

Consiglio Nazionale delle Ricerche

**Wireless network federation for Smart Cities:  
an example of implementation in the Research Area  
of Pisa**

A. Mancini, A. De Vita, A. Gebrehiwot, M. Marinai

IIT TR-02/2016

**Technical Report**

**Marzo 2016**



**Istituto di Informatica e Telematica**

# **Wireless network federation for Smart Cities: an example of implementation in the Research Area of Pisa**

Alessandro Mancini, Andrea De Vita, Abraham Gebrehiwot, Mario Marinai

*IIT Institute, National Research Council of Italy  
via G. Moruzzi, 1 - 56124 Pisa, Italy*

*firstname.lastname@iit.cnr.it*

**Abstract.** Demand for mobility access in the research fields is continuously increasing. Indoor wireless networks have proven results when it comes to increasing productivity, giving researchers more flexibility in real time.

Extending this high-performance wireless coverage seamlessly to the outdoors is a critical requirement. With the proliferation of mobile devices and mobile workers demanding to stay connected whether they are moving inside a building or across campus. We were looking for an outdoor wireless network that provides the throughput and performance that users have become accustomed to at their offices.

Smart Campus project, a campus-wide living laboratory of Smart Cities, has increased these needs introducing new kind of network devices like IP cameras and interconnected monitoring sensors that use wireless network.

This technical report describes how to federate separated wireless infrastructures belonging to different administrative domains. It is also provided the technical implementation successfully deployed at the Research Area of Pisa which can be considered as a best practice for Smart Cities projects.

**Keywords:** *wireless network, wi-fi, eduroam, smart campus, federation, smart cities.*

## **CONTENTS**

1. Introduction .....	3
2. The wireless indoor architectures before the federation.....	3
3. The new Outdoor Wi-Fi solution .....	4
4. Federation of the two wireless domains .....	6
5. Final Remark.....	8

## 1. INTRODUCTION

Smart Cities need to connect wirelessly a multitude of heterogeneous sensors. Often several wireless network are already present managed by separate administrative domains. To promote the spread use of sensor networks it is advisable to federate existing networks rather than redesign a new one.

Within the *Smart Campus project* [1], a simulation of a Smart City, several sensors have been deployed which needed wireless connectivity. A single wireless LAN infrastructure domain, covering the indoor and outdoor area of the Research Area of CNR in Pisa, was needed to allow the operation of the sensors. Two separate indoor wireless infrastructures were already present in the campus but mobility between the two domains was not supported.

Moreover, with the proliferation of mobile devices and mobile workers demanding to stay connected whether they are moving inside a building or across the campus, users were also looking for an outdoor wireless network that provides high throughput and best performance.

The group “Telematics Network of CNR in Pisa” which belongs to the Institute of Informatics and Telematics (IIT) is in charge of managing the common networking infrastructures and network services of the Research Area of CNR and has carried out the process of extending and federating the Wi-Fi network infrastructures.

## 2. THE WIRELESS INDOOR ARCHITECTURES BEFORE THE FEDERATION

Both Wi-Fi infrastructures were made at different times, by means of two distinct solutions covering almost all of the indoor areas.

The first one [2], based on Wireless LAN Controller Cisco Systems [3], is the most extended serving a greater number of clients in fact it makes use of ~70 access points (APs), under the management of the Institute of Informatics and Telematics.

The other one, under the management of the Institute of Information Science and Technologies (ISTI), covers a smaller area and is based on Colubris Networks [4] wireless technology and counts approximately 25 APs.

Each of the two architectures provides:

- A set of APs, responsible for wireless coverage, placed along the corridors and rooms of the campus buildings;
- One or more wireless controllers, used to control the AP stations for automated configuration, management and monitoring of wireless network.

The coexistence of the two domains does not guarantee the continuity of wireless service to the mobile stations moving from one domain to another. Although the same Wi-Fi network were announced on both infrastructures, mobility was not possible since the service was provided through different LAN networks.

### 3. THE NEW OUTDOOR WI-FI SOLUTION

Outdoor wireless service was not available, it was possible to use the service only through the weak radio signal coming from the indoor APs. Therefore it was necessary to extend coverage with outdoor units.

The strategy adopted for implementing the outdoor Wi-Fi technology has been to expand the existing Cisco Wi-Fi infrastructure by simply adding outdoor units. In fact the Cisco controller already in use is able to manage up to 100 APs without any additional license fee. In this way we avoided of having an additional management and monitoring systems furthermore keeping the advantage of all the features we were used to.

The unit chosen for outdoor coverage was Cisco Aironet AIR-CAP1552E-E-K9 Access Point.

