TECHNICAL REPORT

IIT TR-03/2023

A management methodology and system for complex telematic infrastructures

C. Porta

ISTITUTO
DI INFORMATICA
E TELEMATICA

Consiglio Nazionale
delle Ricerche

A management methodology and system for complex telematic infrastructures

Claudio Porta

Computer and Communication Networks
Istituto di Informatica e Telematica - Consiglio Nazionale delle Ricerche
via G. Moruzzi, 1 - 56124 Pisa, Italy

Abstract

A network infrastructure has to be robust, redundant, resilient to failures, with a good level of scalability and flexibility to handle the increasing data traffic that research activities generate. It has also to ensure a good level of data security and integrity, a fundamental requirement for the trust of users. One of the basic prerequisites to obtain this result is the complete knowledge of the network to manage. This document presents a methodology for the management of wide access networks infrastructures. It starts with a brief explanation of the main network components that should be taken into consideration in an access network, classifying them by type and purpose, and it also defines a possible interaction schema between these components in order to have a better management system. Finally, as an example of implementation of the proposed methodology, it describes the software developed for the management of the structured cabling and active devices of the Pisa Research Area campus network.

Keywords: *network management, structured cabling system*

Introduction

One of the main requirements for obtaining good management of wide user access networks [1], such as university campuses or research areas, is the availability of the related documentation regarding the whole infrastructure, which has also to be constantly updated.

Network documentation is not a standard procedure and differs in contents and quantity depending on the characteristics of the related infrastructure. It generally includes information about structured cabling and software configurations of switching and routing equipment.

An incomplete or outdated network documentation can lead to several problems, which may result in economic losses, such as the laying of existing duplicate cabling, or can cause some additional tasks, like the tracking of unreported physical connections, or can increase time detection of faults and anomalies that sometimes affect network operativity.

It is therefore important from a network operator perspective to have a well-organized, updated and easily accessible network documentation.

Additionally, a well organized network documentation can also be used to optimize the infrastructure, providing ideas for new monitoring and security features. In fact, the correlation of this information with data about network traffic detected by other monitoring programmes [2] can enable the development of new functionalities, with the goal for instance to localize current active devices and user stations on network, or to improve load balancing network traffic using alternative passive cabling paths, or even to develop a real-time monitoring of the network devices status.

This paper provides a possible and effective classification of the network components that are relevant for the above mentioned purposes, as well as a practical description of the related work carried out for the monitoring of the Pisa Research Area, actually the biggest Italian public research campus.

Network Components

A first components classification of a telematics network can be performed using the classic distinction between **active** and **passive parts** [3].

Active part

This category includes all hardware devices that route and forward traffic through the network. A further classification can be made also considering the devices functionalities. In fact some of these are used to receive and forward data to user's workstations (e.g. switches), while others are used for interfacing with other networks on the Internet (e.g. routers and gateways). There are also devices with other additional functionalities, like protecting the network from security threats (e.g. firewalls), providing a wireless connection (access points and WiFi controllers), or network application services (e.g. servers, data storage, etc.).

Another heterogeneous set of devices are terminals and user devices (PCs, laptops, smartphones, VOIP[1] phones, printers, etc.). They are not classified as active network devices because they are not part of the network infrastructure but only users.

[1] Voice Over IP

Passive part

The passive part is composed of all the components without power supply that physically transmit the traffic that flows on the network between active components and users devices. In other words it is a set of different cables, which in wide access networks generally corresponds with the structured cabling system [4].

Providing an example, a typical access network can have one or more distributed **technical rooms**. Their number depends on the dimension of the area to be served and on the implemented topology type. In every technical room are installed one or more network **closets** [5] **(or racks)** having the aim to provide connectivity to a given campus area.

Each rack contains:

- Interconnection with other technical rooms (vertical cabling). They are normally optical fiber cables;
- Copper ethernet cabling connection to the user socket workstations (horizontal cabling). This is the set of permutations of all the access sockets installed in a rack;
- Network devices, used to provide connectivity to the above mentioned connections. They are usually switches.
- Patch cords that connect device's interfaces with other device interfaces or with sockets.

All the access socket connections in the network closets are grouped together in patch panels[2] and located in a dedicated space, while their terminations are distributed in the offices workstations. Similarly there is another space in the technical room, generally a different closet or a portion of closet, dedicated for the installation of network devices.

In this context, the cabling system that connects the office workstation sockets with the active device interfaces is called horizontal cabling [4]. Also the set of patch cords inside a closet, which connects switching interfaces and sockets, is part of the horizontal cabling systems. It represents the largest concentration of cables in the building infrastructure and also a critical point for an access network infrastructure. In fact, this is the place in which most of the closet cabling modifications take place.

Logic scheme definition

After a first classification of all the network components it is necessary to understand which of them are useful from a network monitoring perspective.

Considering the active part's items, are particularly important the devices that provide connection to the user's workstations and devices. For that reason switches and access points and their related interfaces have a relevant role. On the other hand, routing devices are not particularly significant because they operate at a higher level than switching devices. They also have a lower interface's density and therefore bring less information about cabling connections.

The same reasoning can be applied to servers and more generally to all the devices that provide services. In any case it is important to keep track of all the device connections, not only of the most important ones.

Talking about passive part components, it is useful to know the buildings and related rooms that are part of the network, distinguishing between personnel offices and technical rooms. It is also relevant to know whether the telematic infrastructure is shared

[2] https://en.wikipedia.org/wiki/Patch_panel

between institutes, the exact location of all the sockets distributed in each room and also the workstations distributions.

Furthermore, It is essential to know the set of all existing cabling connections between active and passive components, which compose the network topology configuration.

Cabling connections can be classified in three different types:

1. patch cords that interconnect switching devices. They are made in copper or fiber optic, and they are located in the active part of a network closet;
2. patch cords that connect switching interfaces with passive sockets. They are generally ethernet cables;
3. structured cabling system, which is the set of cables that connects different network closets (vertical cabling) and another set that connects the sockets inside a closet with the plugs located on the office's workstations (horizontal cabling).

Interaction between components

A well designed network is normally a modular and scalable infrastructure, composed of various components that are in relation to each other. The set of interactions, constraints and properties that define the component relations can be represented schematically using a class diagram, like that in the figure 1 below.

