

# Enhancement of a WLAN-Based Internet Service in Korea

Youngkyu Choi<sup>1,\*</sup> Jeongyeup Paek<sup>2,\*</sup> Sunghyun Choi<sup>3,\*</sup>  
Go Woon Lee<sup>4,+</sup> Jae Hwan Lee<sup>5,+</sup> Hanwook Jung<sup>6,+</sup>

<sup>\*</sup>Multimedia & Wireless Networking Laboratory  
School of Electrical Engineering  
Seoul National University  
San 56-1, Shillim-dong, Kwanak-gu,  
Seoul, 151-744, KOREA  
<sup>1,2,+82-2-880-1755, <sup>3,+82-2-880-1753</sup></sup>

<sup>1</sup>ykchoi@mwnl.snu.ac.kr,  
<sup>2</sup>jypaek@mwnl.snu.ac.kr, <sup>3</sup>schoi@snu.ac.kr

<sup>\*</sup>Service Development Laboratory  
Korea Telecom  
17, Woomyeon-dong, Seocho-gu  
Seoul, 137-792, KOREA  
<sup>4,+82-2-526-6181, <sup>5,+82-2-526-6637,</sup>  
<sup>6,+82-2-526-6460</sup></sup>

<sup>4</sup>barney@kt.co.kr, <sup>5</sup>tasmea@kt.co.kr,  
<sup>6</sup>hanuk@kt.co.kr

## ABSTRACT

A wireless LAN (WLAN)-based Internet service, called *NESPOT*, of Korea Telecom (KT), the biggest telecommunication and Internet service company in Korea, has been operational since early 2002. As the numbers of subscribers and deployed access points (APs) increase, KT has been endeavoring to improve its service quality as well as the network management. In this paper, we introduce a joint effort between Seoul National University (SNU) and KT to achieve it. We have been addressing two major issues as part of the joint project thus far: (1) a unified WLAN management tool; and (2) real-time traffic support enhancement. We present our on-going efforts as well as some preliminary results. Some issues, which need further attention for the future *NESPOT* service enhancement, are also introduced.

## Categories and Subject Descriptors

C.2.3 [Network Operations]: *network management, network monitoring, public networks*

## General Terms

Management, Measurement, Performance, Experimentation, Standardization.

## Keywords

WLAN, IEEE 802.11, Wireless Internet Service Provider (WISP),

\* The work reported in this paper was financed and supported by KT. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of KT.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.  
*WMASH '03*, September 19, 2003, San Diego, California.  
Copyright 2003 ACM 1-58113-768-0/03/0009...\$5.00.

Hotspot Service.

## 1. Introduction

Since the first commercial service of Code-Division Multiple-Access (CDMA)-based digital cellular service in 1996, cell phones have become an essential part of every Korean individual's life. As of July 2003, there are over 33 millions mobile phone subscribers, which represent 68.7% of the whole Korean population. Meanwhile, during the last 5 years or so, Korea also has witnessed astonishing service deployments of the high-speed Internet access based on both Digital Subscriber Line (xDSL) and cable modem. Today, over 75% of the total households in Korea are enjoying the high-speed Internet service. Moreover, as the portable devices, such as laptop, Personal Digital Assistants (PDA), and smart phones, become more and more common, the desire to access the Internet on the roads as well as at home/office using these portable devices, at a high-speed data rate comparable with the wireline Internet access, became apparent.

To meet such a desire, Korea Telecom (KT), the largest telecommunication and Internet service company in Korea, started a Wireless Internet Service Provisioning based on IEEE 802.11b Wireless LAN (WLAN) in early 2002. This WLAN-based Internet service is called *NESPOT*. Today, there are over 260,000 subscribers and about 9000 hotspots in operation. The *NESPOT* service is targeting at two different areas: (1) for residential home users, who subscribe both high-speed Internet service (based on xDSL) and *NESPOT* (for the Internet access of their laptops/PDAs/PCs with the WLAN interface), and (2) for mobile and enterprise users, who subscribe *NESPOT* only for the Internet access in the hotspots, called the *NESPOT Zones*, and/or their office environments. As the numbers of subscribers and deployed access points (APs) increase rapidly, KT has been encountering a number of issues related to the network management/maintenance. Moreover, improving the service quality has become very desirable.

As part of such an effort, Service Development Laboratory at KT initiated a joint project with Multimedia & Wireless Networking Laboratory (MWNL) at Seoul National University (SNU). In this paper, the current progress as well as on-going efforts is

introduced. The current project is addressing two major issues: (1) a unified AP management, and (2) Quality-of-Service (QoS) improvement for real-time services, e.g., Voice over IP (VoIP).

Each AP operates according to a number of operational parameters such as the wireless channel number, IP address, security key, etc. Moreover, the APs typically monitor its operations as well as the network status, e.g., the list of the associated terminals. Accordingly, one can often diagnose the problem of a WLAN by inquiring the current status to the AP and repair some identified problems by changing the operational parameters of the AP. This kind of operations can be performed via an AP manager application, which is based on telnet, HTTP, or a vendor-specific protocol. However, KT realized that it was not desirable to have vendors supplying the APs for the NESPOT service with different managing schemes. Accordingly, we have developed a protocol, called *Dr. Nespot*, which enables all the NESPOT APs to communicate with a unified manager, called Dr. Nespot manager. Dr. Nespot is expected to handle different types of problems encountered during the AP installation time as well as a normal operation.

Currently, KT provides VoIP services for both wireline and wireless (based on NESPOT) Internet users. The voice traffic requires low end-to-end latency in order to maintain the interactive communication. Video on Demand (VoD) is also one of the future target services of KT, especially, for the residential homes. Video traffic also requires a bounded latency even though the requirement is a bit relaxed compared to the voice traffic. It is well-known that the current Internet provides the best-effort service in the sense that it does not provide any QoS (e.g., latency and throughput) required for different types of traffic and applications. It goes the same with the NESPOT service since the current WLAN does not provide any QoS.

