

ENFORCEMENT IN A TELECOMMUNICATION NETWORK

TECHNICAL FIELD OF THE INVENTION

5 The present invention relates generally to telecommunication networks, and, more particularly, to enforcement operations to control quality-of-service (QoS) in a packet-based telecommunication network.

BACKGROUND ART

10 In a rapidly changing telecommunications marketplace, companies can capitalize on the growing opportunities by introducing value-added services to customers seeking more reliable and economical telecommunications services. The tremendous growth in network infrastructure and corresponding growth in Internet Protocol (IP) traffic has resulted in the use of IP as a platform for new
15 telecommunications services that take advantage of voice and data convergence. Examples of new services include video communications, Voice over IP (VOIP), video/audio conferencing, video-on-demand, on-line gaming, etc.

 Because of such growth, Quality-of-Service (QoS) is becoming increasingly important to ensure high-quality transport within the network infrastructure, which
20 includes controlling one or more of the following:

- Service availability, such as the reliability of the user's connection to the Internet Service.
- Delay (also called latency), such as the time interval between transmitting and receiving packets.
- 25 • Delay variation or jitter, which refers to the variation in time duration between all packets in a stream taking the same route.
- Throughput, which is the average or peak rate at which packets are transmitted.
- Packet loss rate resulting from congestion that is the maximum rate
30 at which packets can be discarded during transfer through a network.

 Figure 1 shows an example of a packet-based telecommunication network 10, which in this case is an IP network. The IP network of a generic Telecommunication (TLC) Service Provider (SP) typically includes a backbone

network 12 connecting together two or more access networks, such as shown at 14, 16. Access network 14 is generally made of layer 1- or layer 2-type access/aggregation nodes 20, connecting a number of subscribers 18. Through the above access network, a subscriber can communicate with other subscribers on the same access network or gain access to the backbone network for communications outside the local area. The subscribers 18 can take a variety of forms including a single home user, a company with one or more networks, a generic network device (e.g. application or content server), etc. Likewise, access network 16 has subscribers 22. The access/aggregation nodes 20, 24 may use different technologies to connect the subscribers, such as SDH/Sonet, WDM, Ethernet, Frame Relay, xDSL, etc. Additionally, the above access/aggregation nodes 20, 24 may be provided by different vendors. The access/aggregation nodes 20, 24 communicate with the backbone network 12 through edge routers 30. The backbone network 12 includes a plurality of core routers 32, for providing routing paths generally used in long-distance communication. Both edge and core routers are generally layer 3-type devices.

Figure 1 is a simplified illustration wherein only a small number of edge routers 30 and core routers 32 are shown, but the backbone network is generally a nationwide network and may include many thousands of core and edge routers. Similarly, although only two access networks 14, 16 are shown, there generally are many access networks connected to the backbone 12 in the IP network 10.

There are a number of known techniques for handling QoS in an IP network. IP networks are traditionally based on a best effort approach for delivery of packets, wherein all transmissions or "flows" across the network are treated independently of their characteristics (e.g., source/destination pair, application, etc.). But this solution is insufficient for real-time applications, such as remote video, multimedia conferencing, visualization, and virtual reality. Before such real-time applications can be broadly used, the IP infrastructure has to evolve in order to support QoS functionality, which provides some control over the main quality parameters (such as throughput, end-to-end packet delays, jitter, etc.).

One proposed solution to this problem is called Differentiated Services (DiffServ). DiffServ is based on a classification of the flows that enter the network. Based on that classification, each packet is marked with a code that defines the class

to which it belongs. On each network node, a policy called PHB (Per Hop Behaviour) is defined for each class, specifying the treatment experienced by all packets belonging to that class, crossing that node. In order to support QoS guarantees with DiffServ, it is necessary to guarantee that the total amount of traffic injected for each class doesn't exceed the available resources. As an extension to the basic DiffServ model, centralized agents called bandwidth brokers that receive user requests and that manage the allocation of network resources have been proposed. The bandwidth brokers authenticate the requestor's credentials, check the availability of network resources, update the resource databases, and configure the network nodes to setup the communication (performing the so-called enforcement step). The DiffServ solution is focused on solving problems for backbone networks, rather than access networks. Access networks present peculiar characteristics, as they may differ from backbone networks, in terms of topology and technology. As a result, the DiffServ solution with bandwidth brokers it is not optimized for access networks.

Moreover, access areas can be significantly different also from each other in terms of implementation technology (xDSL, ATM, GBE, etc.). Each implementation technology has its own characteristics, which make it difficult to create a unified architecture according to all the parameters (bandwidth, interfaces, etc.) necessary for managing and controlling quality of service and consequently performing admission control and enforcement operations. Additionally, the different technologies create problems tracking allocated and available resources. Unlike in a backbone network, configuration normally takes place on parameters more closely tied to physical aspects than to the TCP/IP world. Solutions exist which use centralized entities related to access networks in order to deal with requests (e.g. for bandwidth usage) coming from users or application servers and accordingly configure network devices setting policies for traffic conditioning. These solutions typically analyze one particular kind of access network technology and structure, like the Network Resource Controller (NRC) defined within the Digital subscriber Line Forum (DSL Forum) or the Policy Decision Function (PDF) described within the 3rd Generation Partnership Project (3GPP).

A specific solution, inspired to a DiffServ model with bandwidth brokers, called QMTool, is proposed in the paper "*On providing a Dynamic QoS*

Management system for IP Networks”, by L.Dimopoulou et al., Proceedings of 10th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2002), Split & Dubrovnik (Croatia), Ancona & Venice (Italy), October 8-11, 2002, which describes a platform independent of the underlying

5 technologies or vendor-specific equipment. A three-layer approach is described. The lower layer is responsible for the direct communication with managed objects (e.g. routers, workstation, servers). The second layer processes the data provided by the lower layer. Finally, the upper layer serves as a front-end tool facilitating the interaction with a network operator. A Resource Control Layer (RCL) is used as a

10 distributed bandwidth broker and includes a Resource Control Agent (RCA), an Admission Control Agent (ACA) and the End-User Application Toolkit (EAT). The RCA is mainly responsible for the management of network resources within an administrative domain. The ACA is mainly responsible for user authentication and authorization, reservation handling, and flow admission control. The EAT forwards

15 reservation requests from the users to the ACA.

Like the shortcomings of other QoS technologies, the QMTool does not provide admission control and enforcement over the access networks. Instead the focus is only on the backbone network.

For the QoS enforcement step, there is a problem in that there are many

20 vendors, which results in different apparatuses, different configuration interfaces, and different protocols, together with different Layer 2 and Layer 3 technologies. There is industry support for various standardized protocols, such as a variation of the Megaco/H.248 protocol, the Gate Control Protocol (GCP), Common Open Policy Service with Policy Provisioning (COPS-PR), etc. But despite the various

25 possible solutions, there still does not exist a solution that allows QoS enforcement on a network in a unique and standardized way. Additionally, the various protocols such as COPS and GCP are not well supported by various vendors of IP apparatuses. Typically it is possible to access network elements through management protocols such as Simple Network Management Protocol (SNMP),

30 Telnet (Command Line Interface - CLI), Secure Shell (SSH) not specifically oriented to QoS management. Thus, there does not exist a single QoS-enforcement interface that can act with the wide variety of network apparatuses because such

apparatuses have many interfaces that need to be acted upon in order to effectuate enforcement.

US patent application 2002/0181462 A1 describes a system for offering QoS for transmissions through different IP networks. The reference context is in IP
5 Multimedia Subsystem (IMS) networks examined in the framework of Qbone in regard to coordinating bandwidth requisites between domains by using bandwidth brokers. The role of access areas is not addressed, and the solution seems to be focused only on COPS without regard to other protocols.

US patent application 2004/0039803 A1 describes a policy-based
10 management system for carrying out enforcement of QoS through rules to be activated on network apparatuses. It modifies the classic two-level system of the Policy-Based-Management (PBM) model, introducing a layer of software entities called Policy-Enforcement-Agent (PEA), inserted between the PDPs (policy decision points) and the PEPs (policy enforcement points), and “responsible for
15 capturing a policy rule in flight and translating the policy rule to actual policy enforcement action executable at a network node”. Still, enforcement control over the access networks is not addressed and the solution seems to be focused only on COPS.

