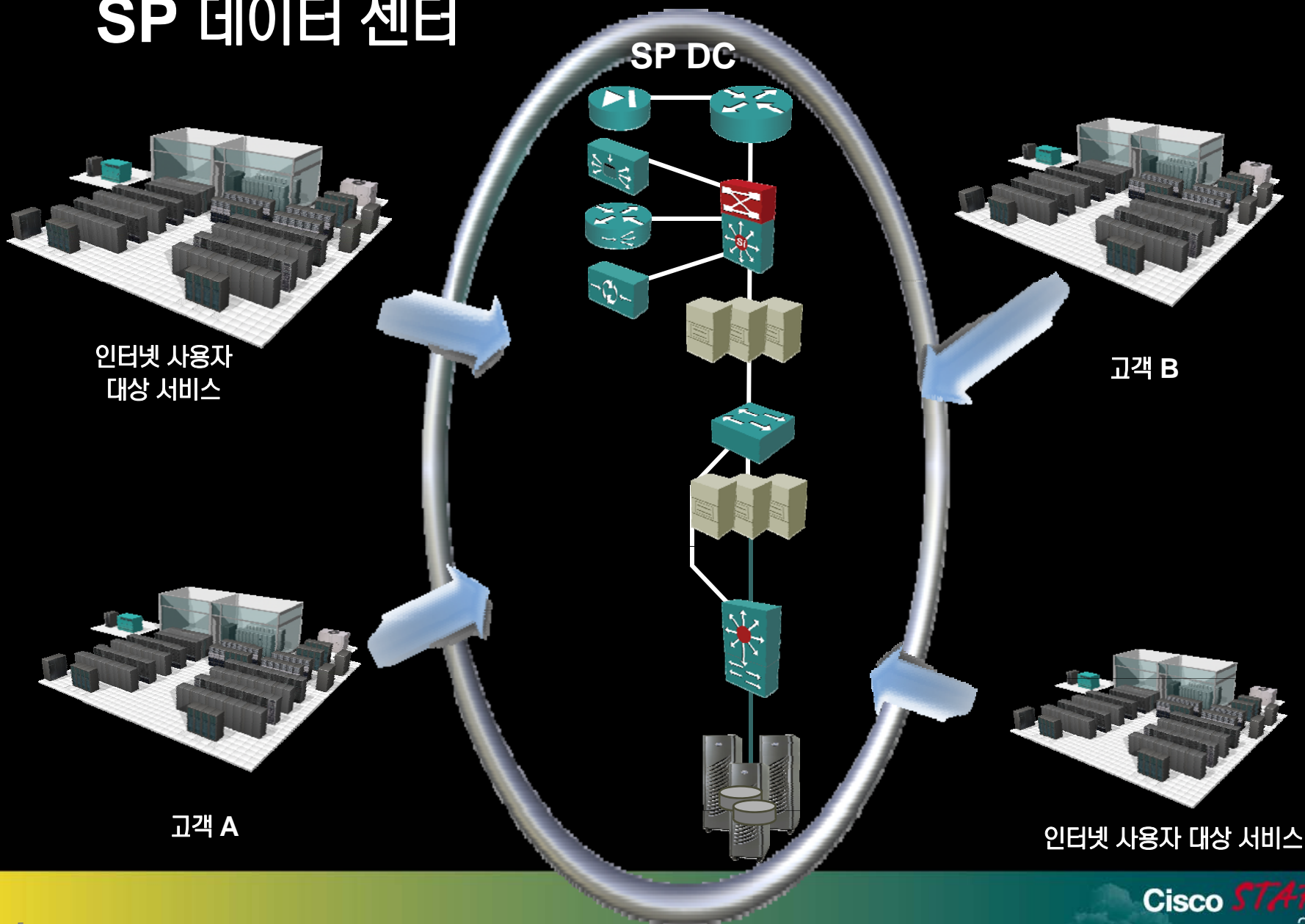


데이터 센터란 ?

- 전력, 온도 등의 환경의 제어가 가능하며, 중요한 컴퓨팅 자원을 가지고 있는 공간
- 중앙 집중형 관리 체계
- 비즈니스 요구 사항을 지원



SP 데이터 센터



기업 데이터 센터 vs SP 데이터 센터

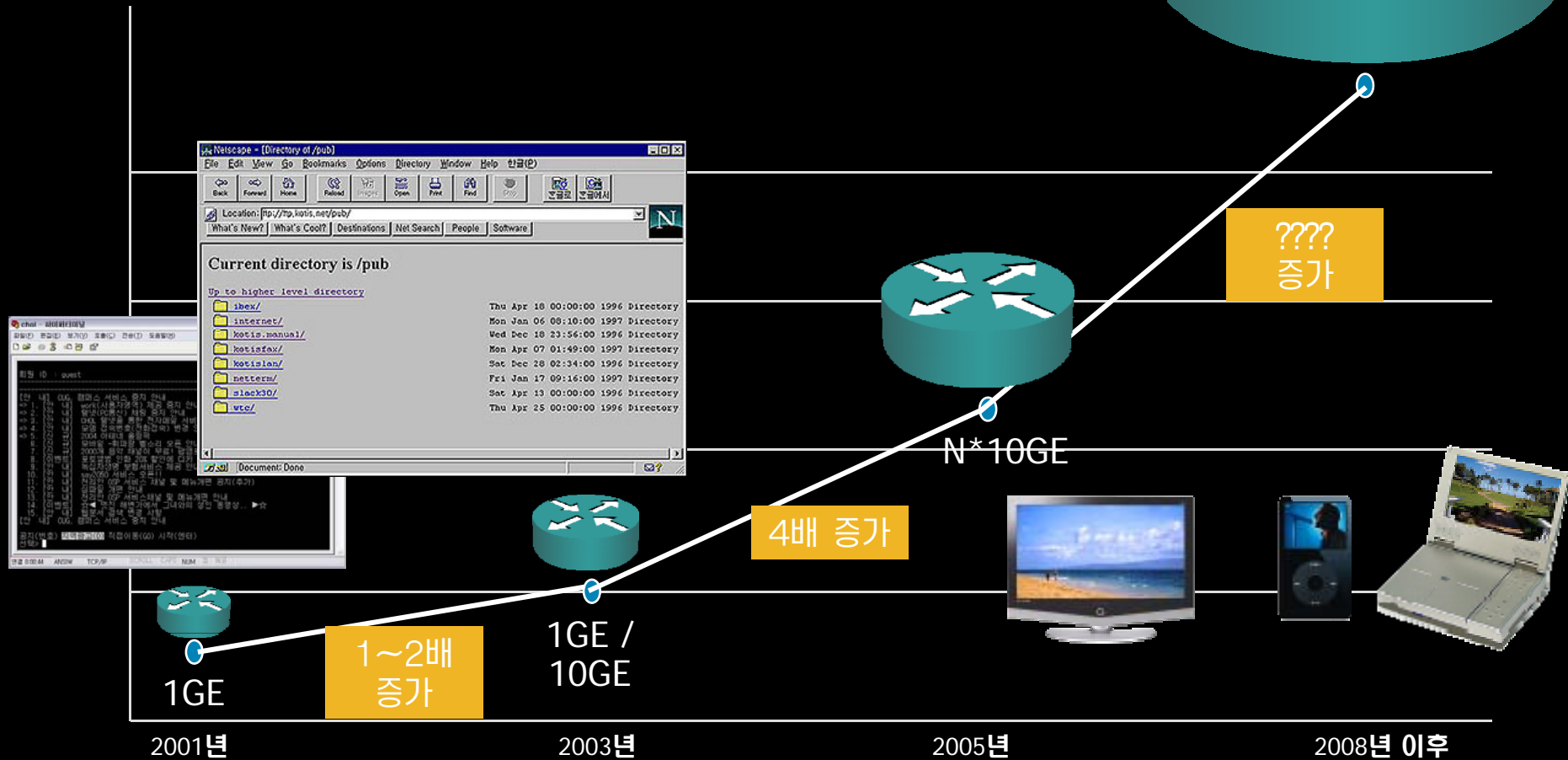
■ 데이터 센터 유형별 비교

기업 데이터 센터		VS	SP 데이터 센터
네트워크 형태	폐쇄형	VS	보안성
가입자 형태	자사 고객 대상	VS	고 가용성
트래픽 양 및 증가율	적음	VS	확장성
Biz 형태	Biz 연속성, 생산성	VS	유연성 (가상화)

