



POLITECNICO DI TORINO

Master of Science in ICT for Smart Societies

Master Thesis

# Testing of virtual routing for an edge device in the Smart Grid

**Advisor**

prof. Daniela Renga

**Candidate**

Marco Cappelli

**Company tutors**

**Gridspertise**

Ing. Gennaro Fiorenza, Ing. Valentina Gilardone

July 2023

# Summary

This thesis work was conducted together with "Enel Grids" company "Gridspertise" [25].

This study will briefly introduce the history of Distribution Networks, the electric power networks that take care of transmitting Medium Voltage (MV) power, i.e. power generated by a potential difference which is between 1 and 100 KV, and Low Voltage power, i.e. power generated by a potential difference which is between 1 and 1000 V, to users.

This thesis will then picture to the reader what a modern Distribution Network looks like, and it will introduce two of the core nodes in a distribution network, the primary and the secondary substation.

This research will describe how Distribution System Operators (DSOs) are either remunerated or penalized basing on quality of continuity of service indicators, an example of such indicators will be provided basing on the data of the Italian Authority ARERA (Autorità di Regolazione per Energia Reti ed Ambiente), to convey the need of DSOs of adopting measures to reduce the duration of interruptions of service (power outages) caused by faults on the network.

This thesis will then describe what **remote controlling** is: the ability of *operators* of opening or closing switches of the network without actually going to where the switches are located but by sending a command from a control room; and what **automation** is: the ability of the *network* to act by its own, and without the intervention of an operator, when a fault occurs, to reduce the duration of the interruption. Some legacy automation tactics and latest state of the art automation tactics will be introduced to highlight how fundamental the role of a **router** is in a power network (or smart grid) an specifically in secondary substations.

The study then will meet his **first goal: a review of the state of the art of communication techniques** in a smart grid, to then dive deeper in details about the functions a **router** needs to provide to a smart grid to match the requirements of DSOs study cases.

This research will then introduce the concept of **edge computing** and **virtualization**, and what benefit they offer to DSOs. Edge computing allows to reduce the latency of communications and virtualization comes with an impacting economic advantage for DSOs. As of now substations requiring *routing capabilities* have no

choice but to be provided with a physical router. When reading this one must consider that substations may run under quite adverse conditions such as: heavy rains, high or low temperatures, floods, high humidity rates and it happens they are subject to thievery.

Distribution System Operators (DSOs) have then to face several consistent expenses concerning routers: they first have to purchase the routers, they have to maintain them periodically and when they fault, it also occurs they have to completely replace the router if it breaks down or if it is stolen. On top of that they also have to send employees to execute the needed maintenance or replacement operations, and these employees need to be trained and to have a partial or sometimes a detailed knowledge of the routers.

Furthermore, DSOs have to face similar expenses for most of the devices installed in their substations (low voltage managers, fault detection devices, peripheral units, etc...), *Gridspertise* then thought of coming up with a single device able to provide with some of the functions which are currently provided by multiple physical devices.

The device in question is the **edge device** which this study described both from a software and a hardware perspective. In its first version it promises to implement: **a virtual router**, a virtual peripheral unit (a device which enables remote controlling of the electrical components, mainly switches, present in substations), a virtual low voltage manager (which is a device able to collect DSOs low voltage clients data, and to execute operations concerning low voltage lines and users) and a virtual fault detection solution (which, when a fault happens, is mainly able to understand which kind of fault that is, and on which line it has occurred).

The purchase cost lowers when compared to the sum of costs of multiple products, and the maintenance operations could be simplified if the devices were virtually implemented: for instance what could before be done by replacing a physical router can now potentially be achieved by a simple restart of the "router application".

This thesis work will then meet his **second goal a review of the state of the art of virtual routers** and their implementation scenarios.

The study will then focus on its **third and last goal, the testing of a first version of a virtual router aimed at verifying the functions it came provided with match the requirements of the smart grid scenario, and more specifically the requirements of DSOs study cases**, the virtual router is installed as a *Docker Container* onto the edge device. **The router responds partially**, from a networking point of view, to the needs of DSOs study cases.

The functions it offered and that were tested are:

- **Dynamic Host Configuration Protocol (DHCP) server.**

This is a function that enables the router to assign IP addresses to connected devices. Here is a scenario where this function could be useful: DSOs could need

to ask an operator who is not accustomed to Telecommunication protocols to execute a task on the router, DHCP would allow the operator to carry out the task without having to set its own device's IP address manually.

- **Secure SHell (SSH) and Hypertext Transfer Protocol Secure (HTTPS) over Wide Area Network (WAN) and Local Area Network (LAN).**

These are protocols enabling expert operators to configure the router. They are essential both before and after deploying the router.

- **Firewalling.**

Firewalling assures only traffic from specific networks and ports are allowed to flow into the router. This is an important security feature.

- **Network Address Translation (NAT)**

This function allows to redirect targeted incoming traffic (which is to say: traffic flowing in through a specific network and port) to another given port and network.

This feature is quite useful in a variety of field of applications.

- **Static routing.**

Static routing is the basic routing function. If not present a router can not be called that. Given an IP address, which the router is able to reach, traffic transmitted to that address must be routed correctly.

- **Internet Protocol Security (IPSec)**

This is a useful security function, it enables to use VPNs (Virtual Private Networks).

Given two peers sharing a common set of security parameters, they must be able to establish a connection (usually called a tunnel when speaking about IPSec).

This study presents the methodologies adopted to carry out testing of the above listed functions, and the results of testing, to eventually draw its conclusions basing on the reviewed literature and the conducted tests.



# Contents

<b>1</b>	<b>Introduction.</b>	1
1.1	A history of power distribution. . . . .	1
1.2	Modern power distribution. . . . .	2
1.2.1	A key distribution network node: the primary substation. . .	3
1.2.2	A key distribution network node: the secondary substation. .	5
1.3	Quality of Service: The Italian authority ARERA. . . . .	7
<b>2</b>	<b>Remote Controlling and Automation.</b>	9
2.1	Remote controlling for DSOs. . . . .	12
2.1.1	Importance of the treatment of neutral points in power networks [6]. . . . .	14
2.2	Automation for DSOs. . . . .	15
2.2.1	A legacy automation tactic: FRG (Fault Detecting Function) [16]. . . . .	15
2.2.2	A legacy automation tactic: FNC (Compensated Neutral Function) [16]. . . . .	16
2.2.3	Latest automation tactics: FSL (Logical Selectivity Function) [16]. . . . .	19
2.2.4	Latest automation tactics: SFS (Smart Fault Selection) [16].	21
2.2.5	Latest automation tactics: SHA (Self Healing Automation) [16]. . . . .	22
<b>3</b>	<b>Communications for the Smart Grid.</b>	31
3.1	Network infrastructure for the smart grid. . . . .	31
3.2	Communications for the Distribution Network. . . . .	32
3.3	Communication techniques research for the smart grid. . . . .	33
3.4	Cybersecurity for the smart grid. . . . .	34
<b>4</b>	<b>Virtualization and edge computing.</b>	35
4.1	Edge Computing. [46] . . . . .	35
4.2	Virtualization. . . . .	36
4.3	Virtual routers. . . . .	37

<b>5</b>	<b>The edge device scenario and the virtual router.</b>	<b>41</b>
5.1	The Edge Device. . . . .	41
5.1.1	Hardware. . . . .	42
5.1.2	Software. . . . .	43
5.2	The virtual router solution. . . . .	43
<b>6</b>	<b>IP and Routers: the tested functions.</b>	<b>45</b>
6.1	The Internet Protocol (IP). [5] . . . . .	45
6.2	Determining whether the destination is local or remote: the router. [5]	46
6.2.1	IP addressing. [5] . . . . .	46
6.2.2	IP addresses. . . . .	47
6.2.3	Subnet Masks [5] . . . . .	48
6.3	The tested functions. . . . .	49
6.3.1	Manual IP address configuration. [5] . . . . .	50
6.3.2	DHCP. [5] . . . . .	50
6.3.3	Firewalls. [8] . . . . .	55
6.3.4	NAT. [55] . . . . .	57
6.3.5	IPSec. [50] . . . . .	57
6.3.6	SSH and HTTPS. . . . .	59
<b>7</b>	<b>Testing objectives.</b>	<b>63</b>
7.1	The laboratory scenario. . . . .	64
<b>8</b>	<b>Methodologies.</b>	<b>67</b>
8.1	User Interface of the virtual router. . . . .	67
8.1.1	Status page. . . . .	68
8.1.2	Status Overview Page. . . . .	68
8.2	Web Administrator Interface of the virtual router. . . . .	69
8.3	Test Case: DHCP server. . . . .	69
8.3.1	Test Case Pre-requisite. . . . .	70
8.3.2	Test Case Objectives. . . . .	71
8.3.3	Test Case Procedure. . . . .	72
8.4	Test Case: SSH and HTTPS Applications over LAN and WAN Interfaces. . . . .	72
8.4.1	Test Case Pre-requisite. . . . .	72
8.4.2	Test Case Objective. . . . .	72
8.4.3	Test Case Procedure. . . . .	72
8.5	Test Case IPSec VPN. . . . .	73
8.5.1	Test Case Pre-Requisite. . . . .	73
8.5.2	Test Case Objective. . . . .	73
8.5.3	Test Case Procedure. . . . .	73
8.6	Test Case Firewall. . . . .	74
8.6.1	Test Case Pre-Requisite. . . . .	74

8.6.2	Test Case Objective. . . . .	75
8.6.3	Test Case Procedure. . . . .	75
8.7	Test Case NAT. . . . .	75
8.7.1	Test Case Pre-Requisite . . . . .	75
8.7.2	Test Case Objective. . . . .	75
8.7.3	Test Case Procedure. . . . .	76
8.8	Test Case Static Routing. . . . .	76
8.8.1	Test Case Pre-Requisite. . . . .	76
8.8.2	Test Case Objective. . . . .	76
8.8.3	Test Case Procedure. . . . .	76
<b>9</b>	<b>Results</b>	<b>85</b>
9.1	DHCP server. . . . .	85
9.2	SSH and HTTPS Applications over LAN and WAN Interfaces. . . .	85
9.3	IPSec VPN. . . . .	88
9.4	Firewall. . . . .	88
9.5	NAT. . . . .	90
9.6	Static Routing. . . . .	90
<b>10</b>	<b>Conclusions and further development.</b>	<b>93</b>
	<b>References</b>	<b>96</b>

# Chapter 1

## Introduction.

### 1.1 A history of power distribution.

Electric power transmission goes back to the 19th century and it refers to the movement of power from the place where it is generated to the place where its deployment is needed. Before that, when power needed to be moved other technologies were used, such as:

- Telodynamic transmission, which makes use of cables to move loads.
- Pneumatic transmission, which uses pressurized air.
- Hydraulic transmission, which make use of pressurized fluids.

In a first phase transmission of electric power was quite inefficient. Defining:

- The electric power  $P$  generated by an electric current  $I$  flowing through an electric potential difference  $V$  as:  $P = VI$ ;
- a generator as a system of devices which is used to generate power usually through combustion, in the late 19th century mainly of coal;
- a load as a component or set of components consuming power;

there were two main reasons behind such inefficiency: on one hand devices needing different voltages, and thus different power levels, required a wide variety of generators to be deployed (each generator answering to a given voltage need), on the other the generators had to be relatively close to their loads (the lower the voltage needed by a load the closer the generator had to be placed to that load) or the power dissipated while being transported to the load would be too much.

A significant contribution to the development of the electric power distribution system was given by Mr *George Westinghouse*, an engineer who noticed that long distance transmission would realistically be possible only using high voltages and

that realistically affordable transformer technology was available for alternating current.

Given a certain amount of power to be delivered ( $P_d$ ) this could be either delivered as  $P_d = V_d I_d$  or as  $P_d = 2V_d \times \frac{1}{2}I_d$ . The second formulation would allow to decrease the current, which would in turn reduce the amount of power dissipated due to Joule's law:  $P_j = I_d^2 R$ , where  $R$  is the resistance of the conductor current  $I_d$  is flowing through.

Combining higher voltages and alternating currents, Mr Westinghouse noticed, it would be possible to reduce the variety of generators needed, thanks to the deployment of transformers, and to locate the generators further away from the loads, the first long distance line running on alternating current was build for *Turin's International Exhibition* of 1884.

When Electric power transmission started to spread, it became clear that it was economically and industrially advantageous to encourage its use and development. The movement of electricity generated by high voltage differences thus came to be called *transmission* and the movement of electricity generated by medium voltage differences came to be called *distribution*. Table 1.1 reports which voltage range belongs to which voltage category.

Definition	Voltage Range
Low Voltage	1 - 1000 V
Medium Voltage	1 - 100 KV
High Voltage	100 - 345 KV
Extremely High Voltage	345 - 765 KV
Ultra High Voltage	> 765 KV

Table 1.1: Voltage Ranges

## 1.2 Modern power distribution.

Before discussing why the functions provided by **routers** are essential to a modern Power Distribution Network, it is worth picturing a meaningful scenario of how power is nowadays produced, transmitted and distributed, focusing, as one may correctly think, on the distribution system.

The key elements in a power network (which is sometimes referred to as **grid**) are:

- *power infrastructure*, this is the infrastructure actually involved in distributing and transmitting power, power lines, substations belong to this category;
- *measurement tools*, they gather raw data concerning the status of the infrastructure, voltmeters and amperometers belong to this category;

- *communication infrastructure*, this infrastructure allows elements in the grid to exchange data over a variety of protocols, routers would belong to this kind of system;
- *control and detection systems*, this is the set of devices that analyzes data, usually coming from measurement tools, and detect anomalies, fault detecting devices belong to this category;
- *operating systems*, they allow operators to act remotely on different kinds of elements in the network.

The Distribution network is a fundamental part involved in that process which allows vastly distributed consumers areas to receive power which is mainly produced in centralized generation facilities.

When it comes to generating power, there are several technologies involved. As Mr. Boillot states in his book "Advanced Smart Grids for Distribution System Operators" [6]:

"...there are many sources of energy generation, notably fossil fuels (gas and coal-fired power stations), nuclear and hydraulic (from run of the river to great dams). These generation sources, known historically as "centralized", were developed in a relatively small number and were capable of supporting the needs of a large number of consumers."

The power thus produced is transmitted at high voltage ranges (see table 1.1 for a detailed voltage range definition) over long distances minimizing the losses due to Joule's effect, this phenomenon was explained in section 1.1.

The transmission network competence stops at the first kind of distribution network infrastructure, and one of the most important, the *primary substation*. From primary substations the potential difference falls into the "Medium Voltage" (MV) range.

Power travels along MV lines to reach *secondary substations* where it can either be directly delivered to a client (medium to large industries and factories might have need of a medium voltage power delivery, they are known as medium voltage clients), or can be further dropped down to enter the "Low Voltage" (LV) range and be eventually delivered to LV clients (households are fitting examples of LV clients), see figure 1.1 for a schematized representation of the modern power network.

### 1.2.1 A key distribution network node: the primary substation.

"HV (High Voltage)-to-MV (Medium Voltage) stations, known as primary substations, are the link between transmission and distribution networks." [6]

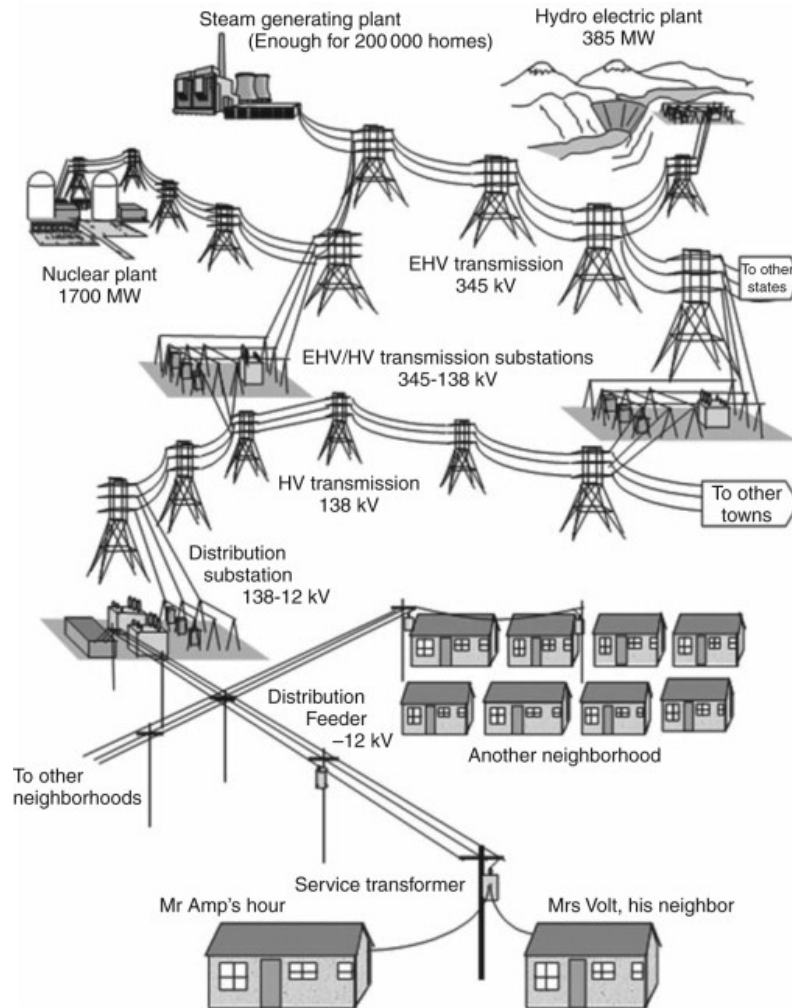


Figure 1.1: Power networks: generation, transmission and distribution scheme.

As Mr. Boillot says in his book, primary substations are the starting point of distribution networks. They are the place where the voltage incoming through high voltage (around 100 kV) lines is dropped down to become what is called "Medium Voltage" (around 20 kV).

They are home to what is usually referred in distribution as "the most important component of the network", that is the HV-to-MV transformer (figure 1.2). This kind of electrical machinery is the core of distribution, they are complex in construction and quite expensive (they average around the hundreds of thousands of euros).

Primary substations are an extremely delicate type of node. They can serve tens of thousands of clients, when a primary substation is powered off due to faults the consequences are quite dear for a DSO. Moreover, they can be part of the remotely

controlled network.



Figure 1.2: HV-to-MV transformer in Italy.

### 1.2.2 A key distribution network node: the secondary sub-station.

Similarly to primary substations, presented in section 1.2.1, secondary substation is the kind of node where another kind of voltage transformation takes place. Secondary substations, in fact, house the MV-to-LV transformer, which brings down incoming MV voltage (around 20 kV) to a potential difference which is in the Low Voltage category (at around 220 V), you can see an example of such transformers in figure 1.3b.

Differently from primary substations, whose most used construction model is made out of an outdoor part and an indoor part, secondary substations are mainly developed indoor, in figure 1.3a you can see what an Italian secondary substation looks like from the outside.

Secondary substations also contain what is generally referred to as a *Low Voltage Manager (LVM)*. This is a key device which allows DSOs to acquire information about the power consumed by any individual LV client, it also enables them to activate or deactivate an user, and the most recent kind comes with fraudulent activities detection strategies implemented.

Just like primary substations, secondary substations can be part of the remotely controlled network.

When that is the case, they contain several devices which allow the substation





(a) Secondary substation in Italy.



(b) MV-to-LV Transformer.

Figure 1.3: Secondary substations: the infrastructure and its transformer

to actually be remotely controlled. These devices play an important role in understanding why a router is needed and consequently why its correct operation is paramount. Such devices mainly are:

- A **peripheral unit**, which allows operator to actually connect to the substation.
- A **fault detection device**, which is able to detect anomalies in case of faulting lines.
- A **router**, this is what actually handles communications among inter-substation devices, and in some cases, among intra-substation devices.

Another kind of device should be mentioned given it is still quite used: a modem. The modem allows operator to reach peripheral units of older generations, this technology is gradually being replaced by routers.

## 1.3 Quality of Service: The Italian authority ARERA.

As anticipated in the summary of this thesis work, DSOs are remunerated or penalized depending on their quality of service standards and performance. This, clearly, is not their only income, but it is a significant part of it, and it is usually profoundly cared for, especially considering DSOs might get penalized due to a low quality of service.

In order to better understand how impactful the indicators of quality of service are for a DSO, and to later analyze what are the tactics operators put in place to better them, such as remote controlling and extended telecommunication systems, this thesis work will describe one particular scenario, the Italian one.

The authority which controls Italian DSOs performances in the field of quality of service is called ARERA that stands for "*Autorità di Regolazione per Energia Reti ed Ambiente*" (in english this would be "*Environment and Power Networks Regulating Authority*").

Since year 2000 ARERA started introducing targets of quality of continuity of service with the purpose of monitoring the quality of service DSOs were providing to their clients.

Basing on how they perform with respect to their respective targets, DSOs are either penalized, if they are not able to reach their targets, or remunerated, when they outperform their targets. Such targets are based on the areas where DSOs are operating.

Arera distinguishes, in his published document dedicated to regulating power networks "*Testo integrato della regolazione output-based dei servizi di distribuzione e misura dell' energia elettrica.*" [1], three main area kinds:

- **highly concentrated areas:** these are the areas counting a number of residents bigger than 50.000;
- **averagely concentrated areas:** the areas whose number of residents are between 5.000 and 50.000;
- **low concentration areas:** areas whose number of residents is smaller than or equal to 5.000.

ARERA declares [1]:

- **long interruptions** interruptions lasting more than three minutes;
- **short interruptions** interruptions lasting between one second and three minutes;
- **temporary interruptions** the interruptions lasting less than one second.

Also, ARERA defines [1]:

- the indicator **NILB**, the average number of long and short interruptions in a year for an LV client as:

$$NILB = \frac{\sum_{i=1}^n U_i}{U_{tot}}$$

where  $n$  is the number of short and long interruptions in a year,  $U_i$  is the number of LV clients affected by the  $i$ -th interruption, and  $U_{tot}$  is the total number of LV clients.

- the indicator **DIL**, the average duration of long interruptions per LV client as:

$$DIL = \frac{\sum_{i=1}^n \sum_{j=1}^m (U_{ij} t_{ij})}{U_{tot}}$$

where  $n$  is the number of long interruptions in a year, for each long interruption  $m$  is the number of groups of clients affected by the same interruption duration,  $U_{ij}$  is the number of clients involved in the  $i$ -th interruption and belonging to the  $j$ -th group,  $t_{ij}$  is the duration of the  $i$ -th interruption for the  $j$ -th group and  $U_{tot}$  is the total number of LV clients.

ARERA then established a target value of **DIL** and **NILB** per area kind, DSOs work towards matching that requirement.

## Chapter 2

# Remote Controlling and Automation.

As stated in chapter 1, section 1.3, DSOs demonstrate a strong interest in being able to improve and deliver a high quality of continuity of service. Before describing what solutions they came up with historically and what are the latest state of the art tactics, it is worthwhile to understand what the main challenges are that they have to face when dealing with quality of service and which pieces and devices of the power distribution infrastructure are involved in the process.

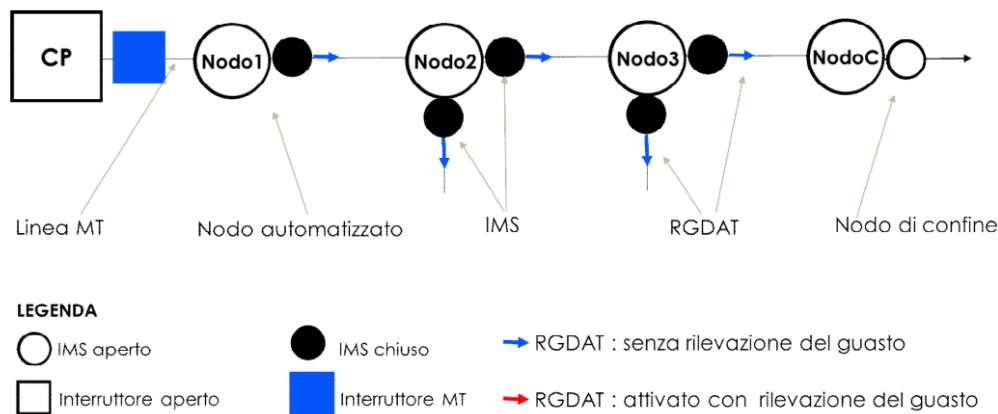


Figure 2.1: MV line standard topology [16].

Figure 2.1 pictures what a normal MV line looks like, it displays all the elements involved in remote controlling and all the relevant elements affected by a fault.

The scheme is taken from an Italian DSO's work instruction [16], a translation of the legend is provided in table 2.1.

Now that the elements involved in a fault are known it is paramount to also

Element	English translation
IMS aperto	Open switch
IMS chiuso	Closed switch
RGDAT: senza rilevazione del guasto	Fault and voltage absence decting device, with fault dection turned off
RGDAT: senza rilevazione del guasto	Fault and voltage absence decting device
Interruttore aperto	Open switch with higher extinguishing power for MV lines
Interruttore MT	Closed switch with higher extinguishing power for MV lines
Nodo	Node
Nodo automatizzato	Automated Node
Nodo di confine	Last node of the line
Linea MT	MV Line
CP	Primary substation

Table 2.1: English legend for figure 2.1

understand what a fault is.

As Mr Tleis states in his book "*Power System Modelling and Fault Analysis*" [51],

"A fault on a power system is an abnormal condition that involves an electrical failure of power system equipment operating at one of the primary voltages within the system."

Faults are mainly of two kinds [51]:

- Phase to phase faults, which are usually caused by an event allowing to phases of a line to make contact, these kind of faults are characterized by a very high fault current;
- Phase to earth faults, which usually occur when one of more phases of a line are able, due to an external event, to discharge to the ground, these kind of faults are characterized by a high fault current.

What is a phase then? One must consider that modern power networks are three phase systems. In an extreme simplification of the system, considering that detailing the characteristics of a three phase system would be enough work for a complete thesis of its own, a three phase system requires that MV lines are build using three distinct cables, or conductors.

Using three phases allows a power network to be more stable and reliable, besides accounting for an optimized generation, transmission and distribution of power [24].

When referring to a phase of an MV line, this thesis works means to refer to one of the three cables of the MV line in question .

Among the most common causes of faults there are: vegetation entering in contact with a line, fauna erroneously touching a line, lightning striking a pole holding a line and thievery. Faults increase in number during the hottest periods of the year.

Faults are quite inconvenient for DSOs, not only they could damage their quite expensive electrical machinery due to their abnormally high currents (see chapter 1, section 1.2.1), but they also have an impact, a negative impact, on the calculation of their quality of continuity of service indicators, as explained in chapter 1, section 1.3, as they usually cause interruptions.

