A Proposed Model for Policy-Based Routing Rules in the IPv6 Offering QoS for IPTV Broadcasting

Mohammad Azmi Al-Madi , Rosnah Idrus, Sureswaran Ramadass, Rahmat Budiarto

NAv6 Centre, Universiti Sains Malaysia, Pulau Pinang, Malaysia

Summary
One of the major applications in the domain of the IPv6 that is being taken into consideration is the Internet Protocol Television (IPTV). This application relates to the Broadcast networks that can be managed with such routing policies. The Internet-Based TV broadcasting performs a high support of quality to the viewers when receiving their channels with efficient delivery. Therefore, the Quality of Service (QoS) which is a major feature in the IPv6 came to be a significant part for this support. Hence, in this paper, we propose an enhanced technique model for policy routing management in the TV broadcasting which is called the PBR and QoS Control Routing for Multi-Channel Adaptive Streaming (PQMAS) technique. Our technique combines three basic concepts which are; QoS, Policy-Based Routing (PBR) and the Controlling Network Traffic (CNT). These combinations are a complement to the Multi-Channel Adaptive Streaming (MCAS) framework, besides, new rules in the PBR were proposed.

Key words:
Quality of Service (QoS), IPv6, Policy-Based Routing (PBR), Internet Protocol Television (IPTV), Broadcasting.

1. Introduction

Due to the limitations in the IPv4 domain, especially, its address space, the IPv6 domain appeared to replace, extend and enhance the role of the IPv4 domain [1]. Such an example, the address of the IPv4 was 32 bits, but, IPv6 came to expand this address to be as 128 bits. In other words, on the planet, each user will certainly have a sufficient number of these expanded addresses [2]. The Internet Protocol (IP) is considered to be as a best-effort in the IPv4 but still has in sufficient acts to cover the customer's needs [3]; therefore, the IPv6 came to expand its use over the IPv4 version.

A development for the IPv6 was performed by the Internet Engineering Task Force (IETF). This organization increased the success to the IPv6 than was in the IPv4 [3], besides, the Quality of Service (QoS) was integrated and developed by the IETF organization. This efficient integrated service is considered to be a development itself and one of the most significant features in the IPv6 domain. The main idea and aim is that the IPv6 provides better support for QoS, so that, in the future, many upgrades will overcome many problems that were faced by the customers. This development is exploited to satisfy the customer's needs. Such an example, better QoS in the Internet Protocol Television (IPTV) will provide better broadcasting of programs (channels) from different internet sources. More specifically, QoS comes to be combined with the routing procedures, in order to efficiently provide better services to the customers with high quality.

The QoS was defined into two definitions [4], the first definition is "The Quality of Service is a generic term and people often use it to express a variety of different things, depending on their discipline, as well as on their particular subject area". The second definition is "QoS can be interpreted as a general effort to apply the necessary mechanisms and techniques, in order to enable different behavior from the network infrastructure among the different types of traffic that are being transmitted over it". As an explanation to both definitions, [5] illustrated that both network types; service types and traffic types can be compared when performing such routing tasks. This is because a protection can be performed to one or more traffic classes in the routing network compared to other network types.

In the IPv6, the traffic is known and handled by new fields [6]. The flow label's field is utilized by the identification of the traffic. This is performed through the IPv6's header. Here, packets are identified and added by routers for special handling of a flow. These packets are ordered and organized in series by this flow among the source and destination. There are main characteristics (features) of the IPv6 over the IPv4, the main ones that this research studies is the better support for QoS [6].

The main aim of this paper is to study and understand the broadcasting network that can be managed by a routing policy. Such an example of an important protocol that plays an essential role through the broadcast is the Internet Protocol Television (IPTV) [7]. The IPTV can be a system

Manuscript received March 5, 2008
Manuscript revised March 20, 2008

that transmits a service of digital television through the infrastructure network, where, the broadband connection makes a transmission for this network.

There are major features of the broadcast networks. These features are:

1. This network transmits the packets to be received by every device in the network. For instance, the information is referred to a segment of the media to as many users as possible.
2. Local Area Network (LAN) enormously limits the broadcast networks.
3. It has a greater performance in LAN that in WAN.
4. It works as a secure system in the network.

For today's interest, the applications of multimedia have appeared to benefit the provider of the internet service and the researchers in order to manage their requirements [4]. In the future, the technology will push us to make a convergence of the broadcast network into Internet Protocol (IP) network; hence this is a strong need that makes this research with a high motivation to be taken into consideration. Moreover, the IPv6 not only overcomes the shortcoming problems in the IPv4, but also, overcomes and benefits the Quality of Service (QoS) in the IPv6.

The rest of the paper is organized as follows. Section 2 discusses many works that have been proposed by many researchers. Section 3 gives an overview of our methodology. Finally, we conclude the paper in Section 4.

2. Related Works

Many studies have been extensively performed by many researchers to develop various different methods for Quality of Service (QoS) and Policy-Based Routing (PBR) in the IPv6 domain. According to this, these works can be classified into two major categories; Quality of Service (QoS) methods and Policy-Based Routing (PBR) methods.