Thus, the prior art lacks a solution for allowing adequate QoS control over
20 an end-to-end transmission in a packet-based telecommunications network. In particular, the prior art lacks an adequate solution that provides enforcement control covering both the backbone network and the access networks, managing with a unified approach the different interfaces available on network devices.

25 OBJECT AND SUMMARY OF THE INVENTION

The present invention therefore provides a method and system for performing QoS enforcement in a packet-based network, such as an IP network, that overcomes the shortcomings of the prior art.

According to the invention, a method and a system are disclosed according
30 to enclosed claims to perform enforcement on a packet-based network.

The IP network of a TLC Service Provider (SP) generally includes a backbone network coupled between at least two access networks. When a first user on a first access network wants to communicate with a second user located on a

different access network, a request is made to a quality server whether network resources are available. The quality server monitors the networks and if resources are available invokes an enforcement portion of the quality server to perform the configuration of network apparatuses associated with the users.

5 In one embodiment, the enforcement portion uses a two-tier approach wherein an enforcement module interacts with a mediation layer. The mediation layer is a software component, inserted between the enforcement module and the Network elements, whose main function is to adapt generic requests to configure QoS operations into specific commands executable on Network apparatuses. The
10 mediation layer provides an Application Programming Interface, composed by a set of software functions (API calls), used by the enforcement module as a means for providing access to the network elements QoS capabilities. The mediation layer is made up of a set of Resource Proxies (RPs), which are software entities used for controlling and managing access to network elements.

15 By activating the API, making specific API calls, the enforcement module directs resource proxies within the mediation layer to execute a desired workflow within a workflow repository. In this way, the resource proxies perform the necessary configuration steps for each network apparatus.

20 BRIEF DESCRIPTION OF THE DRAWINGS

For a better understanding of the present invention, a preferred embodiment, which is intended purely by way of example and is not to be construed as limiting, will now be described with reference to the attached drawings, wherein:

Figure 1 is a diagram of a prior-art telecommunications network including at
25 least two access networks connected through a backbone network.

Figure 2 is a block diagram of a quality server according to the invention for controlling QoS on the access and backbone networks of Figure 1.

Figure 3 is a detailed exemplary system showing the enforcement control portion of the quality server of Figure 2 as a two-layer approach including an
30 enforcement module and a mediation layer.

Figure 4 is a more detailed diagram of the mediation layer of Figure 3.

Figure 5 is a flowchart of a method for performing enforcement.

Figure 6 is a more detailed flowchart of the method of Figure 5.

Figure 7 is a flowchart of a method used by resource proxies for configuring network apparatuses and shows an example of operating steps contained within a generic workflow.

Figure 8 shows of a schematic representation of enforcement primitives.

5

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

Referring to Figure 2, a system 40 is shown having a quality server 42 with a portion 44 for interfacing with users, an admission control portion 46, and an enforcement portion 48. The portion 44 receives a user request to connect a first user on a first access network with a second user on a second access network. The user can take a variety of forms including a single home user, a company with one or more networks, a generic network device (e.g. application or content server), etc. The admission control portion 46 monitors the network and is responsible for determining whether sufficient resources are available to handle the user's request. If sufficient resources are available, the admission control portion 46 signals the enforcement portion 48, and upon receiving a positive response from the enforcement portion, sends a positive response to the portion 44 for communicating the result to the user. The enforcement portion 48 configures the resources in the network 10 by performing enforcement on each of the access networks 14, 16 and the backbone network 12 (as shown at 50, 52, 54). The user interface portion 44 and the admission control portion 46 will be discussed only briefly. Rather, the focus of the present application is on the enforcement control portion 48.

Figure 3 shows an example of the quality server 42 in detail. The portion 44 for interfacing with users is shown as a mapping module and can receive user requests either directly as shown at 60 or indirectly through intermediate elements 62, as shown by path 64. The intermediate elements may take a variety of forms but are shown in this example as a service portal 66 and a service proxy/server 68.

The admission control portion 46 is responsible for determining the availability of resources within the access areas related to users and the backbone network.

As previously mentioned, a positive result from checks performed on different access and backbone networks will result in an activation of the

enforcement module 48 and then in a positive response to the user whether non errors occur during enforcement operations.

The enforcement portion 48 is a two-tier structure including an enforcement module 100 as a top layer, and a mediation layer shown generally at 102. The enforcement module 100 is responsible for translating high-level requests (grouped into the Enforcement Module Interface 103 (EMI)) coming from the admission control subsystem 46 into API calls (grouped in 105 as a Network Proxy Enforcement Interface (NPEI)) for communication with the mediation layer 102.

Before performing the API calls, the enforcement module 100 communicates with a network inventory 104, which is a database containing information on the network apparatuses. This database 104 assists in identifying the proper resource proxy modules associated with the user request, as explained more fully below.

The mediation layer 102 includes a resource proxy interface shown as multiple resource proxies 106 labelled RP1 through RPn, wherein n indicates the number of devices to be managed or a part of them. Thus, a class implementing the resource-proxy interface sits between the enforcement module 100 and the network resources or apparatuses to simplify the task of configuring the network apparatuses by rendering uniform the way the enforcement module 100 performs operations on network devices.

The resource proxies 106 communicate with a workflow repository (WFR) 108 in order to configure the network apparatuses. A workflow is a logical sequence of steps to complete a task, whose execution is based on the dependencies between steps. One step may consist of a set of instructions or commands that are necessary to be sent to the network apparatus through one or more of the Protocol Adapters (e.g., Telnet, COPS, Simple Network Management System (SNMP) Adapter, etc.) and that manage the various protocols. Thus, an API call includes a request for execution of a given workflow and the necessary parameters for executing it. By using the workflow repository 108, the various resource proxies 106 carry out the defined operations on various network apparatuses using the interfaces/protocols (SNMP, COPS, Junoscript, etc.). Although many different types of protocols are used, Figure 3 designates the communication between the

resource proxies 106 and the network apparatuses generically through a so-called Network Element Interface (NEI) shown at 110.

Figure 4 shows further details of the mediation layer 102, which includes the resource proxies 106. The resource proxies are software elements used for controlling and managing access to the objects that they control, which in this specific case are network elements. The resource proxies 106 communicate with the enforcement module 100 through specific APIs. The APIs may provide functions with added value, such as

- transactionality (which allows to group different actions/commands in one single logical operation in order to be executed as one single order with an “all or nothing” paradigm that, if an error occurs, returns the device to the prior state),
- rollback (which is a command to return to a previous state), and
- prioritization of the requests.

The resource proxies also include an internal process engines (PE) 120 for carrying out their own functions and executing the workflows. By using the process engines 120, the resource proxies 106 can manage the dependencies between the steps of a workflow and have access to various protocol adapters 121, such as Telnet 122, SNMP 124, COPS 126, and whatever other protocol adapters are desired, such as shown generically at 128. Using these protocol adapters 121, the resource proxies 106 can communicate with any desired network apparatus in the access networks 14, 16 and the backbone network 12.

Figure 5 is a flowchart of a method for performing enforcement of network apparatuses. In process block 140, a request is received to enforce network apparatuses on two or more access networks, such as 14, 16, and a backbone network 12. For example, the request may be received through the EMI 103 from the admission control subsystem 46. In process block 142, the enforcement module 100 activates two or more API, which implies activating two or more API calls 105, to direct (i.e., to instruct) resource proxies 106 within the mediation layer 102 to perform enforcement functions. In response to the API call and parameters associated therewith, each resource proxy 106 that receives the API call accesses the Workflow Repository (WFR) 108 to perform the necessary configuration of the network devices. In process block 144, the network apparatuses are programmed or configured using the mediation layer 102.

