Expert Group of
Security & Application Networking

제7회 Next Generation Network Security Vision 2008 Seminar

DNS 보안의 중요성과 대응책

2008. 03. 12

|주|엑스퍼넷
금지훈 차장

목 차

인터넷 대한민국

❑ **2007년 12월 기준 만6세 이상 국민의 76.3%(3,482만명)가 인터넷 이용자**

인터넷 이용률 및 이용자수 변화추이 (%, 천명)

연령별 인터넷 이용률 (%)

인터넷 이용 목적 (랭킹)

1. 자료/정보 습득
2. 여가 활동
3. 커뮤니케이션
4. 인터넷 구매/판매
5. 교육/학습
6. 블로그/미니홈피 운영
7. 카페/커뮤니티 활동
8. 인터넷 금융
9. 전자민원
10. SW 다운/업그레이드
11. 구직활동

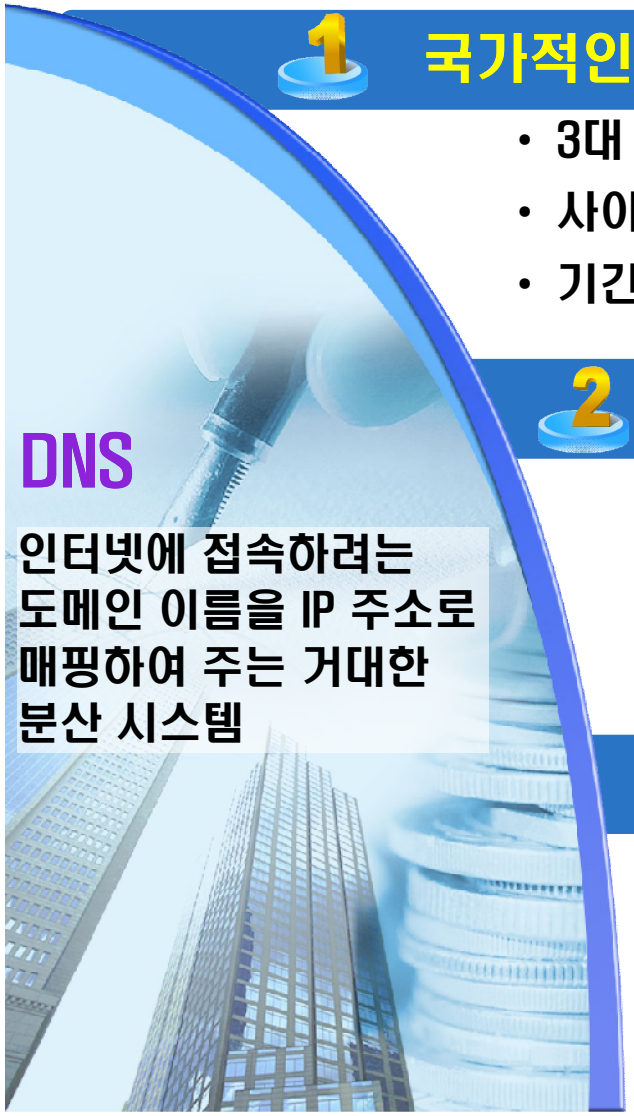
[자료 : 2007년 12월 한국인터넷진흥원, 정보화실태조사]

인터넷 기반 생활 환경의 변화

정보검색 쇼핑 교육/학습 인터넷뱅킹 포토앨범
전자민원 구인/구직 이메일 블로그 카페 게임
UCC 웹하드 웹2.0 개인화 소셜네트워킹 뉴스
영화 부동산 증권 사전 뮤직 여행 지도 교통정보

GLOBALIZATION	인터넷의 확산은 국가간의 경계를 허물며 세계화, 지구촌화에 기여
VIRTUALIZATION	정치, 경제, 사회 전 분야에 걸쳐 인터넷이 생활 필수 수단으로 정착
MUST HAVE	기반 구조 붕괴시 사회 전반적으로 막대한 파급효과 발생

인터넷과 DNS



DNS

인터넷에 접속하려는 도메인 이름을 IP 주소로 매핑하여 주는 거대한 분산 시스템

1 국가적인 의미

- 3대 첨단 인프라상에서 DNS의 중요성 확대 (IPv6, BcN, USN)
- 사이버 영토 수호 및 국익 실현을 위한 인터넷 거버넌스 활동의 대상
- 기간망 인터넷 침해사고 대응을 위한 DNS 보안에 대한 관심 증대

2 기업 환경에서의 의미

- 인터넷이 비즈니스 환경의 기본 인프라로 토착화
- 기업 이미지 재고 및 고객만족 접점으로서의 가치 증대
- 내/외부 DNS의 분리: 기업 정보보호 및 업무 연속성 수단

3 개인 생활에서의 의미

- 전기, 수도와 같은 생활 필수 인프라로서 정착
- DNS 설정은 인터넷 사용을 위한 기본 상식으로 인식
  - 가정: 초고속인터넷 환경에선 DNS 설정 불필요
  - 직장: LAN 접속을 위한 DNS 등록은 필수

DNS란?

- **Domain Name System**
- **인터넷 정보를 담고 있는 이름(yahoo.com)과 IP 주소(216.109.112.135)를 매핑해 주는 거대한 분산 시스템**

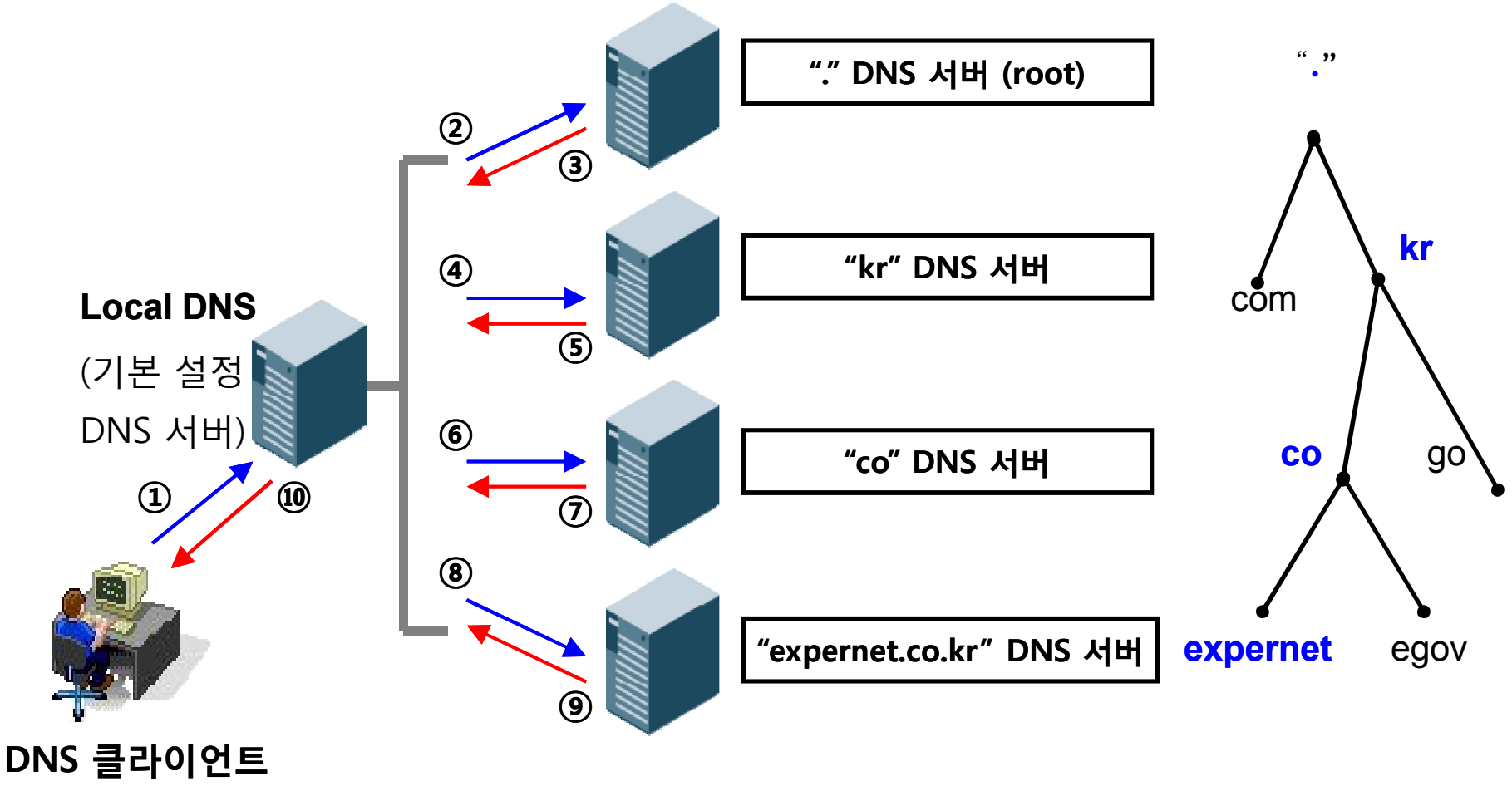
  - Forward Zone (Host → IP)