2.1 Quality of Service (QoS) methods

A framework for assurance QoS was proposed by [4] to cover the customer's needs. This is performed by adding support for a number of differentiated services which must satisfy these needs and the application. In [8], the QoS management API framework that is utilized by Bandwidth Broker implementation was proposed. The main idea was to make a configuration for the underlying routers. Another framework which is called the End-to-End QoS Provisioning framework was proposed by [3]. This framework does not use 5 tuples, but 3 tuples, in the header of the IPv6. In other words, resources are kept by depending on the use of both; the traffic class and the flow label. The main aim was to satisfy customized QoS provision. Here, the flow classification was efficiently improved from 5-tuple in the header of the IPv4 to 3-tuple in the header of the IPv6. This improvement was to make a reduction to the load of the edge router, where, this reduction results with a high speed to deliver the needed packets. In [9], a framework was proposed for QoS to discuss its services over the domain of the IPv6 in order to get three advantages. These advantages are; packet loss, less delay and less jitter. These advantages were resulted by making a collection of services over the traffic of the real-time.

A new pragmatic approach for QoS of the Differentiated Services in the Internet was proposed by [10]. This approach is a design of applications that is considered to be adaptive for the characteristics changes over the network, such as, congestion. In [11], the Securing Quality of Service (SQoS) framework for QoS was evaluated and developed in an efficient way. The main idea of this framework was to secure a system that helps in forming the protocol of the on-demand QoS-Guided Route Discovery. Such example of protocols that are based on this protocol, ARAN protocol [12], AODV protocol [13], Ariadne protocol [14], SAODV protocol [15] and DSR protocol [16].

A testing for the QoS in the IPv6 and the IPv4 was performed by [17] to make an evaluation for the DiffServ QoS over the software of the Dual Stack Network. The main idea was to make some tests on the IPv6 traffic by applying the technique of the DiffServ QoS. The importance of this technique was to check the efficiency and the performance of the function of the whole router in the network. In [18], a framework to integrate the network services was proposed in order to make a study to guarantee the voice of packet telephony that supports and benefit different approaches of the QoS-support, such an example of these approaches; IP/RSVP, IP-prioritization, IP/over-engineering, ATM-VBR, ATM-CBR. The main idea of the work was to utilize a simulated model to make a design for a network that is enormously scaled.

2.2 Policy-Based Routing (PBR) methods

A unified theory for PBR was proposed in [19] in order to solve the following problems; Stable Paths Problem, Sobrino's Routing Algebras Problem and Classical Path Algebras (semi-rings for generalizing minimum-weight routing) Problem. In other words, [19]'s theory depends on both; the relations of the abstract and the properties of these relations. Moreover, it does not depend on the details that are considered to be axiomatic or syntactic of the

theories for PBR. In [20], an algorithm for computing policy-based inter-domain routes (BGP routes) on-demand in a network simulation is performed. This kind of simulation that uses this algorithm is efficient when having forwarding paths that are realistic for the network traffic. In [21], families of routing algorithms were introduced. This group of algorithms performed a developed computation for routes, where, performance constraints and traffic are involved at this role. An alternative routing mechanisms and policy-based protocols are introduced in [22]. The main idea was to make identification for the architecture of the routing. This architecture will probably develop the Defense Information System Network (DISN). Management architecture for active network was proposed in [23] to make programming networks be able for network users whom want to utilize these programs for programming purposes, more specifically; a merging between this ability and the potentials of the PBR is performed to have high performance advantages.

3. Methodology

As mentioned previously, many works have been performed on supporting better QoS in the IPv6. Efficiency and better performance caused better and high services in the both domains; IPv4 and IPv6. Therefore, studies are continuously being performed to control the strategy or policy in serving customers. As a main step, these policy rules that are based on routing packets must be set up and improved to perform the routing operation in many networks (i.e. broadcasting). Hence, in this section, we will study and enhance [24]'s model which is the *Multi-Channel Adaptive Streaming (MCAS)*. This technique will be enhanced by studying and creating some new rules in the PBR. We combined three main concepts to [24]'s technique to create our technique that is the *PQMAS (PBR and QoS Control Routing for Multi-Channel Adaptive Streaming)* model technique. These concepts categories comprise; Policy-Based Routing (PBR), the Quality of Service (QoS) routing and Controlling Network Traffic (CNT) to make integration for the *MCAS* model.

3.1 Overview of the Policy-Based Routing (PBR)

QoS plays an important role on the internet [25]. It provides the users with efficient and integrated services over the network. Some users have no QoS. This is because they didn't pay more money to get this service. A service guarantee is given to users who have paid more money to get more high services with high quality. Despite this, many users are trying to have this service without paying money in an illegal ways. Therefore, the policy-based routing came by adding policy rules to prevent any of those who are trying to have these services without paying money (see later sections at this chapter (the new rules)).

In these developed days, routing and packet forwarding are being implemented by many organizations using their routing policy that is configured to forward these packets. The packets chooses different paths to be routed when customers uses the Policy-Based routing. More clearly, these policies are implemented in the flow of routing these packets when they are sent from the source to the destination [26].

Policy-based routing controls the routing behavior of the packets. More clearly, a user identifies the route way of the received packets to be routed. The user's tasks comprise both tasks; the configuration of packets and the determination of the next hop or output interface. The first task is performed by exploiting many features. The second task is performed to identify either Hop or output interface the packets will be received. In addition, a basic packet-marketing capability is added by this policy [27].

Routing packets is a main task when the PBR plays the role at any network. Before routing any packet to any next hop, output, destination or interface, traffic flows must have a determined policy rules. Routing protocols also play a broad role in the PBR; it provides the user with full control in managing and routing packets by controlling and supporting the available techniques. In the PBR, the IPv6 precedence is set up by the user. This operation is a privilege given by the PBR. Another privilege that the PBR offers to the users is the determination of a suitable path for the traffics to route the packets, such an example of this, the priority traffic over a high-cost link.

Packets are routed using a based configured policy. This is done by setting up the PBR. In other words, it is possible to perform an implementation for policy routing in the purpose of determining whether to make a permission or denier for packets to enter the suitable paths.