Figure 6 shows a more detailed flowchart for programming the network apparatuses. In process block 150, a request is received by the enforcement module 100 from the admission control subsystem 46 to enforce network apparatuses. The request generally contains one or more of the following:

- 5 a) The type of request (e.g., end-to-end enforcement, enforcement operating only in access networks, or removal of previous enforcement; this information is typically implicit in the requested method).
- b) The identifiers of the apparatuses along the path involved in the request on which it is necessary to perform operations of QoS Enforcement.
- 10 c) The information on quality handling that is desired (e.g., input bandwidth, output bandwidth, class of service, DiffServ Code Point (DSCP), etc.).

In process block 152, the enforcement module 100 identifies the resource proxies associated with the network apparatuses. To accomplish this, the enforcement module 100 accesses the network inventory 104 to identify
15 information on the apparatuses concerned and to determine the resource proxies 106 assigned for the management of the specific apparatuses.

In process block 154, the enforcement module 100 generates the necessary API calls for the identified resource proxies. To accomplish this, the enforcement module 100 first identifies the workflows to be executed to meet the requests of
20 QoS Enforcement. Next, the enforcement module 100 composes appropriately and then activates, in parallel or sequentially, a series of API calls for the Resource Proxies previously identified.

In process block 156, each resource proxy 106 that is associated with an API call, accesses the workflow repository 108 in accordance with the API. Thus, the
25 various resource proxies 106, by accessing the workflow repository 108, carry out the operations on the various apparatuses using the interfaces/protocols (SNMP, COPS, Junoscript, etc.) necessary to communicate with the apparatuses.

In process block 158, the resource proxies 106 send a reply to the enforcement module 100 with the outcome of the operations. Included in the reply
30 may be the identifiers of the request that are useful for cancellation of reservations.

Then the enforcement module 100 sends the outcome of the operations of QoS Enforcement to the Admission Control Subsystem 46 which will send a response to the user.

Figure 7 shows a further detailed flowchart of a method performed by the mediation layer 102. Specifically, Figure 7 shows an example of operating steps contained within a generic workflow so as to highlight the aspects linked to rollback and transactionality. In process block 170, the input parameters are checked for consistency. In process block 172, the functions associated to the various protocol adapters of interest are loaded. Next, the resource proxy accesses the apparatus (process block 174) and performs locking of the configuration (process block 176). Some protocol adapters do not enable the locking operation. Therefore, the resource proxy makes available the logic functionality if needed. In process block 178, the resource proxy executes commands on the network apparatus using the required protocol adapters. The type of operations to be executed is detailed in the workflow. In decision block 180, a check is made whether the commands were properly carried out. If yes, a check is made in decision block 182 whether more commands are to be executed. If yes, the method continues with process block 178. Returning to decision block 180, if a command was not properly carried out, an "undo" command can be performed at block 186. This returns the apparatus to its previous state. After decision block 182, if no more commands are to be executed, then the resource proxy performs configuration unlocking (process block 184) and once it is disconnected from the apparatus (process block 188) creates the appropriate message (error/success) to be sent to the requesting enforcement module (process block 190).

The following is a description of possible EMI 103 and NPEI 105 interfaces:

Detailed examples of EMI

For the purposes of the QoS server it is desirable to configure via enforcement two different types of rate limiting: one, which could be defined as End-to-End, applies to a particular traffic route (source/destination); and another, which could be defined as operating only in Access, applies to all the traffic forming part of a given class of service irrespective of its source/destination.

The EMI interface may, then, consist of two distinct primitives: E2EEnforcement and AccEnforcement, which manage the operations connected to control of the bandwidth for the flows accepted, in the case of requests of end-to-end reservation and in access, respectively.

The interface of the enforcement module consequently offers the following primitives:

EMI.E2EEEnforcement: used for implementing the operations of enforcement associated to handling of the requests for management of the end-to-end QoS;

5 EMI.ACCEEnforcement: used for implementing the operations of enforcement associated to handling of the requests of management of the QoS in access;

EMI.RemoveEnforcement: used for removing the configurations regarding operations of enforcement executed.

10

Said primitives may have the following parameters:

E2EEEnforcement:

15 ID1-- Identifier of the apparatus 1 on which to execute the operation of enforcement

 ID2--Identifier of the apparatus 2 on which to execute the operation of enforcement

 ...

20 Idn--Identifier of the apparatus N on which to execute the operation of enforcement

 InProfile_CoS--Class of service (CoS) of the compliant traffic (within the guaranteed bandwidth)

 OutProfile_CoS--CoS of the traffic that exceeds the guaranteed bandwidth (but falls within the maximum bandwidth) (opt.)

25 Bandwidth_Limits--Limits of guaranteed bandwidth (committed rate in Figure 8) and maximum bandwidth (opt.)

 Direction--Direction of the flow

 Source_Host--IP address of the source (opt.)

 Destination_Host--IP address of the destination (opt.)

30 Source_site--Source-site code (opt.)

 Destination_site--Destination-site code (opt.)

 Transport--Transport protocol used by the media (opt.)

 source_port--Source port (opt.)

 destination_port--Destination port (opt.)

35 Handler--Identifier of the request

 Flow-ID--Identifier of the flow in the context of the request.

ACCEEnforcement:

40 ID1-- Identifier of the apparatus 1 on which to execute the operation of enforcement

ID2--Identifier of the apparatus 2 on which to execute the operation of enforcement

...

5 Idn--Identifier of the apparatus N on which to execute the operation of enforcement

InProfile_CoS-- Class of service (CoS) of the compliant traffic (within the guaranteed bandwidth)

OutProfile_CoS--CoS of the traffic that exceeds the guaranteed bandwidth (but falls within the maximum bandwidth) (opt.)

10 Bandwidth_Limits--Limits of guaranteed bandwidth (committed rate in Figure 8) and maximum bandwidth (opt.)

Direction--Direction of the flow

Handler--Identifier of the request

Flow-ID--Identifier of the flow in the context of the request.

15

RemoveEnforcement:

Status--Outcome of the operation,

Handler--Identifier of the request

Flow-ID--Identifier of the flow in the context of the request (opt.)

20

Detailed examples of NPEI and mapping between EMI and NPEI

The primitives of the EMI 103 interfaces are then mapped by recalling primitives at the interface level 105 directed to the Resource Proxies.

25 Described below are the primitives/operations (designated by the letters A, B, C, D, E) made available by the Resource Proxies at the 105 interface. The effect of the execution of said operations on the apparatuses, in terms of handling of the traffic is shown in Figure 8.

The mapping between the primitives of the EMI interface and those of the NPEI interface is represented in the following tables:

30

Parameters of the E2EEnforcement primitive	A Single value of CoS indicated (InProfile_CoS)	A Double value of CoS indicated (InProfile_CoS + OutProfile_CoS)
A Single value of bandwidth indicated (Guaranteed bandwidth)	<i>Recalls the primitive A on the NPEI</i>	Case not handled
A Double value of bandwidth indicated (also Maximum Bandwidth)	Not Admissible	<i>Recalls the primitive D on the NPEI</i>

Parameters of the AccEnforcement primitive	A Single value of CoS indicated (InProfile_CoS)	A Double value of CoS indicated (InProfile_CoS + OutProfile_CoS)
A Single value of bandwidth indicated (Guaranteed bandwidth)	<i>Recalls the primitive B on the NPEI</i>	<i>Recalls the primitive C on the NPEI</i>
A Double value of bandwidth indicated (also Maximum Bandwidth)	Not Admissible	<i>Recalls the primitive E on the NPEI</i>

5 Primitives of the NPEI

A) Set_Single_BW_Limit_E2E (Interface(interface_ID), to({ingress|egress}), bitrate(Int), burst_size (Int), CoS(Int), source_networks (IP_Addr_Prefix_List), destination_networks (IP_Addr_Prefix_List)).

