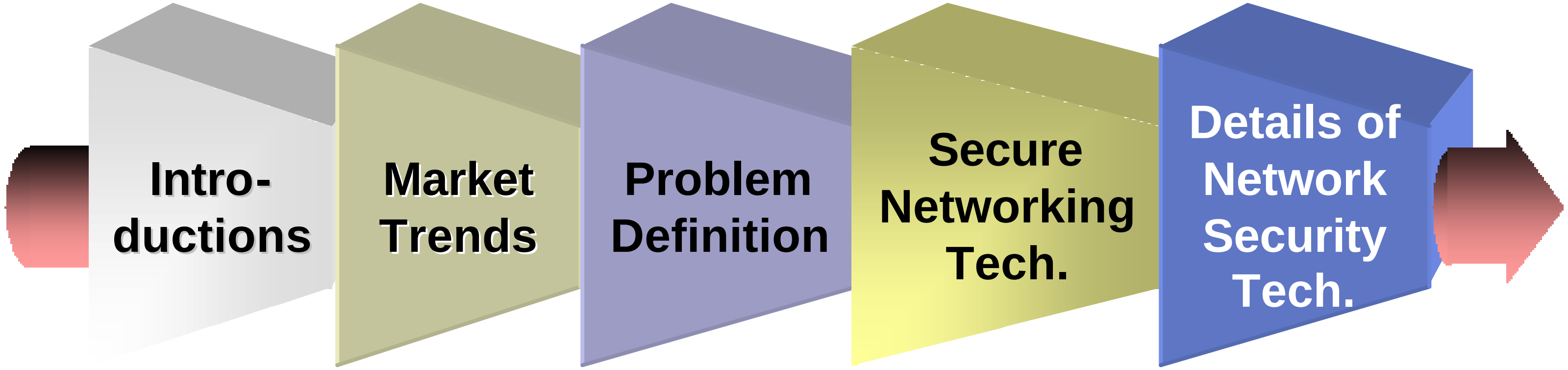
Development of Network Security Technology

2001. 9. 25.

Information Security Technology Division

ETRI
한국전자통신연구원

Contents



Intro-ductions

Market Trends

Problem Definition

Secure Networking Tech.

Details of Network Security Tech.

Internet Paradigm

Everything over Internet !
But ...

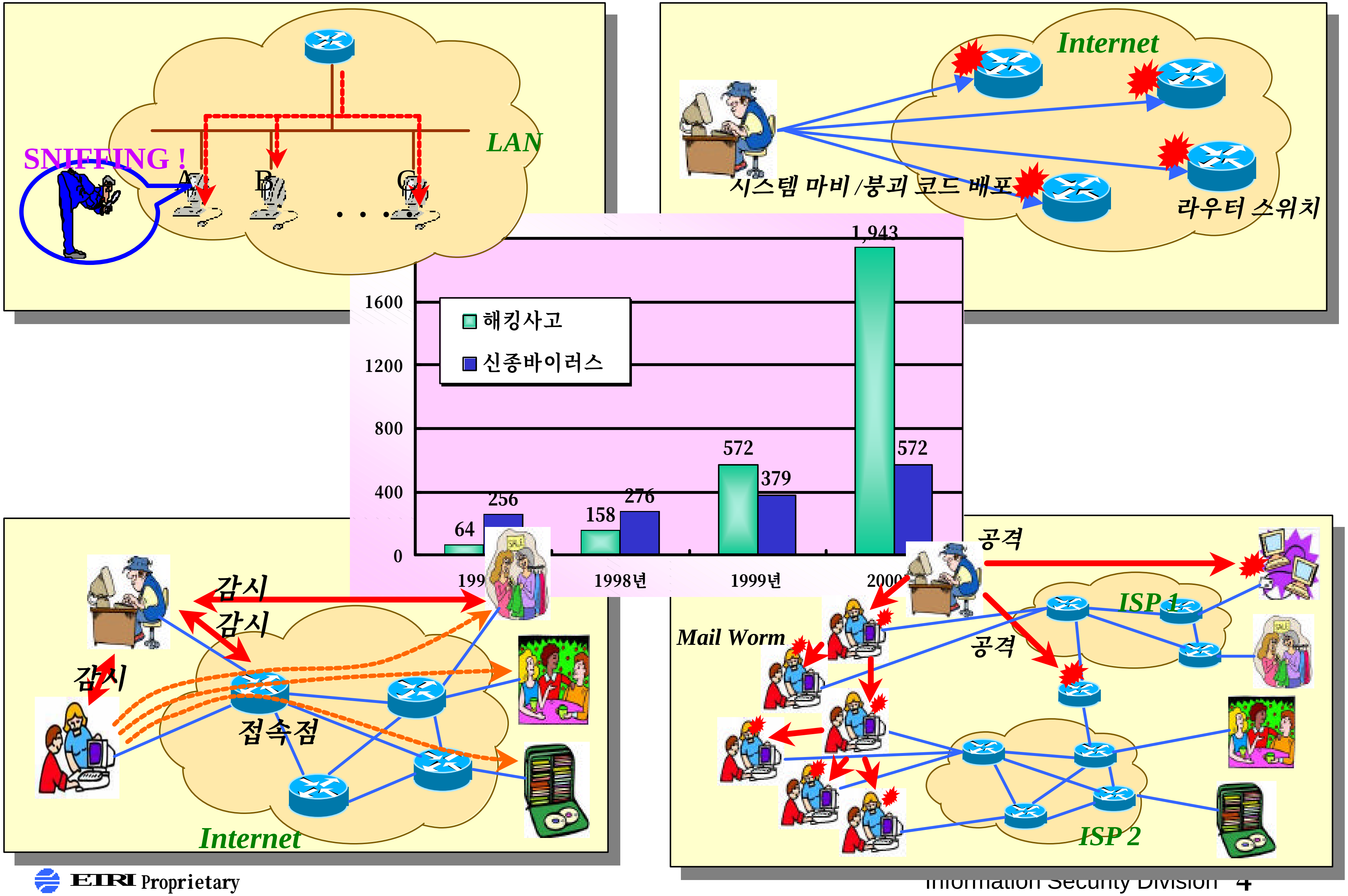
Security Vulnerabilities

☞ Can be easily intercepted by monitoring transmission line
☞ Can be easily monitored and controlled by attackers
☞ Can be possible to disable networks by service disruption attacks

➡ ***Anti-Cyber Terror should be necessary!***

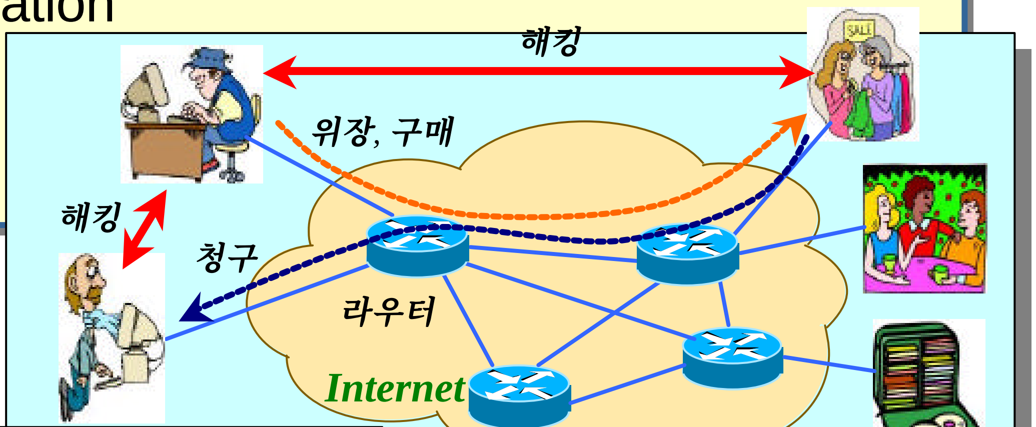
➡ ***Security should be necessary!***

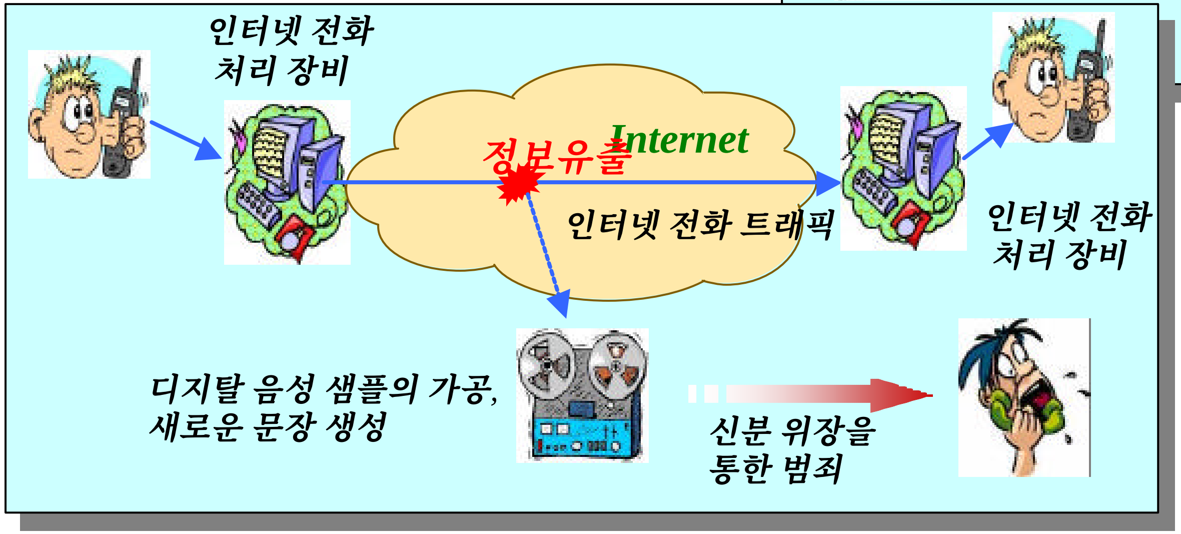
Cyber Terrors ?