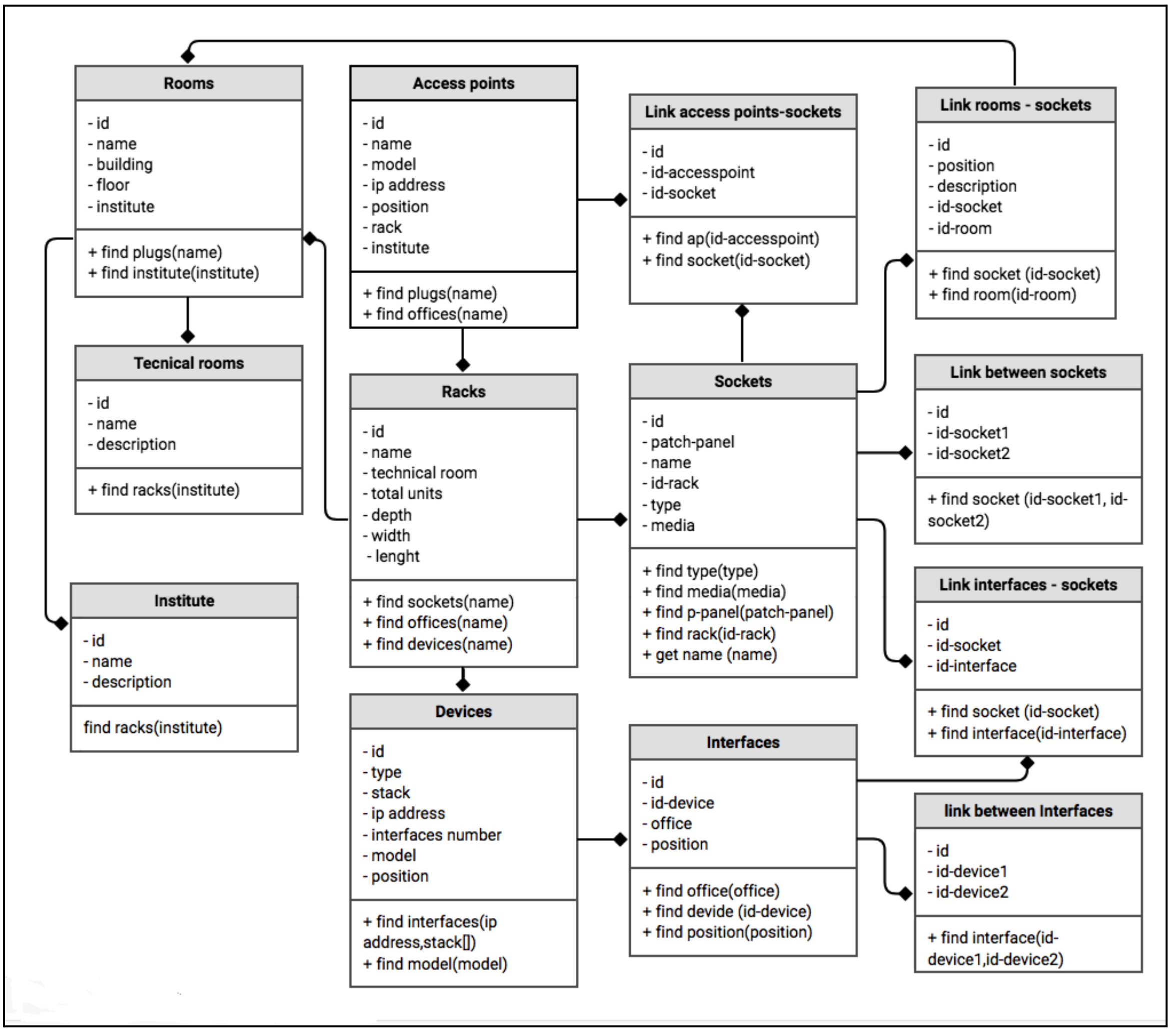


Figure 1: schematic interactions between network components

Each significant component is represented using a class notation, while those considered less significant are defined as class attributes. For example patch panel components are not considered significant ones and are represented as an attribute of the class rack, which represents the set of network racks.
A class can also be an abstract representation of more components. Providing an example, the class “devices” represents generic devices (e.g., router, switch, or server) and their type is specified by the “type” class attribute.

A possible interpretation of the diagram in figure 1 can be the following one:

A network infrastructure can be shared across one or more **institutes**. Every institute is located in one or more buildings composed of **rooms**. Every room is identified by its name, its home institution and some information about its location (building, floor, etc.). There are also **technical rooms**, which are dedicated spaces where network **racks** are installed.
Each room served by the network infrastructure has user workstations with network access **sockets** installed. Each socket is a structured cabling component consisting of a media cable (permanent link) with two plug connectors at both ends having the same name identifier.
Depending on their connector disposition two types of sockets can be classified:

- The name *access socket* is used when the two connectors are located respectively in a network rack's patch panel and an office workstation. The access sockets are represented by the class “**links rooms - sockets**” in the above diagram. They are generally made with copper cables and RJ45 type Ethernet connectors.

- If the connectors are installed in two different racks, the socket is called “relay”, represented in the diagram by the class “**link between sockets**”. In this case, the cabling type is generally a single or multimode optical fiber, depending on the network infrastructure requirements. The connectors can also be of different types (e.g. LC, SR, ST) and installed in dedicated optical boxes.

In addition to sockets, a network closet also contains a dedicated space (active part) in which the **devices** are installed. Depending on the number of devices and on the node importance, an entire rack can be designated as an active part. Devices are generally switches and have two main goals:

1. forward traffic to other devices;
2. provide connectivity to user devices.

Switch interfaces are considered a relevant and critical part of the infrastructure. For this reason there is a dedicated class for these components called “**interfaces**”.
The connections between switching interfaces and sockets inside the rack are made using patch cords, represented by the “**link-interfaces-socket**” class diagram. In the same way, patch cords are used to connect interfaces of devices installed in the same rack, represented by the “**link between interfaces**” class.

Access Points (AP) are devices considered relevant and specific components, because they extend the network operativity with Wi-Fi technologies. For this reason they are represented by a dedicated class. They are connected in uplink to switching devices using sockets, and these connections are represented in the diagram by the "**link Access Point - socket**" class.

Related works

A preliminary operation before the development of a new software was the research on the internet of software instruments for the management access networks and using the logical classification of network components described above.

The goal was to find a modular, scalable and customizable software, suitable for the management of the CNR Pisa campus area network, characterized by multiple distribution closets that servers three main separated buildings, a high density of access sockets, and also several active devices to monitor. Despite the analysis of several programs designed for network management purposes, it was decided to create a new program with custom functions. This for two main reasons:

1. The network monitoring softwares analyzed ([6] [7]) and similar consider principally the information related to devices , poorly taking into account the passive part components. They are useful but in our case should have been integrated with other instruments that consider more in detail also the passive part components.
   Other software automatically detects all network components, generating a map of the active components and their topology. Unfortunately, these are not free tools and do not scale well when the number of monitored devices increases. They are software designed mainly for data center infrastructures, so they are not especially suitable for access networks because of almost ignored passive part components.
2. The research of programs was also oriented to find software tools that manage principally a network passive part instead of the active part components ([8] - [9]). Unfortunately also in this case, these kinds of software are mainly designed for the monitoring of data center networks, which have a small number of user workstations and differ from access networks also from a topological point of view.

So, the optimal solution has been the development of a new customizable software.

An example of implementation: Area Mapping

Starting from the above requirements, the result has been a new software called Area Mapping, which is currently used to monitor the Pisa Research Area network and to manage the huge documentation relating to its components.

Some functionalities have been adapted starting from a previous software used for years to keep track of the network wiring system of the Pisa Research Area campus [10] but actually dated and no longer supported.

The software has been developed in Python language using the Django framework [11]. This is a modular and scalable web application, so that new features could be easily added, and it is accessible only by authentication, using login and password credentials given by system administrators. For each user it is possible to define specific permissions in order to limit access rights or forbid the use of some functionalities.

Specifically, the application allows only authorized users to perform the following functionalities:

- Locate an IP address in the campus area;

- Locate the sockets installed in an office and detect which of these are connected on network;
- Discover all the sockets installed for each Institute. For each socket, discover its location and its corresponding switching interfaces;
- Find a socket position;
- Get the total number of sockets for Institute;
- Get the socket density for each distribution rack, determining which are used. Sockets can be classified according to their type (access ports or relays) and their cabling type (single-mode fiber, multi-mode fiber or copper);
- Check the number of interfaces available on a switch;
- Locate an access point in the campus and its uplink;

The web application memorizes the network information in a relational database, composed of classes representing the network's components and linked together by foreign key constraints.

Talking about the software architecture, the application is composed of two main sections: a Dashboard and an Administration page.

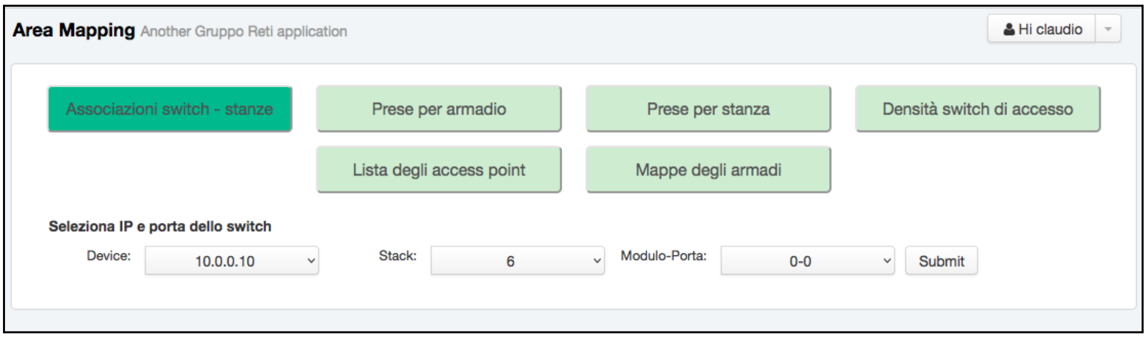
The former is used to present the network data. Using filtering functionalities, a user having proper access rights can easily retrieve the network information needed.

