A Wireless LAN Bridging Solution Based on Campus Network

LIU Hang, MAO Yu-ming
(School of Communication and Information Engineering, UESTC Chengdu 610054 China)

Abstract This paper presents a creative wireless LAN (WLAN) bridging solution, concentrating on the overall realization of a well designed interconnection. This solution integrates effective traffic insulation, intended access control, and required address translation without interfering with the vested interest of internet service provider (ISP). The specific solution can be widely applied on the campus-dorm (off campus)-ISP internetworking mode, where it is hard to implement wired link between campus network and dorm network in terms of cost and existing environmental constraints.

Key words WLAN bridging; wireless link; traffic insulation; access control; address translation

With the increasing development and deployment of wide area network and local campus network, a general situation is widely observed: Universities or colleges implement their own campus networks, and these campus networks share educational and research resources by accessing a nationwide network specialized for education sector, such as China Education and Research Network (CERNET). For student dorms that are usually located some distance away from campus network, the dorms network accesses Internet via service provided by ISP. That is to say, dorm students still have to subscribe to the service provided by ISP even if they only intend to access campus network. Eventually, three chief problems emerge:

1) Dorms students share campus resources most frequently, but they have to pay for accessing the campus network in that the access is via the service provided by ISP.

2) Accessing campus network from public network would confront limitations. Dorms students are unable to utilize all available resources and services on campus network since dorms network is not a subnet of campus network.

3) The fundamental change of the current widespread interconnection would undoubtedly impair the vested interest of ISP and is therefore infeasible.

To solve the problems we mentioned, considering the real environmental constraints for implementing wired link, a WLAN bridging solution is thus proposed.

1 Solution Generality

General Model

The general solution model is shown in Fig.1. This solution establishes a wireless link (based on WLAN bridging system) between campus network and dorm networks, and a router is deployed at the boundary of dorms network. Five intended access paths controls are listed below:

1) Communications are available between campus network and dorm networks via wireless link.

2) Communications are available between dorm networks and ISP.

3) Communications are prohibited between campus network and ISP via wireless link.

4) Communications are prohibited between campus network and dorm networks via ISP.

5) Communications are prohibited between dorm networks and ISP via campus network.

Problems to be Considered

The realization of the proposed solution involves...
several problems. The following issues require us to implement effective and flexible strategies to make the solution well operate.

Wireless Link
The wireless link is established by using WLAN bridging system, therefore a wide range of WLAN standards from IEEE802.11b, to high-speed IEEE802.11a or IEEE802.11g are within option\(^1\). This wireless link is managed and maintained by the university or college that establishes it.

Traffic Insulation
To make possible the five intended access path controls, the boundary router of dorm networks (See Fig.1) functions as a traffic insulator. In performing the vital task of traffic insulation, the router processes incoming packets, then makes decision on valid routing and intended blocking.

Access Control
Because the dorm students are the only authorized users accessing campus network via wireless link, and due to intrinsic vulnerability of wireless access in some aspects, access control is an important issue especially on the campus side. Authentication strategies that can be applied in the solution include RADIUS-based 802.1X, and more powerful scheme point-to-point over Ethernet (PPPoE).

Address Translation
The realization of the solution presents that, on the one hand, dorm networks is a part of public network connecting ISP, on the other hand, it becomes a subnet of campus network via wireless link. Therefore, it is a must to perform address translation procedure when implement the solution. Address translation involves different optional approaches such as network address translation (NAT), port address translation (PAT) and network address port translation (NAPT).

Summary
In light of the solution and the proposals, we see the overall effectiveness in solving the three chief problems provided at the beginning. More importantly, we achieve this without interfering the vested interest of ISP. In the rest part of the paper, an application of this solution with detailed analysis is provided.

2 Solution Realization at UESTC
The student dorms of University of Electronic Science and Technology of China (UESTC), which hold 8000 students, are located about half a kilometer away from the main campus. The dorm network subscribes to the service provided by ISP for Internet accessing. And over 70% students are frequent clients of the service. The three chief problems previously provided are confronted in the case.

2.1 Wireless Link
Wireless bridges linking dorms and the main campus directly is a feasible approach. Firstly, the wired networks and interfaces are already well fixed on both sides. Secondly, line-of-sight between the two sides is about 600 m, and there is no obstacle or radio station between both sides or around. At last, there already exists plentiful of network resources, access interfaces and WLAN management capability on both sides.