Problems

- ☞ Service disruption of E-commerce
- ☞ Exposure of network routing data
- ☞ Misusage of personal information
- ☞ Privacy Infringement
- ☞ Network disruption





Cyber Terror Technology

Trends

☞ Multiple-attacks through networks

☞ Redirect attacks

☞ Attacks against server and PC

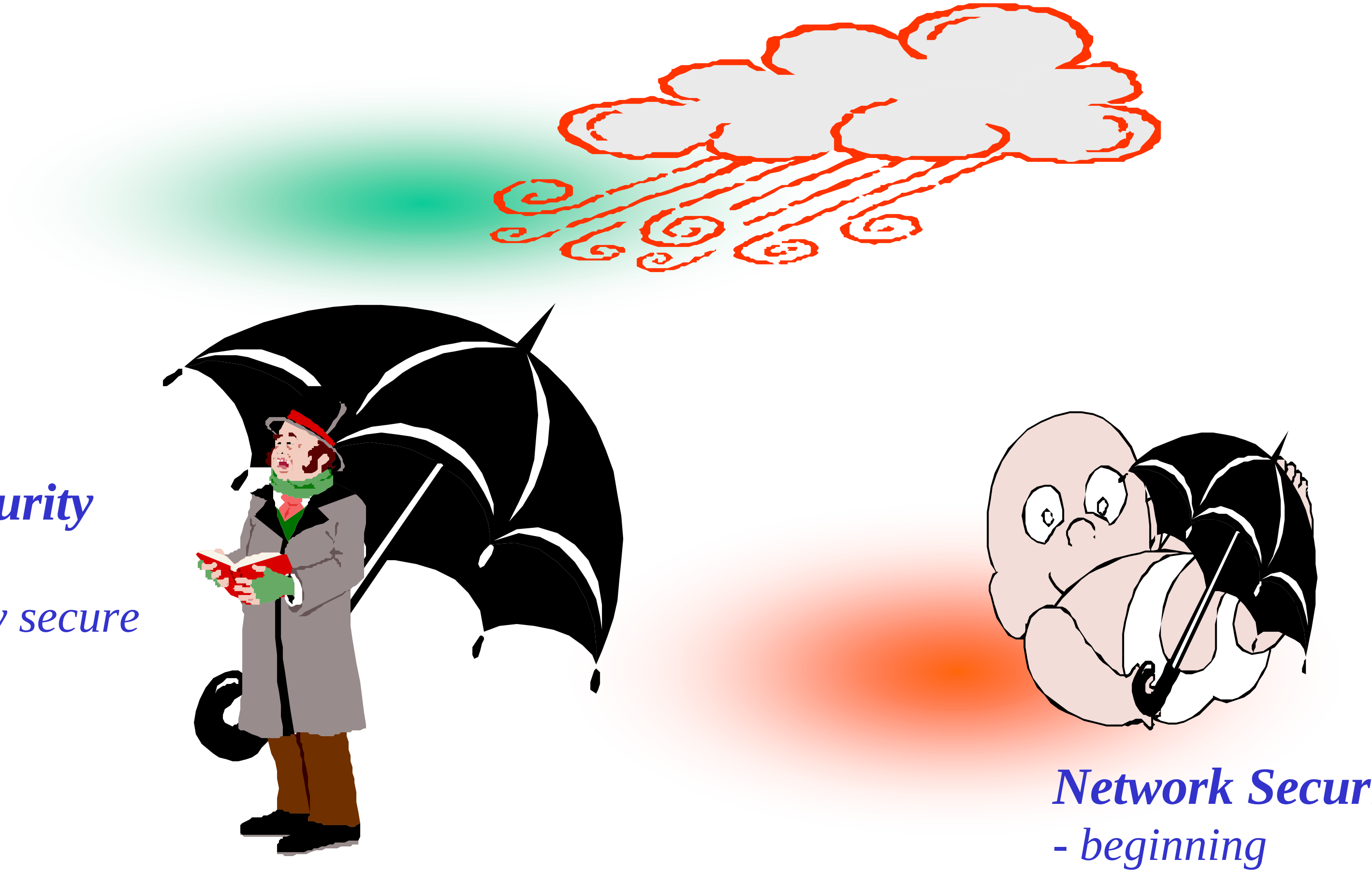
☞ Domestic hacking by foreigners

☞ Attacks by using information security technology

☞ System breakdown / decrease of network performance

→ **Host & network *security should be necessary!***

Host Security vs Network Security



Host Security

- mature

- relatively secure

Network Security

- beginning

- relatively non-secure

Network Security Evolution

Individual Security

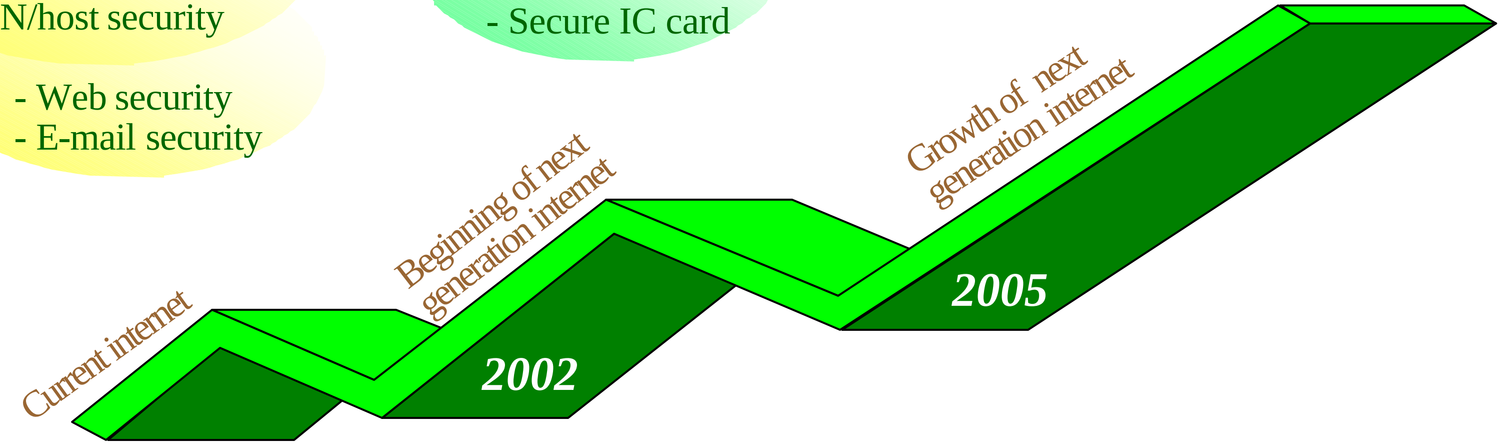
- High secure algorithm
- Intrusion detection
- Intrusion protection
- LAN/host security
- Web security
- E-mail security

Integrated Security

- High speed algorithm
- IPsec
- ESM
- Security policy-based
- Secure OS
- Secure IC card

Intelligent Active Security

- QoS Security
- Information warfare
- Active security
- Optical Security
- Multicast security
- Electronic voting



Current internet

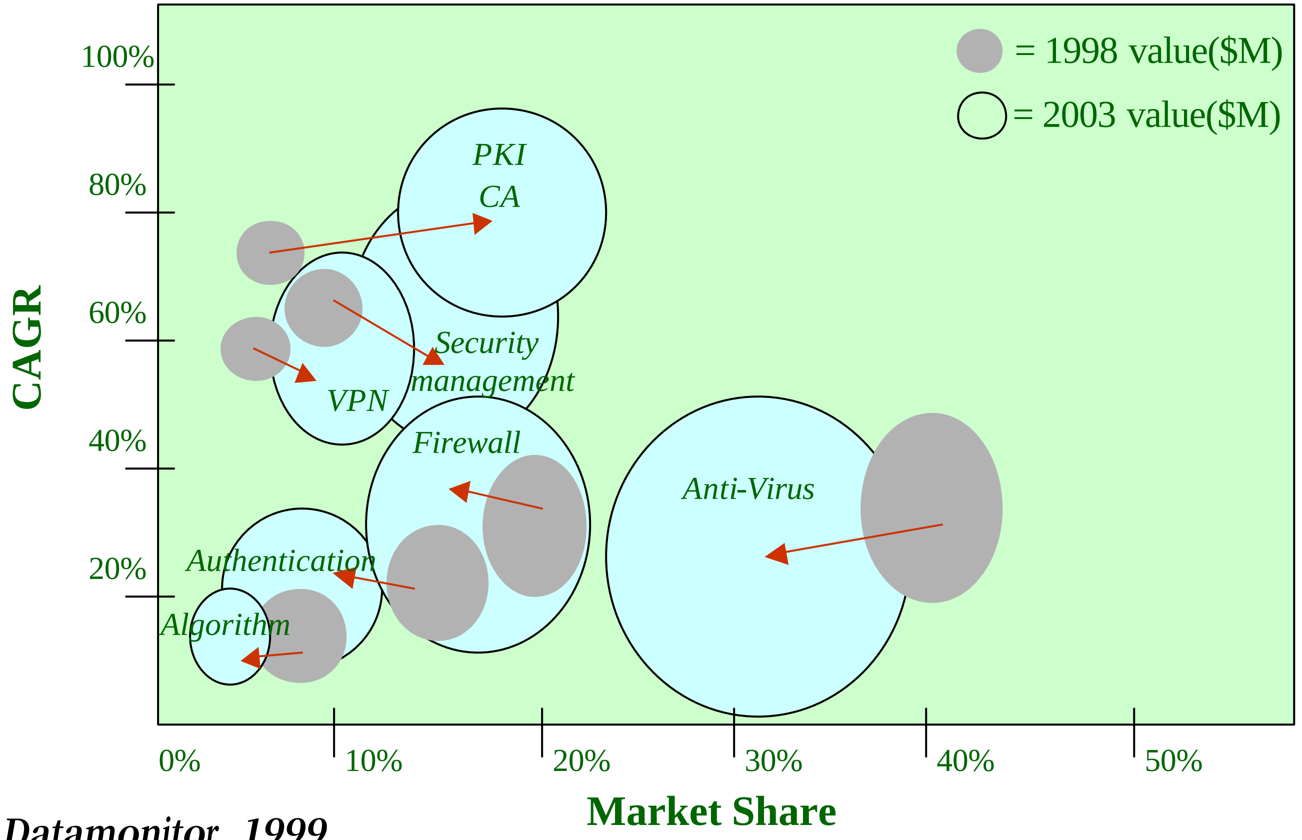
Beginning of next generation internet

Growth of next generation internet

2002

2005

Market of Anti-Cyber Terror products



※ *Datamonitor, 1999*

Products (1)

Firewall

- ☞ For protection of internal networks of company, bank…
  - ☞ Firewall-I(CheckPoint), Gauntlet(TIS)
  - ☞ 수호신(Securesoft), Secureworks(어울림)

IDS (Intrusion Detection System)

- ☞ For risk analysis and system security
  - ☞ Omniguard(Axent), RealSecure(ISS)
  - ☞ Siren(pentasecurity), Neowatcher(Inzen)

Products (2)

CA (Certificate Authority)

☞ PKI-based Authentication : Cyber Banking, EC

- ☞ VeriSign, CyberTrust
- ☞ TrustPro(SDS), ASSURE(Senextech)

Anti-Virus

- ☞ Norton Antivirus(Symantec), PC-Cillin(Trans)
- ☞ V3Pro(안철수), ViRobot(Hauri)

Products (3)

VPN (Virtual Private Network)

- ☞ Major network security system
  - ☞ Cisco1700series(Cisco), VPN-1(CheckPoint)
  - ☞ Secuwaysuite(Future System)

Current trend

- ☞ Increase of integrated security service
  - ☞ ESM (Enterprise Security Management)
  - ☞ Security Consulting

Evolution of IT

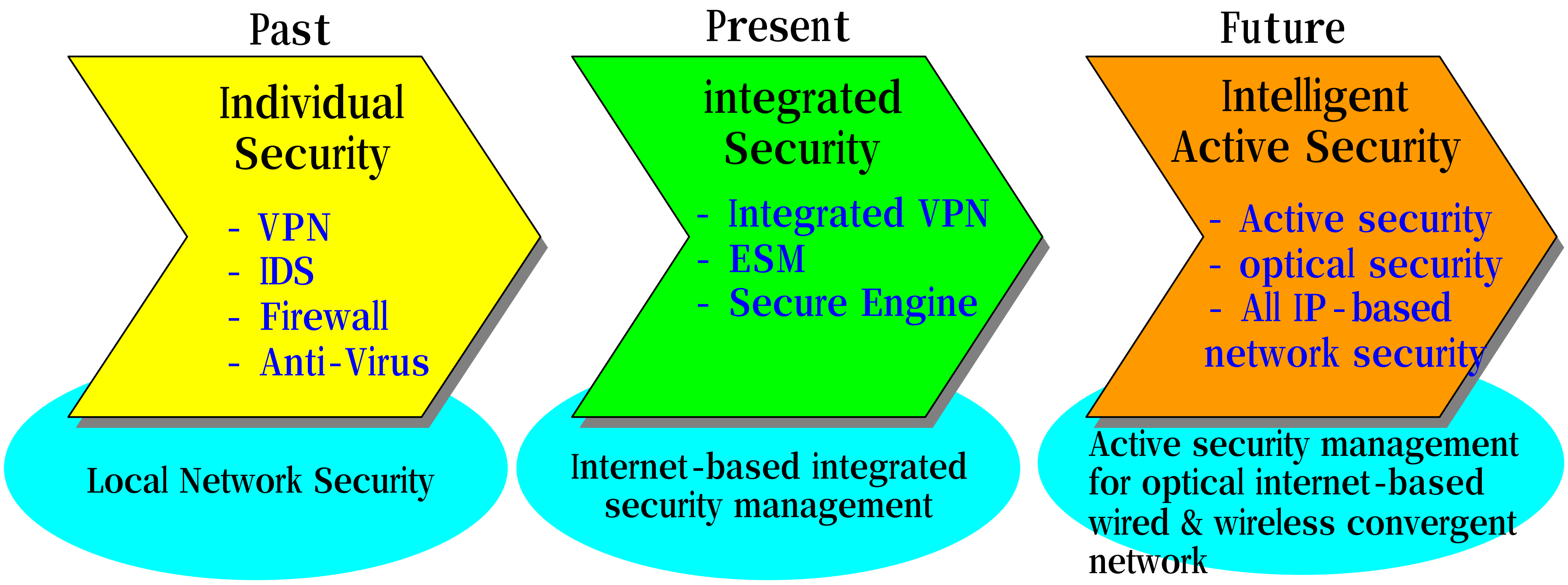
Progress of IT Environment

- ☞ Changing of IT infrastructure due to increasing internet traffic
  - ☞ WDM-based optical network
- ☞ Progress toward All IP-based wired & wireless convergent network
- ☞ Real feeling service by using BT-IT fusion technology

