Perspective on secure network for control systems in SPring-8

Toru Ohata, M. Ishii, T. Fukui* and R. Tanaka
JASRI/SPring-8, Japan
*RIKEN/SPring-8, Japan

Control system cyber-security workshop at Knoxville, USA
October 14, 2007

Contents

- Network architecture
  - Requirement and design concept
- Firewalling and network segregation
  - Logical network topology (Firewall, VLAN, NAT, etc.)
- Network segmentation
  - VLAN and IPS
    - Segmentation, Inspection and Quarantine
  - Authentication gateway for Wireless network
    - Private network segment
- Network monitor
  - Node management by MIB
  - Flow monitoring
- Patch management
  - Windows update, Anti-virus software
  - Mirror for packages and patches

Network architecture

Requirements

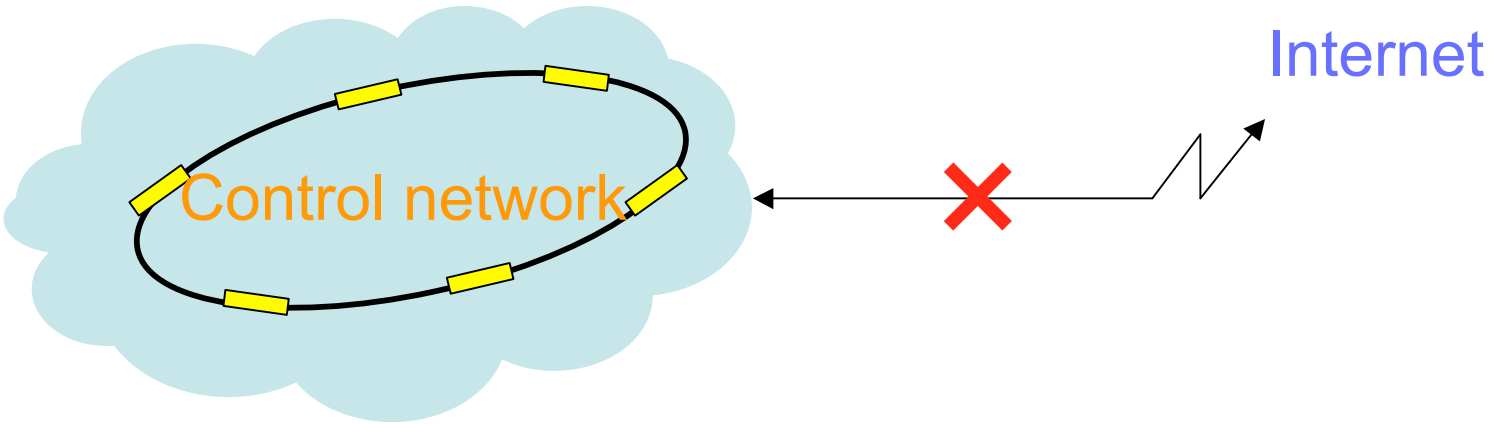
SPring-8 is the largest third-generation synchrotron radiation facility. Since the completion of the facility, many users have come for scientific experiment.

Functions required for network are

- accelerator and beamline control
- user's experiments and data acquisition
- facility management

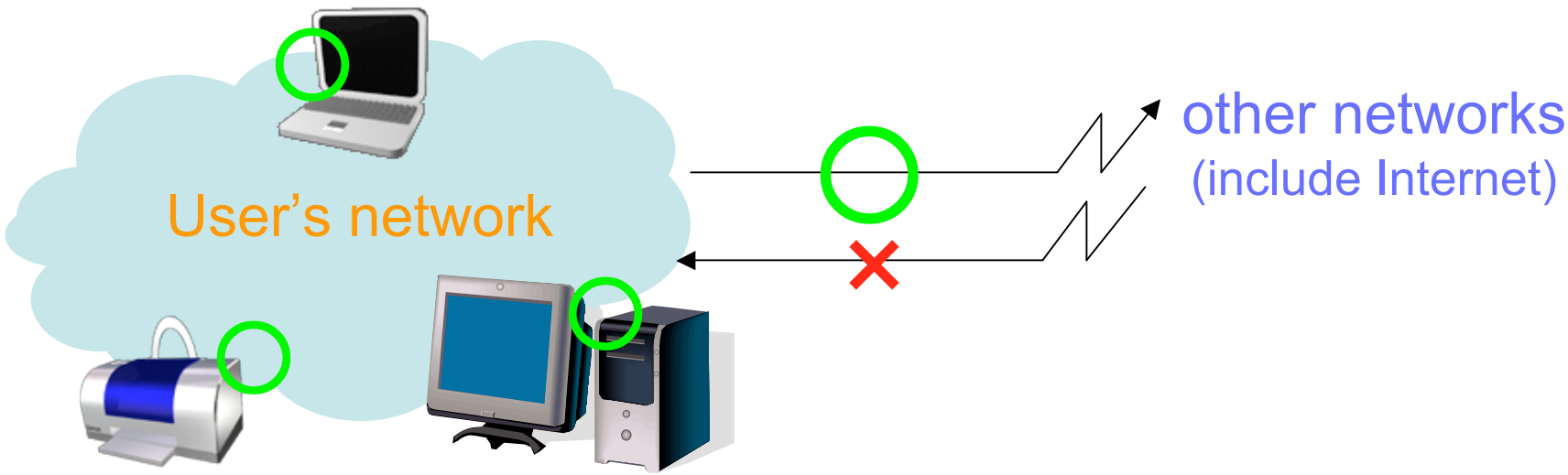
control network

- For facility management, isolation of control network is the most important
  - No needs to control the accelerators from the Internet
    - Except for recovery work at trouble (will be presented by A. Yamashita)



