LETTER

Fast Configuration for Mobile IPTV in IPv6 Networks*

Soohong PARK[†], **Jun LEE**[†], ***Nonmembers, and*** **Choong Seon HONG**[†a)], ***Member***

SUMMARY This letter proposes a new fast network configuration scheme that realizes an IP interface that allows users to view Internet Protocol TV (IPTV) in IPv6 networks more quickly than is possible with the current configuration procedure. The new scheme, a hybrid combination of IPv6, address information, and non-IP information, especially the Domain Name Service, is newly designed based on a technical analysis. The evaluation results show that the proposed scheme is acceptable for real-time television watching in IPv6 networks, even when in motion.

key words: *IPTV, Mobile IPTV, IPv6, DHCP*

1. Introduction

IPTV allows users to transmit and receive multimedia traffic, and provides real-time broadcasting and video on demand (VOD) through IP-based networks. In addition, IPTV is rapidly expanding to both mobile and wireless technologies (a.k.a. Mobile IPTV [1]), and therefore enabling handover between multiple access networks is highly desirable because it can resolve service-coverage limitations and eliminate dead spots in IPTV. Mobile IPTV device is moving and attaching randomly to various wireless access networks, and the network information such as the IP address, Domain Name Service (DNS) server address, and other information should be configured quickly in order to receive IPTV service, particularly real-time based services without delay over IP-based networks. It is because handover bring about the change of the network information on Mobile IPTV.

Recently, IPv6 is fast coming to the home networking, and IPTV can be a primary use case because of a common feature of IP. IPv6 is usually configured by either Neighbor Discovery (ND) Protocol [2] or Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [3].

This letter proposes a new scheme for the IPTV network information configuration in IPv6 networks and adopts new ND options [4] as supplementary methods for IPv6 that can be used to eliminate the DNS configuration delay via the Dynamic Host Configuration Protocol (DHCP) because the time needed for the DHCP server to assign the network information to the client can be on the order of seconds. Using the proposed scheme, the mandatory network information of the IPTV device such as the IP address and DNS can be configured simultaneously in order to reduce the delay before being able to view IPTV. The main reason for focusing on IPv6 in this letter is to suggest an enhanced and efficient IPTV service compared to the existing IPv4 IPTV system.

Section 2 describes both the existing and new schemes for the supplementary IPv6 configuration methods and their technical analyses. In Sect. 3, the detailed procedure is described and the performance evaluation is provided. Section 4 concludes the letter.

2. Analysis of IPv6 Configurations and New Scheme

ND for IP Version 6 [2] and IPv6 Stateless Address Autoconfiguration [5] can be used to configure either fixed or mobile nodes with one or more IPv6 addresses, default routes, and other parameters. To support access to additional Internet services that are identified by a DNS name, such as a web server, the configuration of at least one recursive DNS server is also needed for DNS name resolution.

DHCPv6 [3] currently provides a general mechanism for conveying network configuration information to the IPv6 host. Configuring the DHCPv6 servers in this way allows the network administrator to configure the DNS server, the addresses of other network services, and location-specific information, such as time zones. As a consequence, when the network administrator configures DHCPv6, all of the configuration information can be managed through a single service, typically with a single user interface and a single configuration database.

Because the DNS information is not contained in the Router Advertisement (RA) messages, as depicted in Fig. 1,

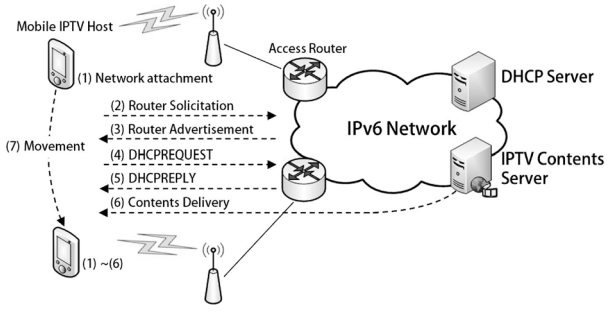


Fig. 1 IPTV network information configuration procedure in IPv6.

Manuscript received April 16, 2011.
Manuscript revised July 21, 2011.

[†]The authors are with the Department of Computer Engineering, Kyung Hee University, Korea.

*This research was supported by MKE, Korea, under the ITRC support program supervised by the NIPA (NIPA-2011-CC1090-1121-0003). Dr. C.S. Hong is a corresponding author.

a) E-mail: cshong@khu.ac.kr

DOI: 10.1587/transcom.E94.B.3595

the IPTV host must receive two messages from the router. In networks in which the bandwidth is at a premium, especially wireless networks, this is a disadvantage, although on most networks it is not a practical concern. In addition to waiting for an RA message, the IPTV host must now exchange packets with a DHCPv6 server. Even if it is locally installed on a router, this will slightly extend the time required to configure the host. For an IPTV device that is moving rapidly from one network to another, this is a disadvantage.