Progress of Security Technology

- ☞ Appearance of new security products due to changing IT environment
  - ☞ Becomes major part of communication system
  - ☞ Progress toward total security solution
- ☞ Increasing importance of network security service
- ☞ Passive security -> Active Security

Progress of Network Security



Past

Individual Security

- VPN
- IDS
- Firewall
- Anti-Virus

Local Network Security

Present

integrated Security

- Integrated VPN
- ESM
- Secure Engine

Internet-based integrated security management

Future

Intelligent Active Security

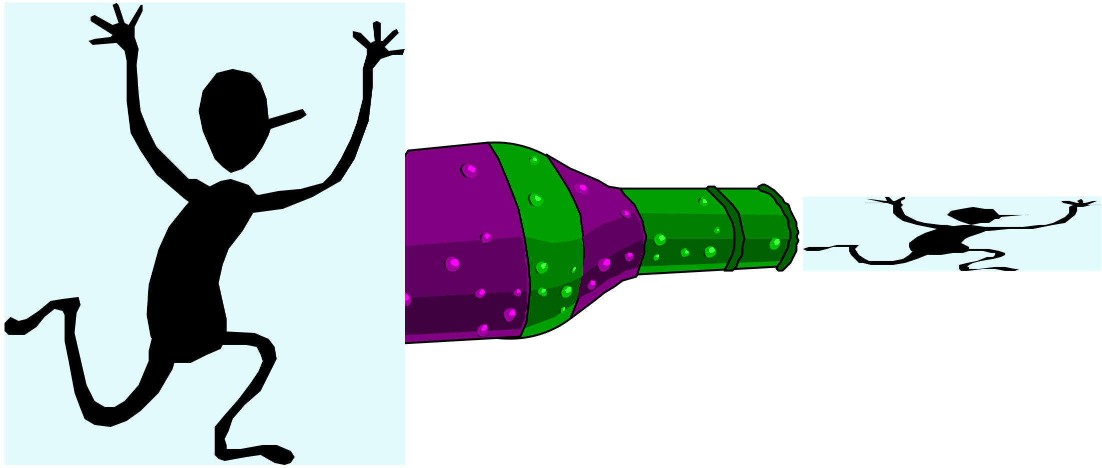
- Active security
- optical security
- All IP-based network security

Active security management for optical internet-based wired & wireless convergent network

Problems of Present Security Tech (1)

Reduction of network performance

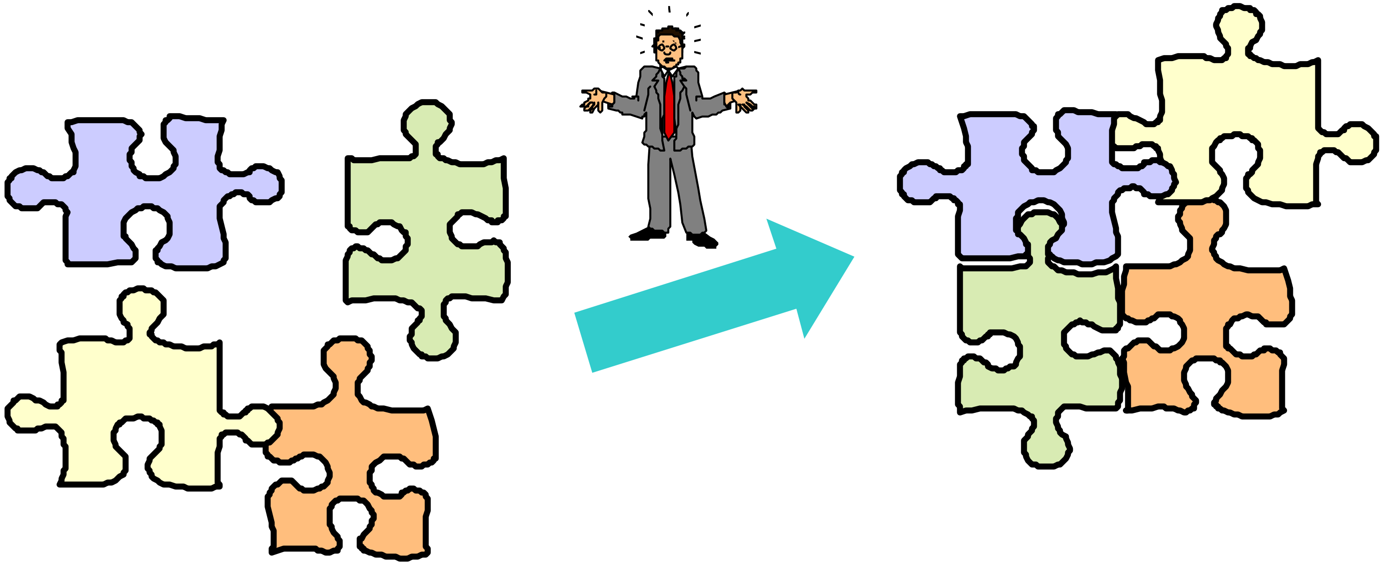
- ☞ As security function is placed in network edge point
  - ☞ Reduction of network performance is occurred
- ☞ As real time communication is difficult without secure OS & engine
  - ☞ Users do not want to use security system



Problems of Present Security Tech (2)

Hard to implement security infrastructure

- ☞ Security infrastructure needs many security functions
  - ☞ As Individual security system is made for single purpose security function
  - ☞ The individual systems can not interwork between them
- ☞ There are no functional regulations between security systems
  - ☞ Hard to implement security infrastructure



Problems of Present Security Tech (1)

No CC-based security system

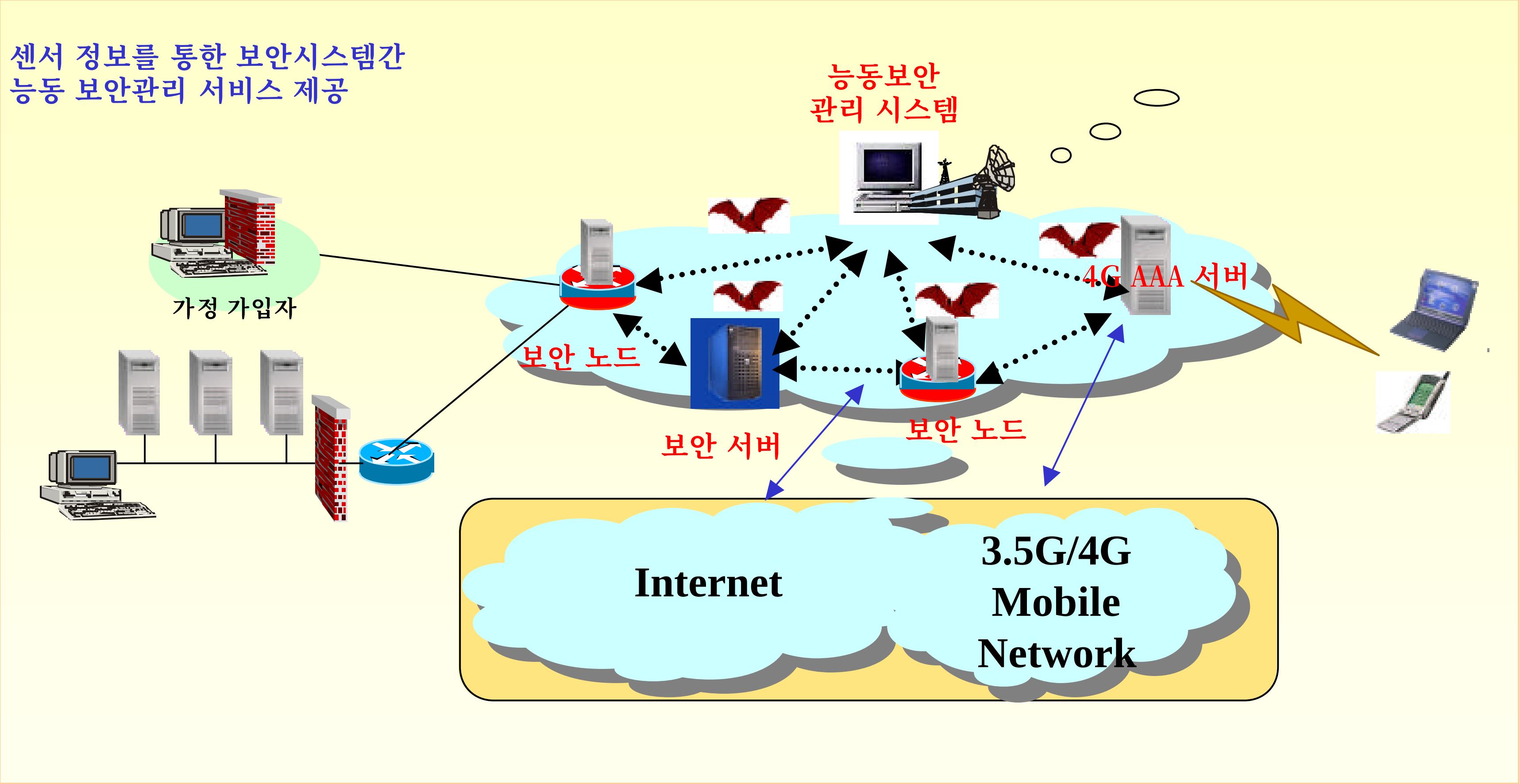
- ☞ Advanced countries develop CC-based security systems
  - ☞ To improve international competition and reliability
- ☞ In korea, there is no CC-based security system
  - ☞ Development of CC-based security system is required

* CC : Common Criteria

Needs of New Security Service

- Security Technology becomes
  - Major function of IT system
  - Basic service of IT service
- Next generation internet
  - Progresses toward All IP-based wired & wireless convergent networks
  - Needs secure logical connection based on the convergent networks
  - Needs new security service model
- Therefore, logical secure service network must be built by using Secure Networking and CC-based security service must be provided
  - Secure Networking for connection between internet nodes is needed to realize integrated intrusion protection and back-tracing
  - CC-based security system is needed to guarantee mutual connection between some different kinds of systems

Secure Networking Concept



Secure Networking Tech. Trend (1)

☞ Advanced countries have built Common Criteria Mutual Recognition Arrangement(CCMRA) for developing CC-based security systems and make a study of secure networking technology