User's network

- User connects own PC to User's network for experiment and data analysis.
- User needs to connect with the Internet and other network resources from User's network
- User want to restrict arbitrary remote control from networks except for own User's network
  - need tunable access control from/to network resources

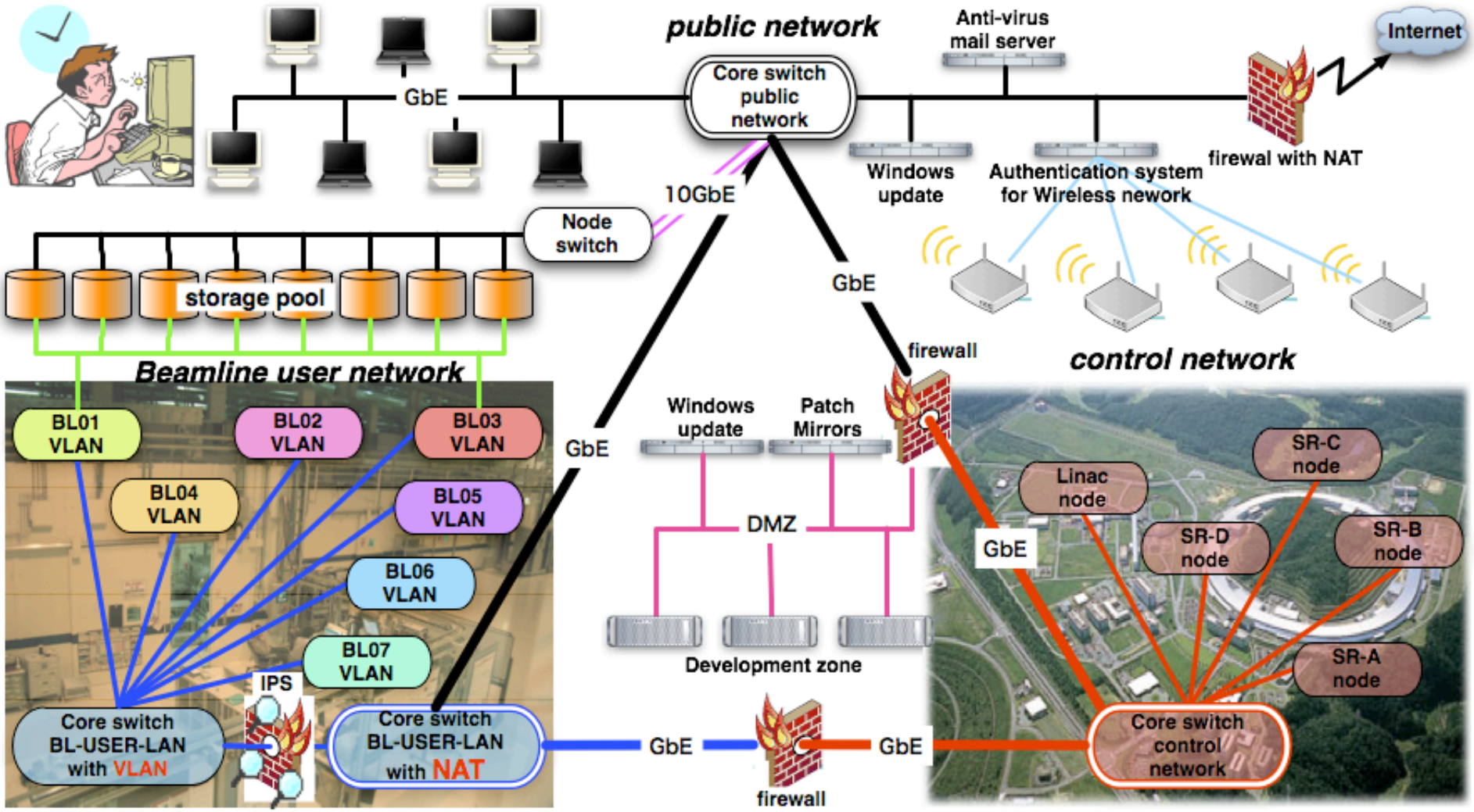


office network

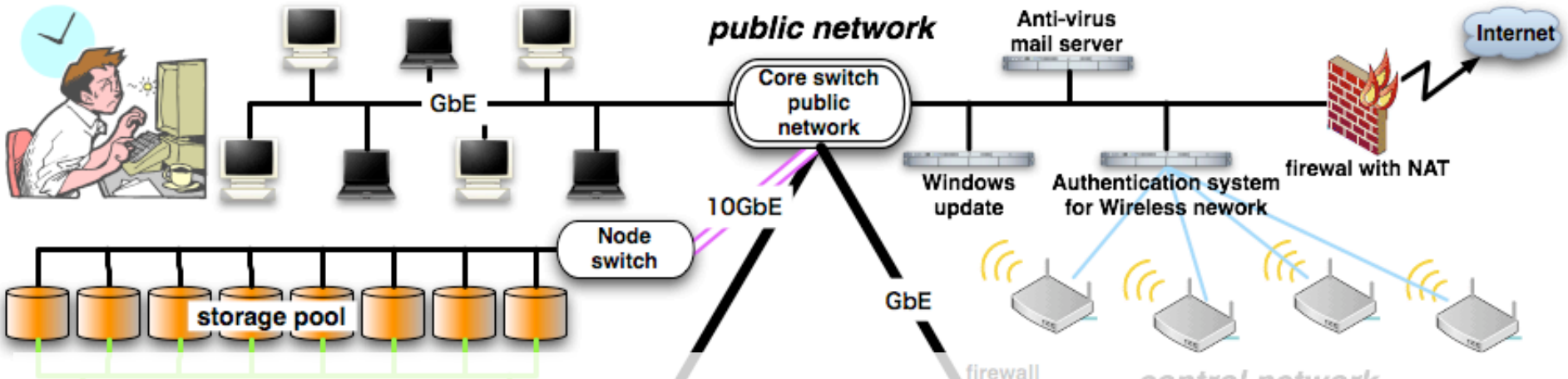
- Office network requires rich and secure information services for facility management
  - various information services
    - Name services Mail server with contents filter
      - Virus, spam mail filters
  - Wireless LAN service and Authentication system
  - Shared high speed storage for experiments