The followings are main tasks to be given to the users by PBR:

1- By depending extended access list criteria, users can categorize the traffic.
2- The user can then make an access to these lists.
3- After that, the user will set up the matching criteria.
4- Now, the user will start setting up the precedence bits of the IPv6.

5- Then, distinguished services will be provided by the network.
6- Finally, determined paths receive the packets that are routed by a determined policy routing rule. These paths are for the traffic-engineering. The importance of this routing of packets is to provide the QoS though the network.

There are descriptors that can be used for simple and complex policy, these are; IPv6 address, port numbers, protocols and the packets size. It is important to notice that if the policy was simple, then the user is allowed to use just one of these descriptors, otherwise, if the policy was complex, then the user have the allowance to use the whole of these descriptors.

At the network edge, the users are allowed by the PBR to categorize and mark the flow of packets. The precedence value of a packet is set up by the users, so that, a mark will performed to these packets by the PBR. After that, the routers use this value in an immediate way. The main idea of this is to combine the QoS with the packets to be routed in the network.

3.1.1 Policy Definition

As stated in [25], "A policy is a set of rules which associate with some services". There are a number of criteria that are configured by the policy rules in order to get high services with high quality. One or more conditions and actions are contained in the policy rules. These rules perform a certain condition before performing the actions to be determined, as shown in Figure 1 below.

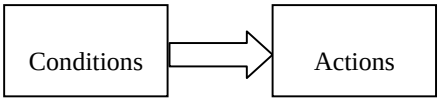

Fig. 1: Policy Rule [25].

Such an example of the policy rule as [25] has discussed, is that in the department of the Computer Sciences, in the lecture's offices, when the traffic flows from these offices, it must have more high priority than if the flow of the traffic was from the student's labs. So, the condition will be as [25] has explained: "If the traffic flows are from lecture's offices"; this is considered to be the condition, but, the action will be as: "Assign higher priority to those flows".

3.1.2 Policy Architecture

A policy framework was developed by the IETF Resource Allocation Protocol (RAP) and was used to be performed to serve the policy between the networks. Various numbers of technologies are related to this architecture [25]. Such an example, the QoS technologies (e.g. DiffServ) and the non-QoS technologies (e.g. network security). Figure 2, shows the whole architecture of the policy routing.

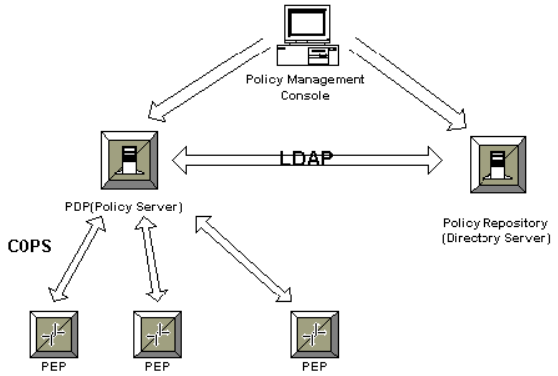

Fig. 2: Policy Architecture [25].

This figure is classified into four main components:

1- Policy Management Console: this component has major functions which are; viewing, editing and entering the rules of the network policies. Moreover, this component makes a full test for these network rules.
2- Policy Repository: this component controls both; the storage and the retrieval of the networks policy. Repeatedly, conditions and actions are considered to be two major types of the policy rules. In other words, more policy rules can be added to any existing or known policy rules.
3- PDP (Policy server): here, this server receives the policy rules. After that, the server provides a number of decisions; these conditions are related to these rules. Moreover, information that is sourced from various entities is efficiently used by the PDP, such an example of this information, SNMP agents and the authentication server.
4- PEP: this component is considered to be the main policy point to be taken into consideration. It performs important routing tasks that support the network policy. More clearly, this component can work as a device of a network that can successfully operate the rules of the policy network. As an example of this component that support the policy rules, the switch or router. At one network device, the both components; PDP and PEP are distributed at the same time in order to be implemented. A lot of PEP's can be controlled by a single PDP into one administrative domain of the same network

device where the both components were distributed.

These four main components are combined with two main communication protocols, these two protocols are; Common Open Policy Service (COPS) and Lightweight Directory Access Protocol (LDAP). COPS's main task is to shares and interfere the information between the last two policy architecture components; PDP and PEP. Its main features are; reliability and extensibility. The COPS can be efficiently applied for general purposes, such as, policy enforcement, router configurations and policy administrations. The LDAP's main task is to configure various different policies and control them by managing the number of packets to be routed. This protocol has also main features which are; firstly, it is an architecture that is general with its purposes. Secondly, it is considered to be as a vendor- and device – independent, because; the policy repository keeps the information of the policy network for main tasks. Thirdly, it is very easy in for policy rules consistency testing.

3.1.3 A Comparison between Policy-Based Routing and QoS-Based Routing

QoS is the backbone of the Policy-Based Routing. This means that the both routing components depend on each other. Despite this, still the QoS needs to be taken into consideration [25]. *Provisioned QoS* and *Signaled QoS* are two types that support the demands of the QoS. Both types are statically and dynamically being created [25]. The static creation relates to the first type (*Provisioned QoS*) and the dynamic creation relates to the second type (*Signaled QoS*). The first type treats and processes the traffic of packets to be routed by the support of QoS. The second type treats and processes the requirements of the QoS information that is available at any signal in the network. This ensures to add *Signaled QoS* while performing the QoS-based routing. In short, the both types are needed for supporting both; the Policy-based routing and the QoS-based routing with a high efficient integration in the routing tasks, so, at the network edge, the packet categorization will be stored and protected.