Advanced Countries

☞ USA invests $67,000,000 in study of security technology(2000)

  ☞ HPCC, IT2 projects

☞ DARPA make a study of new security technology based on active security mechanism

☞ European Union invests 540,000,000 Euros in study of network security (2000)

•*HPCC : High Performance Computing & Communication*
•*IT2: Information Technology 2*

Secure Networking Tech. Trend (2)

- ITO of DARPA make a study of secure networking for network security and survivability
- Research goal
  - Network Fault-Tolerant Survivability
  - Denying Denial-of-Service
  - Active Network Response

Program	# of projects	Investment	Participants
FTN	23	500M$ (2000~200	NAI, Telcordia, Princeton Univ.
DC	21	4)	Telcordia, Stanford, Xerox Palo Alto
AN	59	-	MIT, CMU, NAI, U.Penn

-

FTN : Fault Tolerant Network
AN : Active Network
DC : Dynamic Coalition

Domestic Research Trends

- ☞ Some security products have got domestic evaluation level
- ☞ No international mutual certification

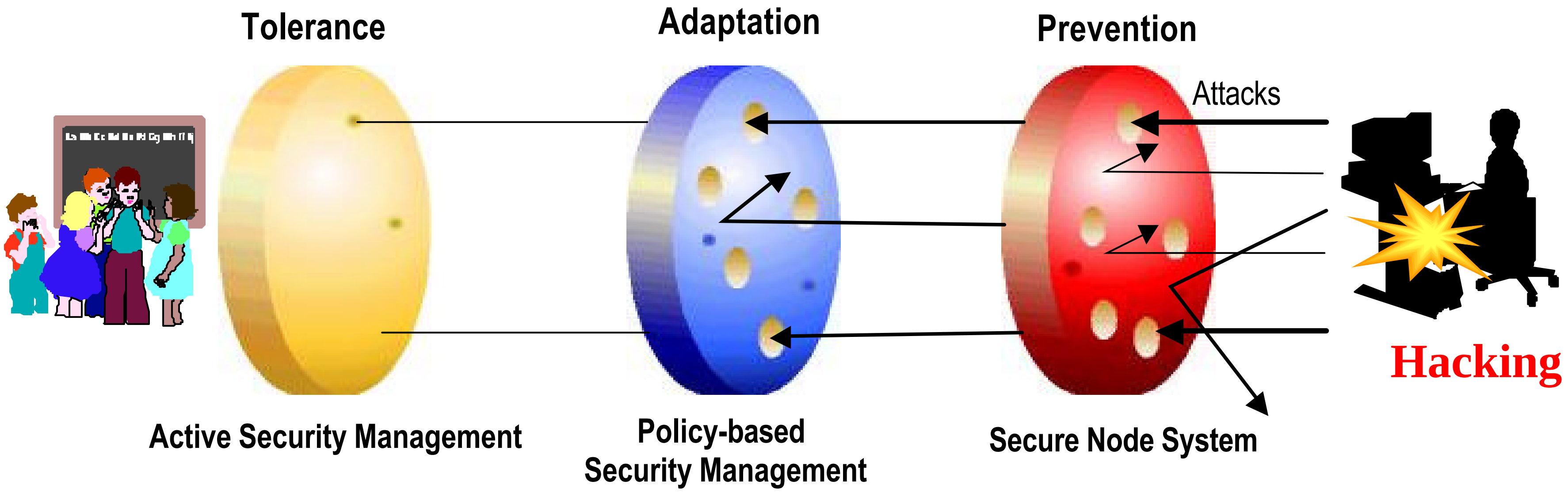
Domestic

- ☞ Some security products have got domestic evaluation level which is not international mutual certification
- ☞ There is no CC-based security system
- ☞ Secure networking is under technical consideration

Secure Networking Technology

Principal Core Technology

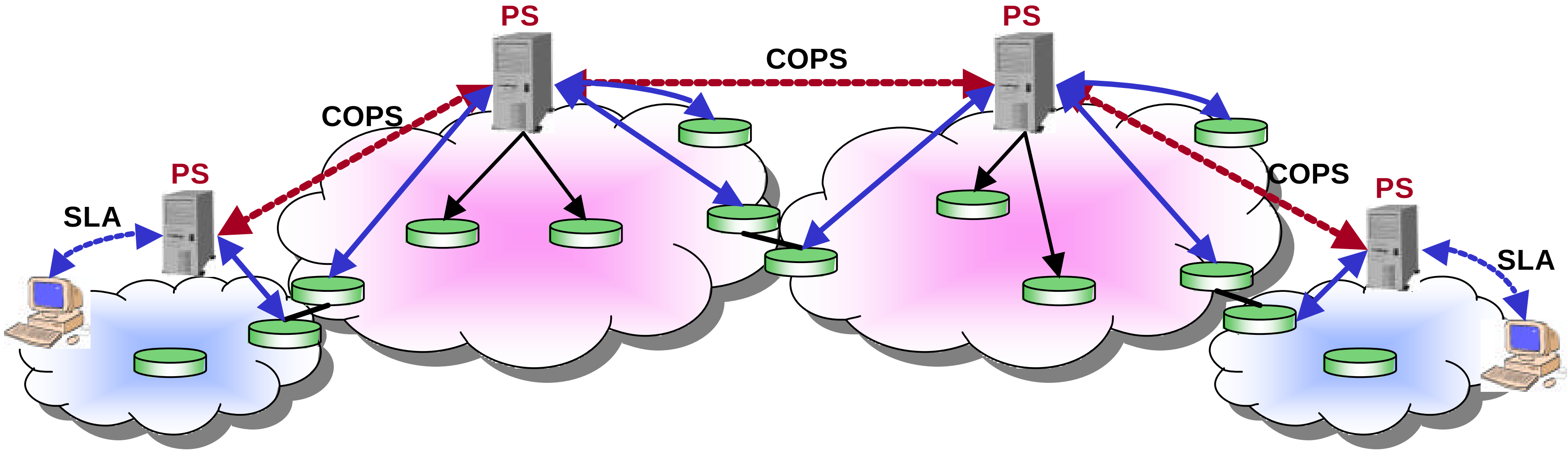
- ☞ Policy-based optical internet security management
- ☞ Active security management
- ☞ Optical Security
- ☞ CC-based secure node system



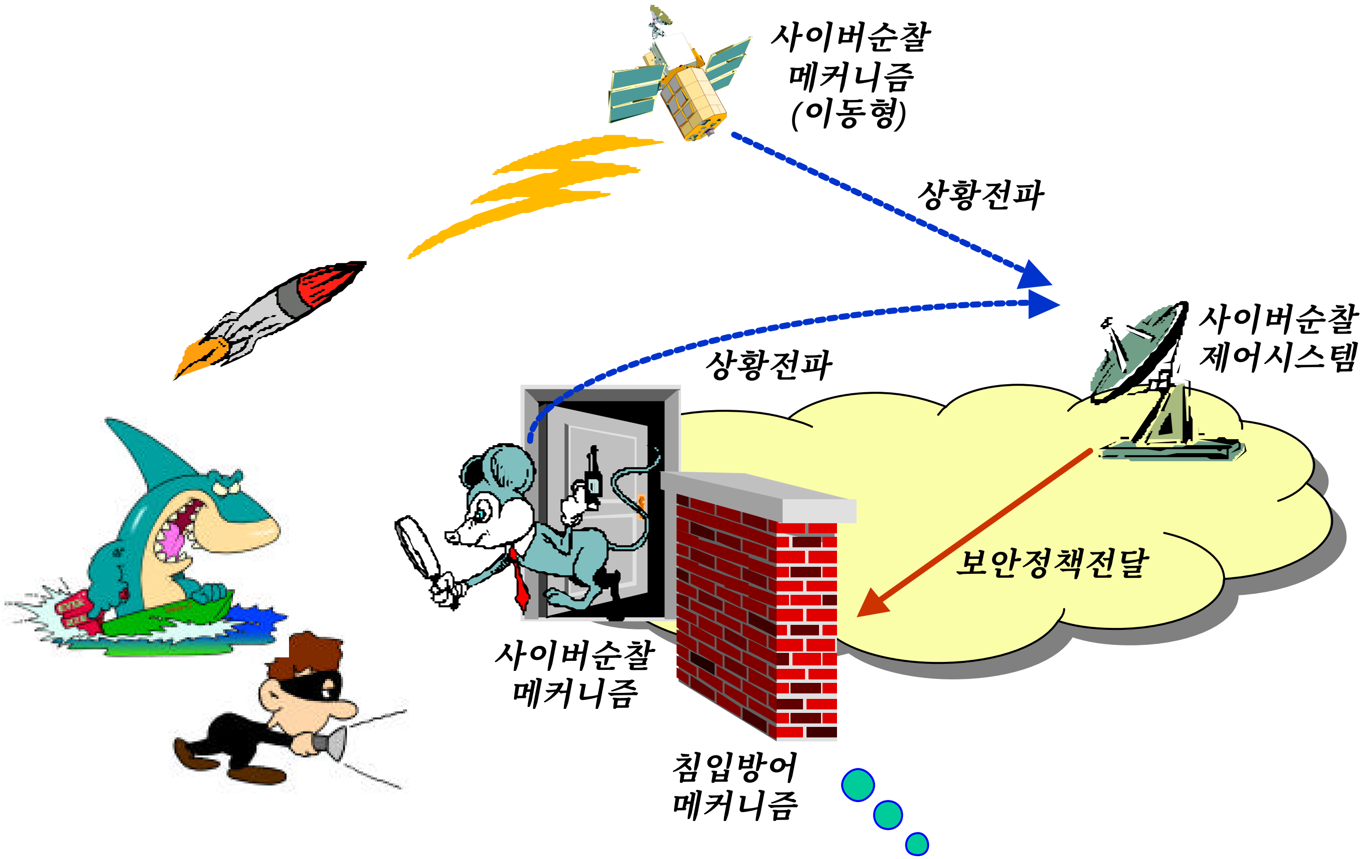
Policy-based Optical Internet Security Management

