Implementation of Campus-wide Wireless Network Services using ATM, Virtual LANs, and Wireless Basestations

John W Lockwood

National Center for Supercomputing Applications (NCSA)

and Department of Electrical and Computer Engineering,

University of Illinois at Urbana-Champaign

405 North Mathews Ave

Urbana, IL 61801

***Abstract-*A campus-wide wireless LAN has been implemented that combines the scalability of virtual LANs and the flexibility of switched Ethernet with the mobility of wireless LAN access. A suite of general-purpose software tools has been developed and deployed to monitor the status of the network, measure the bandwidth utilization, control access to the network, and authenticate users.**

I INTRODUCTION

The wireless network deployed at the National Center for Supercomputing Applications (NCSA) provides untethered access for mobile users scattered throughout the offices and buildings of the Urbana-Champaign campus. This network currently provides the packetized IP services for laptop and palmtop computers, which allow users to browse the web, access email, and share files. The general topology of this network is shown in Figure 1.

II CAMPUS WIRELESS LAN IMPLEMENTATION

The implementation of the NCSA wireless network is unique in the way that it combines the features of several commercially-available hardware technologies along with custom-developed software management and control software.

A Backbone Network

At the core of the network are a collection of high-speed Asynchronous Transfer Mode (ATM) switches that collectively form the backbone. Fiber-optic OC-3c links are used to interconnect major buildings on the campus, each at a rate of 155 Mbps.

Logically, Virtual LANs (VLANs) are established over the backbone to interconnect LAN Emulation Clients (LECs). These LECs exist at the edge of the network and are implemented as a module within a layer-2 Ethernet switch. Each switch provides a multitude of ports, with each port receiving its own dedicated bandwidth. A diagram of the VLAN configuration is shown in Figure 2.

The combined system leverages the manageability of the switched Ethernet and the scalability of the virtual LAN. Unlike traditional Ethernet, which broadcasts packets on a shared media, the switches only forward packets to the specific endpoint for which the packet is destined. Likewise, the LAN Emulation Server (LES) of the VLAN maintains the table of Media Access Control (MAC) addresses. The VLAN clients use this table to map the MAC to an ATM address of the remote LAN Emulation Client (LEC). This ensures that packets are always forwarded along the shortest path to their destination. The Broadcast and Unknown Server (BUS) is used only to forward packets that must be delivered to all hosts.

B Wireless Access

Wireless basestations are attached to ports of the Ethernet switches. The basestations are 802.11-compatible bridges that forward packets between their wired and wireless interfaces. The basestations use frequency hopping at a center frequency of 2.4 GHz to provide 1 Mbps channels to endpoint clients.

The NCSA wireless campus network has been expanded in bandwidth by incrementally adding basestations to switched ports. In areas that have been found to be congested, new basestations have been added to partition the coverage into smaller regions. The frequency hopping operation of the wireless protocol allows a fair degree of coverage overlap without performance degradation.

III MANAGEMENT TOOLKIT

The major contibution of this work is the development of a suite of management tools for this hybrid ATM/switched Ethernet/wireless network. This suite combines new tools and existing shareware utilities into a unified framework. It presents the full status of the network by combining results of information gathered from the directly hardware devices and configuration databases.

The campus LAN management tools are implemented as a suite of Perl routines that gathers current data using the Sim-
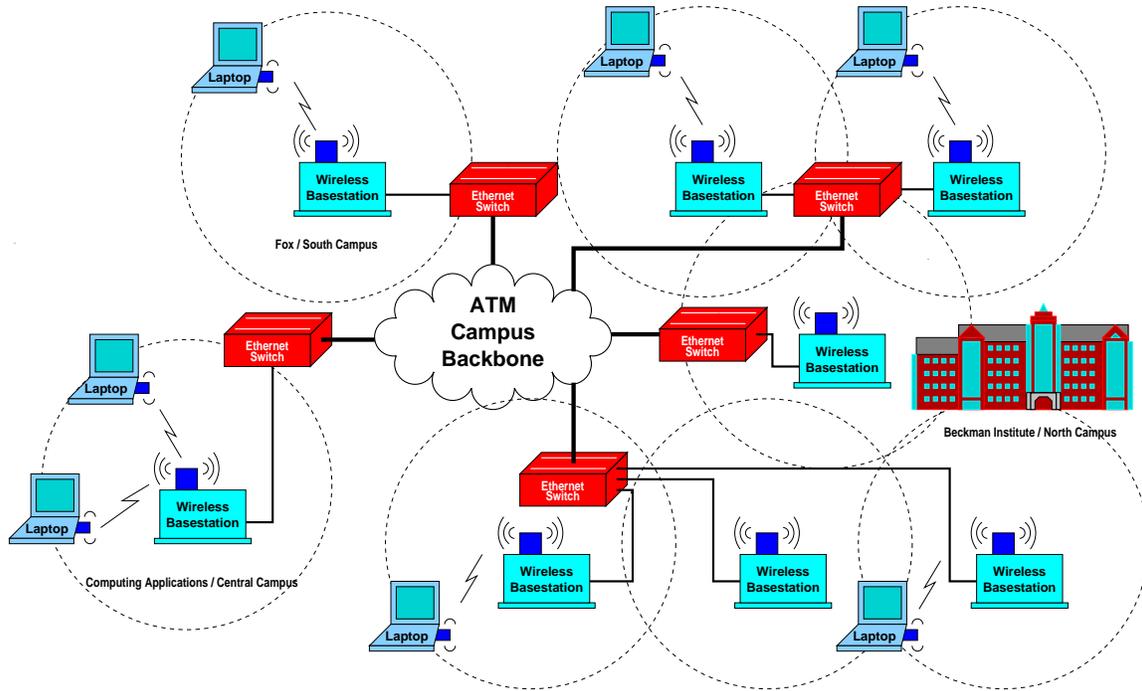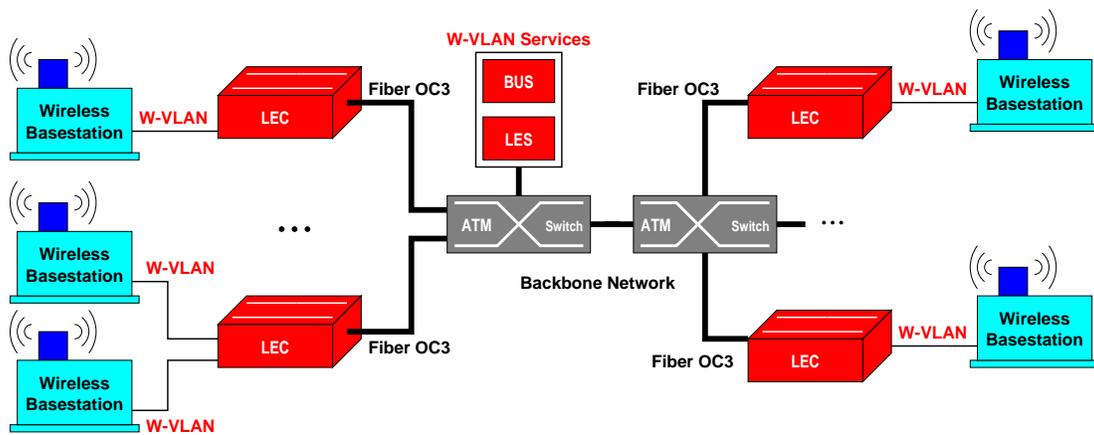
1