The emerging IEEE 802.11e Medium Access Control (MAC), which is an amendment of the existing 802.11 MAC, will provide the QoS [1][7]. The standardization of the IEEE 802.11e is still on-going even if it is in the final stage [3]. Even after the standardization is finalized, it may take some time for the first 802.11e-compliant QoS-enabled WLAN equipments to become available in the market. Moreover, it may be difficult to upgrade/replace the existing APs for the QoS support even if the 802.11e-compliant devices are available. The main problem is that such an upgrade requires the existing WLAN equipment hardware to be replaced since the 802.11e MAC implementation cannot be done by just upgrading the firmware of an existing MAC chip only (provided that the MAC controller runs a microprocessor with a firmware.) Accordingly, in our project, we are working on a software-based solution for a limited QoS support to the real-time traffic. It is limited since it runs on top of the legacy MAC without QoS. However, as will be shown later, it can be quite useful to improve the real-time traffic support.

The rest of this paper is organized as follows: Section 2 briefly introduces the KT NESPOT service by highlighting such aspects as the network architecture and the service plans. Section 3 presents a unified AP management and maintenance, called Dr. Nespot, which we have developed, by describing the needs, considered scenarios, and the protocol itself. In Section 4, we present dual queue architecture to support the real-time traffic. Other issues to enhance the current WLAN services are discussed further in Section 5, and then this paper concludes with Section 6.

## 2. OVERVIEW OF KT NESPOT SERVICE

KT had begun the field trial of a wireless Internet service based on IEEE 802.11b WLAN in October 2001. APs were deployed at so called, hotspot areas, where many people get together, e.g., hotels, hospitals, universities, subway stations, express bus terminals, and coffee shops. A commercial WLAN service started in early 2002 for the first time in Korea. KT is promoting its service for not only hotspots but also residential homes. It is a natural approach since KT serves about 5 millions subscribers (as of July 2003) for the broadband wired Internet service, called Megapass, based on xDSL technology. To build and service such a large network, many complicated issues are encountered, and KT is endeavoring to address many important issues accordingly.

### 2.1 Channel Assignment Strategy

The 802.11b WLANs [6], which KT NESPOT is based on currently, operate at the 2.4 GHz unlicensed band. In Korea, the frequency band of 83.5MHz from 2.4GHz to 2.4835GHz is available. The similar band is available in the US and many European countries. 13 operating channels are available in this frequency band, where two consecutive channels are 5 MHz apart. The center frequency of channel  $n$  is  $2412 + 5(n-1)$  MHz. Each channel of the 802.11b roughly occupies a 22 MHz band; the main lobe of the transmitted signal spans 22 MHz. Accordingly, we can easily imagine that neighboring channels overlap in the frequency band. It should be noted that in the US, only 11 channels are allowed while the entire 13 channels are allowed in Korea as well as in most European countries.

Having more channels (especially, non-overlapping ones) implies a more freedom and a better network performance for multi-AP environments such as large-scale hotspots. Traditionally, cell planning technology to mitigate inter-cell interference has been researched extensively and applied to cellular systems [13]. In the 802.11 WLAN worlds, the studies for effective deployment of WLAN networks are also being discussed [14]. However, because the cell planning in WLAN must be done often in 3-dimensional space while there are few non-overlapping channels, the perfect plan eliminating interferences from other APs is regarded almost impossible. Where there are 11 channels available, e.g., in the US, it is understood that there are 3 non-overlapping channels, i.e., channels 1, 6, and 11. When there are 13 channels available, there are still only three non-overlapping channels. However, when we choose four channels, namely, 1, 5, 9, and 13, the two neighboring channels are very partially overlapped such that the interference between neighboring APs using these channels becomes not very severe.

Figure 1 (from [14] authored by KT researchers) shows the maximum throughput performance of an AP, i.e., AP1, when there exists a neighboring AP, i.e., AP2, for different channel and geographical distances between two APs. The actual performance can vary depending on the AP's transmit power level and the network topology, but the general trend should hold irrespectively. We conclude from this measurement result that having neighboring APs operating at overlapping channels result in poor throughput performance obviously. This is due to the fact that the busy status in an overlapping channel may not be sensible to the WLAN devices, which in turn prevent the 802.11 MAC based on carrier sensing from working properly. However, we observe that when two channels are 20 MHz apart (or channel gap is 4 in terms

of the channel number), e.g., channels 1 and 5, the performance loss is rather negligible. Accordingly, KT is utilizing the four partially overlapping channels, 1, 5, 9, and 13, for its hotspot areas.

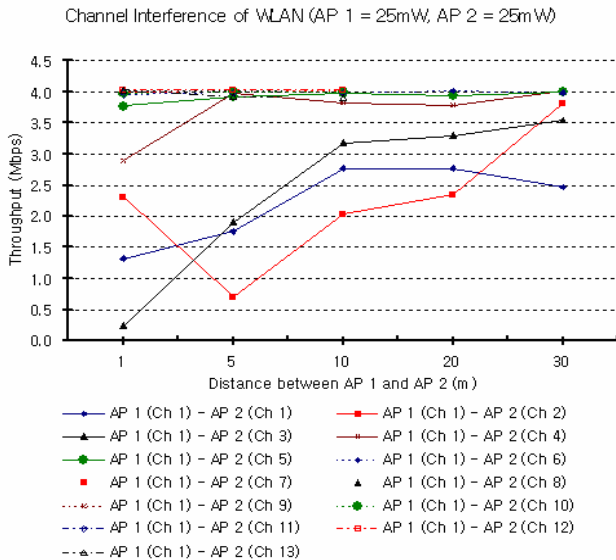


Figure 1. Results of WLAN channel interference experiment

It should be also mentioned that a different strategy for the channel assignment is needed in places where many users with the network interface cards (NICs) produced in other countries supporting only 11 channels are expected to use the NESPOT service. For example, in hotels, where many foreign travelers are expected to stay and use the service, the NESPOT zones should be configured so as not to use channels 12 and 13.

For the actual assignment of an AP's operating channel, there can be two different ways, i.e., manual and automatic configurations. In case of the manual one, a field engineer can, for example, scan all of the available channels at the AP installation time, followed by selecting a channel with the best signal quality, and deciding it as its operational channel. This method seems to be rather heuristic, but has been widely used so far. With the automatic selection, the AP first scans over the candidate channels, e.g., channels 1, 5, 9, and 13, and then selects the best one for its operating channel automatically. The criterion for selecting a channel is dependent on each vendor's specific algorithm. In this context, KT takes the auto channel configuration as one of the requirements in bench marking test (BMT), in which AP vendors participate to supply their APs to KT.

