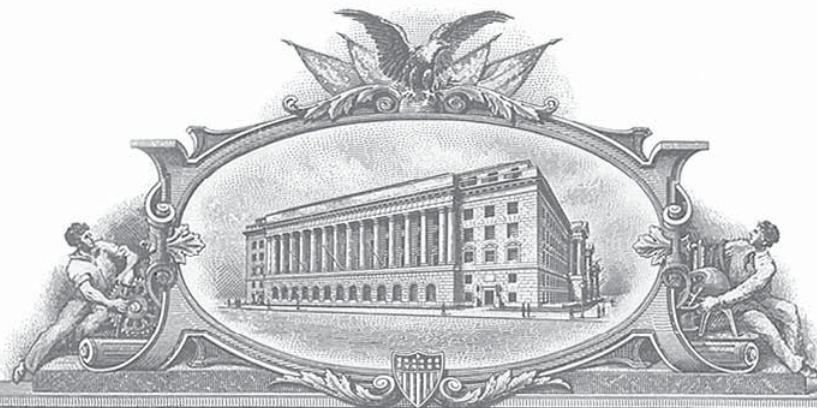


7622489



THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

February 08, 2017

**THIS IS TO CERTIFY THAT ANNEXED IS A TRUE COPY FROM THE
RECORDS OF THIS OFFICE OF THE FILE WRAPPER AND CONTENTS
OF:**

**APPLICATION NUMBER: 09/841,752
FILING DATE: April 24, 2001**



Certified by

Michelle K. Lee

Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

04-26-01

A

04/24/01

JN052 U.S. PTO

PATENT APPLICATION TRANSMITTAL LETTER

(Large Entity)

Docket No.

1000-0216

TO THE ASSISTANT COMMISSIONER FOR PATENTS

Transmitted herewith for filing under 35 U.S.C. 111 and 37 C.F.R. 1.53 is the patent application of:

Sorin Surdila and George Foti

For: System and Method for Providing End-To-End Quality of Service (QoS) Across Multiple IP Networks

JC973 U.S. PTO
09/841752
04/24/01

Enclosed are:

- ☒ Certificate of Mailing with Express Mail Mailing Label No. **EL851565873US**
- ☒ Twelve (12) sheets of drawings.
- ☐ A certified copy of a _____ application.
- ☒ Declaration ☐ Signed. ☒ Unsigned.
- ☒ Power of Attorney
- ☒ Information Disclosure Statement
- ☐ Preliminary Amendment
- ☒ Other: Three (3) cited references

CLAIMS AS FILED

| For | #Filed | #Allowed | #Extra | Rate | Fee |
|---|--------|----------|--------|-----------|----------|
| Total Claims | 11 | - 20 = | 0 | x \$18.00 | \$0.00 |
| Indep. Claims | 4 | - 3 = | 1 | x \$80.00 | \$80.00 |
| Multiple Dependent Claims (check if applicable) <input type="checkbox"/> | | | | | \$0.00 |
| BASIC FEE | | | | | \$710.00 |
| TOTAL FILING FEE | | | | | \$790.00 |

- ☒ A check in the amount of **\$790.00** to cover the filing fee is enclosed.
- ☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. **03-1130** as described below. A duplicate copy of this sheet is enclosed.
 - ☐ Charge the amount of _____ as filing fee.
 - ☒ Credit any overpayment.
 - ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
 - ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

Dated: April 24, 2001

Steven W. Smith
Signature

Steven W. Smith, Reg. No. 36,684
Smith, Danamraj & Youst, P.C.
12900 Preston Road, Suite 1200, LB-15
Dallas, TX 75230
(972) 720-1202

cc:

P01LARGE/REV06

"EXPRESS MAIL" Mailing Label No..EL851565873US..
Date of DepositApril 24, 2001.....

SYSTEM AND METHOD FOR PROVIDING
END-TO-END QUALITY OF SERVICE (QoS) ACROSS
MULTIPLE INTERNET PROTOCOL (IP) NETWORKS

5

BACKGROUND OF THE INVENTION

Technical Field of the Invention

10 [0001] This invention relates to telecommunication systems and, more particularly, to a system and method of providing End-to-End (E2E) Quality of Service (QoS) across multiple Internet Protocol (IP) networks.