Firewalling
and
network segregation

Network topology



Network topology



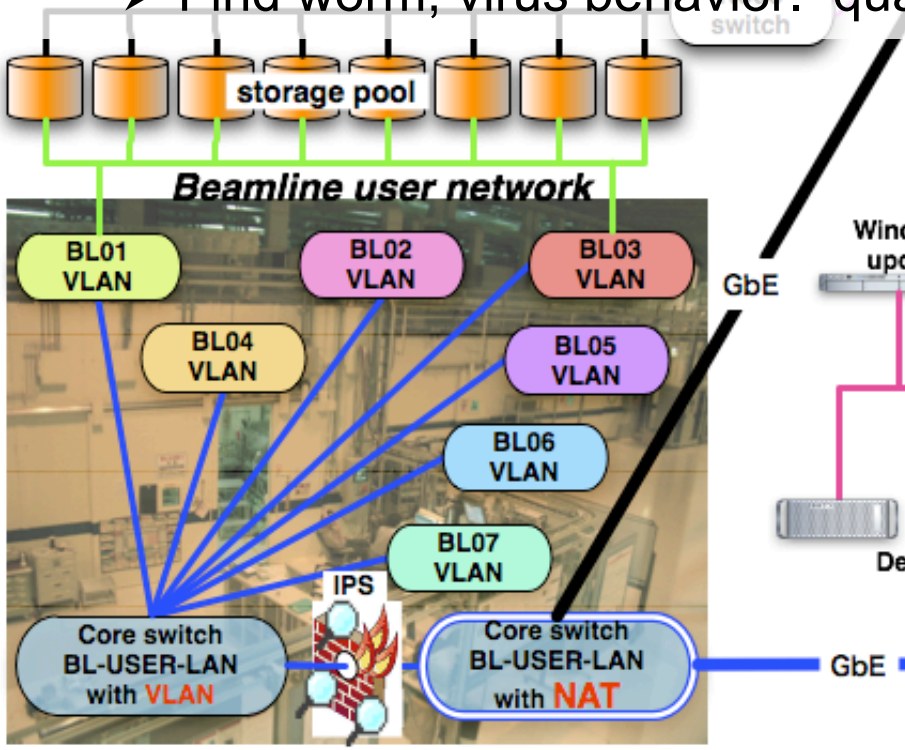
(public) Office network

- Firewall is installed to protect attack from Internet
- We have network services,
  - windows update push server
  - Authentication system for wireless LAN service
  - Shared storage pool for experimental users connected by 10GbE

Network topology

Beamline user's network

- NAT is installed to block connection from external network also enables to connect to external network freely
- IPS is installed to inspect user's PCs
  - ➢ Find worm, virus behavior. quarantines infected PCs to protect network

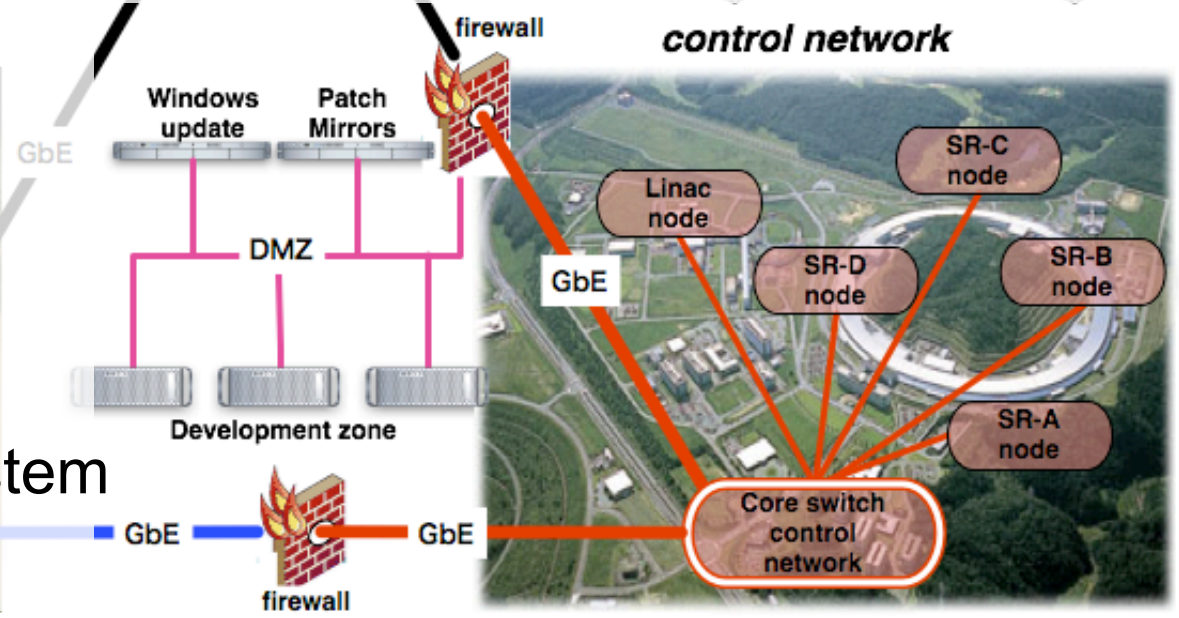


- VLAN keeps beamlines independent
  - ➢No routing between BLs
- Some BL directly connects to shared storage pool for high speed data acquisition (BL-DAQ-LAN)
  - ➢No bridge function between networks