## 2.2 Different Service Plans

There are basically four different service plans as shown in Table 1 depending on the place where the user primarily uses the NESPOT service.

- NESPOT Family/Solo:** this plan is for residential home users. The users of this type of service are also the subscribers of KT's broadband Internet service, called Megapass, based on xDSL. Today, KT provides an Internet service based on different types of xDSL including VDSL (supporting up to 23 Mbps transmission rate.) By paying an

extra fee, 10,000 won ( $\approx$  8.3 US\$) per month, on top of their broadband Internet service fee, the users can enjoy both wireline and wireless Internet services with their laptops/PDAs/PCs using an AP leased from KT.

- NESPOT Biz:** this plan is for people in companies, hotels, universities, etc. One main distinction of this service plan from the others is that the subscriber is an organization, not an individual. The organization is also a subscriber of a high-speed leased-line for the Internet connection. By subscribing to the NESPOT Biz, KT installs multiple APs across the campus of the organization, the organization is supposed to pay a monthly service charge depending on the number of NESPOT service IDs, which determine the number of simultaneous NESPOT users. Depending on the service contract, the subscriber, e.g., a hotel, can also resell the NESPOT service to its customer, e.g., the guests of the hotel.
- NESPOT Pop:** the users of this service plan can access the Internet using the WLAN NIC at hotspot regions, which are called *NESPOT Zones*. The wireline connection to the NESPOT Zones can be one of xDSL, leased-line, and metro-Ethernet. For this type of service, the service charge plan can have two different forms: regular subscriber charge plan and temporary subscriber charge plan. For regular users, both fixed-rate monthly charge and usage time based charge are applicable. For temporary users, a fixed rate charge should be paid hourly or daily basis. The service time should be pre-paid by the subscriber, where the service can be purchased on-line using a credit card. It should be also noted that all other NESPOT users can enjoy the Internet access in the NESPOT Zones without an extra service charge.
- NESPOT Swing:** this is a service plan for a combined service of the wide-area CDMA network and WLAN. This introduces the combined benefits from the abundant throughput of WLAN in hotspots and the wide coverage of CDMA service. KTF, a sister company of KT, which provides a CDMA-based cellular service, and currently has the second market share in Korea, is the sole co-provider of NESPOT Swing currently. One can enjoy the Internet access using either the NESPOT in NESPOT Zones or the cellular service (currently, CDMA2000 1xEV-DO) in any other regions. Current terminals supporting NESPOT Swing basically include separate WLAN and the CDMA modules. The service charge is determined by the sum of the fee for NESPOT based on the Public NESPOT plan and the fee decided by the number of transmitted packets in 1xEV-DO.

Table 1. NESPOT service plans

Type	Location	Charging period
Family/Solo	Home	Monthly
Biz	Company, hotel, university, ...	Monthly
Pop	Hotspots	Monthly, daily, hourly
Swing	NESPOT zone & CDMA coverage	Monthly

### 2.3 Network Architecture

The architecture of the core network for the NESPOT service has mainly two different forms. For example, DSL Access Multiplier (DSLAM)/Network Access Server (NAS) are used to connect xDSL to the Internet while Channel Service Unit (CSU)/router are exploited in case of the leased line or metro-Ethernet. Two servers, namely, Dynamic Host Configuration Protocol (DHCP) and Remote Authentication Dial-In User Service (RADIUS) (for authentication, authorization, and accounting i.e., AAA) servers, make important roles in the core network of NESPOT. Network entities which comprise NESPOT network are shown in Figure 2. While all the NESPOT APs are assigned static IP address, as will be addressed later, all stations use temporary IP addresses dynamically allocated from a DHCP server after being successfully authenticated. The accounting based on each user's service plan contract is performed by the RADIUS (or AAA) server.

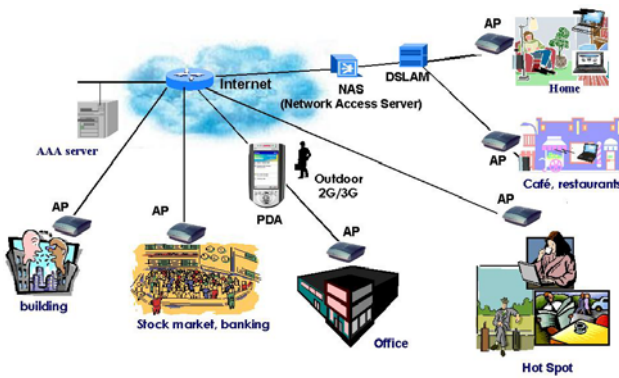


Figure 2. NESPOT network structure

For the wireless side, a NESPOT Zone is composed of a number of APs, and the total number of NESPOT Zones is about 8,700 as of July 2003. To give some sense about the size of the NESPOT Zones, Table 2 presents the statistics of the current NESPOT Zone sizes. We observe that most of the NESPOT Zones are composed of a single AP. The largest NESPOT Zone is composed of about 360 APs. The NESPOT APs have SSID set to "NESPOT," which allows a user device to search the NESPOT APs in a unified manner.

Table 2. NESPOT Zone size statistics

Number of APs	Number of NESPOT Zones
1	~ 7000
> 2	~ 2000
> 10	~ 400
> 50	~ 80
> 100	~ 25

### 2.4 Security and Authentication

The current 802.11 MAC defines a 64-bit RC4 encryption-based security mechanism, called Wired Equivalent Privacy (WEP). Many of currently available 802.11 devices also implement a de-

facto standard based on 128-bit RC4 encryption. However, it is very well known that it is possible to break the 802.11 security very easily, e.g., Fluhrer-AirSnort attack [19]. Due to a flaw in key scheduling algorithm and initialization vector (IV) in the key formation, the keys can be detected in less than 15 minutes. KT NESPOT currently does not employ any link-layer encryption mechanism, e.g., WEP, and recommends using an application-layer security mechanism, e.g., VPN, for security-sensitive data transactions. For example, in Korea, electronic financial transactions, e.g., e-banking, is very popular, and these transactions are protected via application-layer encryption mechanisms. However, a link-layer security mechanism is under consideration of implementation in NESPOT.

