Network System Operation for J-PARC Accelerators


[1] J-PARC Center, KEK and JAEA

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

- The center of the fibre-optic cable network is CCB, where the Core switches are located in CCB.

Relationships with Other Network Systems

- 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 protect the control network from both networks with limited protocols (http and ssh).
- Two servers, a web-server and a login-server, are located in jkcont-DMZ.
- Three types of AV software – AV-s, AV-f, and AV-c – are installed in servers and terminals. AV-s (Sophos) is a default AV provided and supervised by Information Section, AV-f (F-secure) is installed in PC-terminals, both Windows and Linux, while the control network is by Accelerator control group. AV-c (ClamAV) is a free AV for Linux, and installed in NUC terminals.

Security Measures

- Before 2014, the guard system detected and stopped suspicious downloads, a few times in a year. The detection accuracy was improved by external web browsing.
- In 2014, a mechanism to detect a loop or burst packets was implemented in edge-switches. The detected port was disabled automatically.
- In 2014, a mechanism to detect a loop or burst packets was implemented in edge-switches. The detected port was disabled automatically.
- Many stacked switches caused reboot or were damaged during 2014-2016. The company reported that firmware of switches had a bug. Under certain condition, each of switches worked as a master and collapsed. After 2016, switches with new firmware have worked well.

Operational Experience

- Catastrophic faults were ~10 times per year, caused by two reasons (see below). Now in late FY2016, the fault rate looks decreased.
- Redundant switches did not stop switch operations (i.e. each switch has two PS-units).
- Measured data-rates are less than the capacity during the machine cycle (2.48s or 5.52s).

Faults during 2011-2013

- Many edge switches stopped during 2011-2013. In 2013, the company reported that capacitors of switches had a bug. Under certain condition, each of switches worked as a master and collapsed. After 2016, switches with new firmware have worked well.

Trouble Examples (network burst)

- In May, 2012, a low-cost Web-camera was broken and produced burst packets. The vlan “S” 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.
- In 2014, a mechanism to detect a loop or burst packets was implemented in edge-switches. The detected port was disabled automatically.
- In 2014, a mechanism to detect a loop or burst packets was implemented in edge-switches. The detected port was disabled automatically.