Network topology

Control network

- Two sets of firewalls are installed to separate from office network and user's network
- The firewall has demilitarized network segment for development and some network services
  - windows update push server
  - Mirror servers for patch
- Flat network topology to simplify network management
- Low latency switched network
- Network monitoring system by MIB and sFlow



Network segmentation

Network segmentation

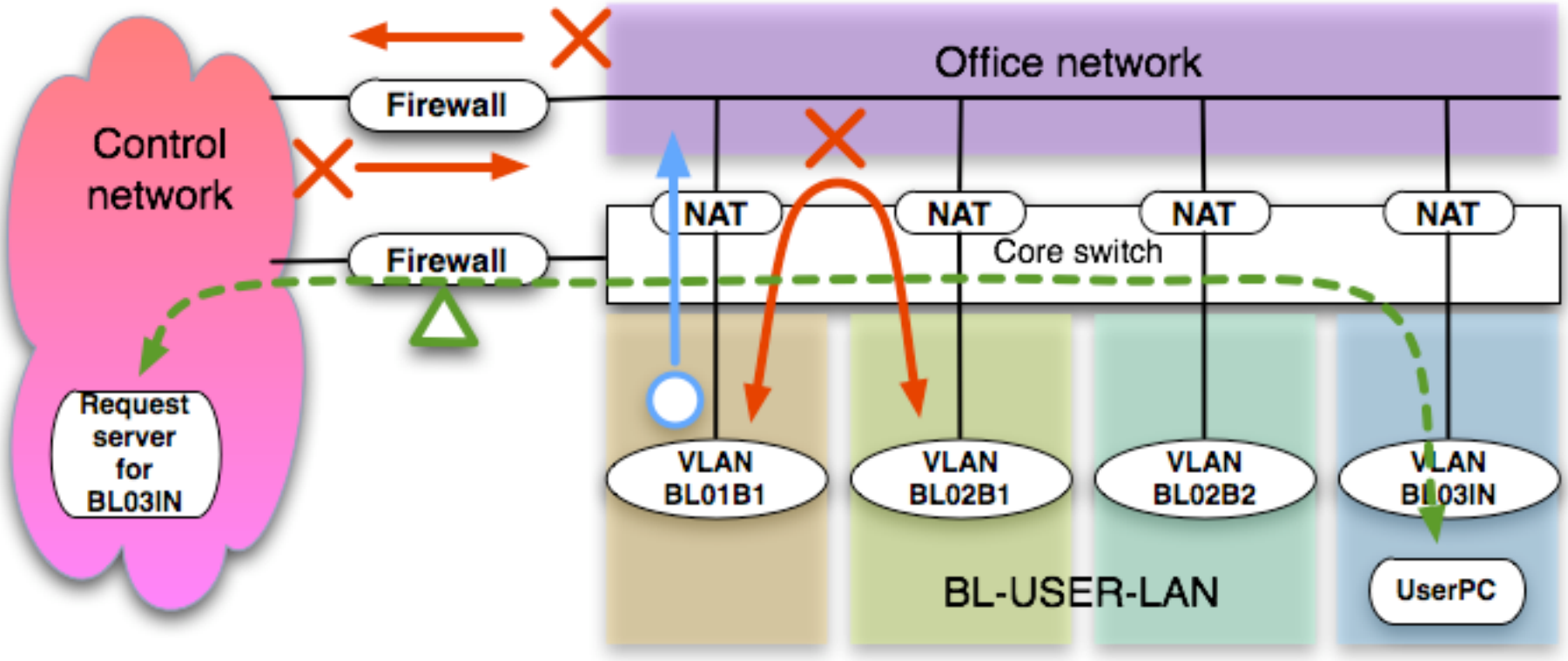
VLAN: Each beamline has independent network segment