Description of Related Art

15 [0002] Wireless telecommunication networks are evolving from second generation (2G) circuit-switched networks to third generation (3G) packet-switched networks. A Policy Framework and Architecture for third generation (3G) wireless Internet Protocol (IP) networks and the Internet is being developed by the Third
20 Generation Partnership Project (3GPP). The purpose of the 3GPP Policy Framework and Architecture is to

establish the real-time network control that is necessary to transform the Internet from a "best efforts" data network to a more reliable, real-time network. There are two releases of the proposal for 3G systems, but neither
5 of the releases addresses the issue of providing proper control of network transport resources when a single application is utilized across several transport networks.

[0003] The first release, referred to as 3GPP Release
10 99, introduces some new radio access technology such as Wideband Code Division Multiple Access (CDMA) and Enhanced Data rates for GPRS Evolution (EDGE). Wideband CDMA introduces not only a new radio technology, but also Asynchronous Transfer Mode (ATM) technology in the radio
15 access portion of the network. In the second 3G release called 3GPP Release 00, a real-time IP network is envisioned with all the infrastructure to carry real-time applications with equal or better quality than circuit-switched networks. It is assumed in Release 00 that the
20 different administrative domains owning the transport resources are over-provisioned in order to ensure an end-to-end QoS to an application.

[0004] The Application Performance Rating Table below
further illustrates the amount of bandwidth required for
25 different types of applications in order to achieve certain levels of Quality of Service (QoS). For example,

if high quality video is carried over an ISDN link at 128 kbps, the end user sees jerky, robotic movement (fair). However, if the video is provided at 384 kbps, the quality of the video is much better. At the other end of the performance spectrum, a voice call can be carried at 9.6 kbps and still have excellent voice quality. For efficient use of network resources, a control mechanism is needed to ensure that the right amount of bandwidth is provided in each transit network to deliver the requested E2E QoS without wasting excess bandwidth.

[0005] The support of E2E QoS is a very important issue related to the launching of real-time applications such as IP telephony, mixed voice/video calls, etc. over the IP infrastructure. The major challenge is to make sure that when a user requests a certain QoS, this QoS can be assured all the way to the recipient. The issue is complicated by the fact that in the general case, the payload path between two users can travel through multiple networks owned and operated by different operators who can choose various QoS solutions, other than over-provisioning, for their own domains.

| | | | | | | | | |
|----|-------------------------|---------------------------------------|------|----|----|-----|-----|------|
| | Data Rates (kbps) | 9.6 | 14.4 | 32 | 64 | 128 | 384 | 2000 |
| | Applications | Application Performance Rating | | | | | | |
| | Voice, SMS | E | E | E | E | E | E | E |
| 5 | E-mail | P | F | E | E | E | E | E |
| | Internet Web Access | P | P | F | F | E | E | E |
| | Database Access | P | P | F | E | E | E | E |
| | Synchronization | E | E | E | E | E | E | E |
| 10 | Document Transfer | P | P | F | E | E | E | E |
| | Location Services | F | E | E | E | E | E | E |
| 15 | Still Image Transfer | P | F | E | E | E | E | E |
| | Video Lower Quality | P | F | F | E | E | E | E |
| | Video High Quality | P | P | P | F | F | E | E |
| 20 | | Excellent (E) Fair (F) Poor (P) | | | | | | |

Application Performance Rating Table

[0006] In order to overcome the disadvantage of existing solutions, it would be advantageous to have a system and method of ensuring a requested Quality of Service (QoS) for a media flow that is transported through multiple transport networks, even if they are

owned by different administrations employing different QoS solutions. The present invention provides such a system and method.