Now, before moving on to explain why developing automation is essential in the effort of trying to reduce the duration and number of interruptions, it would be useful to understand what happens if an interruption was to occur due to a fault in a scenario where DSOs did not implement any measure to reduce its duration. Figure 2.2 depicts the scenario just described, the legend is the same one reported in figure 2.1 and table 2.1.

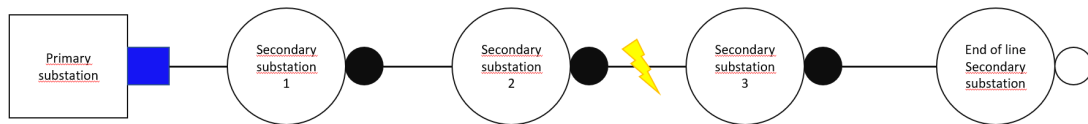


Figure 2.2: MV line without any remote controlling implemented experiences a fault.

In figure 2.2, a fault has occurred between nodes, secondary substations to be precise, 2 and 3.

Since the DSO operating the line has not implemented any tactics to reduce the duration of the interruption caused by the fault, it is not aware of the fault occurring nor of where it has occurred.

The first acknowledgment of the fault by the DSO happens when a client reaches out to the DSO to complain about a lack of power on their end.

At this point the DSO is aware of a fault happening, and using the position of the client who contacted them, is able to understand which line is involved.

That is all the information the DSO has, and this leads to introducing the main activities DSOs are involved in when they discover a fault:

- firstly they need to locate the fault precisely;
- secondly they have to provide the affected clients back with power in as little time as possible.

Going back to the scenario depicted in figure 2.2, the DSO is now aware of the fault and has to locate it. The only way it can do so is by sending operators to the line, and asking them to inspect it. Inspecting a line means analysing it along its

entire length (which for MV lines is usually of the order of the tens of kilometers, the line built for Turin's International Exhibition of 1884, mentioned in section 1.1, was 34 Km long) or until they discover the point where the fault has occurred. This operation can take hours, negatively affecting the **DIL** indicator.

Once the employees are able to visibly locate the branch of the line affected by the fault, they have to reach the node where that branch starts from an open the switch connecting the node to the branch (figure 2.3a), to protect themselves while they are repairing the fault, then they have to go to the node where the affected branch ends and open the switch connecting the affected branch and that node (figure 2.3b).

Eventually, they need to go to the end-of-line node and close the switch that connects the affected line to another line. This enables affected client to start receiving back power, at this point they can start the repair operation on the faulted branch (figure 2.3c).

## 2.1 Remote controlling for DSOs.

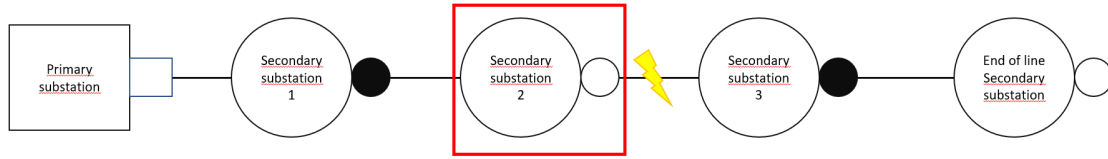
The strategies DSOs deploy when it comes to dealing with faults aim at:

- Reducing the duration of an interruption caused by a fault, this is usually achieved by developing tactics that allow the operations described in section 2 to be executed in as little time as possible, this action affects positively the **DIL** indicator.
- Reducing the number of faults. This is mainly achieved by an effective planning and maintenance of the network. Being able to locate quickly the fault helps in avoiding to overstimulate the network and concurs to its being in good health, this action affects positively the **NILB** indicator.

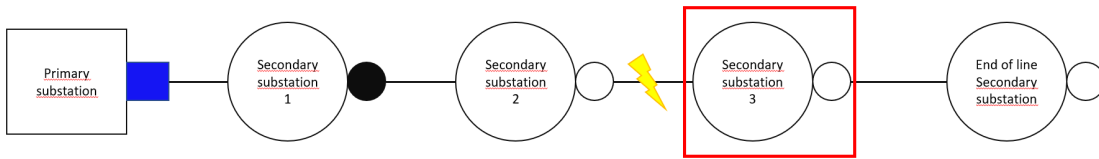
The key field for developing effective tactics that DSOs can use to reduce the duration of interruptions is telecommunications. In this section there will be described legacy automation tactics, and more recent automation tactics, which require to be run over an *LTE* (Long-Term Evolution) network or possibly an *optic fibre network* and use **IP**.

The key technologies used in DSOs' effort to improve their quality of continuity of service are: remote controlling and automation.

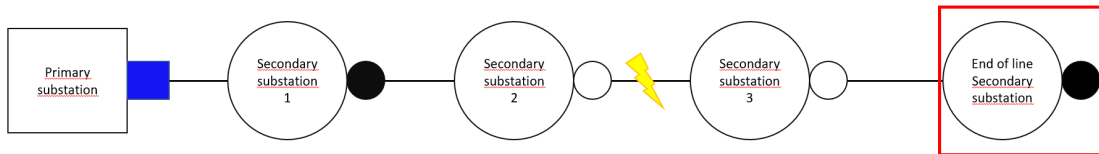
- Remote controlling allows operators to act on a substation, mainly to open or close a switch, remotely, without having to physically reach the substation.
- Automation allows substations to act upon a fault occurrence without having to wait for an operator to send commands or to physically reach them.



(a) Step 2 of handling a fault when no remote controlling is available .



(b) Step 3 of handling a fault when no remote controlling is available.



(c) Step 4 of handling a fault when no remote controlling is available.

Figure 2.3: Handling of a fault along an MV line after inspection of the line.

As anticipated in section 1.2.2 if DSOs are interested in letting a secondary substation being remotely controllable they need to install a set of specific devices in it. The devices adopted by *e-distribuzione* for a secondary substation to become remotely controllable are :

- A *peripheral unit (UP)*, which enacts the commands received by operators from control rooms, an UP per substation is required;
- A *modem*, which enables control rooms to reach older generation peripheral units through **GSM** (Global System for Mobile communications) [14][19], a modem per substation is required .
- A **router**, enabling control rooms to reach latest generation of UPs, using IP, over **LTE** [15] or possibly optic fibre, a router per substation is required.



- **IMs** [16], switches that can be maneuvered remotely or not, when a line is under normal operating conditions (i.e. no fault current is flowing through it), one IMS or ICS per MV line is required.
- **ICs** [16], switches that can be maneuvered remotely or not, even when a fault current is flowing through a line. A switch similar to this kind is always installed in primary substations ("Interruttore MT"), so that if a fault occurs operators are always able to isolate the whole involved line, installing these in secondary substations allows operator to avoid powering off the whole line in case of fault (it concurs in improving the DIL and NILB indicators), one IMS or ICS per MV line is required.

The additional devices they install in order to automate a secondary substation are:

- An **RGDAT** [16], a fault detecting device. It alerts the UP when a fault occurs so that it can act on the IMS or ICS of that MV line, it understand if the fault is phase-to-phase or phase-to-ground, one RGDAT per MV line is required.
- An **RGDM** [16], a new generation fault detecting device that requires an ICS and, differently from an RGDAT, can be directly connected to it and governs it, , it understands if the fault is phase-to-phase or phase-to-ground, it is able to generate packets using standard *IEC 61850* one RGDM per MV line is required.

RGDMs and ICs and *routers* are necessary for latest automation tactics to be deployed.

### 2.1.1 Impotence of the treatment of neutral points in power networks [6].

The neutral point of a line is the contact point between the HV-to-MV transformer to ground in primary substations. Its treatment in power networks is essential because, as Mr Boillot states in his book:

"Neutral point treatment defines the maximum level of a ground fault current in the network, and by extent, the fault detection system, thus profoundly influencing the level of quality ."[6]

On top of that, depending on the presence or absence of certain kind of neutral point treatments, a selection of automation tactics may or may not be available.

Depending on the way DSOs decide to handle this very important connection, the characteristics of the line will change, table 2.2 reports what kind of line characteristics come with their respective way of treating the neutral point.

Neutral point treatment	Characteristics
Neutral grounded via impedance	Simple protection, but risk of power surge
Isolated Neutral	Difficult Fault localization
Directly grounded neutral	Fault Current is very high and risk of damage
Compensated neutral	High level of security but complex protections

Table 2.2: Type of neutral point treatments VS respective characteristic

As of 2014, the year when Mr Boillot’s book was published, North America, areas of South America, Australia and more broadly countries experiencing a strong USA influence together with the UK, adopted some sort of *directly grounded neutral*. Usually the choice of protections of the HV-to-MV transformers is quite limited in these cases, DSOs often opt to install fuses, which is a rudimentary solution causing a delay in the development of automation tactics.

European countries preferred to opt for a *compensated neutral point treatment*, this kind of treatment allows to lower the intensity of phase-to-ground fault currents allowing the line to withstand it for longer periods of time, this is the case in Poland, Germany and Hungary, this kind of neutral treatment is achievable thanks to the installation of **Petersen coils**.

Norway, Sweden, Spain, areas of China and Italy adopted an *isolated neutral point treatment*, even though in Italy the use of compensated neutral point treatment is quite diffused, to the point *e-distribuzione* has developed automation tactics specifically for compensated neutral point treatment lines (FNC being one of them).

*Neutral via impedance* is used in Germany and France.

## 2.2 Automation for DSOs.

### 2.2.1 A legacy automation tactic: FRG (Fault Detecting Function) [16].

FRG is the first automation tactic presented in this study, and one of *e-distribuzione*’s legacy automations. This kind of automation uses RGDATs, one of which needs to be installed for every IMS present in a secondary substation, that is to say, as previously stated in section 2.1, one RGDAT per MV line.

The rules regulating when each switch has to be opened are the following:

1. The "Interruttore MT" of the line (see figure 2.1 and table 2.1) closes according to the cycle reported in figure 2.4.  $T_{RR}$  is a short period of time after which the "Interruttore MT" tries to close back up, this operation helps with transitory faults (for instance a tree branch making contact with a line for a short period of time).  $T_{RLi}$  is a long time period after which the "Interruttore MT" tries to close back for the *i-th* time, hoping the fault has ended or that the branch

of the line involved has been successfully isolated. All these time windows are tuned basing on the type and conditions of the line. The "interruttore MT" opens if it senses a fault is happening.

2. An IMS is opened by the UP if for a given amount of time its RGDAT perceives no voltage and has detected a fault current.
3. An IMS is closed if its RGDAT perceives the return of a potential difference. If given IMS is not the only automated one along the same line, then each IMS will have to wait for its turn before being able to close.
4. An IMS is permanently opened if, after closing following rule #3, in a given time window, its RGDAT perceives a fault current again and no potential difference.

The rules regulating FRG are:

1. If the RGDAT senses no incoming voltage for a set period of time and if it has perceived a fault current then its respective switch is opened.
2. If the switch is open and the RGDAT senses an incoming voltage after a time window  $T_c$ , the UP makes the switch close and starts waiting for a time  $T_d$ .
3. If in the  $T_d$  time window the RGDAT does not sense any incoming voltage, the switch is permanently opened, and all the gathered information is sent to a control room.

Figures 2.5 through 2.12 picture an example of fault happening along a MV line which is automated using FRG, for the sake of this example the time windows are set as:  $T_c = 3s$   $T_d = 3s$  and the **initial period** mentioned in rule FRG #1 is set to 35s.

Moreover,  $T_{RL} = 30s$  and  $T_{RLi} = 70$  with  $\{i \in \mathbb{N}, i > 0\}$ , whereas  $T_{RR} = 0$ .

### 2.2.2 A legacy automation tactic: FNC (Compensated Neutral Function) [16].

The FNC automation tactic can only be applied to MV lines whose neutral point is compensated (as explained in section 2.1.1 a compensated neutral point reduces fault currents for phase-to-ground faults, allowing the line to withstand them for longer), and counting maximum 3 substations. If these conditions are met then:

- if the occurring fault is of the kind phase-to-phase, FNC acts the same way FRG does (see 2.2.1);
- if the occurring fault is of the kind phase-to-ground, FNC will act according to the rules explained in this section.

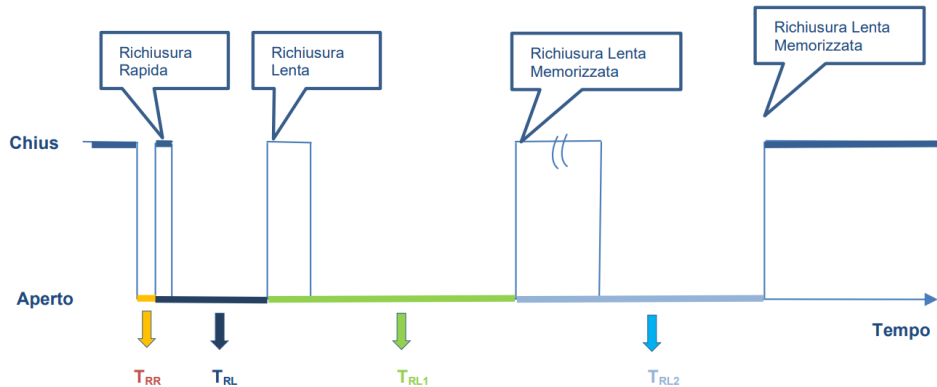


Figure 2.4: Interruttore MT cycle [16].

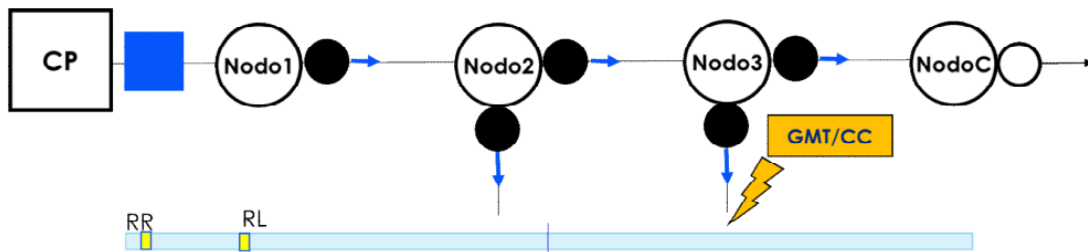


Figure 2.5: A fault occurs on a line starting at "nodo 3", the "interruttore MT" of the line senses it and opens. After  $T_{RR}$  it closes back but the fault is still present so it opens again. After  $T_{RL}$  the "interruttore MT" tries to close again but the fault is still present [16].

The characteristics of FNC are:

- the MV lines are not powered off while the automation locates and then isolates the fault, thus positively impacting both **DIL** and **NILB** indicators;
- the fault is isolated in a maximum amount of time which depends on where the fault has occurred and on whether the switches installed in the line's substations are of the IMS or ICS kind.

The switches of a line automated according to FNC are opened if their RGDAT perceives a fault current and if this perception lasts for a set amount of time, called delay.

The delay of a specific switch of a node in a given line is set depending on its topological position in the line, which is to say, basing on how far it is from the primary substation of that line, the further it is the shorter the opening delay. In

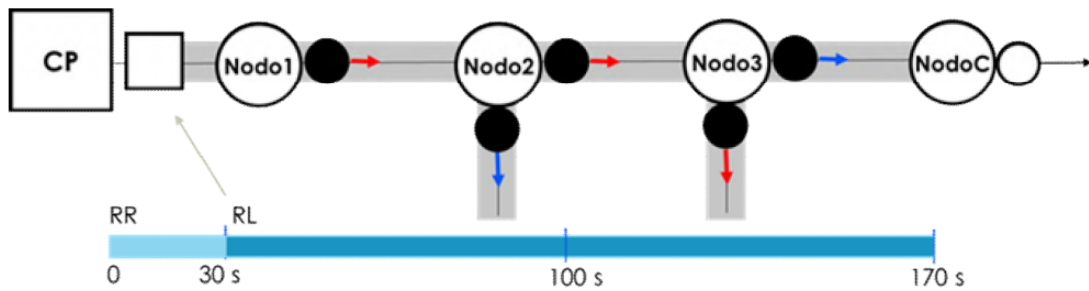


Figure 2.6: "Interruttore MT" then opens again, now the whole line has no voltage.[16].

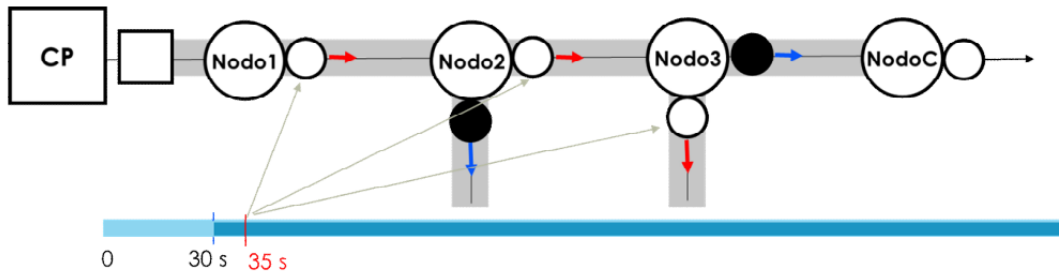


Figure 2.7: After 35 seconds all the switches of the line sensing no incoming voltage and having previously perceived a fault current are opened[16].

other words, a switch in a node further away from the primary substation of that line will be opened sooner than a switch in a node located closer to the primary substation.

When a fault occurs the automation does not begin working instantly, it is instead delayed of a time  $T_d$  which is implemented to let the fault self-exhaust. This is not always the case, and if the fault persists after  $T_d$  seconds, the automation then takes action.

The delays of the substations are:

- 6 seconds for the furthest secondary substation;
- 12 seconds for the second secondary substation of the line;
- 18 seconds for the first secondary substation of the line;
- 20 seconds for the primary substation.

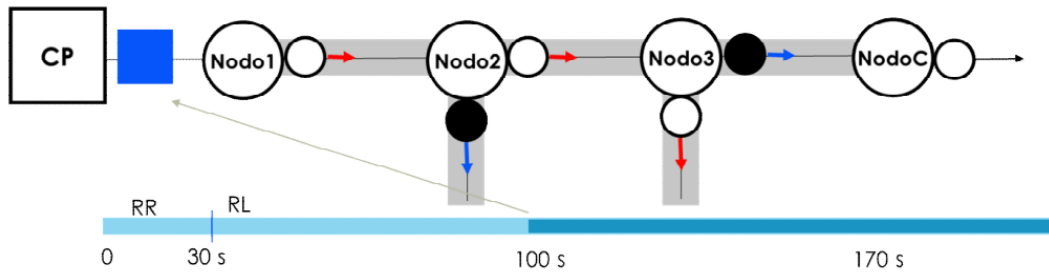


Figure 2.8: After 100 seconds "interruttore MT" closes again, letting voltage come back into the line [16].

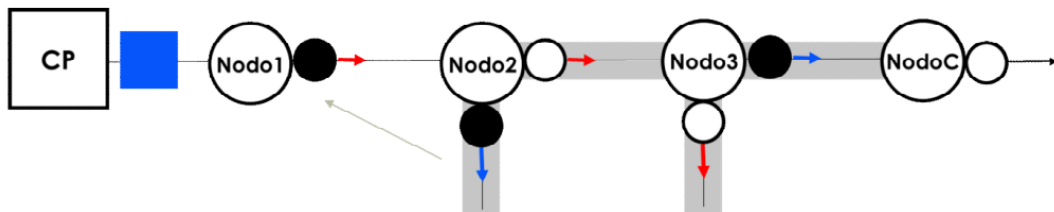


Figure 2.9: When voltage is back, the RGDAT in "nodo 1" senses it and the UP of that substation closes the right switch. After  $T_d$ , given that the RGDAT still senses an incoming voltage, the UP decides that the switch can stay closed and prevents it from opening [16].

Figures 2.14 through 2.17 report an example of a fault phase-to-ground occurring on a line automated via FNC.

### 2.2.3 Latest automation tactics: FSL (Logical Selectivity Function) [16].

A performance improvement with respect to the automation tactics described in sections 2.2.1 and 2.2.2 was achieved when new ones were developed that were no longer based on time delays or constraint that each substation had to respect, but on a strong and quick communication among all automated nodes of a line. This new concept is referred to, in *e-distribuzione* as "logical selectivity", it is different from any kind previously developed mainly in the fact that it needs all nodes of a line to continuously communicate among them, whereas before they each waited their turn to act independently of what other nodes in the line were doing.

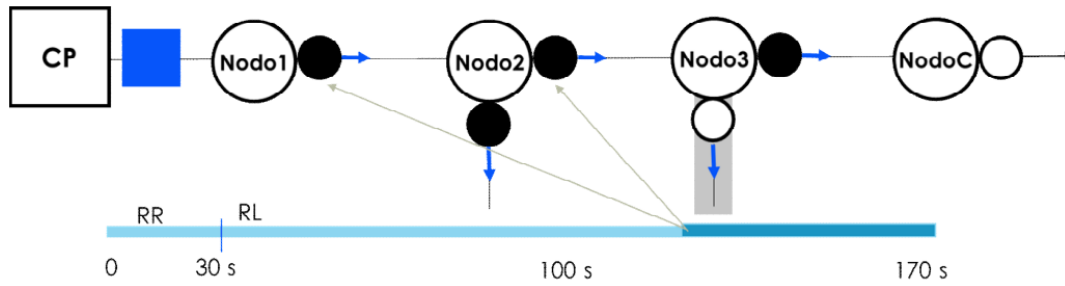


Figure 2.10: The same sequence is repeated for "nodo 2", the line is powered back up to "nodo 3" [16].

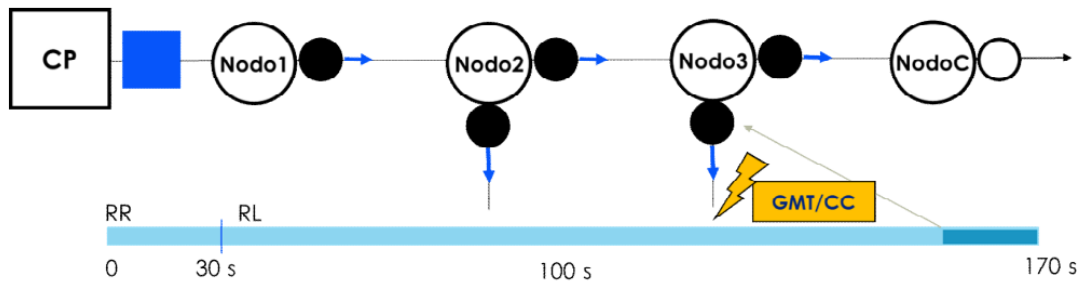


Figure 2.11: When the switch of the line who experienced the fault in "nodo 3" is closed, a fault current will cross the line again [16].

The first ever tactic that uses it is called **FSL** which stands for "Logical Selectivity Function".

These new kind of tactics need a reliable and fast connection (with a latency of a maximum of 100ms), which is deemed only achievable using one of the latest wireless communication standards, **LTE**, or possibly an **optical fibre** connection.

If LTE is used then one must consider that the standard does not assure a maximum latency of 100ms, if the latency is not reachable for certain nodes, then only a few fault kinds can be handled using "Logical Selectivity". These tactics require the line to have a maximum of 3 secondary substation plus the end-of-line secondary substation.

A new actor comes into play which is able to run *IP* and without which these new tactics could not be deployed: the **router**.

Figure 2.18 shows what is the network architecture adopted by DSOs enabling edge-to-edge communications and edge-to-centre communications.

Figure 2.19 shows what the flow of traffic in a secondary substation looks like, highlighting how central the role of the router is. The router transmits and receives IP traffic to and from: the UP, the RGDM and the external networks.

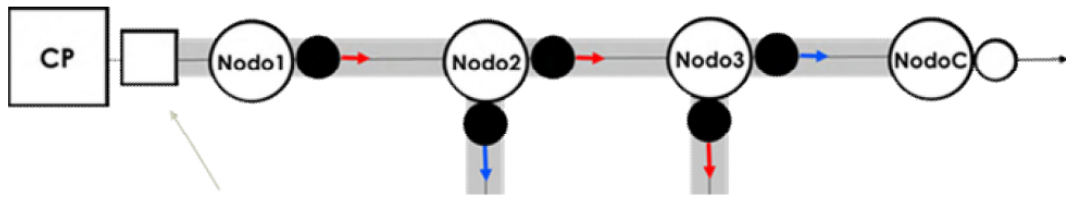


Figure 2.12: "Interruttore MT" will then open again and the line will be powered off[16].

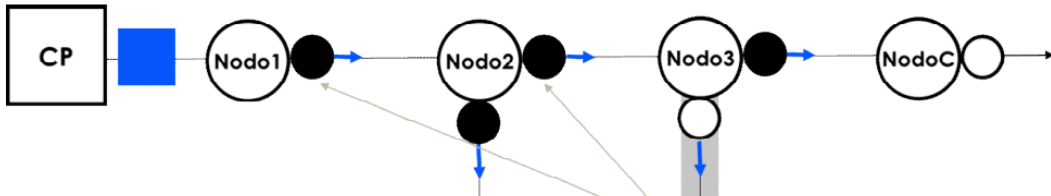


Figure 2.13: The switch whose line has experienced the fault in "nodo 3" will now open and stay that way. All the gathered information is then sent to the control room, and the "interruttore MT" closes again powering back the parts of the line not affected by the fault[16].

The rule in FSL is that when an RGDM senses a fault, it has to alert the RGDM in the node preceding it along the MV line. Figures 2.20 through 2.21 show how the FSL automation works.

#### 2.2.4 Latest automation tactics: SFS (Smart Fault Selection) [16].

SFS automation tactic can be described as the FSL automation tactic with the addition of closing the end-of-line secondary substation switch.

This action allows DSOs to power back the users affected by the fault, using power incoming from a neighbouring MV line. All the operations have to be carried within 1 second so that the interruption falls, at worst, in the "temporary interruption" category (see section 1.3). Figures 2.22 through 2.27 report an example of how SFS works.



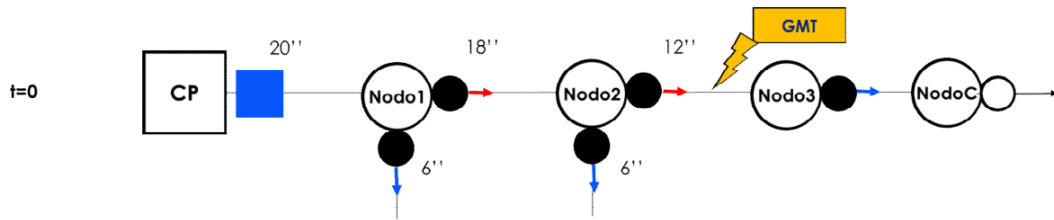


Figure 2.14: A phase-to-ground fault occurs between "nodo 2" and "nodo 3". The fault is sensed in "nodo 1", "nodo 2", and the primary substation, the UPs are alerted and they start to wait [16].