Policy-based Network Management Trend

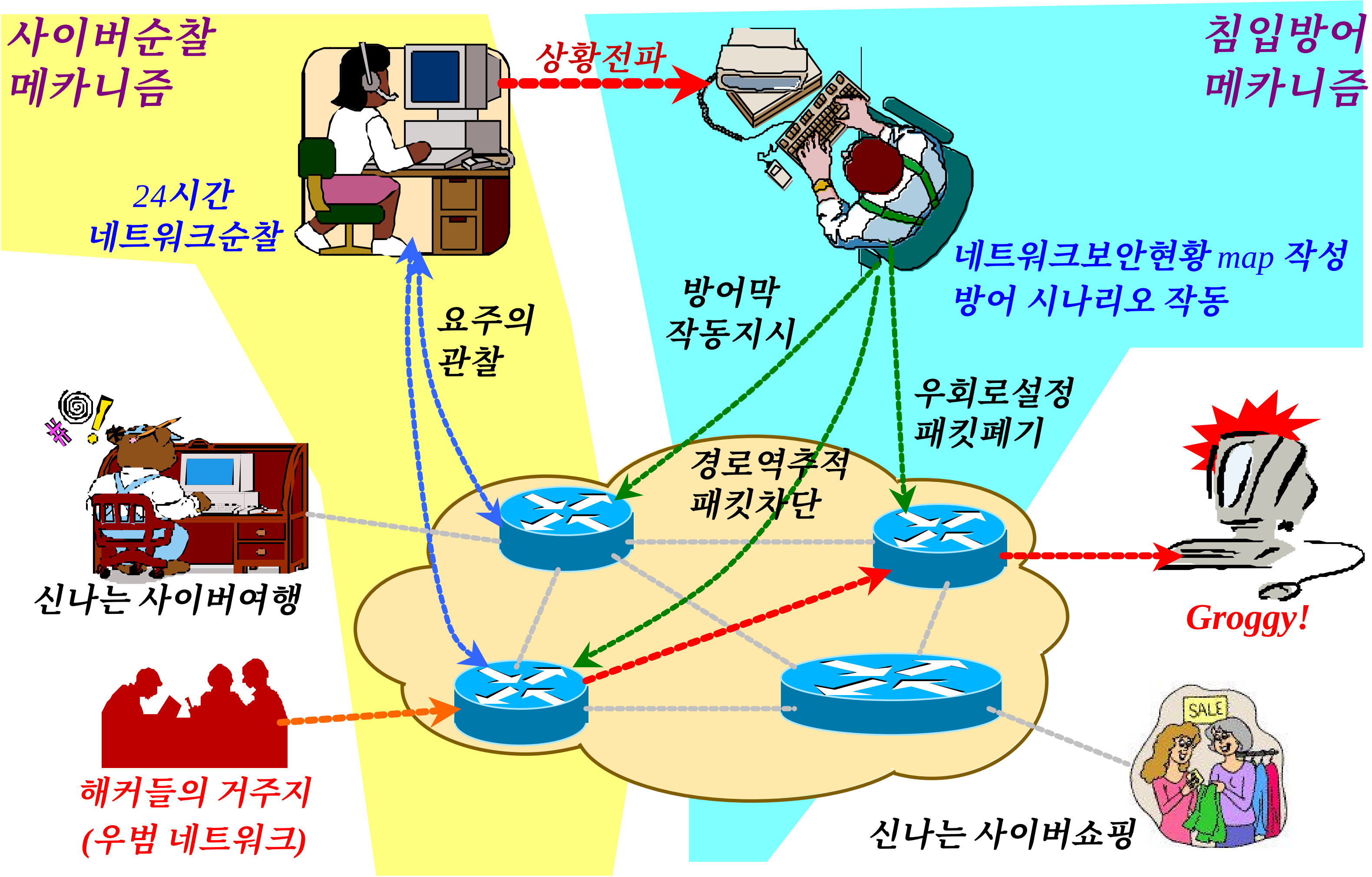
- ☞ Advanced countries
  - ☞ Policy-based Network Management : HP, Extreme Networks, Cisco, Orchestream, Intel
  - ☞ Policy-Framework : IETF Policy, DiffServ WG
  - ☞ Application Networks : vBNS, CA*net II, TEN-155



Policy-based Security Management Concept (1)



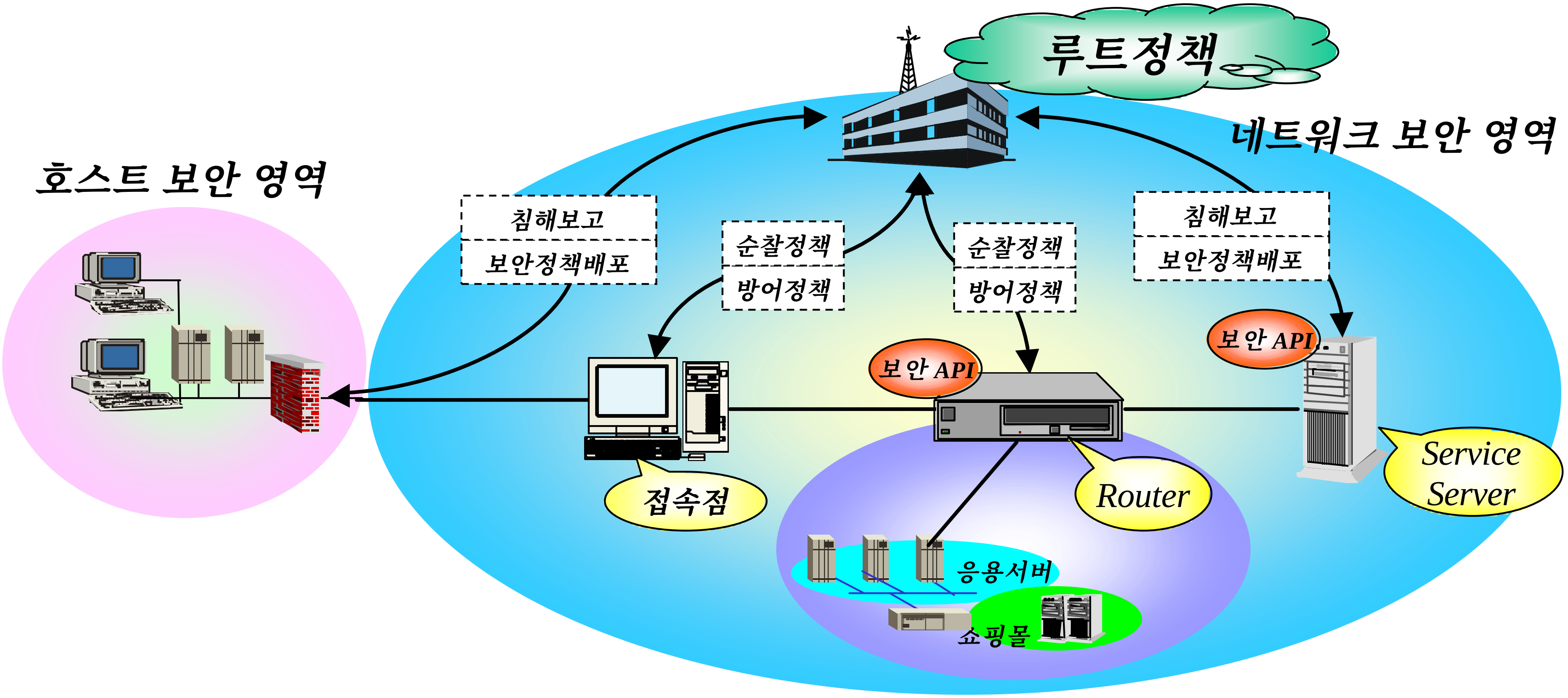
Policy-based Security Management Concept (2)



Policy-based Security Management Concept (3)

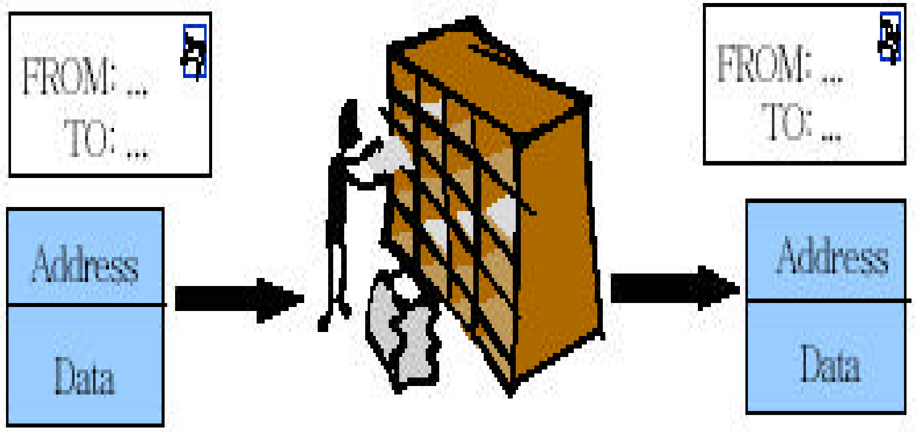
- *Individual Security Management*

  ➡ *Integrated Security Management*



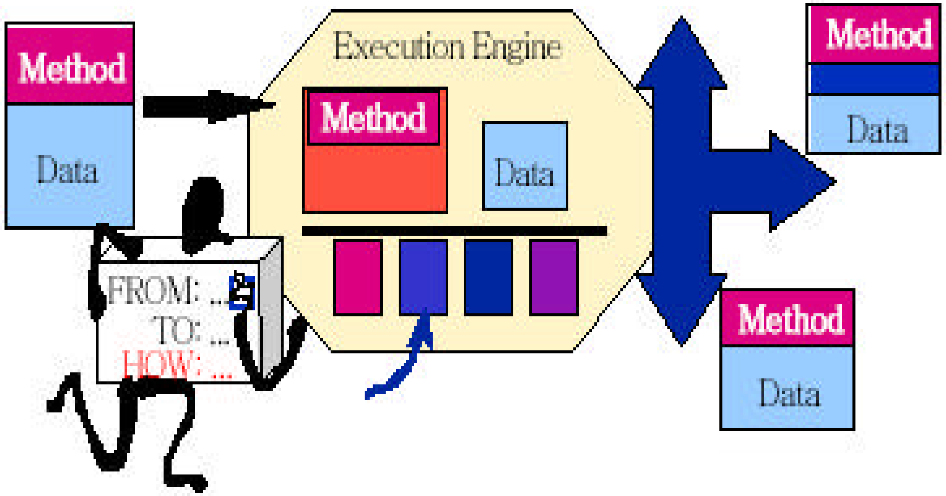
Active Security Management

Active Network Concept (1)



Present Network

- ☞ All packets are processed by an identical method
- ☞ Passive network management



Active Network

- ☞ Real time transformation according to user requirement
- ☞ Flexible active network

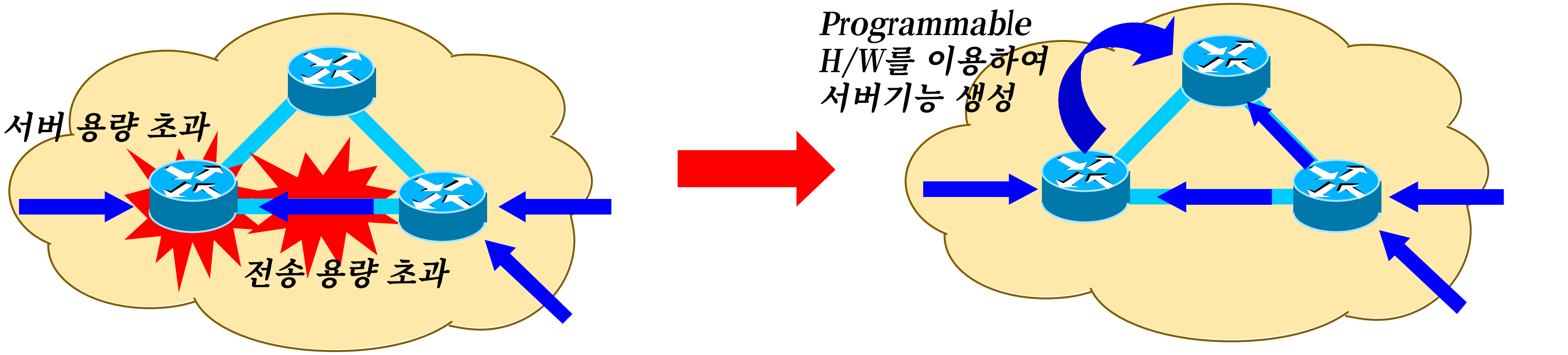
Active Network Concept (2)

Present Network

☞ Hard to respond actively to traffic variations
☞ Hard to accept new service quickly

Active Network

☞ Real time modification of network function can be possible
☞ Can respond actively to traffic variations that cannot been foreseen



Active Security Management

☞ **Active Security Management**

- ☞ **ASM = Active Network Technology + Active Security Technology**
- ☞ **Active sensor network engine**