  - Reverse Zone (IP → Host)

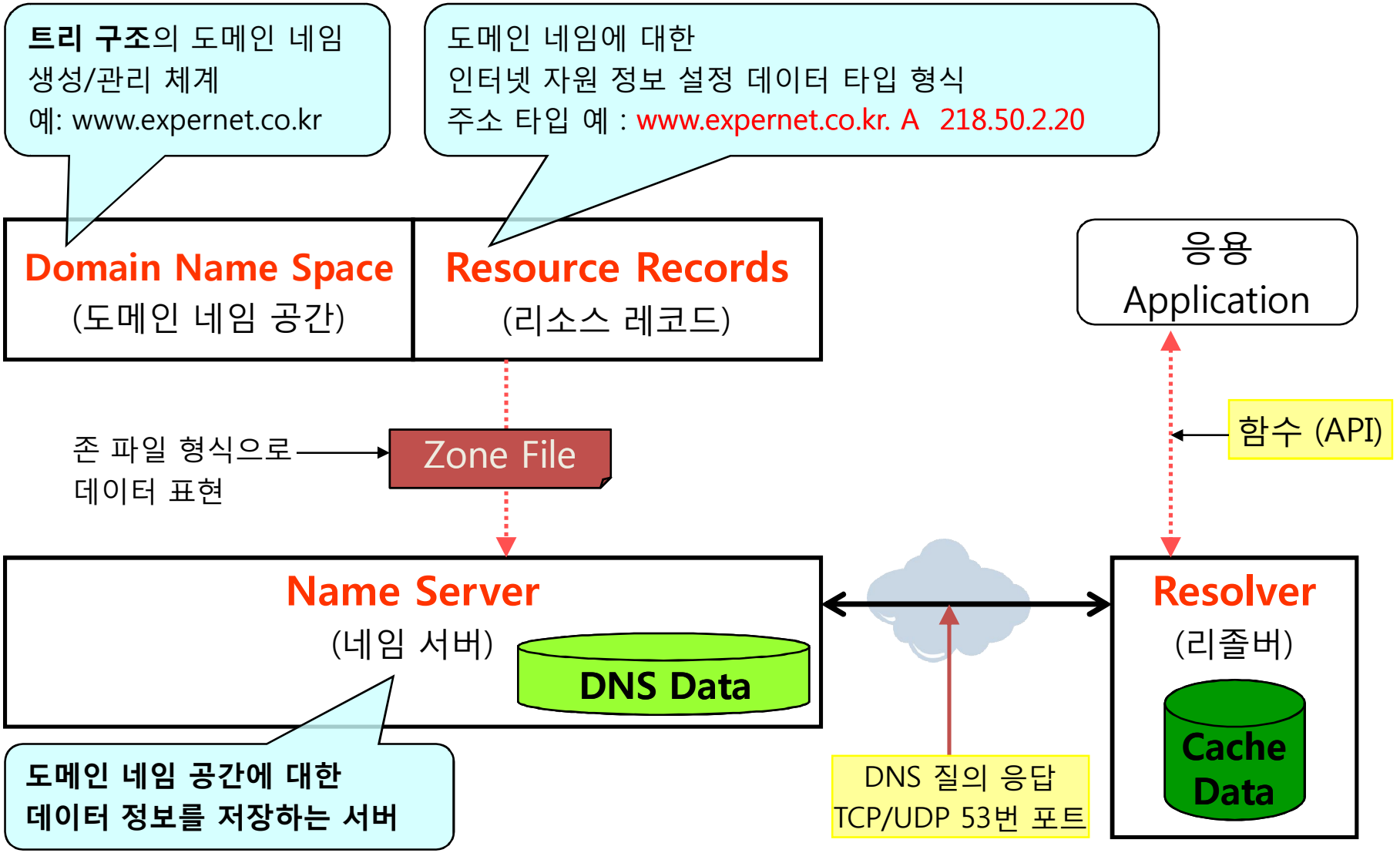
- **UDP / TCP 53 포트 사용**
  - UDP 53 포트: 일반 DNS 질의 응답
  - TCP 53 포트: 1) zone transfer시에 사용
    2) Message의 정보가 클 경우 사용

DNS 작동 프로세스

❑ 예) 클라이언트에서 expernet.co.kr 도메인 질의(query)

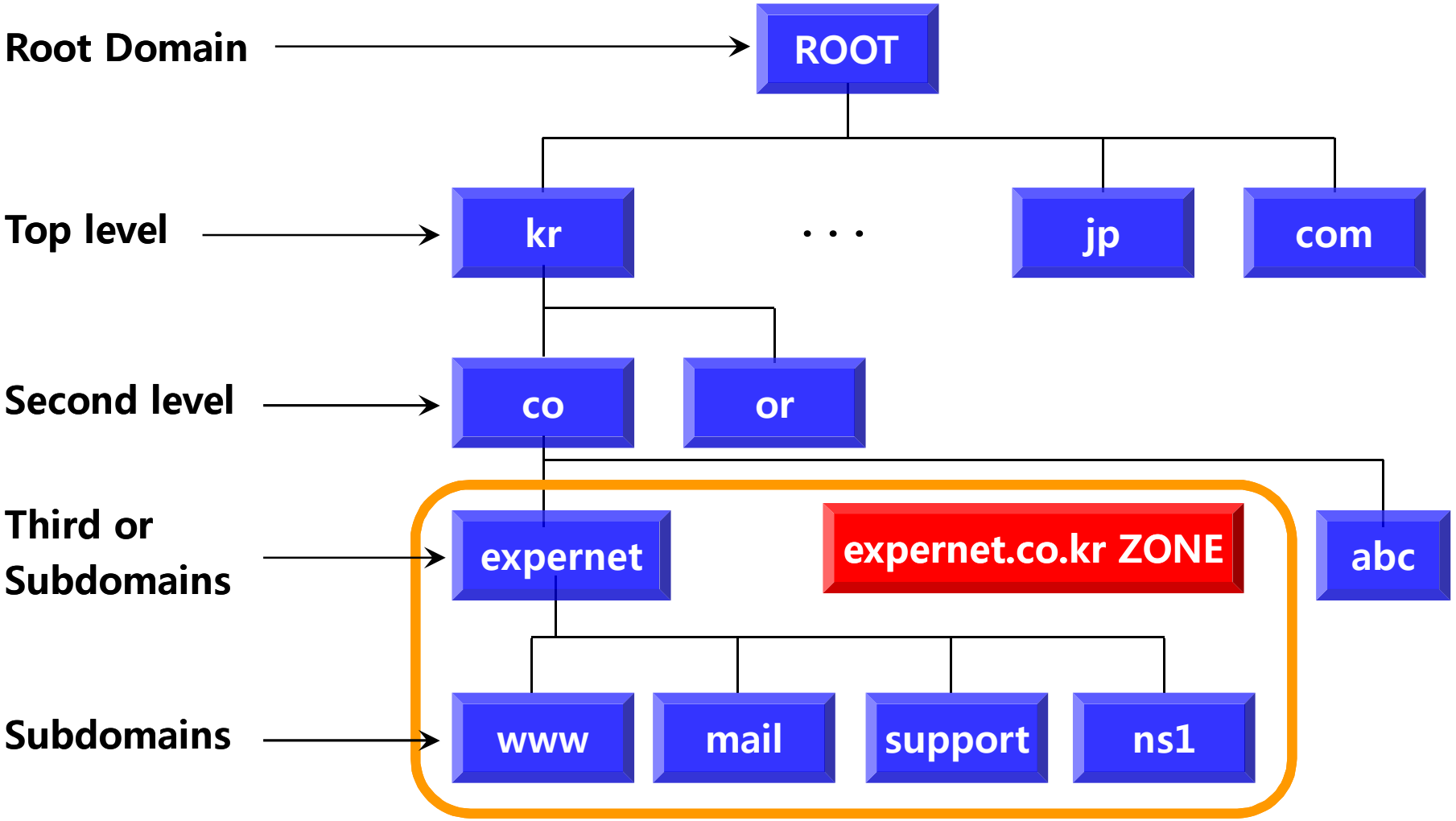


DNS의 구성요소


트리 구조의 도메인 네임
생성/관리 체계
예: www.expernet.co.kr
도메인 네임에 대한
인터넷 자원 정보 설정 데이터 타입 형식
주소 타입 예 : www.expernet.co.kr. A 218.50.2.20
Domain Name Space
(도메인 네임 공간)
Resource Records
(리소스 레코드)
응용
Application
존 파일 형식으로
데이터 표현
Zone File
함수 (API)
Name Server
(네임 서버)
DNS Data
Resolver
(리졸버)
Cache
Data
DNS 질의 응답
TCP/UDP 53번 포트
**도메인 네임 공간에 대한
데이터 정보를 저장하는 서버**

