SYSTEM OF SAFE DATA TRANSMISSION FROM THE SHE FACTORY DC-280

A.S. Baginyan[1], S.V. Pashchenko[1], V.V. Sorokoumov[1]

[1]*Joint Institute for Nuclear Research, Dubna, Russia, 141980*

E-mail: bag@jinr.ru

The article presents a scheme of the data transmission network providing the commissioning of the DC-280 accelerator complex. The main indicators of communication channel characteristics are given. The paper discusses the calculation settings of network devices that provide secure access to network resources. Settings for the transmission of unicast and multicast packets and the IPv4 protocol are shown. An authorization scheme and storage system for the entire switch configuration sequence is presented. The monitoring system of the network is considered, and the payload of links based on SNMP is shown. The forecast for the future utilization of unblocked communication channels is presented. The detail description of the necessity of using DHCP snooping functionality is given. In conclusion, a summary and a forecast are given on the future development of the LAN of the accelerator complex as well as on the backbone of the communication links.

Keywords: network, monitoring, authorization

CEUR-WS.org/Vol-2507/125-129-paper-21.pdf

Andrey Baginyan, Sergey Pashchenko, Vladislav Sorokoumov

Copyright © 2019 for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

1. Introduction

For the past 20 years, five new superheavy elements have been discovered in the Flerov Laboratory of Nuclear Reactions of the Joint Institute for Nuclear Research (JINR) that completed the 7th period of the Periodic Table: 114 (flerovium), 115 (moscovium), 116 (livermorium), 117 (tennessine), and 118 (oganesson). The synthesis of new elements 119 and 120, which are the first elements of the 8th period of the Periodic Table, will be one of the key objectives of the Factory.

A new accelerator DC-280, a new basic experimental facility of our Institute, was launched. One of the most important stages of the launch of the world's first Factory of Superheavy Elements (SHE Factory) was accomplished. This is a very joyful and significant event for the entire international team of the Joint Institute for Nuclear Research. The project intensities of accelerated ions of the new cyclotron are an order of magnitude higher than those achieved previously in the world's leading nuclear physics centers. This will ensure maintaining of the Institute's leading position in one of the most important areas of modern nuclear physics – the synthesis and study of the properties of new superheavy elements of the Mendeleev's Periodic Table[1]. This event is also a bright indicator of the ability of the Joint Institute for Nuclear Research to solve the most ambitious tasks.

Not only do we find the SHE Factory project challenging in terms of physics, but we are also facing problems in data storage, transmission and processing. The DC-280 automat data processing and storage system of the Joint Institute for Nuclear Research is designed as part of the global Internet system and aims at carrying out a full cycle of processing of physics information obtained during experiments, providing of modeling physical processes, and at securing storage and transmission data. The paper is devoted to the result of a data processing center creation at the Joint Institute for Nuclear Research for modeling and processing experiments carried out on test installations of the SHE Factory.

2. Network scheme

The network scheme is presented in Figure 1. The Catalyst 9500-24Q-A7 switch is used at the distribution level of the three-tier network model. Catalyst 2960-48P is at the access level.

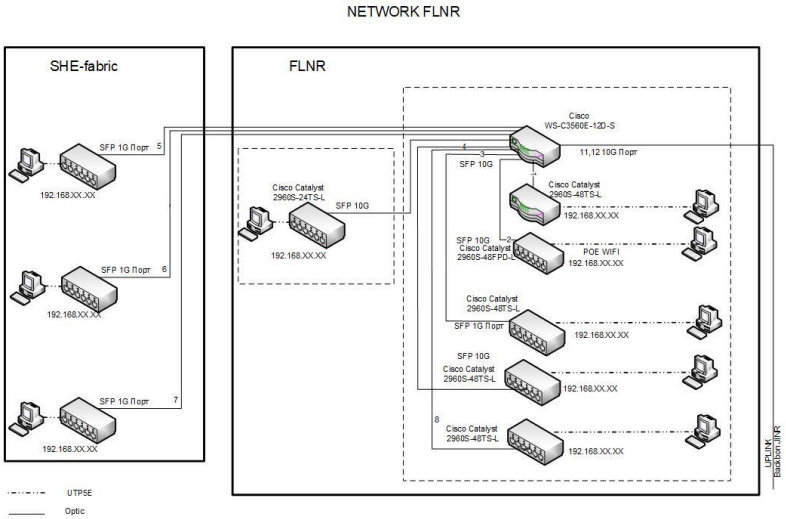

Figure 1. Network scheme

To increase reliability, all devices at the distribution level are connected to the network core by several links.