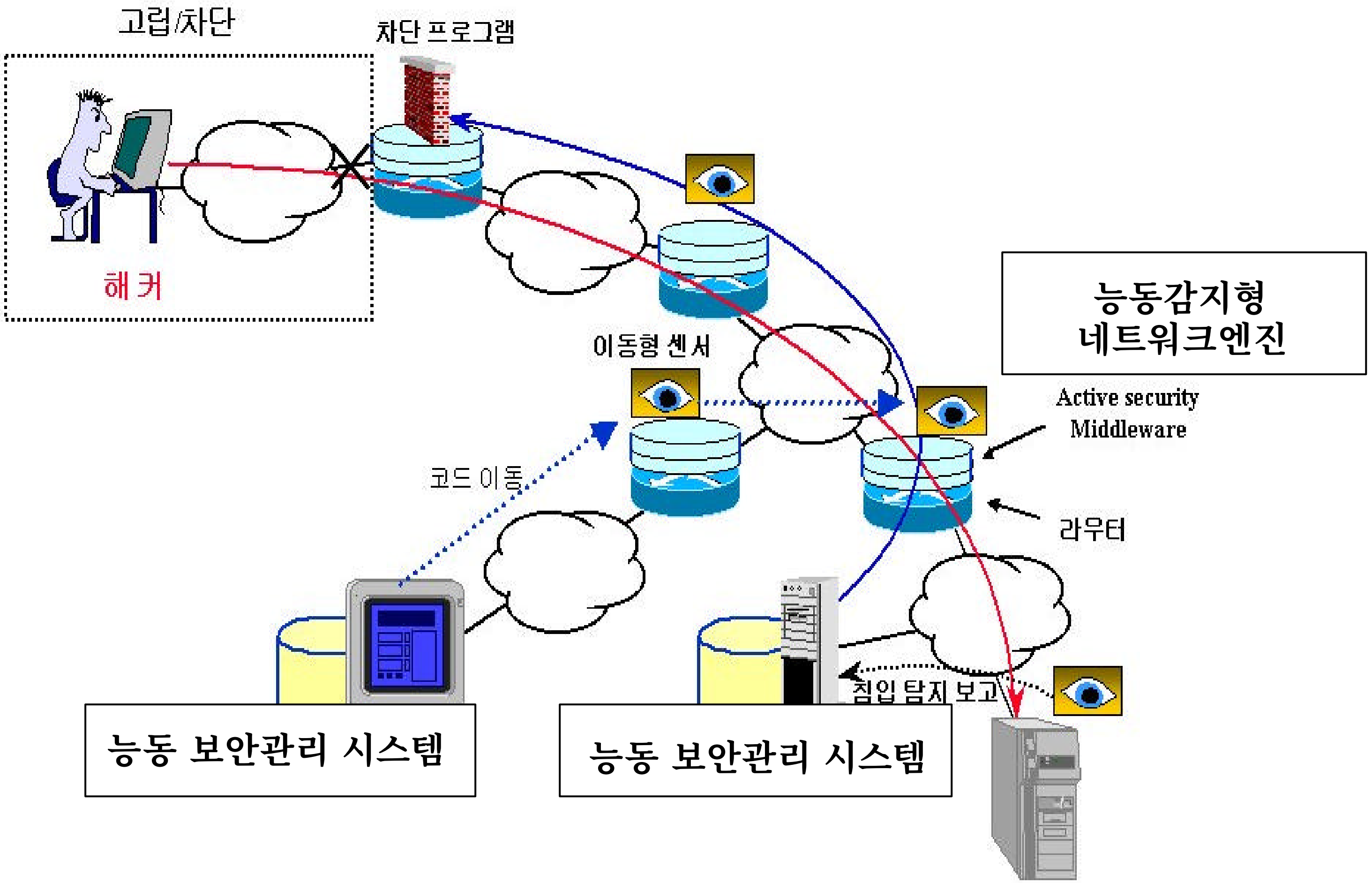
  Performs active security management in real time without regard to network status and kinds of platform
- ☞ **Active sensor programming language**

  Is the description language for programming security mechanism and active security service
- ☞ **Active security management system**

  Performs active security management and control using mobile sensor technology, active sensor network engine, and active security core technology

Active Security Management Concept

☞ Active security management by using mobile sensor technology

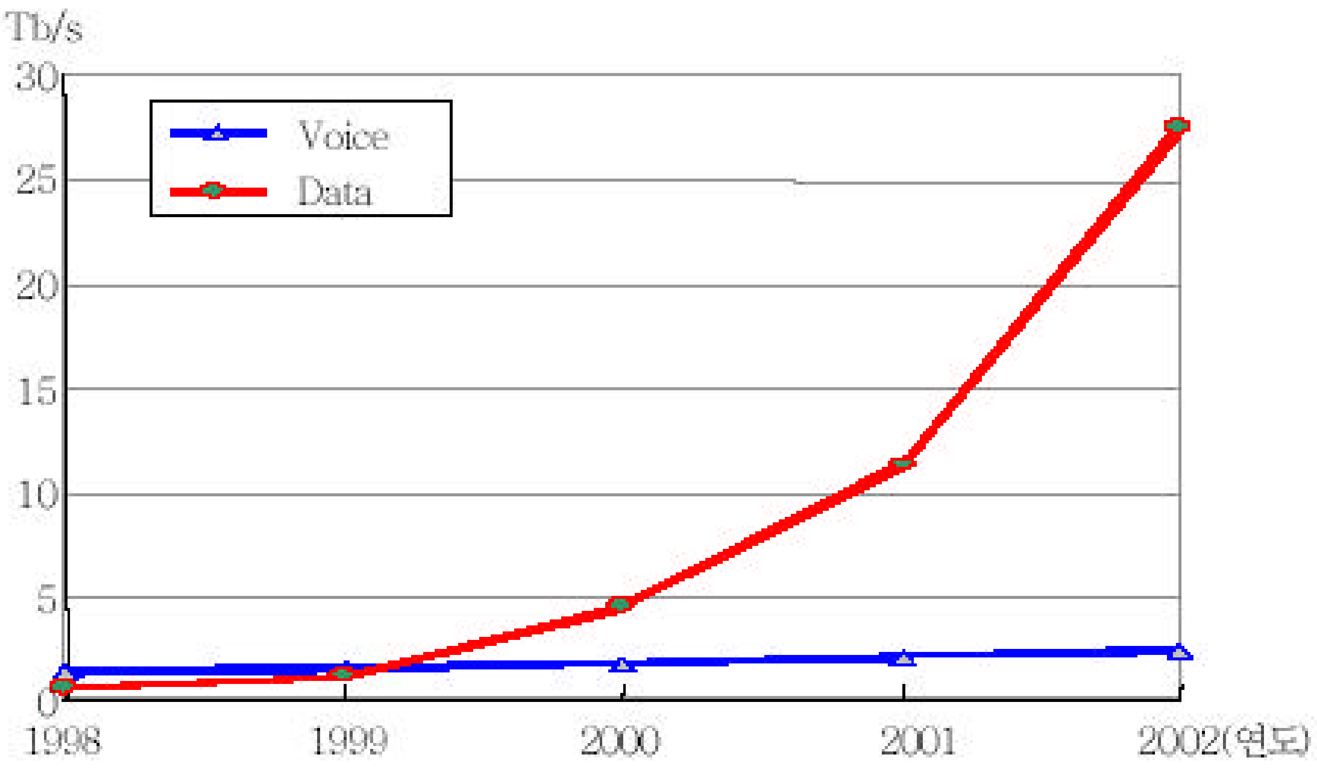


Research Trends

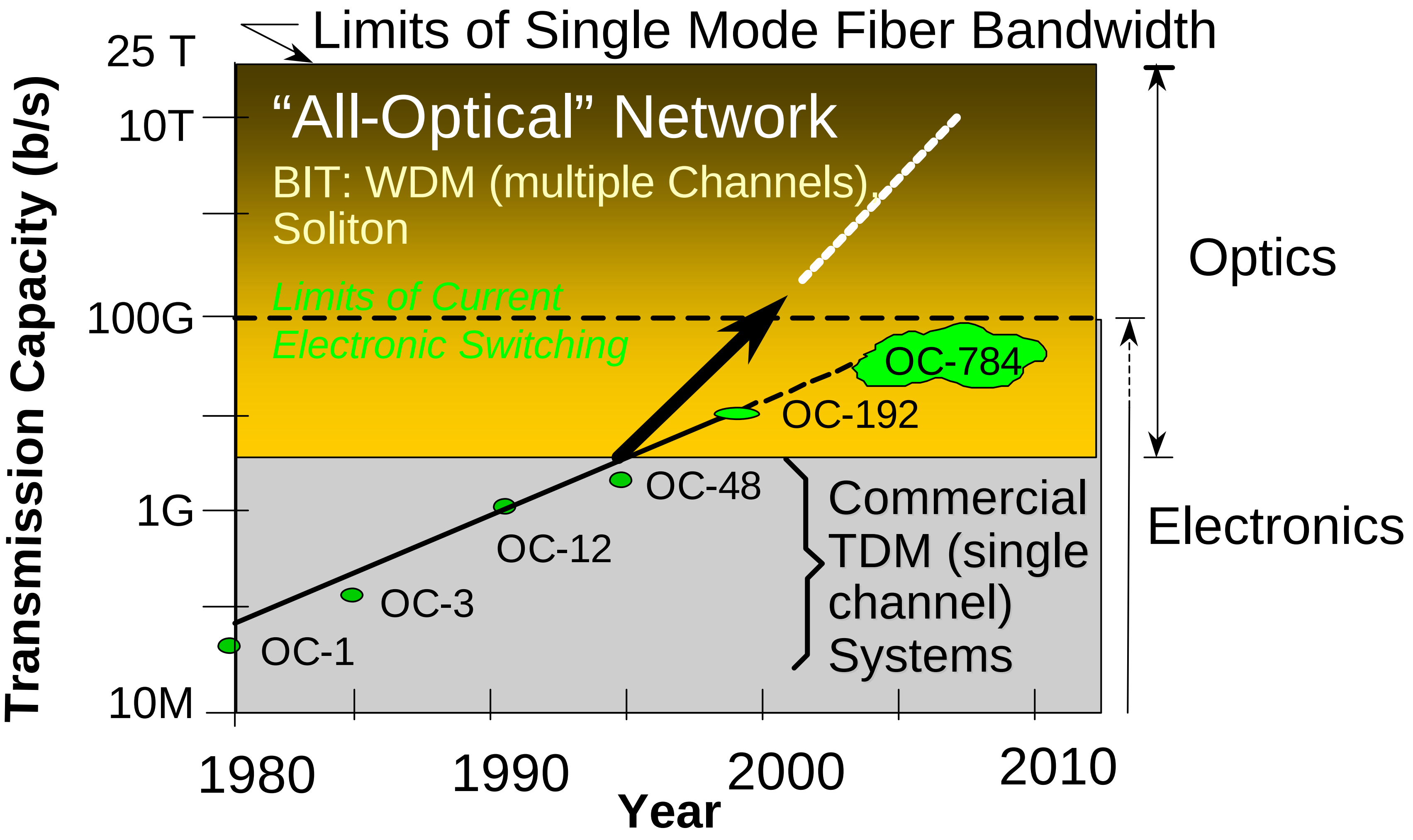
- Active Network
  - ITO of DARPA make a study of secure networking (1994)
  - Participants : MIT, Bellcore, BBN. UCLA, Columbia, TASC, UArizona
- FAIN (Future Active IP Networks) project
  - European Union performs Information Society Technologies (IST) program
  - Develop active node-based ‘reliable, secure, manageable network architecture’
  - Participants : T-Nova Deutsche Telekom, France Telecom, Hitachi Europe Ltd., University College London, Jozef Stefan Institute
- MIRAInet
  - Is next network solution (1999, NTT)
  - Adaptive network
- Domestic research trend
  - ETRI & some universities make a study of active network
  - There is no result about active network