The latter is a typical administration page used to configure and manage the overall functionalities of the application. In this section it is possible to register the users and customize their information access rights, and to consult or modify the stored data using a graphical management interface. It is also possible to upload or download all the network information and system configuration using a communication protocol in a human-readable format, in order to have consultable back-up copies.

The application communicates securely with the SixMonPlus application [2] using web API[3] , in order to correlate cabling information with other information derived from real-time network monitoring activities.

Dashboard

The dashboard is implemented using a minimal, responsive and dynamical web interface. It consists of six activation buttons corresponding to different functionalities. A click in one of these buttons activates the related function that adapts the input fields of the underlying form used to select the input parameters. After the input fields selection and once the submit button is clicked, the results are displayed in a dedicated section at the bottom of the page.



Area Mapping Another Gruppo Reti application
Hi claudio
Associazioni switch - stanze
Prese per armadio
Prese per stanza
Densità switch di accesso
Lista degli access point
Mappe degli armadi
Submit

Seleziona IP e porta dello switch

Device: 10.0.0.10 Stack: 6 Modulo-Porta: 0-0

Figure 2: dashboard with activation buttons and input form

[3] Application Programming Interface - https://it.wikipedia.org/wiki/Application_programming_interface

Dashboard functionalities

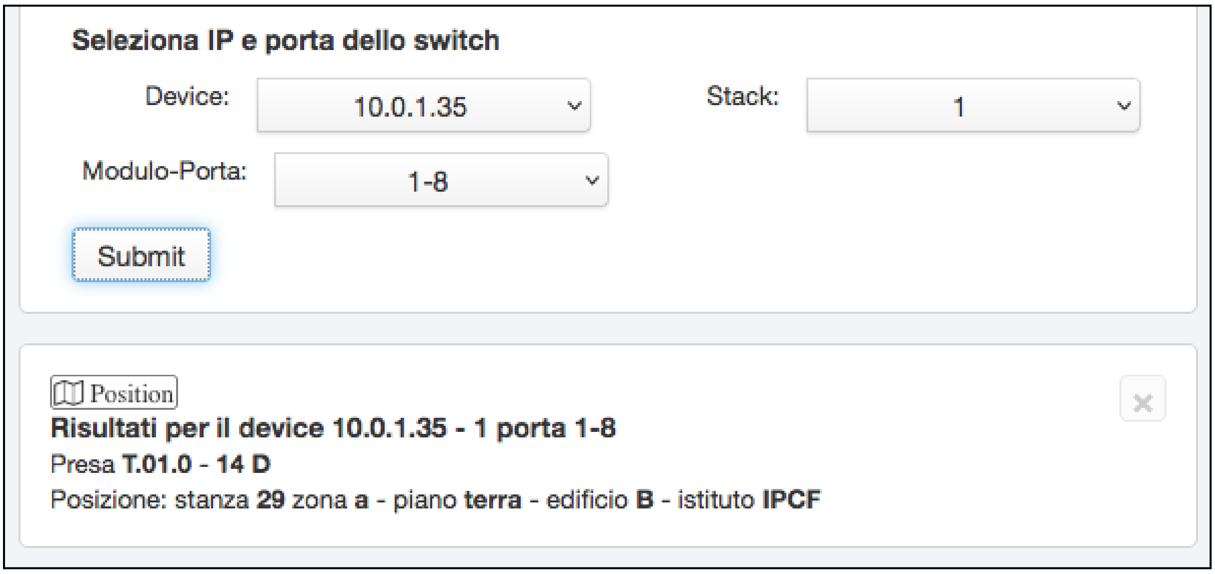
All the functions required input, defined using parameters through the selection of predefined values contained in dropdownlist[4] HTML elements.

Switches - rooms association

This function requires as input three parameters:

1. A switching interface, identified by its numeric id;
2. The switch IP address;
3. The switch stack-number.

The result obtained is the corresponding connected socket (if it exists) and some information about its location (building, floor, room, rack and institute). If the interface is not connected to any socket an "not connected interface" information message is displayed.



Seleziona IP e porta dello switch

Device: 10.0.1.35

Stack: 1

Modulo-Porta: 1-8

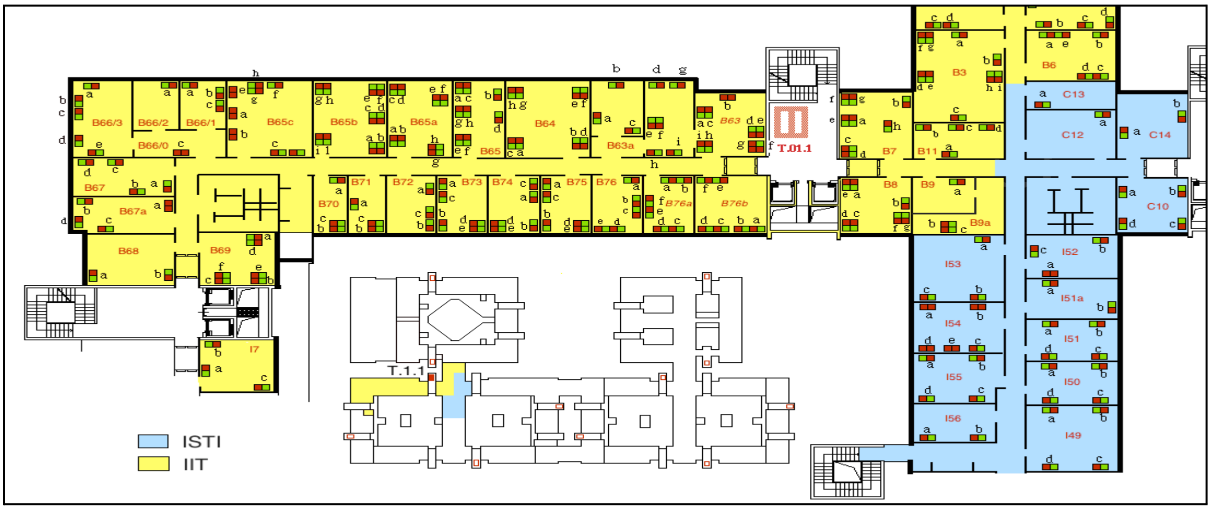
Risultati per il device 10.0.1.35 - 1 porta 1-8

Presa T.01.0 - 14 D

Posizione: stanza 29 zona a - piano terra - edificio B - istituto IPCF

Figure 3: " switch-rooms association" function: search form and obtained result.

A click on the 'position' button shows a map reporting the socket's location and the related racks.



