16th Int. Conf. on Accelerator and Large Experimental Control Systems ICALEPCS2017, Barcelona, Spain JACoW Publishing
ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA047

NETWORK SYSTEM OPERATION FOR J-PARC ACCELERATORS

N. Kamikubota†, S. Yamada, K.C. Sato, N. Kikuzawa and N. Yamamoto, J-PARC, KEK & JAEA, Japan
S. Yoshida, Kanto Information Service, Tsuchiura, Japan
H. Nemoto, ACMOS Inc., Ibaraki, Japan

Abstract

The network systems for J-PARC accelerators has been operated over ten years. This report gives: a) an overview of the control network system, b) discussion on relationships between control network and the office network, and c) recent security issues (policy for antivirus) for terminals and servers. Operation experiences, including troubles, are also presented.

INTRODUCTION

J-PARC (Japan Proton Accelerator Research Complex) is a high-intensity proton accelerator complex. It consists of three accelerators: a) 400-MeV Linac (LI), b) 3-GeV Rapid Cycling Synchrotron (RCS), c) 30-GeV Main Ring (MR), and three experimental facilities: d) Material and Life Science Facility (MLF), e) Hadron Facility (HD), f) Neutrino Facility (NU) [1-2]. Since the initial beam in 2006, J-PARC has been improving beam power. Recent studies demonstrated a 1-MW equivalent beam [3].

The control system for J-PARC accelerators was developed using the EPICS (Experimental Physics and Industrial Control System) toolkit [4-5]. In advance of the initial beam, the network system for the control system started operation for Linac around 2005 [6], followed by extensions to whole facilities. It has been operated over ten years since then.

CONTROL NETWORK FOR ACCELERATORS

Network Overview

The logical configuration of the control network is shown in Figure 1. The "core switches", main and sub, are located in CCB (Central Control Building), which are the center of the network system. The accelerator buildings (LI, RCS, MR-D3) and the MLF building are linked to the core at the 10Gbps rate. While other buildings (MR-D1, MR-D2, NU, HD) are linked to the MR-D3 building at the 1Gbps rate. Buildings layout with fibre-optic cable network is shown in Figure 2.

"Edge switches", which have physical network connections, are shown in the lower part of each building in Figure 1. Typical edge switch has 24 or 48 ports of the 1Gbps rate. Numbers of edge switches in buildings are given in Table 1. Total number is about 250 in 2017. The photo of the core switches and typical edge switches are shown in Figure 3.

†norihiko.kamikubota@kek.jp

As shown in Figure 1, each edge switch has two routes to the core. In normal operation, the main route is used and the sub is stand-by. When the main route is stopped by a trouble, the sub takes over in a few seconds, and network operation continues. This redundancy guarantees non-stop operation against single fault in the system.

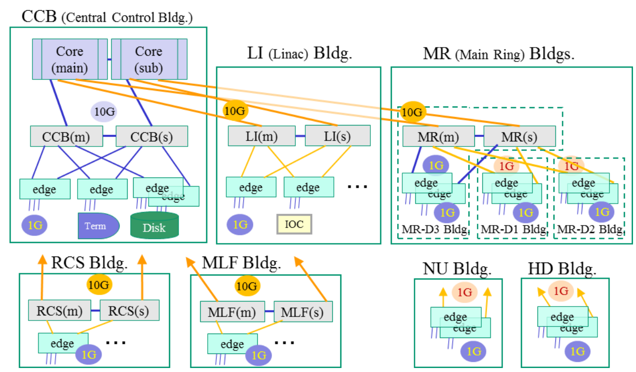

Figure 1: Logical configuration of the network system.

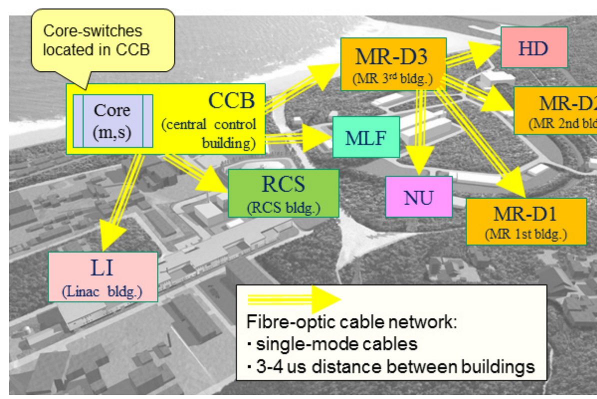

Figure 2: Buildings layout with fibre-optic network.