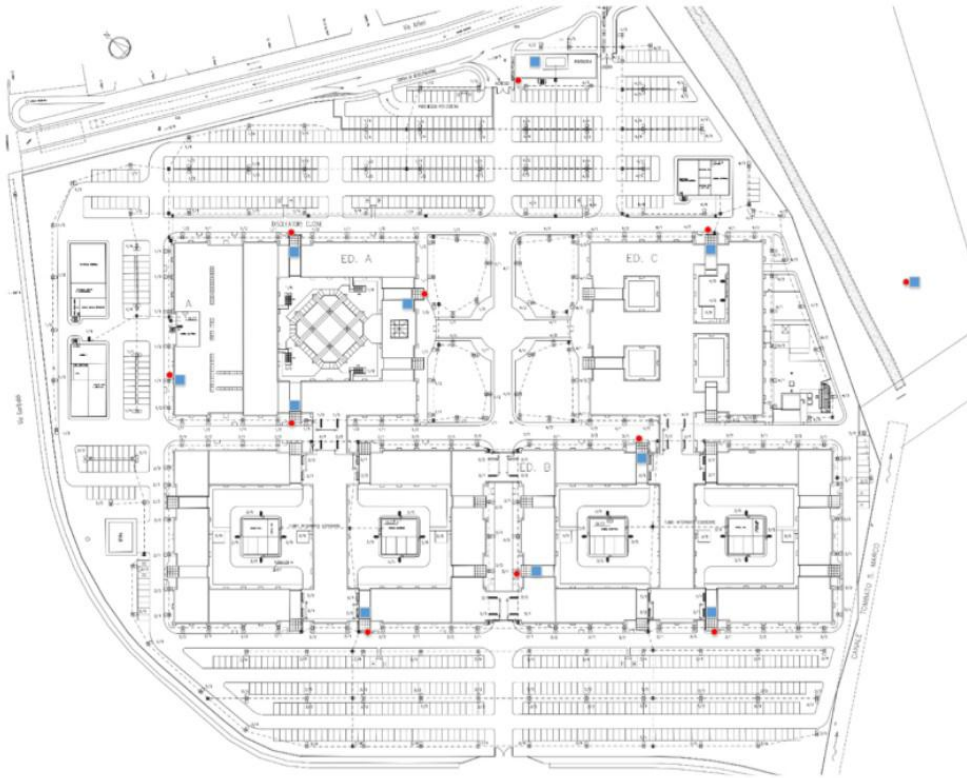


Cisco outdoor AP model AIR-CAP1552E-E-K9

The actions made during the deployment of the outdoor access points has been the following:

- Outdoor coverage planning based on the map of the Campus;
- A site survey making measurements of the Wi-Fi coverage to estimate the appropriate number of APs and to select the best place where to install the equipment. For this activity we used a Cisco demo appliance, model Aironet 1552S, an outdoor Access Point provided by the supplier for a trial;
- Cabling design for network and power supply;
- Wiring setup and access points mounting made by professional technicians;
- Configuration of the outdoor units.

In order to have a proper coverage 11 devices were required. The following picture shows the place where the APs have been installed (red dots) and the corresponding intermediate distribution facility where the cabling system of the access points are terminated (blue dots). The location of the Access Points has been chosen as a trade-off between best coverage and cable length constraints imposed by cabling system.



Campus map indicating the outdoor APs

Ten access points have been installed using a wall mounting kit and omni-directional antennas system at the outer body of the building, which corresponds to the entrance doors as shown following, at approximately 4 meters above the ground level.


The last access point has been installed using a pole mounting kit and a directional antenna at the main entrance of the Campus.



Wall mounted access point

The type of cable used is a composite UTP category 5E + 2x0,75 which provides both the Ethernet and two additional wires for power supply. The characteristic of this cable is described in the following table:

**UTP 5e**



Codice	Formazione	Resist. DC (Ohm/km)	Diam. esterno (mm)	Peso (kg/km)
BNUTP5E	UTP 5e	-	5,25	32,0
BNUTP5E DG*	UTP 5e doble funda	-	6,55	43,0
BNUTP5E05	UTP 5e + 2x0,50	37,7	8,90	85,8
BNUTP5E07	UTP 5e + 2x0,75	24,6	9,28	95,9

\*Doppia guaina Duraflam + PE per resistenza meccanica superiore.  
 Guaina esterna: Duraflam LSZH Blu  
 Tipo di posa: interna / esterna

Cable datasheet

In the wiring closet side the network termination has been connected to a patch panel while on the AP side the network termination has been directly connected to the device.

Surge protectors have also been installed for both the data transmission lines and the power supply units.

#### 4. FEDERATION OF THE TWO WIRELESS DOMAINS

Prior to the federation of the two wireless LAN infrastructures they were managed as two totally independent entities so users were experimenting the following problems:

- When transiting from one infrastructure to other the network sessions get lost;
- Users that are at the border of the two infrastructure experience instability of the wireless connection because their clients were flapping from one AP to another, belonging to two different domains;
- Mobile Wi-Fi users are prompted to login repeatedly when passing from one infrastructure to another.

