

# Urbino Wireless Campus: A Wide-Area University Wireless Network to Bridge Digital Divide

Alessandro Bogliolo  
Information Science and Technology Institute  
University of Urbino  
Urbino, Italy 61029  
Email: [alessandro.bogliolo@uniurb.it](mailto:alessandro.bogliolo@uniurb.it)  
URL: [www.wireless-campus.it](http://www.wireless-campus.it)

**Abstract**—Urbino Wireless Campus (UWiC) is an open wireless access network promoted and implemented by the University of Urbino, in Italy, to virtually extend the University campus over the Montefeltro region, while providing also a significant contribution to bridge the digital divide and promote the widespread diffusion of online services and applications.

UWiC has ranked first among the 82 wireless-campus projects submitted by all Italian universities to the Department of Innovation and Technology of Prime Minister's Office. The project was launched one year ago and most of its targets have already been met.

This paper presents the project, discusses its technical, organizational, and economic aspects, and presents early results.

## I. INTRODUCTION

Wireless broadband network technologies [1], [2] are increasingly used to address digital divide issues, since they offer a viable low-cost alternative to wired technologies both to realize network backbones and to provide last-mile connectivity. The main competitive advantages of wireless technologies are the very low installation costs, the very low intrusiveness, the wide coverage area of each antenna and the inherent capability of supporting ubiquitous/mobile networking. Such features make wireless technologies the natural choice to address digital-divide issues in a region like Montefeltro, in central Italy, which is mostly made of historical towns (Urbino, the capital of Montefeltro, is a Unesco world-heritage site) defended by their hills.

The creation of broadband infrastructures is a priority for most governments, which solicit Internet providers to extend their coverage areas, and local administrations to create network infrastructures to be made available to service providers.

In spite of the well-understood urgency of widespread broadband connectivity, digital divide is still an open issue in Italy as in many European countries. In the Province of Pesaro-Urbino, shown in Figure 1, only the 56% of the municipalities are reached by broadband infrastructures which provide connectivity services only in the most densely populated quarters. The remaining 44% of the municipalities have no broadband connectivity at all. The persistence of this situation in an open market of network connectivity demonstrates that the market law is not able by itself to bridge the gap without public intervention.



Fig. 1: Map of the Pesaro-Urbino Province, ancient land of Montefeltro.

Regional and local administrations are investing in two main directions: the creation of networks to be used for public administration and public protection applications; the creation of local infrastructures to be made available to Internet providers to make it more convenient for them to serve low-populated regions [3], [4], [5], [6].

Universities have the potential for playing an important role in this scenario for many reasons. First, they are traditionally served by broadband connectivity (needless to mention, Internet was originally devoted to academic research). Second, they usually provide wireless connectivity and online services to their students [7], [8]. Third, they are devoted to address challenging issues that can provide direct benefits to population.

The University of Urbino has additional peculiarities which make it particularly suitable to help bridging the digital divide: it is a quite big university with about 20,000 students in a relatively small town with 16,000 citizens; it is located in most of the historical buildings of Urbino; it is the only university in the Pesaro-Urbino Province; it has a very strong relationship with its territory, strengthened during 500 years of history.

All these reasons are behind the vision of an historical land, Montefeltro, infrastructured as a huge university campus.

Urbino Wireless Campus (UWiC) is a project of the University of Urbino, co-financed by the Italian Prime Minister's Office and supported by many partners, aimed at promoting the creation of a region-wide wireless campus with two main purposes: First, making university services (distance learning, registrar's office, electronic libraries, internet browsing, computational resources, ...) available to students from the entire Montefeltro region, thus fulfilling the vision of a region-wide campus; Second, creating a shared infrastructure providing wireless connectivity to citizens and visitors as well.

This paper presents the UWiC project, discusses the policy constraints and the boundary conditions, outlines the technological, organizational and economic aspects of the solutions adopted, and presents preliminary results.

