Development of a monitoring system for the FL-net protocol

M. Ishii, T. Masuda, S. Ueda, JASRI/SPring-8, T. Fukui, RIKEN/SPring-8

PCaPAC 2012, Kolkata, India
December 06, 2012

Introduction

FL-net is an Ethernet-based open standard protocol used for a factory floor networks. It is being used as a communication protocol between the VME system and PLCs in several control system at SPring-8 and SACLA (XFEL).
Its control systems are as follows:

- a status monitoring of linac interlock system at SPring-8
- a vacuum, RF high-power, and low-noise power supply control system at SACLA
- an undulator control system at SACLA
- a precise water temperature control system at SACLA
- a facility control system at both SPring-8 and SACLA
- ……

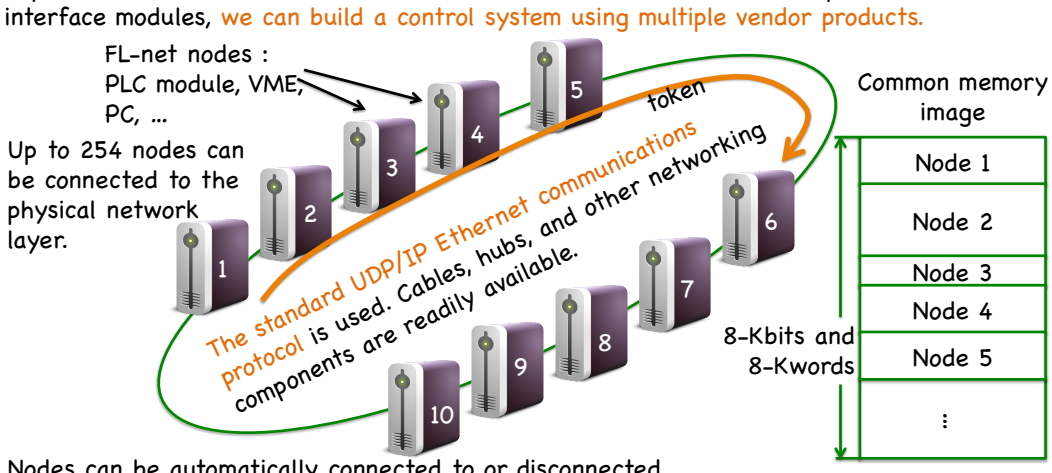
Packet capturing and protocol analyses are helpful for troubleshooting the network. But…

- Analyzing a very large amount of captured data requires a lot of time and effort.
- Since problems may occur at any time, we have to monitor the packets over the long term.
  - Once a day ? Once a week ? Once a month?

We developed a monitoring system for the FL-net protocol.

What is FL-net ?

The FL-net protocol was authorized by the Japan Electrical Manufacturers' Association (JEMA), and was established as a JEM standard in 2000, as an ISO in 2003, and as a Japanese industrial standards (JIS) in 2004. Since several PLC vendors provide FL-net interface modules, we can build a control system using multiple vendor products.



Nodes can be automatically connected to or disconnected from the FL-net network by adopting a master-less token method.

A cyclic transmission uses the common 8-Kbits and 8-Kwords memory shared by all nodes.