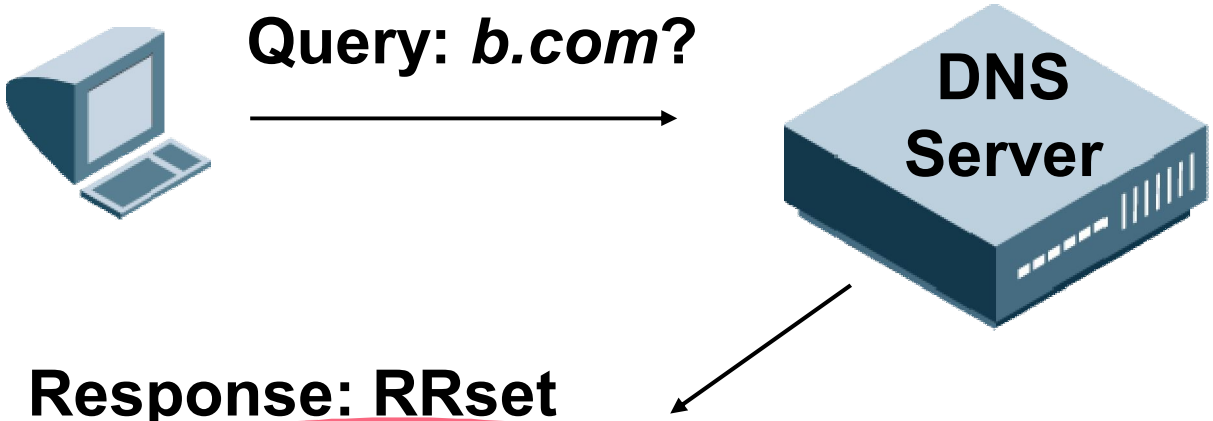
Domain Name Space

❑ 인터넷에서 사용되고 있는 도메인 네임의 계층적 구조 공간



Resource Records

❑ 리소스레코드 (RR, Resource Records): 도메인 네임이 갖는 속성값



Response: RRset
(all resource records matching domain name)

Domain	TTL	Class	Type	RDATA
b.com.	86400	IN	A	192.35.195.222
b.com.	86400	IN	A	207.182.40.12
b.com.	86400	IN	NS	ns1.b.com.
b.com.	86400	IN	NS	ns2.b.com.
b.com.	86400	IN	TXT	"v=spf1 -all"

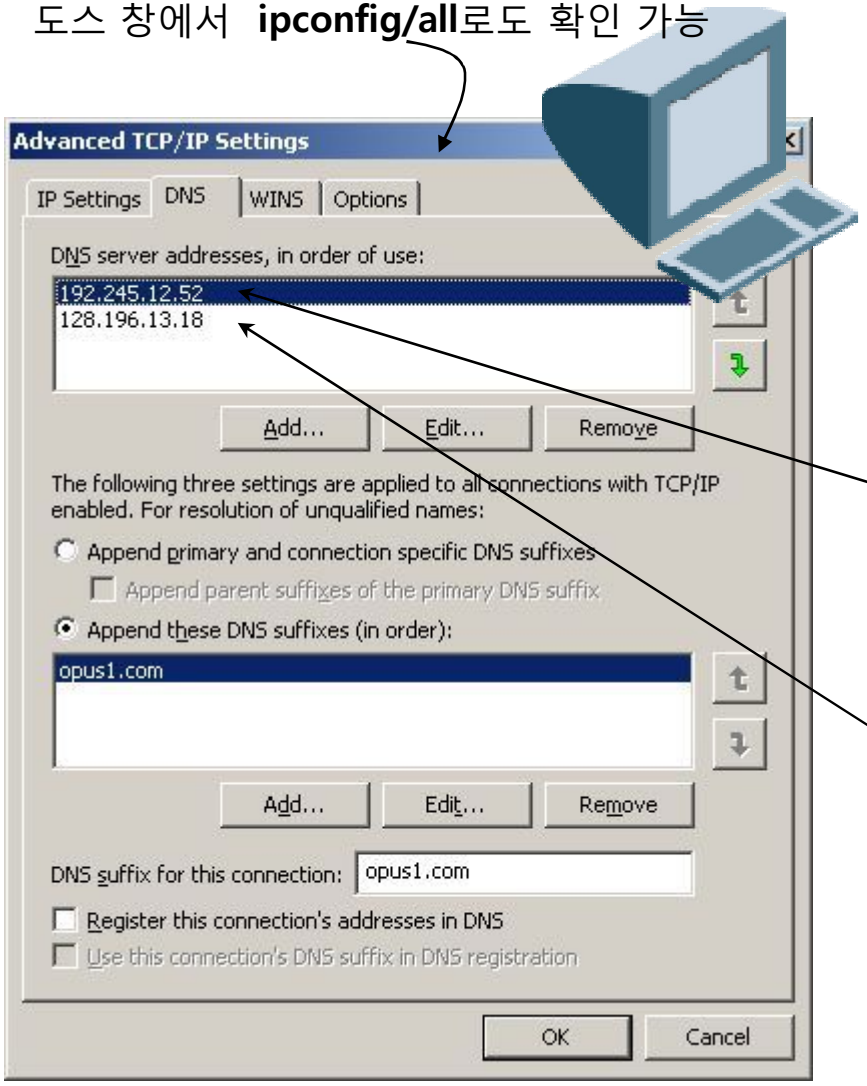
One resource record

An RRset, containing multiple resource records

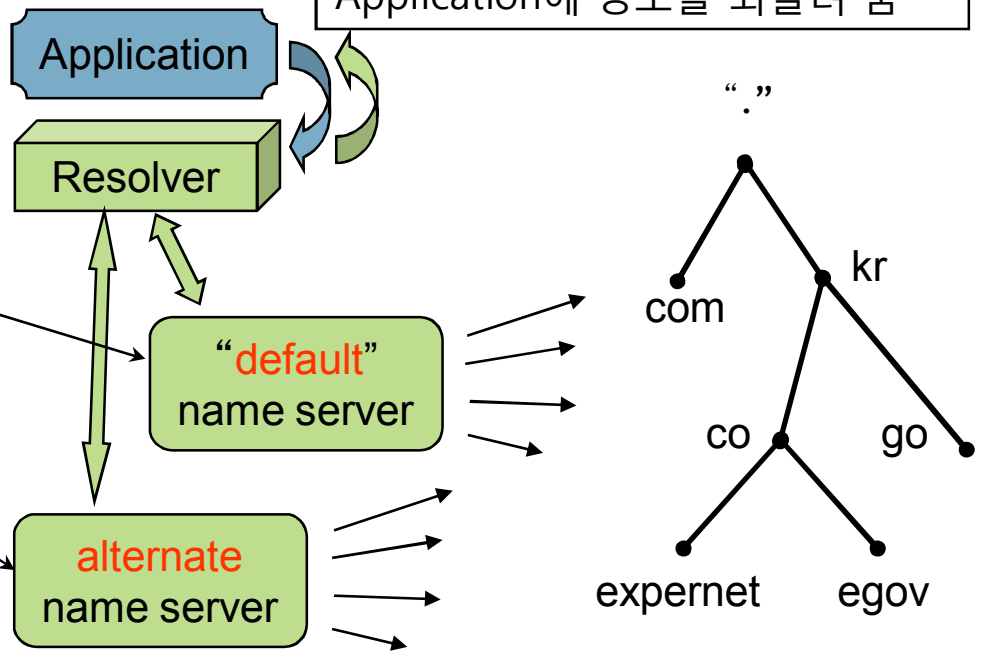
Resolver

- **네임서버를 액세스하는 클라이언트. 보통 PC라고 보면 됨**

도스 창에서 **ipconfig/all**로도 확인 가능



리졸버(Resolver) :
네임서버에 질의(query)를 보내고 응답을 해석한 뒤 요청했던 Application에 정보를 되돌려 줌

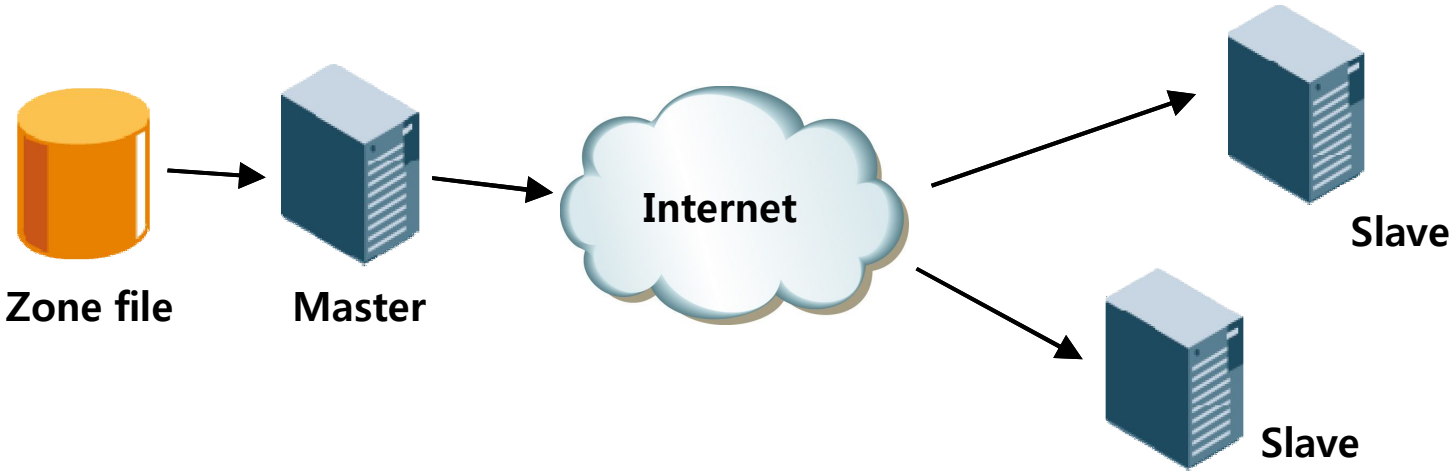


네임서버:
응답이 있는 서버들을 찾기 위해 네임스페이스 계층구조를 어떻게 거쳐야 하는지 알고 있음.