[4] https://en.wikipedia.org/wiki/Drop-down_list

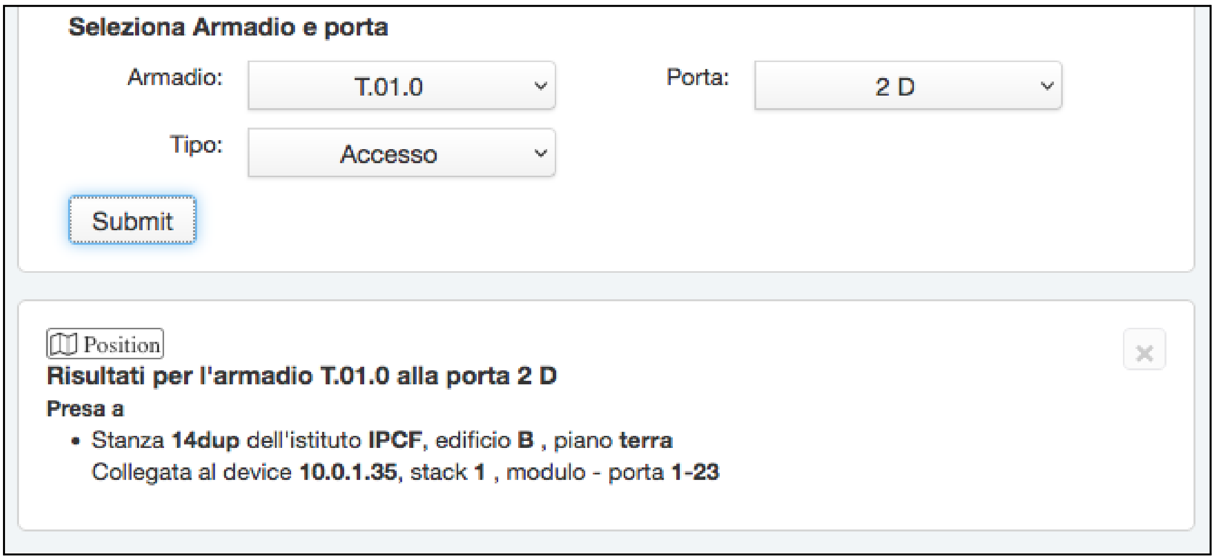
Figure 4: map showing the portion of campus served by a rack. The green and red points are the workstations with access sockets installed.

Racks - sockets associations

This function requires as input three parameters:

1. The name of a network rack;
2. A socket identifier;
3. A socket type (access or relay socket).

The result obtained is the socket position (building, floor, room, institute) and its related switching interface if it is connected on network.



Seleziona Armadio e porta

Armadio: T.01.0

Porta: 2 D

Tipo: Accesso

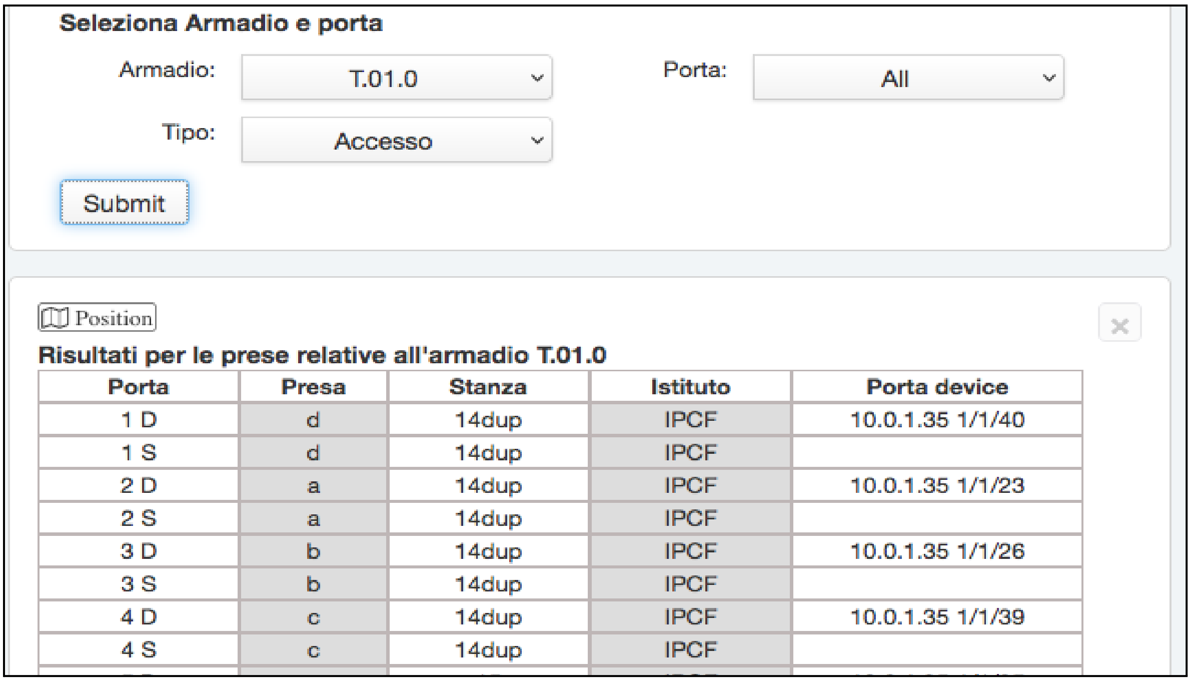
Risultati per l'armadio T.01.0 alla porta 2 D

Presa a

- Stanza **14dup** dell'istituto **IPCF**, edificio **B** , piano **terra**
  Collegata al device **10.0.1.35**, stack **1** , modulo - porta **1-23**

Figure 5: *Racks - sockets associations* function: search form and result obtained for a single rack socket

Optionally, it is also possible to select all the sockets attested in a rack. In this case the result will be a tabular representation, in which every row contains a single socket information. In details for each socket it is reported its position inside an office or room, position in the map, home institution and corresponding switching interfaces if any.



Seleziona Armadio e porta

Armadio: T.01.0

Porta: All

Tipo: Accesso

Risultati per le prese relative all'armadio T.01.0

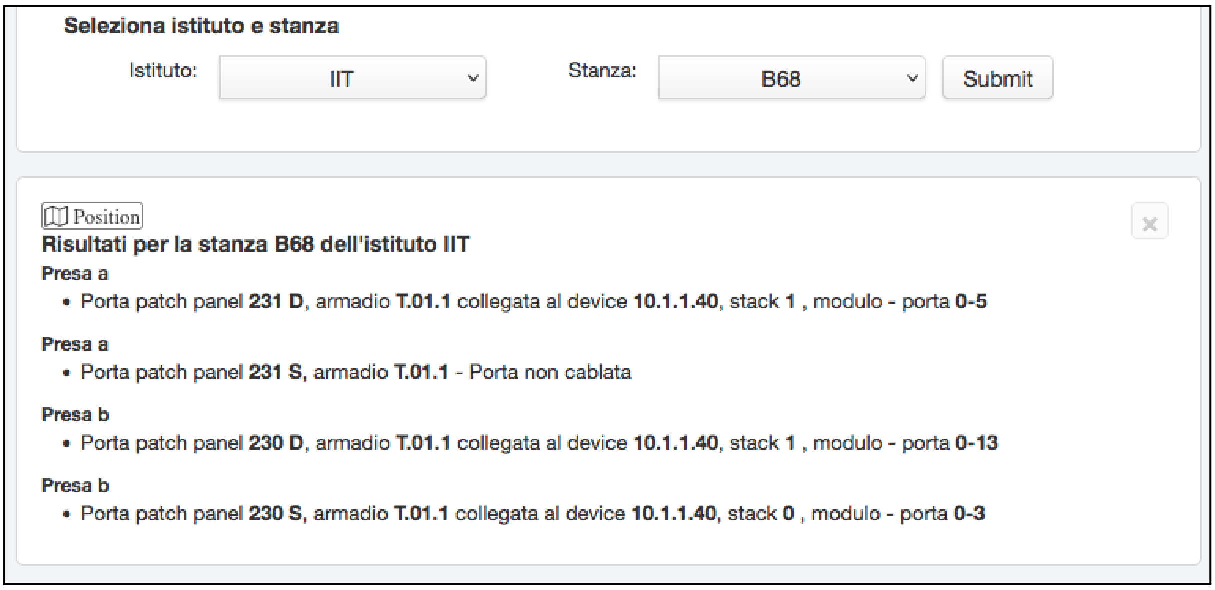
Porta	Presa	Stanza	Istituto	Porta device
1 D	d	14dup	IPCF	10.0.1.35 1/1/40
1 S	d	14dup	IPCF	
2 D	a	14dup	IPCF	10.0.1.35 1/1/23
2 S	a	14dup	IPCF	
3 D	b	14dup	IPCF	10.0.1.35 1/1/26
3 S	b	14dup	IPCF	
4 D	c	14dup	IPCF	10.0.1.35 1/1/39
4 S	c	14dup	IPCF	

Figure 6: *Racks - sockets associations* function: search form and result obtained for all rack's sockets

Like the previous feature, clicking the 'position' button opens an image with the network area served by the selected rack and all the workstations inside every room.