5 **SUMMARY OF THE INVENTION**

10 [0007] In one aspect, the present invention is a method of ensuring a requested Quality of Service (QoS) for a media flow that is routed from a first terminal in an originating network, through at least one transit network, to a second terminal in a terminating network. The originating network includes an Originating Bandwidth Broker (BB-O) and an Originating Media Policy Server (MPS-O). The transit network includes a Transit Bandwidth Broker (BB-T). The terminating network includes a Serving Bandwidth Broker (BB-S) and a Serving Media Policy Server (MPS-S). The method includes the steps of sending an origination message from the originating network to the terminating network with a proposed session description that identifies the requested QoS; determining by the terminating network that the session description is agreeable; and sending a first Resource Allocation Request (RAR) from the BB-S to the BB-T with binding information that identifies the first and second terminals and the requested QoS. The BB-T determines whether a Service Level Agreement (SLA) between the transit network and the terminating network

allows sufficient resources to be allocated to meet the requested QoS. This is followed by sending a second RAR from the BB-T to the BB-O with the binding information, upon determining by the BB-T that the SLA between the transit network and the terminating network allows sufficient resources to be allocated to meet the requested QoS. The resources required to meet the requested QoS are then reserved in the originating network, the transit network, and the terminating network. A multimedia session is then set up to carry the media flow with the requested QoS.

[0008] In another aspect, the present invention is a Multimedia Control Server (MMCS) in a multi-service core network for ensuring a requested QoS for a media flow being routed from a first terminal in the core network to a second terminal in a terminating network. The MMCS includes an Originating Call State Control Function (known as a P-CSCF) that serves the first terminal; a BB-O that manages resources in the originating network; and a first interface between the P-CSCF and the BB-O for passing binding information from the P-CSCF to the BB-O. The binding information identifies the first and second terminals and the requested QoS. The MMCS also includes an Originating Media Policy Server (MPS-O) that provides policy rules regarding allocation of resources in the originating network, and a second interface between the

MPS-O and the BB-O for passing the policy rules from the MPS-O to the BB-O. A third interface passes policy rules from the BB-O to a plurality of edge routers that route the media flow into and out of the originating network.

5 [0009] When the media flow originating from the first terminal is routed through a transport network owned by an administration, and the media flow is routed through at least one transit network that is not owned by the same administration, the MMCS may also include a fourth
10 interface between the BB-O and a BB-T in the transit network for passing the binding information from the BB-T to the BB-O, the binding information having been received by the BB-T from a BB-S in the terminating network.

15 [0010] In yet another aspect, the present invention is a system for ensuring a requested QoS for a media flow from an application on a first terminal that is transported over network resources in an originating network owned by an administration, and is then routed through at least one transit network that is not owned by
20 the same administration to a second terminal in a terminating network. The system includes a first MMCS in the originating network that comprises a P-CSCF that serves the first terminal; a BB-O that manages resources in the originating network; and a first interface between
25 the P-CSCF and the BB-O for passing a session description and binding information from the P-CSCF to the BB-O. The

binding information identifies the first and second terminals and the requested QoS. The system also includes an MPS-O that provides policy rules regarding allocation of resources in the originating network, and
5 a second interface between the MPS-O and the BB-O for passing the policy rules to the BB-O. The system also includes a plurality of originating edge routers that route the media flow into and out of the originating network, and a third interface between the originating
10 edge routers and the BB-O for passing policy rules from the BB-O to the originating edge routers.

[0011] A second MMCS in the terminating network comprises a Terminating Call State Control Function (P-CSCF) that serves the second terminal; a Serving
15 Bandwidth Broker (BB-S) that manages resources in the terminating network; and a fourth interface between the P-CSCF and the BB-S for passing an agreed session description from the P-CSCF to the BB-S. A Serving Media Policy Server (MPS-S) provides policy rules regarding
20 allocation of resources in the terminating network, and a fifth interface between the MPS-S and the BB-S passes the policy rules from the MPS-S to the BB-S. The system also includes a plurality of serving edge routers that route the media flow into and out of the terminating
25 network, and a sixth interface between the serving edge routers and the BB-S for passing policy rules from the

BB-S to the serving edge routers. The transit network includes a Transit Bandwidth Broker (BB-T). A seventh interface between the BB-S and the BB-T passes the binding information from the BB-S to the BB-T in a first Resource Allocation Request (RAR). An eighth interface between the BB-T and the BB-O passes the binding information from the BB-T to the BB-O in a second RAR. This ensures that the binding information is available and known to all domains supporting the application in the provision of end-to-end QoS.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The invention will be better understood and its numerous objects and advantages will become more apparent to those skilled in the art by reference to the following drawings, in conjunction with the accompanying specification, in which:

[0013] FIG. 1 (Prior Art) is a simplified block diagram of the QBone Phase 1 Bandwidth Broker (BB) Architecture;