- 10
- API description: This acts on a physical/logical interface, at an IP level, configuring an instance of rate limiting (e.g., Cisco CAR) for setting a bandwidth limitation, with discard of the traffic that is not compliant. The parameter “to” defines whether the functionality is to be applied at input to or at output from the interface. The flow of
- 15
- traffic on which the rate limiting is applied is defined by the class of service (value of CoS marking), by the IP source address or by the IP source prefixes and by the IP destination address (i.e., by whether it belongs to one of the networks specified by the parameter “destination_networks”, in terms of address prefixes, i.e.,
- 20
- address/mask).
- Types of apparatus on which it will act: (CE Router, PE Router, Network Access Server (NAS), Switch Ethernet Multilayer, Digital Subscriber Line Access Multiplexer (DSLAM) with IP functionality)
 - Elements of the apparatus on which it will operate: physical
- 25
- interface, logic interface, Access Control List (ACL), filtering options
- Set of operations to be carried out on said entities:

1. Define a filter (e.g., ACL) to identify the flow to which to apply the rate limiting.
 2. Define the value of bandwidth and burst to which to limit the traffic of the flow identified.
 - 5 3. Define the discard action for the traffic that is not compliant.
- Return result/value: Outcome of the operation (Status) and identifier (Handler) of the instance of policing configured.

10 B) Set_Single_BW_Limit_Access_Drop (Interface(interface_ID, to({ingress|egress}), bitrate(Int), burst_size (Int), CoS(Int)).

- API description: This acts on a physical/logic interface, at an IP level, configuring an instance of rate limiting for setting a bandwidth limitation, with discard of the traffic that is not compliant. The parameter “to” defines whether the functionality is to be applied at input to or at output from the interface. The traffic flow on which the rate limiting is applied is defined by the class of service (value of CoS marking).
- 15 • Types of apparatus on which it will act: (CE Router, PE Router, NAS, Switch Ethernet Multilayer, DSLAM with IP functionality)
- 20 • Elements of the apparatus on which it will operate: physical interface, logic interface, ACL, filters
- Set of operations to be carried out on said entities:
 1. Define a filter (e.g., ACL), on the basis of the CoS marking, to identify the traffic to which to apply the rate limiting.
 - 25 2. Define the value of bandwidth (and of burst) to which to limit the traffic of the flow identified.
 3. Define the discard action for the traffic that is not compliant.
- Return result/value: Outcome of the operation (Status) and identifier (Handler) of the instance of policing configured.
- 30

C) Set_Single_BW_Limit_Access_Re-mark (Interface(interface_ID), to({ingress|egress}), bitrate(Int), burst_size (Int), CoS(Int), exceed_CoS(Int)).

- 5 ▪ API description: This acts on a physical/logic interface, at an IP level, configuring an instance of rate limiting (e.g., Cisco CAR) for setting a bandwidth limitation, with rewriting of the CoS field for the traffic that is not compliant. The parameter “to” defines whether the functionality is to be applied at input to or at output from the interface. The flow of traffic on which the rate limiting is applied is defined by the class of service (value of CoS marking).
- Types of apparatuses on which it will act: (CE Router, PE Router, NAS, Switch Ethernet Multilayer, DSLAM with IP functionality)
- 10 ▪ Elements of the apparatus on which it will operate: physical interface, logic interface, ACL
- Set of operations to be carried out on said entities:

 1. Define a filter (e.g., ACL), on the basis of the CoS, to identify the flow to which to apply the rate limiting.
 - 15 2. Define the value of bandwidth (and of burst) to which to limit the traffic of the flow identified.
 3. Define the discard action for the traffic that is not compliant.
- Return result/value: Outcome of the operation (Status) and identifier (Handler) of the instance of policing configured.

20

D) Set_Double_BW_Limit_E2E (Interface(interface_ID),
 to({ingress|egress}), committed_bitrate(Int), committed_bitrate_burst(Int),
 maximum_bitrate(Int), maximum_bitrate_burst(Int), CoS(Int),
 source_networks(IP_Addr_Prefix_List), destination_networks
 25 (IP_Addr_Prefix_List), exceed_CoS(Int)).

- 30 • API description: This acts on the IP level, configuring two instances of rate limiting in cascaded fashion, for setting a limitation on two distinct values of bandwidth, on the physical/logic interface. Upon overstepping of the first threshold (defined by the combination of the parameters “committed_bitrate”/“committed_bitrate_burst”) the traffic is re-marked with the value specified by “exceed_CoS”. Said traffic is subjected to the second control of rate limiting

5 (“maximum_bitrate”/”maximum_bitrate_burst”). The traffic that is not compliant also with this second control is discarded. The parameter “to” defines whether to apply the functionality at input to or at output from the interface. The flow of traffic on which the rate limiting is applied is defined by the class of service (value of CoS marking), by the IP source address or by the IP source prefixes and by the IP destination address (i.e., by whether it belongs to one of the networks specified by the parameter “destination_networks”).

- 10 • Types of apparatus on which it will act: (CE Router, PE Router, NAS, Switch Ethernet Multilayer, DSLAM with IP functionality)
- Elements of the apparatus on which it will operate: physical interface, logic interface, ACL
- Set of operations to be carried out on said entities:
 - 15 1. Define a filter (e.g., ACL) to identify the flow to which to apply the rate limiting.
 2. Define a first instance of rate limiting corresponding to the values of bandwidth and of burst specified for the first threshold, with action of re-marking of the traffic in excess and passage to the subsequent instance of rate limiting.
 - 20 3. Define a second instance of rate limiting corresponding to the values of bandwidth and of burst specified for the second threshold (“maximum_bitrate”), with action of discard of the traffic that is not compliant.
- Return result/value: Outcome of the operation (Status) and identifier (Handler) of the instance of policing configured.

25 E) Set_Double_BW_Limit_Access (Interface(interface_ID), to({ingress|egress}), committed_bitrate(Int), committed_bitrate_burst(Int), maximum_bitrate(Int), maximum_bitrate_burst(Int), CoS(Int), exceed_CoS(Int))

30

- API description: This acts on the IP level, configuring two instances of rate limiting in cascaded fashion, for setting a limitation on two distinct values of bandwidth, on the physical/logic interface. Upon

overstepping of the first threshold (defined by the combination of the parameters "committed_bitrate"/"committed_bitrate_burst") the traffic is re-marked with the value specified by "exceed_CoS". Said traffic is subjected to the second control of rate limiting ("maximum_bitrate"/"maximum_bitrate_burst"). The traffic that is not compliant also with this second control is discarded. The parameter "to" defines whether to apply the functionality at input to or at output from the interface. The flow of traffic on which the rate limiting is applied is defined by the class of service (value of CoS marking).

- Types of apparatus on which it will act: (CE Router, PE Router, NAS, Switch Ethernet Multilayer, DSLAM with IP functionality)
- Elements of the apparatus on which it will operate: physical interface, logic interface, ACL
- Set of operations to be carried out on said entities:
 1. Define a filter (e.g., ACL) to identify the flow to which to apply the rate limiting.
 2. Define a first instance of rate limiting corresponding to the values of bandwidth and of burst specified for the first threshold, with action of re-marking of the traffic in excess and passage to the subsequent instance of rate limiting.
 3. Define a second instance of rate limiting, corresponding to the values of bandwidth and of burst specified for the second threshold ("maximum_bitrate"), with action of discard of the traffic that is not compliant.
- Return result/value: Outcome of the operation (Status) and identifiers (Handler) of the instance of policing configured.

F) Clear_BW_Limit (Identifier(handle))

- API description: This removes an instance of rate limiting previously configured; said instance is specified by means of the identifier (handle) assigned at the moment of the configuration.
- Types of apparatus on which it will act: (CE Router, PE Router,
5 NAS, Switch Ethernet Multilayer, DSLAM with IP functionality)
- Elements of the apparatus on which it will operate: physical interface, logic interface
- Set of operations to be carried out on said entities:
 1. Remove the instances of rate limiting configured.
 - 10 2. Remove the filter (ACL) previously configured to define the flow to be subjected to rate limiting.
- Return result/value: Outcome of the operation (Status).

15 It is clear that numerous modifications and variants can be made to the present invention, all falling within the scope of the invention, as defined in the appended claims.

CLAIMS

1. A method of performing operations to control quality-of-service enforcement of network apparatuses in a packet-based telecommunication network,
5 characterized by:

receiving a request to configure apparatuses on the packet-based telecommunication network;

in response to the request, activating one or more application program interfaces (API) that direct a mediation layer to perform the configuration of
10 quality-of-service operations on said apparatuses; and
configuring said apparatuses using the mediation layer.