There are several solutions for providing data transmission in multiply connected networks, each having its advantages and disadvantages. One of the most well-known protocols—the Shortest Path First SPF protocol based on the Dijkstra algorithm [2]—finds the shortest distance from one of

the vertices of the graph to all the others. It works only for the graphs without negative weight edges, which is suitable for the use in data networks.

In cloud services and data centers, a distributed network architecture is used for data warehouses, queries, and search services. With such architecture, huge horizontal traffic (east-west traffic) is created in the cluster. Nowadays, data have been obtained on the loading of some links between the level of distribution and the core of the network, reaching up to 12G. Virtualization technologies are nowadays used more and more widely in computing cluster, thus each server starts performing much more tasks than before, which, in turn, leads to a significant increase in traffic on in/out interfaces. Virtualization increases reliability, reduces the cost of IT services, and increases the flexibility in the deployment of services.

Considering the above, the traditional approach, in which the Spanning Tree Protocol [3] or the Level 3 protocols work at the aggregation/core level, cannot fully solve the problem of transmitting horizontal traffic since a significant part of the cable infrastructure remains unused.

The newest data transfer protocols, such as EVPN MP BGP[4] or TRILL[5], allow one to build a non-blocking architecture that provides complete network utilization entirely unnoticeable to users (fig. 2). They also help, without prejudice to working devices, to introduce new devices into operation because all links remain reserved.

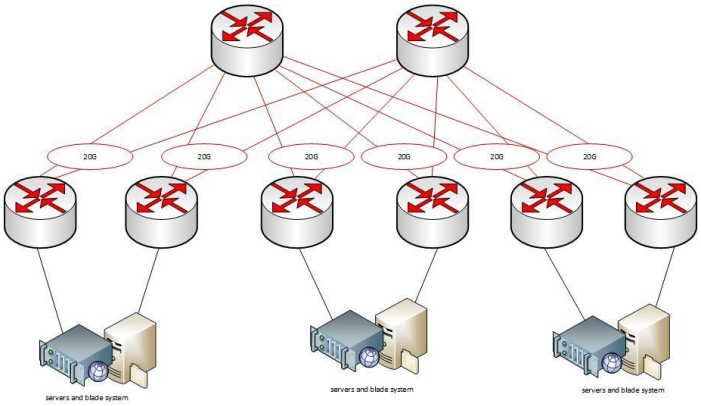

Figure 2. Non-blocking architecture

The network architecture of the SHE fabric data center at JINR is designed with a dual route between the distributed level and the core level on the Cisco equipment. Each server will have an access to the network segment with two equal-value connections of 10G with a total bandwidth of 20G. In addition to the tasks of virtualization in the Flerov Laboratory of Nuclear Reactions of the Joint Institute for Nuclear Research, experimental events simulation has a significant load on the network.

The connection between the core level and the distribution level will have 2 10G routes, which will ensure the transfer of 20G data. The 10G SFP + module consist of optical signal transmitters, each providing bi-directional 10G data transmission.

3. Monitoring system

The software package 10-Strike is used to monitor the state of links. The SNMP software is employed for creating graphs [6]. The 10-Strike collects statistical data for certain time intervals and allows you to display them in a graphical form. Standard templates are used to display statistics on the CPU usage, memory allocation, the number of running processes, and the use of incoming/outgoing traffic.

Figure 3 presents data on loading I/O interfaces between the links of the distribution level and the access level.

Figure 3. Monitoring system

The alert system is also configured by sending an e-mail and SMS in the event of the failure of any network device or the peak download links.

4. DHCP services

For network security, DHCP snooping [7] functionality is implemented. DHCP snooping is a security feature that prevents unauthorized users from connecting to a third-party DHCP server network in order to intercept client DHCP requests. The essence of DHCP snooping is to close the ability to handle DHCP requests on untrusted ports. The network administrator must manually configure trusted ports — the ports behind which this DHCP server is located.