SP 데이터 센터 구현 시 고려 사항 - 확장성



SP DC Traffic History



확장성

2007 Uplinks

N * 10 GbE

N * 10 GbE

N * GE/10 GbE

GbE/10GbE

FE / GE



2008+ Uplinks

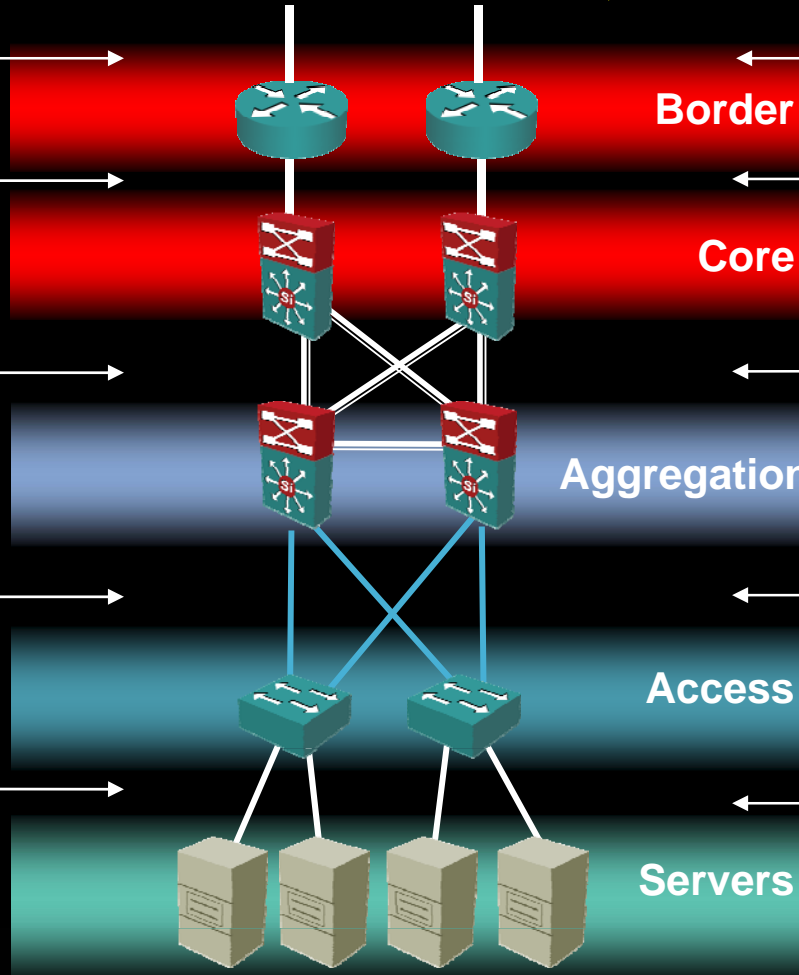
???

???

N*10GE/???

10GE/ ???

GE/10GE



확장성

- **IEEE HSSG (High Speed Study Group)**

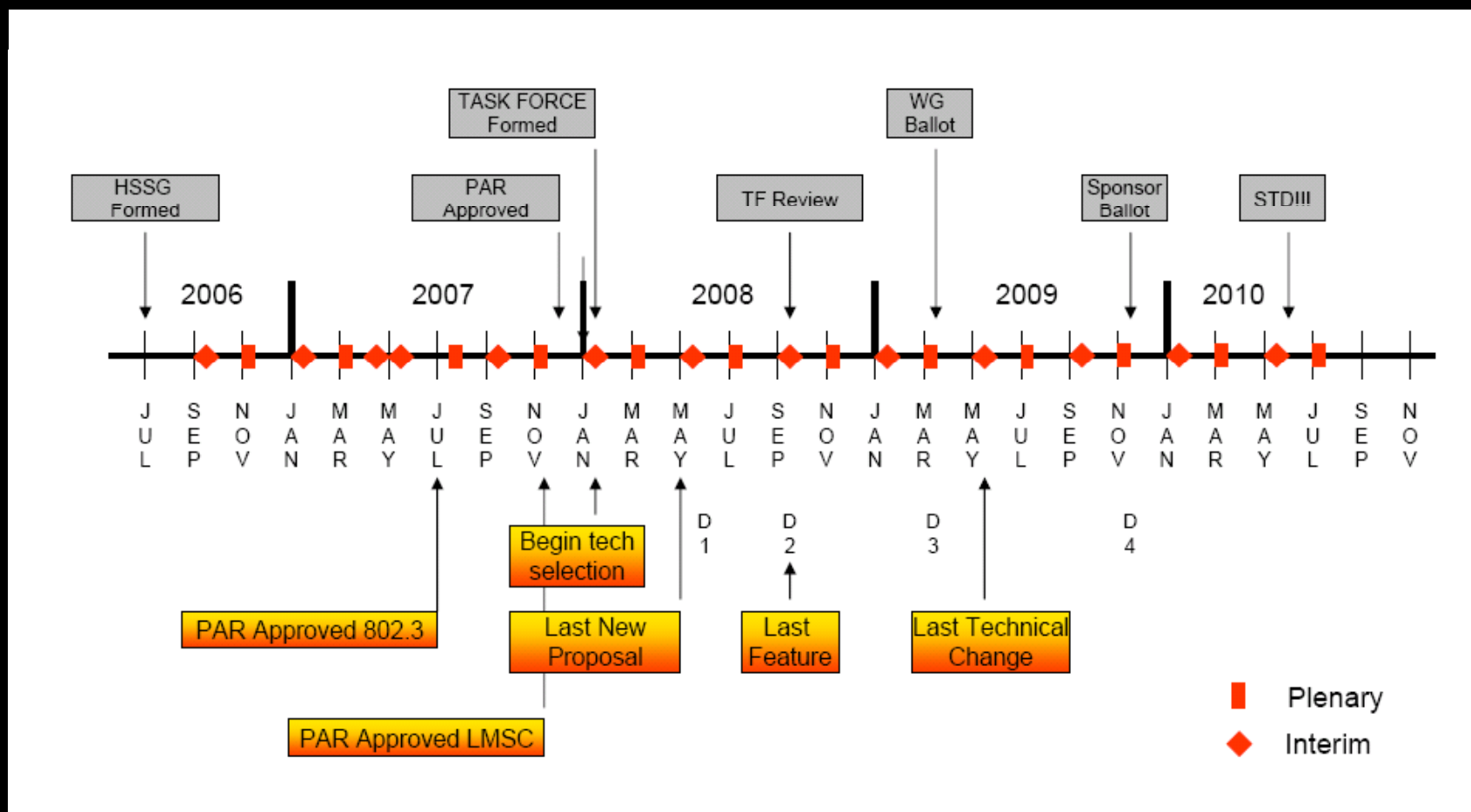
- 현재는 100Gbps / 40Gbps 이더넷에 대한 연구를 진행 중

- **HSSG의 목표는 아래와 같음 (일부 생략)**

- Support full-duplex operation only
- Preserve the 802.3 / Ethernet frame format
- Preserve Min/Max Frame Size of current 802.3 Std
- Provide Physical Layer spec which support 40 Gb/s operation
- Provide Physical Layer spec which support 100 Gb/s operation

확장성

- 차세대 이더넷 속도 표준화 타임 라인



http://grouper.ieee.org/groups/802/3/hssg/public/sept07/tutorial_01_0907.pdf

확장성

■ WAN 구간

- 제한적인 광 코어
- ECMP의 한계 및 LAG의 한계성
- WAN 구간은 2008년 이후에는 40G PoS
- 2010년 이후에는 40GE/100GE 이더넷 고려 가능

■ LAN 구간

- 각 계위에 맞는 확장성 고려
- Core : 40GE/100GE
- Aggregation : 10GE / 40GE
- Access : 1GE/10GE

확장성 *Fibre Channel Over Ethernet*

- T11.3 워킹 그룹에서 표준화 작업 중

FC-BB-5 WG: Defining the FCoE model and Encapsulation

- 표준화 작업 내용

- Support I/O over Ethernet Networks by defining a mapping of FC over Ethernet.
- Mapping to provide benefits beyond those related to FCIP and iSCSI as it provides a direct mapping to Ethernet (not IP or TCP), and compatibility with storage drivers and management tools
- Current efforts include frame format, addressing, forwarding, N-port Virtualization, etc.