User can access to external network

User can not connect between beamlines

Firewall: Control network is separated by others

permits access between specific hosts

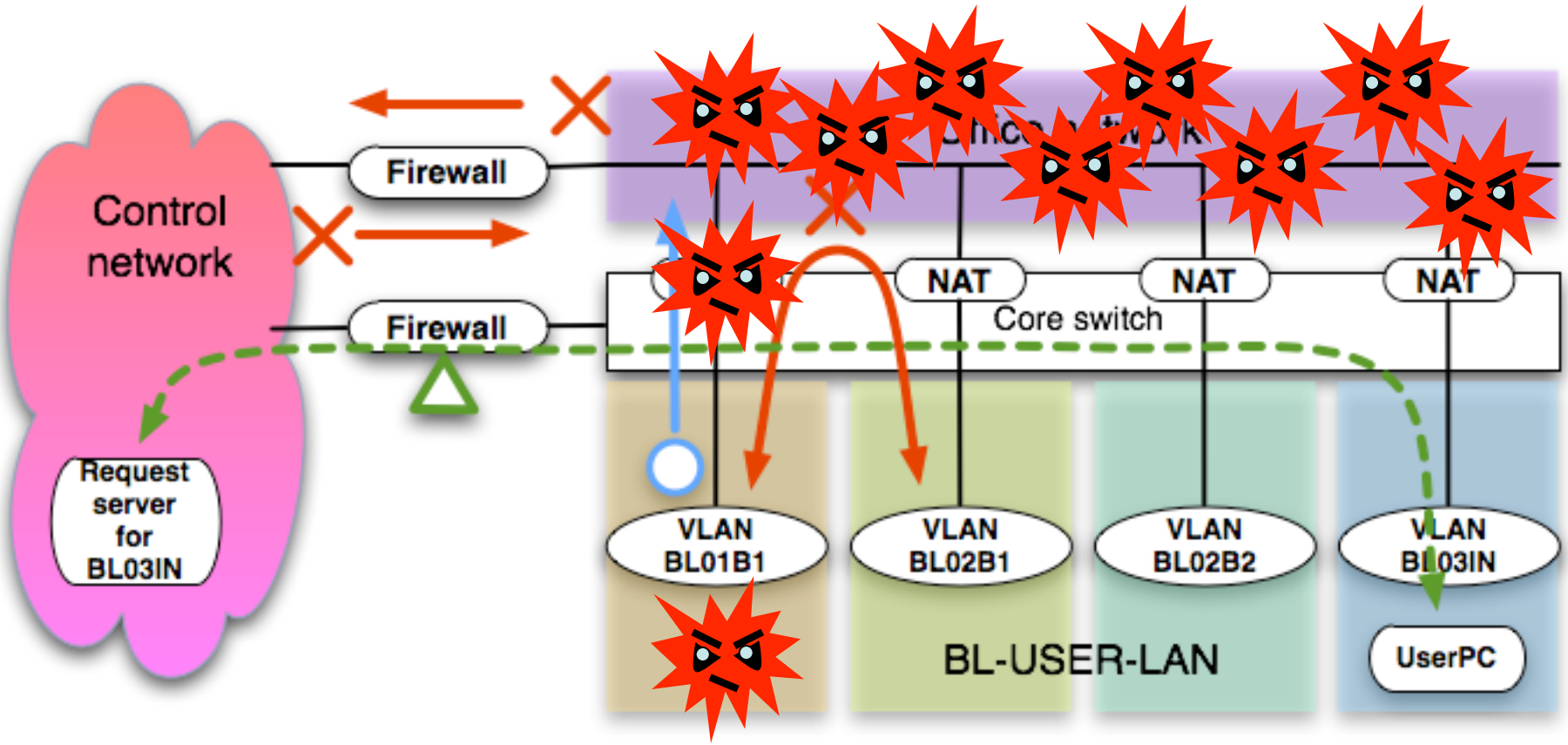


Network segmentation

If a virus comes in a beamline,

Stops the virus spreading between beamlines

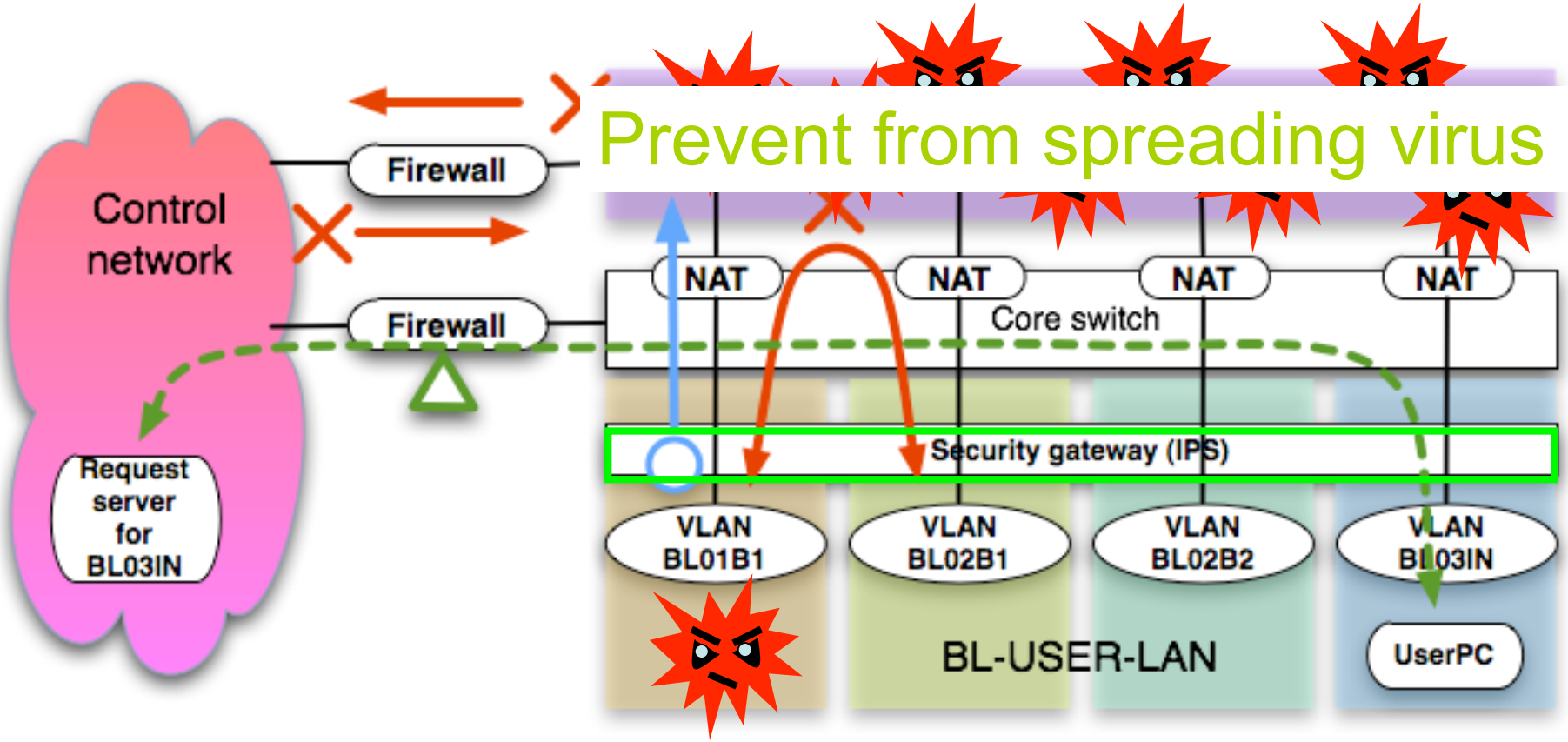
But… Weak point of the attack from inside to outside