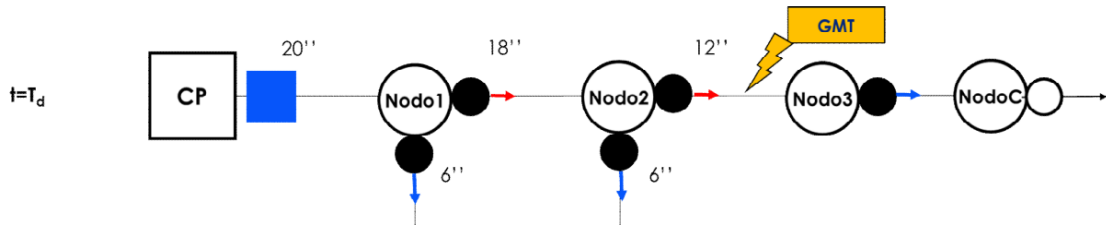


Figure 2.15: The UPs have waited for  $T_d$ [16].

### 2.2.5 Latest automation tactics: SHA (Self Healing Automation) [16].

SHA was built in an attempt to give a line more time to execute all the maneuvers prescribed by an automation by opening the "intruttore MT" located in the primary substation thus powering off the whole line, similarly to what happens in FRG (see section 2.2.1). Opening the "interruttore MT" helps with not overstimulating the line, since no fault current can flow in an open circuit, and allows the automation to take up to 5 seconds to end its processes.

Figures 2.28 through 2.36 show an example of SHA working.

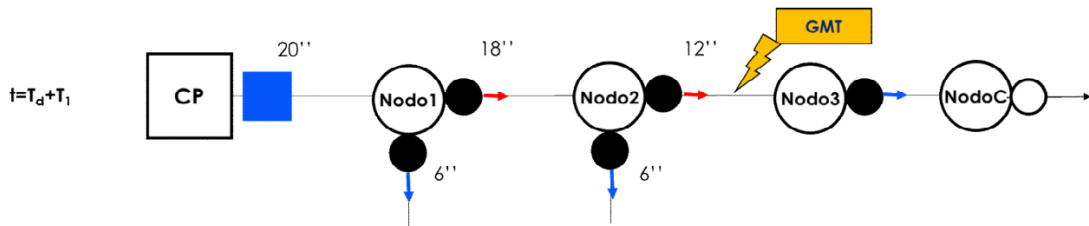


Figure 2.16: After  $T_d$  the UP in the furthest substation experiencing the fault ("nodo 2" in this example) starts waiting for its delay [16].

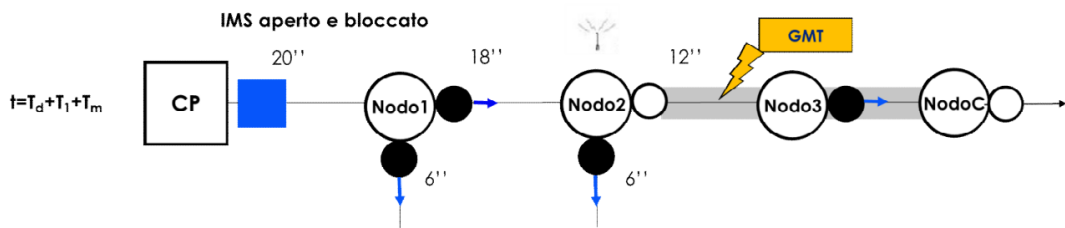


Figure 2.17: After the delay of "nodo 2" the switch is opened, the other nodes do not sense any fault current any more, the procedure has ended [16].

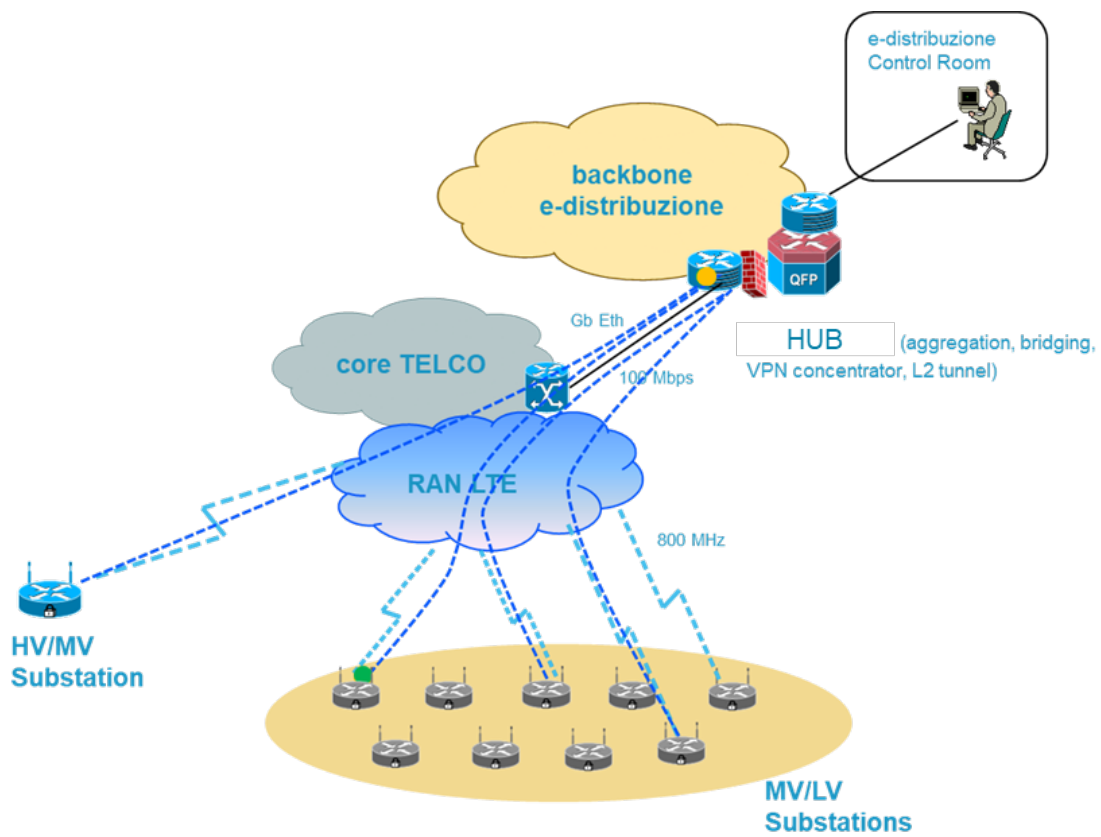


Figure 2.18: DSO's network architecture enabling edge-to-edge communications and edge-to-centre communications [25]

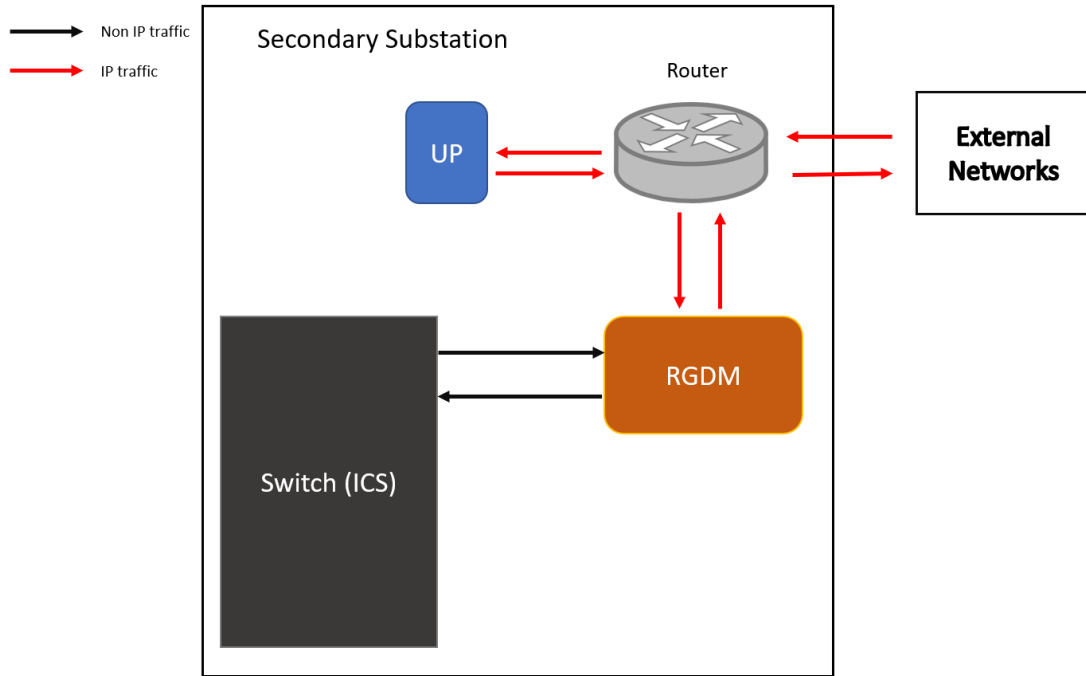


Figure 2.19: Traffic flows between elements involved in automation using logical selectivity of secondary substations.

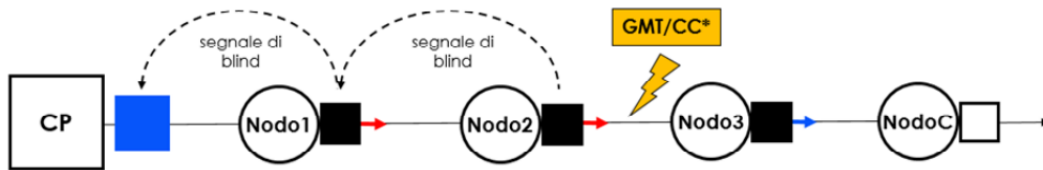


Figure 2.20: A fault occurs between "nodo 2" and "nodo 3", the primary substation, "nodo 1" and "nodo 2" are all able to sense the fault. The primary substation receives a message from "nodo 1" stating that "nodo 1" is able to sense the fault, so the primary substation does not have to open its switch. "Nodo 1" RGDM receives a message from "nodo 2" RGDM, stating that "nodo 2" is able to sense the fault, so "nodo 1" does not open its ICS. "Nodo 2" does not receive any such message, but it is able to sense the fault [16].

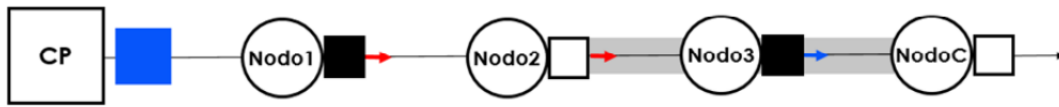


Figure 2.21: "Nodo 2" RGDM has to open its ICS. The procedure has ended.[16]

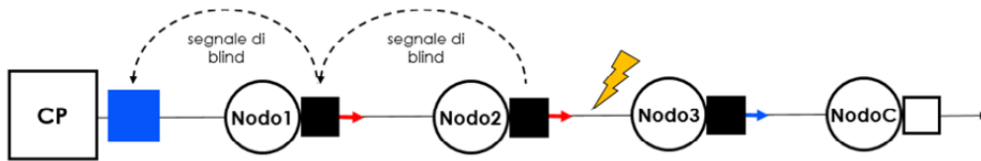


Figure 2.22: A fault occurs between "nodo 2" and "nodo 3", the primary substation, "nodo 1" and "nodo 2" are all able to sense the fault. The primary substation receives a message from "nodo 1" stating that "nodo 1" is able to sense the fault, so the primary substation does not have to open its switch. "Nodo 1" RGDM receives a message from "nodo 2" RGDM, stating that "nodo 2" is able to sense the fault, so "nodo 1" does not open its ICS. "Nodo 2" does not receive any such message, but it is able to sense the fault [16].

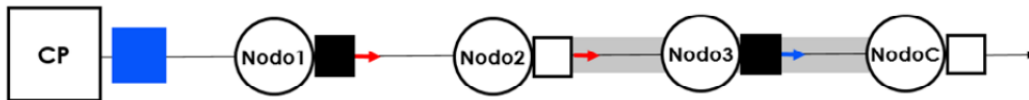


Figure 2.23: "Nodo 2" RGDM has to open its ICS. [16]

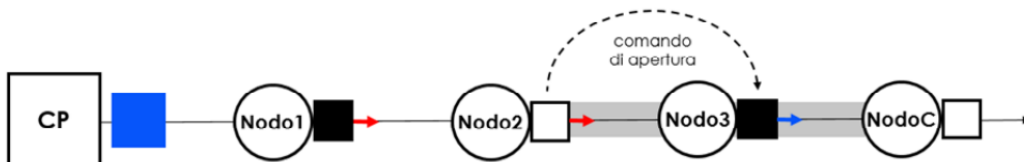


Figure 2.24: "Nodo 2" tells "nodo 3" that it has opened due to a fault and that "nodo 3" should open its switch as well so that it can be later be powered back through the end-of-line substation.[16]

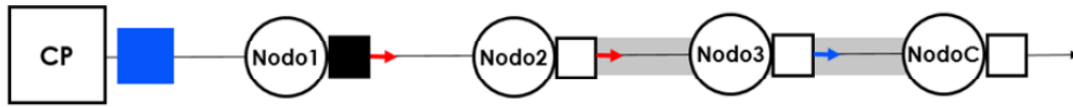


Figure 2.25: "Nodo 3" receives the message and opens its switch. [16]

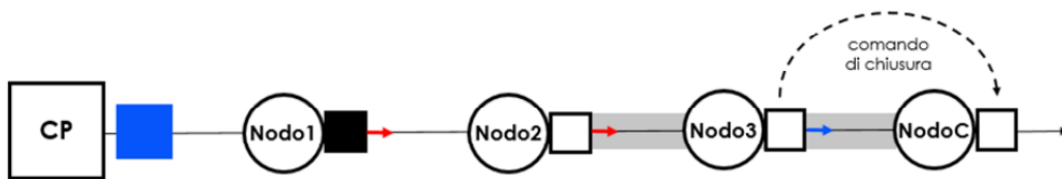


Figure 2.26: "Nodo 3" sends a message to the end-of-line substation asking it to close its switch so that "nodo 3" can be powered back from another line. [16]



Figure 2.27: The end-of-line substation receives the message and closes its switch to allow power coming in through a neighbouring line to power back the users affected by the fault. [16]



Figure 2.28: A fault occurs between "nodo 2" and "nodo 3", the primary substation, "nodo 1" and "nodo 2" are all able to sense the fault.[16]



Figure 2.29: "Interruttore MT" then opens, powering off the whole line. [16]

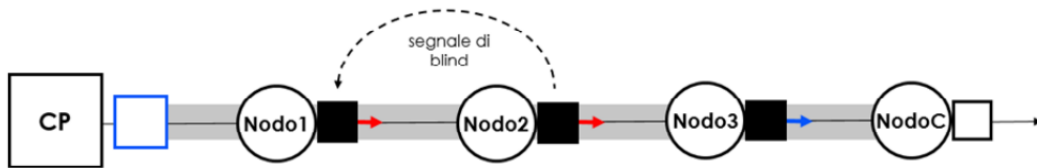


Figure 2.30: "Nodo 1" RGDM receives a message from "nodo 2" RGDM, stating that "nodo 2" is able to sense the fault, so "nodo 1" does not open its ICS.[16]

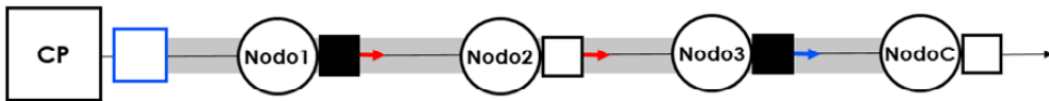


Figure 2.31: "Nodo 2" does not receive any message, so it opens its ICS. [16]

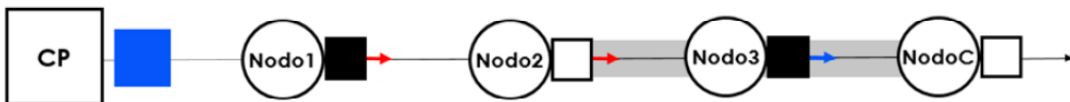


Figure 2.32: "Interruttore MT" closes, powering back up part of the line (up to "nodo 2"). [16]

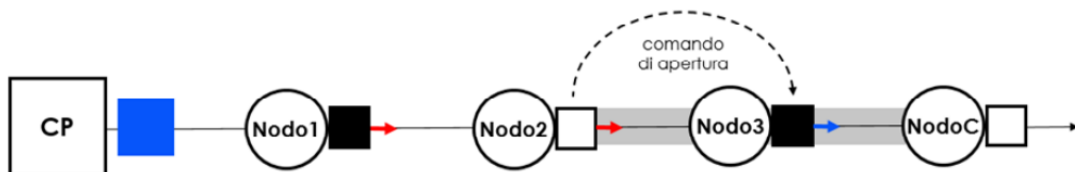


Figure 2.33: "Nodo 2" sends a message to "nodo 3" asking it to open its switch.[16]

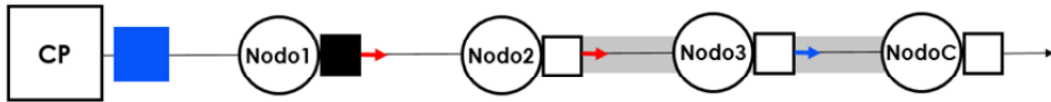


Figure 2.34: "Nodo 3" receives the message and opens its switch.[16]

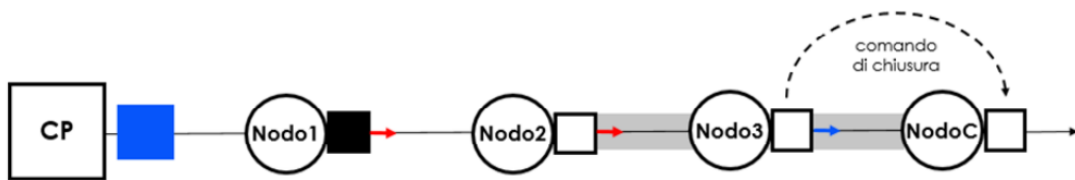


Figure 2.35: "Nodo 3" sends a message to the end of line RGDM asking to close, so that "nodo 3" can receive power from a neighbouring MV line. [16]



Figure 2.36: The end-of-line substation receives the message and closes its switch to allow power coming in through a neighbouring line to power back the users affected by the fault. [16]





## Chapter 3

# Communications for the Smart Grid.

This chapter will present the reader with a review of the network infrastructure of the smart grid and its main characteristics, it will present the main communication standards of the distribution network, the chapter will introduce a few new interesting research fields regarding communications in the smart grid and it will be concluded by a some information about cybersecurity for the smart grid.

### 3.1 Network infrastructure for the smart grid.

This research has introduced in chapter 1 what the energy transmission network looks like from an electrical point of view.

The electrical network presented is backed up by different types of communication networks which this study will present together with their main characteristics, usually a hierarchical three-tiered framework is considered when talking about network infrastructure for the smart grid [27], as displayed in figure 3.1:

- The Wide Area Network (WAN) connects all the main systems involved in power delivery in the smart grid: the Supervisory Control and Data Acquisition (SCADA) system, the Distribution network, the Transmission Network, the energy generating facilities and communication sub-networks are all connected in the WAN. Communications can be wired or wireless and new techniques are being adopted, this research will present a review of the state of the art of such communication techniques in section 3.3.
- The Neighbourhood Area Network (NAN) definition varies depending on the reviewed literature. There are studies defining it as consisting of a few households [27], others define it as consisting of thousands to millions of devices distributed both in rural and urban areas [9]. Generally speaking, the review

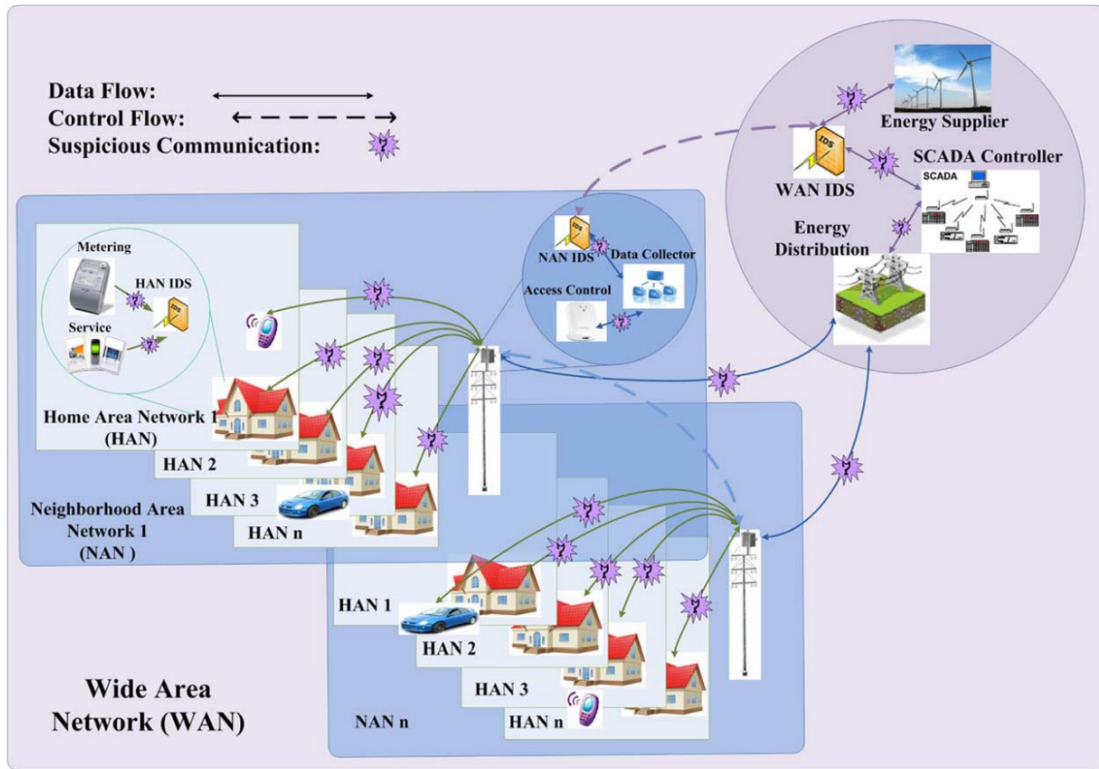


Figure 3.1: Three-tiered communication infrastructure for the smart grid [58]

literature agrees with the fact that NANs are a sub-network of WAN in the smart grid. They include several entities and cover areas of different dimensions. They in turn have sub-networks called Home Area Networks.

- The Home Area Network (HAN) is a sub-network of the NAN and geographically speaking it usually covers the area occupied by a household. It allows to bring smart grid's self-monitoring and auto-balancing features inside the home by exploiting a variety of protocols. HANs allow users to connect remotely to and control their digital devices inside their homes [28].

### 3.2 Communications for the Distribution Network.

When it comes to distribution systems many communications standards are adopted depending on the scenarios where they need to be deployed.

- The latest communications for substations inside a smart grid follow the **IEC 61850** standard. IEC 61850 Edition 1 is a communication standard first released in 2005.

It was originally developed to allow communications for substations automation systems.

In the years since IEC 61850 evolved and it started being used in others fields like: hydro-power systems, wind power systems and distributed power systems.

As new areas started making use of the standard, new sections of it were added and its title was eventually changed from "Communication Network and Systems in Substations" to "Communication Networks and Systems for Power Utility Automation".

Given its versatility, interoperability and long-term stability, it has been chosen as the base communication standard for the next step in power distribution: the **smart grids** [52]. Signals in IEC 61850 have two main categories, time critical signals, transferred through **generic object oriented substation events** or **GOOSE** signals, and **Sampled Measured Values** or **SVM**. GOOSE signals are sporadic and are used by Intelligent Electronic Devices (IEDs) during their protection operations, like the operations introduced in chapter 2. GOOSE messaging is a type of publishersubscribed messaging which travels over Ethernet. SVM on the other hand are usually generated by periodically sampling currents and voltages signals. [2]

- NANs are characterized by the deployment of a wider plethora of communication standards, WiFi is adopted to communicate with the smart metering devices inside the NAN [41], but also 5G and Power Line communications are used, as this study describes in section 3.3.

### 3.3 Communication techniques research for the smart grid.

Smart Grids is a field where information and communication technologies, and networking particularly, play a fundamental role [18].

There are several communication protocols deployed in a smart grid.

There are innovative research fields exploring how to reach remote areas, which are usually not as well connected as urban areas, but show an interesting potential as far as renewable energies are concerned, through a network of energy self-sufficient radio relays nodes [7].

As expressed in chapter 2, the development of smart grids comes with stronger constraint of latency of communications. This brings solution to explore the possibilities offered by **5G**, but 5G equipment requires a significant amount of investment and its effective deployment is estimated to require between 3 and 5 years. Other solutions offering low latency are being studied, for instance **Optical Wireless Communications** (OWC). OWC reuses already existing illumination infrastructure, which is incredibly capillarized, and optical antennas, while still offering low

latency. [59].

5G itself is being explored and several solutions have been proposed to allow to reach areas not as well connected, for instance **Energy Efficient 5G LoRa Ad-Hoc Networks**, LoRa is a technology that provides LOnG RAnge communications at low data rates. [56]

New ways of combining Narrowband Powerline Communications (**NB-PLC**), that is PLC transmitted using the frequency band below 500 KHz, and wireless communications are being studied. [45] [21]

**PLC** is also being explored as the possible communication solution to the problem of *islanding*. Islanding is the phenomenon that takes place when a distributed generator of power (DG) still inputs power in the grid, even if the grid is powered off, degrading ,on the long run, the physical network of the grid. Generally speaking PLC is one of the most explored communication technologies for the smart grid, there are studies focusing on routing approaches for PLC [3].

The theme of smart grids communication is always evolving going hand in hand with the development of the smart grid itself, a wireless optical approach has already being introduced, but there are others, even more impacting. There are studies conducted with the purpose of replacing radio frequencies with **FSOC** (Free Space Optical Communications) which are communication systems using lightwaves (not impactful to nor perceivable by humans) as wireless communication medias, allowing to overcome some of the problems affecting radio frequencies in the smart grid, such as interference or noise or bandwidth constraints [53].

### 3.4 Cybersecurity for the smart grid.

The number of cyber attacks targeting critical infrastructure is growing and so is the need of protecting such infrastructure, and more specifically Cyber Physical Systems (CPSs) like the smart grid, from these incidents. The President's National Infrastructure Advisory Council (NIAC), an American institution involved in infrastructure decisions, has recommended to strengthen defense against cyber attacks too [30].

"Given the vast and complex design of the grid and the increasing sophistication of targeted cyber attacks, risk assessment along with security resource allocation in the grid to prevent cyber intrusions proves to be challenging " [30]

Different methods have been researched in an effort to estimate the right amount of cybersecurity resources needed, including: a Markov Decision Processes (MDP) approach, attack trees and graphs, a multiarmed bandits (MAB) approach and game theory [30].

