NETWORK ARCHITECTURE AT TAIWAN PHOTON SOURCE OF NSRRC

Chih-Hsien Huang, Yin-Tao Chang, Yung-Sen Cheng, Chang-Hor Kuo and Kuo-Tung Hsu
NSRRC, Hsinchu 30076, Taiwan

Abstract

A robust, secure and high throughput network is necessary for the 3 GeV Taiwan Photon Source (TPS) in NSRRC. The NSRRC network divides into several subsets according to its functionality and includes CS-LAN, ACC-LAN, SCI-LAN, NSRRC-LAN and INFO-LAN for the instrumental control, subsystem of accelerator, beam-line users, office users and servers for the information office respectively. Each LAN is connected via the core switch by routing protocol to avoid traffic interference. Subsystem subnets connect to control system via EPICS based channel-access gateways for forwarding data. Outside traffic will be block by a firewall to ensure the independence of control system (CS-LAN). Various network management tools and machines are used for maintenance and troubleshooting. The network system architecture, cabling topology and maintainability will be described in this report.

INTRODUCTION

Taiwan photon source (TPS) [1] is a 3 GeV synchrotron radiation facility with ultra-high photon brightness and extremely low emittance in National Synchrotron Radiation Research Center (NSRRC). The construction began in February 2010, and the commissioning started in the third quarter of 2014.

A high secure and robust network is necessary for such a new accelerator. In order separate the traffic of various kinds of users, 5 layer-3 middle switches are used. TPS control system used for the operations of accelerators and beamlines is implemented by the experimental physics and industrial control system (EPICS) [2, 3] software toolkit. Control devices are connected by the control network and integrated with EPICS based input output controller (IOC).

THE NETWORK ARCHITECTURE OF NSRRC

The NSRRC campus hosts a 1.5 GeV Taiwan light source (TLS), several buildings for office and experimental users, and TPS building. In order to maintain the network functionality of the existed infrastructure and transport to TPS new infrastructure, it is gathered by a middle-layer switch labelled with NSRRC-LAN that the exited wired network including the control system of TLS in the first step. The bandwidth of the backbone upgrades to 10 Gbps and upgrades to 1 Gbps for users gradually. During the upgrade, vlan introduces to the setting of switches in order to replace the use of the public internet protocols (IPs).

In the building of TPS, three subnets including CS-LAN, ACC-LAN and SCI-LAN are created for the control system, subsystems of accelerator and beam-line, shown in Fig. 1. The office automation users belong to the NSRRC-LAN. The subdomain of each LAN is setting in a layer-3 switch. The traffic between middle switch and core switch is through the routing protocol. Single mode fibers supporting 10/40 Gbits/sec link between network rooms and equipment areas at reasonable cost. 10 G links are setup as backbone at this moment.

Control and subsystem network services are available in 24 control instrumentation areas (CIAs) with an individual edge switch in the inner ring area. Major devices and subsystems are installed inside CIAs. There are 4 network rooms and one network & server room outside the ring. These provide the network for the experimental users and the fiber adapter of timing system and intranet network between the middle-layer switch and edge-layer switch, which is installed within beam line station.

There are many servers (e. g. e-mail server, AD server, employee portal server, Web server) belonging to the information office that serve for the employee or various kinds of users. An INFO-LAN will be created for this kind of usage after the servers are moved to TPS. Two subnets with one public IP and one private IP will be signed in the INFO-LAN for the internet and intranet servers.

The traffic of the wireless LAN (WLAN) is independent of the wired network in order to insure the normal operation of the wireless network while the local wired network breaks down. Each access point (AP) broadcasts four service set identifiers (SSIDs), i.e. NSRC-Staff, NSRRC-TEL, NSRRC-Roaming and NSRRC-Guest for staff, IP phone, roaming and guest users. Each user must be certificated before using the wireless. For the staff users, the traffic is direct into core switch without passing through firewall for the intranet access. However, for the Roaming or guest users, the traffic must pass through the firewall and the usage of the intranet is limited by the policy of the firewall.

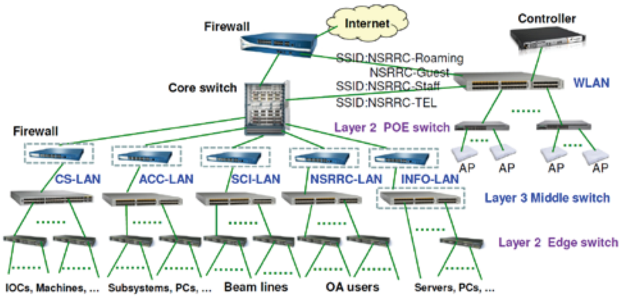

Figure 1: The network infrastructure in NSRRC campus.