A secure authentication scheme is another important element for a commercial WLAN service. The authentication scheme prevents a rogue user to use the NESPOT service (using others' accounts) without paying for the service. NESPOT chose EAP (Extensible Authentication Protocol)-MD5 (Message Digest) based on IEEE 802.1x as the authentication scheme [15].

## 3. DR. NESPOT – A UNIFIED NETWORK MANAGEMENT

In this section, we present a unified NESPOT AP management and maintenance protocol, called Dr. Nespot, which was developed as part of the joint project of SNU and KT. We first describe the motivation, which led the development of Dr. Nespot.

### 3.1 Needs for Dr. Nespot

Multiple vendors or manufacturers have been supplying the APs to KT for the NESPOT service. All the APs provide all the mandatory features, which involve a number of operational parameters related to AAA, DHCP, security, etc. For most parameters, there exist default values determined by KT.

One may think that a new AP installation is so simple that there should not be any trouble. However, as the NESPOT network size grows, many different kinds of problems have been encountered. One class of problems arises due to the fact that field engineers often complete their work without evaluating the newly installed AP's performance properly. In other cases, when an AP becomes out of order, it is difficult to repair it because the installed position, e.g., ceil and wall, is often difficult to reach. Moreover, the fact that the hotspots are often crowded busy places makes a timely maintenance more difficult. Considering these situations, it is highly desired that the management operations be performed via a remote (wireless) access. Since APs supply the interfaces for administrators to get or set its current operational parameters related to (1) 802.11 MAC operation; (2) AAA; (3) wired link; and (4) statistics, operators can take care of APs by accessing through the network. These interfaces are typically built in the form of telnet, HTTP, or a vendor-specific management program. However, the fact that the interfaces of APs from different vendors have proprietary contexts as well as different appearances makes operators confused, thus resulting in ineffective management. Accordingly, the need for a unified utility to handle erroneous situations and maintenance was raised.

One may say that the Simple Network Management Protocol (SNMP)-based Network Management System (NMS), which has been extensively used in wired network management, can also be

exploited to manage a large-scale WLAN such as the NESPOT network. Apparently, KT is currently using the NMS for its network management/maintenance as well. However, the existing NMS cannot replace Dr. Nespot since many NESPOT APs, especially, those at residential homes, repeat power on-and-off. If thousands of APs repeat on-and-off, the maintenance via an existing NMS tool does not give a merit because meaningless trap messages informing up and down of an AP would just waste the precious resources. Moreover, even though an NMS-based management can give superior insights over the whole network by storing various metrics into database and transforming those to useful statistics, it has intrinsic limitations to give urgent maintenance, measure particular and temporal performance, and satisfy the customized requirement of the service provider.

### 3.2 Scenarios in Consideration

The scenarios we intend to address with the Dr. Nespot protocol can be mainly classified into three cases as follows.

First, a staff (or a server program) at a service administrative center wants to confirm that a field engineer properly installed an AP satisfying their customers. Of course, a field engineer needs to ensure that her/his installation work has been done successfully before reporting it to the administrative center. This could be executed by checking whether the terminal is (1) properly associated with the newly-installed AP, (2) successfully authenticated through the 802.1x/EAP, and (3) allocated an IP address via the DHCP server. After ensuring these essential procedures, she/he may finish the installation work by sending a group of data which contain the profile of newly-installed AP to a repository at the administrative center. Data collected in this way can be utilized in handling troubles from a customer in the future.

For the next scenario, a customer reports that the WLAN service does not operate at all via a phone call. A staff receiving the call from the customer can check the AP based on the installation profiles. If the AP of the reporting customer can be reachable remotely (e.g., via ping), at least the wireline portion of the AP can be judged to be operational. Then, one could predict that the reported trouble is resulted from either the malfunctioning of the wireless portion or from the problem of the customer's terminal. To resolve the causes of the trouble more in detail, it would be effective to remotely inquire of the information such as system log, configuration profiles of AAA and DHCP, associated stations' list of the AP, and so on. After assuring that AP does not have any misbehavior and the customer's terminal is associated with the AP, the staff may investigate the operational parameters of the customer's terminal (e.g., type of NIC, OS, memory, IP, BSSID, RSSI, channel number, transmission rate, etc.). Some abnormal values may provide important clues for resolving the WLAN's malfunction. If the customer's terminal does not have any impending misses, assuring that the AP is registered to a proper authentication server and the pair of ID/Password is valid would be the final step of the maintenance procedure. During all the above procedures, the initial profiles collected during the AP installation can be very useful.

As the final scenario, a customer complains about the QoS of the WLAN service. Metrics of QoS could be the throughput and delay at the application layer. To get practically useful data, measuring the performance in both the wired section between a remote node and the AP and the wireless section between the AP

and the user's terminal could be conducted separately. This scenario could be cooperated closely with the second scenario. For example, whenever a customer complains about a poor performance of the WLAN service, operators should confirm objectively how much performance is achieved because people sometimes feel the network performance subjectively. If considerable degradation is observed via the measurement, it is desired to investigate the internal status of the customer's AP since unexpected users may be parasitic on the AP or a lot of packets may be dropped due to a poor channel status. That is, the statistics based on the exact measurement could help KT invest restricted resources in a cost-effective way.

### 3.3 Dr. Nespot Overview

Normally, Dr. Nespot involves two network entities, namely, *Dr. Nespot manager* and *Dr. Nespot agent*. Dr. Nespot manager, a managing entity, is located in a terminal of a field engineer or an operator while Dr. Nespot agent, a managed entity, is located in each NESPOT AP. Dr. Nespot is an application-layer protocol, which exploits the UDP over IP for communication between a manager and an agent with encrypted protocol data units (PDUs) for the security protection. The TCP over IP is not adopted due to the overhead and delay involved with the connection setup and termination.

For Dr. Nespot to operate, the terminal with Dr. Nespot manager should be associated with an AP or should be connected to the wireline network, e.g., Ethernet, which constitutes the backhaul of the NESPOT network, directly via a wireline cable. This implies that the terminal can exchange data frames carrying Dr. Nespot PDUs with AP(s). We briefly overview the functions of Dr. Nespot, required to handle the scenarios discussed in Section 3.2.