2. The method of claim 1, wherein the mediation layer includes a plurality of resource proxies, each of said resource proxies being associated with a respective
15 apparatus of said telecommunication network or with part of it.

3. The method of any of the preceding claims, wherein the packet-based telecommunication network comprises a first and a second access networks and wherein configuring said apparatuses comprises defining a connection path between
20 said first and second users.

4. The method of claim 3, wherein the mediation layer includes a plurality of resource proxies and the method further includes determining which resource proxies are associated with said apparatuses.
25

5. The method of claim 3 or 4, wherein the packet-based telecommunication network (10) comprises a backbone network interposed between said first and second access networks, wherein at least one of said apparatuses is located in said backbone network.
30

6. The method of any preceding claims, wherein at least two of the apparatuses use different protocols for configuration management purpose.

7. The method of any preceding claims, wherein at least two of the apparatuses use different vendor-specific equipment.

5 8. The method of claim 2, wherein activating one or more application program interfaces comprises making an application program interface call to one of said resource proxies.

9. The method of claim 8, wherein the resource proxies access a workflow repository and perform a workflow as directed by the application program interface
10 call.

10. The method of claim 8 or 9, wherein each of said application program interface calls identifies a workflow to be executed and parameters associated with the workflow.

15 11. The method of any of the preceding claims, further including grouping different commands in a single configuration instruction to be performed in one or more of said apparatuses.

12. The method of claim 11, further including performing said configuration
20 instruction in said one or more apparatuses and, if an error occurs during said step of performing, returning said one or more apparatuses to a previous state.

13. The method of any of the preceding claims, further including performing an "UNDO" command (186) on one or more of said apparatuses to
25 return such apparatuses to a previous state.

14. The method of any of the preceding claims, further including in response to an application program interfaces call:

- 30 a) locking (176) a configuration of one of the apparatuses;
b) performing (178) configuration commands on said apparatus;
c) unlocking (184) the configuration.

15. A system for performing operations to control quality-of-service enforcement in a packet-based telecommunication network (10), the system characterized by:

- an enforcement module (100) configured to receive a request to configure
5 QoS operations on apparatuses of said network; and
a mediation layer (102) coupled to the enforcement module, the enforcement module configured to communicate with the mediation layer through an application program interface (API) to perform the configuration.

10 16. The system of claim 14, wherein the mediation layer includes a plurality of resource proxies (106), each of said resource proxies being associated with a respective apparatus of said telecommunication network or with part of it.

17. The system of claim 15, further comprising an admission control
15 subsystem (46) configured to determine availability of connection resources on said network and to send said request to configure QoS operations on the apparatuses of said network to an enforcement module.

18. The system of claim 16, further including a network inventory (104)
20 coupled to the enforcement module (100), the network inventory having stored therein information pertaining to the location of the apparatuses of said network and their association with the resource proxies.

19. The system of claim 15, wherein the network comprises a backbone
25 network (12) coupled between at least first and second access networks (14, 16).

20. The system of claim 19, wherein the first and second access networks
(14, 16) and the backbone network (12) each use different transmission technologies.