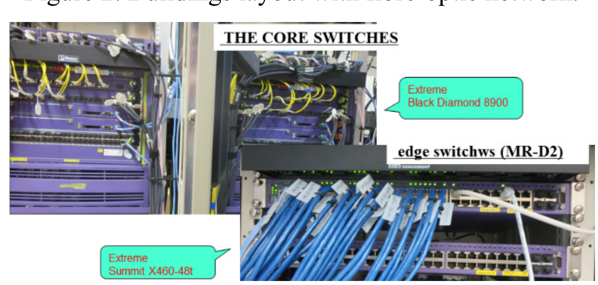

Figure 3: The core switches and typical edge switches.

VLAN Configuration

In order to avoid traffic concentration, we divided the control network into multiple VLANs. As shown in Table

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA047

1, they correspond to the buildings, but also reflect the divisions and the sections in the J-PARC organization. Class-A private IP addresses are used. Because we control all accelerators (and watch out all experimental facilities) from the Central Control Room (hereafter CCR) in CCB, all the VLANs exist in CCB. It is worth noting that an edge switch can have multiple VLANs, if necessary.

Table 1: Building and VLANs with Number of Switches

Building	VLAN (dominant)	IP assignment	No. of switches
CCB	ccr	10.8	13
LI	li	10.16	83
RCS	rcs	10.32	39
MR-D1,D2,D3	mr	10.64	9
MLF	mlf, mlk	10.48, 10.56	56
NU	nu	10.80	2
HD	hd	10.88	2
Others	l3bt, 3nbt	10.16, 10.40	48

Relationships with Other Network Systems

The office network for J-PARC (hereafter JLAN) and the control network (jkcont) are different networks. The jkcont is managed by the accelerator control group, while JLAN is managed by Information System Section (the computer center of J-PARC, hereafter ISS). As shown in Figure 4, direct communication between two networks is not allowed. Thus, a firewall, "jkcont-FW", was introduced to have another network (jkcont-DMZ). It accepts connections from both networks with limited protocols. Two servers, a web-server and a login-server, are located in the jkcont-DMZ.

There are two other network systems shown in Figure 4: the radiation safety system and the PPS (Personnel Protection System) [7]. The radiation safety system has an isolated network. A dedicated one-way data-link to the control network was developed to provide observed data of radiation monitors [8]. The PPS also has an isolated network. The beam safety signals are fed into EPICS IOCs using hardwire cables [9]. Since both systems handle safety functions, careful considerations were made not to be affected from the control system.

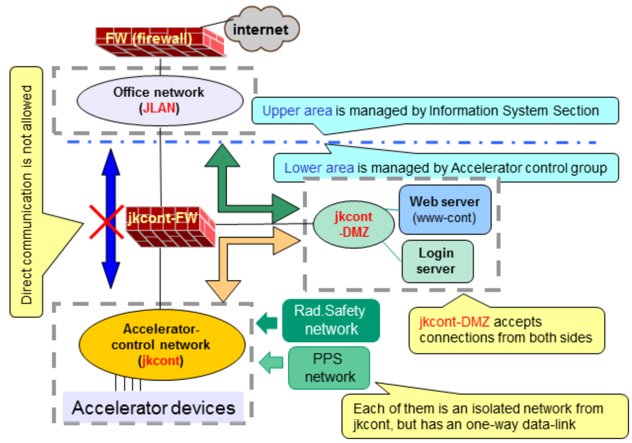

Figure 4: Relationships between network systems.

SECURITY ISSUES

Introduction

The accelerator control network can't be an isolated network. We need to watch at accelerator status from JLAN, or even from out of J-PARC. In addition, we need a route to the control network from JLAN for emergency maintenance. In order to protect the control network against external threat, layered countermeasures have been introduced (Figure 5).

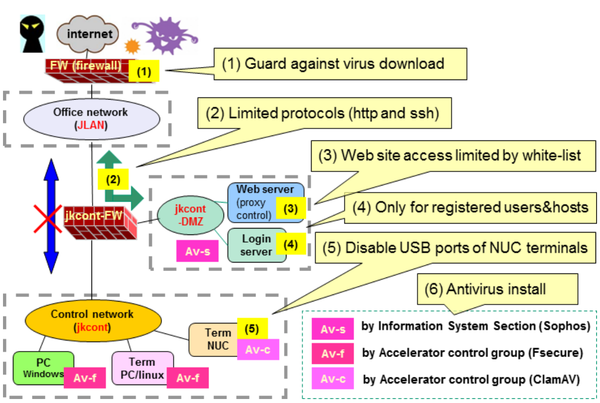

Figure 5: Layered countermeasures against threat.