Name Server

❑ **도메인 존(domain zone) 정보를 소유하고 이에 대한 질의에 응답하는 역할 수행**

Master Server	•도메인에 대한 소유권을 가지고 있는 네임서버 •Zone file에서 자료를 로딩	**Authoritative Server**
Slave Server	•Master가 비정상 작동시 부하를 분산시키기 위해 운용 •zone transfer를 통해 Master로부터 복제된 자료를 전송 받음 •다수 존재 가능	
Cache Server	•도메인에 대한 데이터를 관리하지는 않고, resolving만 처리 •성능 향상을 위해 한번 응답된 정보는 일정기간 메모리에 캐싱	**cf) Forwarder** : 다른 캐싱서버를 이용하는 캐싱서버



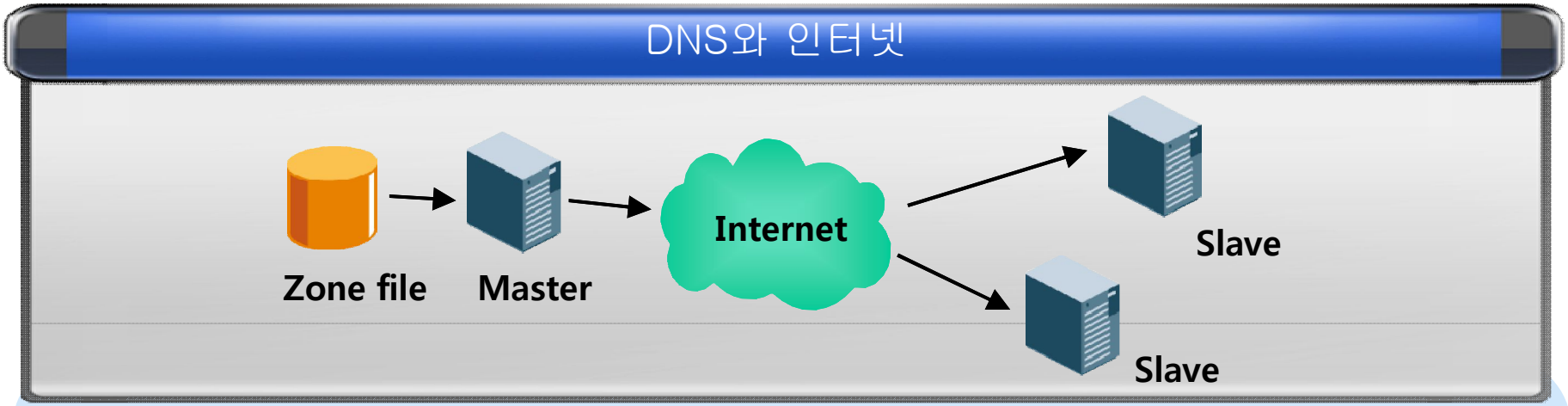
DNS 용어 설명

❑ DNS 관련 주요 용어 정리

항목	설명
Zone file	abc.com이라는 도메인 사용시 해당 도메인에 대한 소유권, 관리번호, 호스트명, 매핑 IP 정보들이 실제적으로 설정되고 저장되는 file
RR (Resource Record)	리소스 레코드 도메인 네임이 갖는 각종 속성 정보
Authoritative Answer	Query된 도메인의 네임서버에서 직접 데이터를 얻어 응답을 해줄 경우
Non-Authoritative Answer	클라이언트의 resolving 요청에 대하여 DNS의 cache나 다른 네임서버가 가진 데이터로 응답
TTL (Time To Live)	외부의 다른 서버가 zone file을 갖고 있는 Master/Slave 서버에서 도메인에 대한 변경 여부를 확인하는 시간
RTT (Round Trip Time)	갔다가 되돌아 오는 총 시간. BIND가 내부적으로 타 네임서버에 대한 RTT값을 기록하고 있다가, 요청 도메인에 대해 다수의 네임서버중에 RTT값이 가장 낮은 네임서버로 쿼리

DNS 보안의 중요성

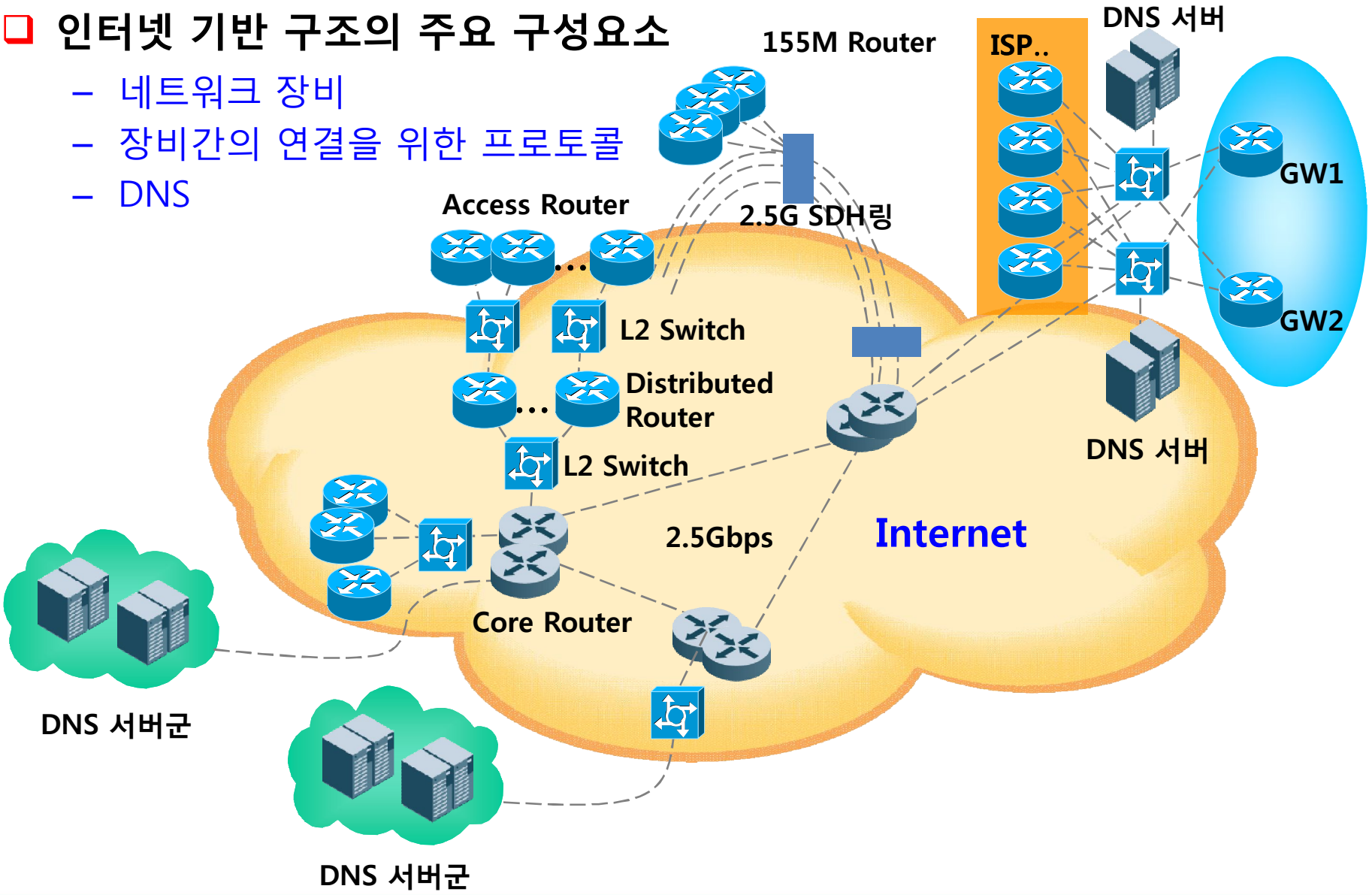
❑ 인터넷 접속의 핵심 기반 시설인 DNS의 보안성 강화는 필수!



