14. Network Management Office

Overview

Network Management Office (NMO) has been established on April 2009 by the merging of the former Network working group in Department of Simulation Science and the LHD LAN management group.

The information network is fundamental for the research activity. The advanced NIFS campus information network named "NIFS-LAN" is the information infrastructure which contributes to the development of nuclear fusion research. NIFS has 300 staffs and the number of their hosts is near 3,000. NMO provides 100Mbps / 1Gbps bandwidth to users' host. NIFS-LAN consists of three autonomous clusters which have their own purposes and usages as follows;

1. *Research Information Cluster* (Kiban-LAN) is the network of general use, and covers the campus whole region.

2. *LHD Experiment Cluster* (LHD-LAN) is provided for LHD experiment, and covers the building relevant to LHD experiment.

3. *Large-scale Computer Simulation Research Cluster* (PS-LAN) is provided in order to support the large-scale computer simulation research efficiently.

NIFS-LAN is connected to Science Information Network 4 (SINET4) managed by National Institute of Informatics. The block diagram of NIFS-LAN is shown in Fig. 1.
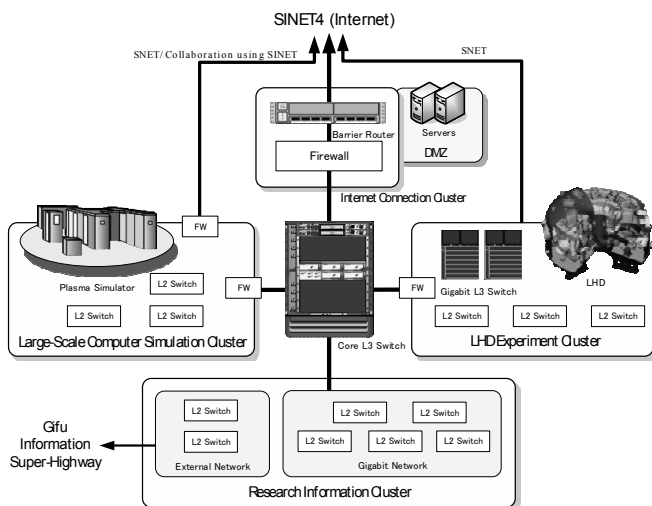

Fig.1. Block Diagram of NIFS Campus Information Network

Activities in FY2012

1) Operations and administrations of information network

a) The e-mail is a basic communication tool for the research activities. NMO has operated the mail server for NIFS to realize the effective communication. 49 new accounts (e-mail address) were created and 59 accounts were deleted and the mailing list service has also provided. 61 lists ware created and 62 lists were deleted in FY 2012.

b) To manage the network, NMO has administrated the following information system;

* Routers and Layer 2 / Layer 3 switches.

* Firewall

* SSL-VPN and Access Gateway servers

* Mail, Mailing-list, DNS and DHCP servers

For example, 129 hosts were added to DNS server and 127 hosts were deleted on Kiban-LAN and PS-LAN, 263 hosts were added and 165 hosts were deleted on LHD-LAN in FY 2012. NMO also guides the staff of NIFS on information network and information systems.

c) TV conference system is a common tool for the remote conference. NMO has assisted 50 events with TV conference in FY 2012.

2) Security incidents at NIFS-LAN

Three security incidents were treated by NMO in FY2012.

- Virus infection by browsing malicious web site
- Virus detection in the backup file
- Virus detection during the download of freeware

Most virus infections cannot be prevented by the vaccine software even with latest virus definition file, because there are wide variety of malformation virus which includes spyware and adware and the time to be change is very short. More attention is needed to prevent to virus infection. The malware uses not only the flaws of OS and the Web application but also its plug-in software, such as the flaws of Acrobat Reader, Acrobat flash, Java Runtime Environment, and so on. We need to pay more attentions to the update of the plug-ins.

3) Security improvements at Kiban-LAN

To keep the high-level security, Kiban-LAN has introduced the firewall and other security equipments. In FY 2012, the following activities were performed to maintain the network security.

a) Owners of hosts who bring them from outside of NIFS are requested to make a security check before connecting them to NIFS network. The quarantine network room was offered

for such a security check and supports of quarantine processing to be sanity. This room was used more than 116 times in FY 2012.

b) Secure Socket Layer-Virtual Private Network (SSL-VPN) is a kind of VPN, which uses web browser as a client's software. The SSL-VPN in the NIFS has also the function to check the security level of the client before VPN connection is established. User is needed to use the One-Time Password token as the authentication. 14 accounts were newly created, 124 accounts were renewed, and 9 accounts were removed in FY 2012. The number of accounts for NIFS is 92 and the number of accounts for research collaborator is 32.

4) Security improvements at LHD-LAN

LHD-LAN is requested as the highly secure network because of LHD experimentation. A host should be check by the staff of NMO before connecting to LHD-LAN. The staff checks whether OS and the virus definition file are recently updated or not. The statuses of vaccine software on users' host are monitored during the connection to LHD-LAN. If the warning message on the monitor is found, the staff warns the user to check his/her host. The number of hosts connected to LHD-LAN is 1174. Before the LHD experiment campaign, security condition of every host is checked with the criterion described above by the monitor system.

3) Notable activities in FY 2012

a) Upgraded the core system on Kiban-LAN

The traffic required by the researcher is increasing year by year, however, the facility of Kiban-LAN did not have enough capacity. To overcome this situation, the core system was upgraded to the latest facility which has the capability to connect the switches with 10 Gbps. The devices of the core system are listed below;

- Barrier L3 switch
- DMZ L2 switches
- Core L3 switch
- Network servers which support the network administration

The lines between core switch and DMZ switch are 10GbE, and DMZ switch offers 10/100/1000BASE-T ports to servers. Network servers were built as the virtual server on two physical servers. The network server can continue to provide services to users, even if one physical server fails.

The rack which loaded these network devices in network facility room were replaced to one with seismic isolation design.

The bandwidth for users is still 100 Mbps because the edge switch which connect users' host did not replaced. The edge

system and the other support system would be upgraded in the near future.

b) Replaced the firewall and SSL-VPN server on LHD-LAN

The LHD-LAN firewall is operated to prevent the hosts on LHD-LAN from the infection by the malware in other cluster. Most of connections from Kiban-LAN are rejected by this firewall. LHD experimenters can access LHD-LAN from Kiban-LAN via SSL-VPN server with the authentication. New Access Gateway was installed because the available bandwidth of SSL-VPN had been too narrow to transfer massive data. After the user authentication, Access Gateway adds the temporary access-list to the firewall for the connections from the experimenter's host to the server in LHD-LAN.

c) Lecture for information network and its security

Four lecture classes on the subject of the campus network of NIFS, information security and how to register the MAC address were delivered in FY2012 and 248 staffs joined. This lecture was held under "Information Security Policy" with the Information Security Committee. Only the attendance of this lecture can be the MAC address registrar (183 members) who can register MAC address of host to DHCP system in NIFS.

d) Joined to UPKI initiative

University Public Key Infrastructure Initiative (UPKI initiative) operated by NII provides universities and institutes with a digital certificate free of charge. A digital certificate is mainly installed in web server. 12 certificates were issued in FY2012.

4) Others

- Installed the secondary firewall on NIFS-LAN for redundancy
- Renewed the wireless access points to support both 2.4GHz and 5GHz bands. New AP supports only WPA/WPA2 encryption.
- Renewed NTP server, aka time server.
- Provided and supported the network infrastructure for ITC-22
- Updated the software of ISC BIND for fixing the security hole

(Yamamoto, T.)