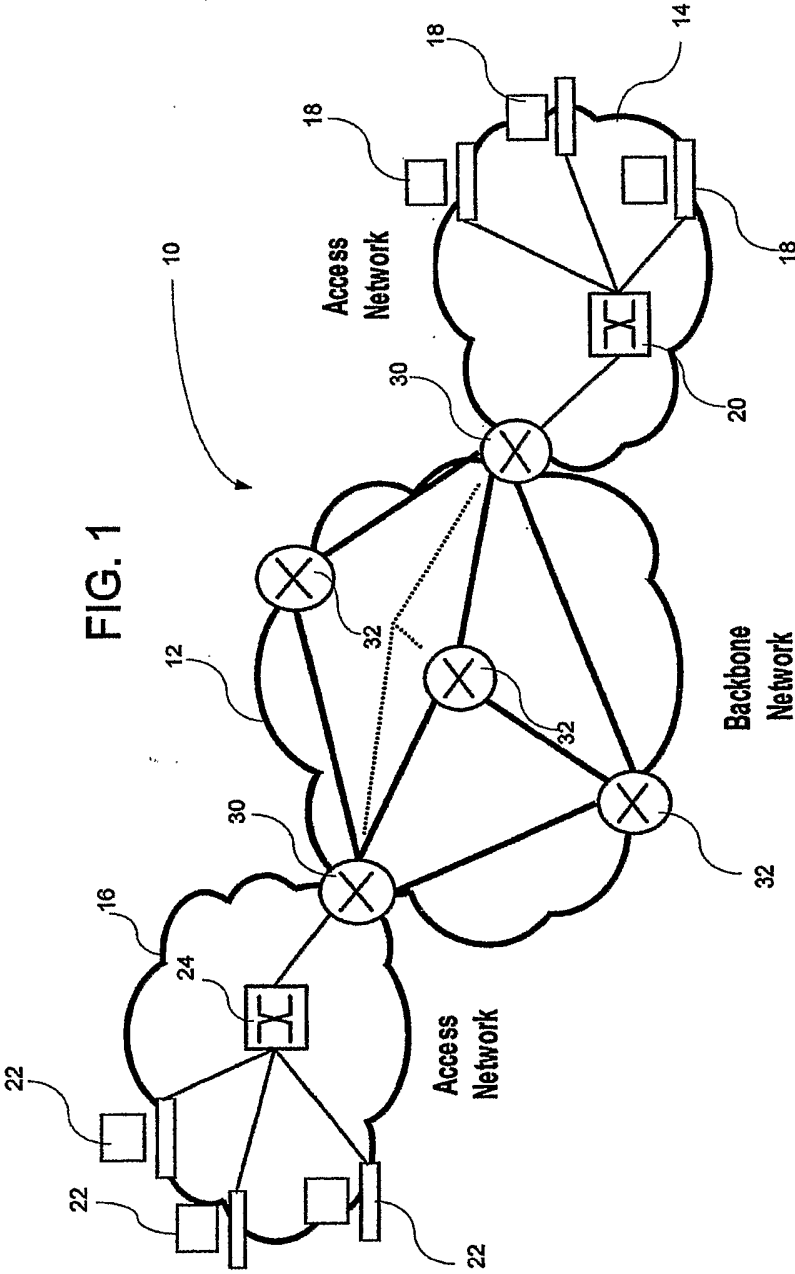
30

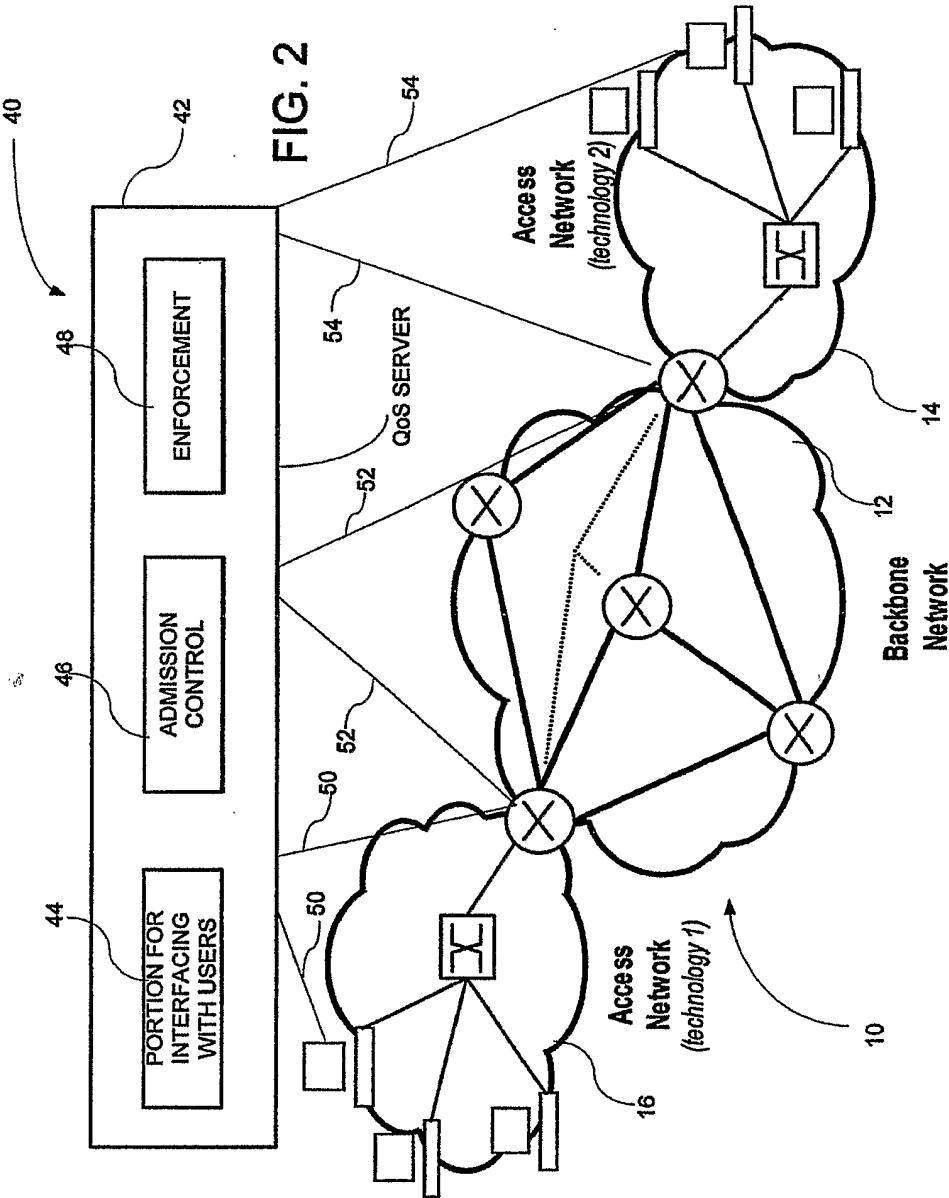
21. The system of claim 20, wherein the first and second access networks
(14, 16) include different vendor-specific equipment.

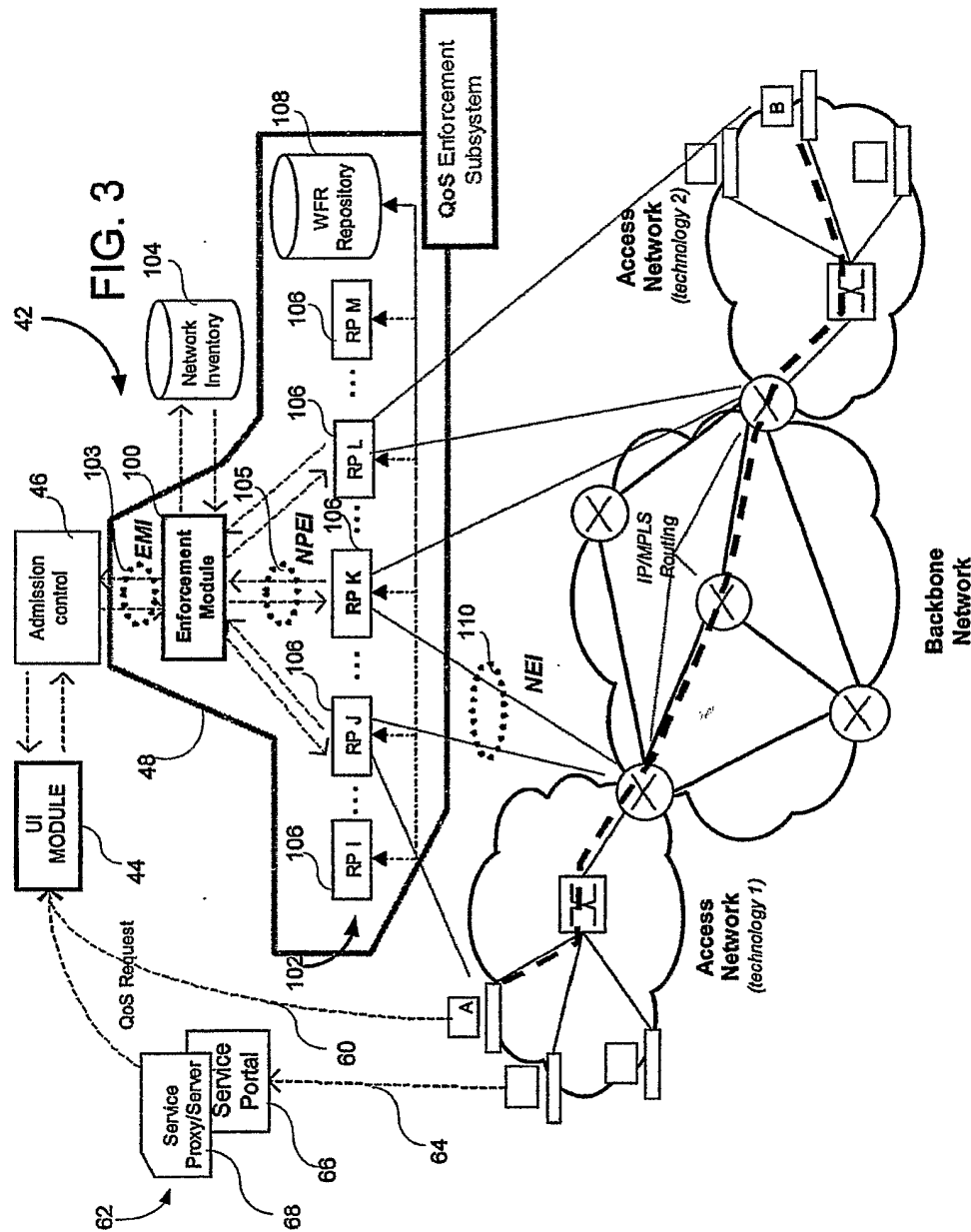
22. The system of any of claims 15 to 21, wherein at least two of the apparatuses use different protocols for configuration management purpose.