확장성

■ Cisco 솔루션



CRS-1

- 40G PoS 이미 지원 중
- 100GE Capable



Nexus

- 32 port 10GE Now Available
- **100GE Capable (230Gbps per slot)**
- Fiber Channel over Ethernet 지원 예정



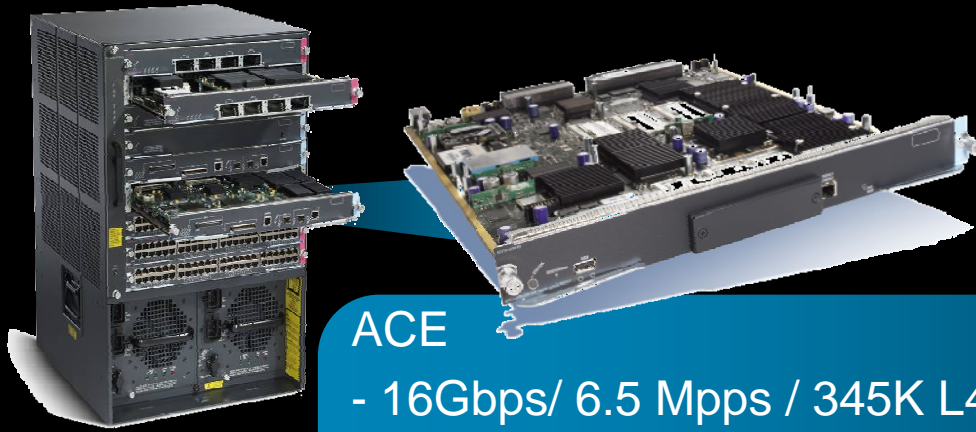
Catalyst 6500

- 10GE Already Available
- 40GE Capable (현 SUP 기준)

Catalyst 4900M

- 10/100/1000 & 1GE & 10GE Already Available

확장성



ACE

- 16Gbps/ 6.5 Mpps / 345K L4 CPS/ 동시 접속 4M Session
- Chassis 당 최대 4장 까지 추가
- 4000개 Vlan 제공 , 256K ACL , 1M NAT 성능 제공
- 최대 250 개 Virtual Context

FWSM

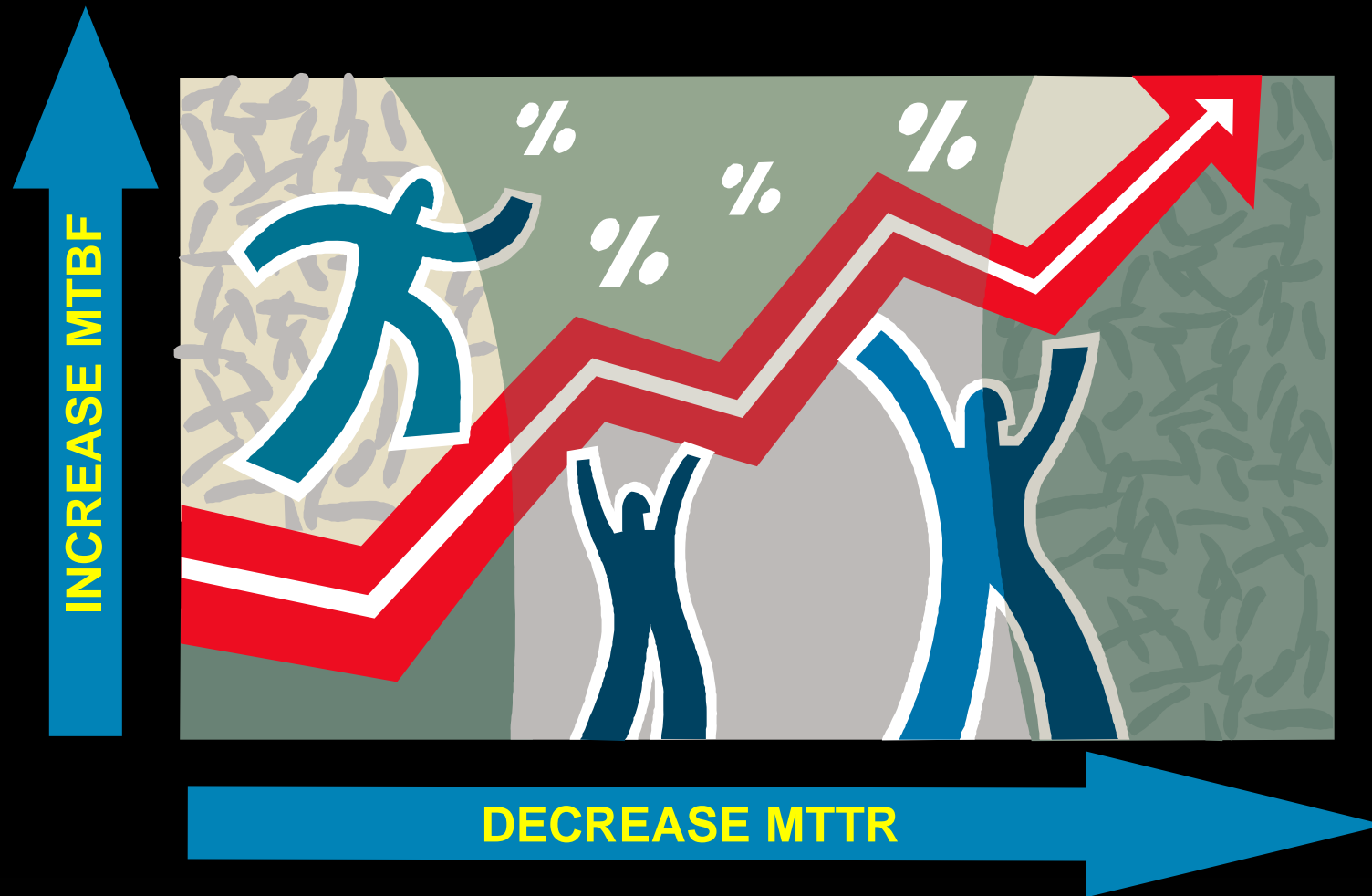
- 최대 40G 제공
- 1K개 VLAN , 80K ACL , 256 NAT/PAT 성능 제공
- 최대 256 개 Virtual Firewall

SP 데이터 센터 구현 시 고려 사항 - 고가용성



가용성이란?

- MTBF와 MTTR의 혼합 된 기능



고가용성이란?

Availability	DPM	Downtime Per Year (24x365)		
99.000%	10000	3 Days	15 Hours	36 Minutes
99.500%	5000	1 Day	19 Hours	48 Minutes
99.900%	1000		8 Hours	46 Minutes
99.950%	500		4 Hours	23 Minutes
99.990%	100			53 Minutes
99.999%	10			5 Minutes
99.9999%	1			30 Seconds

“High Availability”

Downtime 의 원인 분석

- 네트워크 및 소프트웨어 어플리케이션 (60%)

- 하드웨어 장애

- 소프트웨어 장애

- 링크 장애

- 전력 및 그 밖의 환경 문제

- 자원 이용 문제

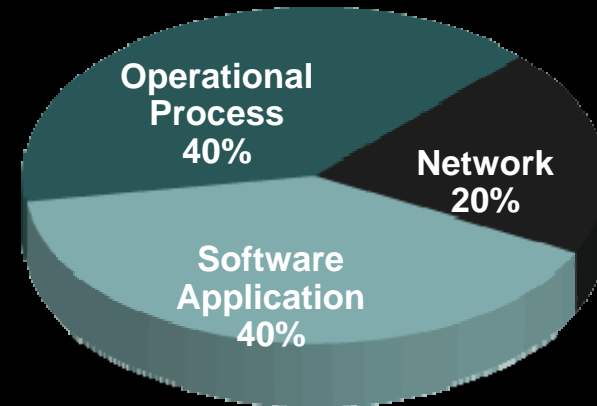
- 운영 프로세서 상의 문제 (40%)