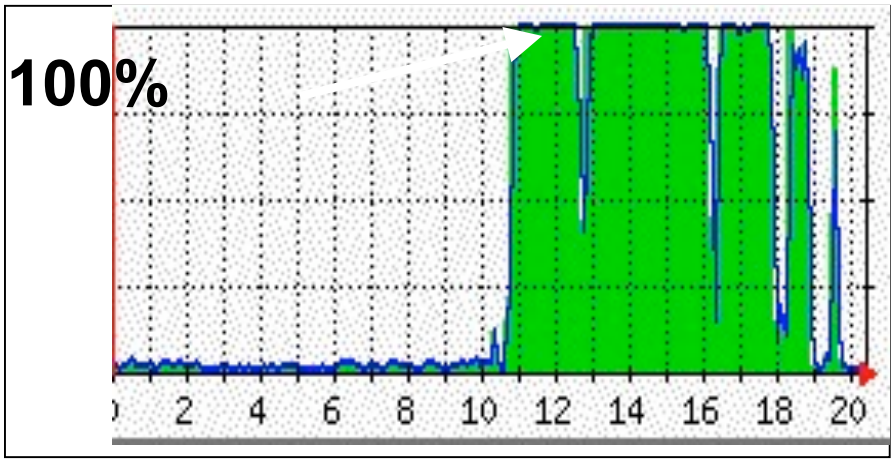
Security gateway (IPS)

Intrusion Protection System

- monitor behavior and signature
- quarantine the virus inside the network



If… without IPS

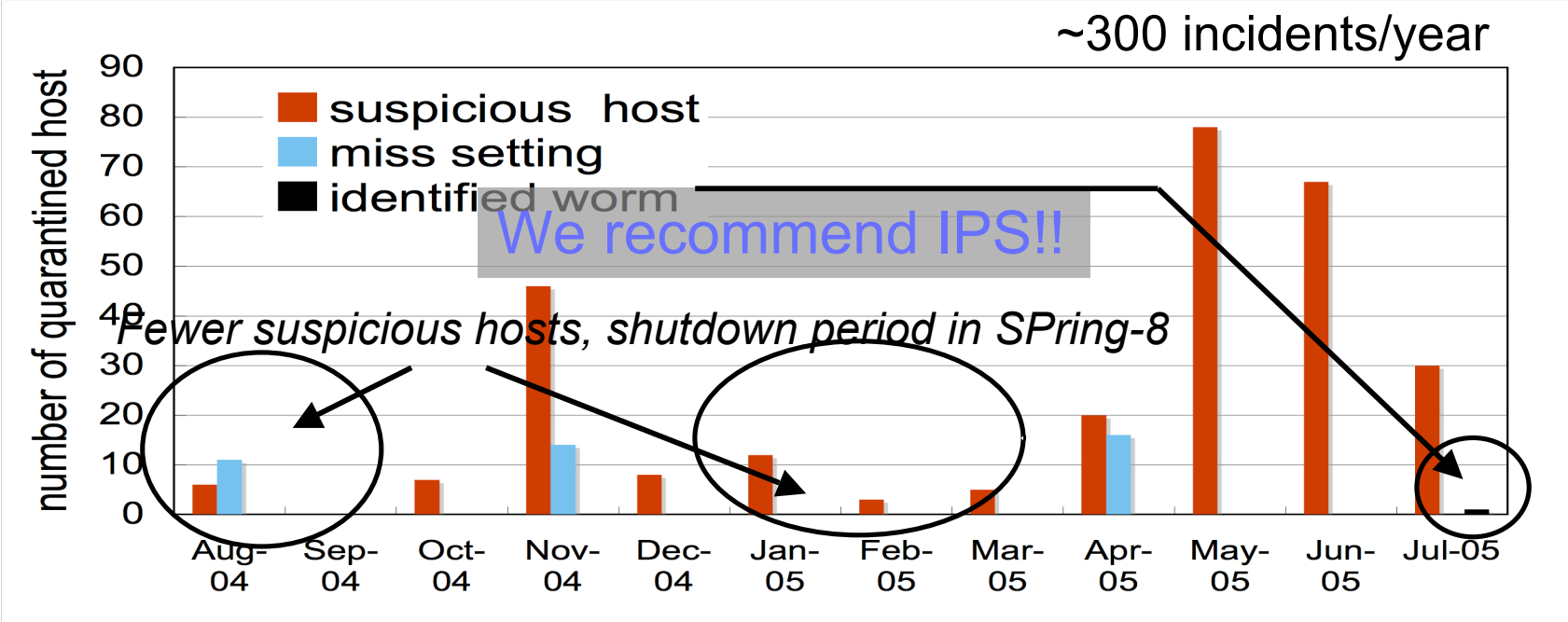


The CPU utilization
of a network switch

Before installing IPS, the network switch was overloaded by ping traffic of blaster.w32 worm.

Because NAT perfomed on the CPU of switch

Statistics on IPS



Most incidents had shown undesirable behavior such as sweep port scan

When checked “quarantine list” and go to the host, we found “Trojan Horse”

“miss setting” was caused by the wrong detection of pattern string.