## II. THE UWIC PROJECT

UWiC aims at exploiting wireless networking to meet numerous goals: *i*) providing ubiquitous access to the online services offered to students, *ii*) fully realizing the idea of a city-campus with which Urbino has always identified, *iii*) extending the campus over the Montefeltro region, *iv*) enhancing online services and distance-learning programs to meet the needs of working students, *v*) helping bridge the digital divide in inland communities, *vi*) working with local government and public and private bodies and associations to offer communication and information services to residents and tourists.

Starting from the need for updating the online services and the wireless connectivity provided to its students, the University of Urbino realized that it was possible, with the same budget, to deploy a shared access network able not only to meet the institutional needs of the University, but also to provide a significant seed of a wide-area public access network.

To facilitate the sprouting of the seed, the University developed a network integration model that made it possible to put together at low marginal cost all the initiatives independently carried out by local municipalities, mountain districts and regional administrations. The opportunity of sharing network infrastructures and online services attracted numerous partners. Moreover, the opportunity of making directly available through the access network all the online services of a real university campus was perceived as a decisive added value by most local administrations.

One of the distinguishing features of UWiC is the deployment of a wireless access network that is not a passive bridge to the Internet, but a network rich of services and contents by itself. There are three main kinds of services in UWiC: open access information services made accessible to everybody without authentication, free personal communication services (e.g., VoIP) made accessible to everybody upon authentication, university services made accessible to the students. In addition, the integration model makes it possible for the partners to deliver their own services and to implement their own access

policies. Finally, the wireless infrastructure can be used by internet providers to offer broadband connectivity to residential users.

## III. BOUNDARY CONDITIONS

Since its first design stages, the project has been heavily influenced by three types of boundary conditions: the initiative of the Italian government aimed at promoting the enhancement of wireless networks within university campuses; the limited market of broadband access in low-populated areas; and the tight policy constraints imposed to internet providers to avoid internet abuses and preserve civil rights.

The call for wireless campus projects issued by the Department of Innovation and Technology of the Italian Prime Minister's Office stimulated the initiative of the University of Urbino and worked as an accelerator for the decision process by imposing a hard deadline to the submission of a fully-fledged proposal. The first place ranking achieved by UWiC among the 82 Italian university projects deserved the highest public contribution and made it easier for the university of Urbino to find public and private partners and supporters.

The stalemate of the market is mainly caused by the lack of the conditions needed to close the positive feedback between network users and online services: Local institutions are not motivated to deliver online services because of the lack of a critical mass of potential users, while the population is not motivated to gain access to the network because of the lack of a critical mass of online services. A university network has the potential for closing the positive feedback loop since it has both a large number of network users (i.e., students) and a wide range of online services the users are interested in (online courses, data bases, online libraries, computational resources, ...). UWiC overcomes market stalemate by creating a wide-area wireless access network that retains all the positive features of a university network.

Internet providers are bound between conflicting policy constraints. On one hand, they need to provide technical support to the detection and prosecution of crimes by storing internet transaction data. On the other hand, they need to protect users' privacy by guaranteeing the secrecy of users' data and transaction contents. Italy has adopted the EU Directive on privacy (2002/58/EC) and imposed data retention by the Legislation of July 2005 on anti-terrorism measures. Furthermore, in march 2006 the European Union has formally adopted a Directive on telecommunication data retention (2006/24/EC). The fulfillment of data retention and data protection requirements imposes to internet providers to identify internet users, to track internet transactions, to securely store transaction data, and to guarantee the secrecy of transaction contents. Such compelling obligations make it difficult to manage a free-access wireless network covering a wide geographic area.