ISBN 978-3-95450-146-5

ACCELERATOR CONTROL SYSTEM NETWORK

Accelerator operators are the principal users of the control system. Control consoles with remote multi-display are used to manipulate and monitor the accelerator through network. In order to remote monitoring and control TLS facility, dedicated control consoles are also installed in TPS control room. The control console computers, EPICS control servers, database servers, and network equipment are all in the network and server room.

Control network services are not only available at the control room, but also at the network and server room, 24 CIAs, linear accelerator equipment area, tunnel, transport lines, main power supply equipment room and control system laboratories. The TPS control network infrastructure is shown in Fig. 2. Connection between CS-LAN and the core switch will be through a firewall. Outside traffic will be block by the policy of firewall except for some particular purposes such as the remote access for maintaining machines which is proposed in advance.

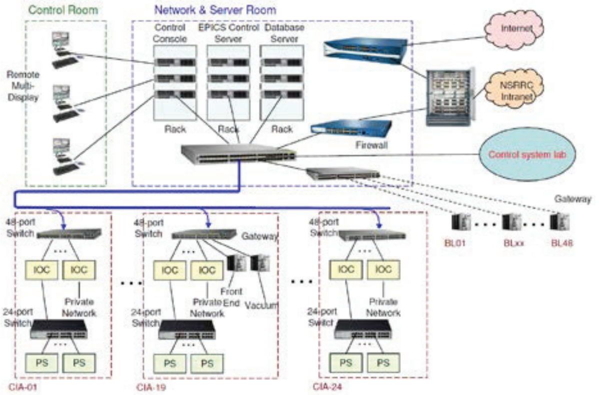

Figure 2: TPS control network infrastructure.

A high performance switch with 48 10-Gbps and 4 40-Gbps fiber ports is defined as the middle-layer switch of CS-LAN. There are two types of switches used in every CIA for control system. The first type is defined as the edge switch which is used to connect IOC nodes and uplink to the high-speed backbone through 10-Gbps fiber uplinks. A 24-port switch is selected as the switch for gathering the uplink for power supplies.

One class B subnet (172.20.0.0) is used for IOC network. For the IP 172.20.xx.yy, xx represents locations (e.g. number of CIA) and yy identifies for functional groups. This IP addressing schema makes identify the locations of IOCs and devices easily. This is also helpful to speed up finding the devices for maintenance and troubleshooting. There are multiple Class C private networks for respective subsystems, such as power supplies, motion controllers, GigE Vision, etc. These Class C private networks use IP range 172.21.xx.yy in which schema is also the same as above.

The fieldbus of the TPS control system needs highly reliable Ethernet. Power supplies for dipole, quadrupole and sextupole are connected to the EPICS IOCs by Class C private Ethernet within the CIAs. In order to reduce the network traffic and provide additional access security, EPICS based CA gateway or IOC provide necessary connectivity and isolation. Its functionality is to forward channel access to different network segments.

GigE vision for diagnostics is based on the IP standard and can be adapted to EPICS environment. The images can be easily accessed through network for machine studies. The GigE vision cameras connect to control system through Ethernet with the data transfer rate up to 1 Gbits/s. To decrease traffic loading, one Class C private network and one CA gateway will also be used for the GigE vision cameras to connect with the control system.

ACCELERATOR SUBSYSTEM NETWORK

Many technical groups prefer their own subnets to monitor and control their system outside the control system (CS-LAN). The ACC-LAN serves for this purpose for vacuum, front-end, glider control system, radiation monitoring and access control system, RF system, etc., shown in Fig. 3. It only responses for the non-critical safety data transfer. Two subnets of private IP, labelled as intranet private IP (IPIP) and regional private IP (RPIP) are provided for each subsystem. The traffic of RPIP is limited within its subnet and the traffic of the IPIP is allowed inside NSRRC campus via the routing of core switch and outside the Campus via the network address translation (NAT) of the firewall. The IPIP provides the convenience to remote monitoring the status of each subsystem from the office and the RPIP provides the network security protection of each machine. The data exchange between each sub-system and the control system is through dedicated EPICS gateways.

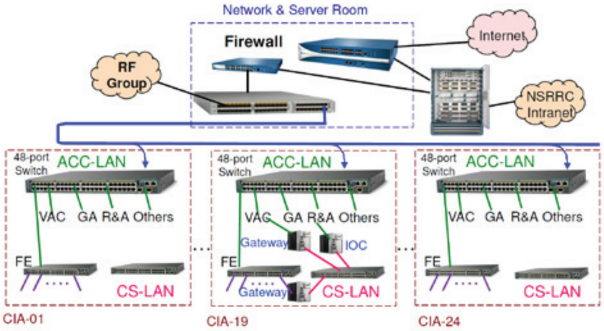

Figure 3: TPS ACC-LAN infrastructure for the vacuum (VAC), front-end (FE), gilder alignment (GA), radio frequency (RF), radiation monitoring and access (R&A) control system, etc.