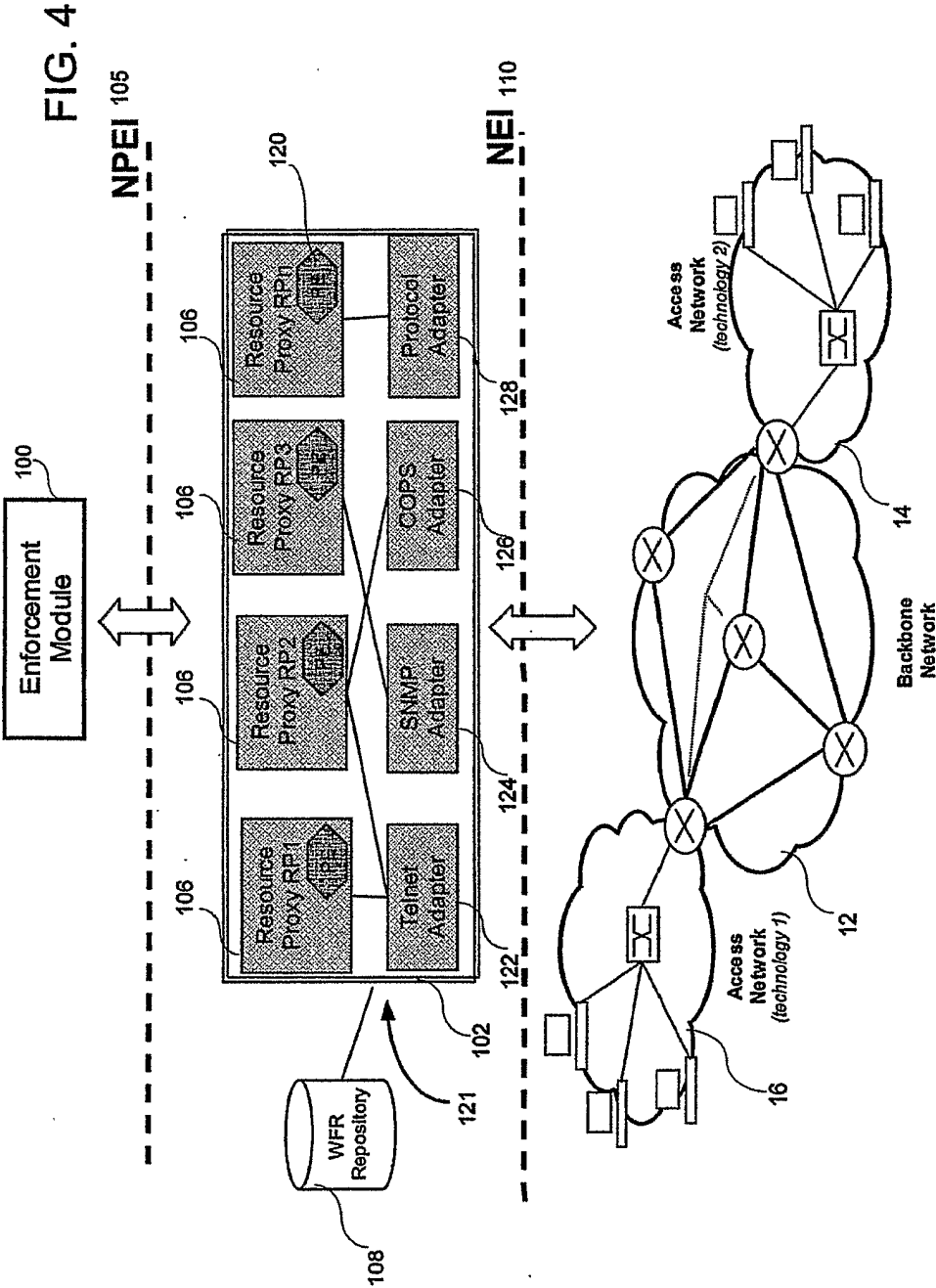
23. The system of claim 16, wherein the resource proxies include a process
5 engine (120) that executes workflows and uses protocol adapters (102) to communicate with the apparatuses of said network.

24. The system of any of claims 15 to 21, wherein the mediation layer
comprises a workflow repository including a plurality of workflows for translating
10 an application program interface call (105) in a set of operations to communicate with the apparatuses.