Rooms - sockets associations

This function returns the number of sockets installed in a single room, or optionally the list of rooms with the related network socket installed in each of these. For each socket it is possible to read the corresponding switching interface if present.
Also in this function there is the button 'position', and its activation displays an image with the rooms and sockets selected in the related map.



Seleziona istituto e stanza

Istituto: IIT

Stanza: B68

Risultati per la stanza B68 dell'istituto IIT

Presa a

- Porta patch panel **231 D**, armadio **T.01.1** collegata al device **10.1.1.40**, stack **1** , modulo - porta **0-5**

Presa a

- Porta patch panel **231 S**, armadio **T.01.1** - Porta non cablata

Presa b

- Porta patch panel **230 D**, armadio **T.01.1** collegata al device **10.1.1.40**, stack **1** , modulo - porta **0-13**

Presa b

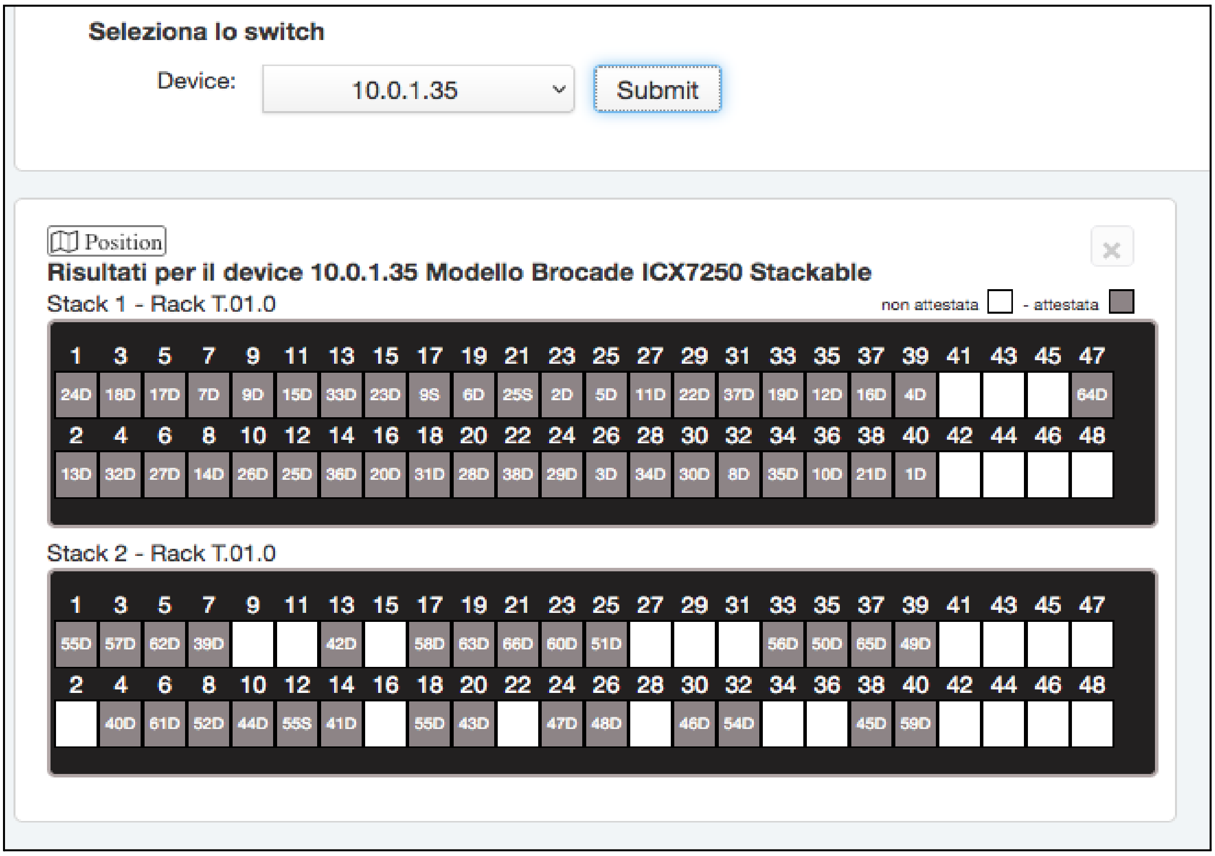
- Porta patch panel **230 S**, armadio **T.01.1** collegata al device **10.1.1.40**, stack **0** , modulo - porta **0-3**

Figure 7: *Rooms - sockets associations* function: search form and result obtained for the selected room.

Access switch density

After the selection of an IP address as input parameters from a dropdownlist menù, this function returns all the switching interfaces of the switch with the IP selected. Active interfaces are represented by a gray square with an alphanumeric identifier inside. This identifier can represent the interface of another device, a user access socket or a relay to another rack depending on the connection type. The not connected interfaces are represented with a white color instead.

The selection of an active socket opens a dialog box containing the information about the socket position (floor, building, institute, room) and a button 'Position' that if clicked displays an image with the socket position in the institute map.



Seleziona lo switch

Device: 10.0.1.35

Risultati per il device 10.0.1.35 Modello Brocade ICX7250 Stackable

Stack 1 - Rack T.01.0

non attestata □ - attestata ▨

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
24D	18D	17D	7D	9D	15D	33D	23D	9S	6D	25S	2D	5D	11D	22D	37D	19D	12D	16D	4D				64D
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48
13D	32D	27D	14D	26D	25D	36D	20D	31D	28D	38D	29D	3D	34D	30D	8D	35D	10D	21D	1D				

Stack 2 - Rack T.01.0

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
55D	57D	62D	39D			42D		58D	63D	66D	60D	51D				56D	50D	65D	49D				
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48
	40D	61D	52D	44D	55S	41D		55D	43D		47D	48D		46D	54D			45D	59D				

Figure 8: "access switch density” function": search form and the result obtained for switch 10.0.1.35, which consists of a stack composed of two modules installed in the T.01.0 rack.

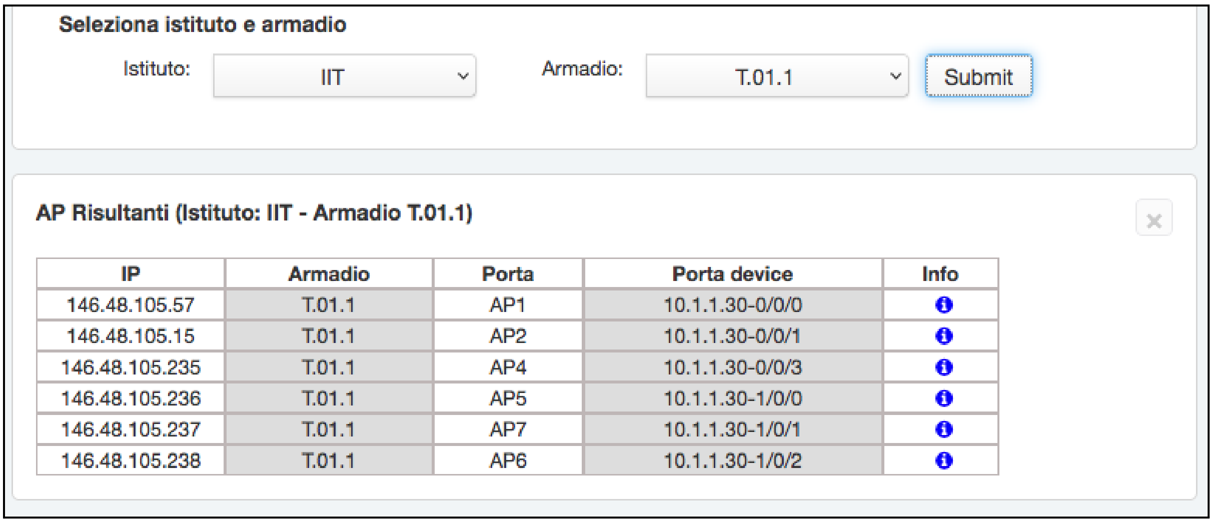
Access Point List

This feature can be used to get information about the Access Points of the WI-FI network. Access Points (APs) search can be improved according to two criteria:

1. filtering by institute
2. filtering by network rack

The result is tabular information regarding the selected APs, containing their IP addresses, uplink sockets and related racks, and the switching interfaces that provide connection.