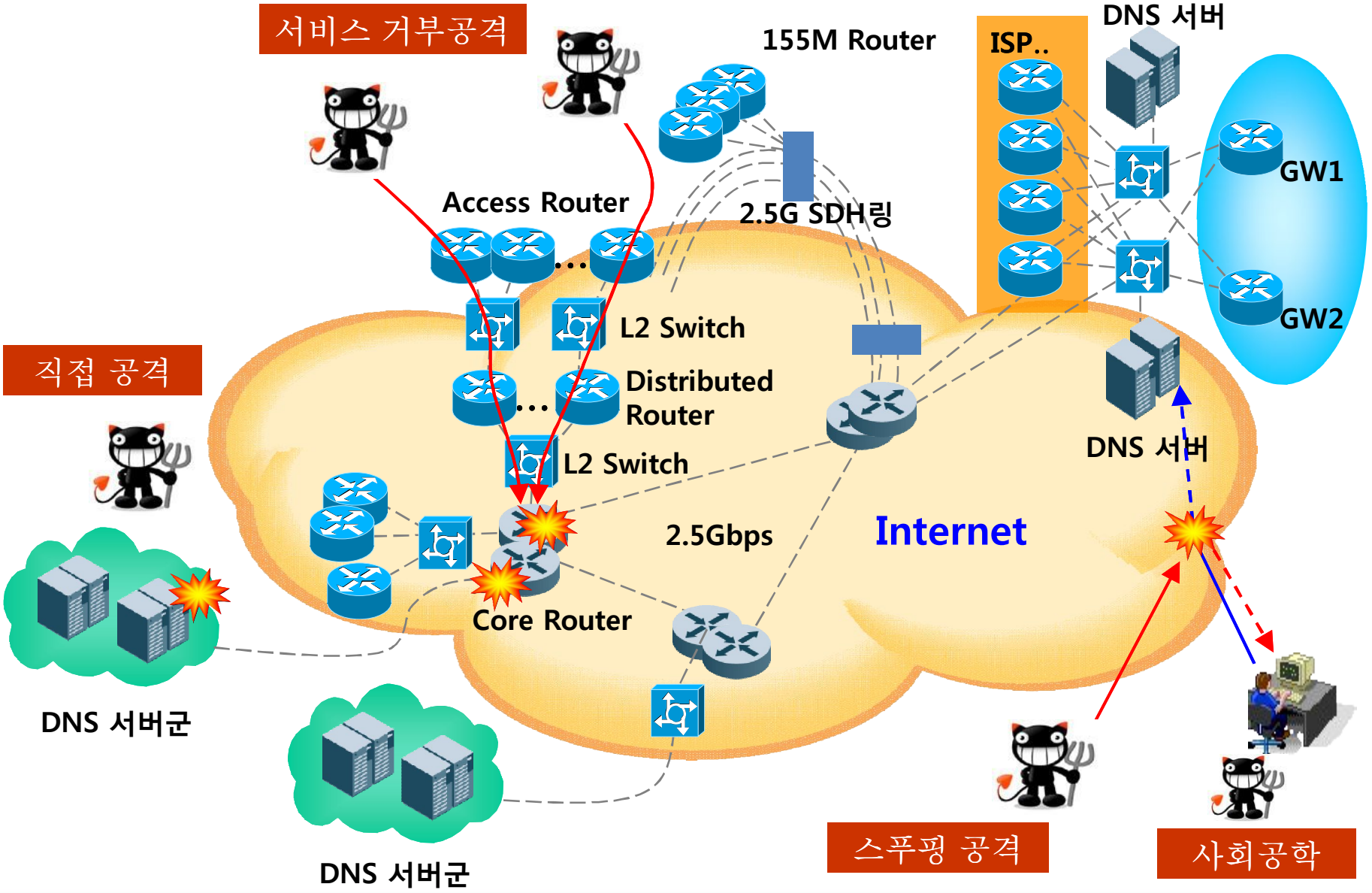
- DNS 프로토콜은 인터넷 발전 초창기에 보안이 고려되지 않아 스푸핑 등의 해킹에 취약하여 도메인 정보 위·변조 시에 사용자가 의도하지 않은 사이트로 접속될 우려가 있음
- IP 관리 체계의 내부 보안 중요성은 확대되나, 도메인에 대한 기술적/보안적 관리는 매우 허술 (DNS 장애시 파급효과 치명적)
- DNS 보안사고 급증에 대한 예방 환경 확보 필요
- 외부 접속자의 악의적 도메인 접근 시도에 대한 모니터링 체계 정비 필요

인터넷 기반 구조의 구성

- **인터넷 기반 구조의 주요 구성요소**
  - 네트워크 장비
  - 장비간의 연결을 위한 프로토콜
  - DNS



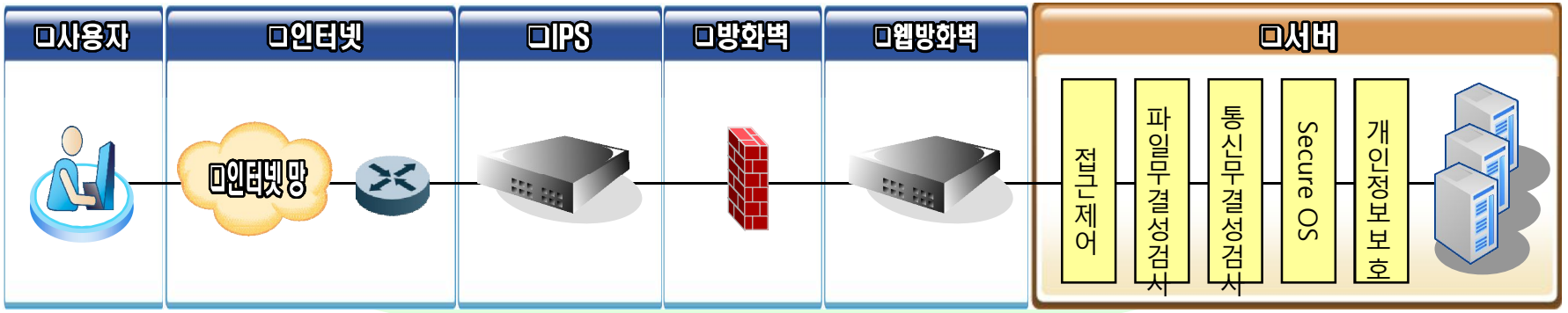
인터넷 기반 구조의 취약성



인터넷 보안 강화 요소

EXPERNET
㈜ 엑스퍼넷

❑ 일반적인 인터넷 보안 구성의 예



DNS 서버 자체는 체계적으로 관리되고 있었는가?

구분	DNS 서버 구성시 선택사항	관리 포인트
DNS	BIND 9.3.2, 9.2.6, 8.4.7 / Microsoft DNS 서버 구성 마법사	•S/W 업데이트 •S/W 보안패치
OS	Windows / HP-UX / solaris	•OS 보안패치 •애플리케이션 패치
H/W	PC	•시스템 사양 •H/W 업그레이드
Vendor support	hp / Sun microsystems / IBM / DELL	•기술지원 범위

현재의 DNS 운영 환경 진단

EXPERNET
㈜ 엑스퍼넷

❑ DNS 현안과제

DNS 문제 및 이슈사항

DNS Performance : 성능 측면

- DNS 서버의 유휴 장비 이용에 따른 성능 제약
- 일부 도메인의 DNS resolve 기능 장애 빈번
- 웹 기반 인트라넷 증대에 따른 DNS 쿼리량 급증
  (특정 DNS 서버에 쿼리 집중화 만연)

DNS Management : 관리 측면

- 서비스 영역에 따른 DNS 구성 분리 필요
  (External/Internal)
- 사업장별 DNS 백업 체계의 효율적 분산화 한계
- 용도별 개별 관리 포인트 발생

DNS Simplicity : 운영편의성 측면

- 사업장별 변경 내용에 대한 수작업 동기화로 오류 가능성 높음
- 사용 이력의 수작업 관리 → 즉각 대응 어려움

DNS 잠재적 장애요인

DNS Security : 보안성 측면

- 서버 OS 보안패치 또는 S/W 업그레이드 시 리부팅으로 인한 DNS 서비스 중단 불가피
- BIND DNS의 보안 취약성 상존
  → 장애 발생 가능성 내재

DNS Availability : 가용성/안정성 측면

- DNS H/W 노후화 및 유지보수의 제약성
- DNS 장애시 백업 체계의 수작업 관리
  → 업무 중단 초래

DNS의 보안 취약점

❑ DNS의 태생적 제약사항

- 인터넷 초기에 보안을 고려하지 않고 설계된 프로토콜
- 인터넷의 급격한 확산 ➔ 침해 공격 시도 지속 증가
- 침해 공격으로 인한 장애 발생시 문제 심각 (정보 유출, 금융사고)

❑ DNS 취약성

- **DNS 서버 자체의 취약성**
  - DNS 서비스를 운영하는 서버 자체의 OS 취약성
  - DNS Application 버전상의 취약성
- **서비스 거부 공격**
  - 과도한 DNS query
  - 과도한 트래픽
- **스푸핑 공격**
  - DNS poisoning
- **정보 유출**
  - Zone transfer 악용
  - 내부 네트워크 토폴로지
  - 내부 중요 서버 IP 정보