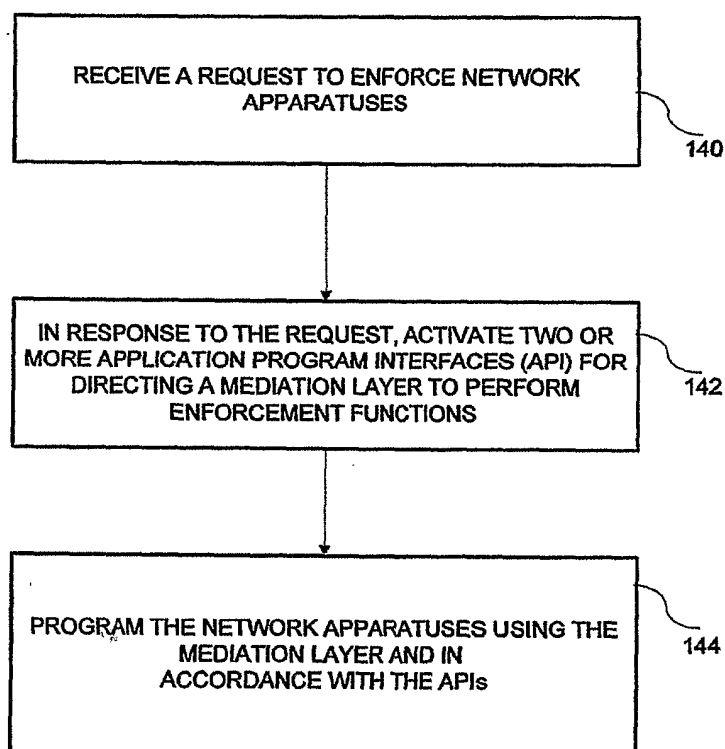






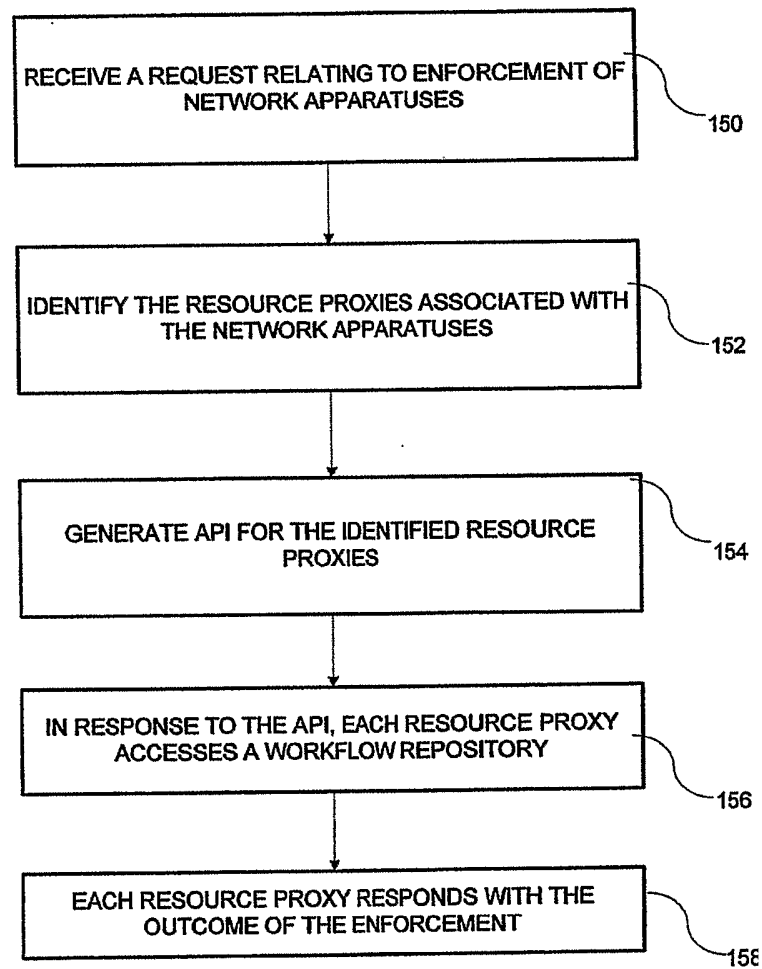
5 / 8

FIG. 5



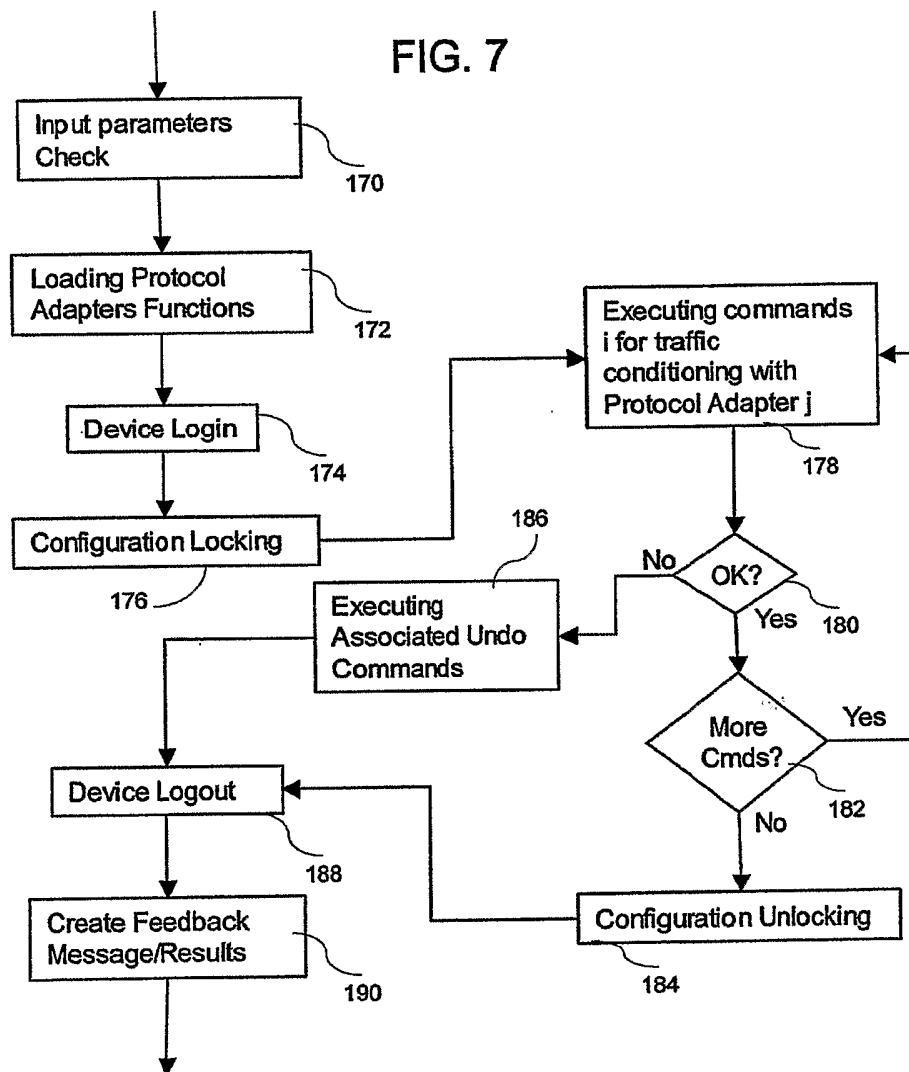
6 / 8

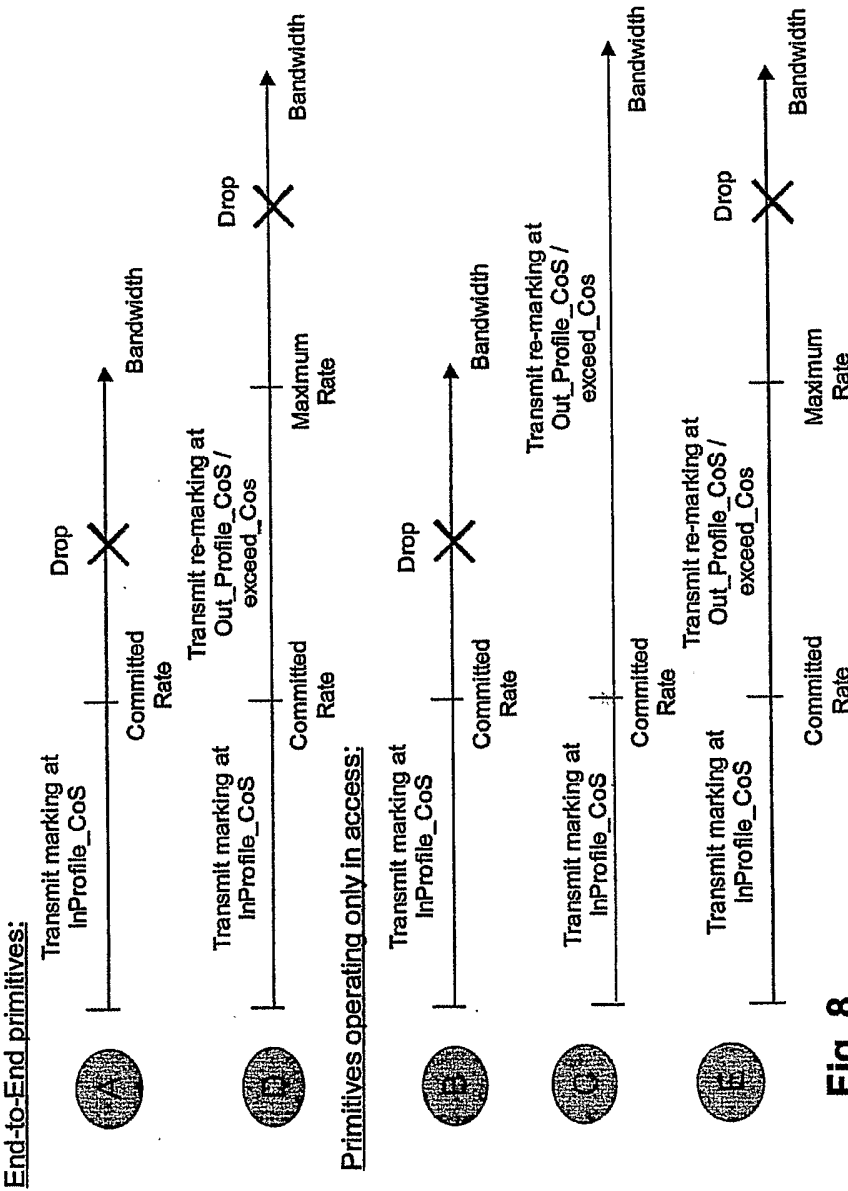
FIG. 6



7 / 8

FIG. 7





INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/053735

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/24 H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

A document defining the general state of the art which is not considered to be of particular relevance

E earlier document but published on or after the international filing date

L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O document referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

G document member of the same patent family

Date of the actual completion of the international search

15 April 2005

Date of mailing of the international search report

04/05/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Fischer, E

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/053735

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DIMOPOULOU L. SAMPATAKOS P, NIKOLOUZOU E, KARADIMAS Y, VENIERIS I S: "On providing a Dynamic QoS Management system for IP networks" 10TH INTERNATIONAL CONFERENCE ON SOFTWARE, TELECOMMUNICATIONS AND COMPUTER NETWORKS, 'Online! 11 October 2002 (2002-10-11), XP002324588 SOFTCOM 2002, DUBROVNIK, CROATIA Retrieved from the Internet: URL:http://www-st.inf.tu-dresden.de/aquila/files/pub/softcom2002-ntu-qos_management.pdf> 'retrieved on 2005-04-12! cited in the application	1,3, 5-10,15, 17-24
A	page 1, right-hand column, line 15 - line 18; figure 1 page 3, paragraph 3.1; figure 3 page 4, left-hand column, line 7 - line 34; figure 4 -----	9,10,23, 24
Y	VICENTE J, KOUNAVIS M, VILLELA D, LERNER M, CAMPBELL A: "Programming Internet Quality of Service" TRENDS TOWARDS A UNIVERSAL SERVICE MARKET CONFERENCE, 'Online! 13 September 2000 (2000-09-13), XP002324589 USM 2000, MUNICH GERMANY Retrieved from the Internet: URL:http://comet.ctr.columbia.edu/{campbell/papers/usm00.pdf> 'retrieved on 2005-04-13!	1,5-8, 15,17-22
A	page 2, line 10 - line 40 page 3, line 12, paragraph 2.1 - line 18, paragraph 2.1 page 3, paragraph 2.2 - page 4, paragraph 2.2; figure 1 page 7, paragraph 3.2 - page 8, paragraph 3.2; figure 2 -----	2,4,8, 11-14,16
Y	US 6 085 250 A (PERRY ET AL) 4 July 2000 (2000-07-04) column 2, line 36 - line 54 column 3, line 45 - column 4, line 20; figures 1,2 column 4, line 65 - column 5, line 16 -----	3,9,10, 18,23,24 1,15
A	----- -/--	

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/053735

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	BAK A; BEAR E; DABROWSKI M; DIMOPOULOU L; TSETSEKAS H; ET AL: "Aquila Final system specification" AQUILA PROJECT (ADAPTIVE RESOURCE CONTROL FOR QOS USING AN IP-BASED LAYERED ARCHITECTURE), 'Online! 26 February 2003 (2003-02-26), XP002324590 Retrieved from the Internet: URL: http://www-st.inf.tu-dresden.de/aquila/files/pub/d1203-b1.pdf 'retrieved on 2005-04-13! the whole document -----	1-24

Information on patent family members

PCT/EP2004/053735

Form PCT/ISA/210 (patent family annex) (January 2004)