GERDA Scientific / Technical Report: **GSTR-09-002**

March 6, 2009

Underground Network Structure for the GERDA Experiment at LNGS

R. Brugnera[ab], F. Costa[b] and A. Garfagnini[ab]

[a]) Dipartimento di Fisica dell'Università di Padova, Padova, Italy
[b]) INFN Padova, Padova, Italy

Abstract

In this note the layout of the GERDA network structure is summarized. All the hardware infrastructures will be placed in the GERDA building in Hall A. Particular emphasis is given to the available network services, their accessibility and on the user authentication procedures.

1 Introduction

The present note describes the layout of the network infrastructure for the GERDA experiment at Laboratori Nazionali del Gran Sasso (LNGS). After a short introduction to the LNGS network environment, details are given on the structure of the GERDA private network and on the available services and facilities.

2 LNGS Network Environment

The LNGS laboratories are organized into two sites: the external and underground laboratories, inside the A24 motorway (Roma-Teramo). The network of the underground laboratories is connected to the external labs by means of a certain number of optical fibers which are shared among the different experiments according to their throughput needs. Two multi-

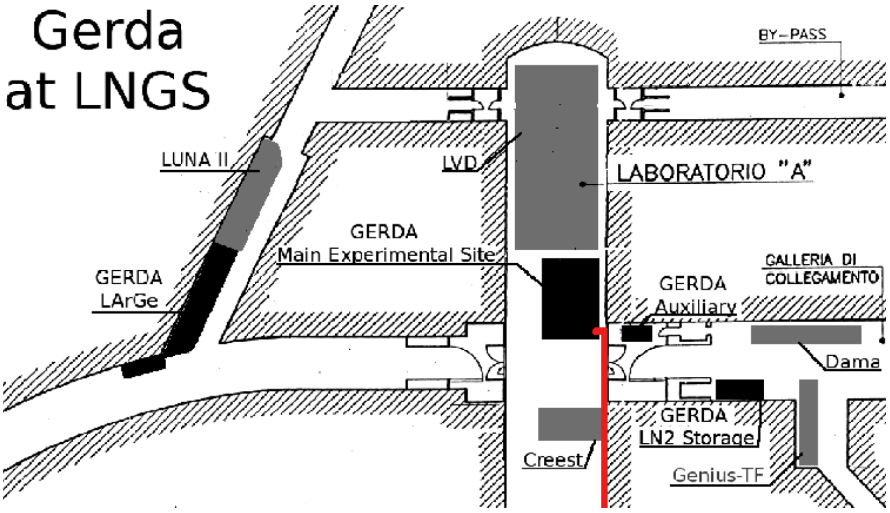

Figure 1: Location of the GERDA experiment in the Experimental Hall A of the Underground Laboratories. The path of the GERDA multimode optical fibers is indicated with a red line, running along the corridor side of Hall A, from the LNGS network cabinet to the GERDA building.

modal optical fibers have been explicitly dedicated to the GERDA experiment. Figure 1 shows a layout of the experimental Hall A and the neighboring corridors and Halls. The GERDA fibers run along the corridor side of hall A, from the LNGS network cabinet (located in the south-east corner of the hall) to the GERDA building.

3 GERDA Network Structure

The path of the GERDA optical fibers ends outside the experiment building, where in a small cabinet, the fibers are connected to a network switch [1]; the latter provides 44 auto sensing ports (10/100/1000) and offers access security and advanced prioritization and traffic-monitoring capabilities. The different network lines are routed inside the GERDA rucksack.

The switch is directly connected to a dedicated server [2] which provides network routing facilities and acts as a firewall and user authentication server.
The GERDA public access server is `ge-gate.lngs.infn.it`, with a public `IP` number `172.16.2.32`, associated dynamically by the LNGS computing center to a public IP, reachable from the outside (NAT 1:1). At the moment, this is the only public service available directly from the external networks and should be used to access all GERDA internal network resources and services.
The server has two network interfaces, one connected to the LNGS public network and a second port connected to the `GERDA` virtual LAN 27 (`Vlan-27`) with logical name `gerda-27.lan`
The following IP ranges have been assigned to our `gerda-27.lan` local network:

- `192.168.39.xxx/24`
- `192.168.40.xxx/24`

A Port Address Translation (PAT) network device will be used, internally, to translate TCP/UDP communications between GERDA private network computers and public network hosts. (A description of the available resources is given in the next sections.)