Within the Smart Campus project it was necessary to ensure the mobility of authenticated Wi-Fi users inwardly the whole Research Area of Pisa. Our goals were to solve the problems mentioned above, by authenticating end users only once and allowing the mobility, indoor and outdoor, without losing network sessions when moving from one infrastructure to another.

Before the federation of the two Wi-Fi infrastructures, distinct VLAN IDs and IP address space were used, so it was evident that active TCP and UDP sessions were interrupted during the mobility even if connected to the same SSID. When passing from one infrastructure to another, end users were supposed to disconnect and reconnect to the Wi-Fi infrastructure to start a new network sessions.

Being based on users' feedback and our evaluation, we focused on the following goals:

- Users need to authenticate only once to access the network using a federated wireless account;
- Users should be able to move within the network coverage of both infrastructures without losing connectivity and sessions;
- The same SSIDs and authentication mechanisms, on a single address space, should be present on both infrastructures to guarantee the mobility of the users.

For this reason it was necessary to find a way to manage both Wi-Fi infrastructures as a unique federated Wi-Fi network using the existing equipment. The two institutes, IIT and ISTI, agreed to reconfigure the devices as follows:

- The same SSID has been defined on both infrastructures with the same authentication mechanism;
- Every SSID have been be mapped on the same VLAN ID (e.g. for SSID EDUROAM [5], both infrastructures are configured to use VLAN ID 48) using the same IP address space (146.48.48.0/21).

EDUROAM is a federated Wi-Fi network with 802.1x [6] authentication mechanism. For this network, the above configuration is enough to unify the two domains. Tests has been done to check functionality.

Guest users, who do not have EDUROAM account, can use a Web-based authentication mechanism. When a client tries to access a Wi-Fi guest network, a login authentication page is prompted.

Since the two wireless infrastructures managed by IIT and ISTI were completely separate, end-users were supposed to have separate Wi-Fi accounts to be used depending on the selected network.

This problem has been solved by federating the Wi-Fi domains in the following way:

- Open SSID “wifi-guest” has been defined;
- A new VLAN ID 900 has been defined for the “wifi-guest” network;
- A MikroTik RouterOS [7] has been installed for authentication before accessing the public network. This device acts as DHCP server, captive portal and access control for all Wi-Fi guest users.

The overall functionalities of the solution is as follows; when a guest user selects the SSID “wifi-guest”, being an open network, access is granted to the user and public IP address will also be assigned by the DHCP server, while external connectivity remains blocked by the MikroTik captive portal. As soon as the user try to browse, the captive portal will redirect the client to an authentication page. After providing a valid credentials, full access to external network is granted.

Guests can define a login account autonomously by providing a mobile phone number on a registration form. Credentials are delivered immediately using an SMS gateway. This is a way to keep track of users' identity in compliance with the GARR regulation [8].



## **5. FINAL REMARK**

The Smart Campus needs have been accomplished, indoor and outdoor mobility is now possible using the existing wireless infrastructures. The federation of wireless networks have been implemented using both 802.1x and Captive Portal authentications. The Wi-Fi access of the Research Area of Pisa has been simplified and users access the network using a single login credential. The wireless coverage has been extended using existing solutions, installation of new units was only necessary in those areas not covered by the service.

It is typical to find different Wi-Fi infrastructures managed by different administrative domains.

For Smart Cities applications federating existing wireless implementations results cost effective and simplifies the usage for end users. The proposed approach is mainly based on a proper configuration of the infrastructures which needs some agreements between the administrators. This cost effective and efficient approach may be used as best practice.

## REFERENCES

- [1] "Smart Area," [Online]. Available: <http://www.smart-applications.area.pi.cnr.it/>.
- [2] A. Gebrehiwot and A. De Vita, "Accesso Wi-Fi federato dell'Area della Ricerca di Pisa, WiFi@PiCNR," IIT TR-01/2011, Pisa, Italy, 2011.
- [3] "Cisco 5508 Wireless Controller," [Online]. Available: <http://www.cisco.com/c/en/us/products/wireless/5508-wireless-controller/index.html>.
- [4] "Colubris Networks," [Online]. Available: <http://www.connect802.com/colubris.htm>.
- [5] "eduroam," [Online]. Available: <https://www.eduroam.org/>.
- [6] "802.1X - Port Based Network Access Control," [Online]. Available: <http://www.ieee802.org/1/pages/802.1x.html>.
- [7] "MikroTik RouterOS," [Online]. Available: [http://download2.mikrotik.com/what\\_is\\_routeros.pdf](http://download2.mikrotik.com/what_is_routeros.pdf).
- [8] "GARR Acceptable Use Policy," [Online]. Available: <http://www.garr.it/utenti/regole-di-accesso/acceptable-use-policy-aup>.