#### 3.3.1 Finding Neighbor APs

This operation allows a Dr. Nespot manager to search APs in the same subnet. A PDU is sent by a manager at the broadcast address, i.e., 255.255.255.255. It is common that broadcast datagram is filtered out by routers so as not to flood the entire network. Due to this reason, the AP searching range is limited to the same sub-network. A Dr. Nespot agent which receives this request PDU transmits a response PDU at the broadcast address. The intended receiver of this response PDU is the searching manager, but the broadcast address is used since the manager and the agent may have IP addresses belonging to different subnets. That is, Dr. Nespot is designed to perform properly even if the IP addresses of the manager and/or APs were not properly configured. Note that setting a proper IP of an AP could be one of the jobs to be done with Dr. Nespot. The response PDU can contain the additional information about responding AP, e.g., IP, WLAN parameters, AAA, AP description, and WEP. The described AP searching should be differentiated from the active scanning via probe request/response defined in the 802.11 MAC [1]. Note that the 802.11 active scanning is performed to find the APs in the proximity before getting associated with an AP. Dr. Nespot AP searching is done in the application layer when the searching manager terminal is associated with an AP already or is connected to the wireline backhaul via a cable connector.

#### 3.3.2 Accessing to an AP

A Dr. Nespot agent in an AP should permit the access to its operating parameters only to the authorized user (or Dr. Nespot

manager) due to the security reason. Valid users should be informed of the account information, i.e., ID and password, in advance. The authorized users are classified into two groups. One, referred to as get-set user, has the ability to change the operating parameters of an AP. The other, referred to as get-only user, has only the ability to read them. To ensure the consistency, Dr. Nespot agent allows a single get-set user at a given time. On the other hand, there can be many get-only users simultaneously.

If a Dr. Nespot manager succeeds in gaining the access authorization into an agent, the agent registers the MAC address of the user terminal to the user table along with its corresponding authorization level, i.e., get-set or get-only. Then, subsequent PDUs are confirmed by comparing the MAC address of the sender with the list of the table. Any PDU from an unauthorized user is rejected with a proper error code which indicates the reason of rejection. If the available seats are full, the following access gain request is rejected accordingly. An authorized access gain is released via a proper access release PDU from the manager or an activity time-out at the agent. The time-out mechanism is defined in order to handle some erroneous situations, e.g., the manager program is terminated suddenly without the access release procedure.

### 3.3.3 Getting and Setting AP Parameters

Basically, the scheme for getting the parameters from an AP or setting them is borrowed from Simple Network Management Protocol (SNMP). Once a query with intended parameter identifiers is sent to an agent from an authorized manager, the agent collects the values of requested parameters locally, and transmits a PDU, which contains a set of parameter identifier and value pairs as a response. The set operation is performed in a similar manner; an authorized manager sends a PDU with a set of parameter identifiers along with desired values, and then the agent confirms the change of the parameter values via a response PDU after setting the new values. During this operation, many erroneous situations can occur. In order to inform such cases to the Dr. Nespot manager, an error map is defined specifying the position of parameters with errors and the reason of rejection. Intuitively, the set behavior, changing the parameters is allowed to only the get-set user. For example, when a get-only user requests the change of a parameter, a response PDU with a proper error code will be returned.

The exchange between the manager in the staff's terminal and the agent in an AP can be extended to that between a manager and a client station. Getting information, such as the type of OS and CPU, the amount of total and available memory from client stations, helps the operator to recognize the causes of problems. All the transmissions between a manager and client station are performed through the agent in an AP.

### 3.3.4 Measuring the Performance in the Air Link

The 802.11b provides up to 11 Mbps transmission rate in the physical layer, but the maximum throughput experienced in the application layer is up to 5 Mbps depending on the network condition. Practically, the actual throughput could be smaller than this due to many different reasons. For example, there can be many stations associated with one AP, which in turn reduces the user-perceived throughput performance. In other words, the AP is too heavily utilized. In another situation, a terminal may be associated with a neighboring AP even if there is a closer AP in

his own place. This can happen when either the closer AP or the terminal itself does not work properly. Note that all the NESPOT APs' use the same Service Set ID (SSID) "NESPOT." The channel quality could be severely degraded due to interferences from other neighboring APs. Moreover, each individual customer's perception about the WLAN performance can be different. Someone may even complain about her/his WLAN, which operates normally. The operator needs to measure how the WLAN performs quantitatively to decide a proper remedy. If the performance of the air-link is considerably poor, the service provider should install a new AP additionally or replacing the old one or change the allocated channels of other neighboring APs. That is, the process to measure the performance over the air link can be an initial step for satisfying the customer and provisioning the network.

The architecture for building this function is based on a 3-way handshake among Dr. Nespot manager, Dr. Nespot agent, and client station. The manager at the remote node or near associated station sends an initial PDU, which requests the performance measurement, to an AP. Then, the AP begins measuring the performance metrics, e.g., throughput, delay, and jitter by repeating dummy packet transmissions to a specific client station during a specific time interval. The results of measurement are calculated by client and sent to Dr. Nespot manager through the agent.

## 4. QOS PROVISIONING EFFORTS

Currently, KT provides VoIP services for both wireline and wireless (based on NESPOT) Internet users. The voice traffic requires low end-to-end latency in order to maintain the interactive communication. Video on Demand (VoD) is also one of the future target services of KT. Video traffic also requires a bounded latency even though the requirement is a bit relaxed compared to the voice traffic. It is well-known that the current Internet provides the best-effort service in the sense that it does not provide any QoS (e.g., latency and throughput) required for different types of traffic and applications. It goes the same with the NESPOT service since the current WLAN does not provide any QoS. In order to improve the service for the real-time traffic such as voice and video, an enhancement of the existing WLAN is needed.

### 4.1 Emerging IEEE 802.11e for QoS

The emerging IEEE 802.11e MAC, which is an amendment of the existing 802.11 MAC, will provide the QoS [1][7]. The standardization of the IEEE 802.11e is still on-going at the final stage [3]. In this subsection, we briefly introduce the 802.11e before presenting our approach.