주요 DNS 보안 이슈의 해결방안

EXPERNET
㈜ 엑스퍼넷

❑ **대부분 해결방안이 제시되어 있으나 조치 이후에도 꾸준한 관리가 필요**

DNS 보안 이슈	해결방안
Zone 정보 노출 (Zone Exposure)	전송(transfer) 제한; 뷰(view) 생성
포이즈닝 (Poisoning)	재귀적 질의(recursive queries) 제한
서비스 거부 (Denial of Service)	IPS (Intrusion Prevention Systems) 사용 동시 사용 규모의 내부적 제한
비 인가 전송 및 업데이트 (Unauthorized Transfer or Update)	TSIG (Trusted Signature)
업데이트시 인가 및 인증 체계 구현 (Authorization and Authentication of Updates)	TSIG, DNSSEC

권장 DNS 보안 정책

권장 방안	세부 내용
DNS 서버의 물리적 분리 구성	서로 다른 네트워크, 건물, OS에 Master, Slave 설치
DNS 서버의 용도에 따른 분리 구성	Advertising과 Resolving으로 구분하여 설치
재귀적 질의(Recursive query) 제한	named.conf 수정 → ***options { allow-recursion {none;} };***
Zone Transfer 제한	named.conf 수정 → ***options { allow-transfer {none;} };***
Dynamic Update 제한	named.conf 수정 → ***options { allow-update {none;} };***
TSIG를 이용한 보안 강화	zone transfer, notify, 순환 질의, dynamic update 시 암호화 키를 사용
View를 이용한 DNS 분리 (BIND9)	동일 도메인 중 내부 사용자와 외부 사용자가 각각 별도의 응답이 필요할 경우
BIND 버전 정보 유출 제한	named.conf 수정 → ***options { version "unknown"; };***
DNS 방화벽 정책	DNS만을 위한 별도의 네트워크 구축 (네임 서비스에 필요한 포트만 개방)
DNS 질의 모니터링	http://dnstop.measurement-factory.com

공개소프트웨어의 딜레마

EXPERNET
㈜ 엑스퍼넷

❑ 대다수 사용중인 BIND DNS의 이력

Bind 4.x – 개발 중단.

Bind 8.x – root DNS 및 대부분의 DNS 에서 사용
일반적인 Query 응답률이 가장 좋음
No new feature, only major security patch.
ISC의 BIND8 버전 업그레이드 및 패치 중단 발표 (2007. 8. 27)
신규 버그 및 보안 취약점으로 인한 장애 발생시 기술지원 全無

Bind 9.x – DNSSEC등 보안을 고려한 최신 기술 반영
기존 버전의 기능 개선 및 multi-thread 지원
(answering queries while loading zones)

BIND 9 업그레이드 시 이슈사항

EXPERNET
㈜ 엑스퍼넷

- **권장 최신 버전으로 업그레이드하여도 공개 S/W의 근본 제약사항 여전**
  - H/W적인 Failover 체계 없음 (서비스 가용성 확보 불가)
  - OS 의존적 서비스 제약성 (잦은 보안패치, 서버 리부팅시 서비스 일시 중단 불가피)
  - TEXT 기반의 수작업 환경으로 도메인 관리 대상이 방대할 경우 체계적인 관리 어려움

- **버전 업그레이드 & DNS 데이터 이관의 실효성 미약**
  - 운영중인 도메인 정보의 신속한 마이그레이션 보장 불확실 (이관 자체의 불안정성)
  - 최신 적용 버전이 차후 동일한 지원 중단 발표시 DNS 서비스 안정성 확보 어려움

- **도메인 접근 이력에 대한 직관적인 로깅/모니터링 체계 마련 시급**
  - DNS 보안사고 급증에 대한 예방 환경 확보 필요
  - 외부 접속자의 악의적인 도메인 접근 시도에 대한 모니터링

DNS Paradigm

EXPERNET
㈜ 엑스퍼넷

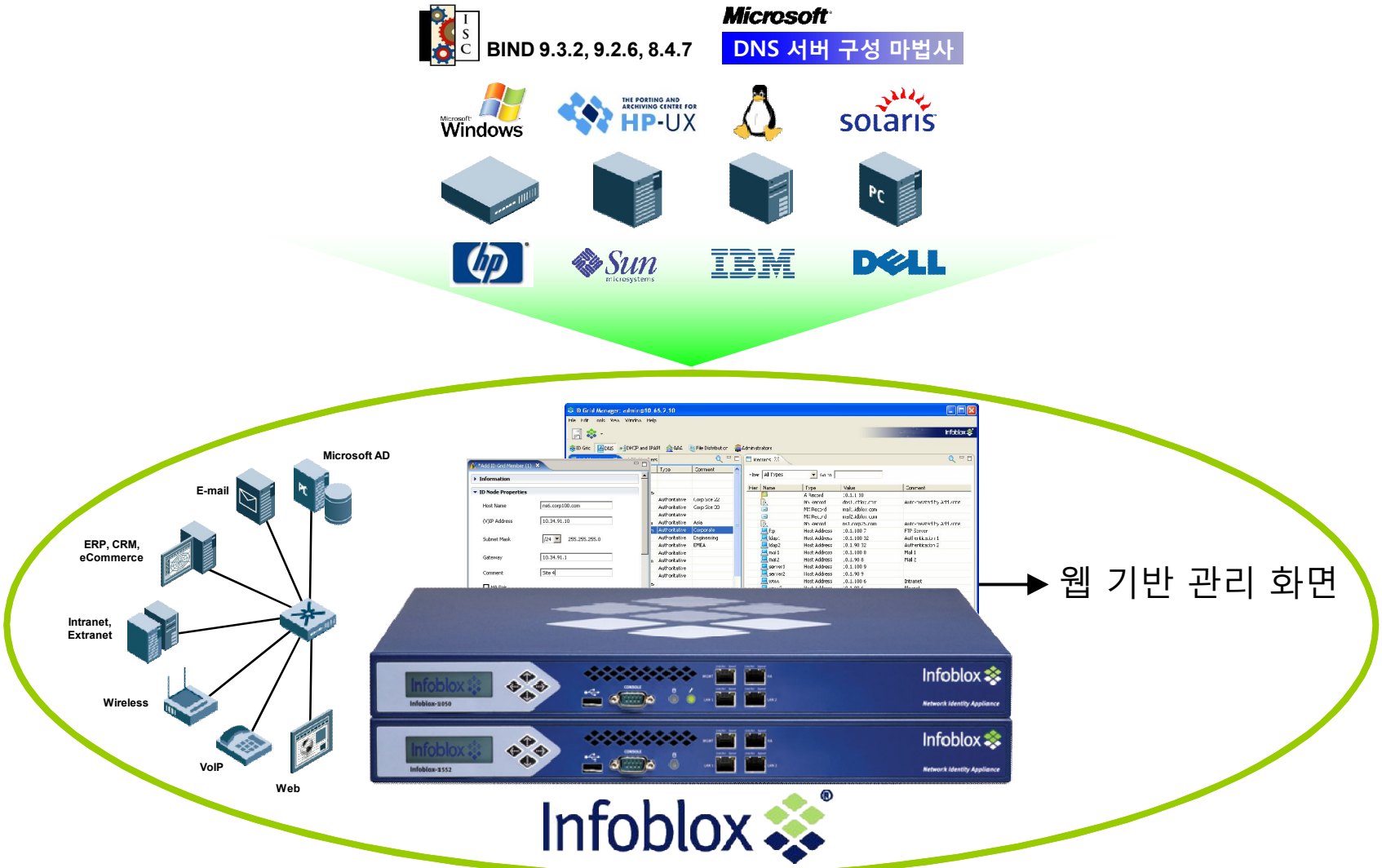
❑ DNS 전용 플랫폼의 도래

과거	현재	
라우팅 소프트웨어 탑재형 유닉스 박스		멀티-프로토콜 라우터
파일 스토리지 탑재형 표준 서버		스토리지 어플라이언스
보안 소프트웨어 탑재형 표준 서버		방화벽 어플라이언스
DNS 전용 일체형 표준 서버		DNS 서비스용 전용 어플라이언스