To enable DHCP snooping on the switch, type the *ipdhcp snooping* command and then specify the VLAN(s) to which this action will be distributed using the *ipdhcp snooping vlan XX*, where XX is the VLAN number. Now, using the *ipdhcp snooping trust* command, specify those interfaces that look towards the DHCP server (the command is written on the interface). Most often these are the main communication channels, trunks, and the interface itself which the DHCP server is connected to.

The technology prevents the use of an unauthorized DHCP server on the network, which allows, for example, a man-in-the-middle attack. It also protects the network from DHCP depletion attacks (DHCP starvation/exhaustion), which is not particularly relevant.

The technology monitors DHCP communication on the network, which (mainly) consists of four packets:

- DHCP Discover - sends only a client request for receiving IP via DHCP;
- DHCP Offer - sends only a server, a configuration offer from a DHCP server;
- DHCP Request - sends only a client, the choice of a specific configuration and server;
- DHCP ACK - sends only a server, the final confirmation.

Before activating DHCP snooping, you must specify the "trusted" port(s) that the DHCP server is behind. Only trusted ports will send a DHCP Offer and DHCP ACK (packets from the server). In this regard, no device behind other interfaces of this switch can perform the work of the DHCP server, offering its own network configuration options.

5. AAA system

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a device or a network access server [8]. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX workstation. TACACS+ provides for separate and modular authentication, authorization, and accounting (AAA) facilities. TACACS+

allows a single access control server to provide each service authentication, authorization, and accounting independently. Each service can be tied to its own database to take the advantage of other services available on that server or network, depending on the capabilities of the daemon.

A network access server provides connections to a single user, a network or a subnetwork, and to interconnected networks. The entities connected to the network through the network access server are called network access clients. TACACS+, administered through the AAA security services, can provide the following services:

- Authentication – provides complete control of authentication through login and password dialog, challenge and response, messaging support. The authentication facility provides the ability to conduct an arbitrary dialog with the user.
- Authorization – provides fine-grained control over user capabilities for the duration of the user's session, including but not limited to setting auto commands, access control, session duration, or protocol support. You can also enforce restrictions on what commands a user may execute with the TACACS+ authorization feature.
- Accounting – collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon. Network managers can use the accounting facility to track user activity for a security audit or to provide information for user billing. Accounting records include user identities, start and stop times, executed commands, number of packets, and number of bytes.

The TACACS+ protocol provides the authentication between the network access server and the TACACS+ daemon and ensures confidentiality because all protocol exchanges between the network access server and the TACACS+ daemon are encrypted.

5. Conclusion

Engineering infrastructure, which allows the confirmation of theoretical and practical results and comfortable data analysis, is crucial for a successful experiment. The monitoring system fully provides an insight into the current links payload. It also provides timely information on how the engineer should react in order for the experiment to be successful. The AAA system allows you to track all interventions in the network cluster and to control the access to various nodes. DHCP snooping prevents man-in-the-middle attack. Experimenters highly appreciated the level of functioning of the network cluster.

References

[1] http://www.jinr.ru/wp-content/uploads/2019/03/SHE_Factory_Press_Release_eng.pdf viewed 23 April 2019.

[2] E. W. Dijkstra A note on two problems in connexion with graphs/ NumerischeMathematik 1, 269 - 271 (l959)

[3] Perlman, RadiaAn Algorithm for Distributed Computation of a Spanning Tree in an Ex-tended LAN / ACM SIGCOMM Computer Communication Review. 15 (4): 44–53 1985.

[4] VXLAN network with MP-BGP EVPN control plane: http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/guide-c07-734107.html viewed 23 April 2019.

[5] Touch, J. and R. Perlman, "Transparent Interconnection of Lots of Links (TRILL): Problem and Applicability Statement," RFC 5556, May 2009.

[6] J. Case, K. McCloghrie, M. Rose, S. Waldbusser RFC 1448 – Protocol Operations for version 2 of the Simple Network Management Protocol / April 1993.

[7] Banks, Ethan. "Five Things To Know About DHCP Snooping". Packet Pushers. Retrieved 29 February 2016.

[8] Anderson, Brian (December 1984). "TACACS User Identification Telnet Option". Internet Engineering Task Force. Archived from the original on 12 August 2014. Retrieved 22 Feb-ruary 2014.