# Chapter 4

## Virtualization and edge computing.

### 4.1 Edge Computing. [46]

Due to the proliferation of wireless networks and the broader use of the Internet of Things (IoT), the number and amount of data of edge devices have been on a steady and fast increase.

"According to International Data Corporation (IDC) prediction [20], global data will reach 180 zettabytes (ZB), and 70% of the data generated by IoT will be processed on the edge of the network by 2025." [46]

In this scenario the centralized processing cloud-computing approach will not be able to keep up with the data generated by the edge.

The centralized processing approach transfers all the data to the cloud data centre via the network and then exploits its processing power to solve the computing and storage problems, thus inducing a significant economic benefit.

With the inexorable advent of the IoT this approach faces a set of obstacles:

- *latency*: IoT applications do come with real-time constraints, for instance high speed autonomous self-driving vehicles need their data processed in real time.
- *bandwidth*: Transmitting the amount of data produced by edge devices to the cloud will cause great pressure on networks bandwidth, a Boeing 787 produces more than 5GB/s of data.
- *availability*: an always increasing number of Internet services promise a 24/7 continuity of service. It will be a challenge respecting such promise while handling the huge loads of data generated by the edge.

- *energy*: data centres consume a lot of energy. Given the increasing number of sources and amount of data, the energy needed to process it in data centres is bound to become a bottleneck.
- *security and privacy*: a significant amount of data produced by the edge does contain sensible information, for instance indoor cameras generate sensible information regarding the habits of the inhabitants of a household. Transmitting such data to data centres exposes them to potential leakings and other kinds of attacks.

"Edge computing is a new paradigm in which the resources of an edge server are placed at the edge of the Internet, in close proximity to mobile devices, sensors, end users, and the emerging IoT." [46]

Usually the terms used in literature to address such small, edge-located computing hardware are: "fog", "micro data centres", "cloudlets". One thing is certain, they are the counterpart of the consolidated, massive data centres.

The edge of the internet is an interesting place, it is usually located "one hop away" from their associated edge device, it often allows emerging application needs, such as public safety, augmented reality, autonomous driving, to be addressed with low latency

In a regime of *edge-computing*, edge devices are not only consumers of data but they produce data as well, effectively generating two main data flows, or stream of data: one coming from the edge towards data centres, and the other coming from data centres towards the edge.

Edge computing has been adopted in different fields, for instance smart buildings can use it to detect acoustic events [39].

This is the scenario where the **edge device** of Gridspertise comes to play. As stated in chapter 2, the latency for MV lines automated using logical selectivity is under the constraint of being at worse of 100 ms.

Transferring data towards centralized processing units could potentially prevent the automation from working within the planned time intervals by worsening the latency of communications, with a subsequent negative effect on the indicators introduced by the authority and introduced in this study in chapter 1, section 1.3.

That is why Gridspertise proposes a edge-computing solution, where all the needed processing is executed right in secondary substations: the edge device.

## 4.2 Virtualization.

Virtualization is a strategy "*in which a resource's consumers are provided with a virtual rather than physical version of that resource*" [11].

This strategy has helped address a wide variety of problems including: security, high availability, elasticity, efficiency, mobility, fault containment and scalability.

Virtualization has been around for about half a century:

"In the 1960s and 1970s, IBM developed the Control Program/ Cambridge Monitor System (CP/CMS) which led into VM/370. These systems let each user run what appeared to be an isolated system, but all within one timeshared computing environment. "[11]

And again:

"Language-level virtualization was introduced around the 1980s to support application-level portability and isolation (Smalltalk-80, developed by Xerox PARC, is probably the best example of this)."[11]

As one would expect the *World Wide Web* was too affected by virtualization.

For instance, the Java Virtual Machine, introduced by *Sun* in the 1990s, offered developers a chance to add executable content to the Web in a secure and portable manner.

Once the challenges of virtualizing modern computer systems were addressed, the advance of machine-level virtualization was fast and inexorable.

Although Virtual Machines are evidently the most obvious example of virtualization, there are others. Desktop sharing (Virtual Network Computing), virtual storage, virtual networks, **virtual routers** and many more: for instance there are studies already taking into consideration how to virtualize optical transceivers, given how important optical networks appear to be for the future [40].

This thesis work is concerned with the testing of a virtual router. As just explained, a virtual router is a resource, specifically a router, which is not provided in its physical form but virtually, as an application installed in a device.

## 4.3 Virtual routers.

Virtual routers are being used in a variety of communication applications. They are being implemented in 5G networks to obtain router with **faster round trip times for client-server applications** [34].

They come with several benefits, for instance their implementation requires **less human intervention, shorter configuration times** and generally speaking it induces less mistakes [48].

Virtualizing routers also means that more routers can run of the same platform, this incentivizes the implementation of strategies to optimize the use of shared physical resources [22] [23].

Virtual router can also be considered in the effort of increasing energy awareness through the adoption of **virtual routers migration tactics** basing on the traffic flow conditions at a given time [17].



In the field of **network scheduling**, network scheduling is a strategy that dynamically allocates resources in order to satisfy networks requirements through time, there are new techniques, like CreditBank, which allocate resources to virtual routers dynamically basing on the bandwidth requirements at a given time [35].

Virtual router are also used in **educational environments** to allow students to approach and practice networking skills and more specifically to provide students with practical IP networking skills experience [33].

This last scenario is particularly interesting, the researchers have developed a complete virtual network starting by listing out a series of skills they deemed necessary for students to try out after studying the suite of protocols of TCP/IP, these included:

- how to start a router;
- how to connect a router and a PC;
- how to operate a router by commands;
- how to configure different kinds of routing protocols;
- how to read a router's log.

The researchers' program also prescribed students to try to configure a DHCP or NAT on a router.

They describe on their paper [33] how they have developed functions, using User Mode Linux (UML), which enables to run several virtual Linux machines on the same PC, and Java, to create the functions needed to enable students to train the skill above listed, these functions included:

- a function that creates virtual routes for packets to follow;
- a function allowing students to operate routers via command line;
- a function to configure static routing;
- a function to configure dynamic routing;
- a function that outputs logs.

The virtual network they wished to develop included various kinds of devices: virtual routers, virtual hosts and virtual hubs; each device was meant to be virtualized by a virtual Linux machine.

The researchers have then developed a Graphical User Interface (GUI) which enabled users to set up the network they needed, with any number of virtual routers and virtual hosts and which allows to even set the protocols used by any two nodes

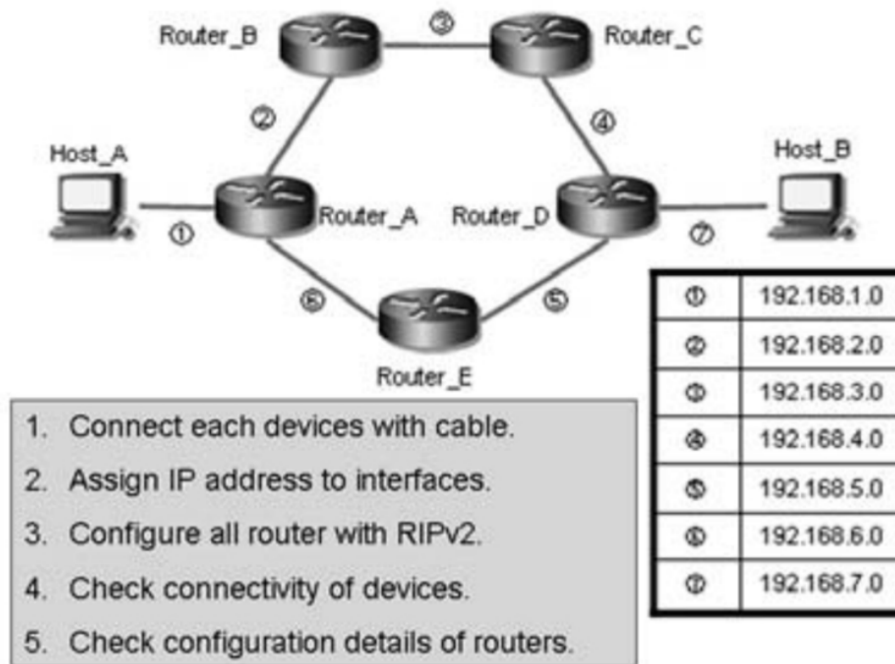


Figure 4.1: GUI presented by researches in the paper "IP Network Construction Learning System utilizing Virtual Router" [33].

of the network, figure 4.1 reports an example of a network set-up.

The deployment of virtual routers for applications in the smart grid scenario appears to not be deeply documented in the reviewed literature. The studied literature suggests that the plan of Gridspertise of implementing such devices in the smart grid scenario is innovative and experimental.



# Chapter 5

## The edge device scenario and the virtual router.

### 5.1 The Edge Device.

As pictured in the summary to this thesis work, the virtual router which was tested is installed on an edge device, meant to be deployed in secondary substations (section 1.2.2).

This section wants to describe what are the characteristics of the edge device in order to allow the reader to better comprehend the limitations and the advantages of the device itself.

The edge device was born out of the idea of providing DSOs with a single device that could offer several other functions, nowadays essential functions, present in a secondary substation and currently executed by different physical devices.

The main devices meant to be found in the edge device object of this study are:

1. an RGDM, introduced in this work in section 2.2;
2. an LVM, or Low Voltage Manager, introduced in section 1.2.2;
3. an UP, or Peripheral Unit, introduced in section 2.1;
4. a virtual router.

The benefits of implementing such a device would be several for DSOs, the principal ones will be presented.

Firstly, buying one device rather than multiple devices has an evident economical efficiency.

Secondly, virtualizing devices would allow DSOs to not have to worry about replenishment of the quantity of replacement units they must have in case of failure of a device. If a failure of a device occurs and the device is virtualized, the solution

would too be a software solution, in many cases a simple restart of the failed virtual device.

Thirdly, DSOs would have the chance of installing in the edge device future virtualized devices that are not yet present as solutions today but might be developed further down the road. Figure 5.1 shows a render of the edge device.



Figure 5.1: Render of the edge device.

### **5.1.1 Hardware.**

Hardware-wise the device was built to communicate, via adequate input/output interfaces, with any device involved with secondary substations, as shown in figure 5.2.

The device comes provided with a Octa-Core 64 bit processor clocked at 3 GHz, 8 Gbytes of RAM, Digital Signal Processors, Graphical Processor Units and an Artificial Intelligence Engine.

All of this is delivered as a SoC solution (System on Chip) that can be deployed in temperatures between 25 and 70 degrees Celcius, with an estimated life-time of more than 10 years.

Moreover, the device is provided several ethernet ports.

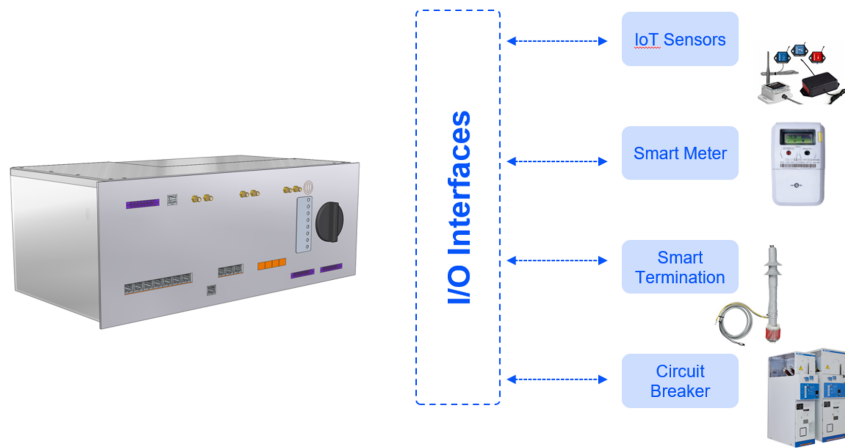


Figure 5.2: Connection between device and other elements.

### 5.1.2 Software.

Software-wise the system runs *Ubuntu Core*, a secure, application-centric IoT OS (Operating System) for embedded devices.

This choice of OS, allows the installation of applications through *Snaps*, a linux proprietary packaging format.

This detail profoundly affects the way virtualized devices are installed onto the device.

Snaps are not uniquely identifiable via different IP addresses, every snap on the device would have to use the same IP address.

This characteristic would make it harder to develop a structure similar to the one described in section 2.2 (see figure 2.19), where each device involved in automation tactics needs a different IP address.

The solution Gridspertise came up with is to use Docker Containers to install applications. Docker containers are another kind of application packaging, still available for Ubuntu Core, which mainly differs from Snaps in the fact that they can be each given a unique IP address.

## 5.2 The virtual router solution.

The virtual router that has been tested for this study is delivered onto the edge device as a docker container. The details of development were not subject to inspection for this study, its focus was instead the correct functioning of the utilities provided by the router with **the purpose of making sure the provided functions work correctly for some of the study cases the smart grid scenario presents.**



## Chapter 6

# IP and Routers: the tested functions.

This chapter will detail what a router is and what are the main characteristics of the **Internet Protocol**, which is the fundamental protocol whose implementation requires the deployment of routers.

### 6.1 The Internet Protocol (IP). [5]

Two people can communicate in a variety of ways: French, Italian, English, even in sign language, but one thing is certain, they must use the same language.

The same principle holds for computers.

TCP/IP is a set of protocols, called a suite of protocols, which explains how two computers can address each other and exchange data.

TCP/IP is the "de facto" suite of protocols of the **Internet**. For the sake of this thesis work, IP, i.e. Internet Protocol, will be explained. IP is the protocol of the network layer, it is the protocol determining the transmitter and receiver addresses of every packet. This function is a fundamental part of one of the main task taking place while running over IP, **routing**.

Every host is given an IP address by the network administrator. An IP address refers to a logical address, differently, for instance, from a *MAC* address, which instead refers to the physical network card of a device.

Here is an example of IP address: 192.168.2.51 .

The address is made of 32 bits, which is to say, 4 bytes. Together with the address, its *subnet mask* needs to be declared, and is used to understand to which network an IP address belongs to. Part of the address will then link a host to its network, another part of the address will uniquely identify the host in its network.

To better grasp this concept here is an example. An host named "Harry" lives in a house whose address is "Via dei Pizzaioli" at number 22. If Harry is to receive



a letter, the address on the letter would be "Via dei Pizzaioli 22", but the letter would be for Harry, not the house.

If "Harry" moves, the address on the letter would change, but the letter would still be for Harry. The house address, in this example, is the logical address (IP address) given to Harry.

IP source and destination addresses are contained in the packet's IP header. A device belonging to the network is responsible for determining if the destination address of a packet is local, that is reachable via one of the links of such device, or remote. This decision is taken basing on the subnet mask of the address of the intended receiver.

## 6.2 Determining whether the destination is local or remote: the router. [5]

IP must know how to get a package to its destination.

If the intended receiver is located on the local network then IP can transmit to it directly. On the other hand, if the destination is on a "remote network", the protocol will pass the packet to the default gateway.

The key device for an IP network is the router. As Mr. Andrew G. Blank states in his book *"TCP/IP Jumpstart: Internet Protocol Basics"*:

"The default gateway, also called a router, is the address of a host of the network, that offers a route off of the network. In other words, the default gateway is the door providing access off of the network."

One could imagine IP working like mailing a letter does. If the sender lives on the same street as the intended receiver, they might be able to deliver the letter themselves. If that is not the case though, the letter would have to be handled by a post office, which would have to figure out a way that letter could be delivered. The post office and the sender, in this simple example that has been introduced, would work as routers, figure 6.1 displays it.

In figure 6.2, Harry (the sender) makes sure that the addressee of their letter is on their same network (checking IP subnet masks), if the addressee is not local then Harry would have to check his own routing table to understand what the best next step of the letter should be, among all possible other reachable routers, if none of the routers that Harry can reach are able to deliver the letter, then Harry would give it to the default gateway.

### 6.2.1 IP addressing. [5]

Every host in an IP network must have a valid address. The address the host has must be unique a network and allows it to send or receive data. Every packet in

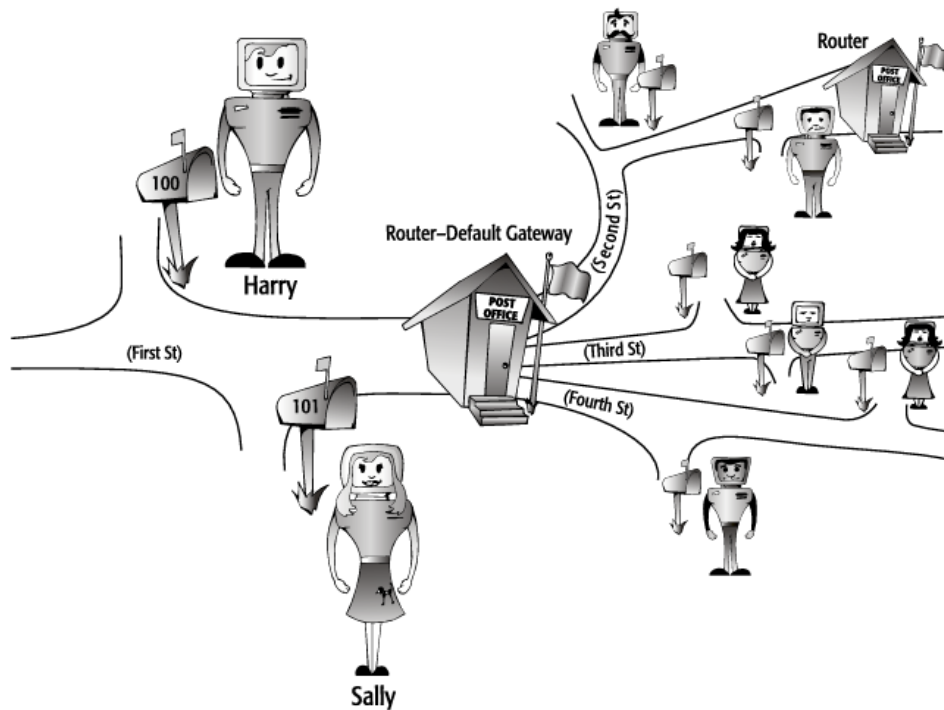


Figure 6.1: Post office as a router example.[5]

the network has a header, in the header the sender and receiver IP addresses can be found, the information is then used to route the packet.

IP addressing then is the action which involves configuring correctly an IP host by giving it a valid IP address. To be successfully connected to the Internet a host need be configured correctly, by having an IP address which not only does identify the host, but the network the host belongs to as well.

An administrator of a network needs to be aware of correct IP addressing techniques to allow hosts on the network to work as intended.

### 6.2.2 IP addresses.

IP addresses are registered on 32 bits. Generally, people prefer using decimal numbers, four decimal numbers, separated by dots, rather than a series of thirty two ones and zeros. This four decimal numbers, each representins 8 bits of the IP address, are called *octets* or **bytes**.

The notation representing IP address via four decimal numbers separated by dots is called *dotted decimal notation*.

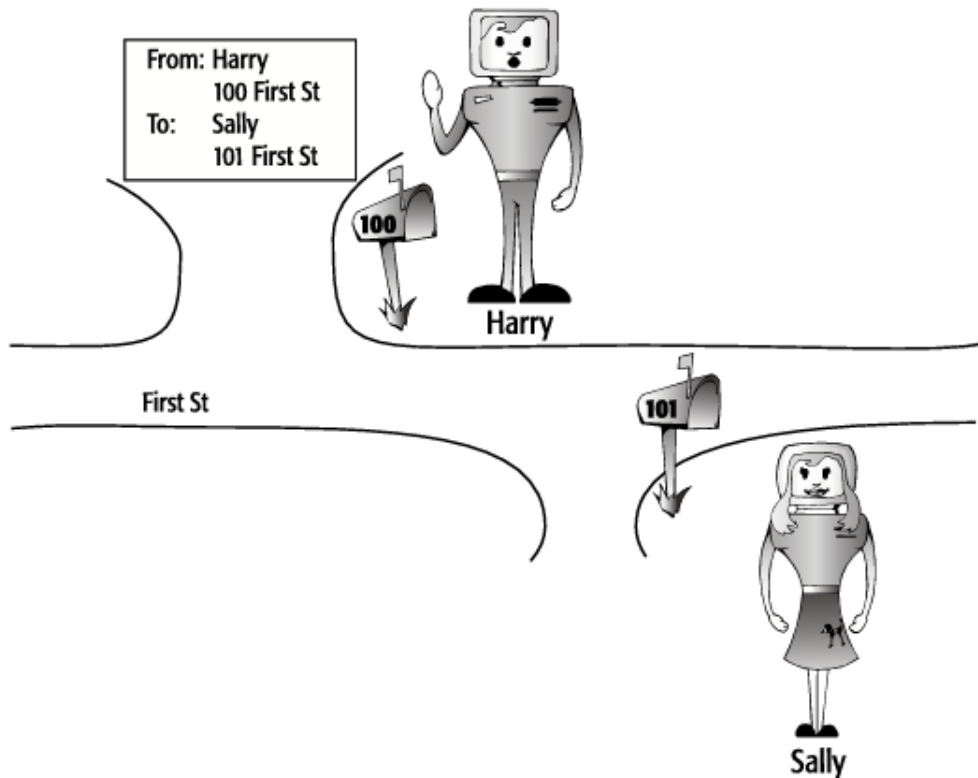


Figure 6.2: Local vs Remote.[5]

### 6.2.3 Subnet Masks [5]

What is a subnet mask? A subnet mask is an important part of an IP address. It states how many bits of the address are used to identify the network part of the address itself by "masking" the IP address's network part.

For every incoming packet IP has to be able to understand whether the intended receiver is on the same local network or on a remote network. If the intended receiver is on the same local network, then IP can deliver the packet directly, otherwise, if the receiver is on a remote network, IP will send the packet to the default gateway (router).

Similarly to how telephone systems use area codes to understand to which area a number belongs, IP uses subnet masks to understand whether the receiver is on a local network or a remote one.

When receiving a packet, IP determines whether that packet is bound for a local network or a remote one by comparing the network part of the sender's IP address, to the same number of bits from the intended receiver's IP address's network part.

If the bits are different then IP decides that the receiver's network is remote.

To know how many bits need to be compared, IP evaluates the subnet mask of the host sending the packet.

In the mask, there are a set of *1s* and a set of *0s*. To evaluate a subnet mask IP has to understand how many bit are set to 1, once IP successfully knows the number of bits set to 1, then it knows the number of bits to compare between sender's and receiver's addresses.

A subnet mask is a mandatory part of every IP address.

A subnet mask can be declared in a number of ways.

- It can be displayed in a way that resembles the IP address itself: if 192.168.2.51 is an IP address and 255.0.0.0 (in bits it would be: 1111 1111. 0000 0000. 0000 0000. 0000 0000) is its subnet mask, then the first byte of the address, starting from the left, will be the one used to identify the address's network. In this example the network would be identified by *192*.
- It can be displayed in a way that highlights the number of bytes (or bits) belonging to the address which is used to identify the address's network. For instance: if the address is displayed as 192.168.2.51/24, then the number of bytes of the address used to identify its network is  $\frac{24}{8} = 3$ , starting from the left. In this example the network is identified by *192.168.2* .

The bigger the subnet mask, the smaller is the number of hosts which can be uniquely identified on the network.

## 6.3 The tested functions.

This study has thus far presented what the role of a router is in a distribution network from the electrical point of view, what are then the functions routers offer that allow DSOs to rely on them for their automation?

- *traffic segregation*: this approach makes use of functions like VLAN (virtual local area network) and VRF (Virtual Routing and Forwarding) to separate services;
- *dynamic and static routing*: these are two kinds of protocols dictating how routers communicate and allowing them to pick a route between two nodes in a network (the node transmitting information and the node receiving it). Static routing requires an administrator to manually set up routing tables - routing tables are the place where each router stores information about where packets need to be forwarded basing on their intended receiver's IP address - for every router in the network. Dynamic Routing automatically updates routing tables [54];
- *IPSec*: IPSec allows VPNs to let IP traffic flow securely;

- *L2TP*: or Layer 2 Tunnelling Protocol [36], allows VPN to securely transmit GOOSE traffic, *GOOSE* is a kind of packet generated in a regime of IEC 61850;
- *Firewalling*: it is a security feature that allows to impose conditions on incoming traffic and reject it in case those conditions are not met;
- *implement AAA protocols*: AAA stands for Authentication, Authorization and Accounting, authentication requires users to present their credentials, authorization requires a user to be formally allowed to operate and accounting allows to monitor the consuming of resources (RADIUS is one of such protocols) [37];
- *SNMP*: or Simple Network Management Protocol, allows to manage the network [49].

The first version of virtual router that has been tested for this thesis work provided those function partially. The functions the virtual router came with are described in sections 6.3.1 through 6.3.6.

### 6.3.1 Manual IP address configuration. [5]

An administrator with a relatively small number of hosts in their network might find effective assigning manually an IP address, and consequently a subnet mask and potentially other optional parameters, to each one of them.

This tactic would inevitably prove less time-effective is the number of hosts grows significantly.

Hosts usually prefer using *DHCP* to assign IP addresses regardless of the number of hosts in their network. Manually assigning an IP address might be an useful tactic in testing scenarios, where an host may wish to be sure of the IP addresses his devices are using.

### 6.3.2 DHCP. [5]

DHCP stands for **Dynamic Host Configuration Protocol**. It is a server/client protocol which allows an IP host to automatically obtain its own IP address together with other information, such as its subnet mask and default gateway address.

There are four steps in getting an IP address from a DHCP server, they are respectively: DHCP discover, DHCP offer, DHCP request and finally DHCP acknowledgment.

#### DHCP discover.

As a new host joins a network, according to the first step of "DHCP", it broadcasts, that is it sends to every other host in the network, a message letting them know that a new host has recently joined the network.

This broadcast is quite useful since it prevents hosts from having to know the address of the host which is currently acting as a server a priori. Figure 6.3 displays Harry, a new host in a network, in need of a DHCP server. To find one Harry broadcasts a discover packet.