Infoblox DNS Appliance 소개

EXPERNET
㈜ 엑스퍼넷

❑ 소프트웨어 타입에서 발생되는 보안 취약성 및 관리 복잡성을 근본 개선



기존 DNS 환경 대비 특장점

❑ BIND vs Infoblox

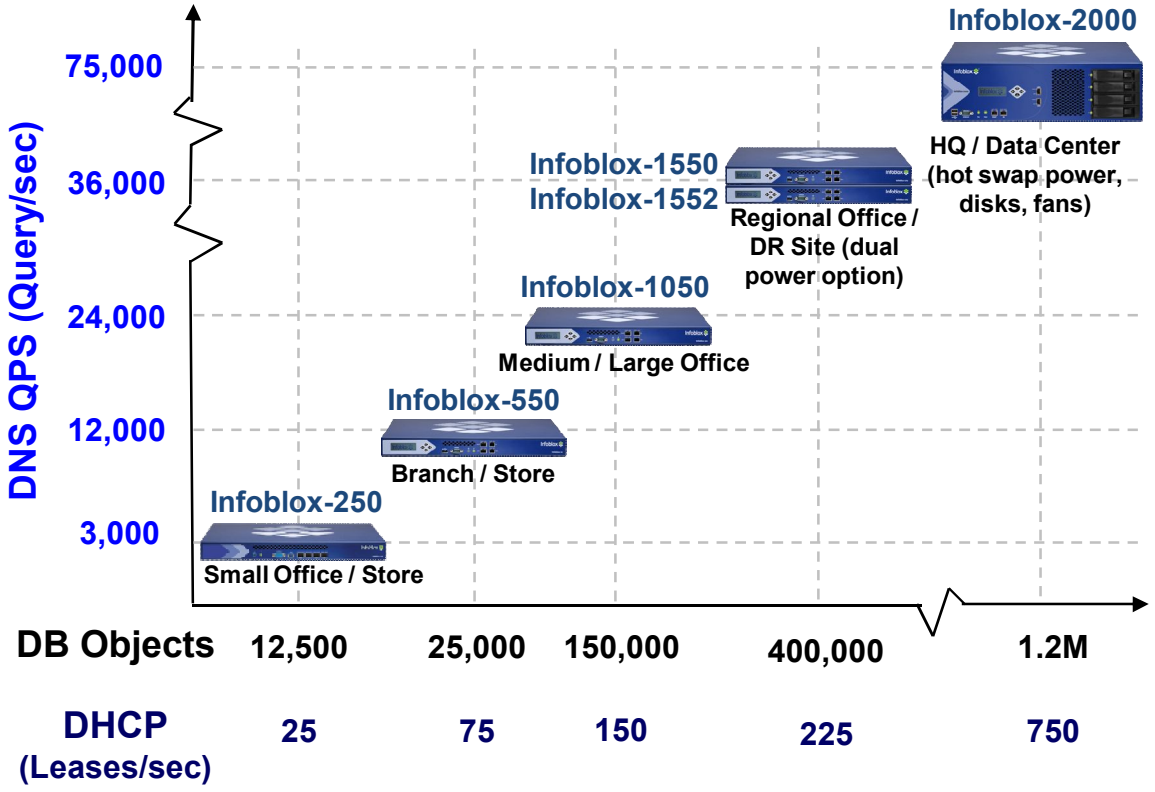
구분	소프트웨어 형태 DNS	Infoblox DNS Appliance
DNS플랫폼	**BIND DNS (무료)**	**DNS 전용 장비 (상용)**
구성요소	복잡 • H/W (일반 서버) • OS (Unix or Linux) • DB (SQL, Oracle, MySQL 등)	간단 • 어플라이언스 (일체형 전용 장비) – 자체 엔진, Application, 자체 DB, H/W 일체형
보안성	보통 • OS 자체 취약점 주기적 패치 필요 • 각종 open된 서비스 관리 필요 • (Application)	매우 높음 • 전용 OS 사용 → 해킹 불가 • 웹 기반 GUI (HTTPS) • 강력한 사용자 인증 환경 제공 (RADIUS/AD 관리자 인증)
가용성	낮음 • 별도의 시스템이나 토폴로지로 해결 수준	매우 높음 • HA기능, 동기화 기능 기본 탑재 – 전용 OS에서 자체 지원 • 장비간 모든 구성 및 사용 정보 실시간 동기화
관리편의성	불편 (MS DNS의 경우 일부 GUI 제공) • CLI 기반 또는 제한적 콘솔 환경 수준 • 관리자의 OS 및 시스템 관리 지식 요구 • 설치, 이관 및 운용 어려움 • 외부 기술지원 없음. 직접 오류 해결 요구	매우 편리 • 직관적인 웹 기반 GUI로 DNS 전반 설정/관리 • 다수의 시스템 통합관리 기능 제공 • Auto-Configuration 기능으로 관리자 오류 최소화 • 전담 기술지원. 트러블슈팅 시 책임소재 명확화
설치시간 /기술수준	보통 4시간 이상 소요/요소별 전문인력 필요	최대 30분 이내 / 비 전문가도 가능

제품 라인업

EXPERNET
㈜ 엑스퍼넷

❑ **Infoblox 어플라이언스는 DNS 외에도 DHCP, RADIUS 서버 기능을 제공**

하드웨어 플랫폼 구성

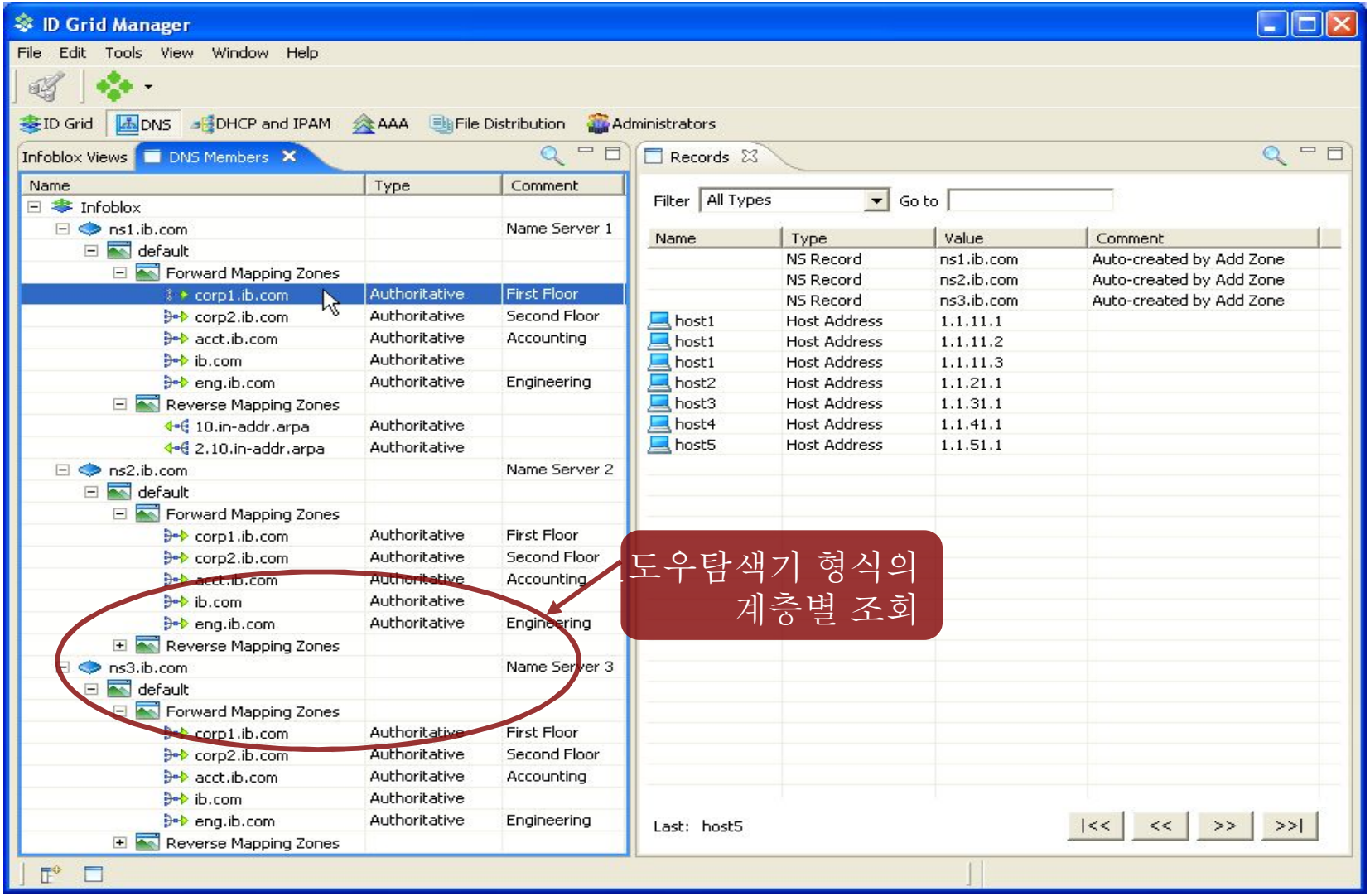


패키지 구성

PACKAGES / MODULES	DNSone	DNSone + Grid	NSV	NSA	NSS	NSQ	WinConnect
DNS	■	■			■		
DHCP	■	■	■		■		
IPAM	■	■	■		■		
RADIUS				■	■		
Grid		■	■	■	■	■	
IPAM for Microsoft							■