- 네트워크 디자인 문제

- 하드웨어 및 소프트웨어 구성에 관한 표준화의
결여

- 장애 관리 및 계획에 대한 프로세스 미 정립

- 교육의 결여



Sources of Network Downtime *

*Source: Gartner Group

HA를 위한 기술 검토

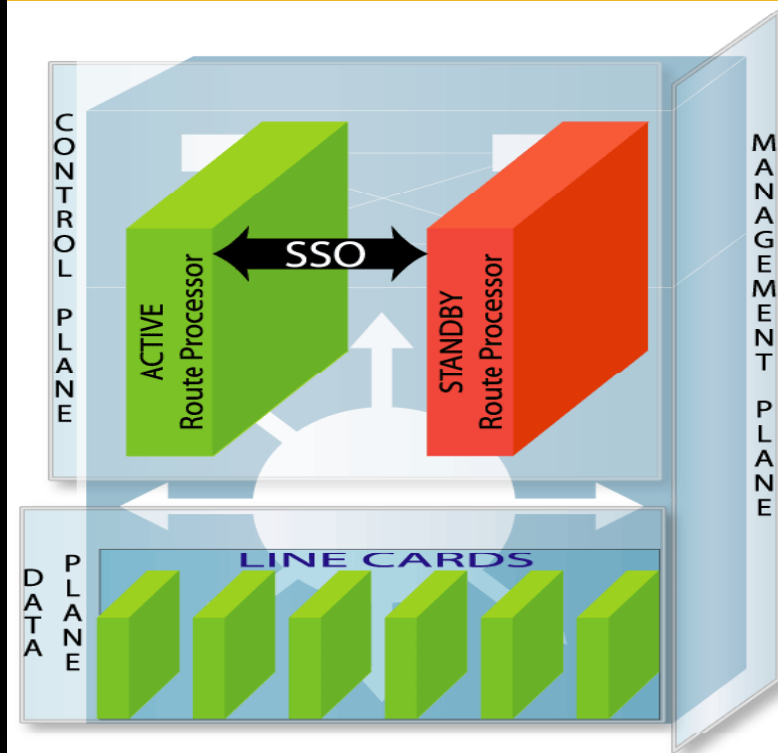
- 시스템 레벨의 가용성 향상
- 네트워크 레벨의 가용성 향상
- 보안성 향상

고가용성 향상

- 시스템 레벨의 고가용성

- Hardware Architecture
제어부와 데이터부의 분리
- 상태 보존형 Switchover
- Non-Stop Forwarding (NSF)
- Modular Software Architecture
- In-Service Software Upgrade (ISSU)
- Non-Stop Routing (NSR)

System Resiliency Features Protect Against Any Node- Related Failure

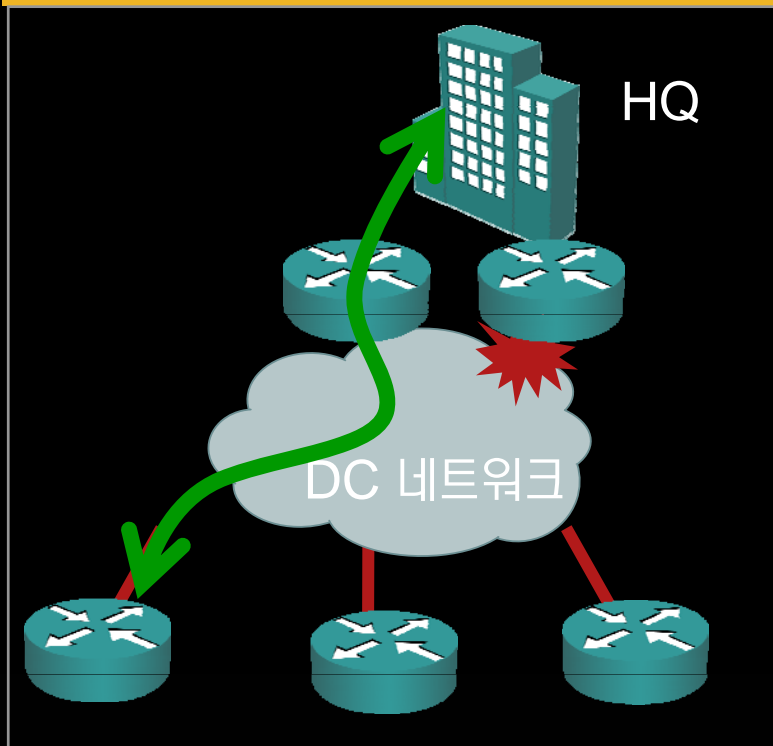


고가용성 향상

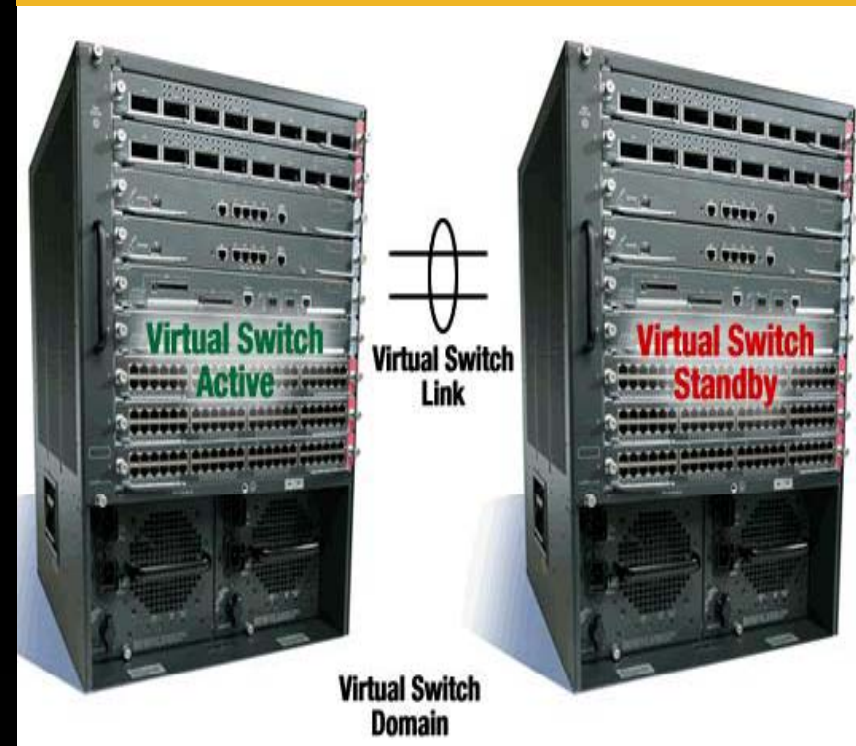
- 네트워크 레벨의 고가용성

- IGP Fast Convergence
- VSS Technology

IGP Fast Convergence – 신속한 우회



VSS – STP 제거 등의 가용성 향상



고가용성 향상

- 보안성

- 망이 개방 되어 있으므로 언제나 DDoS 등의 공격의 대상이 될 수 있을 뿐 아니라, 중요 Application (예 : IPTV) 도 포함 가능
- SP DC는 Managed Security 서비스 뿐 아니라, SP DC 망 자체의 안정성 향상 및 네트워크 자원의 효율적 이용을 위해 보안성을 향상 시켜야 함
 - 공격의 자동 발견 및 차단
 - 정책 적용 시의 서비스 지속성
 - 어플리케이션 계층 보안 적용 기술
 - 비디오 서비스 보안