3.2 Broadcasting Routing Network

Messages are sent by one host or a number of hosts to many or all hosts, such examples for this operation, stock market updates, reports for weather service distribution and provided that, the best example is that all hosts or machines will be perfectly broadcasted from the programs of the radio to serve the listeners in hearing various types of news sources [28].

When a packet is efficiently being sent at the same time to all destinations, this is called as *Broadcasting*. There are five major methods for the Broadcast Routing [28]; *Source Sending* method, *Flooding Routing* method, *Multidestination Routing* method, *Spanning Tree* method, and finally, *Reverse Path Forwarding* method. These methods perform efficient broadcasting tasks for packets to be routed.

3.3 Multi-Channel Adaptive Streaming (MCAS) Technique

In the peer-to-peer streaming concept, many researchers have studied many different methods in the IPTV for this concept [24], such as, in [29, 30, 31]. In the IPTV, the single channel streaming is taken into account. A viewer has the ability to get multiple channels. This ability is provided by the IPTV. According to this, [24]'s method forms the problem on how the bandwidth of packets will be managed by the network manager to serve the subscribers with multiple channels. Therefore, they proposed hierarchical semantic-driven multi-channel streaming technique to serve the viewers. This technique is used with peer-to-peer networks that depend on the support of three concepts. These concepts are; the user-level semantic information, the QoS sensitive membership management and also the state-of-art single-channel adaptive streaming techniques. These concepts and techniques made an easy exploitation of the multi-channel streaming design. In Figure 3, below, illustrates the Multi-channel streaming technique.

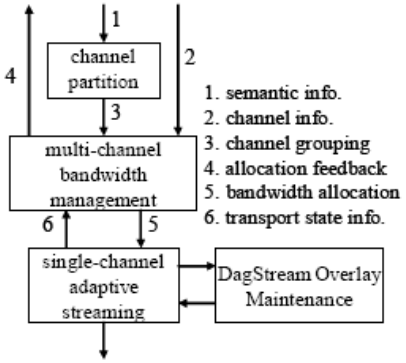

Fig. 3: Multi-Channel Adaptive Streaming (MCAS) technique [24].

The Multi-Channel Adaptive Streaming (MCAS) technique is classified into four module steps, as shown in Figure 3.6. These steps are; *Channel Partition, Multi-*

Channel Bandwidth Management, Single Channel Adaptive Streaming and DagStream Overlay Maintenance.

Each of these steps is discussed as follows:

1- *Channel Partition*: This module step is called the Top-most layer. At this layer, the user preference (e.g. the scoring mechanism) sends the semantic information towards the module of the channel partition. At this channel, the information will be fed. After that, priority groups are given to all channels that are determined to be partitioned with the fed information into these groups.
2- *Multi-Channel Bandwidth Management*: This is the Middle layer, where the channel information and the bandwidth status are taken by this step to make a bandwidth allocation for each channel. This allocation is dynamically being performed by this layer.
3- Single-Channel Adaptive Streaming: This step utilizes the bandwidth allocation to support both; the media adaption and the sender coordination.
4- DagStream Overlay Maintenance: This step controls the streaming module in the purpose of maintaining the parents and children peers of what and to where the media data will be streamed. At the same time, a feedback is sent to the upper layer. This sending will efficiently treat the dynamics of the bandwidth. For example, a special bandwidth allocation wouldn't be known when the peers leave. In other words, a notification must be performed for the module of the upper layer in order to make the bandwidth allocation with a certain updates.

3.4 PBR and QoS Control Routing for Multi-Channel Adaptive Streaming (PQMAS)

As explained in the previous technique (MCAS) technique, the main idea was to provide the viewers with an efficient protocol of channel service. According to this, our enhanced model combines more main significant concept services with the MCAS technique, provided that, our technique adds more policy rules in the PBR to manage the data packets being sent. All these are enhanced in order to provide a fully integrated service for the viewers (subscribers).

Our technique is called the *PBR and QoS Control Routing for Multi-Channel Adaptive Streaming (PQMAS) technique.* In Figure 4 below, illustrates our technique. The main concepts that were combine to the MCAS technique are; the Controlling Network Traffic (CNT), the Quality of Service (QoS) and the Policy-Based Routing (PBR). These concepts are essential at any routing technique in the networks.

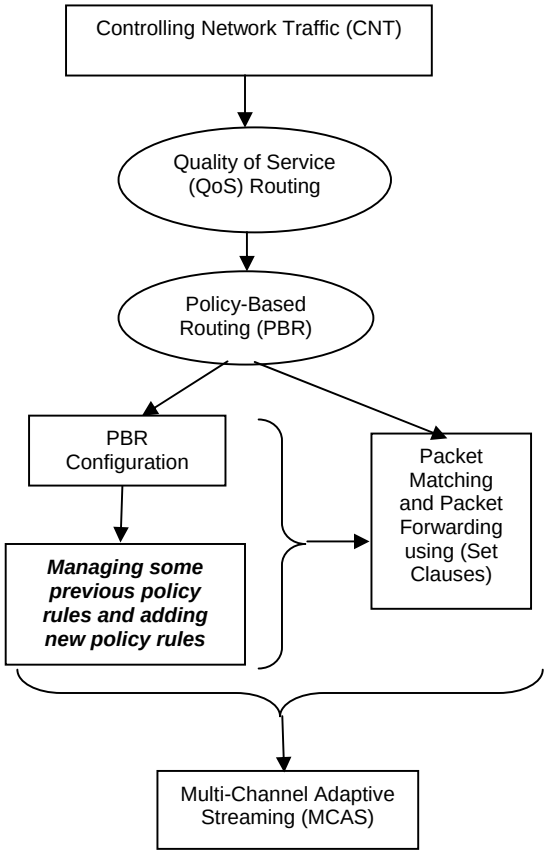

Fig. 4: The Proposed Enhanced Model Technique (PQMAS) Model Technique.