A pattern string for detection worm is simple.
The detection strings of Sasser worm is “\\sarpc$”.
Normal connections such as Active Directory of Microsoft uses this string.

Authentication gateway

- Wireless network of user service

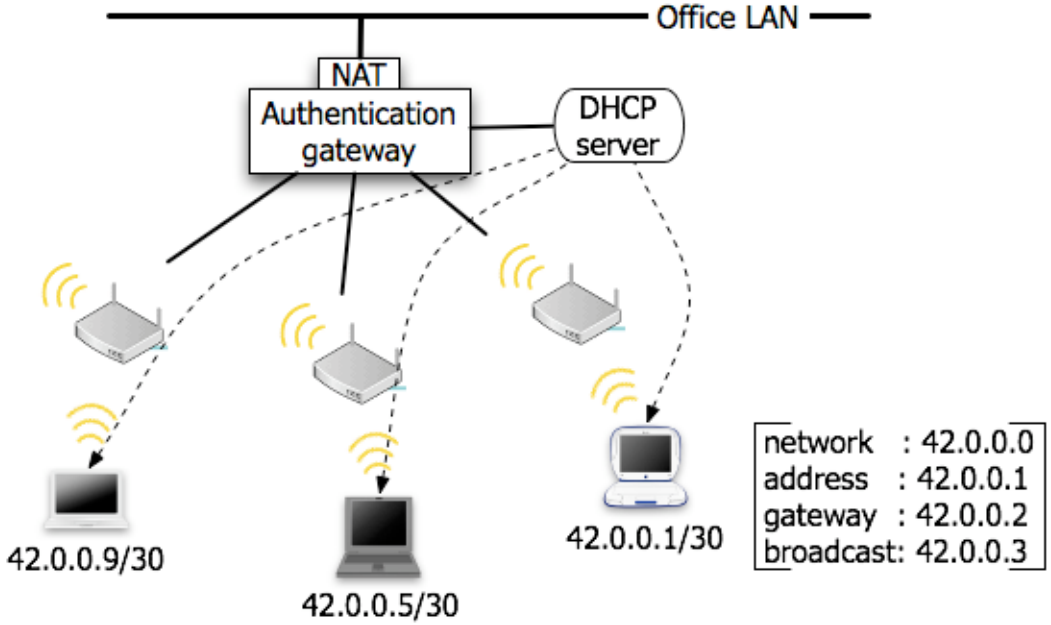
Brief specifications

Performance	300Mbps
Encryption	DES, 3DES, AES
Security	IPSec, PPTP/L2TP
Authentication	LDAP, RADIUS, Active Directory, Local database, 802.1x

Difficult to understand the state of the wireless network
Rogue AP, No WEP, No WPA, No hide of SSID,…
We will install a monitoring system of wireless network

Authentication gateway

- Private IP segment assigned by DHCP



- Wireless network monitoring system
  - Difficult to understand the state of the wireless network
    - Rogue AP, No WEP, No WPA, No hide of SSID,…

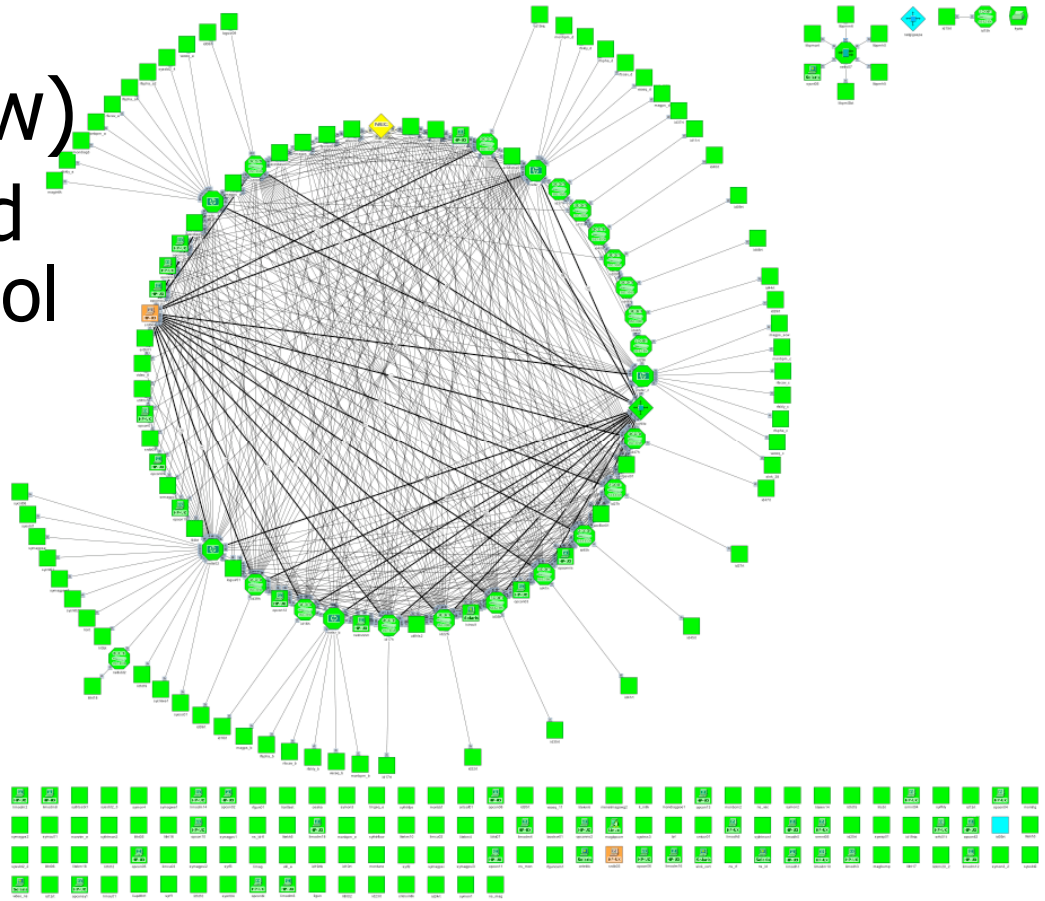
We will install a monitoring system of wireless network