고가용성 향상

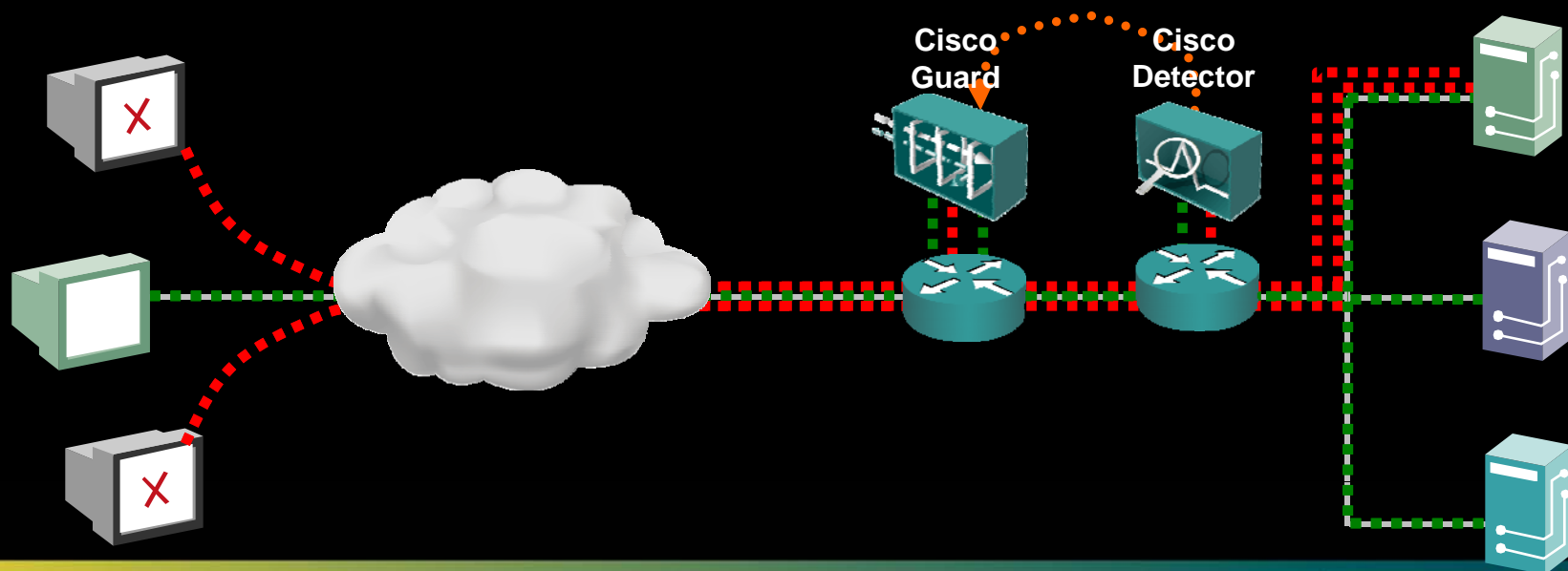
- 보안성 : 공격의 자동 발견 및 차단

공격에 대한 탐지 및 경감 기능 제공

Attack Flow 만을 제어 – Service 중단 없음

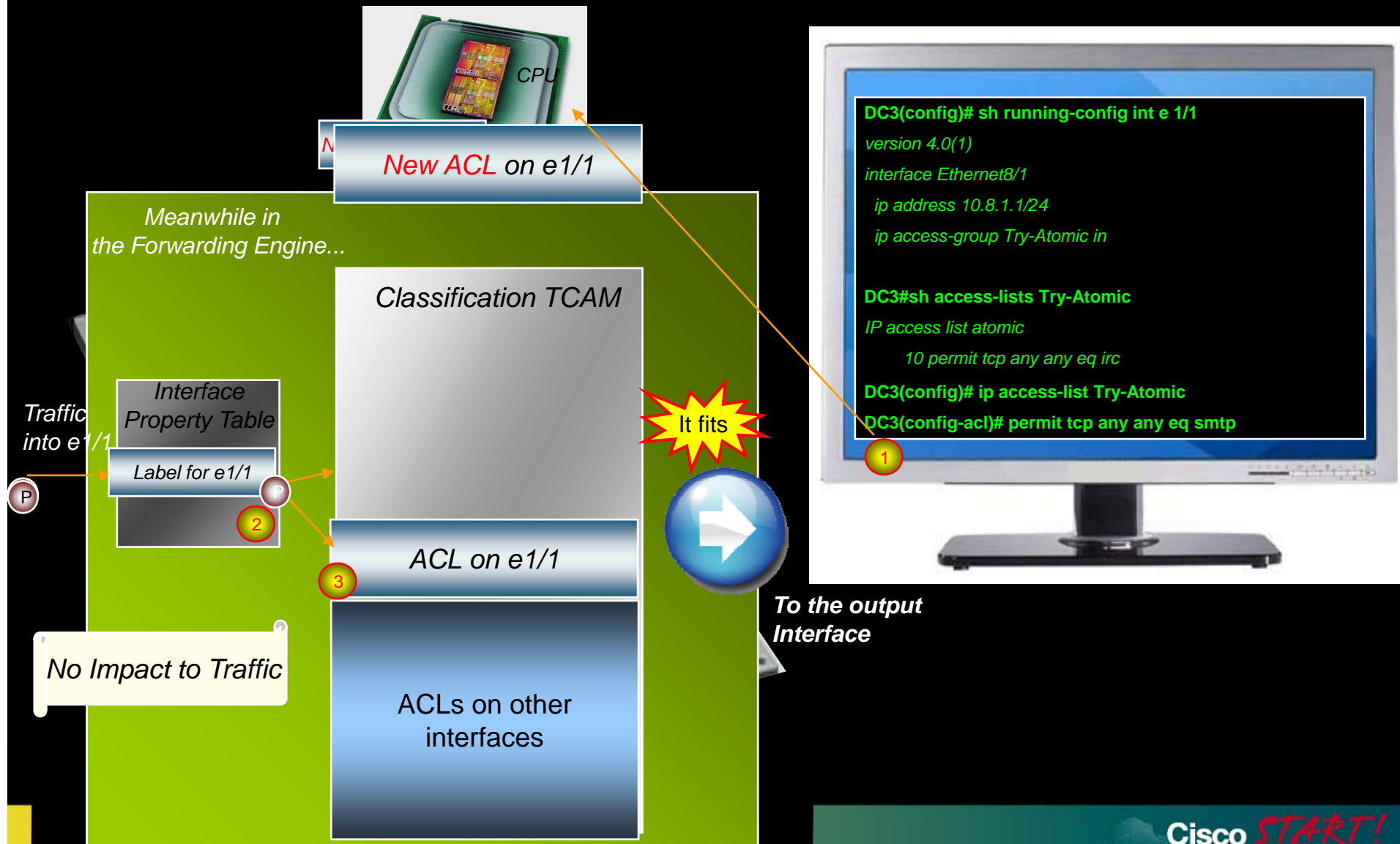
대규모 망에서 갑작스런 공격이나 대규모 공격에 강력한 제어

디자인 확장성이 높고, 외부로부터의 다양한 공격에 솔루션 제공



고가용성 향상

- 보안성 : 보안 정책의 지속성

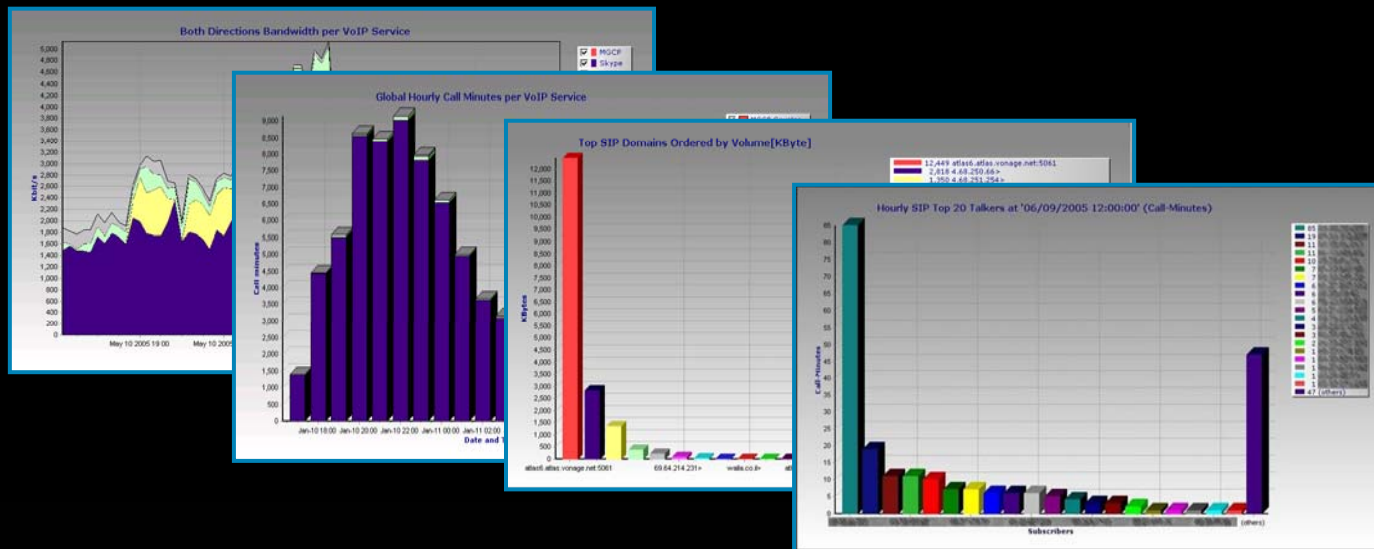


고가용성 향상

- 보안성 : 어플리케이션 계층의 보안성

- Deep Packet Inspection (DPI) 을 통한 어플리케이션 계층의 제어 및 보안성 강화 이를 통한 고객 만족도 증가 가능

- Application 별 차등화 서비스 제공
- Time-Based 서비스
- Application 제어 서비스



고가용성 향상

- 보안성 : 비디오 보안

데이터 계층

- Detects traffic anomalies & respond to attacks in real-time
- Technologies: NetFlow, IP source tracker, ACLs, uRPF, QoS tools