The current 802.11 MAC has a mandatory distributed coordination function (DCF), which is based on carrier sense multiple access with collision avoidance (CSMA/CA). While there is another optional coordination function, i.e., polling-based point coordination function (PCF), most of today's 802.11 WLAN devices implement the DCF only. The channel access of the DCF is shown in Figure 3. Basically, when a station has a frame to transmit, it waits until the medium becomes idle. When the medium becomes idle, it senses the medium for a fixed amount of period, called distributed inter-frame space (DIFS), which is 50 usec for 802.11b WLANs, followed by a random backoff period

(which can range from 0 to 620 usec provided there is no frame transmission failure for 802.11b WLANs), during which the MAC continues to sense the medium. When the medium stays idle during the backoff period, the MAC transmits the pending frame. Due to the random backoff procedure before a transmission attempt, the collisions can be avoided mostly, but it potentially results in a large delay, especially, when there are collisions.

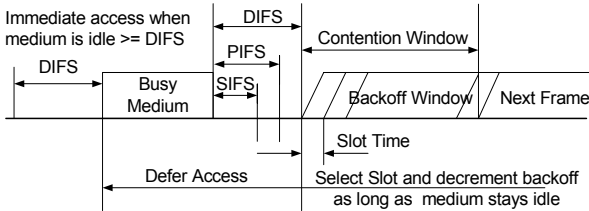


Figure 3. IEEE 802.11 DCF channel access

The emerging 802.11e MAC for QoS support defines a single coordination function, called hybrid coordination function (HCF). A key mechanism of the 802.11e is the enhanced distributed channel access (EDCA), which is an enhancement of the legacy DCF, for the prioritized QoS support. Under the DCF, there is basically a single first-in first-out (FIFO) queue inside the MAC. However, with the 802.11e EDCA, there are basically four FIFO queues located in the MAC as shown in Figure 4. A frame from the higher layer arrives at the MAC with a priority label (from 0 to 7), and each frame is enqueued into one of the four queues according to its priority value. Each queue has a channel contending entity, called access category (AC), which is a virtual DCF. Basically, four ACs contend for the channel independently. When multiple ACs finish the backoff process simultaneously, the highest priority frame is actually transmitted into the medium. In order to support the differentiated channel access for different priority frames, the EDCA uses an enhanced CSMA/CA as shown in Figure 5. Basically, instead of DIFS of the DCF, an AC under the EDCA uses AIFS[AC], whose value differs depending on AC. The upper bound of the backoff period is also determined depending on AC. Basically, the higher the priority (of the AC), the larger the AIFS value, and the larger the upper bound of the backoff period. In this manner, we can ensure that the higher priority frame is transmitted into the medium faster probabilistically.

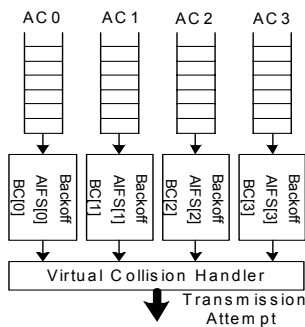


Figure 4. Four access categories (ACs) for EDCA

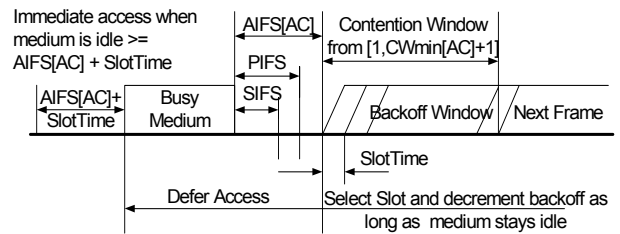


Figure 5. IEEE 802.11e EDCA channel access

We do not present all the details of the 802.11e MAC. However, basically it is expected that the 802.11e can provide different types of QoS support in the WLAN environments.

## 4.2 Our Approach via Software Upgrade

A negative aspect of the 802.11e in the service provider's perspective is that it requires a hardware upgrade. That is, the legacy 802.11 MAC controllers cannot support the 802.11e. Our approach is to implement multiple queues in the device driver of the 802.11 MAC controller so that a frame scheduling can be performed in the driver level. A similar approach was made in [12][17]. In case of AP, this software upgrade means the firmware upgrade of the AP, which can be done even remotely.

Figure 6 shows the device driver structure for both the original device driver and a modified device driver supporting our approach. We have used the HostAP driver [2] of Intersil's Prism 2.5 chipsets for our implementation. In the original driver, there is basically no queue for the frame transmission. A frame from the higher layer or from the wireline port is processed for the header and so on, and is forwarded to the MAC controller for the transmission. The MAC controller basically has a single first-in first-out (FIFO) queue. We have implemented two queues in the device driver level as shown in Figure 6 (b). We classify each frame to transmit into real-time (RT) or non-real-time (NRT). The current IP datagrams do not carry any information about the corresponding applications, and hence our implementation uses the port number as well as UDP packet type to classify a RT frame. That is, the device driver is provided the specific port number information of the real-time application in consideration. For example, KT's VoIP application utilizes a pre-assigned range of port numbers along with RTP over UDP protocols. For transmission scheduling, we have implemented a simple priority queuing so that the NRT queue is never served as long as the RT queue is not empty. We are currently investigating a more intelligent scheduling as will be discussed below.

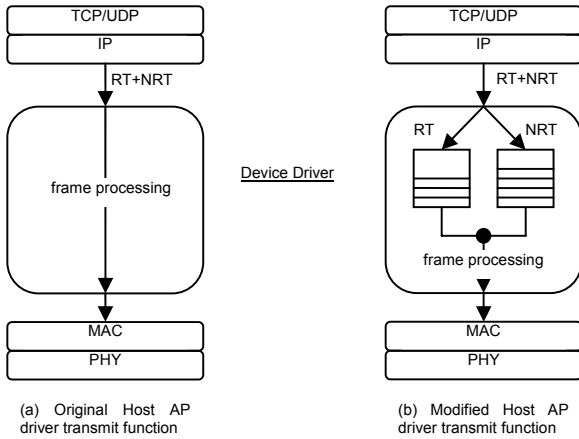


Figure 6. Device driver structures

### 4.3 Performance Evaluation

Here, we present some preliminary measurement results from our prototype. The network set-up for the measurement is shown in Figure 7. We have used NetIQ's Chariot for the measurements. Basically, the server provides both FTP and video (with 1.448 Mbps CBR streaming over RTP/UDP) services to a client across an AP implementing the dual queues. The console is the entity needed for Chariot in order to measure the network performance.