## IV. ORGANIZATIONAL AND ECONOMIC ASPECTS

The key organizational elements of UWiC are the leadership of the University of Urbino and the openness of the initiative. The university took the lead of the project because of its

institutional role and technical capabilities and because of the "university campus" connotation granted to the wireless network since its conception. This unquestioned leadership resulted in a strategic advantage not only to speed up technical decisions, but also to encourage the participation of many partners in the project. In fact, it is generally much easier for public and private organizations to get involved individually in a university project rather than to form a joint venture with many different partners. To facilitate this aggregation process the University developed a minimum-effort network integration model and promoted the collaboration of anyone interested in expanding the network and/or providing new services. According to this model, in a few months the University has become the center of a star-structured network of tens of partners (including the provincial government, the regional students' right organization, many municipalities, mountain districts, public healthcare organizations, local service companies, bank foundations, ...) which share the vision of UWIC and bring their own contribution to the project while also taking advantage of it.

From the economic stand point, the development of UWIC is made possible by the synergy among the partners, by the cost-effectiveness of the university lab (called *UWiC lab*) where technical solutions are developed and tested, and by the inherent capability of the project to attract interest and fundings thanks to its innovative nature and social utility. The sustainability model is mainly based on the possibility of sharing the same network infrastructure to deliver both institutional and private services: Management expenses can be covered by leasing part of the bandwidth to wireless Internet service providers (WISPs).

## V. TECHNICAL SOLUTIONS

### A. Network architecture

The network architecture of UWIC is shown in Figure 2.b and contrasted with that of a conventional university network, shown in Figure 2.a.

In a conventional campus (Figure 2.a) wireless access points are connected directly to the university Intranet, which provides access to local services and to the Internet (represented as a globe connected to the intranet through a firewall). In order to gain wireless access, users must be registered with the university and go through the authentication process. Hotspots are inaccessible to those who do not have an account with the university. The authentication process is represented in the figure by a small rhombus which lies between the hotspot and the user's PC.

In UWIC (Figure 2.b) hotspots are not connected directly to the university Intranet. Rather, they are connected to an independent wireless access network (the white rectangle denoted by UWIC in the figure) which is connected to the university Intranet through a gateway. Since the access network does not expose critical data or services, and it is not part of the Internet, policy constraints can be significantly relaxed, making it possible to provide free and unconditional access to information and communication services delivered directly

within the access network. Authentication (represented by the small rhombus) is required only to pass through the gateway to enter the university Intranet and possibly go on the Internet.

The wireless access network is extended by many other white regions that represent partner networks seamlessly connected to UWIC thanks to a common network integration model. Boundaries among partner networks are transparent to the users, granting ubiquitous access to the wireless campus. It is worth noting that peripheral wireless networks can be used also to access third party services and Intranets, according to specific authentication procedures and authorization policies autonomously managed by their owners.

### B. Wireless access network

The wireless access network consists of several elements: the backbone, the distribution network, the hotspots and the inter-network links.

The core of the backbone is a ring of P-P *Hiperlan/2 bridges* connecting strategic points on top of the hills around Urbino [2]. The ring supports BGP routing and it is redundantly connected to the UWIC server farm and to the University gateway.

The wireless distribution network is composed of *Hiperlan/2 P-MP base stations* directly connected to the backbone. Residential users can connect to the base stations by means of *Hiperlan/2 CPEs*.

Hotspots are free *WiFi* access points placed in most public places to provide ubiquitous, nomadic access to the wireless campus [9]. Each external hotspot is connected to a *Hiperlan/2 CPE* associated with a base station. In addition, a *virtual LAN* (VLAN) propagates inside the university network to make it possible to connect indoor UWIC hotspots directly to specific network plugs available inside all the university buildings.

Finally, connections between the UWIC backbone and partner networks are heterogeneous in nature. They can be radio bridges, cabled links, or even simple VPN tunnels across the public Internet. The reachability of UWIC services is guaranteed in any case by the routing policies.

### C. Services

The services offered through UWIC can be divided into three main categories: *open anonymous services*, *open authenticated services*, which have no access restrictions but require user identification, and *reserved services*, which can be accessed only upon authentication and authorization.