제어 계층

- Defense-in-depth protection for routing control plane
- Technologies: Receive ACLs, control plane policing, neighbor authentication, BGP best practices

관리 계층

- Secure and continuous management of Cisco IOS network infrastructure
- Technologies: CPU & memory thresholding, dual export syslog, image verification, SSHv2, SNMPv3, security audit, CLI views

고가용성 향상

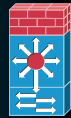
- 보안성 : 데이터 센터 내의 비디오 보안

10GE/MPLS/IP Connectivity

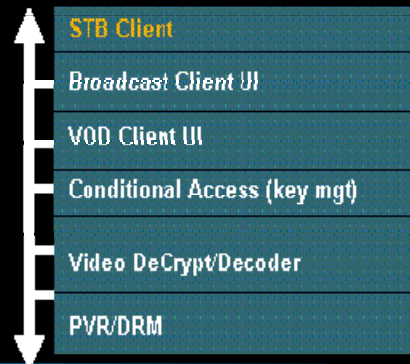
ACE 250 Virtual Contexts

ACE Resource Mgt per Context

Active/Active High Availability



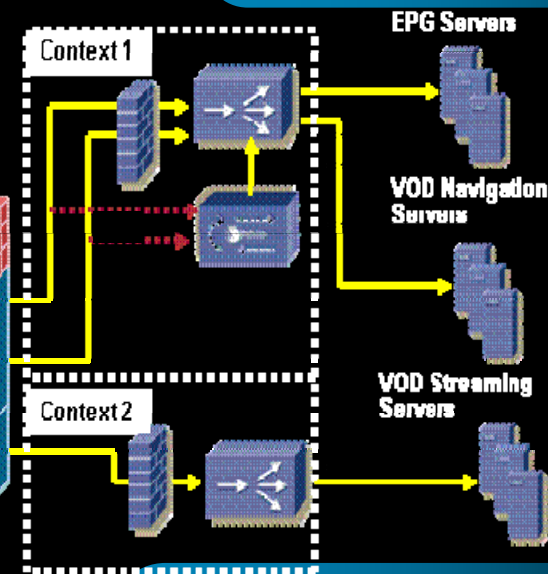
Middleware / VOD
Services



L2-L7 Load Balancing

HTTP/RTSP Application Load
Balancing

ServerFarm Failover



SSL 3.0 TLS 1.0

AES, RC4, 3DES ciphers

RSA key / Digital Certs



ACLs w/ Logging

TCP/IP Normalization

uRPF

NAT

Web Application Inspection



고가용성

■ Cisco 솔루션



CRS-1

- 전 컴포넌트 이중화 및 네트워크 계층의 고 가용성 지원
- 모듈화 소프트웨어 디자인을 통한 시스템 자체의 고가용성 향상



Nexus

- 전 컴포넌트 이중화 및 네트워크 계층의 고 가용성 지원
- 모듈화 소프트웨어 디자인
- Atomic ACL 을 통한 보안의 지속성

Catalyst 6500

- 전 컴포넌트 이중화 및 네트워크 계층의 고 가용성 지원
- 모듈화 소프트웨어 디자인 (SXH)
- Guard & Detector 기능을 통한 자동 방어 기능