The PQMAS technique is classified into three main concept steps. These steps are; the Controlling Network Traffic (CNT), the Quality of Service (QoS) and the Policy-Based Routing (PBR). These concepts are essential at any routing technique in the networks. These steps are combined because they perform efficient tasks in serving the customers needs, in addition to that, these steps provide an integrated support for packet routings.

3.4.1 Controlling Network Traffic (CNT)

The traffic is classified by the network manager with the control of the Policy-based routing. This allowance depends on how the traffic will utilize the Access Control Lists (ACLs). As a next step, the IP precedence and the Type of Service (TOS) values are initialized, according to this, a defined classification will control the packets in the network [26].

Traffic is identified by the network manager when the policy-based routing contains the traffic that has been classified. The aim of this identification is to support the perimeter network that contains different classes of service. The next step is to let QoS be implemented, where; the whole classes of service are defined by the QoS in the core network. This definition depends on the utilization of certain techniques, such as, custom technique, priority technique and weighted fair queuing technique. Finally, in the core or backbone network, the classification of the traffic will be efficiently reduced at the whole interface of the WAN and the network will be with high performance [26].

3.4.2 Quality of Service (QoS) Routing

In general, when routing packets from source to destination, it is better to choose the shortest path and at the same time, taking into account, that there are enough bandwidth between the source and destination [25]. For example, notice the example in Figure 5, if we considered that between both nodes; A and C respectively, there is a traffic flow, the path between them won't be chosen (i.e. path A-B-C), although it is the shortest path. The reason of this is that there is no enough bandwidth (only 4M) to send these flows of packets. So, as a result, path A-D-E-C will be the suitable path to be chosen.

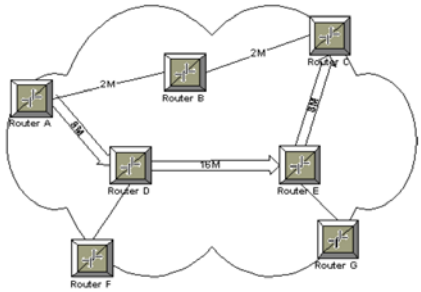

Fig. 5: QoS-Based Routing Example [25].

3.4.3 Applying Policy-Based Routing (PBR)

When performing any policy that will allow packets to be routed, this policy must be configured at first in order to take its place. As soon as, the PBR is configured in the network, the PBR must contain such rules to be involved in sending packets that will be controlled by these policy rules. In other words, no packets are sent from source to destination unless the configured PBR rules will grant these packets to be sent to as many destinations.

An application is included for PBR to interfere the packets for routing [26]. When routing the packets, they will arrive on the interface. As soon as they reach this interface, the PBR will be defined and enabled to route these packets. After that, in the enhanced packets filters, these packets are passed to these filters which are to be called the route maps. Packets will be forwarded or routed to next hop that is suitable for these packets by depending on the route map criteria [26].

3.4.4 PBR Configuration

PBR can be efficiently configured by performing the following steps as introduced in [32]:

1- First of all, a required policy will allow the route map to be defined and configured. This step is achieved by using the **route-map** command, for example, **route-map** [route-map name].

2- Now, here, the **match** statements are define and configured based on their route map. As an example of the route map is as:
match ip address [access-list number].

3- The new routing policy will be defined and configured by adding and utilizing the set commands. Here, many set commands can be taken into consideration for major purposes. There are orders on how to perform these sets, these orders are as follows:
set ip {precedence [*value_0-7* | *name*] | **tos** [*value_0-8* | *name*] }
set ip next-hop *ip_address*
set interface *interface_name*
set ip default next-hop *ip_address*
set default interface *interface_name*

4- Now, in the inbound interface, the policy router must be configured. To do so, the following interface command will be performed:
router (config-if)# **ip policy route-map** *route-map name*

Referring to step 2, the **match ip address** is used for performing a call for three important things which are; a standard, extended Access List (ACL), or expanded-range for Access List (ACL). Now, the **match length** is defined and configured also to make a matching with layer 3 packet length, which is in measured in bytes of size. This includes all the whole headers and trailers. The length of minimum and maximum packet must be entered. By depending on the packet size, the **match length** command will be utilized allow policy to route the flow of packets. In addition to that, small sizes or large ones of packets can be exploited to make a routing for traffic to a chosen network area.

3.4.5 Policy-Based Routing (PBR) Management Rules (Managing and Adding New Rules)

When the interface of the PBR receives the packets, an enhanced packet filters routes these packets into them. These kinds of filters are called the *Route Maps.* The policy is being managed and understood by depending on the use of the PBR that controls the route map [27]. A number of rules are being managed by the PBR route map. Each rule is expressed into statements (i.e. if, then). These statements are marked as *permit* and *deny.* These rule statements are three rules, which are in Figures 6, 7 and 8.

RULE 1 (Existing Rule):
If *(the route map was marked as* ***permit*** *and a packet* ***matches all*** *match statements)* ***then:***
The policy will route the packet using the set statements.
Else
If *(the route map was marked as* ***deny*** *and a packet* ***didn't match*** *all the match statements)* ***then:***
The packet is normally being forwarded to its destination.

Fig. 6: PBR Rule 1 (Existing Rule).