Countermeasures against External Threat

Six countermeasures are shown in Figure 5. (1) At the top, a guard system is operated by ISS to protect virus download. (2) Accesses from JLAN to the jkcont-DMZ are limited. The firewall, jkcont-FW, is configured to deny all protocols but http and ssh. (3) The web-server acts as a proxy server from the control network. It limits accesses to external web-sites using a white-list. (4) The login-server accepts only pre-registered users and hosts. (5) USB ports of each NUC terminal are disabled. (6) Antivirus software is installed in all terminals in CCR and the servers in the jkcont-DMZ.

In the past before 2014, the guard system detected and stopped suspicious downloads a few times per year.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA047

Downloads were always caused by external web browsing. In November, 2014, a white-list at the proxy server was introduced. It showed a significant effect.

Antivirus Policy

Three different types of antivirus software are used: (a) Av-s (Sophos), an antivirus provided by ISS, (b) AV-f (F-secure), an antivirus introduced by the accelerator control group, and (c) AV-c (ClamAV), a free antivirus software.

In CCR, we have PC-terminals running Linux, NUC-terminals [10], and Windows PCs for operators and for device maintenances. In principle, we install Av-f to all the terminals and PCs. However, for NUC terminals, AV-c is used. This is because that NUC terminals are configured to invoke operation applications only, and the functions of AV-c are enough. The two servers in the jkcont-DMZ are accessible from JLAN. For them, we apply the policy of ISS, thus, AV-s is used.

OPERATION EXPERIENCE

Faults of Switches

The faults of switches during 2011 and 2016 are summarized in Figure 6. The "Catastrophic" faults stopped edge switches, hence, accelerator operations were also influenced. While the "Redundant" faults did not give influences on the network operation, which is blessed with the designed redundancy scheme.

The catastrophic faults were caused by two reasons. Firstly, for the faults during 2011 and 2013, the manufacturer reported that capacitors used in 2007-2008 were produced under bad assembly condition. The mass introduction of edge switches overlapped the bad season accidentally. We replaced switches with new ones using good capacitors. Secondary, the faults during 2014 and 2016 occurred only at stacked switches. The manufacturer reported that the early versions of switch firmware had a bug. Under certain conditions, each of stacks wanted to be a master and collapsed. We installed a bug-fixed firmware to stacked switches. In 2017, such catastrophic faults seem disappeared.

Faults of switches	2011	2012	2013	2014	2015	2016
(Catastrophic)	Bad capacitors			Firmware bug for stack		
Reboot, Stop	6	17	6	10	9	4
Core fault	1	0	0	0	0	1
(Redundant)						
GBIC	3	2	3	3	0	3
PS unit	1	0	1	3	2	6
else	0	0	2	0	0	1

Figure 6: Numbers of switch faults during 2011 and 2016.

Major Network Traffic

During beam-delivery operations, major traffic flow is from MR buildings to CCB. As shown in Figure 7, each of MR buildings generates ~100Mbps network traffic, originated from beam diagnostic devices. In CCB, a traffic flow of 460Mbps was observed from the core switches to servers, disks, and terminals in CCB [11].

All the observed traffic rates are less than the network capacities (10Gbps) in average. However, momentary peaks exceed the capacities in recent operation. Plan to upgrade core-switch capacities from 10Gbps to 40Gbps (or 100Gbps) is under discussion.

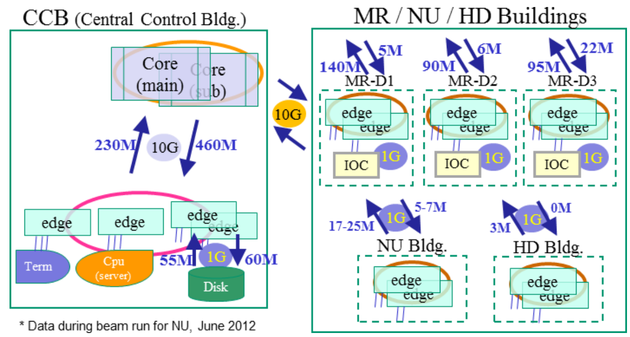

Figure 7: Major network traffic during operation.

Trouble Examples

In our environment, Cacti, a free network graphing tool [12], has been used to supervise network traffics [13]. Here we introduce two impressive troubles (Figure 8).