There is also an info button, and its click displays a dialog box with additional information (custom name, location, model, number of interfaces).



Seleziona istituto e armadio

Istituto: IIT

Armadio: T.01.1

Submit

AP Risultanti (Istituto: IIT - Armadio T.01.1)

IP	Armadio	Porta	Porta device	Info
146.48.105.57	T.01.1	AP1	10.1.1.30-0/0/0	ℹ
146.48.105.15	T.01.1	AP2	10.1.1.30-0/0/1	ℹ
146.48.105.235	T.01.1	AP4	10.1.1.30-0/0/3	ℹ
146.48.105.236	T.01.1	AP5	10.1.1.30-1/0/0	ℹ
146.48.105.237	T.01.1	AP7	10.1.1.30-1/0/1	ℹ
146.48.105.238	T.01.1	AP6	10.1.1.30-1/0/2	ℹ

Figure 9 “Access Point list" function: search form and result obtained filtering by Institute (IIT) and by rack (T.01.1).

Rack maps

This function is used to display graphically the parts of the campus served by each of the technical rooms and related network racks.

Every map corresponds to a different area of coverage, marked in different colors according to their corresponding home institution. In each room are also shown the user workstation having network sockets, represented by red and green squares and a letter. Generally the green color represented data sockets, while the red one represented sockets dedicated to telephony. The association between the letter and the room name defines the workstation of every socket inside the maps.

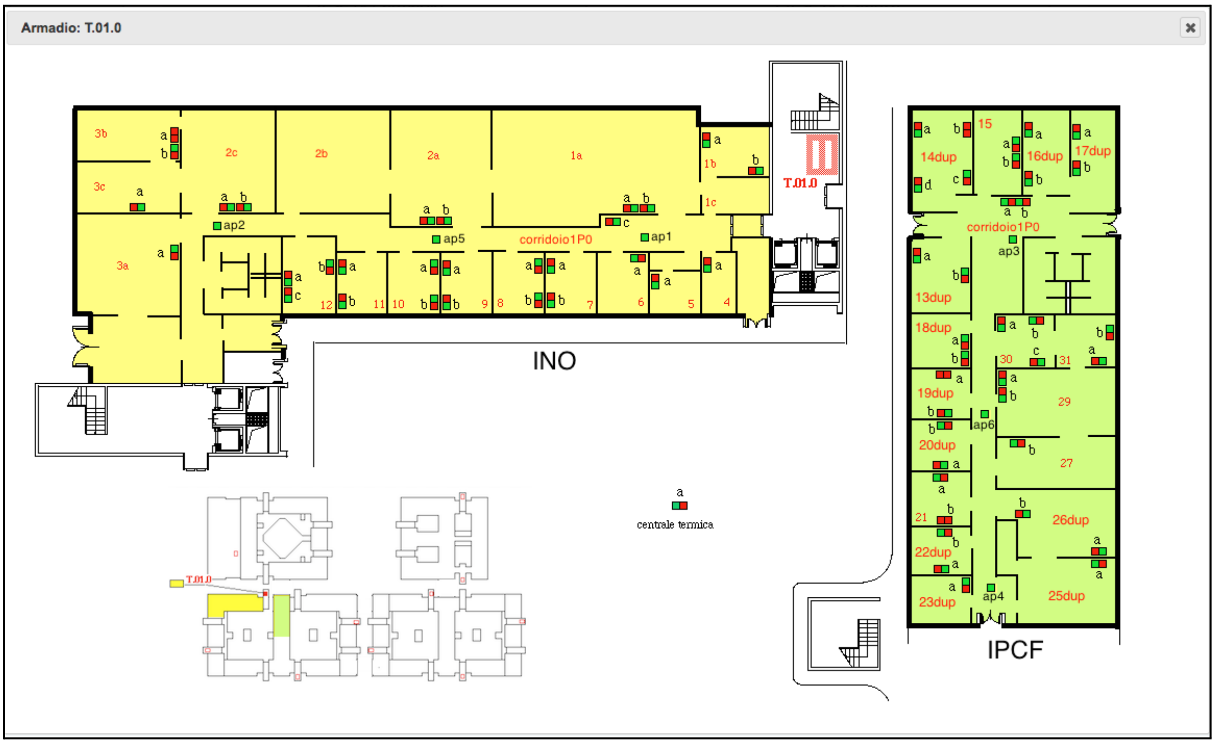
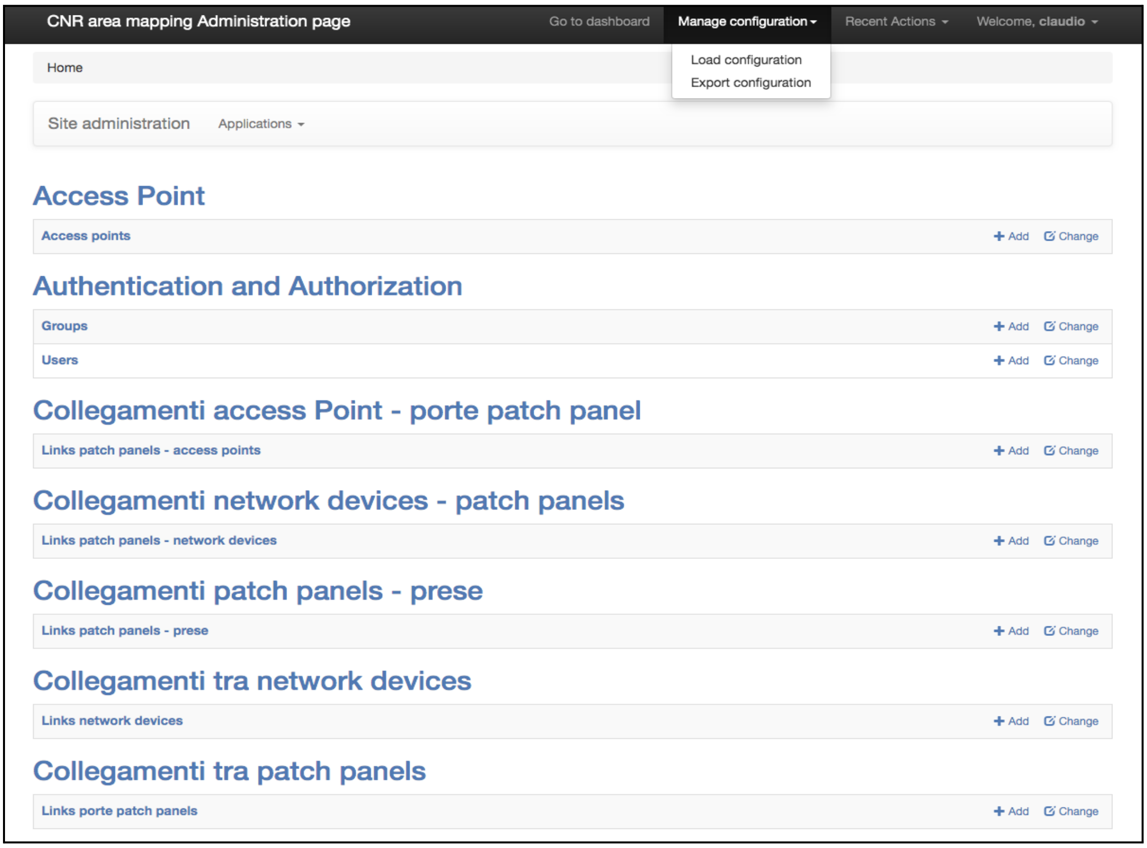


Figure 10 Graphical representation of the portion of the building served by cabinet T.01.0. The yellow color represents the INO institute, while the green color represents the IPCF institute. The names in red represent the names of the individual rooms, while the squares represent the

workstations. The thumbnail at the bottom left represents the area campus in the building served by the rack in the 1.0 technical room.