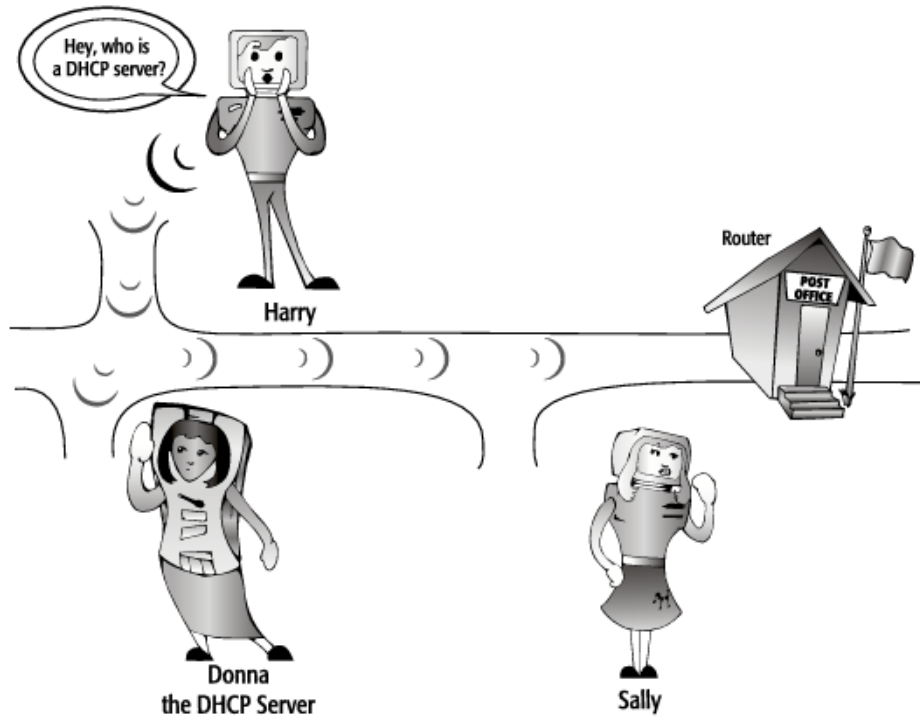


Figure 6.3: DHCP discover packet example. [5]

The information inside a discover packet is usually the MAC address of the new host, the sender IP address is set to  $0.0.0.0$  since the new host has not yet received an IP address, and the receiver address is  $255.255.255.255$  which is the broadcast address, which is to say: the address inserted when a packet is intended for every host in the network.

When a new host joins a network, they do not only send one discover packets, but a volley of them. If the host is not able to receive a valid IP address then an error message will be displayed, and the host will wait for about five minutes before sending another volley of discover packets.

### DHCP offer.

The DHCP server of a network is continuously listening for DHCP discover packets. When it receives one then the server checks for whether it has any available address for the specific network the discover packet is coming from. If an IP address is available then the server will send a DHCP offer by broadcasting it.

At this point of the procedure the server is not aware of which host has sent the discover packet, so it has to broadcast it. In the discover packet though, the host needing an IP address has provided its own MAC address, and this information is carried in the offer packet as well.

An administrator might have configured several hosts as servers in a network. In this case the new host will accept the first DHCP offer it receives after sending his discover packet.

In figure 6.4, Donna the server, after having received the discover packet from Harry (but not yet knowing it was Harry who sent the packet), broadcasts a DHCP offer packet providing a valid IP address and subnet mask and the *duration of the lease for the provided IP address*.

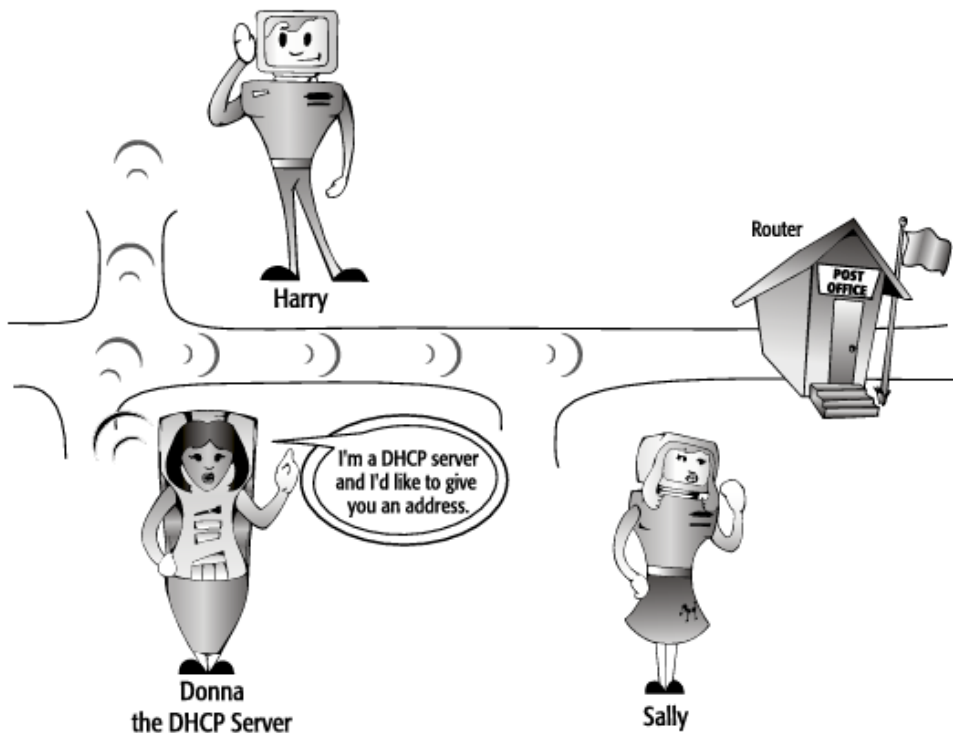


Figure 6.4: DHCP offer packet example. [5]

### DHCP request.

After having receiving a DHCP offer the host joining the network as to accept it. To do so it sends a DHCP request.

This packet is once again broadcast across the network for a few reasons:

- firstly, even though the new host has been offered an IP address, the procedure is not yet concluded and the *lease* not yet initiated, which means that the new host can not yet use its IP address and thus can not participat in IP correctly;
- secondly, the new host might have received offers by several DHCP server. Broadcasting the DHCP request allows servers whose offer has not been accepted to be aware that the IP they had previously allocated for the new host is not being utilized and they can reassign it to another host.

Figure 6.5 shows Harry broadcasting a message where they tell Donna they would accept the IP address they have been offered.

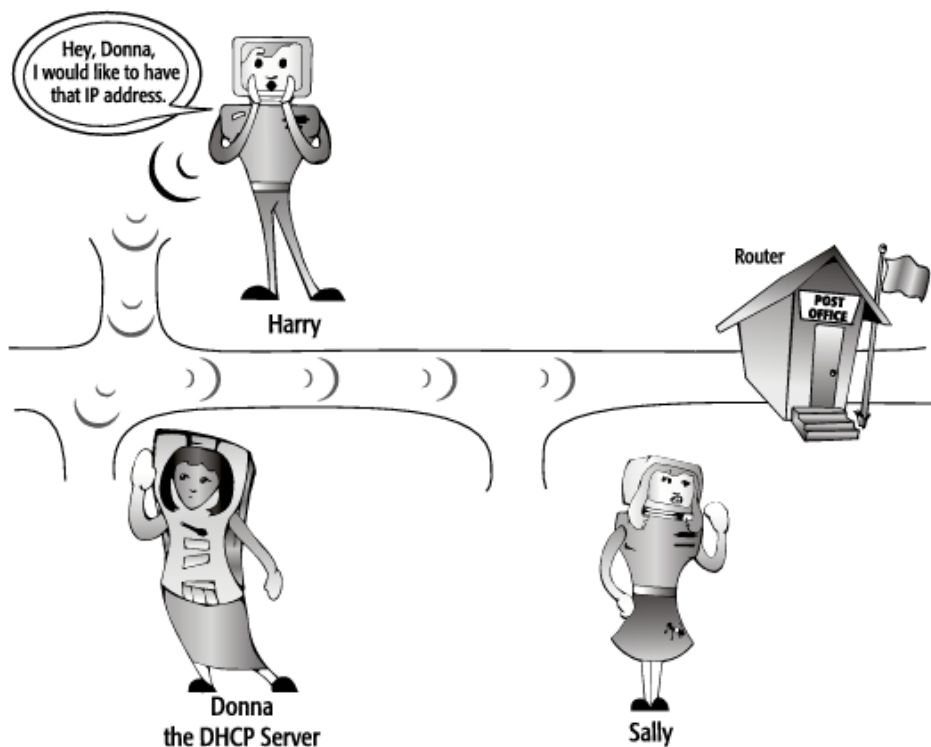


Figure 6.5: DHCP request packet example. [5]



### DHCP acknowledgment.

DHCP acknowledgment is the last step of the DHCP protocol. A new host has joined a network, the host broadcast a message stating that it needs to lease an IP address, a DHCP server has received the message and has offered one, the new host then requests the offered IP address to the server. At this point the server has to accept the request of the new host, and it does that by broadcasting the acknowledgment packet.

The packet is once again broadcast given that the new host does not yet have a valid IP address.

Figure 6.6 shows Donna accepting the request from Harry by broadcasting their response.

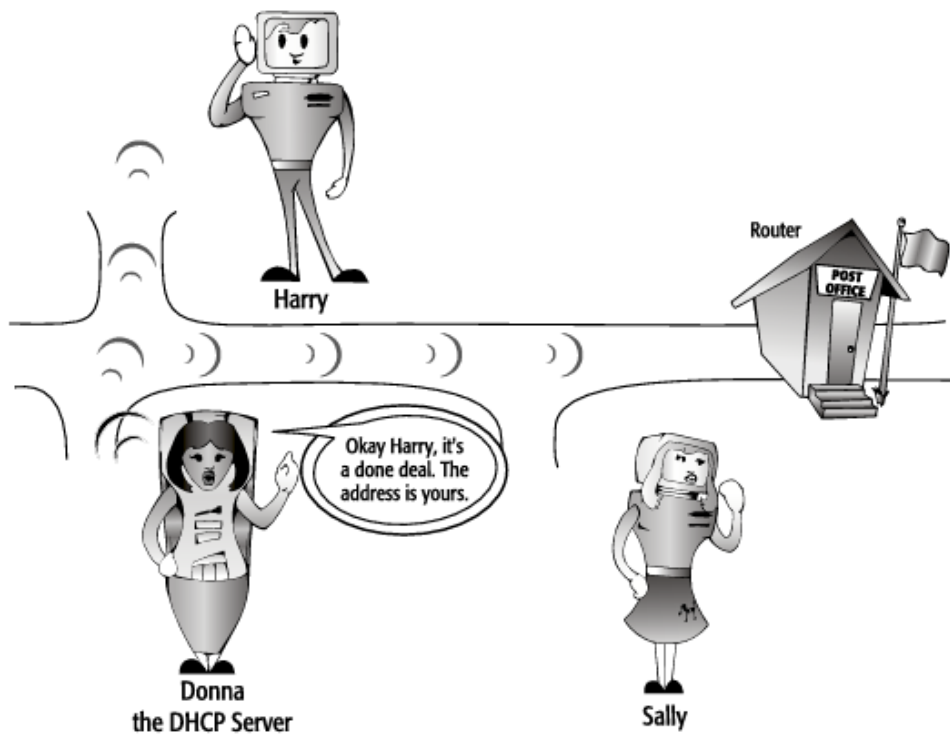


Figure 6.6: DHCP acknowledgment packet example. [5]

### DHCP leases.

The IP addresses offered by DHCP server do not last forever, they are instead rented by new hosts joining a network. Each IP address comes with its own *Time*

*To Live* (TTL). When an IP address's TTL has reached half of its duration, the host contacts the server to request using the address for a longer period.

### 6.3.3 Firewalls. [8]

A firewall is a device used to secure network access, which is generally partly hardware and partly software.

In the past companies might have had at best one firewall protecting the edge of a network, that is because most companies were not connected to the Internet, or might have had just a couple of stations needing to be connected to the Internet, or to be linked with other computers.

After the 1990's the need of connecting to the internet became undeniable.

Initially companies used to connect to the internet using a public IP address. This was not a scalable solution, and even less so a secure one. So they began installing a router connecting their own networks to the internet, a default gateway for their own network, this was already a rudimentary form of firewalling.

The need of better security and of the ability of thwarting always new styles of attacks on networks, brought firewalls to the state they are in today.

#### Packet Filters.

A packet filter is the most basic firewall function. This function filters packets basing on their source IP address, destination IP address, source port and destination port.

It does so on a packet-per-packet basis to determine whether each single packet should be allowed through or not.

What is a **port**?

The best way to convey this concept is through an example. When one uses a television, they can find a different program on every different channel. Ports work much in a similar way. Each port on a device allows to access the content or application which is hidden behind that port.

There are a set of well defined ports which conventionally always give access to the same type of content or application independently of the devices they are on. Figure 6.7 reports a list of the most well known ports and their respective content or application type.

Back to *packet filters*, the most simple packet filters do not offer a good enough level of security in most circumstances.

For instance, if a packet filter is implemented basing on IP source, any packet *incoming* from that source will be denied. If one does not wish to limit traffic *outbound* to that same IP source, the filter would not allow to receive any kind of return packets (sometimes referred to as acknowledgment packets, similar to those introduced in section 6.3.2), consequently compromising any *outbound* traffic.

Well-Known TCP Ports		Well-Known UDP Ports	
FTP	21	DNS	53
SSH	22	DHCP-Relay	67
Telnet	23	TFTP	69
SMTP	25	NTP	123
HTTP	80	IKE	500
IMAP	143	Syslog	514
HTTPS	443	H.323	1719

Figure 6.7: Conventional use of ports. [8]

### Application Proxy.

Another kind of firewall is known as *Application Proxy*. Application Proxy is considered as the most secure kind of firewall. The Application Proxy sits between the protected network (*net A*) and the network one wishes to be protected from (*net B*).

Any time an application in *net B* makes a request, the Application Proxy intercepts it, to then initiate its own request towards *net A*.

When the destination server replies to the proxy, the proxy will in turn reply to the request as if it was the destination server itself.

The whole interaction takes place without any application in *net A* ever making contact with a server in *net B*.

### Stateful Inspection.

*Stateful Inspection* is another firewall implementation quite reminiscing of packet filters, introduced in section 6.3.3.

The two implementation work in a similar way, Stateful Inspection too filters packets basing on: IP source, IP destination, source port, destination port, but, contrary to packet filters, it keeps track of the state of the connection, overcoming the problem introduced in section 6.3.3.

When a return packet is expected, Stateful Inspection will make sure the proper access is ready and open to receive it, to then close it once the return packet has been received.

Being able to allow return packets avoids compromising outbound traffic, but it raises a question regarding those protocols, such as ICMP (which is the protocol used when sending *pings*) or UDP (another quite spread protocol for communications frequently run together with IP), that do not expect any return packets. Generally each manufacturer deals with these kinds of protocols in a different way.

### 6.3.4 NAT. [55]

*NAT* or *Network Address Translation* is a device, in most cases a router, that usually sits in between two networks (*net A* and *net B*). It allows hosts sitting on the same network (*net A*), which is usually a private network, to be addressed by any host sitting in another network (*net B*), quite often from the Internet, by a common public IP address, the one of the NAT device.

The device mechanism performs transformations on IP addresses and ports. For each host sitting in *net A* a specific device's port is allocated by the device itself.

When inbound traffic is received, the NAT device forwards it to the right recipient depending on the port the traffic is received on as showed in figure 6.8.

NAT was developed to mainly cope with the scarcity of unique IP addresses. Giving the possibility to a network to be addressed by a single public IP address, allows the network itself to be identified internally (behind the NAT) by a subnet mask which is already used externally (outside the NAT) [26].

### 6.3.5 IPsec. [50]

IP does not come with any layer of built-in security. IP packets are vulnerable to a plethora of attacks including: re-transmittal of old packets, forging addresses, changing or replacing content, and on top of that they are completely modifiable in transit.

When it comes to IP, there is no assurance that a packet actually comes from the intended sender, nor that the data contained in a packet was the data which actually was transmitted. Even ignoring these two alarm bells, there is still no assurance that the transmitted data remained private.

*IPsec* or *IP Security* is a suite of protocols and was created to make up for these potential vulnerabilities by providing: **authentication, encryption, message authentication** and more generally applying existing security concepts to the communication.

- **Encryption** is the conversion of a plaintext into an intelligible ciphertext, assuring that only the intended parties are able to read messages. This feat is usually achieved by the use of a *key* and an *algorithm*: the plaintext is combined with the key using the algorithm. There are two main categories of encryption: *symmetrical* which requires both party of the encrypted communication to own the same key to both encrypt and decipher messages; *asymmetrical* which makes us of two kinds of keys: a public key (distributed to anyone needing or wanting it) and a private key (confidential). Data can be encrypted using either keys, but the receiving party must know the corresponding key to perform decryption.
- **Message authentication** consists in assuring integrity of a received message. The most common strategy to achieve this is **MAC** or Message Authentication

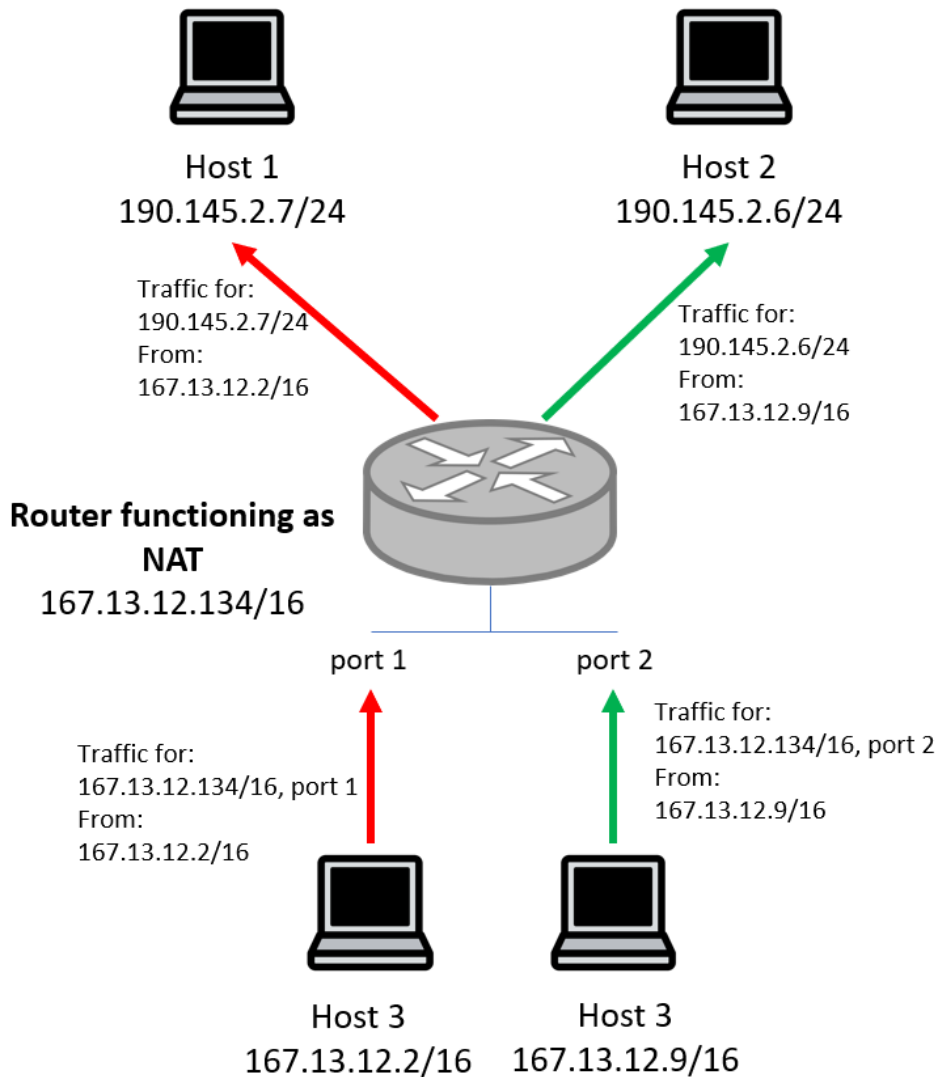


Figure 6.8: Instance of NAT working.

Code. The strategy prescribes sending messages together with a code generated irreversibly by using both the message itself, a key and an algorithm. Once a receiver possessing the right key receives the message, they can verify the integrity using the received message and their key in a verification algorithm. If the received code and the one their verification algorithm provides are the same, integrity is assured.

- **Authentication** allows a system to determine the identity of an entity which is presenting its credentials.

Authentication is based on factors, and more specifically on the exploitation of:

1. something the user knows;
2. something the user has;
3. something the user is.

Combinations of the exploitation of two or more of these factors results in an efficient authentication strategy. IPSec and IPSec VPNs usually adopt a two factor authentication. They could ask an user to provide their username and password (something the user knows, factor 1), together with an OTP (One Time Password) they receive on their phone ( something the user has, factor 2). When talking about factor 3 (something the user is) one generally refers to biometrics (fingerprints, eyes scanners, etc...).

## VPNs.

For most VPN (Virtual Private Network) is defined as an extension of an enterprise's network across a public network, usually the Internet. What differentiate VPNs is the level of security associated with them. IPSec VPNs, or VPNs built using the suite of protocols IPSec, are VPNs providing with: authentication, confidentiality (encryption) and private communications (message authentication and encryption) over a public and not trusted medium.

### 6.3.6 SSH and HTTPS.

#### SSH.

"Secure Shell (SSH) is a program used to secure communication between two entities. SSH uses a client/server architecture, where SSH clients, available on all versions of Windows, different flavors of Unix, and various Macintosh operating systems, connect to SSH servers, which can be operating systems such as Sun Solaris or Microsoft Windows or devices such as a Cisco router. **In its simplest sense, SSH is used to execute remote commands securely on another entity**, often used as a replacement for Telnet and the Berkeley "R" protocols such as remote shell (RSH) and remote login (Rlogin)"

"In addition to executing remote commands, SSH is used as a secure remote copy utility, replacing traditional protocols such as the File Transfer Protocol (FTP) and Remote Copy Protocol (RCP).

Despite the name Secure Shell , SSH is not a shell at all. Unlike other traditional shells found in different flavors of Unix, such as BASH, KORN, and C, SSH provides encryption between entities, not a shell interface between entities. The encryption methods and algorithms used for SSH are all based on industry standards such as 3DES, Blowfish, Twofish, and AES. " [12]

SSH has been used in many fields, it has been tested to set up robots as well [38].

## HTTPS.

### HTTP.

The Hypertext Transfer Protocol (HTTP) is a family of stateless, application-level, request/response protocols that share a generic interface, extensible semantics, and self-descriptive messages to enable flexible interaction with network-based hypertext information systems.

HTTP hides the details of how a service is implemented by presenting a uniform interface to clients that is independent of the types of resources provided. Likewise, servers do not need to be aware of each client's purpose: a request can be considered in isolation rather than being associated with a specific type of client or a predetermined sequence of application steps. This allows general-purpose implementations to be used effectively in many different contexts, reduces interaction complexity, and enables independent evolution over time. [32]

### What is HTTPS?

HTTPS is a later development of HTTP that uses for transport layer security a protocol called **TLS**, or *Transport Layer Security*.

### TLS. [4]

TLS, or Transport Layer Security is a suit of protocol widely used in the World Wide Web and built on top of a secure and reliable transport layer protocol such as TCP, built to ensure security through the means of cryptography.

The suit of protocols of TLS rely on: a TLS connection, a transport layer transient client-server connection always associated to a session: a TLS session, which is a client-server association taking place through TLS's handshake protocol; each session defines a set of cryptographic parameters that can then be used across several connections. Both connection and session keep a set of parameters helping them recollecting their state.

The suite of protocols involved in TLS are shown in figure 6.9. Among them:

- the *Handshake Protocol* is used to establish a session, during the handshake client and server exchange several information, including security information;

- the *Alert Protocol* is used between client and server to exchange alert messages, they are two bytes encrypted messages;
- the *Record Protocol* encapsulates all other protocols data and adds its own header before sending the packet to the next layer.

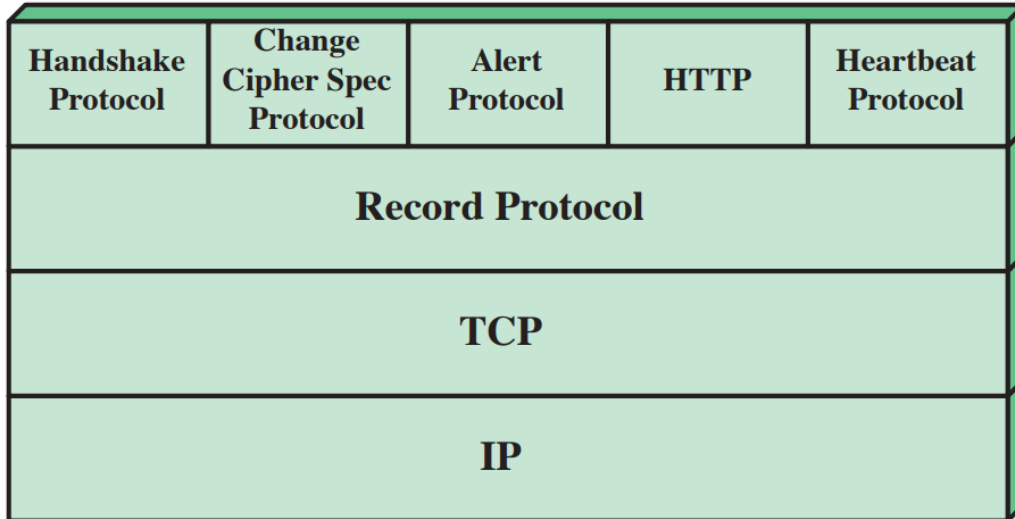


Figure 6.9: Protocols involved in TLS. [4]





# Chapter 7

## Testing objectives.

The objective of the experimental part of this thesis work was **verifying the functions of the virtual router presented to Gridspertise matched the requirements of the smart grid scenario and more specifically of DSOs study cases.**

Mainly, the functions a router needs to provide to match DSOs study cases requirements are:

- *traffic segregation*: this approach makes use of functions like VLAN (virtual local area network) and VRF (Virtual Routing and Forwarding) to separate services;
- *dynamic and static routing*: these are two kinds of protocols dictating how routers communicate and allowing them to pick a route between two nodes in a network (the node transmitting information and the node receiving it). Static routing requires an administrator to manually set up routing tables - routing tables are the place where each router stores information about where packets need to be forwarded basing on their intended receiver's IP address - for every router in the network. Dynamic Routing automatically discover remote networks, maintain up-to-date information, chooses the best path to the destination, finds new best paths when there is a topology change and dynamic routing can also share static routes with the other routers. [54];
- *IPSec*: IPSec allows VPNs to let IP traffic flow securely;
- *L2TP*: or Layer 2 Tunnelling Protocol [36], allows VPN to securely transmit GOOSE traffic, *GOOSE* is a kind of packet generated in a regime of IEC 61850;
- *Firewalling*: it is a security feature that allows to impose conditions on incoming traffic and reject it in case those conditions are not met;

- *implement AAA protocols*: AAA stands for Authentication, Authorization and Accounting, authentication requires users to present their credentials, authorization requires a user to be formally allowed to operate and accounting allows to monitor the consuming of resources (RADIUS is one of such protocols) [37];
- *SNMP*: or Simple Network Management Protocol, allows to manage the network [49].