관리자 인터페이스

❑ 직관적인 웹 기반 관리자 화면 제공



Data Import Wizard

❑ 기존 데이터의 마이그레이션 툴 제공

Microsoft
DNS & DHCP

ISC
BIND & DHCP

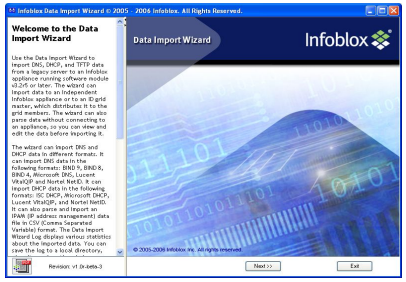
Lucatel VitalQIP™
DNS & DHCP

Nortel NetID™
DNS & DHCP

CSV File
DHCP
MAC Filters
IPAM Info

TFTP
Files & Directories

Infoblox
Data Import Wizard



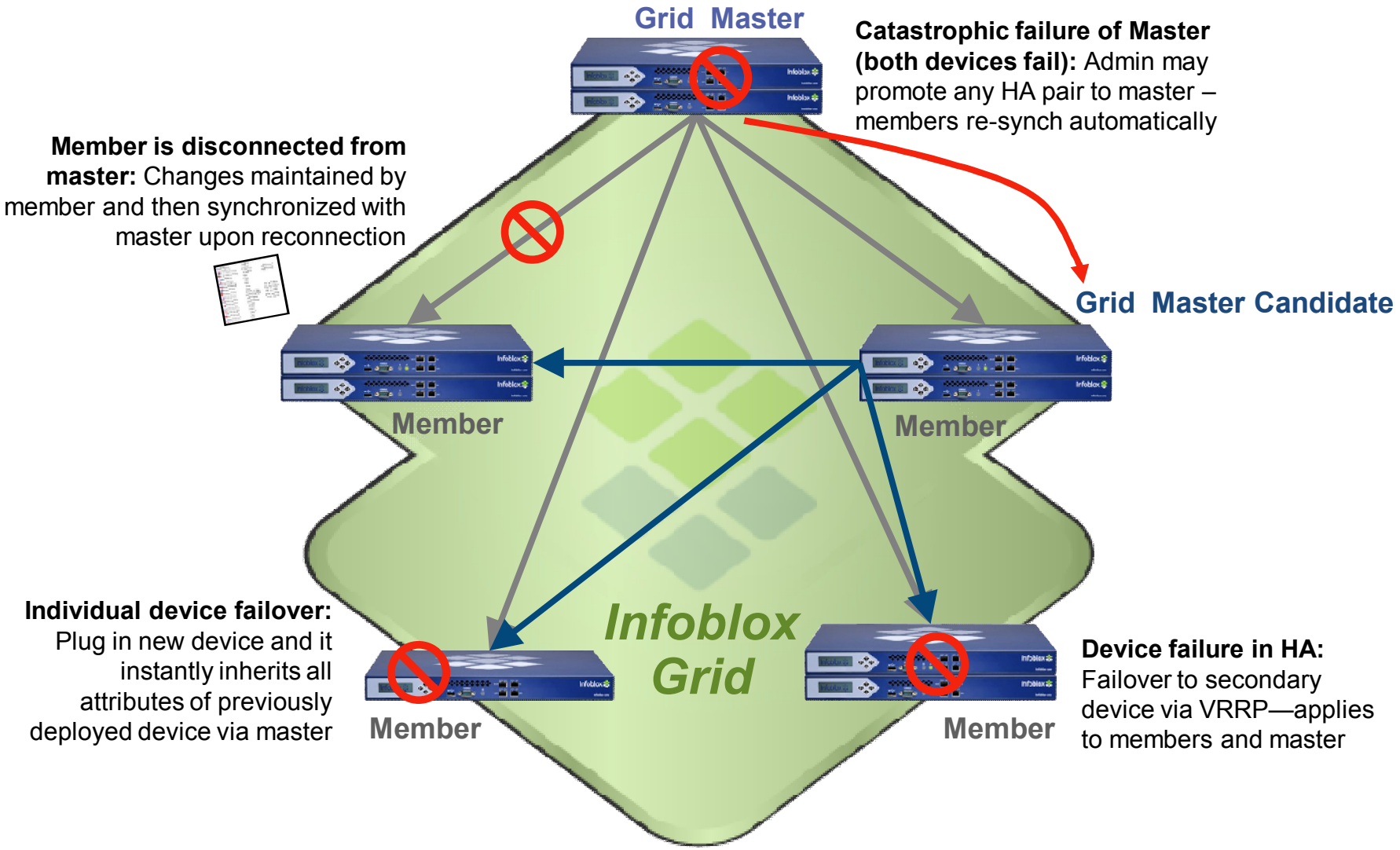
마이그레이션 전용 툴로 간편하게 Infoblox DNS 서비스 환경으로 신속하게 전환 가능

Infoblox

DNSone Appliances

Grid & HA Failover

❑ 권역별 사업장의 DNS 데이터에 대한 자동 동기화 및 중앙관리 편의성 제공



Infoblox 주요 레퍼런스

EXPERNET
㈜ 엑스퍼넷

금 융

제 조

교 육

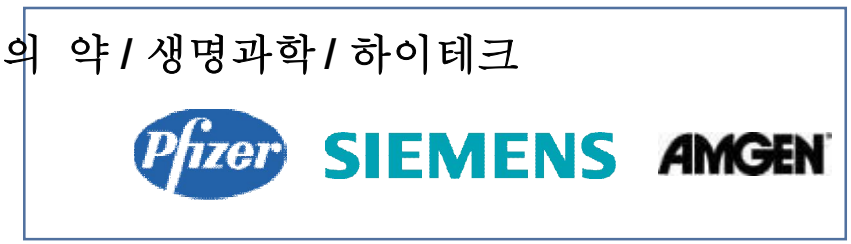
정부기관

미디어 / 인터넷

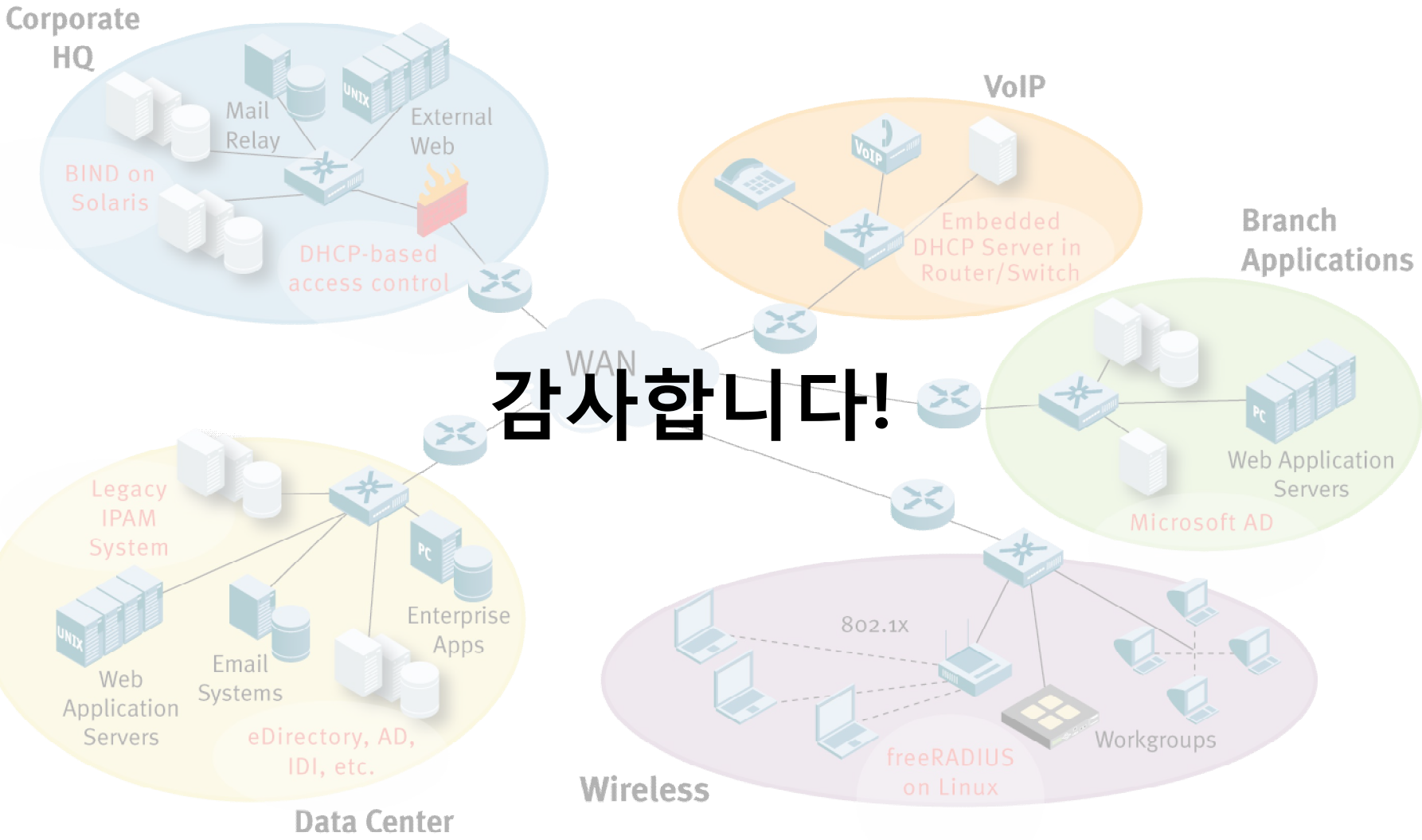
통 신

리테일 / 서비스

의 약 / 생명과학 / 하이테크



마치며...


Corporate HQ
Mail Relay
External Web
BIND on Solaris
DHCP-based access control
VoIP
Embedded DHCP Server in Router/Switch
Branch Applications
Web Application Servers
Microsoft AD
WAN
Legacy IPAM System
Enterprise Apps
Email Systems
Web Application Servers
eDirectory, AD, IDI, etc.
Data Center
802.1x
Workgroups
freeRADIUS on Linux
Wireless

감사합니다!