Control system using FL-net

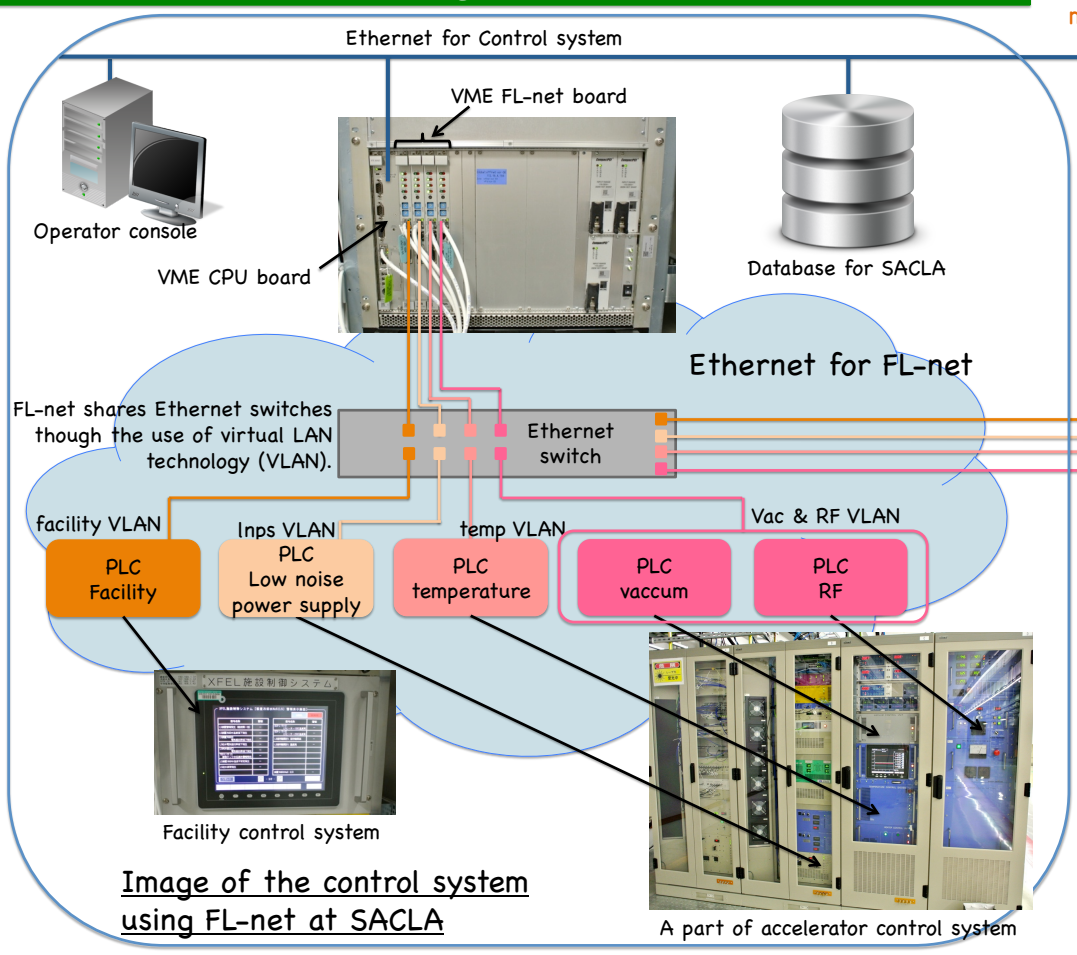


Image of the control system using FL-net at SACLA

Design of a monitoring system

Our design policy was to capture and analyze all packets flowing through the Ethernet of the FL-net network, and to record all problematic events.

In FL-net, network packets continuously flow at a rate of ~ 4 Mbps. If all packets of the captured data are saved as files in pcap format, which is a standard format treated by open-source network analyzers such as tcpdump and Wireshark, the disk usage reaches up to ~ 30 GB/day.

We have to store only the necessary data to save disk space.

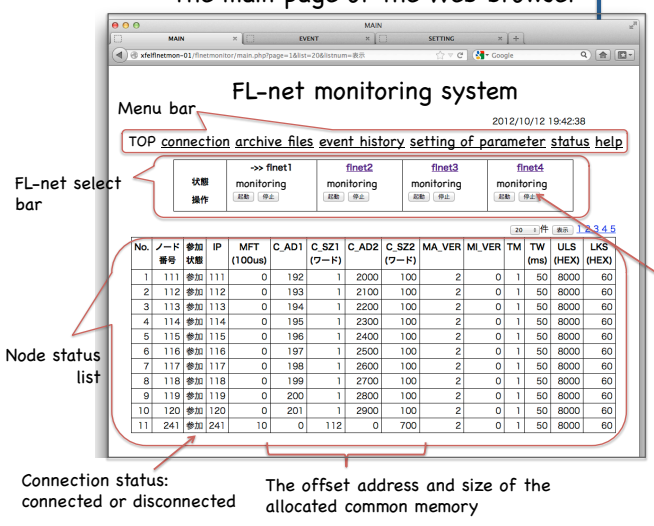
A monitoring system for the FL-net protocol

We developed a software-based monitoring system running on a Scientific Linux.

Features of the monitoring system :

- The monitoring system automatically saves only several 10-s long data packets including the problem event as a pcap format file.
- We can select parameters such as the type of detection events, and save directory using a Web browser.
- The system stores information on a problem event with a time stamp in a relational database. We can easily refer to this information using a Web interface.
- The system has no influence on the operation of the FL-net system.
- The system monitors several FL-net network segments, and we can access the monitoring system through the Ethernet.
- The system has the highly portability and is independent from the hardware.