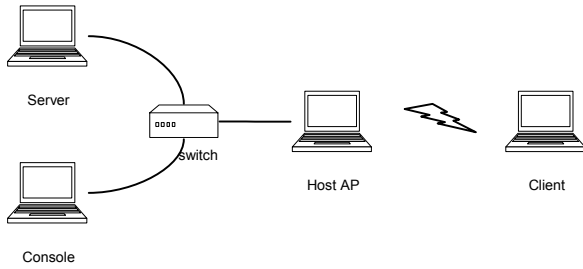


Figure 7. Network set-up for the experiments

Table 3. Performance comparison between the original AP and a modified AP with two queues

		Comparison		
		Original	Two queue	Gain
Throughput	TCP	3.851	3.703	-3.84%
	RTP	1.448	1.448	0.00%
Jitter of RTP	Avg.	2.9	2.6	-10.34%
	Max.	4.0	3.0	-25.00%
	Min.	2.0	2.0	0.00%
One-way delay of RTP	Avg.	30.7	20.2	-34.20%
	Max.	32.0	23.0	-28.13%
	Min.	30.0	18.0	-40.00%

Table 3 shows the measurement results for a number of performance parameters. First of all, we observe that the one-way delay of RTP (or RT traffic) is reduced by over 30%. This at least verifies that our goal is achieved via this simple modification of

the device driver. The jitter of RTP is a bit improved as well. In case of throughput, we observe that there is no change with the RTP throughput as it should be as the case with a CBR traffic, but the TCP (or FTP traffic) throughput is a bit reduced. We predict that this happens due to an increased delay of the FTP traffic out of the priority queuing of the modified device driver.

### 4.4 Limitations and Future Work

The priority queuing implemented currently achieves a prioritization among different types of frames, thus achieving a lower delay for RT traffic. However, this approach is limited in a number of ways. First, even if there are dual queues in the device driver, there is a single FIFO inside the MAC controller, and we cannot do any scheduling of the frames once a frame is forwarded to the MAC controller. Second, for the actual medium contention, every device including the AP contends in a fair manner based on the 802.11 CSMA/CA. Therefore, for example, a RT frame in an AP and a NRT frame in a terminal contend with the same channel access rule. Accordingly, in certain situations, the performance of the proposed scheme will be severely compromised. For example, if a terminal transmits a large amount of data, the scheduling within the AP explained above may not be that effective. Currently, we are investigating a class of algorithms to handle this problem.

Independent from the scheduling algorithm itself, we need more experiments as well. For example, we will need to check the VoIP performance with more contending terminals. Once we are assured that a reasonable performance based on this software queue implementation is achieved, we are planning to implement this approach into the existing APs of NESPOT to enhance the VoIP services as well as a potential VoD service.

## 5. OTHER FUTURE ISSUES AND ENHANCEMENTS

In this section, we discuss a number of possible enhancements to improve the NESPOT service in the future.

### 5.1 Towards 802.11a/g

As explained earlier, the current NESPOT is based on the 802.11b WLAN. However, today there are a couple of new WLAN versions called IEEE 802.11a [5] and 802.11g [9], which support the data rates in physical layer up to 54Mbps. Even though the standardization of IEEE 802.11a was finalized in year 1999, when IEEE 802.11b was finalized, the 802.11a devices became available in the market only in early 2002. On the other hand, the 802.11g is a brand-new WLAN standard. One major distinction between 802.11a and 802.11g is the frequency bands; the 802.11a operates at the 5 GHz bands while the 802.11g does at the 2.4 GHz bands. Moreover, the 802.11g actually includes the 802.11b, and hence can co-exist with the 802.11b at the same channel without a severe problem.

One minor problem with the 802.11a today in Korea is the available frequency spectrum at the 5 GHz band. As of today, the Korean government allows for the WLAN to use a spectrum of 100 MHz from 5.725 to 5.825 GHz. There exist four orthogonal channels of 20 MHz in this 100 MHz band. This is a much smaller band compared to other countries. For example, in the US, there exist 300 MHz band at 5 GHz, opening 12 channels for the 802.11a. The Korean government is planning to open up more

spectrum for the 802.11a WLAN in the future as the demand grows.

The higher the network speed, the better as long as a comparable cost is met. Accordingly, KT is currently planning to employ these new technologies for its future NESpot deployment. One imminent demand for the 802.11a/g, especially for the personal NESpot plan, is the fact that the highest speed xDSL, i.e., VDSL, provided by KT supports 23 Mbps transmission rate to the home. Accordingly, having a wireless connection inside home lower than 23 Mbps may not be a reasonable story for the customers who pay for this high-speed Internet service along with the personal NESpot service plan.

## 5.2 Security Consideration

As explained earlier, NESpot does not use a link-layer encryption today while it uses an authentication scheme based on EAP-MD5. An encryption scheme is under consideration for implementation, based on Tunnelled Transport Layer Security (EAP-TTLS) [20]. This allows an encryption in the WLAN by utilizing a dynamic WEP key assignment. Using EAP-TTLS, a WEP key is assigned to each terminal in a dynamic manner, and this will reduce the potential security attacks.

Even if a security mechanism is arranged in the link layer, a major effort should be made on the application-layer security solutions such as VPN and SSL since those are cost-effective and many certified technologies are mature enough to deploy along with the wide-spread of E-commerce.

## 5.3 Interworking with Other Networks

The NESpot Swing, which was described earlier, is the most primitive form of the interworking between the WLAN and cellular networks by combining only the billing of separate services for a dual-mode terminal. In the future, we expect a more comprehensive and close interworking between these two heterogeneous networks. Ultimately, the transitions between two networks should be so smooth that the users cannot recognize such transitions. A number of standard bodies including 3GPP and ETSI-BRAN are working on this issue currently [21][22].