Optical Security

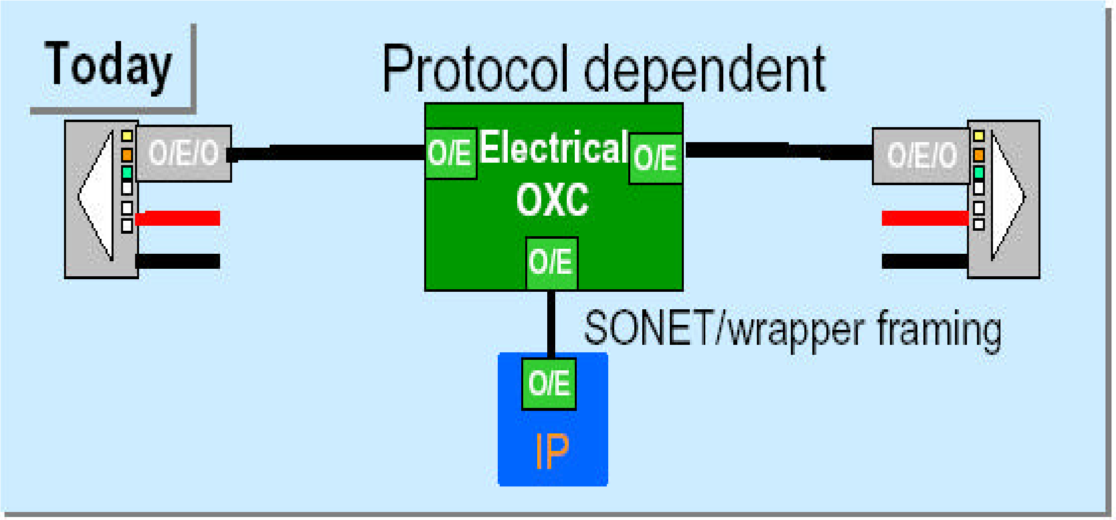
International IT traffic

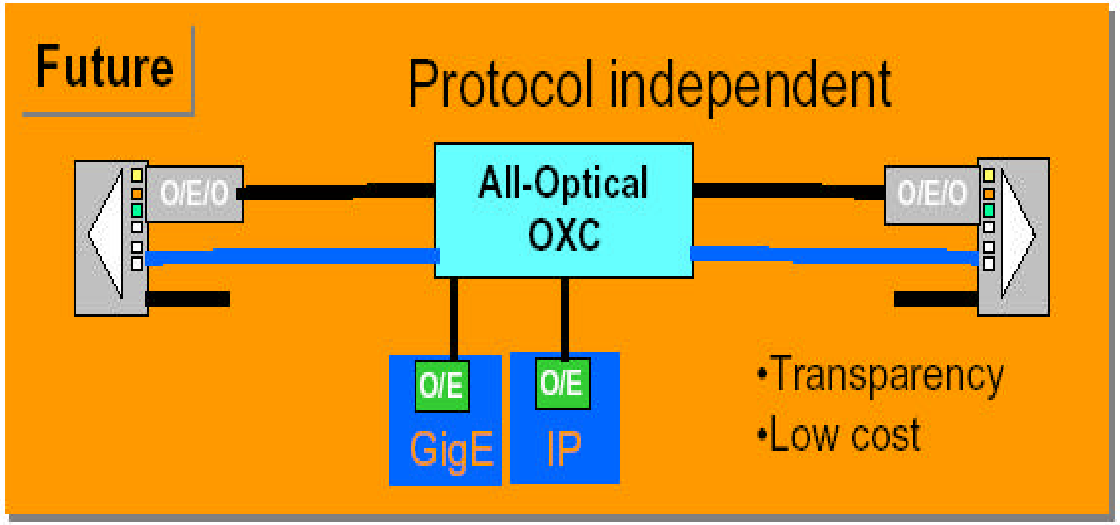


Evolution of Optical Internet

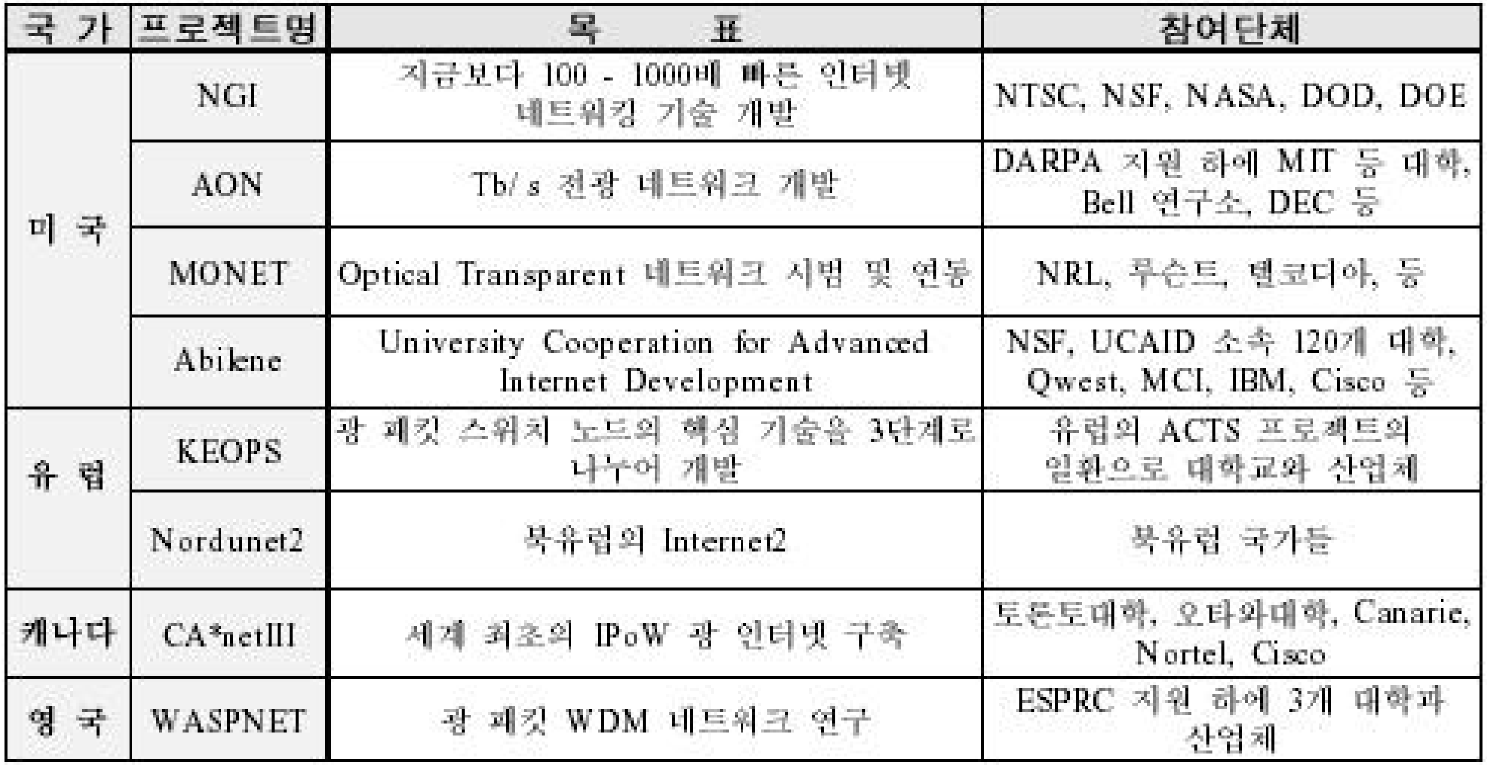


Comparisons



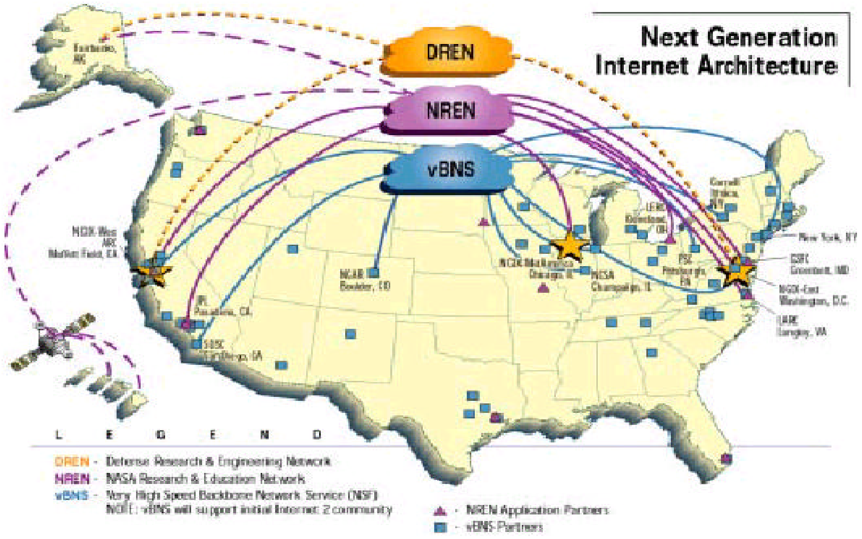


Optical Internet Testbed



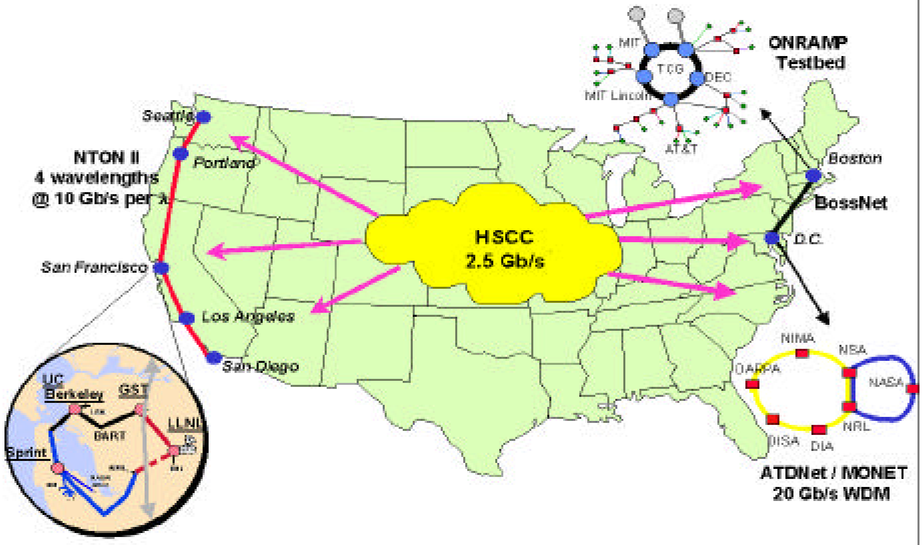
국 가	프로젝트명	목 표	참여단체
미 국	NGI	지금보다 100 - 1000배 빠른 인터넷 네트워킹 기술 개발	NTSC, NSF, NASA, DOD, DOE
	AON	Tb/s 전광 네트워크 개발	DARPA 지원 하에 MIT 등 대학, Bell 연구소, DEC 등
	MONET	Optical Transparent 네트워크 시범 및 연동	NRL, 루슨트, 텔코디아, 등
	Abilene	University Cooperation for Advanced Internet Development	NSF, UCAID 소속 120개 대학, Qwest, MCI, IBM, Cisco 등
유 럽	KEOPS	광 패킷 스위치 노드의 핵심 기술을 3단계로 나누어 개발	유럽의 ACTS 프로젝트의 일환으로 대학교와 산업체
	Nordunet2	북유럽의 Internet2	북유럽 국가들
캐나다	CA*netIII	세계 최초의 IPoW 광 인터넷 구축	토론토대학, 오타와대학, Canarie, Nortel, Cisco
영 국	WASPNET	광 패킷 WDM 네트워크 연구	ESPRC 지원 하에 3개 대학과 산업체