Information services within the wireless campus fall into the category of open anonymous services. They are provided through the UWIC portal, which contains original information and free services provided by the University of Urbino and its partners specifically for wireless campus users. In addition, the portal contains copies of external websites reproduced internally to make them freely accessible in accordance with current guidelines. By law, surfing the Internet outside UWIC is not allowed without user identification. Unidentified users will be redirected to the UWIC portal when they attempt to access external sites.

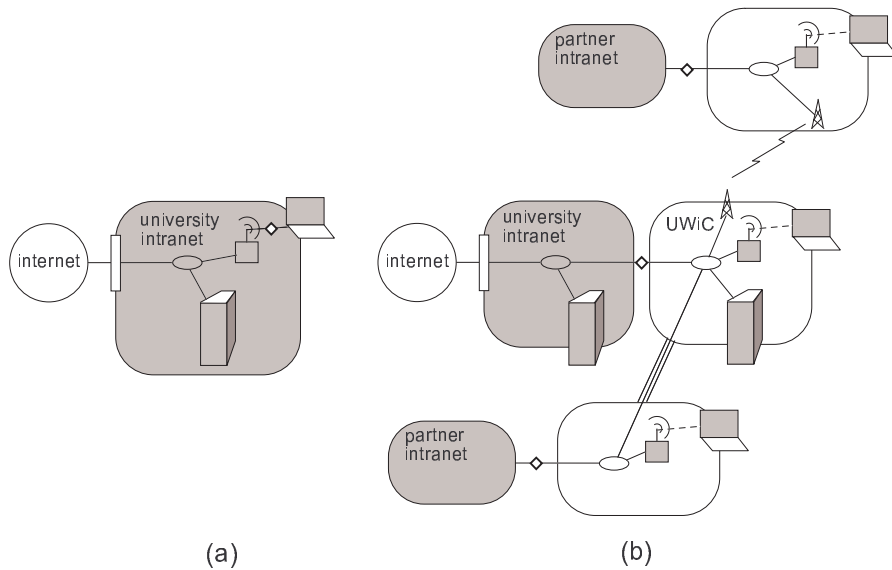


Fig. 2: Network architecture.

Communication services in UWiC fall within the category of open authenticated services, in that they are freely available to everybody but they require user identification since data retention policies also apply within wide-area private networks. Communication services include chat, blog, forum and voice over IP (VoIP). Time-limited web browsing, that will be provided for free to all UWiC users upon authentication, falls into this category as well.

The third category (i.e., reserved services) includes access to University resources (reserved to students, university faculties, employees and visitors), unrestricted access to the Internet, and access to services provided by UWiC partners for particular user groups (e.g., employees or customers of partner organizations).

#### D. Identity management

The network architecture described so far raises challenging identity management issues in order to grant access to free communication services that require authentication while reducing *password fatigue* [10] for users who can access multiple services.

The architecture of the identity management system is shown in Figure 3, where a dashed horizontal line denotes the boundary between the University intranet and UWiC. Credentials for regular students and University staff members are automatically created based on the information contained in the authoritative data bases managed by the Registrar's office and by the Human resource office, respectively. A direct ID provisioning procedure allows university Institutes and Departments to grant credentials directly to their own guests and visitors. A similar procedure allows the organizers of academic events (seminars, conferences, ...) to grant IDs to participants. All the University IDs are contained in a central data base, denoted by IDMS-Univ in Figure 3, which exposes