The first version of virtual router this thesis work has tested does not provide all of the functions above listed. The functions provided are those presented in chapter 6 and they are:

- DHCP server, function introduced in section 6.3.2
- SSH and HTTPS applications, function introduced in section 6.3.6;
- Firewalling, function introduced in section 6.3.3;
- NAT, function introduced in section 6.3.4;
- IPsec VPN, function introduced in section 6.3.5;
- Static Routing, presented in section 6.2.1.

Basing on the list of provided functions this study highlights that the tested virtual router matches only partially the requirements of DSOs study cases, no dynamic routing was provided by the virtual router, nor L2TP or Traffic Segregation.

Moreover, the functions the virtual router was provided with were tested according to the methodologies reported in chapter 8, and their results reported in chapter 9.

## 7.1 The laboratory scenario.

Gridspertise intended to test the functions not to build up a comparative model, but to confidently state the functions provided were ready to use in case of deployment of the solution.

Gridspertise laboratory was provided with: one edge device, with the virtual router already installed, two laptops, one running *Windows* and the other *Linux*, an external physical router and all the cables needed to connect the devices during testing.

As shown in figure 7.1, the edge device was set to be connected on one side directly to a laptop via Ethernet (LAN interface), creating network 10.0.0.x/24, on the other the device was connected to a router to simulate a WAN (Wide Area Network), this allows the virtual router to actually receive or transmit traffic from/to a

network which is not directly connected to it, as it would in a WAN, in the lab set-up the external router would be routing traffic flows between two distinct networks: *Network 2*, which is the network the WAN interface of the virtual router belongs to, whose subnet mask is  $192.168.24.x/30$ , an *Network 3* whose subnet mask is  $192.168.4.x/24$ .

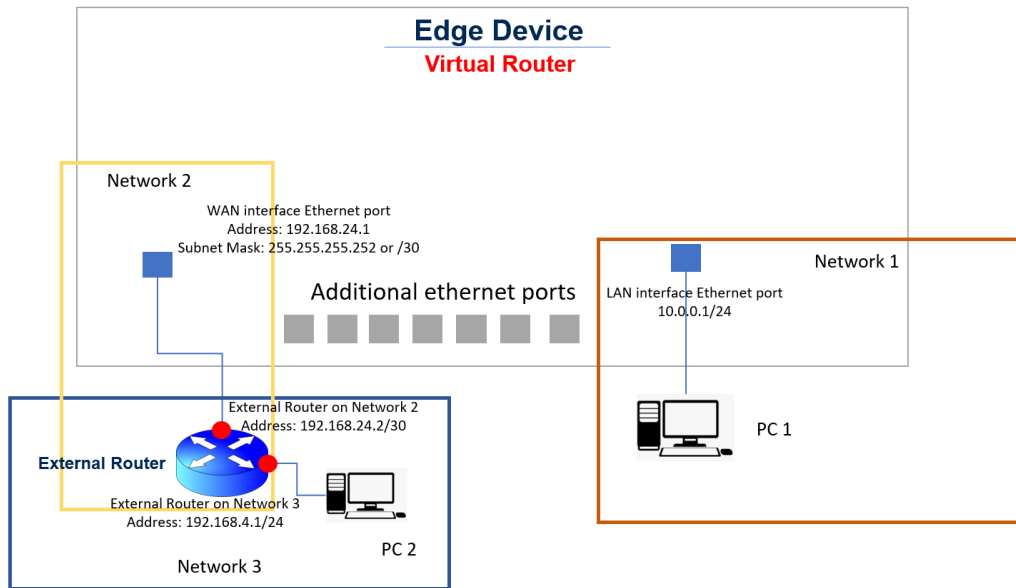


Figure 7.1: Lab set-up.

More specifically, the router was set as follows:

- One of its Ethernet interfaces (interface A) was assigned the IP address 192.168.24.2 with subnet mask 255.255.255.252;
- one of its Ethernet interfaces (interface B) was assigned the IP address 192.68.4.1 with subnet mask 255.255.255.0;
- the default gateway for inbound traffic on interface B was 192.168.24.1 with subnet mask 255.255.255.252, which is to say traffic incoming from interface B was automatically directed to the WAN interface of the virtual router by the external router.



# Chapter 8

## Methodologies.

The purpose of this thesis work is to make sure that the functions the provided virtual router came with actually worked as expected.

This section will provide insights about how each test was conducted. Moreover it will allow the reader to become better acquainted with the interface of the product to then better understand the setting passages of each test.

The virtual router solution, as previously stated, is not developed in house by Gridspertise but it is sourced externally. The manufacturer, or better, the developer of the solution, provided with it an user guide where several testing scenarios were depicted, each thought out specifically for testing one function.

The tested functions were:

- DHCP server, function introduced in section [6.3.2](#)
- SSH and HTTPS applications, function introduced in section [6.3.6](#);
- Firewalling, function introduced in section [6.3.3](#);
- NAT, function introduced in section [6.3.4](#);
- IPsec VPN, function introduced in section [6.3.5](#);
- Static Routing, presented in section [6.2.1](#).

### 8.1 User Interface of the virtual router.

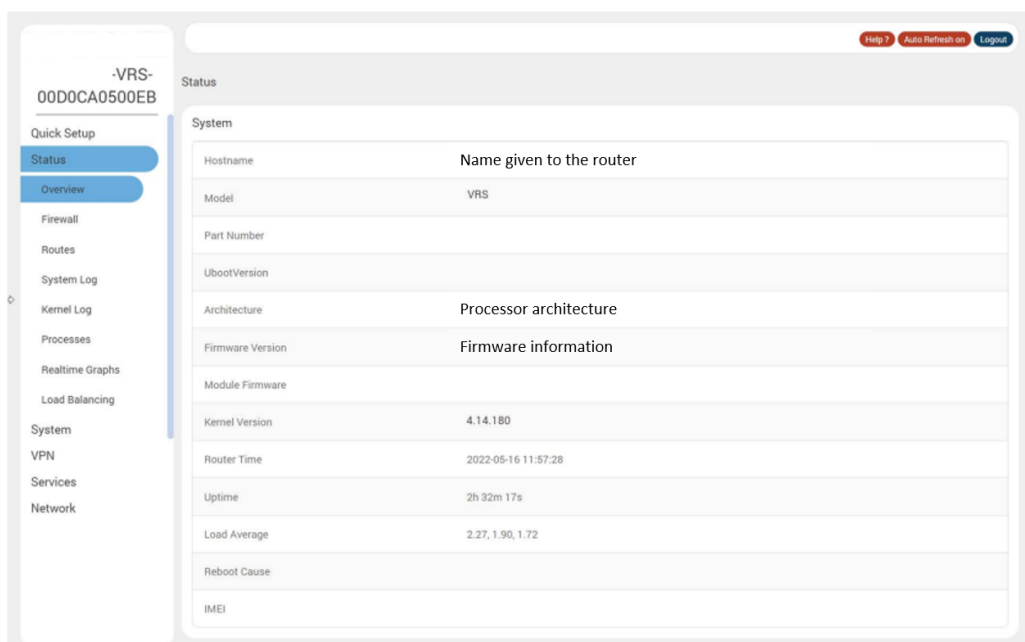
The virtual router has its own user interface. This is an element of paramount importance for the conducted testing: even though the router can be set via SSH (see section [6.3.6](#) for more detail about what SSH is), the most user friendly way of setting it is through its user interface, on top of that, this would realistically be the means through which a network operator would set it.

### 8.1.1 Status page.

The status page, is the page welcoming the user once they log in. The developer reports in the page the vital configurations of the virtual router, and they give the opportunity to the user to select the page the are interested in.

### 8.1.2 Status Overview Page.

The status overview page provides a listing of important system and network parameters.



System	
Hostname	Name given to the router
Model	VRS
Part Number	
UbootVersion	
Architecture	Processor architecture
Firmware Version	Firmware information
Module Firmware	
Kernel Version	4.14.180
Router Time	2022-05-16 11:57:28
Uptime	2h 32m 17s
Load Average	2.27, 1.90, 1.72
Reboot Cause	
IMEI	

Figure 8.1: Status page of the router.

#### System Status.

The system section provides the model and software related information, as reported in table 8.1.

#### Memory Status.

The memory section provides information about the available memory in KB, the details are reported in table 8.2.

Parameters	Description
Hostname	Name assigned to the edge device for addressing purposes
Model	Model number
Architecture	Processor architecture type
Firmware Version	Base firmware version number
Router Time	Internal router time
Reboot Cause	Displays the last reboot cause and time whenever possible

Table 8.1: System Status details

Parameters	Description
Total Available	Total available RAM memory
Free	Free RAM memory
Buffered	Size of buffer's memory that is occupied

Table 8.2: Memory Status details

### Active DHCP leases.

The active DHCP Leases shows information about the devices that have been leased an IP address by the DHCP server. The information of this status section is reported in table 8.3.

## 8.2 Web Administrator Interface of the virtual router.

The web administrator interface allows the administrator and other authorized users to configure and manage the VRS (Virtual Routing Solution) using most web browsers (Firefox, Internet Explorer or Safari web applications with the latest browser updates).

The page displays a menu on the left side (#1 in figure 8.2), an active content area (#2 in figure 8.2), a section redirecting to helpful information (#4 in figure 8.2) and allows to save the desired configuration (#3 in figure 8.2).

### 8.3 Test Case: DHCP server.

VRS can act as the DHCP server and assign IP addresses to devices connecting to the LAN network. The DHCP server maintains a database of available IP addresses and configuration information. When it receives a request from a client, the DHCP server determines the network to which the DHCP client is connected, allocates an



Parameters	Description
Host Name	Name of the device that has been leased an IP address by the DHCP server.
IP Address	IP address assigned by the DHCP server
MAC Address	MAC address of the devices to which an IP address has been given by the server.
Leasetime remaining	The remaining time for which each device can use the DHCP server leased IP address.

Table 8.3: DHCP Leases detailed information.

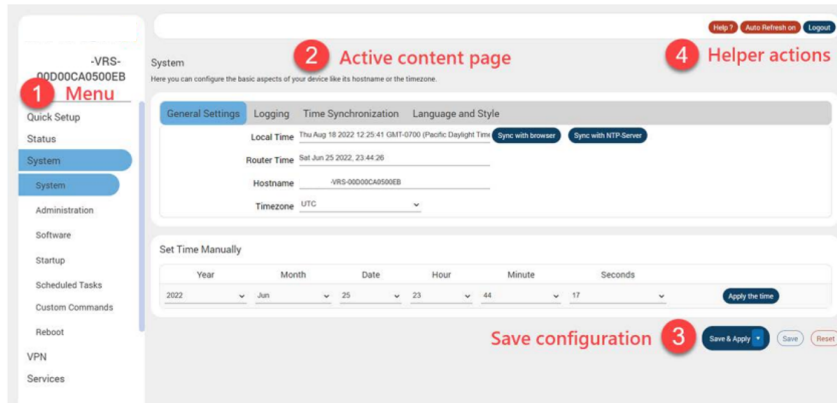


Figure 8.2: Web Administrator Interface of the virtual router.

IP address or prefix appropriate for the client, and sends configuration information appropriate for that client.

DHCP servers typically grant IP addresses to clients for a limited interval called a lease. DHCP clients are responsible for renewing their IP address before that interval has expired, and must stop using the address once the interval has expired, if they have not been able to renew it [47].

### 8.3.1 Test Case Pre-requisite.

DHCP server on the LAN interface should not be disabled. To make sure it is not disabled one must verify under the the section *Network -> Internfaces -> Lan -> DHCP Server -> General Setup page* that the *Ignore Interface box* is not checked and note the pool of IP addresses to be allocated matches the number of IP addresses that one wishes to allocate.

In the example of figure 8.4 the box is unchecked, the pool of IP addresses is set to accommodate 50 hosts and the leased IP addresses last for 12 hours.

The schematized lab set-up is reported in figure 8.3, with a laptop connected on the LAN interface Ethernet port.

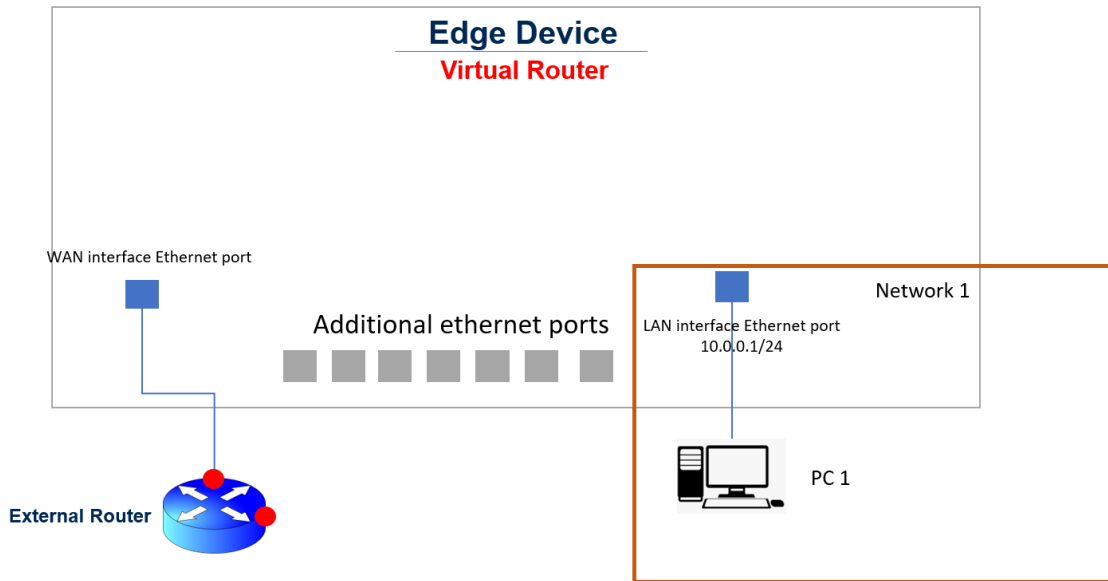


Figure 8.3: Lab scheme for DHCP testing.

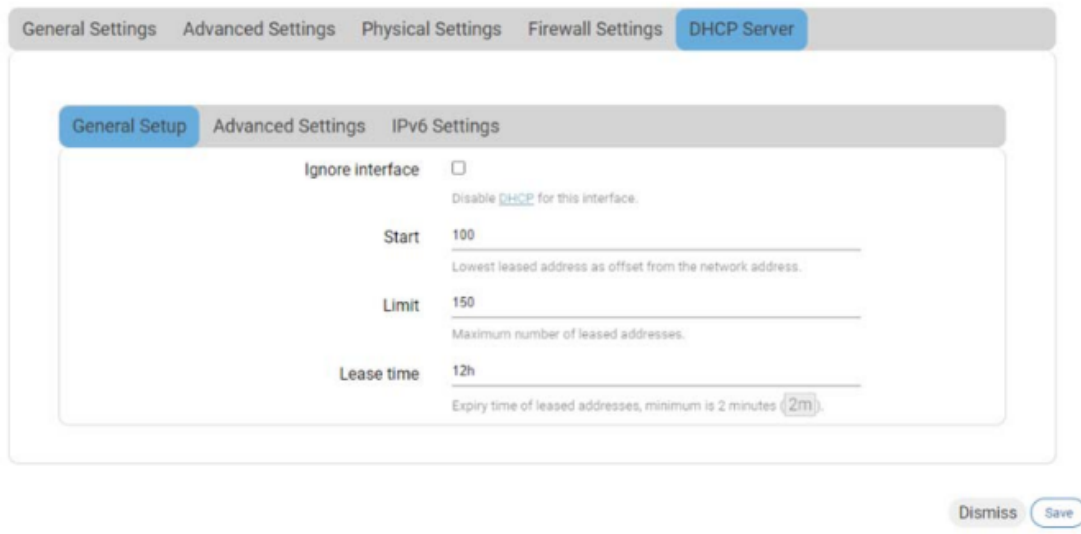


Figure 8.4: DHCP setting for LAN interface.

### 8.3.2 Test Case Objectives.

Verify that the virtual router allocates IP addresses to connected LAN hosts.

### 8.3.3 Test Case Procedure.

1. Set a PC to be a DHCP client, i.e. set it to be able to automatically receive an IP address;
2. Connect PC to Ethernet LAN of the edge device;
3. verify that the PC is assigned an IP address.

## 8.4 Test Case: SSH and HTTPS Applications over LAN and WAN Interfaces.

HTTPS and SSH can be used to securely access and configure the VRS. Figure 8.5b displays the laboratory scheme to test HTTPS and SSH via LAN, figure 8.5a shows the laboratory scheme of the set-up for testing HTTPS and SSH via WAN.

### 8.4.1 Test Case Pre-requisite.

SSH and HTTPS access must be granted via WAN and LAN. Putty needs to be installed on the device accessing the virtual router. Putty is a software that allows to communicate using SSH protocol, when an IP address and a port are provided as the target to access.

### 8.4.2 Test Case Objective.

Verify that the device can be accessed via SSH and HTTPS.

### 8.4.3 Test Case Procedure.

1. Try to SSH to the virtual router via LAN (IP address reported in figure 8.5b) on port 8022 via Putty;
2. once the connection is established enter the virtual router provided username and password;
3. verify that SSH login is successful;
4. repeat steps 1 through 3 after connecting the laptop via WAN interface (IP address reported in figure 8.5a), on port 8022;
5. open a browser and try connecting to the IP address of the LAN interface;
6. verify connection is successful;
7. repeat steps 5 and 6 after connecting via the WAN interface.

## 8.5 Test Case IPsec VPN.

A Virtual Private Network (VPN) tunnel carries traffic of a private network from one endpoint system to another over a public network such as the Internet. The traffic of a private network so carried over a public network does not know about the existence of the intermediate hops between the two endpoints. Similarly, the intermediate hops are also not aware that they are carrying the network packets that are traversing the tunnel. The tunnel may optionally compress and/or encrypt the data, providing enhanced performance and some measure of security.

The IP Security (IPsec) suite of protocols are designed for cryptographically secure communication at the IP layer. The identity of communicating users is checked with the user authentication based on pre-shared keys (PSK) or X.509 certificates.

Figure 8.6 shows the lab set-up needed for the testing of the IPsec VPN function of the router. Notice that the peer used for testing, and displayed in the picture, was provided by the manufacturer of the virtual router, located in another country.

### 8.5.1 Test Case Pre-Requisite.

VPN peers need to be able to adopt the IKE protocols (Internet Key Exchange) used to securely exchange keys across the Internet. All IPsec parameters (pre-shared key and authentication methods) should match between the peers taking part in the VPN [57].

### 8.5.2 Test Case Objective.

Verify IPsec tunnel can be successfully established between the virtual router and the VPN peer device.

### 8.5.3 Test Case Procedure.

1. configure both peer so that the parameters reported in table 8.4 and table 8.5 match between peers. The two tables report the setting of the parameters from the point of view of the virtual router, the setting of the VPN endpoint provided by the manufacturer would be specular;
2. report the desired configuration on the virtual router UI, as shown in figure 8.7;
3. connect the virtual router in the VPN by clicking on the "connect" button, as shown in figure 8.8;
4. verify the connection has been successfully established by pinging the peer.

Parameters	Description
Remote IPsec Router	202.53.10.133/24
Remote Address	172.16.16.16.0/24
Remote ID	202.53.10.133/24
Local Network	10.0.0.0/24
IPSec Authentication Mode	Pre-shared key
IPSec Pre-Shared Key	Key shared between the peers
IPSec Encryption algorithm	AES-256
IPSec Hashing algorithm (MAC)	SHA2-256
IPSec Key Sharing algorithm	DH Group15(3072)

Table 8.4: IPSec parameters.

Parameters	Description
IKE Authentication Mode	Pre-Shared Key
IKE Pre-Shared Key	Key shared between peers for IKE protocol
IKE Mode and Version	MAIN (IKEv2)
IKE Encryption algorithm	AES 256
IKE Hashing algorithm (MAC)	SHA2-256
IKE Key Sharing algorithm	DH Group15(3072)

Table 8.5: IKE parameters.

## 8.6 Test Case Firewall.

The firewall policy helps secure the network and is the mechanism by which network traffic is filtered coming through the router. Traffic can be discarded (dropped) without any further action, rejected with an appropriate response to the source, or accepted and routed to the destination.

VRS follows a zone-based firewall concept. Every interface, whether physical or virtual, needs to be assigned to a firewall zone, and all traffic routed through that interface is bound by the assigned policy. At a minimum, there are two firewall zones, the LAN zone and WAN zone, with one or more interfaces assigned to each zone.

Figure 8.9 shows the laboratory scheme used to test the firewall function of the virtual router.

### 8.6.1 Test Case Pre-Requisite.

No pre-requisite is required in order to conduct the firewall test.

### 8.6.2 Test Case Objective.

Verify that the firewall can be used to either allow or deny traffic through the WAN interface of the edge device.

### 8.6.3 Test Case Procedure.

1. connect to the edge device through the WAN interface (figure 8.9);
2. verify that the firewall is **off**, which is to say the "firewall rule", as the manufacturer calls it, is **on**, as shown in figure 8.10a;
3. open a browser and try to connect to the WAN interface's IP address (figure 8.9);
4. verify that a connection is successfully established;
5. turn the firewall **on**, which is to say make sure the firewall rule is **off**, as shown in figure 8.10b;
6. open a web browser and try to connect to the WAN interface's IP address (figure 8.9);
7. verify connection is unsuccessful.

## 8.7 Test Case NAT.

The laboratory set-up for testing the NAT function is displayed in figure 8.11.

### 8.7.1 Test Case Pre-Requisite

For this test a laptop in listening mode will have to be connected on the LAN interface of the edge device. To allow a laptop running linux to start listening for TCP or UDP connection, one can use the *NetCat* command, from the command line, in mode *-l*, and specifying the port the device should be listening on, as shown in figure 8.12, *nc -l 2001* that is to say: listen on port 2001 for TCP or UDP dataframes.

Moreover, a device able to establish a *Telnet* connection is needed. Telnet is a communication protocol which is not encrypted, this will allow the listening laptop to verify the received messages.

### 8.7.2 Test Case Objective.

Verify traffic transfers from WAN to LAN network.

### 8.7.3 Test Case Procedure.

1. create a *"traffic rule"* to accept traffic on a specific port of the WAN interface of the edge device as displayed in figure 8.13;
2. create a *"port forwarding rule"* to forward the desired traffic to a specific port of a device whose IP address is targeted, as shown in figure 8.14.
3. connect a laptop on the WAN interface and another on the LAN interface of the edge device;
4. from PC2 (figure 8.11), open a *Telnet* connection towards PC1, on Linux this can be done using the command `telnet 10.0.0.209 2001`, 10.0.0.209 is the IP address of PC1 and 2001 is the port PC1 is listening on;
5. verify that PC1 is able to receive the Telnet messages.

## 8.8 Test Case Static Routing.

Static routing is the most basic function of a router, given a set of statically defined IP address, and given the virtual router has access to all of them, will they be successfully reached?

The laboratory setting is the same used for the NAT test, reported in figure 8.11.

### 8.8.1 Test Case Pre-Requisite.

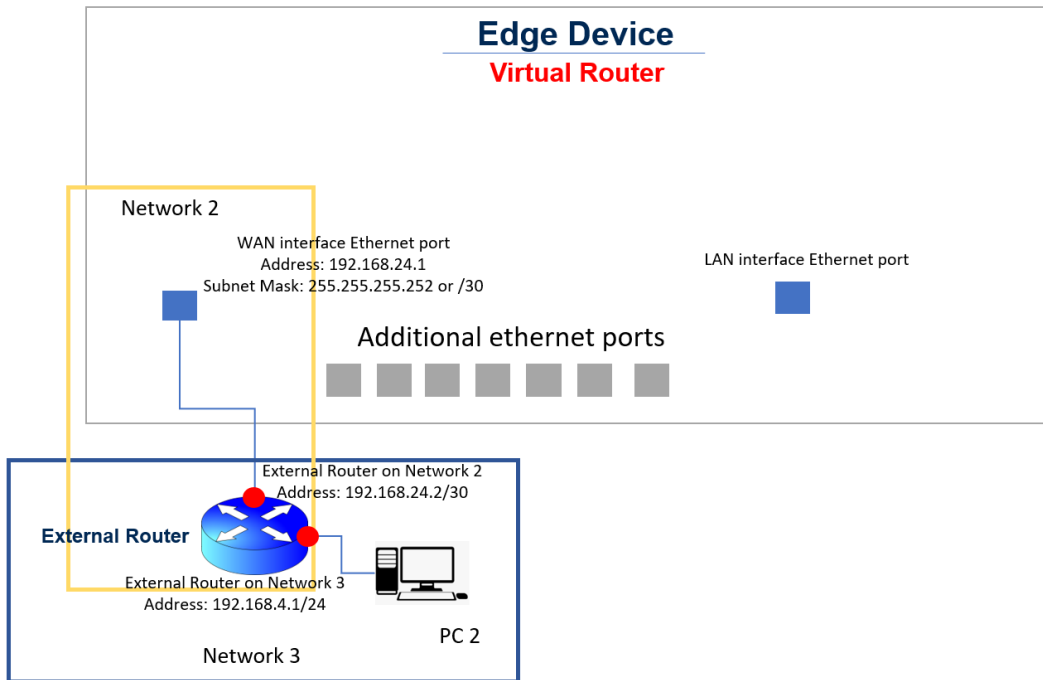
All the elements one wishes to reach in the network need to have been given an IP address manually by the administrator of the network.

### 8.8.2 Test Case Objective.

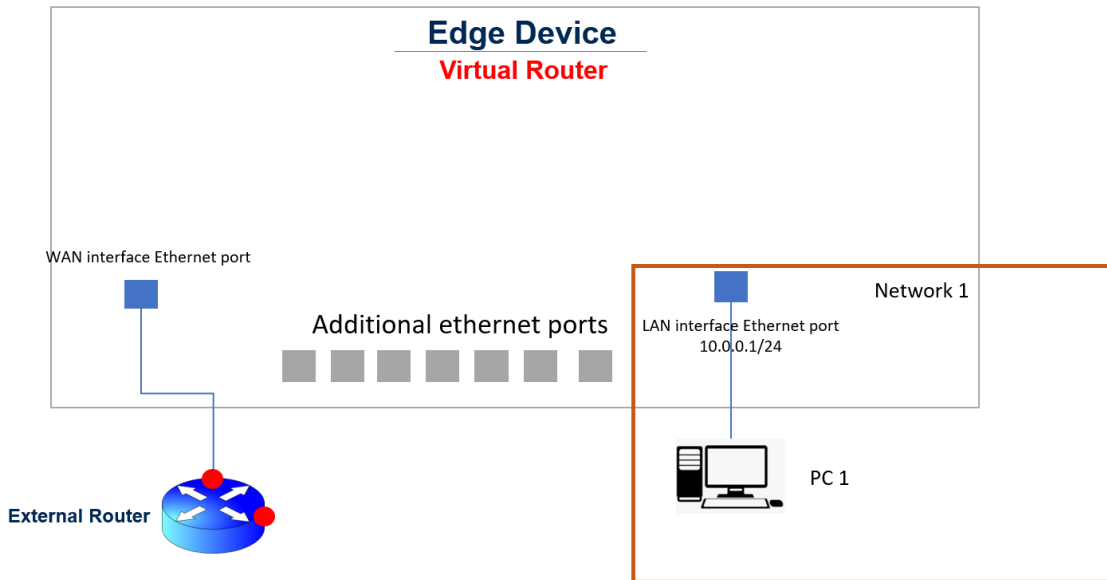
Verify the elements in the network are reachable through the virtual router.