RULE 2 (Existing Rule):
If *(the route map was marked as* ***deny*** *and a packet* ***matches any*** *match statements)* ***then:***
The packet is not related to PBR and is normally forwarded.

Fig. 7: PBR Rule 2 (Existing Rule).

RULE 3 (Existing Rule):
If *(the route map was marked as* ***permit*** *and a packet* ***didn't match*** *any match statements)* ***then:***
The packets are sent back through the normal forwarding channels and destination-based routing is performed.

Fig. 8: PBR Rule 3 (Existing Rule).

In Figures 9 and 10, we introduce our new rules (Rule 4 and Rule 5) of the PBR. We classified our rules into 2 types; *General and Specific rules.* We refer to the previous three rules including our new rules (Rule 4 and Rule 5) as the *Specific rules.* The *General rules* will be also introduced afterwards (i.e. after proposing Rules 4 and 5). Note that, in Rules 1,2 and 3, there are, **permit** with **match all, deny** with **didn't match, deny** with **match any, permit** with **didn't match.** Now Rule 4, will consider **deny** with **match all.** Rule 5, will consider **permit** with **match any.**

RULE 4 (NEW RULE):
If *(the route map was marked as* ***deny*** *and a packet* ***matches all*** *match statements)* ***then:***
The policy will route the packet using the set statements.
After that, the packet is forwarded normally.

Fig. 9: PBR Rule 4 (NEW RULE).

RULE 5 (NEW RULE):
If *(the route map was marked as* ***permit*** *and a packet* ***matches any*** *match statements)* ***then:***
The policy will route the packet using the set statements.
After that, the packet will be also subjected to PBR and is normally forwarded.

Fig. 10: PBR Rule 5 (NEW RULE).

The both new rules are added to make a complement of the possibilities as been explained when using (permit and deny) and (match all, match any and didn't match). Note that, in the available rules (i.e. Rule1, 2 and 3) there are 4 probabilities when using the If-Statements for routing packets. Therefore, Rules (4 and 5) were proposed to be as a complement to these statements. When Rules 4 and 5 were introduced as a complement to there previous rules (Rules 1, 2 and 3), it is noticed that the answers after the If-Statement will be merged a kind of in between the answers of these previous rules.

There is an important notice that must be taken into consideration; the interface that receives the packets must have the determined PBR, not on the interface where the packet is started to be sent.

3.4.5.1 Packet Matching

In the IPv6, packets will be matched with the PBR by depending on the use of the **match IPv6 address** command through the route map of the PBR. The IPv6 Access Lists (ACL) has developed such criteria for matching the packet [27]. These are:

1- Input Interface.
2- Source IPv6 address by using a prefix list or a standard or extended access list (ACL).
3- Destination IPv6 address (standard or extended ACL).
4- Protocol (extended ACL).
5- Source port and destination port (extended ACL).
6- Differentiated services code point (DSCP) (extended ACL).
7- Flow-label (extended ACL).
8- Fragment (extended ACL).

By depending on the **length,** a matching between the packets will be performed. This is done by making a use of the **match length statement** through the route map that is to be certainly related in the PBR application tasks [27]. The **match IPv6 address** command contains criteria in order to make an evaluation for the match statements. Another evaluation is performed in the **match length** command. Hence, if the user uses both ACL and the length statement, the packet will be based on the ACL

match. After the packets are based on the ACL, the length match will be then a basic for these packets. At last, a routing policy is performed for just packets that make an access to ACL and the length statement [27].

3.4.5.2 Packet Forwarding Using Set Statement

A number of statements control the PBR through the packet of the IPv6 [27]. This is to help in routing packets to the destinations to where packets should be received. This control is performed in the route map of the PBR. Each of these statements gives the ability to the PBR to let the specified packets be forwarded to their destinations. The PBR itself controls these statements by making an evaluation to them. Moreover, these statements are orderly performed.

After the match clauses are performed for such certain tasks, a usage for any of these following statements will be efficiently achieved to perform packet routings [27]. These are:

1- *IPv6 next hop:* the next hop to where it should receive the packet. The Routing Information Base (RIB) should contain this next hop to where it should receive packets. A direct connection is performed for the RIB; as so, the RIB is to be considered as a global address of the IPv6. The set statement is ignored when the next hop is invalid.
2- *Output interface:* when determining an interface that receives packets in the PBR, a forwarding task is performed out from this interface. The IPv6 RIB must have an entry that is based on the address of the packet destination, provided that, the path set must contain the interface of the determined output interface. The set statement is ignored when the determined interface is invalid.
3- *Default IPv6 next hop:* also, this considered to be the next set to where it receives the packet. A global address of the IPv6 must be provided in here. When the packet destination contains unknown entry through the IPv6 RIB, this statement is the only to be utilized.
4- *Default output interface:* when determining an interface that receives packets in the PBR, a forwarding task is performed out from this interface. When the packet destination contains unknown entry through the IPv6 RIB, this statement is the only to be utilized.
5- *IP TOS (Type of Service):* in the IPv6 packets, a specification for the type of service is performed when specifying the value and keyword in these packets.
6- *IP precedence:* in the IPv6 packets, a specification for the IP precedence is performed when specifying the value and keyword in these packets.

These set statements commands can be used together with others when performing the routing operation. If the packets didn't match any type of the match criteria, then, to the destination-based routing process, the packets will be normally routed. If the packets failed to be routed to the destination-based routing process and also failed to perform a dropping for packets that didn't match any of these matching criteria, then the interface that was determined to be considered as a first interface will be now determined as the last list of the interface by depending on the set clause.