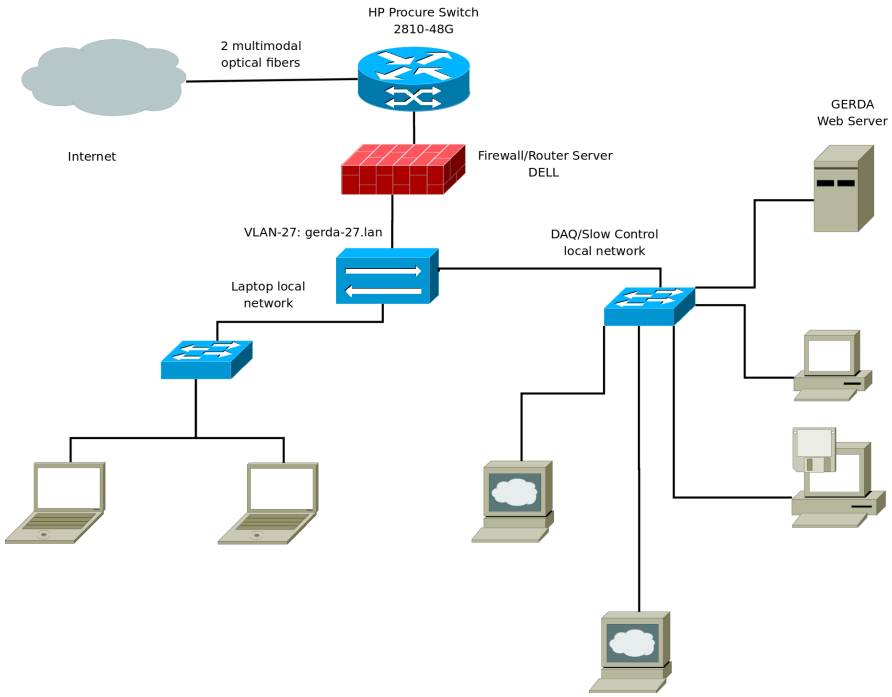

Figure 2: GERDA Network layout. A description of the different parts is given in the text.

Figure 2 shows the layout of the GERDA local network. Two separate logical networks are visible: the DAQ/Slow Control network, where mission critical machines are connected, and a network branch for user laptops and computers temporarily connected to the LAN.

3.1 Network Services

The following centralized services are available:

`NIS` server for user authentication;

`DNS` server for host name resolution;

`DHCP` server for the DAQ/Slow Control machines and all the computers attached temporarily to the network (i.e. laptops)

`Web` server for the whole experiment (`gerdaweb.lngs.infn.it`);

Additional resources, provided by the individual groups of the GERDA Collaboration, will be made available on demand. Their availability will be achieved through the PAT network device.

As an example, it will be possible to access the Web Servers of specific components from the outside network, only by authorized experts, for hardware monitoring and parameter setting purposes.

3.2 User Authentication

According to the Italian Law n. 547 (23.12.1993)[1] and to the following "Rules Anti-Terrorism" (D.D.L. 16.08.2005), all the users of the INFN network resources should be properly registered, and their identity verified through a digital acquisition of a valid identity document.

In order to simplify the bureaucracy, but comply to all law constrains, all users needing an account for the GERDA underground network, have to follow the following steps:

- apply for an account on the LNGS Linux cluster;
    1. an application form has to be filled, at the LNGS;
    2. the module has to be signed by the LNGS GERDA group leader who will forward the application to the LNGS computing center for the creation of the account. (with the same procedure the user can request an authorization to use the LNGS Wireless services).
    3. once the account has been created, the same username will be authorized to login on the GERDA underground network.

A `username` and `password` will be provided to all GERDA users with a LNGS linux account; the former will allow to login on the GERDA gateway server (`ge-gate.lngs.infn.it)` and grant access permission to the internal network.

The authentication service is provided by a dedicated NIS (Network Information Server) server and the authentication can be used to provide access to all machines connected to the `gerda-27.lan`. Currently the same authentication procedure is used for the global slow control machine, in order to provide a uniform access to all computers and have only one place for user credential (`username/password`) storage.

[1] "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalitá informatica" ("Modifications and integrations to the Italians laws on the topic of computer crimes")

3.3 Portable Computers

Especially during the commissioning phase of the experiment, various computers, including personal Laptops, will be connected to the GERDA `gerda-27.lan` underground network.
An `IP` numbers will be given by the `DHCP` server and the temporary machine will be connected on the local network.
If the MAC Address of the computer has been previously registered in the LNGS database (following the procedure available at the LNGS help desk), the machine will be properly identified and it will be able to reach any IP of the outside network; otherwise it will connect only the machines on the `gerda-27.lan` local network.

4 Access to the GERDA network resources

As stated previously, the GERDA network access point is provided by (`ge-gate.lngs.infn.it`): this is the only computer available for direct access from the outside network.

In order to provide access to internal GERDA resources (mainly internal Web servers), a `proxy` service has been setup. Once configured, it will be possible to access internal Web servers, through the main GERDA Web server (`gerdaweb.lngs.infn.it`).

As an example, we need access to the local web server provided by the Alarm Dispatcher Unit. The local web server is running on the port 80, but the machine is not visible from the outside network. Using the `proxy` server, the Alarm Dispatcher Web server can be reached through the GERDA Web server, at the URL:
`http://gerdaweb.lngs.infn.it/alarm-dispatcher/`.

References

[1] Hewlett Packard ProCurve Switch 2810-48G.

[2] DELL Power Edge R300, Quad Core Xeon X3323, 2.5 GHz.