### 8.8.3 Test Case Procedure.

1. Define an ARP table including all elements in the network through the virtual router UI (figure 8.15). An ARP table is a table kept by a router, where all IP address the router can reach are associated with their respective MAC (Media Access Control) address [29];
2. verify the hosts in the network can be reached via pinging.



(a) Lab set-up for SSH and HTTPS testing through WAN interface.



(b) Lab set-up for SSH and HTTPS testing through LAN interface.

Figure 8.5: Lab set-ups for testing SSH and HTTPS.



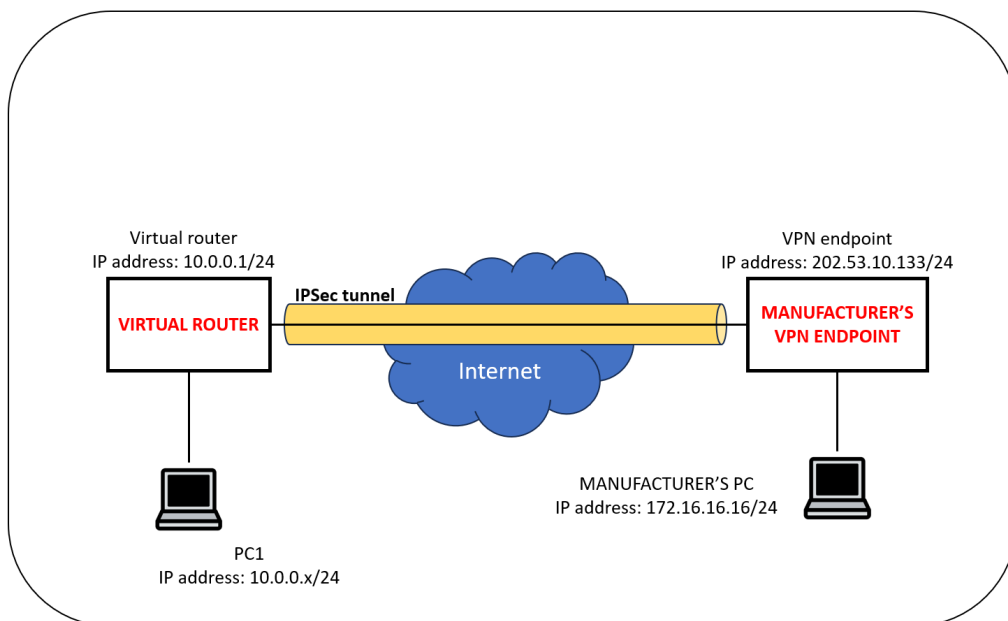
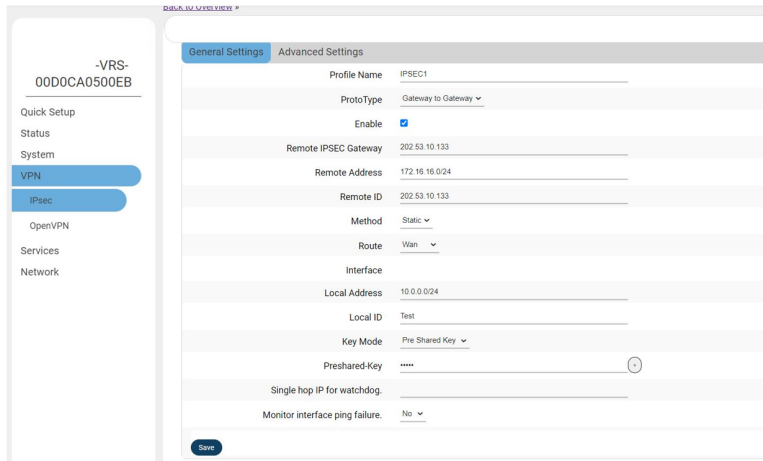
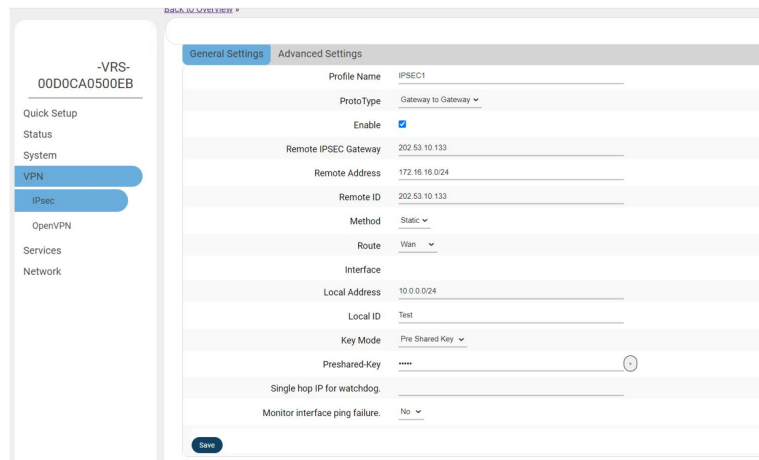


Figure 8.6: Lab scheme IPSec VPN testing.



(a) IPsec configuration on the virtual router UI.



(b) IKE configuration on the virtual router UI.

Figure 8.7: IPsec VPN configuration on the virtual router UI.

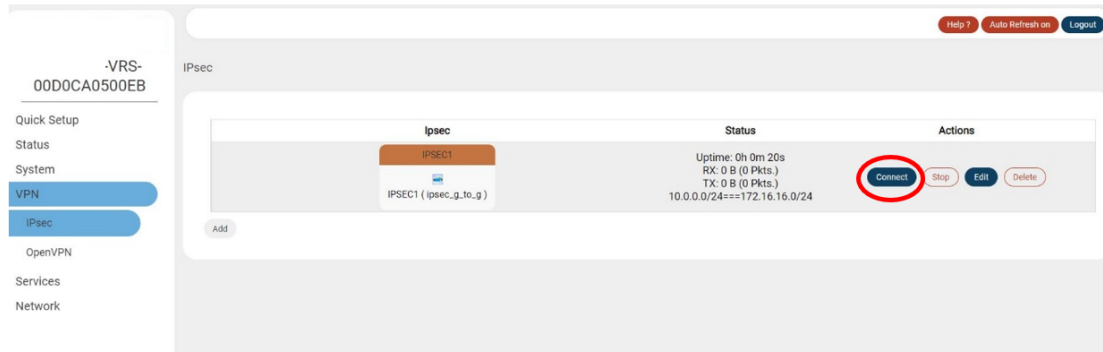


Figure 8.8: Launch of the IPsec VPN.

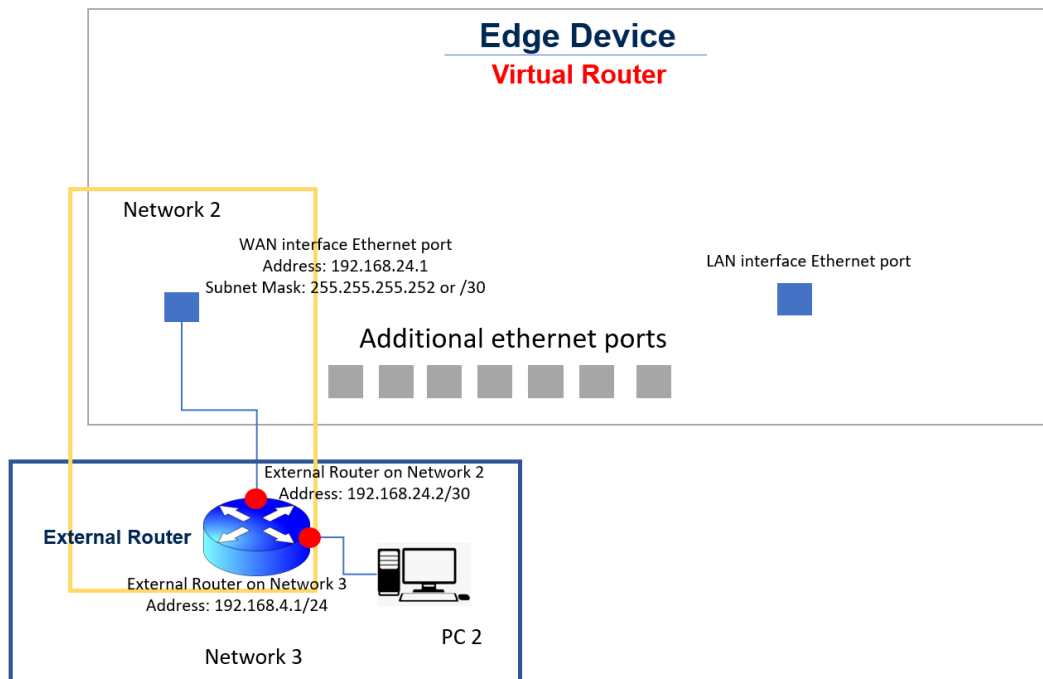
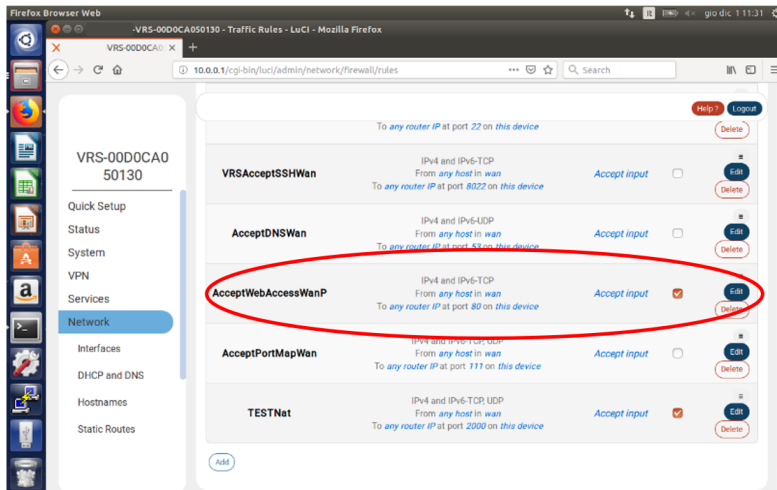
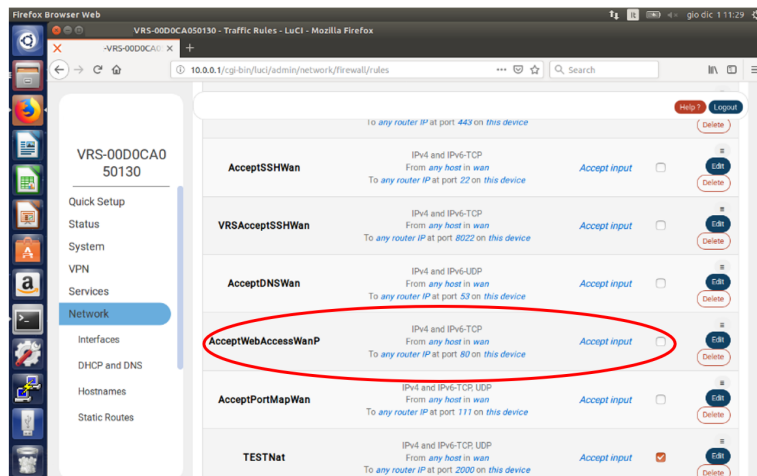


Figure 8.9: Lab scheme for testing Firewall.

## 8.8 – Test Case Static Routing.



(a) Firewall off, traffic can flow.



(b) Firewall on, traffic is stopped.

Figure 8.10: Firewall settings through virtual router UI.

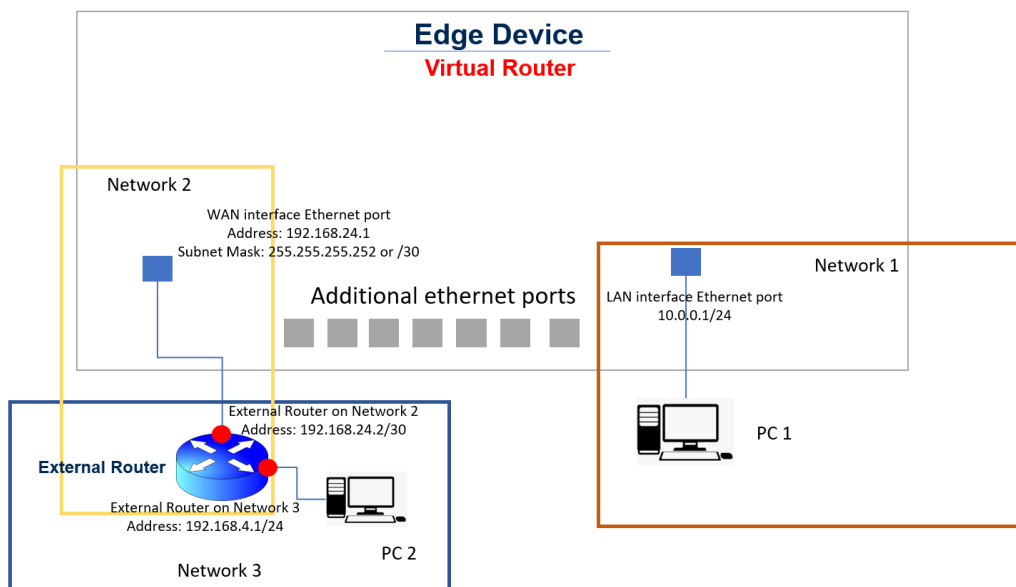


Figure 8.11: Lab set-up for NAT testing.

```
gennaro@gennaro-HP-Compaq-6530b-GW688AV:~$ nc -l 2001
```

Figure 8.12: Command for configuring a Linux laptop in listening mode.

**testnatwan** IPv4 and IPv6-TCP, UDP

From *any host in wan* Accept input

To *any router IP at port 2001 on this device* 
Edit Delete

Figure 8.13: Rule enabled to allow traffic on port 2001 from WAN interface of the edge device.

Port Forwards

Name	Match	Forward to	Enable
<b>Unnamed forward</b>	IPv4 and IPv6-TCP, UDP From <i>any host in wan</i> Via <i>any router IP at port 2001</i>	IP <i>10.0.0.209</i> , port <i>2001</i> in <i>lan</i>	<input checked="" type="checkbox"/> <span>Edit</span> <span>Delete</span>

Figure 8.14: Rule enabled to forward traffic inbound from port 2001 of the WAN interface, to port 2001 of the device connected onto the LAN interface of the edge device whose IP address is 10.0.0.209/24.

ARP

IPv4-Address	MAC-Address	Interface
10.0.0.209%eth1	D8:D3:85:0C:B6:61	lan
10.0.0.126%enp1s0	08:26:AE:30:A4:E2	lan
169.254.204.18%enp1s0	C8:F7:50:16:CA:8E	lan
169.254.169.99%enp1s0	88:A4:C2:46:C2:4C	lan
10.0.0.110%lo	88:A4:C2:46:C2:4C	lan
192.168.24.2	70:B3:17:F7:A7:80	wan
10.0.0.241	C8:F7:50:16:CA:8E	lan

Figure 8.15: ARP table.



# Chapter 9

## Results

This chapter deals with the results of the tests listed in chapter 8 and conducted according to the procedures that were too depicted in chapter 8.

### 9.1 DHCP server.

The function of DHCP server is quite significant for a device that is meant to be deployed in secondary substations: it enable operators to automatically receive an IP address when connecting to the edge device, allowing even operators with less experience in the field of telecommunications to execute tasks involving the edge device.

The test was conducted according to the procedure described in section 8.3.

The test was successful, as expected when connecting a device capable of automatically receiving an IP address, the device successfully receives an IP address from the virtual router when it is set to operate as DHCP server.

Figure 9.1 shows a device capable of automatically being given an IP address actually receiving one when connected to the edge device.

### 9.2 SSH and HTTPS Applications over LAN and WAN Interfaces.

Being able to access the virtual router through HTTPS or SSH is of paramount importance for operators. Any kind of setting of the virtual router has to be configured either via its user interface (HTTPS) or via command line (SSH). Setting the router to work as DHCP server, assigning to it a static IP address, setting it to be able to take part into a VPN, accessing it to verify its correct functioning, all of this can only be achieved by either connecting to the router via HTTPS or SSH.

The test was conducted according to the procedure described in section 8.4.



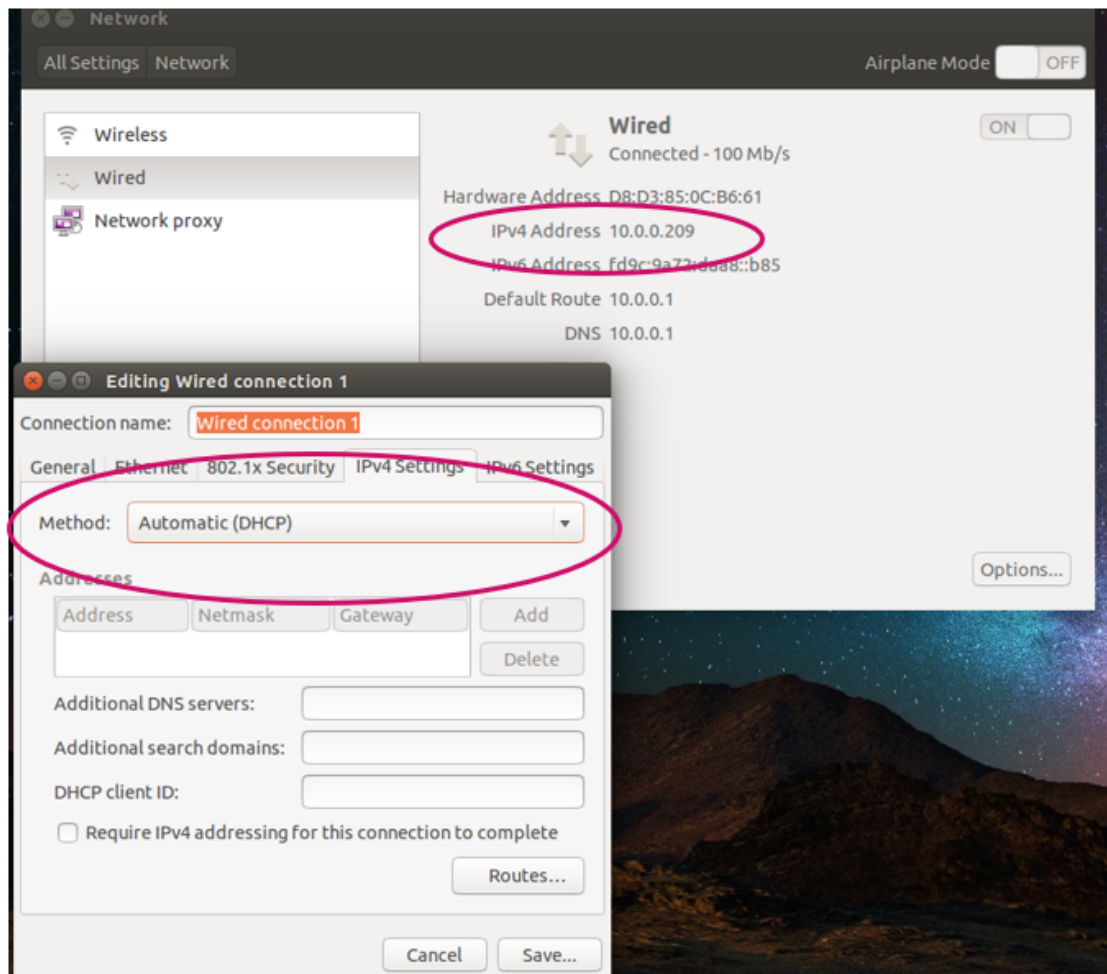


Figure 9.1: DHCP test is successful, a device capable of automatically receiving an IP address does actually receive one when connected to the edge device.

The test was successful, as expected the virtual router is accessible both via HTTPS and via SSH whenever no firewalling for these specific traffic kinds is active on the LAN or WAN interface.

Figure 9.2 shows the welcoming page of the virtual router when it is accessed via SSH, figure 9.3 displays the landing page displayed by the virtual router when it is accessed via HTTPS.

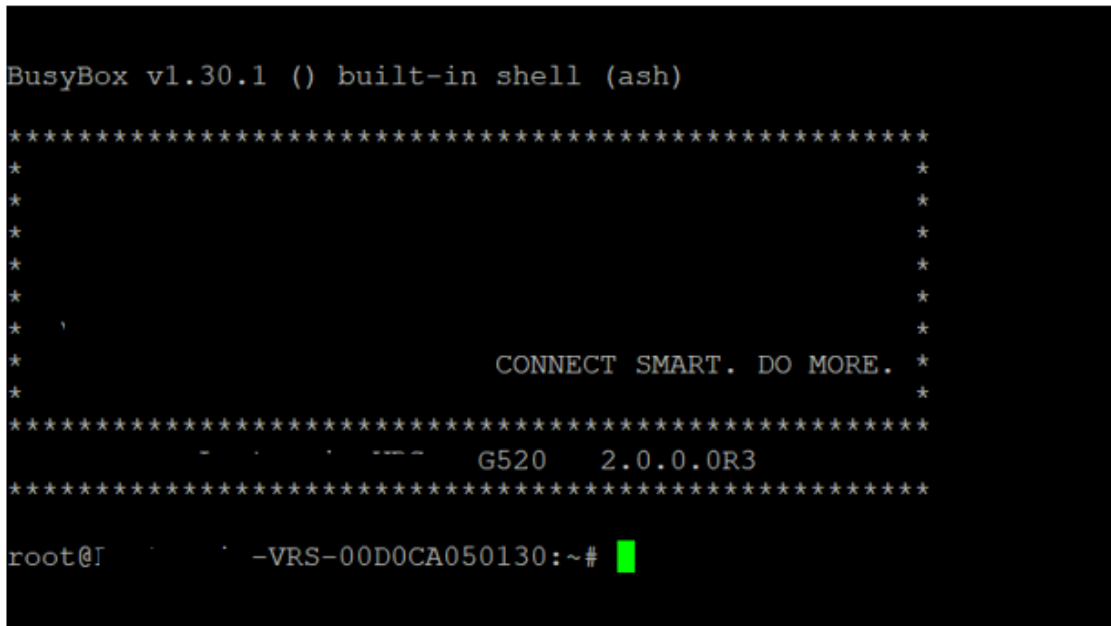


Figure 9.2: The virtual router is accessible via SSH, when accessing it using Putty the user is welcomed by a prompt displaying the manufacturer’s logo (hidden due to an NDA agreement).

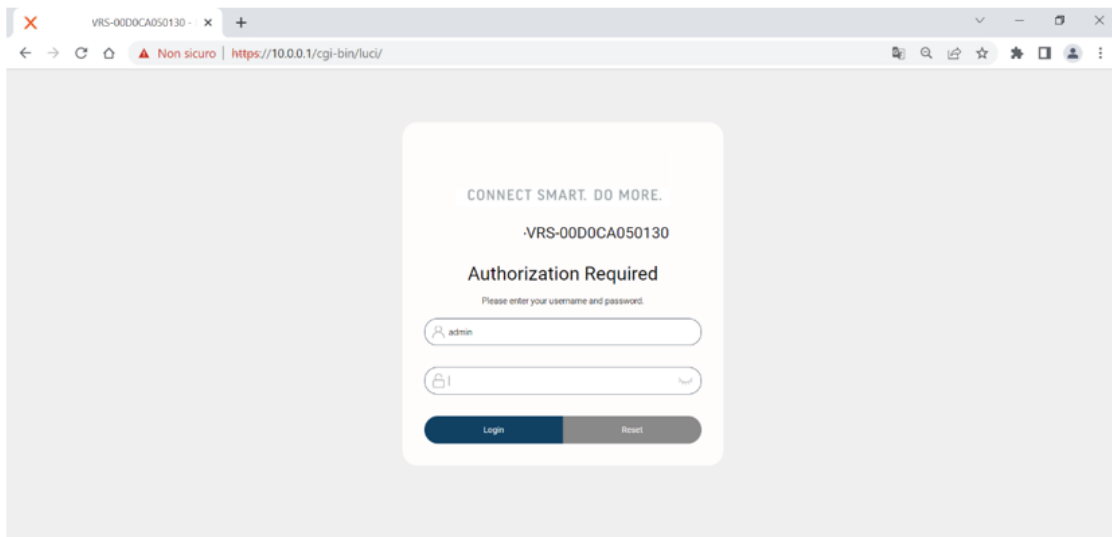


Figure 9.3: The virtual router is accessible via HTTPS, when connecting to the virtual router IP address (figure 8.5) using an Internet browser the user is welcomed by the virtual router UI requiring *Username* and *Password*.

## 9.3 IPsec VPN.

The IPsec VPN function allows the router to take part in a secure Virtual Private Network which is resilient to a wide plethora of cyber attacks. This is a function whose value is always increasing and has reached the point of being almost paramount in any modern enterprise.

The test was conducted according to the procedure described in section 8.5, and the needed parameters were set as displayed in tables 8.4 and 8.5.

The test was successful, even though it was conducted, due to time constraints, only using a peer provided by the manufacturer of the virtual router itself. It would be recommended further inspecting this function, possibly adopting a peer which is not provided by the developer of the virtual routing solution, in order to more confidently state that the IPsec VPN function of the router works even when the developer of the router is not on the other side of the communication setting-up the peer.

That being said an IPsec tunnel was successfully established between the virtual router and the provided peer, which was reachable after the establishment of the tunnel.

Figure 9.4 shows PC1 (with respect to figure 8.6) successfully pinging, i.e. reaching, the IP address assigned to the peer, shown in figure 8.6.

```
gennaro@gennaro-HP-Compaq-6530b-GW688AV:~$ ping 172.16.16.16
PING 172.16.16.16 (172.16.16.16) 56(84) bytes of data:
64 bytes from 172.16.16.16: icmp_seq=1 ttl=63 time=234 ns
64 bytes from 172.16.16.16: icmp_seq=2 ttl=63 time=232 ns
64 bytes from 172.16.16.16: icmp_seq=3 ttl=63 time=232 ns
64 bytes from 172.16.16.16: icmp_seq=4 ttl=63 time=232 ns
64 bytes from 172.16.16.16: icmp_seq=5 ttl=63 time=233 ns
64 bytes from 172.16.16.16: icmp_seq=6 ttl=63 time=230 ns
64 bytes from 172.16.16.16: icmp_seq=7 ttl=63 time=230 ns
64 bytes from 172.16.16.16: icmp_seq=8 ttl=63 time=231 ns
64 bytes from 172.16.16.16: icmp_seq=9 ttl=63 time=230 ns
64 bytes from 172.16.16.16: icmp_seq=10 ttl=63 time=229 ns
64 bytes from 172.16.16.16: icmp_seq=11 ttl=63 time=232 ns
```

Figure 9.4: Peer is reachable through IPsec tunnel (VPN).