In Korea, a new portable high-speed Internet system is expected to emerge in two years or so. This system will operate at a licensed 2.3 GHz band. This new portable Internet system is targeted at a wireless service of 1~2 Mbps per user with a low and medium mobility (up to 60 km/h speed). At this time, the exact specification of the system is not determined, but this system is expected to bridge the gap between the high-mobility high-cost conventional cellular system (e.g., 3G) and the low-mobility low-cost WLAN system. Accordingly, the interworking between this new portable Internet system and the existing WLAN will be another interworking issue in Korea in the near future.

## 5.4 Roaming and Resource Management

Along with the interworking with another wireless system discussed above, the roaming across WLAN APs is another important issue. The current NESpot supports the handoff of the users as long as a user hands off within a subnet. The areas called "NESpot streets," where WLAN subnet roaming is possible, are set up in 8 locations within Seoul currently. The handoff operation is expected to be improved, especially, considering the security perspective, via the IEEE 802.11f Inter-Access Point

Protocol (IAPP) recommended practice [8]. It may be also desired to support the handoff across subnets via mobile IP or so in the future.

For the WLAN-based Internet service provider like KT, it is highly desired to be able to monitor the usage/status of the WLAN. The current 802.11 provides different types of information via Management Information Bases (MIBs) [4], which can be accessed via SNMP or other protocol such as Dr. Nespot. Currently available MIBs seem not enough for the service providers in many situations. That is one of the reasons why many AP vendors support proprietary MIBs which are not part of the standard specification. Currently, the 802.11 working group is enhancing the radio resource management capability of the 802.11 WLAN by developing IEEE 802.11k [11]. The 802.11k will provide a much richer set of MIBs as well as many radio resource management capabilities desired to establish an intelligent WLAN environment.

## 6. CONCLUDING REMARKS

A WLAN-based Internet service of KT, called NESpot, is expanding in a remarkable manner since its inception in early 2002. However, the public service by WLAN is expected to encounter intrinsic limits of the technology, which was not originally designed for the public service. Those problems include security issue, maintenance, incompatibility among vendor-specific protocols and implementations, and QoS issues, etc.

In this paper, we have presented an overview of the joint effort between SNU and KT in order to enhance the WLAN-based NESpot service. Our efforts are to improve the network management/maintenance capability as well as the real-time application support. The schemes suggested in this paper would help both vendors and carriers to design and develop the WLAN products and services in a way to enhance the service quality and to enlarge the WLAN market. As the network size as well as the number of subscribers increase, it is expected more and more unexpected problems arise while more enhanced services are desired. To push the current WLAN technology and service over 3G service towards 4G wireless, many more issues are remained to be resolved by academia, vendors, and carriers in a cooperative manner.

## 7. ACKNOWLEDGMENTS

The authors would like to thank other MWNL members, including Youngsoo Kim, Jeonggyun Yu, and Jack Jang, who participated in the prototyping of the Dr. Nespot protocol.

## 8. REFERENCES

- [1] Choi, S., del Prado, J., Shankar, S., and Mangold, S, IEEE 802.11e Contention-Based Channel Access (EDCF) Performance Evaluation in Proceedings of IEEE ICC'03 (Anchorage, Alaska, USA, May 2003), IEEE.
- [2] Jouni Malinen, Host AP driver for Intersil Prism2/2.5/3, <http://hostap.epitest.fi/>, online link.
- [3] IEEE Working Group (WG), <http://www.ieee802.org/11>, online link.
- [4] IEEE Std. 802.11-1999, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)

- specifications, Reference number ISO/IEC 8802-11:1999(E), IEEE Std 802.11, 1999 edition, (1999), IEEE.
- [5] IEEE Std. 802.11a, Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band, IEEE Std. 802.11a-1999, (1999), IEEE.
- [6] IEEE Std. 802.11b, Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-speed Physical Layer Extension in the 2.4 GHz Band, IEEE Std. 802.11b-1999, (1999), IEEE.
- [7] IEEE 802.11e/D4.2, Draft Supplement to Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS), (February 2003), IEEE 802.11 WG.
- [8] IEEE 802.11f/D5.0, Draft Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution System Supporting IEEE 802.11 Operation, (January 2003), IEEE 802.11 WG.
- [9] IEEE 802.11g/D8.2, Draft Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band, (April 2003), IEEE 802.11 WG.
- [10] IEEE 802.11i/D4.1, Draft Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Control (MAC) Security Enhancements, (July 2003), IEEE 802.11 WG.
- [11] IEEE 802.11k/D0.4, Draft Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Specification for Radio Resource Measurement, (July 2003), IEEE 802.11 WG.
- [12] Jain, A., Qiao, D., and Shin, K.G., RT-WLAN: A Soft Real-Time Extension to the ORiNOCO Linux Device Driver, to appear in Proceedings of IEEE PIMRC'2003, (Beijing, China, September 7-10, 2003), IEEE.
- [13] Katzela, I. and Naghshineh, M., Channel Assignment Schemes for Cellular Mobile Telecommunication Systems: A Comprehensive Survey, IEEE personal communications, (June 1996).
- [14] Kim, D., Kim, S., Jung, H., and Gweon, S., WLAN Interference Reduction Method by Channel Assignment with Field Test Results, Proceedings of JCCI'03, (Anmyundo, Korea, April 2003).
- [15] KT NESPOT, <http://first.nespot.com/english/web/>, online link.
- [16] O'Hara, B., and Petrick, A., The IEEE 802.11 Handbook: A Designer's Companion, Standards Information Network, (1999), IEEE Press.
- [17] Spectralink, <http://www.spectralink.com>, online link.
- [18] RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, (December 2002).
- [19] AirSnort, <http://airsnort.shmoo.com>, online link.
- [20] draft-ietf-pppext-eap-ttls-02, EAP Tunneled TLS Authentication Protocol (EAP-TTLS), (November 2002).
- [21] 3GPP TSG SA WG1, <http://www.3gpp.org/TB/SA/SA1/SA1.htm>, online link.
- [22] ETSI TR 101 957, HIPERLAN/2; Requirements and Architecture for Interworking between HIPERLAN/2 and 3<sup>rd</sup> Generation Cellular Systems, (August 2001), ETSI.