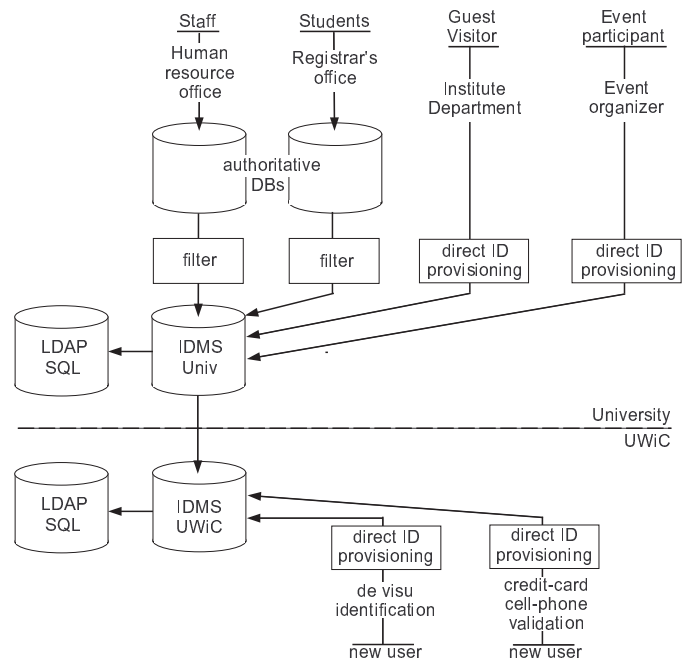


Fig. 3: Identity management system.

both LDAP and SQL interfaces for authentication purposes.

University users are also users of the wireless campus. To allow each user to use the same password to access all services, credentials propagate from IDMS-Univ to IDMS-UWiC, which is the data base that contains the IDs to be used in UWiC to gain access of the free services that require authentication.

Credentials for external users (cityzens, tourists, ...) are created directly in IDMS-UWiC by means of a distributed ID

provisioning system. The main challenge here is to guarantee the identity of new users without imposing them the burden of going to a central office to be identified. A web based interface has been developed to this purpose that makes ID provisioning procedures accessible from everywhere in the wireless campus. Three forms of personal identification are supported: *de visu* identification performed by the employees of the points of presence, *de visu* identification performed by authenticated users acting as guarantors for new users, indirect identification performed by validating credit-card or cell-phone numbers belonging to the new users. Both the usability and the legal soundness of all these forms of ID provisioning are still under test.

### E. Implementation

The implementation of UWIC is mainly based on open standards and open-source software. Proprietary solutions and appliances are used only when needed to enhance performance or provide non-conventional services.

The wireless access network is implemented using *Townet*<sup>1</sup> Hiperlan equipments, which guarantee full compatibility with current standards and security extensions certified by the *WiFi Alliance*. In addition, *Townet* Hiperlan equipments implement a proprietary protocol, called *Xplode*, which enhances radio channel performance and enables advanced monitoring features.

The UWIC server farm is made up of virtual *Linux* machines running on top of a *VMWare* cluster. Virtualization is used in UWIC for scalability, load balancing and maintainability purposes. The identity management system is based on *OpenLDAP* and *MySQL*, while *FreeRadius* is used for authentication and authorization. The UWIC portal and all web-based services are implemented in *PHP* and *MySQL* and published on *Apache* HTTP servers. Gateway and firewall functionalities are implemented using *Linux NetFilter*. The VoIP system is based on *Asterisk*.

Connections between UWIC and its partner networks are created by means of *Linux* VPNs.

Two main techniques are used to guarantee secure access from UWIC to reserved services and private networks: client provisioned *virtual private networks* (VPNs) and *point-to-point over ethernet* (PPPoE). Client provisioned VPNs create a virtual tunnel between the user's PC and the gateway of the private network the user wants to access. Communication security is guaranteed by packet encapsulation and encryption, independently of the nature of the underlying infrastructure. This makes VPNs particularly suitable for granting access to reserved services from open hotspots or from third party access networks that are not directly managed by the University. PPPoE, on the contrary, is mainly used by residential users who are connected directly to the encrypted backbone by means of Hiperlan CPEs.