## 9.4 Firewall.

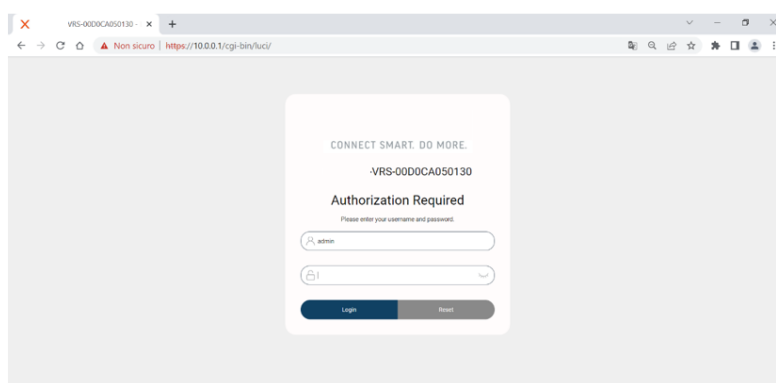
The firewall function, much like the IPsec VPN function, is a quite important function, it allows DSOs to potentially let their connected devices be reachable only through one of the networks the virtual router can reach, for instance a DSO

might wish to deny all kind of connection incoming from the WAN interface and only let its devices be reachable through a connection established locally, through the LAN interface.

The test was conducted according to the procedure described in section 8.6.

The test was successful, when the firewall was off (figure 8.10a), PC2 (see figure 8.9) is able to establish a connection to the virtual router through the WAN interface, figure 9.5a shows the virtual router interface asking for *username and password* after the connection is successfully established.

On the other hand, when the firewall was on (figure 8.10b), PC2 (with respect to figure 8.9) is not able to access the virtual router, and figure 9.5a shows the attempted connection being denied.



(a) Firewall is off, connection is successfully established through the WAN interface to the virtual router.



(b) Firewall is on, a connection can not be established through the WAN interface to the virtual router.

Figure 9.5: Firewall test results.

## 9.5 NAT.

The NAT function gives users a way to respond to the scarcity of available IP addresses. This might not be a straightforward problem DSOs have to face, but one must consider that bigger DSOs might have to address a number of secondary substation that is in the order of the hundreds of thousands, and each substation then needs more than one IP address.

The test was conducted according to the procedure described in section 8.7.

The test was successful, once an *"allow traffic rule"* (figure 8.13) and a *"port forwarding rule"* (figure 8.14) are set, PC1 (see figure 8.11) in listening mode is able to receive Telnet messages as shown in figure 9.6.

```

gennaro@gennaro-HP-Compaq-6530b-GW688AV: ~
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:228 errors:0 dropped:0 overruns:0 frame:0
        TX packets:228 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:17177 (17.1 KB)  TX bytes:17177 (17.1 KB)

wlan1   Link encap:Ethernet  HWaddr 00:26:82:56:80:00
        inet addr:10.69.80.166 Bcast:10.69.80.255 Mask:255.255.255.0
        inet6 addr: fe80::226:82ff:fe56:8060/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:48 errors:0 dropped:0 overruns:0 frame:505
        TX packets:124 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:5758 (5.7 KB)  TX bytes:17396 (17.3 KB)
        Interrupt:17

gennaro@gennaro-HP-Compaq-6530b-GW688AV:~$
gennaro@gennaro-HP-Compaq-6530b-GW688AV:~$
gennaro@gennaro-HP-Compaq-6530b-GW688AV:~$
gennaro@gennaro-HP-Compaq-6530b-GW688AV:~$ nc -l 2000
Clad
  
```

Figure 9.6: PC1 is able to receive the Telnet messages through the NAT function of the virtual router.

## 9.6 Static Routing.

Static routing is the most basic function of a router. It is already implicitly tested by all the other tests conducted for this thesis work.

Following the procedure described in section 8.8, it can be stated the test was successful and specifically reachability was proved to be effective according to the routes listed in table 9.1, built with respect to the lab scheme of figure 8.11.

<b>Source</b>	<b>Destination</b>	<b>Result</b>
PC2 (Address: 192.168.4.30/24)	PC1 (10.0.0.209/24)	Success
PC2	Virtual Router LAN Interface (10.0.0.1/24)	Success
PC2	Virtual Router WAN Interface (192.168.24.1/30)	Success
PC1	External Router on Network 2 (192.168.24.2/30)	Success

Table 9.1: Static Routing Reachability table.



## Chapter 10

# Conclusions and further development.

The role of the router in a modern society is of paramount importance, it has become an essential device even in those realities where telecommunications played a secondary role until recently, such as in power networks.

The need of DSOs all around the world to assure a certain level of quality of service has induced them to adopt telecommunication systems, and reliable telecommunication systems at that, that can perform the same tasks an operator would, just as effectively, but in a smaller amount of time.

When it comes to reducing the duration of interruptions DSOs have adopted several automation tactics. Automation allows to locate the branch of the network where the fault causing the interruption has occurred in a significantly smaller amount of time when compared to operators, as depicted in chapter 2.

Latest automation tactics require secondary substations to be always connected, in order to react to a fault as quickly as possible. This need of having their substations always connected urged DSOs to adopt the IP (Internet Protocol) for their communications.

This is where **routers** come into play. IP requires the deployment of devices called routers to determine which is the best next "hop" in the trajectory that delivers packets from source to destinations, as described in chapter 6.

Gridspertise has studied a solution, **the edge device**, that allows, through the adoption of *edge computing and virtualization*, to perform the tasks needed for automation, and more, while reducing the cost of implementing automation, by buying only one device instead of multiple, and on top of that giving the opportunity to still install virtualized future developments (chapter 4).

The work conducted together with the colleagues at Gridspertise aimed at verifying the functions that came with the first version of virtual router that was provided worked as expected (chapter 8).



The goal was not to approach testing in order to define a comparative, structured model that would allow on one hand to answer to the question "**do the functions work?**" and on the other to answer to the question "**how well do the functions work?**", rather to verify that they worked and would have performed the required tasks in case of deployment of the solution.

Even though the virtual router, in its first version, does not supply with all the main functions required to satisfy DSOs study cases constraints, functions presented in chapter 7, the tests conducted for this thesis proved that the provided functions work as expected, with the results described in chapter 9. The IPSec VPN function of the router though, was tested using as peer one provided by the manufacturer of the virtual router itself, and testing would probably yield more solid results if in the future the same function could be tried with a peer not provided by the manufacturer.

This approach undoubtedly offers a significantly practical perspective of the validity of the **virtual router**, once deployed operators are likely to need a solution which is as close to "plug&play" as possible, i.e. which requires as little setting as possible, and that performs the needed tasks.

It is undeniable, though, that the examined bibliography highlights a constraint on the latency of communications, topic dealt in chapter 2, that could potentially be negatively affected by any poorly performing device in a secondary substation, router included.

The question comes spontaneously, how can one state which is the best virtual router solution among a set of tested virtual routers?

The answer probably lies in the  $\frac{\text{performance}}{\text{price}}$  ratio.

One way of measuring such ratio could be:

1. define a performance indicator, it could be the same for all functions that need to be tested, or it could differ from function to function, this could be measured as  $\frac{\text{bytes}}{\text{seconds}}$ ;
2. define a score range for each function. For instance: rate each function between 0 and 5;
3. examine each function. Is the function present in the virtual routing solution under test? If yes go to the next point, if no score 0 for that function;
4. if the function is present, rate it depending on the performance indicator defined in point #1;
5. once all functions have been tested sum up their score and divide them by the price of the virtual routing solution under test, thus obtaining a new indicator which would be measured in  $\frac{\text{performancepoints}}{\text{euros}}$ .

Defining a structured comparative testing method, similar to the one shown in the diagram of figure 10.1, would allow to not only to gauge the performances of

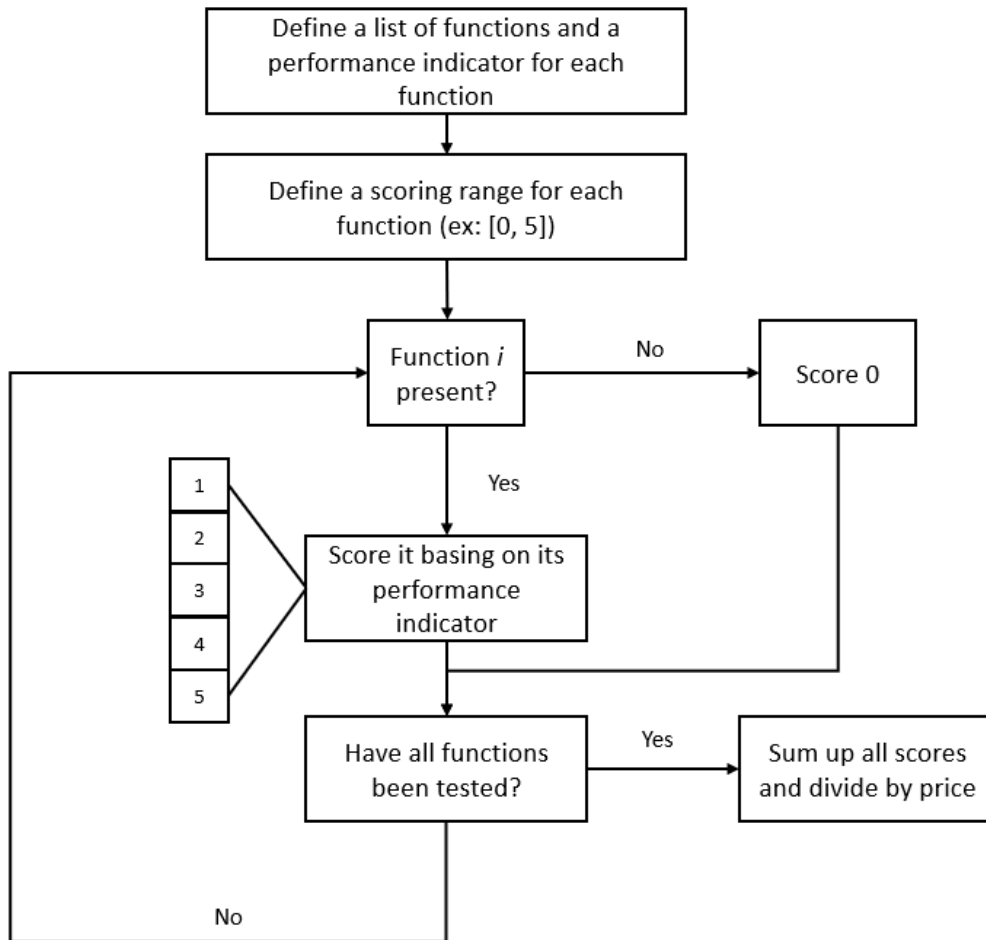


Figure 10.1: Possible comparative testing structure diagram.

each router with respect to their prices, but it would enable the company to state how the tested solution compares with respect to the currently deployed physical router.



# Bibliography

- [1] ARERA. URL: <https://www.arera.it/it/operatori/ele%5C%20testintegrati.htm>.
- [2] Tanuhsree Bhattacharjee and Majid Jamil. “GOOSE Publishing and Receiving Operations of IEC 61850 Enabled IEDs”. In: *2019 IEEE 1st International Conference on Energy, Systems and Information Processing (ICESIP)*. 2019, pp. 1–6. DOI: [10.1109/ICESIP46348.2019.8938272](https://doi.org/10.1109/ICESIP46348.2019.8938272).
- [3] Mauro Biagi and Lutz Lampe. “Location Assisted Routing Techniques for Power Line Communication in Smart Grids”. In: *2010 First IEEE International Conference on Smart Grid Communications*. 2010, pp. 274–278. DOI: [10.1109/SMARTGRID.2010.5622056](https://doi.org/10.1109/SMARTGRID.2010.5622056).
- [4] Tiziano Bianchi. *Applied Information Security and Cryptography, TRANSPORT LAYER SECURITY*.
- [5] Andrew G. Blank. *TCP/IP Jumpstart: Internet Protocol Basics*. Sybex, 2000.
- [6] Marc Boillot. *Advanced Smart Grids for Distribution System Operators, volume 1*. Wiley - ISTE, 2014.
- [7] M. Brew et al. “UHF white space network for rural smart grid communications”. In: *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. 2011, pp. 138–142. DOI: [10.1109/SmartGridComm.2011.6102305](https://doi.org/10.1109/SmartGridComm.2011.6102305).
- [8] Rob Cameron. *Configuring NetScreen Firewalls*. Elsevier Science & Technology Books, 2004.
- [9] Kuor-Hsin Chang. “Interoperable nan standards: a path to cost-effective smart grid solutions”. In: *IEEE Wireless Communications* 20.3 (2013), pp. 4–5. DOI: [10.1109/MWC.2013.6549274](https://doi.org/10.1109/MWC.2013.6549274).
- [10] Docker. URL: <https://www.docker.com/>.
- [11] Fred Dougllis and Orran Krieger. “Virtualization”. In: *IEEE Internet Computing* 17.2 (2013), pp. 6–9. DOI: [10.1109/MIC.2013.42](https://doi.org/10.1109/MIC.2013.42).

- [12] Himanshu Dwivedi. *Implementing the SSH: Strategies for Optimizing the Secure Shell*. John Wiley & Sons Incorporated, 2003.
- [13] *e-distribuzione, Automazione di Rete*. URL: <https://www.e-distribuzione.it/progetti-e-innovazioni/smart-grids/automazione-di-rete.html#:~:text=I%5C%20sistemi%5C%20di%5C%20telecontrollo%5C%20sono,continuit%5C%C3%5C%A0%5C%20del%5C%20servizio%5C%20elettrico%5C%20fornito..>
- [14] Jorg Eberspacher et al. *GSM - Architecture, Protocols and Services*. Wiley, 2009.
- [15] Ayman ElNashar et al. *Design, Deployment and Performance of 4G-LTE Networks : A Practical Approach*. Wiley, 2014.
- [16] e-distribuzione Enel Grids. “WKI-O&M-NOM-21-0007-EDIS”. In: (Sept. 2021).
- [17] Vincenzo Eramo, Emanuele Miucci, and Mostafa Ammar. “Study of Migration Policies in Energy-Aware Virtual Router Networks”. In: *IEEE Communications Letters* 18.11 (2014), pp. 1919–1922. DOI: [10.1109/LCOMM.2014.2360190](https://doi.org/10.1109/LCOMM.2014.2360190).
- [18] Claudio Estevez and Sandra Cespedes. “Improving performance of TCP-based applications in power line communications for smart grids”. In: *2015 7th IEEE Latin-American Conference on Communications (LATINCOM)*. 2015, pp. 1–5. DOI: [10.1109/LATINCOM.2015.7430132](https://doi.org/10.1109/LATINCOM.2015.7430132).
- [19] *ETSI - GSM*. URL: <https://www.etsi.org/technologies/mobile/2g>.
- [20] J. Farquharson, A. Wang, and J. Howard. “Smart Grid Cyber Security and substation Network Security”. In: *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*. 2012, pp. 1–5. DOI: [10.1109/ISGT.2012.6175788](https://doi.org/10.1109/ISGT.2012.6175788).
- [21] Stefano Galli and Thierry Lys. “Next generation Narrowband (under 500 kHz) Power Line Communications (PLC) standards”. In: *China Communications* 12.3 (2015), pp. 1–8. DOI: [10.1109/CC.2015.7084358](https://doi.org/10.1109/CC.2015.7084358).
- [22] Xianming Gao et al. “A general model for the virtual router”. In: *2013 15th IEEE International Conference on Communication Technology*. 2013, pp. 334–339. DOI: [10.1109/ICCT.2013.6820396](https://doi.org/10.1109/ICCT.2013.6820396).
- [23] Xianming Gao et al. “Research of improved mechanisms for virtual router data plane”. In: *Proceedings of the 32nd Chinese Control Conference*. 2013, pp. 6403–6408.
- [24] Alejandro Garces. “A Linear Three-Phase Load Flow for Power Distribution Systems”. In: *IEEE Transactions on Power Systems* 31.1 (2016), pp. 827–828. DOI: [10.1109/TPWRS.2015.2394296](https://doi.org/10.1109/TPWRS.2015.2394296).
- [25] *Gridspertise*. URL: <https://www.gridspertise.com/>.

- [26] D.L. Herbert, S.S. Devgan, and C. Beane. “Application of network address translation in a local area network”. In: *Proceedings of the 33rd Southeastern Symposium on System Theory (Cat. No.01EX460)*. 2001, pp. 315–318. DOI: [10.1109/SSST.2001.918538](https://doi.org/10.1109/SSST.2001.918538).
- [27] Huamiao Hu et al. “Performance Analysis of IEEE 802.11af Standard Based Neighbourhood Area Network for Smart Grid Applications”. In: *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*. 2015, pp. 1–5. DOI: [10.1109/VTCSpring.2015.7146000](https://doi.org/10.1109/VTCSpring.2015.7146000).
- [28] Md. Zahurul Huq and Syed Islam. “Home Area Network technology assessment for demand response in smart grid environment”. In: *2010 20th Australasian Universities Power Engineering Conference*. 2010, pp. 1–6.
- [29] Mohammed Abdulridha Hussain et al. “ARP Enhancement to Stateful Protocol by Registering ARP Request”. In: *2016 International Conference on Network and Information Systems for Computers (ICNISC)*. 2016, pp. 31–35. DOI: [10.1109/ICNISC.2016.017](https://doi.org/10.1109/ICNISC.2016.017).
- [30] Burhan Hyder and Manimaran Govindarasu. “A Novel Methodology for Cybersecurity Investment Optimization in Smart Grids using Attack-Defense Trees and Game Theory”. In: *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. 2022, pp. 1–5. DOI: [10.1109/ISGT50606.2022.9817467](https://doi.org/10.1109/ISGT50606.2022.9817467).
- [31] “IEEE Vision for Smart Grid Controls: 2030 and Beyond Reference Model”. In: *IEEE Vision for Smart Grid Control: 2030 and Beyond Reference Model* (2013), pp. 1–10. DOI: [10.1109/IEEESTD.2013.6598993](https://doi.org/10.1109/IEEESTD.2013.6598993).
- [32] IETF. *HTTP*. URL: <https://datatracker.ietf.org/doc/html/rfc9110>.
- [33] Nobukazu Iguchi et al. “IP network construction learning system utilizing virtual router”. In: *Proceedings of 2011 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*. 2011, pp. 107–112. DOI: [10.1109/PACRIM.2011.6032876](https://doi.org/10.1109/PACRIM.2011.6032876).
- [34] Koya Ito and Noboru Izuka. “Proposal of Client-Server Based Vertical Handover Scheme Using Virtual Routers for Edge Computing in Local 5G Networks and WLANs”. In: *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*. 2023, pp. 0999–1004. DOI: [10.1109/CCWC57344.2023.10099150](https://doi.org/10.1109/CCWC57344.2023.10099150).
- [35] Kyungwoon Lee et al. “Dynamic Network Scheduling for Virtual Routers”. In: *IEEE Systems Journal* 14.3 (2020), pp. 3618–3629. DOI: [10.1109/JSYST.2019.2939409](https://doi.org/10.1109/JSYST.2019.2939409).

- [36] Zhengyi Liu and Baihui Tang. “Communication Between Remote LANs Based on L2TP”. In: *2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS)*. 2018, pp. 221–224. DOI: [10.1109/ICSESS.2018.8663781](https://doi.org/10.1109/ICSESS.2018.8663781).
- [37] R.M. Lopez, G.M. Perez, and A.F. Gomez Skarmeta. “Implementing RADIUS and diameter AAA systems in IPv6-based scenarios”. In: *19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers)*. Vol. 2. 2005, 851–855 vol.2. DOI: [10.1109/AINA.2005.211](https://doi.org/10.1109/AINA.2005.211).
- [38] Rajesh Kannan Megalingam et al. “Robot Operating System Integrated robot control through Secure Shell(SSH)”. In: *2019 3rd International Conference on Recent Developments in Control, Automation Power Engineering (RD-CAPE)*. 2019, pp. 569–573. DOI: [10.1109/RDCAPE47089.2019.8979113](https://doi.org/10.1109/RDCAPE47089.2019.8979113).
- [39] Yanik Ngoko and Christophe Cerin. “An Edge Computing Platform for the Detection of Acoustic Events”. In: *2017 IEEE International Conference on Edge Computing (EDGE)*. 2017, pp. 240–243. DOI: [10.1109/IEEE.EDGE.2017.44](https://doi.org/10.1109/IEEE.EDGE.2017.44).
- [40] Yanni Ou et al. “Online and offline virtualization of optical transceiver”. In: *Journal of Optical Communications and Networking* 7.8 (2015), pp. 748–760. DOI: [10.1364/JOCN.7.000748](https://doi.org/10.1364/JOCN.7.000748).
- [41] Imtiaz Parvez et al. “LAA-LTE and WiFi based smart grid metering infrastructure in 3.5 GHz band”. In: *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*. 2017, pp. 151–155. DOI: [10.1109/R10-HTC.2017.8288927](https://doi.org/10.1109/R10-HTC.2017.8288927).
- [42] *PuTTY*. URL: <https://www.putty.org/>.
- [43] Zhengfeng Qian et al. “Performance of traffic aggregation versus segregation for Optical Flow Switching networks”. In: *2011 International Conference on Information Photonics and Optical Communications*. 2011, pp. 1–3. DOI: [10.1109/IPOC.2011.6122860](https://doi.org/10.1109/IPOC.2011.6122860).
- [44] YanMing Ren et al. “Testing system for substation automation system based on IEC61850”. In: *2011 International Conference on Advanced Power System Automation and Protection*. Vol. 3. 2011, pp. 2396–2399. DOI: [10.1109/APAP.2011.6180829](https://doi.org/10.1109/APAP.2011.6180829).
- [45] Mostafa Sayed, Theodoros A. Tsiftsis, and Naofal Al-Dhahir. “On the Diversity of Hybrid Narrowband-PLC/Wireless Communications for Smart Grids”. In: *IEEE Transactions on Wireless Communications* 16.7 (2017), pp. 4344–4360. DOI: [10.1109/TWC.2017.2697384](https://doi.org/10.1109/TWC.2017.2697384).

- [46] Weisong Shi, George Pallis, and Zhiwei Xu. “Edge Computing [Scanning the Issue]”. In: *Proceedings of the IEEE* 107.8 (2019), pp. 1474–1481. DOI: [10.1109/JPROC.2019.2928287](https://doi.org/10.1109/JPROC.2019.2928287).
- [47] Pratik Shrestha and Tshering Dolkar Sherpa. “Dynamic Host Configuration Protocol Attacks and its Detection Using Python Scripts”. In: *2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF)*. 2023, pp. 1–5. DOI: [10.1109/ICECONF57129.2023.10084265](https://doi.org/10.1109/ICECONF57129.2023.10084265).
- [48] Andra-Flavia Sicoe et al. “Fully Automated Testbed of Cisco Virtual Routers in Cloud Based Environments”. In: *2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*. 2022, pp. 49–53. DOI: [10.1109/BlackSeaCom54372.2022.9858288](https://doi.org/10.1109/BlackSeaCom54372.2022.9858288).
- [49] W. Stallings. “SNMP and SNMPv2: the infrastructure for network management”. In: *IEEE Communications Magazine* 36.3 (1998), pp. 37–43. DOI: [10.1109/35.663326](https://doi.org/10.1109/35.663326).
- [50] James S. Tiller. *Technical Guide to IPsec Virtual Private Networks*. AUERBACH, 2005.
- [51] Nasser Tleis. *Power System Modelling and Fault Analysis, Theory and Practice*. Newnes - Elsevier, 2008.
- [52] Valentin Vlad et al. “Control architecture for power distribution systems based on IEC 61850, IEC 61499 and holonic concepts”. In: *2014 International Conference and Exposition on Electrical and Power Engineering (EPE)*. 2014, pp. 132–136. DOI: [10.1109/ICEPE.2014.6969883](https://doi.org/10.1109/ICEPE.2014.6969883).
- [53] Wei Wang and Zhou Zhou. “Exploring Novel Internet-of-things Based on Free Space Optical Communications for Smart Grids”. In: *2020 IEEE 4th Conference on Energy Internet and Energy System Integration (EI2)*. 2020, pp. 4277–4281. DOI: [10.1109/EI250167.2020.9347166](https://doi.org/10.1109/EI250167.2020.9347166).
- [54] Chandra Wijaya. “Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network”. In: *2011 First International Conference on Informatics and Computational Intelligence*. 2011, pp. 355–360. DOI: [10.1109/ICI.2011.64](https://doi.org/10.1109/ICI.2011.64).
- [55] Dan Wing. “Network Address Translation: Extending the Internet Address Space”. In: *IEEE Internet Computing* 14.4 (2010), pp. 66–70. DOI: [10.1109/MIC.2010.96](https://doi.org/10.1109/MIC.2010.96).
- [56] Jian Wu et al. “Energy Efficient 5G LoRa Ad-Hoc Network for Smart Grid Communication”. In: *2021 IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC)2021 IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC)*. 2021, pp. 1–4. DOI: [10.1109/ICEIEC51955.2021.9463809](https://doi.org/10.1109/ICEIEC51955.2021.9463809).



- [57] Liang Yu et al. “An IPsec seamless switching mechanism with high availability and scalability by extending IKEv2 protocol”. In: *2011 International Conference on Advanced Intelligence and Awareness Internet (AIAI 2011)*. 2011, pp. 25–29. DOI: [10.1049/cp.2011.1421](https://doi.org/10.1049/cp.2011.1421).
- [58] Yichi Zhang, Lingfeng Wang, and Weiqing Sun. “Trust System Design Optimization in Smart Grid Network Infrastructure”. In: *IEEE Transactions on Smart Grid* 4.1 (2013), pp. 184–195. DOI: [10.1109/TSG.2012.2224390](https://doi.org/10.1109/TSG.2012.2224390).
- [59] Zhou Zhou et al. “Application of Optical Wireless Communications for the 5G enforced Smart Grids”. In: *2020 IEEE 4th Conference on Energy Internet and Energy System Integration (EI2)*. 2020, pp. 756–760. DOI: [10.1109/EI250167.2020.9347307](https://doi.org/10.1109/EI250167.2020.9347307).