SCE

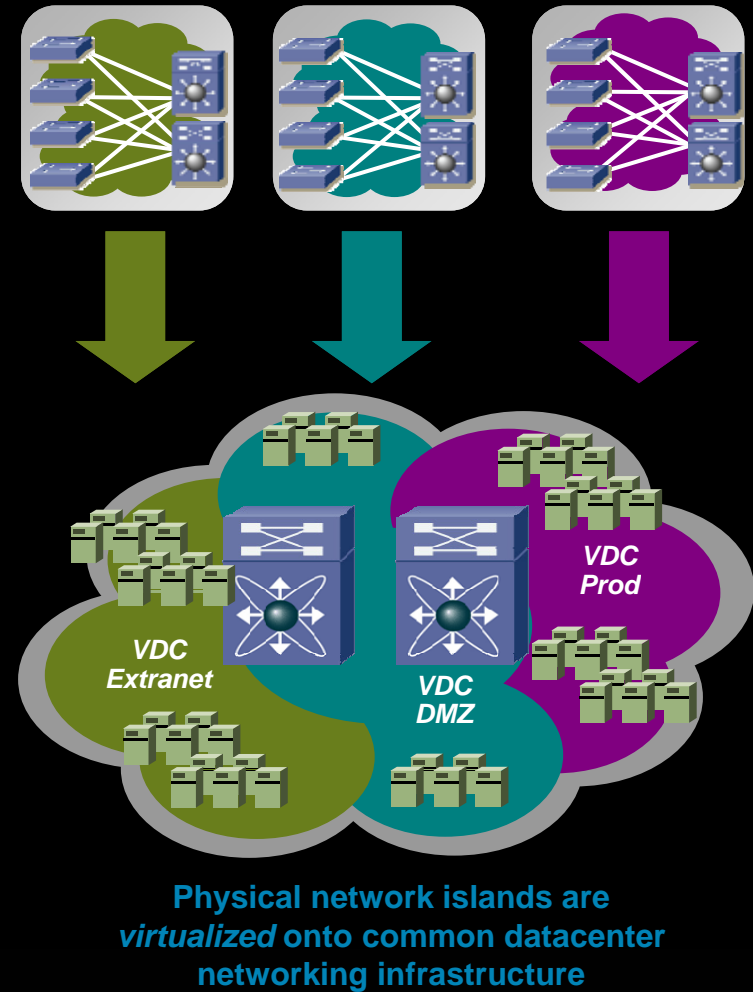
- DPI를 통한 Application 별 제어 서비스

SP 데이터 센터 구현 시 고려 사항 - 가상화를 통한 유연성



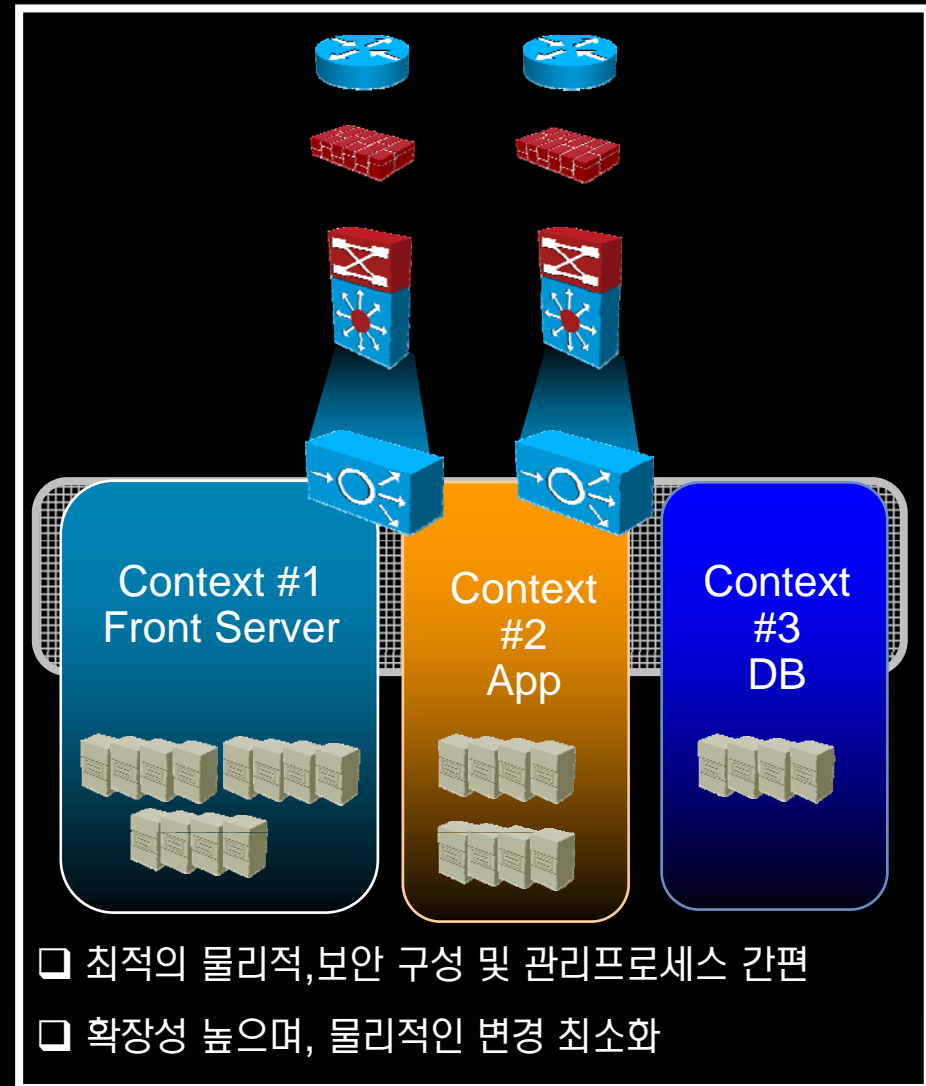
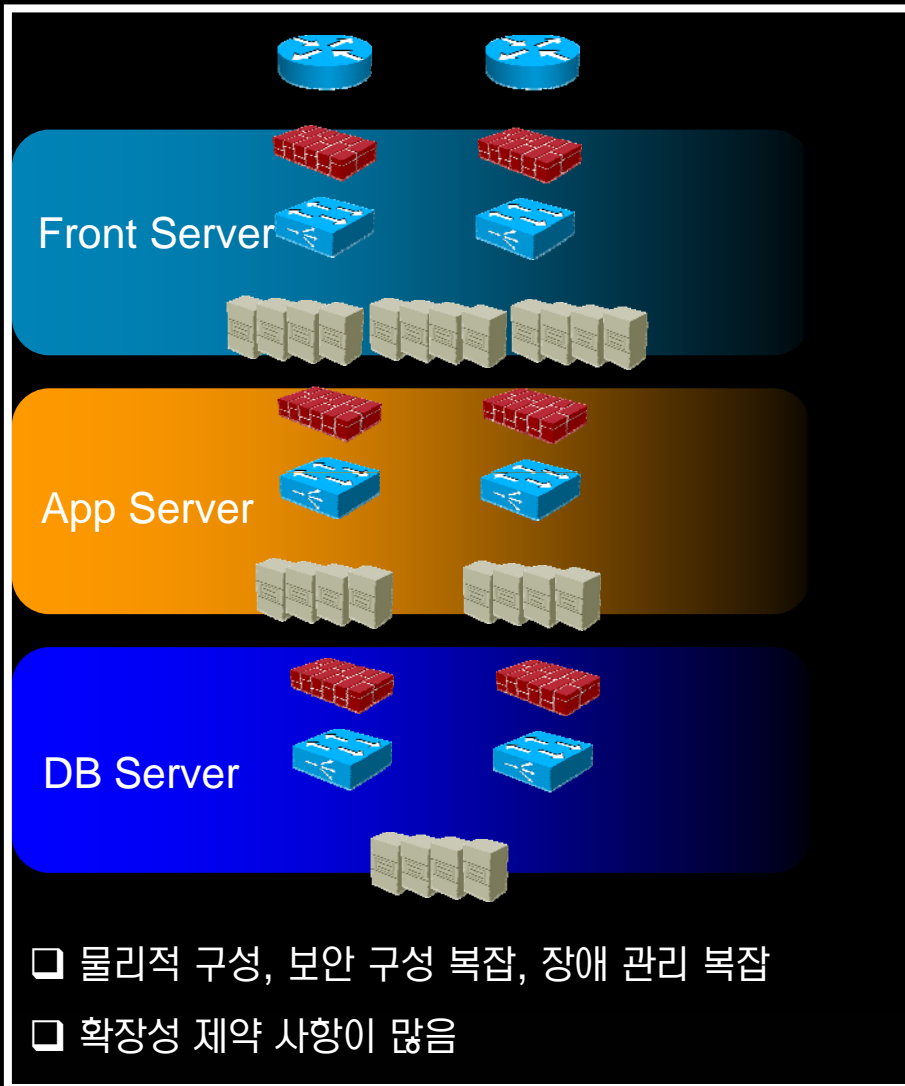
가상화

- 전통적 구성은 공간, 전력 등의 물리적 한계에 도달할 경우 신속한 서비스 제공 및 구성 변경 등의 유연성을 제공하지 못함
- 가상화는 물리적 인프라를 논리적 인프라로 변환하는 동시에 동일한 수준의 보안, 관리 등을 제공함으로써 서비스의 유연성 및 신속성을 확보
- SP DC의 가상화 서비스 예
 - 방화벽 서비스
 - 어플리케이션/고객 별 SLB 서비스
 - 스토리지 서비스 등