Network monitor

Network monitor(1)

- Network Node Manager (OpenView)
  - SNMP, RMON based MIB* monitoring tool
  - monitors
    - node status
    - statistics
    - threshold
    - …

Logical network topology of control network



*MIB (Management Information Base)

Network monitor(2)

Sometimes packet capturing tools are needed
when falls into unknowable network problem

But…

have to go to faraway switch, change configuration of switch for mirror port and setup capturing tool…

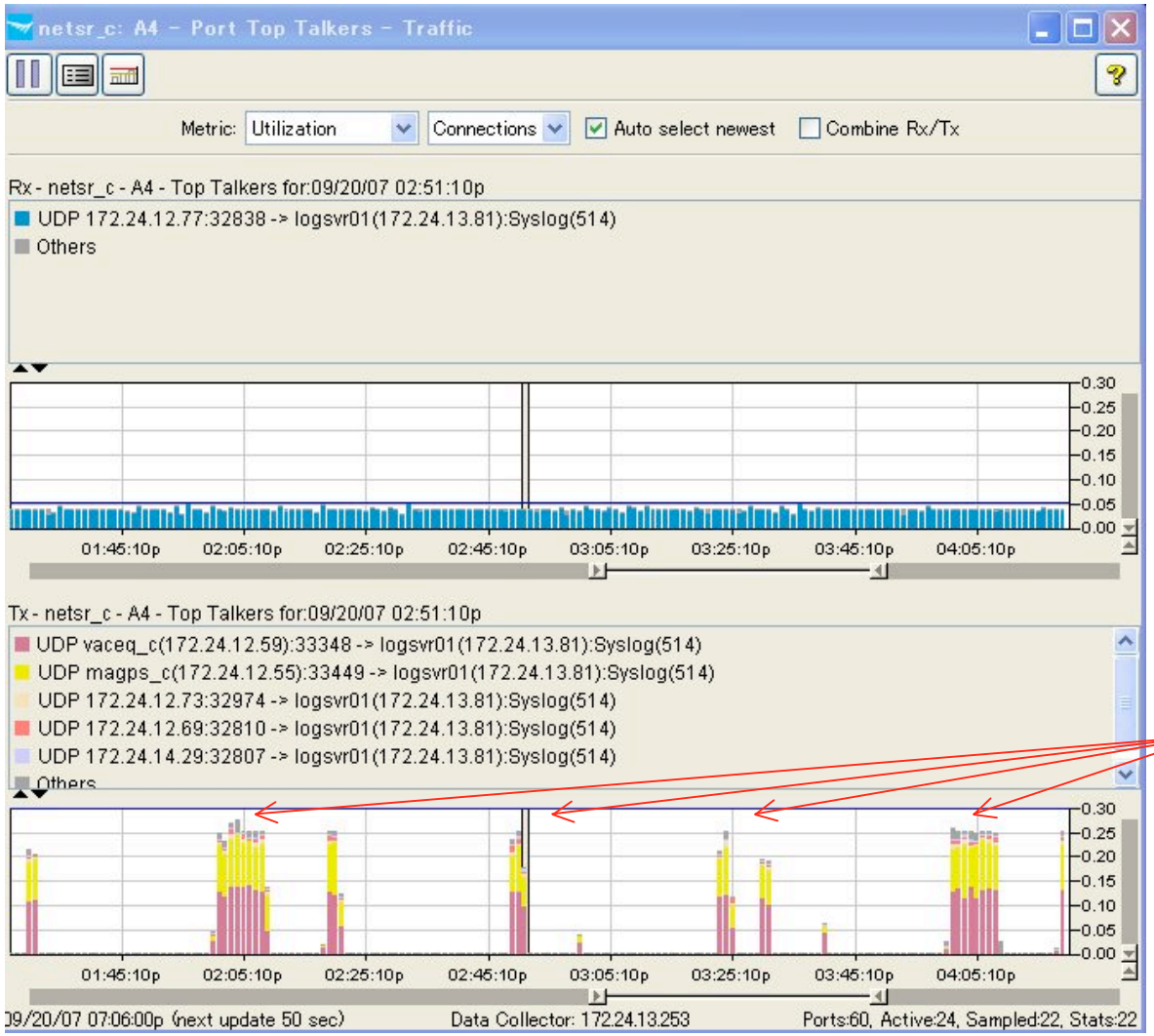
It is difficult

sFlow monitor (ProCurve Manager plus: PCM+)

- Capture (sampling) network packets at switches
- Display details of traffic such as source, destination, application type and so on
- Detect problem such as worm attack, link layer trouble
- Analyze problems

Making the network visible

Network monitor(2)



Screenshot of PCM+

PMC+ makes visible the detail of MAC flooding problem in the control network

<-- Rx

Flooding

<-- Tx

Patch management

Patch management

- Windows update, anti-virus software update server
  - push patches into clients

  Target: daq front-end with LabVIEW, Oscilloscope, etc.
- Linux mirror servers
  - YaST mirror of SuSE Linux Enterprise 10
  - apt mirror of Ubuntu and Debian

  Target: operator consoles, daq front-end, etc.

Conclusion

The most important approach concerning the network security is a segmentation design of the network.

but…

Network system has various kind of security threat

⇩

Security cannot be kept by only single method

Pay attention to the latest trend of attack and security