NGI Testbed (x1000)

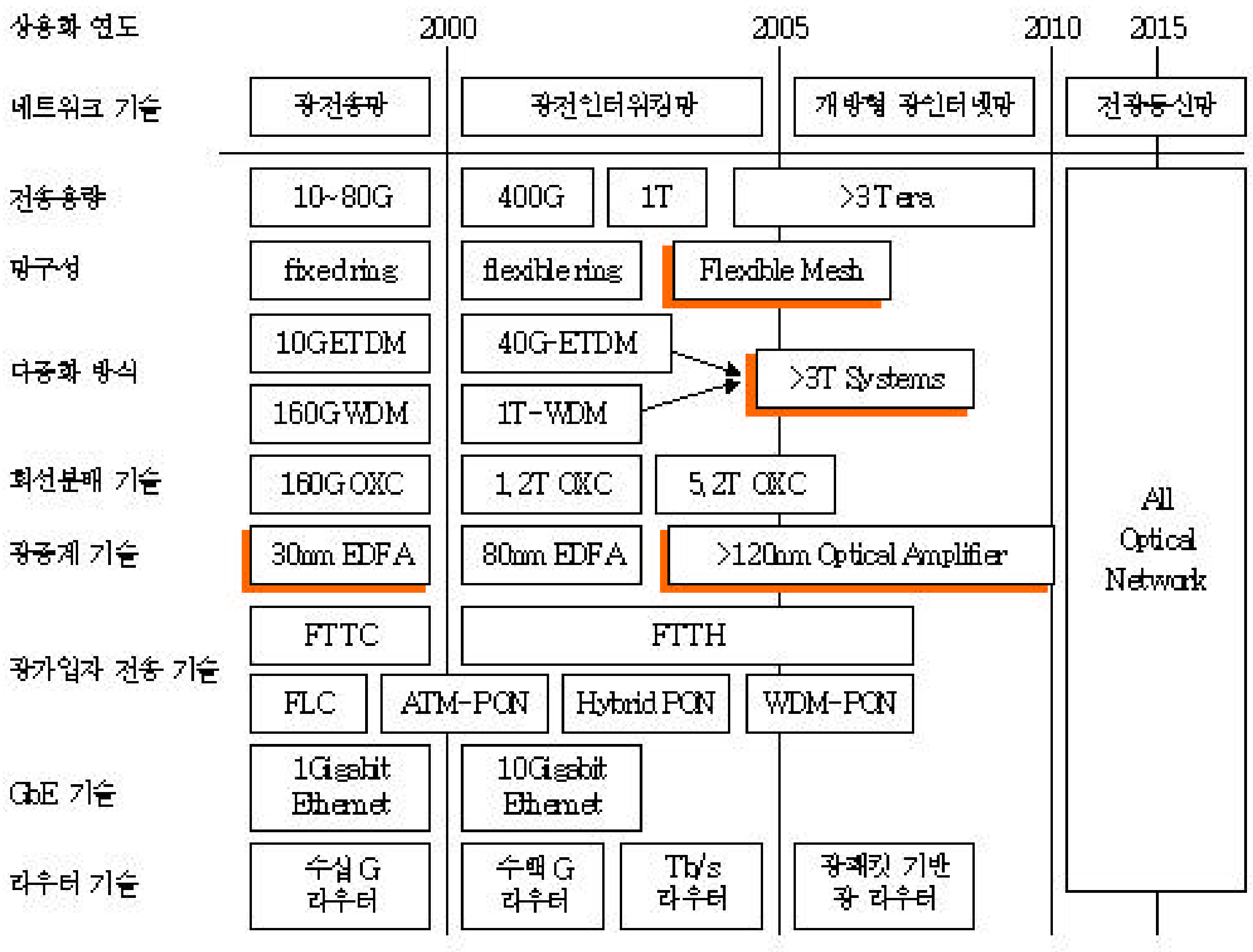

Next Generation Internet Architecture
DREN
NREN
vBNS
Fairbanks, AK
NGIX-West ARC Moffett Field, CA
JPL Pasadena, CA
SDSC San Diego, CA
NCAR Boulder, CO
NGIX-MidAmerica Chicago, IL
NCSA Champaign, IL
LERC Cleveland, OH
Cornell Ithaca, NY
PSC Pittsburgh, PA
New York, NY
GSFC Greenbelt, MD
NGIX-East Washington, D.C.
LARC Langley, VA
L E G E N D
DREN - Defense Research & Engineering Network
NREN - NASA Research & Education Network
vBNS - Very High Speed Backbone Network Service (NSF)
NOTE: vBNS will support initial Internet 2 community
▲ - NREN Application Partners
■ - vBNS Partners

X100 Testbed

X1000 Testbed



Directions of Optical Internet Development



상용화 연도: 2000, 2005, 2010, 2015

네트워크 기술: 광전송망, 광전인터워킹망, 개방형 광인터넷망, 전광통신망

전송용량: 10~80G, 400G, 1T, >3 Tera

망구성: fixed ring, flexible ring, Flexible Mesh

다중화 방식: 10G ETDM, 160G WDM, 40G-ETDM, 1T-WDM, >3T Systems

회선분배 기술: 160G OXC, 1.2T OXC, 5.2T OXC

광중계 기술: 30nm EDFA, 80nm EDFA, >120nm Optical Amplifier

광가입자 전송 기술: FTTC, FTTH, FLC, ATM-PON, Hybrid PON, WDM-PON

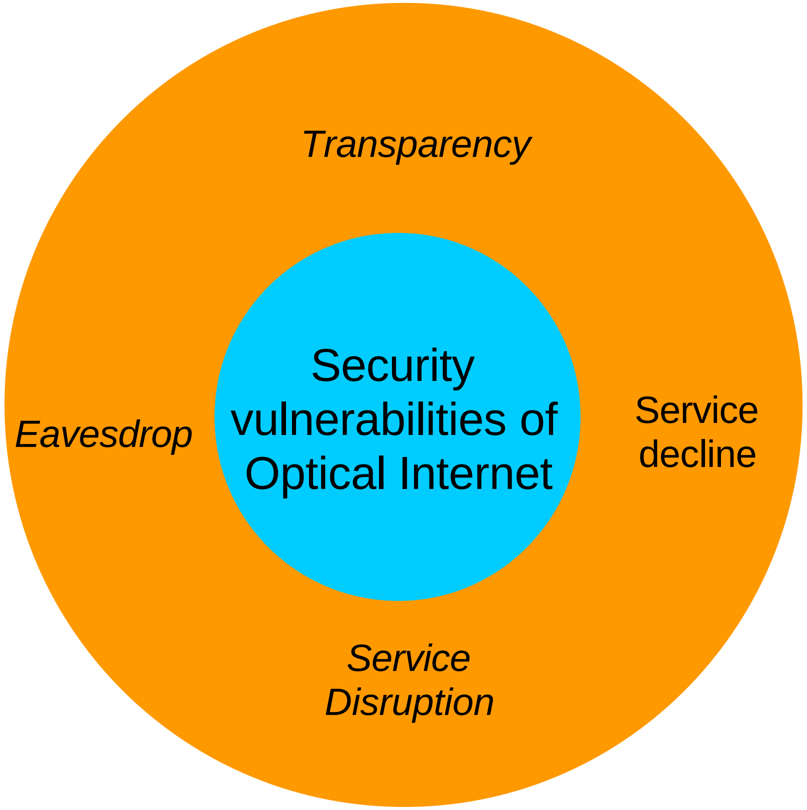
GbE 기술: 1Gigabit Ethernet, 10Gigabit Ethernet

라우터 기술: 수십 G 라우터, 수백 G 라우터, Tb/s 라우터, 광패킷 기반 광 라우터

All Optical Network

Security Vulnerabilities of Optical Internet

☞ **Vulnerabilities of Optical Internet ? Vulnerabilities of present Internet**

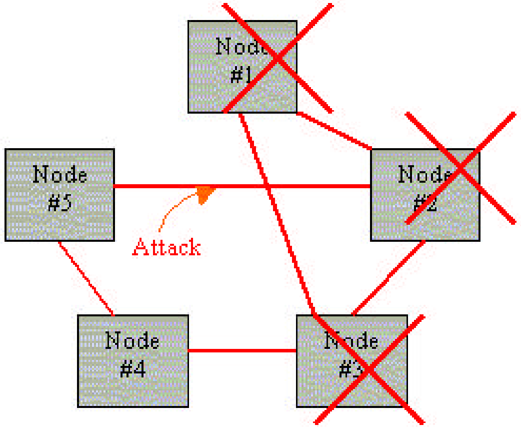

Transparency

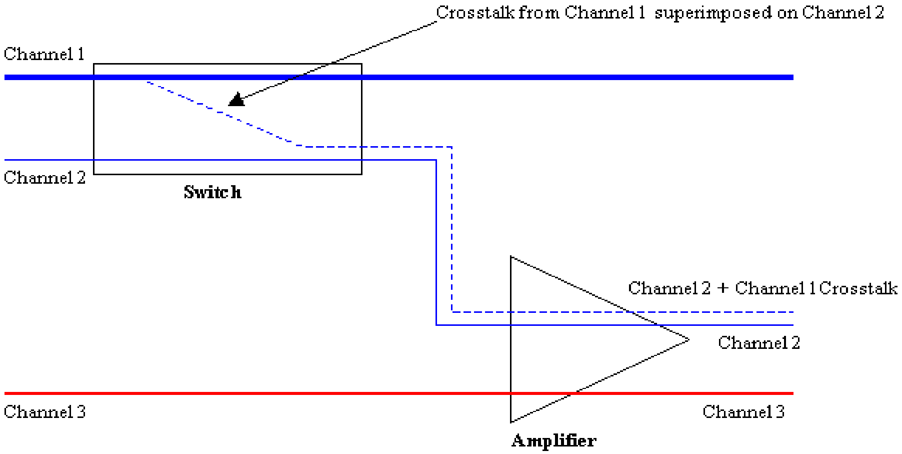
Eavesdrop

Security vulnerabilities of Optical Internet

Service decline

Service Disruption




Crosstalk from Channel 1 superimposed on Channel 2
Channel 1
Channel 2
Switch
Channel 2 + Channel 1 Crosstalk
Channel 2
Channel 3
Channel 3
Amplifier

Optical Security Concept

Needs

- ☞ Security vulnerabilities of optical internet are serious
- ☞ Tbps level encryption technology is needed for optical internet
- ☞ Absolutely secure crypto-algorithm is needed

Major Technologies

- ☞ Tbps level optical encryption technology
- ☞ Tbps level optical random generator
- ☞ Key distribution technology based on quantum cryptography
- ☞ Multi-dimensional encryption technology
- ☞ End-to-End optical crypto-system

The other technologies

The other technologies

- ☞ High secure crypto-algorithm
- ☞ Crypto-protocols for all IP wired & wireless convergent network
- ☞ Plug-in secure module
- ☞ Gbps level security on chip
- ☞ Secure OS
- ☞ Secure routing engine
- ☞ Secure gateway
- ☞ VPN service router
- ☞ Secure Node system
- ☞ Next generation wireless security technology
- ☞ Implementation of CC-based security system and standardization

Conclusions

Needs of Secure Networking Technology

- ☞ Individual security system -> multifunctional integrated security system
- ☞ New security mechanism is needed for mutual connection between security systems
- ☞ Functional regulations between security systems are needed
- ☞ Passive security system -> active security system
- ☞ CC-based security system for improving international competition

Core Technologies

- ☞ Policy-based optical network security management
- ☞ Active security management
- ☞ Optical security
- ☞ CC-based secure network node