가상화

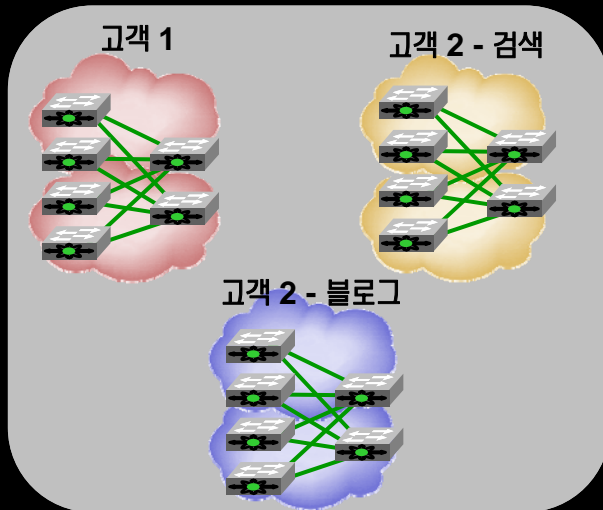
- Application 별 가상화를 통한 로드밸런싱 구현



가상화

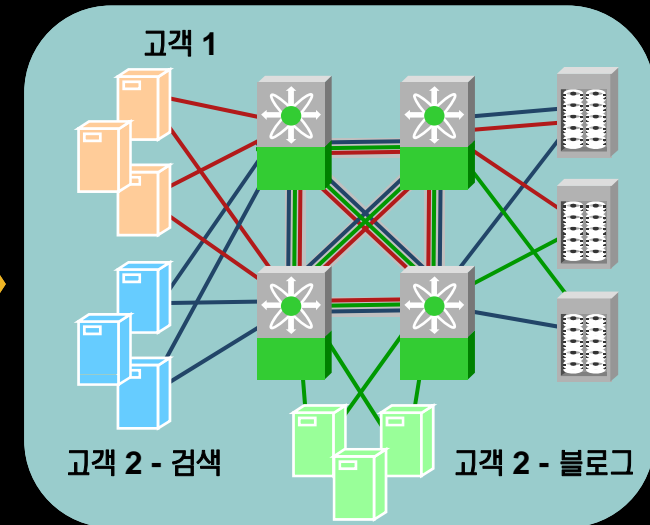
- 스토리지 가상화를 통한 고객별 신속한 서비스 적용

SAN Islands



논리적으로는 독립성을 유지하며
물리적인 SAN 스위치 인프라
공유

통합 가상화 패브릭

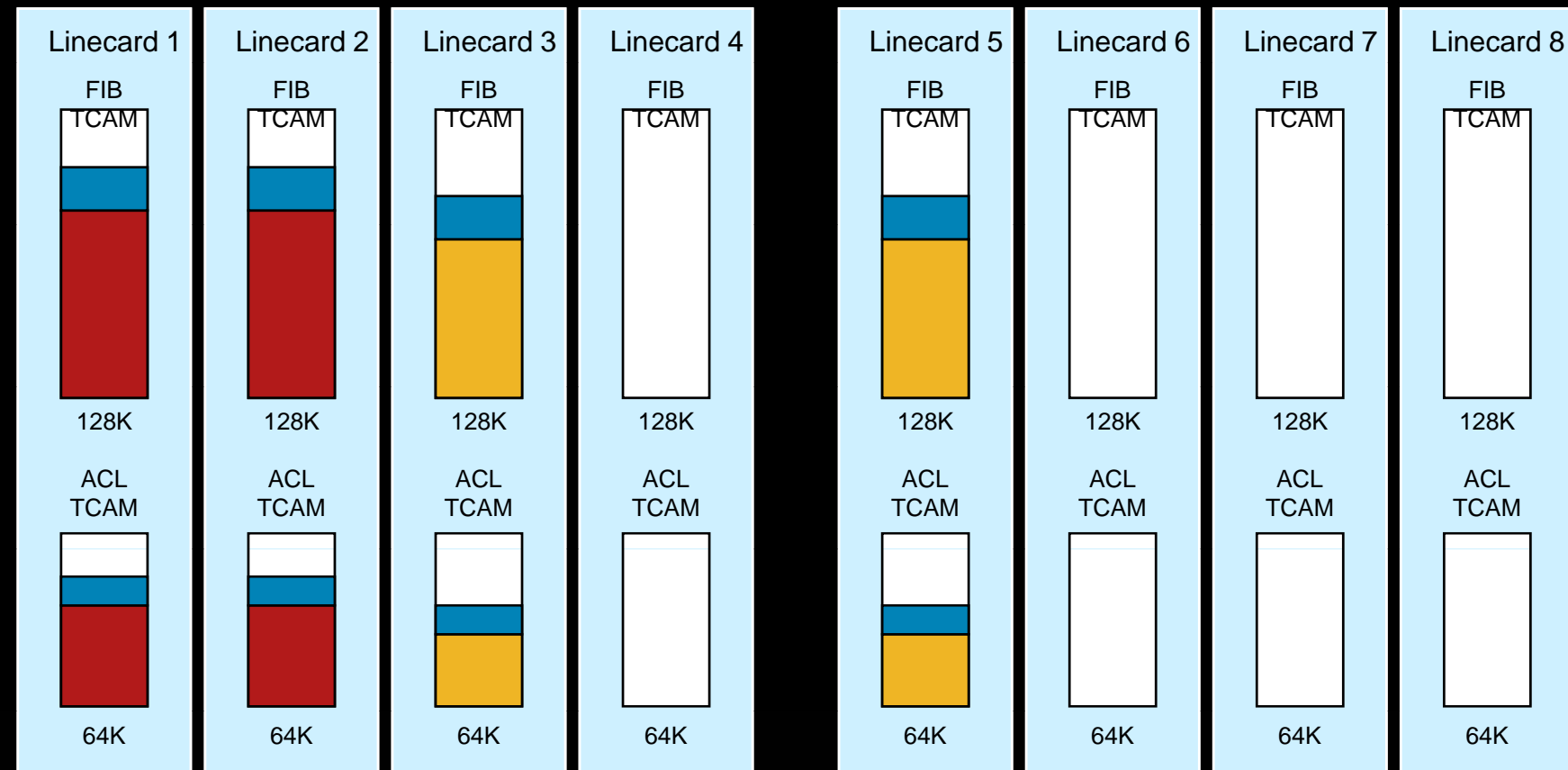


SAN Island 구조	Attribute	통합 가상 패브릭
많음	SAN 스위치 수	적음
불가능	디스크/테이프 장비 공유(ILM)	가능
불가능	DR 시설의 공유	가능
복잡함	SAN 관리성	단순
높음	전력, 공간 활용 등의 전체적인 TCO	낮음

가상화 예 : VDC를 통한 자원 활용 예

■ VDC 10
 ■ VDC 20
 ■ VDC 30

FIB과 TCAM의 자원 활용의
효율성이 극대화 됨



가상화

■ 가상화의 이점

- 자원 활용의 극대화 → Lower CAPEX
- 재 사용 가능한 자원 및 신속한 서비스 적용 → Flexibility
- 가상 자원의 동적 할당 → Automation
- 통일 된 중앙 집중형 정책 → Lower TCO

유연성

■ Cisco 솔루션



CRS-1

- 모듈화 소프트웨어 디자인 및 SDR을 통한 가상화 지원



Nexus

- 모듈화 소프트웨어 디자인 및 VDC 등을 통한 가상화 지원



Catalyst 6500

- 모듈화 소프트웨어 디자인 (SXH)
- vFW, ACE 등을 통한 가상화 지원



Cisco MDS 9000

- VSAN 등을 통한 가상화 지원

시스코 SP 데이터 센터 비전



SP 데이터 센터의 특징을 위한 시스코 솔루션

- WAN 구간의 확장성을 위한 기술 제공 (OC768)
- Dense 40GbE/100GbE ready
- Fiber Channel over Ethernet 기술 제공
- 모듈러 샤시 기반의 F/W 및 ACE

5 9s 이상의 서비스 가용성을 위한 H/W, S/W 아키텍처
네트워크 계층의 고가용성을 위한 Tunable FC 및 VSS 기술
자동 보안 및 Atomic ACL을 이용한 보안의 지속성
어플리케이션 계층의 통합 보안 제공

Front-End 및 Back-End의 종합 가상화 솔루션 제공
가상화를 통한 고객 별 서비스 제공
서비스 별 신속한 서비스 제공 및 공간 한계 극복

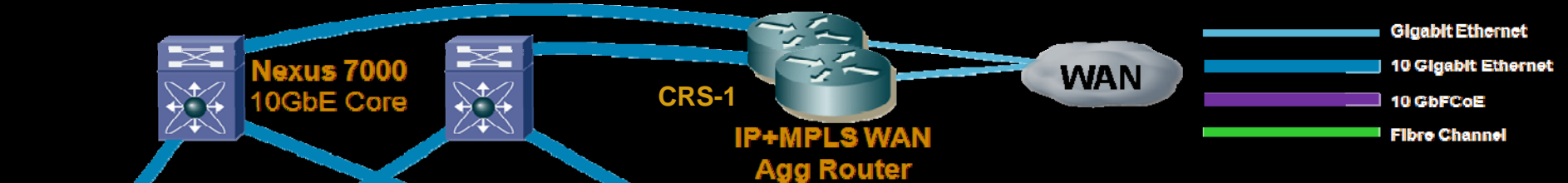
확
장
성

고
가
용
성

가
상
화

SP용 시스코 데이터 센터 솔루션 아키텍처 비전

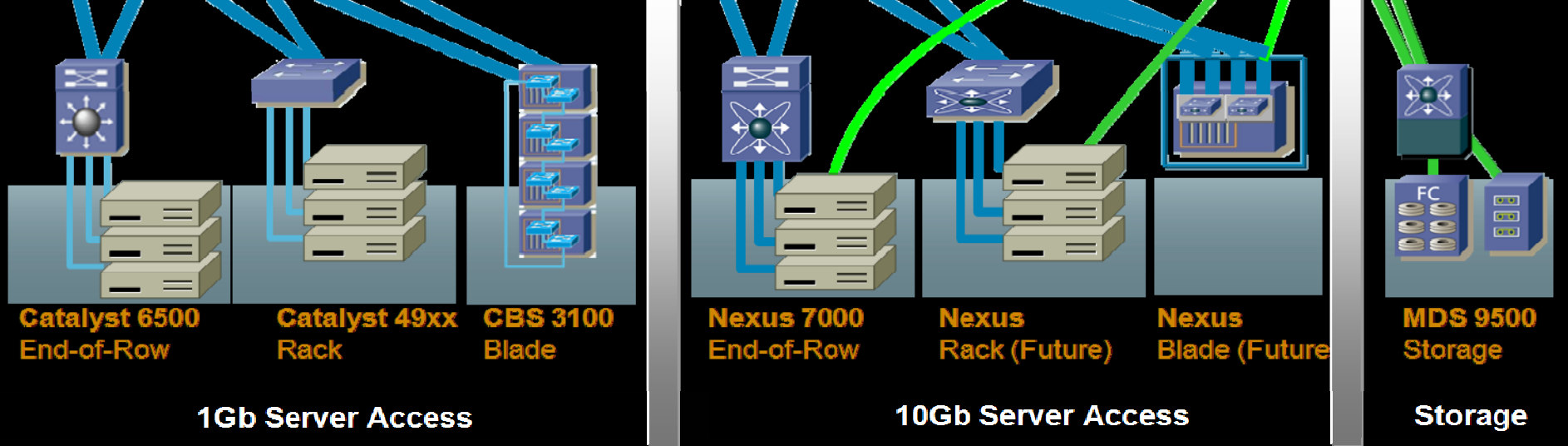
DC Core



DC Aggregation



DC Access



SP용 시스코 데이터 센터 솔루션 아키텍처 비전