3.4.5.3 General Proposed Rules

In this section, the general rule is proposed. As was explained previously, a number of rules are being managed by the PBR route map. But here, a number of general rules are being managed by the *network manager* to manage the payment of the customers (subscribers) when receiving the service of packets to be routed. Therefore, these sections rules are called the general rules, where as, the previous rules was called the specific rules, since the previous ones works more as an infrastructure rules of the network. In other words, the previous rules was more related on how practically packets are routed to their destination by a configured PBR instead of generally concerning on the behavior of the payment customer's rules for how these packets were routed to serve them.

Now, each rule is expressed into statements (i.e. if, then), as was explained before. Here, these statements are marked as *paid* and *not paid.* More clearly, these new proposed rules indicate to the behavior of the customers pays when receiving any packet service from the company or network source. Note that the customer must pay on time duration (e.g. monthly) since a service is brought to him/her (i.e. every month). The new rule statements are three rules, which are in Figures 11 and 12.

RULE 1:
If *(a chosen customer's situation was* ***paid*** *for the previous month)* ***then:***
Send the packet to the destination to where it belongs to this customer

Fig. 11: Payment Rule 1 (NEW RULE).

RULE 2:
If *(A chosen customer's situation was* ***not paid*** *for the previous month)* ***then***
The customer is given more 3 days at the new month;
If *(The new month started and not yet exceeded 3 days)* ***then***
Send the packet to the destination to where it belongs to this customer;
Send a warning informing that the customer must pay very soon (between the three days);
Else
If *(The new month started and has exceeded 3 days)* ***then***
Cut the service of sending the packets to that customer that hasn't paid unless he pays;

Fig. 12: Payment Rule 2 (NEW RULE).

As a result of our analysis, adding the new *Specific* rules as a complement to the existing rules will improve more integrated services based on the Quality of Service (QoS) for high support and service to the customer's requirements. In addition, the complement rules will increase the performance of traffic balancing mechanism, since we use a broadcast network to send and receive the packets.

4. Conclusion

In this paper, we presented an enhanced model technique that controls the routing of a determined packet in the TV broadcasting under a policy rules management which is the Policy-Based Routing (PBR). Our method combines major significant concepts to have a fully integrated model. These concepts are Controlling Network Traffic (CNT), the Quality of Service (QoS) and the Policy-Based Routing (PBR). Moreover, new rules in the PBR were proposed over the existing rules and are categorized into two types of rules which are; Specific and General rules. The Specific rules indicate to the infrastructure of how packets are routed. The General rules indicate to the payment behavior of the subscribers when receiving their TV channels after the packets were either specifically routed or not from the previous rule type (Specific rules).

Acknowledgments

The authors would like to thank the Universiti Sains Malaysia (USM) for the research grant.

References

[1] J. S. Silva, S. Duarte, N. Veiga, and F. Boavida, "MEDIA – An approach to an efficient integration of IPv6 and ATM multicast environments," Universidade de Coimbra, Departamento de Engenharia Informatica, 2000.

[2] Super Internet Access Group, "Tech Info," July 2007, http://www.zytrax.com/tech/protocols/ipv6.html

[3] C. N. Lin, P. C. Tseng, and W. S. Hwang, "End-to-End QoS Provisioning by Flow Label in IPv6," In *proceedings of the 9th Joint Conference on Information Sciences*, 2006.

[4] P.D. Pezaros and D. Hutchison, "Quality of Service Assurance for the next Generation Internet," Computing Department, Faculty of Applied Science, Lancaster, UK, LA1 4YR, 2001.

[5] G. Huston, *Internet Performance Survival Guide: QoS strategies for multiservice networks:* Wiley Computer Publishing, 2000.

[6] "IPv6 features," [Online]. Available: http://technet2.microsoft.com/windowsserver/en/library/7dc20b9e-6538-429d-b222-81eb6b7fcdfb1033.mspx?mfr=true [Date Last Modified: 21/1/2005].

[7] J. Taplin, "The IPTV Revolution," Annenberg School for Communication, University of Southern California, 2005.

[8] G. Stattenberger, T. Braun and M. Brunner, "A Platform-Independent API for Quality of Service Management," Institute of Computer Science and Applied Mathematics, University of Bern, 2000.

[9] C. Bouras, A. Gkamas, D. Primpas, and K. Stamos, "Quality of Service Aspects in an IPv6 Domain," Research Academic Computer Technology Institute, Computer Engineering and InformatiCS Dept., 2004.

[10] F. Baumgartner, T. Braun, and P. Habegger, "Differentiated Services: A new approach for Quality of Service in the Internet," Institute of Computer Science and Applied Mathematics, University of Berne, Berne, Switzerland, 1998.

[11] Y.C. Hu and D.B. Johnson, "Securing Quality of Service Route Discovery in On-Demand-Routing for Ad Hoc Networks," *Proceedings of the 2nd ACM Workshop on Security of AD Hoc and Sensor Networks*, SANS'04, 2004, pp. 106-117.

[12] K. Sanzgiri, B. Dahill, B.N. Leviene, E. Royer, C. Shields, M. Elizabeth and B. Royer, "A Secure Routing Protocol for Ad Hoc Networks," *Proceedings of the 10th IEEE International Conference on Network Protocols*, ICNP'02, 2002, pp. 78-89.

[13] C.E. Perkins and E.M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, WMCSA'99, 1999, pp. 90-100.

[14] Y.C. Hu, A. Perrig and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Proceedings of the 8th Annual International Conference on Mobile Computing and Networking*, MobiCom, 2002, pp. 12-23.