Admin section - data management and configurations

The application also has a control part for system administrators. In this section it is possible to manage the users permissions and use a graphical interface to perform data modifications.



Access Point

Access points + Add Change

Authentication and Authorization

Groups + Add Change

Users + Add Change

Collegamenti access Point - porte patch panel

Links patch panels - access points + Add Change

Collegamenti network devices - patch panels

Links patch panels - network devices + Add Change

Collegamenti patch panels - prese

Links patch panels - prese + Add Change

Collegamenti tra network devices

Links network devices + Add Change

Collegamenti tra patch panels

Links porte patch panels + Add Change

Figure 11: main page on the admin section.

Data loading

In the admin section there is the possibility to upload and export data using files in a human-readable format, with the aim to create backups available for consultation.
This functionality can also be used for the editing of big amounts of data at once.

There are two main possibilities to perform data modification:

1. Using the admin interface,;
2. By deleting the data to change and reloading into the system the edited data, with all the modification done in a backup file.

The first solution is suitable for small changes, while the second is useful for big editing changes that involve several network's components.

The loading data procedure is divided into three main steps:

1. Upload of passive cabling information (racks, institutes and rooms, network sockets);

2. Upload of active device configurations (all the network devices and their interfaces, the patch cord connections between interfaces and network sockets).
3. Upload of access point configurations.

This solution has been implemented in this way for two main reasons:

- To separate the information on the structured cabling from that of the active part;
- Avoiding data-overriding in the case of partial changes that affect only some components.

The loading data procedure does not overwrite the information already saved in the system. In order to load and save any change, it is therefore necessary to delete the part of information to change.
Deleting the data of a rack from the application also deletes on cascade all its related information of the passive parts (rooms, network sockets and its associated connections). Similarly, deleting a device configuration deletes all its associated information in the active part (interfaces and its related connections).

Passive part - network access sockets

Passive component data is uploaded using text files sorted by lines in “.txt” format. Each line corresponds to a single socket with additional information about its location (room, institute and position inside the room) and the rack and patch panel in which it is installed
In the example below is reported a line of information, which is a series of ordered alphanumeric strings separated by spaces.

T.01.1	10	9.D	I.I.T.	B2 - b	B
1	2	3	4	5	6

Each string contains a piece of information related to a single socket:

1. The name of the rack in which the socket is installed.
2. The numeric part of the socket identifier. According to the nomenclature inherited from IBM, most sockets are identified for each rack by a number and a letter, "D" or "S", separated by a space (e.g. "22 S"). Other sockets are identified only by a number and an optional string to avoid duplicate identifiers.
   Originally, the letter “S” meant sockets reserved for telephony, while D denoted data sockets, but this distinction has faded with the introduction in the area network of VOIP[5] phones.
3. This string contains two types of information separated by a period. The first is the patch panel in which the port is installed, while the second is the previously mentioned literal part of the socket identifier .
4. It represents the institute owner of the room in which the socket is installed.
5. This part also contains two pieces of information, separated by the "-" sign. The first is the name of the room in which the socket is installed, while the second is a letter that indicates the socket position in the room, useful for its detection in the map of the related rack.
6. Indicates the building in which the socket is installed (A, B or C).

[5] Voice Over IP

Passive part - links between cabinets

Also in this case the information is uploaded on the system using textual files in .txt format and splitted in lines. Each line corresponds to a single link between racks, and the information is divided into substrings.
Providing an example, the following line configuration is splitted into seven strings:

T.19.0	T.19.1/3	10.rilancio	T.19.1-10	T.19.0/3	ethernet	58 D
1	**2**	**3**	**4**	**5**	**6**	**7**

A link connection can be imagined as a cable that starts in a rack (source) and arrives in another rack (destination).

1. The name of the rack in which the socket is installed.
2. The socket identifier in the source rack.
3. The patch panel number in which the socket is installed and the type of connection (relay). The two information are separated by a dot;
4. The destination rack's name and, separated by a '-' sign, the patch panel identifier in which the socket is attested in the destination rack.
5. The socket identifier in the destination rack.
6. The type of physical connection (Ethernet, singlemode fiber or multimode fiber).
7. The seventh string is optional, and defines a further connection with this link connection. In this specific case, it means that a patch cord connects the rack destination port (T.19.0/3) to another access port (58 D) installed in the same rack.

Active components

The upload on the system of the active part data is performed using .xlsx files (open excel format). Every .xlsx file is composed of sheets, and each sheet is used to memorize the information of a single physical device. Therefore if a device is composed of two stacked units, its configuration will be stored in two separated sheets.

Each sheet contains two main sections:

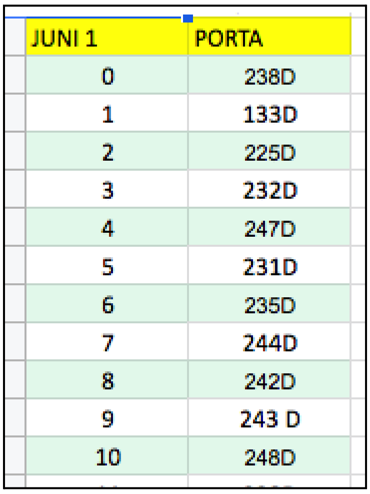
- An header at the first line that contains the general information of the device;
- A series of lines, divided in two or more columns, representing the associations between device interfaces and network sockets (or other device interfaces)

An example of a header row is the following. Each string is a different data:

Switch	Brocade ICX7250 Stackable	48	10.0.1.35	1	T.01.0_1	1 unità rack	10.0.1.35-1 primo in alto	10.0.1.35
1	2	3	4	5	6	7	8	9

1. The device type (router or switch);
2. The device model;
3. The number of ports of the device;
4. A logical address identifier (in this case an IP address);
5. A physical address identifier (in this case the stack number);
6. The rack where the device is installed;
7. The space occupied by the device, expressed in rack units;
8. A generic description of the installation position;
9. The IP address of the device.

The other rows contain information about the device interfaces and their related connections. The first column shows the device interfaces, while the second column shows the corresponding connections, which can be passive (access sockets or relays to other rack) or active (other device interfaces installed in the same rack).



JUNI 1	PORTA
0	238D
1	133D
2	225D
3	232D
4	247D
5	231D
6	235D
7	244D
8	242D
9	243 D
10	248D

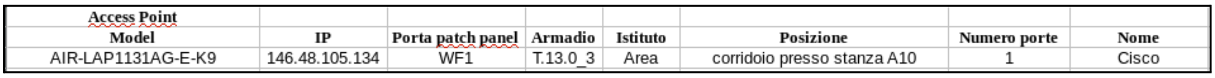
Figure 12: Representation of the connections between device interfaces and network access sockets.

Access Point

Access points (APs) represent a particular active component class that differs from the others, because they are connected to switching devices using structured cabling systems like user devices, but they are used to provide Wi-Fi connectivity. Their information is contained in a single readable ".xlsx" configuration file. Each line corresponds to information related to a single access point.