2.1 New Scheme for IPTV Configuration in IPv6

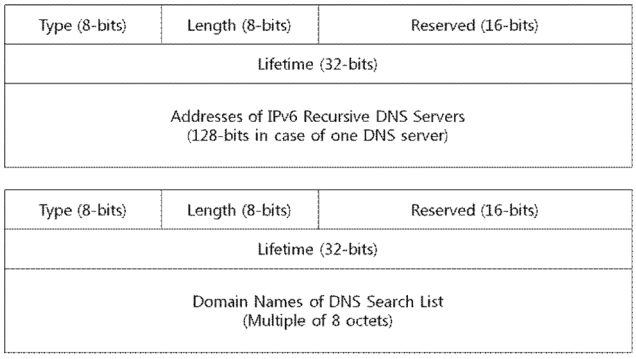
The DNS information is still missing parts of IPv6 autoconfiguration, as described above. To reduce the delay in the DNS configuration caused by redundant procedures like DHCP, new ND options [4] that contain the DNS information are suggested in the proposed scheme. There procedures are existing ND transport mechanisms (solicitations and advertisements) which operate in the same way as that through which hosts learn about routers and prefixes. The IPv6 host can configure the IPv6 addresses of one or more DNS servers and domain names via the RA message that is periodically sent by a router or solicited by a Router Solicitation (RS).

The proposed scheme requires that the DNS information be configured in the advertising routers. The configuration of the DNS addresses can be performed manually by an operator or in other ways, such as automatic configuration through a DHCPv6 client. An RA message with one DNS option can include as many DNS server addresses as needed. Using the ND protocol and DNS option, along with a prefix information option [2], the IPv6 host can simultaneously perform the network configuration of its IPv6 and DNS server addresses.

The RA option for DNS can be used in any network that supports the use of ND. The RA approach is useful in some mobile environments in which the addresses of the DNS server are changing because the RA option includes a lifetime field that allows the client to use a nearby DNS. The lifetime field can be configured to a value that will cause client time out and a switch to another DNS server address. However, from the implementation viewpoint, the lifetime field seems to make matters more complex. Instead of just writing to a DNS configuration file such as *resolv.conf* for the list of DNS server addresses, we use a daemon (or a program that is utilized at defined intervals) that continually monitors the lifetime of the DNS.

The preference value of the DNS, which is included in the DNS option, allows the IPv6 hosts to select the primary DNS from several DNSs to balance the load of the DNS. To carry the DNS information in the RA, this letter adopts two new ND options: (1) the Recursive DNS Server (RDNSS) option and (2) the DNS Search List (DNSSL) option according to [4] to the fast network configuration scheme in the IPTV service model proposed by this letter.

The RDNSS option contains one or more IPv6 addresses of recursive DNS servers, all of which share the same lifetime value. If it is desirable to have different lifetime values, multiple RDNSS options can be used. Figure 2 shows the format of the RDNSS option.



Field Description: RDNSS option type is 25, DNSSL option type is 31; length is the length of options; lifetime is the maximum time, in seconds (relative to the time the packet is sent), over which the RDNSS address and DNSSL domain name may be used for name resolution. A value of zero means that the information can no longer be used.

Fig. 2 RDNSS option format (upper) and DNSSL option format (lower) in an IPv6 router advertisement message.

Also, the DNSSL option contains one or more domain names for the DNS suffixes, all of which also share the same lifetime value. If it is desirable to have different lifetime values, multiple DNSSL options can be used. Figure 2 shows the format of the DNSSL option. For simple decoding, the domain names must not be encoded in a compressed form. Because the size of this field must be a multiple of eight octets, for the minimum multiple including the domain name representations, the remaining octets other than the encoding parts of the domain name representations must be padded with zeros.

An RDNSS address or a DNSSL domain name must be used only as long as both the RA router lifetime advertised by an RA message [2] and the corresponding option lifetime have not expired. This is so because, in the current network to which the IPv6 host is connected, the RDNSS may not be currently reachable, the DNSSL domain name may no longer be valid, or these options do not provide service to the host's current address.

2.2 New Scheme and Implementation Considerations

The procedure of the DNS configuration through the RDNSS and DNSSL options is the same that of any other ND option [2]. When an IPv6 host receives DNS options through the RA messages, it processes the options as follows:

- The validities of the DNS options are determined using the length field; that is, the value of the length field in the RDNSS option is greater than or equal to the minimum value (3), and the value of the length field in the DNSSL option is greater than or equal to the minimum value (2).
- If the DNS options are valid, the host should copy the values of the options first into the DNS repository and then into

the resolver repository. Otherwise, the host must discard the options.