The VPN concentrator granting access to the university Intranet is a Cisco IPSEC appliance. The use of a dedicated



Fig. 4: The historical town of Urbino viewed from a public park which is covered by UWIC.

appliance is motivated in this case by scalability and performance requirements. On the other hand, the open standard supported by the appliance makes it possible for the users to use their preferred IPSEC VPN clients.

## VI. PRELIMINARY RESULTS AND CONCLUSION

The UWIC proposal was submitted to the Italian Prime Minister's Office in March 2006. In June of the same year the University set up the UWIC lab and started the project. The project was split into five parallel tasks focusing on: wireless infrastructure, network configuration and management, network services, identity management, and inter-networking. Dependences among the tasks were analyzed and minimum synchronization requirements were imposed. The basic technical solutions were developed and tested within the UWIC lab in a few months by making use of *pre-alpha* prototypes in order to address practical issues and to assess feasibility, reliability and scalability.

In September 2006, the *pre-alpha* prototypes were integrated to give rise to the *alpha* version of the wireless campus, which was officially presented before actually realizing the Hiperlan backbone. The wireless access network was emulated by the HotSpots connected to the UWIC VLAN propagated within the university network, while the server farm was composed of *Linux* PCs and a geographic connection was established between Urbino and Pesaro to demonstrate the integration of third-party networks.

The *beta* version of the wireless campus, implementing all the technical solutions described in this paper, has been released in January 2007. The Hiperlan/2 umbrella covers the entire city of Urbino, while WiFi hotspots grant free access from the main public places (see Figure 4 for an example) and from the university buildings. Free information and communication services are provided within the campus, while more than 20,000 accounts have been created to establish VPN tunnels from UWIC to the university intranet and to the Internet. Peripheral wireless access networks have been

<sup>1</sup><http://www.townet.it/>

implemented in Fano and Pesaro, and integrated in UWic by means of dedicated channels.

The *gold* version of the wireless campus has been released in June 2007. The gold version provides a stable starting point for extending the access network to the entire Montefeltro region and for developing advanced services in cooperation with public and private partners.

#### REFERENCES

- [1] J. G. Andrews, A. Ghosh, and R. Muhamed, *Fundamentals of WiMAX: Understanding Broadband Wireless Networking*, ser. Communications Engineering and Emerging Technologies Series. Prentice Hall, 2007.
- [2] A. Doufexi, S. Armour, M. Butler, A. Nix, D. Bull, J. McGeehan, and P. Karlsson, "A comparison of the hiperlan/2 and ieee 802.11a wireless lan standards," *IEEE Communication Magazine*, vol. 40, no. 5, pp. 172–180, 2002.
- [3] W. Lehr, M. Sirbu, and S. E. Gillett, "Municipal wireless broadband: Policy and business implications of emerging access technologies," MIT, Tech. Rep., 2004.
- [4] I. Fodil and G. Pujolle, "Roaming and service management in public wireless networks using an innovative policy management architecture," *Int'l Journal of Network Management*, vol. 15, pp. 103–121, 2005.
- [5] S. E. Gillett, "Municipal wireless broadband: Hype or harbinger?" *Southern California Law Review*, vol. 79, pp. 561–594, 2006.
- [6] R. D. J. Kramer, A. Lopez, and A. Koonen, "Municipal broadband access networks in the netherlands - three successful cases, and how new europe may benefit," in *Proc. of AccessNets-06*, 2006.
- [7] D. Schwab and R. Bunt, "Characterizing the use of a campus wireless network," in *Proc. of InfoCom-04*, 2004.
- [8] D. Kotz and K. Essien, "Analysis of a campus-wide wireless network," in *Proc. of MOBICOM-02*, 2002, pp. 107–118.
- [9] A. Balachandran, G. M. Voelker, and P. Bahl, "Wireless hotspots: Current challenges and future directions," *Mobile Networks and Applications*, vol. 10, pp. 265–274, 2005.
- [10] A. Josang and S. Pope, "User-centric identity management," in *Proc. of AusCERT-05*, 2005.