BEAM-LINE NETWORK

The SCI-LAN is planed for network of the TPS beam-line and experimental stations. Each beam-line has a Class C RPIP for control and data acquisition and IPIP for the internet/intranet access. Data exchange with the accelerator control system is via a dedicated EPICS gateway for each beam-line, shown in Fig. 4. The TPS

ISBN 978-3-95450-146-5

networks support high through data transfer with 10/40 Gbps rate between beam-line and experimental station to the storage farm or computation farm which locates at different area within the TPS facility.

Beam-line users can access accelerator control system by PVs via CA gateways. This design provides necessary connectivity between the machine control system and beam-line control system and also restricts unnecessary network traffic across different network segments.

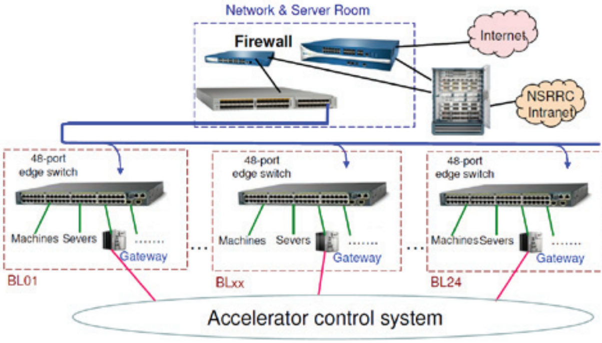

Figure 4: TPS SCI-LAN infrastructure.

NETWORK MANAGEMENT

Spanning tree protocol (STP) or rapid spanning tree protocol (RSTP) is configured to prevent looping. Network monitoring software (e.g. Cacti, MRTG,) is used to monitor traffic and usage information of the network devices. By collecting and analyzing the packets, it can measure the traffic to avoid bandwidth bottlenecks.

It is necessary to access the control system from outside to realize the machine problems. Remote maintenance or troubleshooting has the advantages of convenience and time-saving. Virtual private network (VPN) is used to penetrate the firewall system of the protected network. It can establish an encrypted and compressed tunnel for TCP or UDP data transfer between control network and public networks inside or outside the TPS.

The network time protocol (NTP) and precision time protocol (PTP) serve for timekeeping. NTP is used for synchronizing the clocks of computer systems over the TPS network with millisecond precision. PTP is served also for microsecond precision application.

CYBER SECURITY

Current accelerator control systems are commonly based on modern Information Technology (IT) hardware and software, such as Windows/Linux PCs, PLCs, data acquisition systems, networked control devices, etc. Control systems are correspondingly exposed to the inherent vulnerabilities of the commercial IT products. Worms, viruses and malicious software have caused severe cyber security issues to emerge.

It is necessary to use network segregation to protect vulnerable devices. Combining firewall, NAT, VLAN… technologies, control network is isolated to protect IOCs and accelerator components that require insecure access services (e.g. telnet).

Firewall only passes the packets from authorized hosts with pre-defined IP addresses outside control network and opens specific service ports for communications. But firewall is not able to resist the spread of worms. Worms are not only designed to self-replicate and spread but also consume the network bandwidth. Intrusion prevention system (IPS) can detect and stop network threats such as worms, viruses, intrusion attempts and malicious behaviors. The next generation firewall which combines functionality of firewall and IPS is adopted for TPS network. Security always puts at the highest priority for the TPS networking system. Restricted security policy for network is essential for TPS facility and equipment. However, balance between security and convenience will be addressed also.

CURRENT STATUS

All backborn fiber network are finished in October, 2013. Full access of the network for ACC-LAN, CS-LAN, WLAN is available in the first quarter of 2014 for the subsystem installing and beam commissioning. The network for the SCI-LAN is scheduled and under installing. That will be finished before the users of beamline is needed.

It is finished that the basic function of network manager tools such as Cacti and IPScan which provide us to realized the traffic of each node and the IP or Mac using in the network. The detail setting is under way for obtaining the complete information.

SUMMARY

This report describes the infrastructure of network in NSRRC. NSRRC-LAN, ACC-LAN, CS-LAN, SCI-LAN and INFO-LAN are or will be created for various users. An individual wireless LAN is also setup for ensure the network service while local wire network is out of function. An adaptive, secure and fault-tolerant control network is essential for the stable operation of the TPS. The control network is separated from the general purpose network for imposing security. Subsystem and beam-line subnets connect to the control system via EPICS CA gateways or IOC for forwarding data and reducing network traffic. Network management tools are used to enhance productivity. Remote access mechanism with proper authentication is implemented for the system maintenance and troubleshooting.

REFERENCES

[1] TPS Design Book, v16, September 30, 2009.
[2] EPICS, http://www.aps.anl.gov/epics/.
[3] Y. S. Cheng et al., “Construction of the TPS Network System”, ICALEPCS 2013, San Francisco, USA.