When the IPv6 host has gathered a sufficient number of RDNSS addresses (or DNS search domain names), it should maintain a sufficient number of RDNSS addresses (or DNS search domain names) such that the most recently received RDNSS or DNSSL is preferred over the previous ones; that is, when the number of RDNSS addresses (or DNS search domain names) is sufficient, the new one replaces that with the shortest remaining lifetime. As an exceptional case, if the received RDNSS addresses (or DNS search domain names) already exist in the IPv6 host, their expiration times, when the corresponding DNS information expires in the IPv6 host, are updated; when the lifetime field is zero, the corresponding RDNSS (or DNS search domain name) is deleted from the IPv6 host.

Other than this update, the IPv6 host should ignore other RDNSS addresses (or DNS search domain names) within an RDNSS (or a DNSSL) option and/or additional RDNSS (or DNSSL) options within an RA. The sufficient number of addresses is a system parameter that can be determined using a local policy. Also, separate parameters can be specified for the sufficient number of RDNSS addresses and that of the DNS search domain names, respectively. In this section, the recommended sufficient number is three, considering both the robust DNS query and the reasonably time-bounded recognition of the unreachability of a DNS server.

For the case in which the DNS options of RDNSS and DNSSL can be obtained from multiple sources, such as RA and DHCP, the IPv6 host should maintain some DNS options from each source. Unless explicitly specified for the discovery mechanism, the exact number of addresses and domain names to maintain is a matter of local policy and implementation choice. However, it is recommended that at least three sets of addresses and domain names be stored from at least two different sources. The DNS options from RA and DHCP should be stored into the DNS repository and resolver repository so that the information from DHCP appears there first and therefore takes precedence.

For the configuration and management of the DNS information, the advertised DNS configuration information can be stored and managed in both the DNS repository and the resolver repository. For environments in which the DNS information is stored in the user space and ND runs in the kernel, it is necessary to synchronize the DNS information (RDNSS addresses and DNS search domain names) in the kernel space and the resolver repository in the user space. For the synchronization, an implementation in which the ND operating in the kernel provides a write operation to update the DNS information to the resolver repository. One simple approach is the use of a daemon that continually monitors the lifetimes of the RDNSS addresses and the DNS search domain names. Whenever there is an expired entry in the DNS repository, the daemon can delete the corresponding entry from the resolver repository.

In DNS repository management, the kernel or user-space process (depending on where the RAs are processed) should maintain two data structures: (1) the DNS server list that maintains the list of RDNSS addresses, and (2) the DNS search list that maintains the list of DNS search domain names. Each entry in these two lists consists of an RDNSS address (or DNSSL domain name) and an expiration time as follows:

- RDNSS address for the DNS server list: the IPv6 address of the recursive DNS server which is available for recursive DNS resolution service in the network advertising the RDNSS option.
- DNSSL domain name for the DNS search list: the DNS suffix domain names that are used to perform DNS query searches for short, unqualified domain names in the network advertising the DNSSL option.
- Expiration time for the DNS server list or DNS search list: the time at which this entry becomes invalid. The expiration time is set to the value of the lifetime field of the RDNSS option or DNSSL option plus the current system time. Whenever a new RDNSS option with the same address (or DNSSL option with the same domain name) is received on the same interface as is a previous RDNSS option (or DNSSL option), this field is updated with a new expiration time. When the expiration time becomes less than the current system time, this entry is considered to be expired.

Whenever an entry in the DNS server (search) list expires, it is deleted from the list, and the RDNSS address (DNSSL domain name) corresponding to the entry is deleted from the resolver repository.

3. Performance Comparison and Results

We evaluated the performance of the proposed scheme and compared it with that of the existing scheme using *Omnet++*, an extensible, modular, component-based *C++* simulation of communication networks. We designed the IPTV service model, the currently most common commercial model, using the current network IPv6 configuration and the proposed fast configuration for IPTV. Our simulation was used to compare the IPv6 address configuration delay and the packet loss when the Mobile IPTV device changed its point of connection. Practically, the time delay and the packet loss were closely related to the quality of service and quality of experience on the user's IPTV device. These aspects are very critical and sensitive for the use of real-time IPTV services. We chose both wired (Ethernet) and wireless (Wi-Fi, IEEE 802.11b/g) network interfaces for the evaluation since those networks are the most popular in current commercial IPTV networks. Figure 3 shows the reference network model, and the specific network parameters are described in Table 1.