[0014] FIG. 2 (Prior Art) is a simplified block diagram of the QBone Phase 2 BB Architecture;

[0015] FIG. 3 is a simplified block diagram of the preferred embodiment of the Phase 1 BB Architecture of the present invention;

[0016] FIGS. 4A-4B are portions of a sequence diagram illustrating implementation of a Push Policy Mechanism for End-to-End QoS for a SIP call during Phase 1;

5 [0017] FIGS. 5A-5B are portions of a sequence diagram illustrating implementation of a Pull Policy Mechanism for End-to-End QoS for a SIP call during Phase 1;

10 [0018] FIG. 6 is a simplified block diagram of the preferred embodiment of the Phase 2 BB Architecture of the present invention when there are BBs in every transit network;

[0019] FIGS. 7A-7B are portions of a sequence diagram illustrating implementation of a Push Policy Mechanism for End-to-End QoS for a SIP call during Phase 2 when there are BBs in every transit network;

15 [0020] FIG. 8 is a simplified block diagram of the preferred embodiment of the Phase 2 BB Architecture of the present invention when there are BBs in some, but not all, transit networks; and

20 [0021] FIGS. 9A-9B are portions of a sequence diagram illustrating implementation of a Push Policy Mechanism for End-to-End QoS for a SIP call during Phase 2 when there are BBs in some, but not all, transit networks.

DETAILED DESCRIPTION OF EMBODIMENTS

QBone Working Group Architecture

5 [0022] A working group known as the QBone Working Group has defined, as part of the Internet 2 initiative, an architecture for coordinating bandwidth requirements across multiple networks at the transport level. The QBone group has published a description of the architecture in a paper entitled "QBone Bandwidth Broker Architecture" found at <http://www.internet2.edu/qos/qbone/papers/sibbs/>, and this paper is incorporated by reference in its entirety herein. This paper defines the functionality of a Bandwidth Broker (BB) and contains a brief specification of a BB protocol which is to be introduced in Phase 2 of the QBone implementation program.

10 [0023] The terms Bandwidth Broker, Network Control Point, and Bearer/Resource Manager are used interchangeably in the industry to refer to the same functional node, but Bandwidth Broker is currently preferred by the majority. As referred to herein, the BB does more than merely control bandwidth. Often, for example, an edge router will have the bandwidth available to carry a given application, but cannot carry the packets with the required latency to provide the desired QoS. Therefore, the BB instructs the edge router to deny access. This action is typically performed by having the

BB install a policy in the edge router that denies the admission of the incoming flow. BBs do not exist today, but are proposed for the Internet Engineering Task Force (IETF) policy framework architecture in order to support a real-time IP network.

[0024] The BB is a server application. The BB understands all IP protocols such as the Routing Information Protocol (RIP). Therefore, it builds a database that allows the routers to understand the topology of the network it controls. It knows what paths in the network, by default, packets will use in crossing the network. It knows what nodes need to be controlled in order to ensure all of an application's packets flow through the network in such a way that they fulfill the appropriate Service Level Agreement (SLA).

[0025] The functions of the BB are to:

1. Know the QoS availability of the resources in the network it controls;
2. Receive all the requests for QoS and decide whether or not to accept them. This decision is based on various criteria such as resource availability, agreements with the downstream networks, network policies, subscriber rights, etc.
3. Make sure that the requested QoS is available end-to-end. To assure this, the BB may need to

communicate with the BB's of neighboring networks to request the End-to-End QoS reservation.

4. Instruct specific routers in its network to install appropriate policies for treating the payload flows.

5

[0026] The QBone group has established a two-phase implementation of the end-to-end QoS solution. The distinction between Phase 1 and Phase 2 is that in QBone Phase 1, there will be BB's only in the multi-service core networks, but no BBs in the transit networks. It is assumed that the bandwidth capacity in the transit networks is dimensioned to cover all of the SLAs with the neighboring transport networks (either multi-service core or transit). In QBone Phase 2, BBs are implemented in all of the transit networks as well.