The wireless system applies to 802.11b (11Mbps), so that it can be compatible with the current 802.11b-compliant WLAN in the main campus. (Suppose 1 000 users access the campus network via this wireless link simultaneously, each user can approximately have an access speed of only 11 Kbps). They can also be dual-frequency devices as alternatives so that it will be flexible to be upgraded 802.11a or 802.11g with a maximum transmission speed of 54Mbps.
2.2 Traffic Insulation

The purpose of this solution is to enable only dorm students (legitimate users) to access the campus network cost-freely and with high speed. Each legitimate user should be allocated unique username and password in order to ensure that accessing campus network via wireless link is unavailable to unauthorized users.

R1 has the essential responsibility to discriminate packets from the dorm network and to secure routing packets correctly, which means, if the destination address of a packet from the dorm network belongs to the campus network, R1 routes it to the wireless link, otherwise to Internet via ISP. For the packets from campus via the wireless link to R1, they should only have the destination addresses of the dorm network. In other words, accessing Internet from campus through this particular wireless link is prohibited. Furthermore, R1 should also be capable of deterring packets from ISP in going through the wireless link.

In conclusion, the wireless link we proposed actually offers a proprietary route that is affordable with a high bandwidth between the main campus and dorms exclusively. R1 takes the important position of effective traffic insulation as shown in Fig. 3.

At the recipient, wireless bridge A functions for access control. For this specific application, data privacy can be relaxed a little, thus the traditional 64/128-bit WEP is deployed[3].

2.3 Access Control

To allow access by legitimate users exclusively is the key issue at reception. The use of 802.1X offers an effective framework for authentication and user traffic control to a protected network, as well as dynamically varying encryption keys[4].

Initial 802.1X communications begins with an unauthorized supplicant (user) attempting to connect with an authenticator (AP). AP responds by enabling a port for passing only extensible authentication protocol (EAP) packets from the user to an authentication server located on the campus network. It is not until the AP can verify the user’s identity using an authentication RADIUS server (by username and password), the AP will not allow the user to make further access. Once authenticated successfully, AP opens the user’s port for other types of traffic.

We can also implement dynamic keys exchange. The 802.1X authentication server can return session keys to AP along with the accepted message. The AP uses the session keys to build, sign and encrypt an EAP key message. Then the key message is sent to the user immediately after sending the “success” message. The user can use the contents of the key message to define applicable encryption keys. In typical 802.1X implementations, the user can dynamically change encryption keys as often as necessary. This access control strategy can also be applied to authenticate users via outdoor APs around the dorms.

2.4 Address Translation

All the IP addresses of campus network are allocated global addresses, and the overall network consists of many sub-networks varying in scale. With regard to the bridging solution, the dorms network is actually a subnet at a remote site connected with a wireless link to the backbone campus network. On the other side, the dorms network is also a subnet of Internet with local addresses kept unaltered. In order to secure the dorms network a real subnet of the campus network both physically and logically, in parallel to other subnets on campus, the essential procedure of address translation is hence required. The translation between global addresses and local addresses usually applies to connect private network with Internet, and it is done on the boundary router connecting them (See Fig. 4)[5].

Considering the large number of addresses to be translated in the dorms network, here a combined approach NAPT is used. That is, all the local addresses are going to be translated into a limited number of global addresses with each global address combined with different port addresses. On the opposite direction, the combined global addresses are translated back into the original local addresses correspondingly. This approach enables each user to be uniquely identified.
both in the dorms network and the campus network. This translation procedure between the dorms network and the campus network can achieve efficiency without requiring an overall network resetting.

3 Conclusions

A general model for a wireless LAN bridging solution is firstly proposed, and then we are targeting a specific implementation at UESTC. Since there are many campuses with circumstances resemble that described in this paper, this solution is beneficial in practice and is preferred for the following reasons.

1) Establishment of a proprietary high-quality wireless link makes extended cost-free campus resources sharing available, and it is manageable because this wireless link is built and maintained in-house.

2) The solution provides effective traffic insulation in realizing the five intended access paths control.

3) Reliable and flexible authentication mechanism is attained in the solution to secure rigid access control requirement.

4) The dorms network is adopted as a subnet of the campus network without interfering the vested interest of ISP, thus the solution is highly applicable.

5) Implementation of this solution does not need large-scale rewiring and brings no damage on the current network, and it well balances the effectiveness, cost, and the maximum compatibility in long-term.

References


Brief Introduction to Author(s)

LIU Hang (刘航) was born in Sichuan Province, China, 1983. He is now pursuing B.S. degree of Network Engineering in UESTC.

MAO Yu-ming (毛玉明) was born in 1956. He received M.S. degree from Chengdu Institute of Radio Electronic Engineering in 1984. He is currently a professor and department head of network engineering in School of Communication and Information Engineering, UESTC. His research interests include computer communications, internetworking, network architecture and protocols.