In May, 2012, a low-cost Web-camera produced burst packets, and occupied the capacity of the port (100Mbps). The vlan "li" became unusable for a few hours. The camera was set in the Linac tunnel, and was broken due to radiation damage. Later in 2014, a mechanism to detect burst packets was implemented to edge switches. The detected port is disabled automatically, in order not to spread burst packets.

On a Friday evening in March, 2015, the traffic rate of the HD facility increased from 3Mbps to 100-300Mbps. The traffic was generated by ClamAV of multiple NUC terminals in HD. Due to a miss-configuration, all NUC terminals started to scan a remote data-disk of 24TB. We re-configure ClamAV not to scan the remote disk.

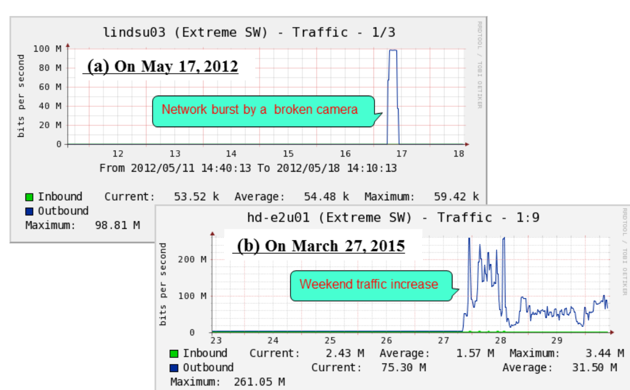

Figure 8: Two trouble examples.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA047

CONCLUSION

The network system for J-PARC accelerator controls is reviewed. The logical configuration with VLAN IP assignments, layout of buildings, and its redundancy are described in detail. The relationships to other network systems, especially to the office network (JLAN) is discussed with security issues.

During long operation of the control network, we had several faults of network switches caused by two reasons. In addition, examples of troubles are also given.

We appreciate all the J-PARC staff members and companies for their efforts to maintain and update the control network system.

REFERENCES

[1] J-PARC website: http://j-parc.jp/index-e.html

[2] S. Nagamiya, "Introduction to J-PARC", Prog. Theor. Exp. Phys. (2012)02B001.

[3] K. Hasegawa *et al.*, "Performance and Status of the J-PARC Accelerators", in *Proc. IPAC'17*, Copenhagen, Denmark, May 2017, TUPVA090, pp. 2290-2293.

[4] EPICS, http://www.aps.anl.gov/epics/

[5] N. Kamikubota *et al.*, "J-PARC Control toward Future Reliable Operation", in *Proc. ICALEPCS'11*, Grenoble, France, Oct. 2011, paper MOPMS026, pp. 378-381.

[6] H. Yoshikawa, "Current Status of the Control System for J-PARC Accelerator Complex", in *Proc. ICALEPCS'07*, Knoxville, Tennessee, Oct. 2007, paper TOAB02, pp. 62-64.

[7] Y. Takeuchi, "Personnel Protection System of japan Proton Accelerator Research Complex", in *Proc. ICALEPCS'03*, Gyeongju, Korea, Oct. 2003, pp. 404-406.

[8] N. Kamikubota *et al.*, "Integration of Independent Radiation Monitoring System with Main Accelerator Control", in *Proc. PCaPAC'14*, Karlsruhe, Germany, Oct. 2014, paper FPO006, pp.167-169.

[9] H. Nemoto *et al.*, "Development of J-PARC PPS Monitoring System for J-PARC Accelerator Control System", in *Proc. of 6th Annual Meeting of Particle Accelerator Society of Japan (PASJ'09)*, Tokai-mura, Japan, Aug. 2009, pp.542-544.

[10] S. Yamada *et al.*, "Renovation of PC-based Console System for J-PARC Main Ring", in *Proc. PCaPAC'14*, Karlsruhe, Germany, Oct. 2014, WPO021, pp.81-83.

[11] N. Kamikubota *et al.*, "Improvement of Computer Systems for J-PARC MR Control", in *Proc. of 9th Annual Meeting of Particle Accelerator Society of Japan (PASJ'12)*, Osaka, Japan, Aug. 2012, pp.741-744.

[12] Cacti, https://www.cacti.net/

[13] M. Takagi *et al.*, "CPU Loads and Network traffic in J-PARC MR Control", in *Proc. of 7th Annual Meeting of Particle Accelerator Society of Japan (PASJ'10)*, Himeji, Japan, Aug. 2010, pp.693-695.