10

15

[0027] FIG. 1 is a simplified block diagram of the QBone Phase 1 Bandwidth Broker (BB) Architecture. In the illustrated configuration, a first Session Initiation Protocol (SIP) phone 11 is conducting a multimedia session with a second SIP phone 12. Access networks 13 and 14 are utilized to access Multi-Service Core Networks 15 and 16, respectively. The session is transported between the core networks through transit networks 17 and 18. Core network 15 includes a BB 19 which utilizes the Common Open Policy Service (COPS) protocol to communicate

20

25

with Label Edge Routers (LERs) 21 and 22. The LERs function as edge routers that also insert a specific label in the data packets to identify a specific media flow at the entry to the network, and remove the label upon exiting the network. The Multi-Protocol Label Switching (MPLS) protocol then routes packets based on the labels inserted by the LERs rather than the IP addresses. Core network 16 likewise includes a BB 23 which utilizes the COPS protocol to communicate with LERs 24 and 25. The transit networks include border routers 26-29. The border routers do not do any labeling; they utilize the Differential Services (DiffServ) protocol for routing packets.

[0028] The marking and remarking of IP packets when transiting from one network to another is done by border routers at the entry point into the network (marking) and the exit point from the network (remarking). Optionally, and through administrative agreements, LERs can perform packet marking for transit networks utilizing DiffServ.

[0029] In Phase 1, there is no BB protocol. Moreover, the BB of the multi-service core network needs to install policies only in the ingress LERs 21 and 25 (the point of entrance of the access network traffic). It is assumed that the end-to-end QoS relies on sufficient Service Level Agreements (SLAs) and over-provisioning between the core network controlled by the BB and the other transit

networks. In Phase 1, the two core networks 15 and 16 involved in a call will act as two separate islands. Therefore, for telephony calls, the bandwidth reservation inside these islands should be done for bidirectional flows.

5 [0030] FIG. 2 is a simplified block diagram of the QBone Phase 2 BB Architecture. In Phase 2, BBs are installed in all networks, and the BB protocol is introduced to link all the BBs. As illustrated, BBs 31-10 34 are modified to communicate with neighboring BBs using the BB protocol, and are installed in the Multi-Service Core Networks 35 and 36, and in the transit networks 37 and 38. BB 31 utilizes the COPS protocol to communicate with LERs 21 and 22 within the core network 35, and BB 3415 utilizes the COPS protocol to communicate with LERs 23 and 24 within the core network 36. BB 32 utilizes the COPS protocol to communicate with border routers 26 and 27 within the transit network 37, and BB 33 utilizes the COPS protocol to communicate with border routers 28 and20 29 within the transit network 38.

[0031] A problem with the QBone Architecture is that it is based on a transport-centric view which totally ignores the application that uses the transport resources, and ignores the interaction between the25 transport layers and the application layers. There is no binding between the applications and the transport

resources allocated by those applications for providing end-to-end QoS. Collaboration between the applications and the transport layers has several benefits related to providing end-to-end QoS such as prevention of theft of the bearer, proper usage of the bearer for intended users, prevention of denial of service attacks, etc. Another problem with the QBone Phase 2 Architecture is that it assumes that all the networks in the payload path have a BB. However, this is not necessarily the case since many transit network operators may decide to use the Phase 1 solution for a long period of time in which no BB will be installed.

Architecture of the Present Invention

[0032] The present invention provides proper control of network transport resources when a single application is utilized across several transport networks. Proper control includes the ability to bind the utilization of transport resources across several administrative domains to the application utilizing these resources for the provision of end-to-end QoS. This binding is necessary regardless of the QoS solution used in each administrative domain for the provision of end-to-end QoS. QoS solutions can include over-provisioning based on Service Level Agreements (SLAs) between different domains, centralized Bandwidth Brokers for control of

transport resources, etc. The information to bind the application to the transport resources utilized by that application is referred to as "binding information". The binding information must be unique for each application execution.

5 [0033] FIG. 3 is a simplified block diagram of the preferred embodiment of the Phase 1 BB Architecture of the present invention. For clarity, some network elements involved in session setup signaling have not
10 been shown. Within an originating Multi-Service Core Network 41, a BB-O 42 interfaces with a Media Policy Server (MPS-O) 43 using the COPS protocol. Before talking to the LERs, the BB-O must first verify that the policy allows for media packets belonging to a specific
15 session to be admitted. The MPS-O functions to enable the network operator to provide instructions on how the bandwidth in the network should be allocated. For example, the IETF has standardized four classes of services: Best Efforts, Interactive, Real-time Stream,
20 and Conversational, and the operator may instruct that 25% of the available bandwidth be reserved for Best Efforts and Interactive traffic. The MPS-O also interfaces with a Clearing House 46 using the Open Systems Protocol (OSP). The Clearing House performs the
25 functions of an IETF Authorization, Authentication, and Accounting (AAA) server.