We measured the IPTV traffic in 30 trials, and the results are shown in Figs. 4 and 5. As we can see in Fig. 4, the delay time, which is the roundtrip time between the DHCPREQUEST and DHCPREPLY messages in Fig. 1

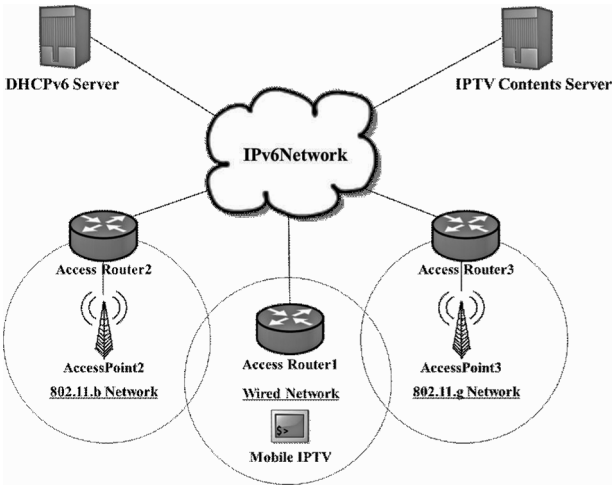


Fig. 3 Reference model for Mobile IPTV evaluation.

Table 1 Configuration parameters used in the performance evaluation.

Network Parameters			
Network Type	802.11b	802.11g	Wired
Frequency	2.4 GHz	2.4 GHz	-
Data rate	4.5 ~ 11 Mbps	19 ~ 54 Mbps	100 Mbps
Range	115 feet	125 feet	-
IPTV Content Server Parameters			
Service	Bandwidth	Period	Payload
HDTV	20 Mbps	1 ms	2500 Bytes
Mobile IPTV Parameters			
Network Interface	Ethernet, 802.11b, 802.11g		
Mobility type	Linear mobility		
Mobility speed	3 ~ 6 km/h (working speed)		

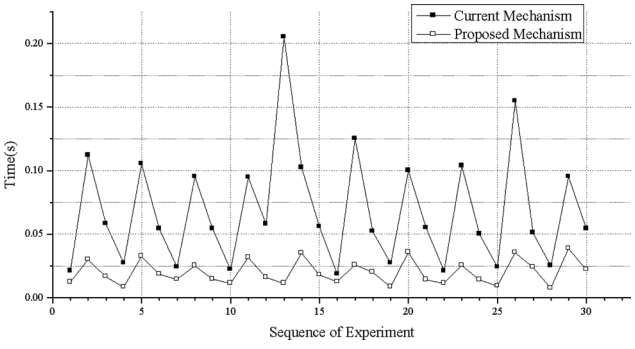


Fig. 4 Time delay between wireless and wired networks.

needed to configure the DNS information when attaching a new network, is definitely enhanced compared to that of the existing scheme, and the operation of the IPv6 address configuration is more stable than that of the existing scheme for the IPTV streaming service.

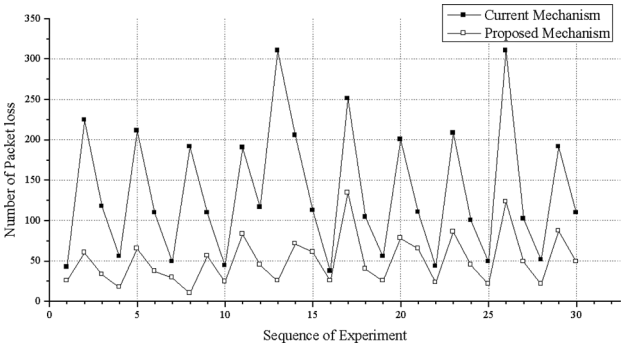


Fig. 5 Packet loss between wireless and wired networks.

Likewise in Fig. 5, we evaluated the performance of our proposed scheme with regard to the packet loss for Fig. 3 network topology when the Mobile IPTV device was operating the IPTV streaming service from the IPTV content server over different networks. Through this evaluation, we showed the reduced packet loss and more stable IPTV streaming for the proposed scheme compared to those of the existing scheme.

4. Concluding Remarks

This letter described the current issue with the IPv6 configuration in IPTV and suggested a new configuration scheme to reduce the time delay and the packet loss when deploying IPTV service in IPv6 networks. In doing so, the DNS options have been newly defined to support the proposed configuration scheme. Also, a performance evaluation and comparison have shown that the proposed scheme has shorter delay than the existing scheme, has reduced packet loss, and is acceptable for viewing IPv6 network television in a real-time manner, even when in motion.

References

[1] S. Park and S. Jeong, "Mobile IPTV approaches, challenges, standards, and QoS support," IEEE Internet Computing, vol.13, no.3, pp.23–31, May-June 2009.
[2] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor discovery for IP version 6 (IPv6)," IETF RFC 4861, Sept. 2007.
[3] R. Droms, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," IETF RFC 3315, July 2003.
[4] J. Jeong, S. Park, L. Beloeil, and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration," IETF RFC 6106, Nov. 2010.
[5] S. Thomson, T. Narten, and T. Jinmei, "IPv6 Stateless Address Autoconfiguration," IETF RFC 4862, Sept. 2007.