The main page of the Web browser



We can start/stop the monitoring by the click of a button.

A computer specification of the monitoring system

CPU	a quad core Xeon 2.4 GHz
memory	16 GB
HDD	1 TB
Ethernet port	5 one port is for web access and the other ports are for monitoring four FL-net network segments.

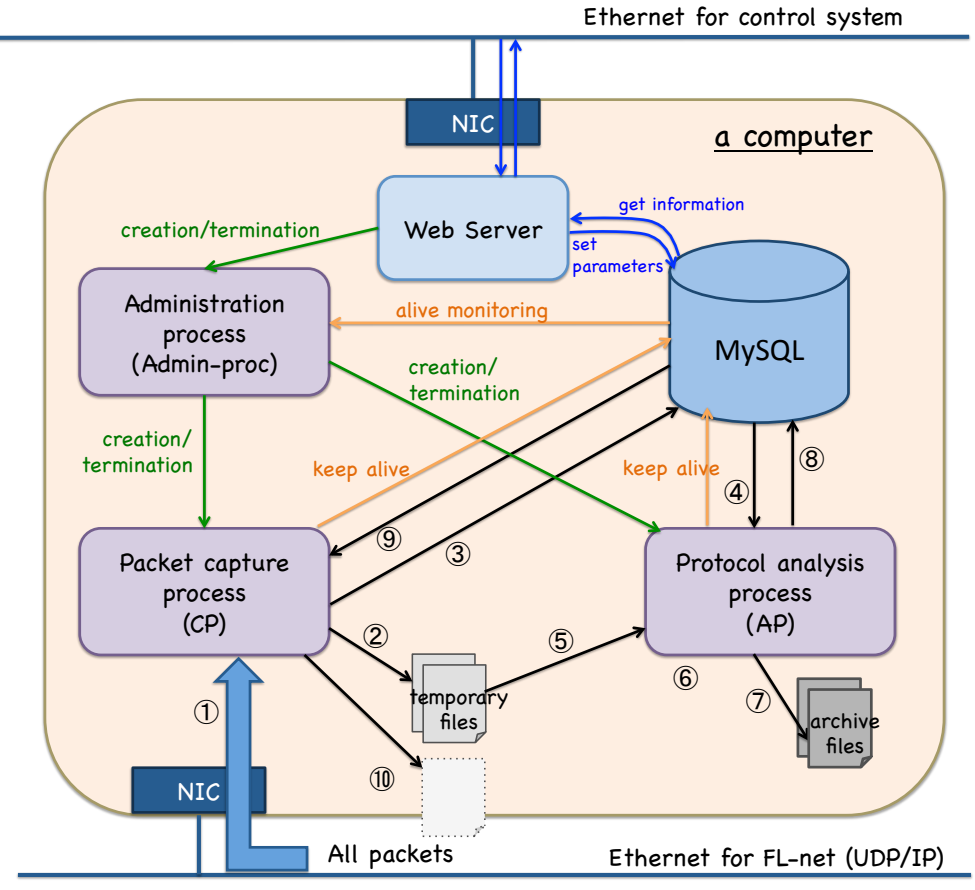
The type of events

- A node connects to the FL-net.
- A node disconnects from the FL-net.
- A duplication of node number
- A duplication of node's IP address
- Token skip
- Token cyclic time (measurement value) > token watchdog timer (parameter)
- …

When many token skips occur and the token cyclic time exceeds the token watchdog timer set for each node, the control system is unstable. So we need to tune the token watchdog timer.

a processing flow

① CP captures all incoming packets.
② CP saves as a temporary file.
③ CP writes the name of the temporary file to a db.
④ AP acquires the name of the temporary file from the db.
⑤ AP reads the temporary file.
⑥ AP analyzes the temporary file.
⑦ If AP detects an event in the temporary file, it saves the packet data including the event as an archive file. If the FL-net is normal, an archive file is not generated.
⑧ AP writes the event information with a time stamp to the db. Then AP sets an analysis complete flag for the temporary file to the db.
⑨ CP acquires the name of the temporary file with the analysis complete flag from the db.
⑩ CP deletes the temporary file.



Schematic view of the monitoring system for the FL-net protocol