

## **Network System Operation for J-PARC Accelerators**

N. Kamikubota<sup>[1]</sup>, S. Yamada<sup>[1]</sup>, K.C. Sato<sup>[1]</sup>, N. Kikuzawa<sup>[1]</sup>, N. Yamamoto<sup>[1]</sup>, H. Nemoto<sup>[2]</sup> and S. Yoshida<sup>[3]</sup> [1] J-PARC Center, KEK and JAEA [2] ACMOS Inc. [3] Kanto Information Service (KIS)

### **Abstract**

The network system for J-PARC accelerators has been operated over ten years. An overview of the control network system, and relationships with other systems are given. In addition, recent security-related issues and operation experiences, including troubles, are also reported.

## **Overview of the J-PARC Control Network**

## **Security Measures**



#### LOGICAL CONFIGURATION

- "Core switches", main and sub, are the center of the system.
- Each building is linked to the Core at 10Gbps rate. (NU and HD buildings are linked at 1Gbps rate)
- Each "edge switch" uses the main route to the Core. When the main route stopped, the sub takes over within few sec. - Typical "edge switch" has 24 or 48 ports of 1Gbps.

#### **VLAN CONFIGURATION**

FIBRE-OPTIC CABLES BETWEEN BUILDINGS - The center of the fibre-optinc cable network is CCB, where the Core switches are located in CCB. Core-switches



#### **PHOTO: THE CORE SWITCHES**





#### **MEASURES AGAINST EXTERNAL THREAT**

(1) Guard system against virus download (by Information Section, J-PARC)

- (2) Limited protocols for accesses from the office network (JLAN) to the control network (jkcont-DMZ)
- "jkcont-FW" is configured to deny all protocols but http and ssh

(3) Limited accesses to external web-sites from the control network (jkcont)



**THPHA047** 

- Major Vlans are shown below. Class-A IP addresses (10.x) are assigned.

- An "edge switch" can have multiple Vlans, if necessary.

#### **NO. OF EDGE SWITCHES (2017)**

Facility Build.	VLAN	IP assign.	No. of edge	in total	
	(dominant)		switches		
Central Control Bldg. (CCB)	ccr	10.8	13		
Linac	li	10.16	83		
RCS	rcs	10.32	39		
Main Ring	mr	10.64	9		
MLF	mlf, mlk	10.48, 10.56	56		
Neutriro / Hadron	nu / hd	10.80 / 10.88	2, 2		
Other buildings (L3BT, 3BNT)		10.16, 10.40	48		

# **PHOTO: EDGE SWITCHES (MR-D2)**

- The Web server is a proxy server with a white-list, and deny access requests to unlisted web-sites
- (4) The Login server accepts only pre-registered users and hosts
- (5) USB ports of each NUC terminal are disabled
- (6) Antivirus installed in servers and terminals
- Three types of AV software AV-s, AV-f, and AV-c
- AV-s (Sophos) is installed in servers in "jkcont-DMZ", where servers have JLAN addresses - Sophos is a default AV provided and supervised by Information Section
- AV-f (F-secure) is installed in PC-terminals, both Windows and Linux - F-secure is a default AV of the Accelerator control group
- AV-c (ClamAV) is a free AV for Linux, and installed in NUC terminals

Before 2014, the guard system detected and stopped suspicious downloads, a few times in a year. The detections always caused by external web browsing. A white-list at the proxy server, introduced in Nov., 2014, showed a significant effect.

**Operation Experience** 

## **Relationships with Other Network Systems**

~250 edge switches



#### **RELATION WITH THE OFFICE NETWORK**

- The office network (JLAN) and the control network (jkcont) are different networks. JLAN is managed by Information Section (=Computer Center of J-PARC), while the control network is by Accelerator control group. - Direct communication between two networks is not allowed. Thus, a firewall, "jkcont-FW", was introduced to have another network, jkcont-DMZ, accepts connections from both networks with limited protocols (http and ssh). - Two servers, a web-server and a login-server, are located in jkcont-DMZ.

#### **OTHER SUBSYSTEMS**

- The Radiation Safety system has an isolated network. One-way data-link to the control network was developed to provide observed data of radiation monitors.

- The PPS (Personal Protection System) has an isolated network. The beam safety signals (hardwire) are fed into EPICS IOCs in the control network.

Faults of switches	2011	2	012	2013	20	14	2015	2016	
(Catastrophic)		1	_						
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	

#### FAULTS during 2011-2013

- Many edge switches stopped during 2011-2013. In 2013, the company reported that capacitors introduced in 2007-2008 was produced under bad assembly condition. After 2014, replaces switches with good capacitors have worked well.

#### CCB (Central Control Bldg.)



## **NO. OF SWICH FAULTS (2011-2016)**

- Catastrophic faults were ~10 times per year, caused by two reasons (see below). Now in late FY2016, the fault rate looks decreased.

- Redundant faults did not stop switch operations (i.e. each switch has two PS-units).

#### FAULTS during 2014-2016

- Many stacked switches caused reboot or were unstable during 2014-2016. The company reported that firmware of switches had a bug. Under certain condition, each of stacks wanted to be a master and collapsed. After 2016, switches with new firmware have worked well.

#### **MAJOR NETWORK TRAFFIC**

- Significant amount of data (~400Mbps) is generated in MR buildings, then transferred to CCB. - The averaged data-rates are less than the capacity





29

Average: 31.50 M

1.57 M Maximum: 3.44 M

edge

(10Gbps), however, momentary peaks exceed the capacity during the machine cycle (2.48s or 5.52s). - Plan to upgrade inter-building capacities from 10Gbps to 40Gbps (or 100Gbps) is under discussion.

## **About J-PARC**



Operation online: http://j-parc.jp/Acc/en/operation.html Web: http://j-parc.jp



50km



2.43 M Average:

Current: 75.30 M

Maximum: 261.05 M

Tokyo-Narita

Int'l Airport

#### **TROUBLE EXAMPLES (network burst)**

- In May, 2012, a low-cost Web-camera was broken and produced burst packets. The vlan "li" became unusable. - In Dec., 2012, a loop between two MR buildings was made accidentally. Burst packets stopped the vlan "mr".

In 2014, a mechanism to detect a loop or burst packets was implemented in edge-switches. The detected port was disabled automatically.

#### **TROUBLE EXAMPLE (unscheduled traffic increase)**

On a Friday evening in March, 2015, the traffic rate of HD facility increased to 100-200 Mbps. The traffic was caused by ClamAV of multiple NUC terminals. Due to missconfiguration, each NUC started to scan a data-disk of 24TB !

**Re-configure ClamAV not to scan a remote data-disk.**