The data memorized are:

- Access Point name and model;
- IP address;
- The socket's uplink connection and its rack;
- The institute served by the AP;
- A textual description of its location.
- The AP's interface number



Access Point							
Model	**IP**	**Porta patch panel**	**Armadio**	**Istituto**	**Posizione**	**Numero porte**	**Nome**
AIR-LAP1131AG-E-K9	146.48.105.134	WF1	T.13.0_3	Area	corridoio presso stanza A10	1	Cisco

Figure 13: Single line of the Access Point configuration file.

Data exporting

In the admin section it is also possible to export data. Like the upload procedure, it is possible to choose which part of information to export, selecting the passive part, the active components part or only the information regarding the APs.

The files exported have the same format of the files used in the upload procedure. For this reason they can also be used as backup copies, useful in the event of a system restore operation.

API Area Mapping

The application is able to communicate with other monitoring systems [2] in order to correlate its data with other useful remote information and in this way facilitate the network administrators tasks. All the remote communication takes place using API[6]s in JSON format [13] .

In detail, there are three implemented method that can be used for communicate using API with other applications:

- **find_plug**: it takes as input a device's IP address and an interface number, then returns the connected socket and others information regarding its location;
- **find_rack**: it takes in input a device's IP address and returns the related network rack in which the input device is installed;
- **find_position:** it takes in input a network rack's identifier and displays the area with all the network sockets positions served by this rack.

All these methods can be invoked only by authenticated users.

Communication security

All the communications occur using the HTTPS protocol [12]. For any request, the integrity of packets is verified performing an header signature check. Packet headers are generated using a SHA256 function that takes as parameters the body of the message, a shared secret key between the communicating applications and a timestamp expressed in unix epoch time format.
The request header must have the signature and timestamp fields, containing the generated signature and the timestamp of the request.

Communication protocol

Find_plug

Input parameters

ip: a device's IP address
port: a device's interface identifier, depending on the device's model (e.g. eth1/1/22)

```
{ "method":"find_plug",
  "param":{"ip":"ip_device", “port”:”port_device”}  }
```

Response

- error

```
 {“status”: “error”, “errors”:[error_list]}
```

- result not found

```
  {“status”: ”not found”, "porta": ”porta_device”, "device":
 “device_ip”, ”stack”:”stack_id” }
```

[6] Application Programming Interface

- partially found result

```
{“status”: ”found”, "rack": ”rack_id”, "ppp":
“porta_patch_panel”, ”warning”: [warning_list] }

{“status”: ”found”, "rack": ”rack_id”, "ppp":
“porta_patch_panel”, “presa”:”id_presa”,”warning”:
[warning_list] }
```

- result complete

```
{“status”: ”found”, "rack": ”rack_id”, "ppp":
“porta_patch_panel”, “presa”:”id_presa”, “stanza”:”stanza”,
”piano”:”piano”, “istituto”:”istituto”, “edificio”:”edificio”}
```

Find_rack

Input parameters

ip: a device’s IP address
port (optional): a device’s interface identifier

Response

- error

```
{“status”: “error”, “errors”:[error_list]}
```

- result not found

```
{“status”: ”not found”, "rack": ”rack_id”,
”warning”:[warning_list]}
```

- result complete

```
{“status”: ”found”, "rack": ”rack_id”}
```

Find_position

Input parameters

rack: the rack’s identifier

Response

- error

```
{“status”: “error”, “errors”:[error_list]}
```

- result not found

```
{“status”: ”not found”, "rack": ”rack_id”,
”warning”:[warning_list]}
```

- result complete

```
{“status”: ”found”, "rack": ”rack_img”}
```

Future works

The application was initially implemented as a prototype and after a successful testing phase is now one of the main monitoring software for the Pisa Research Area's cabling system. Although the main functionalities are now implemented, stable and tested, there are still improvements that could be made as well as eventual bug fixes.

Some of these relate to graphics, others to the integration of new functions and protocols, and others refer to a more detailed representation of data type.

Talking about the program’s graphical aspect, a good improvement would be a new implementation of the maps related to network racks, using for instance new graphic models of 3D libraries. This could be done taking care of the interface’s rendering aspects, avoiding to use too many computational resources because the system has to be used also available on mobile devices. Other graphic improvements could involve the whole interface, with a restyling using another new javascript framework.

For what concerns the integration of new functionality, as far as the compatibility issue allows, the use of SNMP and automation tools would lead to other additional dynamical features, enabling for example the real-time monitoring of the interfaces status of all the active devices. Should be further investigated whether if the new proposed features could be really useful, because of the additional traffic generated to retrieve the information and the consequent additional workload on the networks components, and also to avoid the generation of duplicate information that may be available on other monitoring tools and should therefore be integrated together and not implemented again.

Another useful improvement could be a better integration with other existing traffic analysis tools, with the aim to geolocalise in real time the IP addresses used on the network.

Another innovation being pursued is a better representation of the whole cabling system in order to obtain a better detailed classification in particular for the fiber cabling system that composes the vertical wiring of the area's telematics network.

Conclusions

Managing a large telematics network infrastructure and maintaining high standards is a challenging task, especially if not supported by accurate and up-to-date documentation and monitoring systems .

This document provided a possible classification regarding the main active and passive network components that need to be monitored in order to have useful and easily accessible documentation. After a description and a classification of typical network components it also describes the logical interactions between these components and that characterized a network infrastructure.

It also provided a practical example of this classification, describing the tool developed for the management of the structured cabling systems and all the active components that compose the access network of the Pisa Research Area. In detail it described all the features implemented and the mechanisms to communicate and interact with active and used other monitoring tools, as well as the possible future developments of the application.

The application has proved to be useful for several monitoring operations, especially interacting with other programs, as well as for documental and information purposes. In particular, the sharing of data through API communication with the SiXMoNPluS [2] tool enable network administrators to quickly localize IP addresses inside the campus. This operation is essential to perform a fast detection and solving of network problems caused by users, such as the physical connection of unauthorized devices, the setup of abusive DHCP servers, IP addresses collision, loops and broadcast storms or simply malfunctioning of switching devices and access points because of hardware or software problems.

In addition to the rapid solution of this kind of problems, it is normally used to detect information regarding the passive cabling system, in particular for the connection between access network sockets and access points location with their related switching interfaces. Consequently, the implemented tool significantly reduces the time required for network interventions compared to the past. There are also some improvements that could be done, but currently the system, despite a limited number of functions has proved very useful, also for the monitoring of the structured cabling system.

References

[1] Access Network - Wikipedia
https://en.wikipedia.org/wiki/Access_network

[2] A.Gebrehiwot, A. De Vita, F.Lauria, A.Mancini, C.Porta - 6MoNPlus: Geographically distributed Dual Stack network monitoring
Terena Networking Conference 2016, 12 - 16 June, Praga, Czech Republic

[3] *Active and Passive network components*
http://www.poradykomputerowe.eu/en/active-passive-devices-in-a-computer-network/

[4] Cisco networking academy program
https://www.ccri.edu/faculty_staff/comp/tonyrashid/files/CCNA1_CS_1_en.pdf Pag. 5 - 23

[5] What's in a Network Closet? - LDP Associates, Inc.
https://www.ldpassociates.com/what-is-a-network-close

[6] InterMapper -Website
https://www.helpsystems.com/products/network-monitoring-software

[7] Zabbix - Website
https://www.zabbix.com/

[8] SunBird - Data Center Infrastructure Management - Website
https://www.sunbirddcim.com/what-data-center-monitoring

[9] Patch Manager - Website
https://patchmanager.com/product/

[10] Mario Marinai - IAT-B4-2001-012 - Sistema di gestione ed informativo della Rete Telematica dell'Area di Ricerca di Pisa - 1 Ottobre 2001

[11] Diango - Website
https://www.djangoproject.com/

[12] Roy T. Fielding, Mark Nottingham, Julian Reschke, 2022. RFC 9110 - HTTP Semantics
*Retrieved from https://tools.ietf.org/html/rfc*9110

[13] JSON - JavaScript Object Notation) - Website
https://www.json.org/json-en.html