Figure 1: Wireless Overlay Network
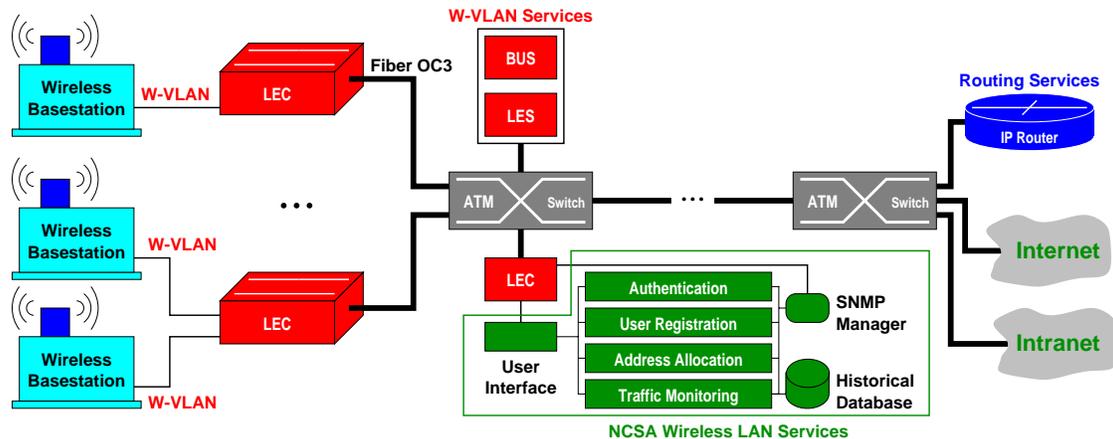

Figure 2: Spanning Wireless over the VLAN

2

Figure 3: Complete Wireless LAN Services

ple Network Mangement Protocol (SNMP) and historical data from an SQL database. They exchange data directly from the Ethernet switches and routers via SNMP. Existing shareware and freeware tools have been employed wherever possible to avoid duplication of existing functionality. A block diagram of the Wireless LAN services is shown in Figure 3.

The NetDocs user interface consists of a collection of web pages and CGI programs that collectively provide a unified interface to the network management tools. The ATM switches, Ethernet switches, and network links are represented as clickable icons on a web page graphic. Clicking on a network switch, for example, shows the users are accessing the network and their current locations. In the case of wireless users, the tables show each users' access points. Using the database records, the network addresses are reverse-mapped to determine their corresponding network names.

A Address Allocation

Access to the wireless network services is controlled by multiple mechanisms. Firstly, the wireless hardware device provides a weak degree of security by performing data-link-layer scrambling of the data. Knowledge of a randomly-generated scramble code is needed to utilize the wireless link.

Secondly, a DHCP server is used to selectively control the assignment of layer-3 Internet addresses. By maintaining a database of users, IP addresses, and MAC addresses, network access is restricted to only those machines that belong to users who have been authorized to use the network.

B Authentication and User Registration

All Internet hosts in the NCSA LAN are registered with entries in a network database. From a web browser on any existing registered host, users may register new machines or update their existing information. To secure access to this database, users must authenticate their login via their password. The Secure

Socket Layer (SSL) is used to avoid transmission of clear-text passwords.

C Traffic Monitoring

Statistics are collected by a SNMP query of the Ethernet switch. Results of the queries are stored in a database to allow historical charting. Clicking on a link on the Netdocs web page yields a graph showing the link utilization. Three plots are shown to represent the transmit and received bandwidth on the link for the past 24 hours, 7 days, and 12 months. The MRTG toolkit is used to autoscale and format these graphs.

IV CONCLUSIONS

The implementation of the NCSA wireless network has demonstrated that scalable, wireless services can be provided in a campus-wide network. The major contibution of this work has been the development of a suite of management and monitoring tools for this hybrid ATM/Switched Ethernet/wireless network. These tools provide a unified interface for monitoring, measuring, and securing access to Internet services in the campus-wide wireless network.