[15] M.G. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," *Proceedings of the 1st ACM Workshop on Wireless Security*, WiSe, 2002, pp. 1-10.

[16] D.B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts," *Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications*, WMCSA, 1994, pp. 158-163.

[17] C. Bouras, A. Gkamas, D. Primpas and K. Stamos, "IPv6 QoS Testing on Dual Stack Network," *Proceedings of the AAA-Idea06*, 2006.

[18] J. Hwang and M.B.H. Weiss, "Cost/Benefit Tradeoff of Quality of Service Mechanisms in Integrated Services Networks," Telecommunication Program, University of Pittsburgh, Pittsburgh PA 15260, 1999.
[19] C.K. Chau, R. Gibbens and T.G. Griffin, "Towards a Unified Theory of Policy-Based Routing," *Proceedings of the 25th IEEE International Conference on Computer Communications*, Infocom, 2006, pp. 1-12.
[20] M. Liljenstam and D.M. Nicol, "ON-DEMAND COMPUTATION OF POLICY BASED ROUTES FOR LARGE-SCALE NETWORK SIMULATION", *Proceedings of the 2004 Winter Simulation Conference*, 2004, pp. 215-223.
[21] B.R. Smith and J.J.G.L. Aceves, "Efficient Policy-Based Routing without Virtual Circuits," *Proceedings of the 1st International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks*, QSHINE'04, 2004, pp. 242-251.
[22] Z. Avramovic, "POLICY BASED ROUTING IN THE DEFENSE INFORMATION SYSTEM NETWORK," *Proceedings of the Military Communications Conference*, MILCOM'92, 1992, pp. 1210-1214.
[23] E. Boschi and G. Carle, "Active Control Architecture implementing Policy-Based Routing," *Proceedings of the 10th International Conference on the Telecommunications*, ICT'03, 2003, pp. 53-57.
[24] J. Liang, B. Yu, Z. Yang and K. Nahrstedt, "A Framework for Future Internet-Based TV Broadcasting," *Proceedings of the International World Wide Web Conference, IPTV Workshop*, 2006, Edinburgh, Scotland, United Kingdom.
[25] W. Sun, "QoS/Policy/Constraint Based Routing," [Online]. Available: http://www.cse.ohio-state.edu/~jain/cis788-99/qos_routing/index.html [Date Last Modified: 12/1/1999].
[26] "Policy-Based Routing," [Online]. Available: http://www.cisco.com/warp/public/732/Tech/plicy_wp.htm
[27] "Implementing Policy-Based Routing for IPv6," [Online]. Available: http://cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_pbrv6.htm
[28] A.S. Tanenbaum, *Computer Networks*, 4th edition, New Jersey, USA, Prentice Hall PTR, 2003.
[29] Y. Cui, K. Nahrstedt, "Layered peer-to-peer streaming," *Proceedings of the 13th International Workshop on Network and Operating Systems Support for Digital Audio and Vidoe*, NOSSDAV, Monterey, CA, USA, June 2003.
[30] M. Hafeeda, A. Habib, B. Botev, D. Xu and B. Bhargava, "PROMISE: peer-to-peer media streaming using CollectCast," *Proceedings of the 11th ACM International Conference on Multimedia*, Berkeley, CA, USA, November 2003.
[31] O. Lotfallah, M. Reisslein and S. Panchanathan, "Adaptive bitstream switching of pre-encoded PFGS video," *Proceedings of the ACM Workshop on Advances in peer-to-peer multimedia streaming*, P2PMMS'05, Hilton, Singapore, November 2005.
[32] "CCIE Practical Studies: Configuring Route-Maps and Policy-based Routing," [Online]. Available: http://www.ciscopress.com/articles/article.asp?p=102092

Mohammad Azmi AL-Madi received the BSc. degree in Computer Information System (CIS) from AL-Zaytoonah University, Amman, Jordan in 2004. Currently he is a M.Sc. student at the School of Computer Sciences, Universiti Sains Malaysia (USM). His expected date of completion of M.Sc. is on the end of May 2008.

Rosnah Idrus is a Senior Lecturer and the Chairperson for Information Systems Programme of the School of Computer Sciences, Universiti Sains Malaysia (USM). She was selected for Asian Development Bank Visiting Scholar Program to IUPUI-Indianapolis, Indiana University Bloomington, Purdue University, and UCI-Irvine in 1994. Her R&D interests include virtual/digital library, integration of heterogeneous databases, knowledge-based systems, and social informatics. Her current research focus is in developing an ERP system for small and medium sized enterprises especially in managing capacity planning.

Sureswaran Ramadass received B.Sc. degree and Master of Science in Electrical/Computer Engineering from University of Miami, Coral Gables, Florida in 1987 and 1990, respectively, and PhD in Computer Science from Universiti Sains Malaysia in year 2000. Currently, he is an associate professor at School of Computer Sciences, USM. He is the director of National Advanced IPv6 (NAv6) Center, USM. His areas of concentration is Computer Networks and Data Communication, with special focus in: Multimedia Conferencing Systems and Multimedia Networks, Real-Time Network Monitoring, Network Security and IPv6. He is currently the Director of Network Technology Area of APAN.

Rahmat Budiarto received B.Sc. degree from Bandung Institute of Technology in 1986, M.Eng, and Dr.Eng in Computer Science from Nagoya Institute of Technology in 1995 and 1998 respectively. Currently, he is an associate professor at School of Computer Sciences as well as the deputy director of National Advanced IPv6 (NAv6) Center, USM. His research interest includes IPv6, network security, Intelligent Systems. He was chairman of APAN Security Working Group.