[0034] The BB-O 42 also interfaces with an originating SIP CSCF (P-CSCF-O) 44 using a new link and a combination of the COPS protocol and the BB protocol (BBP). The interface between the P-CSCF-O 44 and the BB-O 42 provides a link between the control plane and the transport plane, and the combination of the BB-O 42, the MPS-O 43, and the P-CSCF-O 44 form a functional entity known as a Multimedia Control Server (MMCS) 45.

[0035] Within a terminating Multi-Service Core Network 47, a BB-S 48 interfaces with a Policy Server (MPS-S) 49 using the COPS protocol. The BB-S also interfaces with a terminating SIP CSCF (P-CSCF-S) 51 using a combination of the COPS protocol and BBP. The interface between the P-CSCF-S 51 and the BB-S 48 provides a link between the control plane and the transport plane, and the combination of the BB-S, the MPS-S, and the P-CSCF-S form an MMCS 52.

[0036] The present invention focuses on the BB protocol used between the BB and the Originating Call State Control Function (P-CSCF-O) serving the originating terminal, and proposes Binding Information that helps correlate a BB reservation session with an application session (e.g., SIP call establishment). Moreover, it defines the new BB behavior that takes into consideration this Binding Information.

5 [0037] Use of the Binding Information in the BB
protocol along with the new BB behavior ensures that the
benefits of collaboration (represented by the binding
information) between the application and the transport
layers will be realized. Use of the Binding Information
also enables the establishment of a consistent migration
path from Phase 1 onward by preserving the BB's behavior
principles. In Phase 1, where a BB is implemented in
each multi-service core network 41 and 47 for the two
10 terminals (SIP phones 11 and 12) involved in the call,
the two BBs behave as independent entities. When the
corresponding CSCFs request a QoS reservation from the
BBs, the BBs respond by focusing on their area of
control, which is limited to their core networks.

15 [0038] When the P-CSCF-O 44 requests the BB-O 42 in
the originating core network to reserve the QoS, the BB-O
has to determine whether a reservation was previously
made for the same media flow of the same session. This
is only possible if there is certain information that
20 allows it to check whether a previous reservation was
made. This is the Binding Information which has to be
carried by the BB protocol. The Binding Information must
be carried in the SIP messages so that it can be
transmitted from the P-CSCF-O 44 to the BB-O. However,
25 since SIP is a mature protocol already implemented, the
preferred embodiment of the present invention does not

modify the SIP protocol to transport this information. With respect to the BB protocol, the preferred embodiment does not add a new parameter to transfer the information between BBs. With this in mind, the invention uses the session information carried by the Session Description Protocol (SDP) within the SIP signaling as the binding information to uniquely identify the flows for which the QoS reservation is performed. The invention then focuses on transferring the Binding Information within the BB protocol by using the Resource Allocation Request (RAR) ID parameter within the RAR message for that purpose. The RAR ID parameter already exists, but is currently of little use.

[0039] The preferred embodiment includes the source IP address plus an identification of a Real Time Protocol (RTP) port assigned by the originating terminal, along with the destination IP address plus an identification of an RTP port assigned by the destination terminal as the Binding Information in the BB protocol. This information, which is included in the SDP within the SIP signaling, is extracted by the BB-S 48 in the terminating network from the QoS reservation request received from the P-CSCF-O 44 as well as from the response returned from the destination.

[0040] When the Binding Information is being utilized, and a core network BB receives a Resource Allocation Request (RAR) from another BB, the core network BB:

- 5 1. Determines whether the SLA between the two networks allows this reservation.
2. Determines whether its network has available resources for this reservation.
3. Eventually installs the applicable policies in the selected routers.
- 10 4. Stores the Binding Information (resource and destination IP addresses and RTP ports) for the flow for which the QoS was requested. This information is received in the RAR.
- 15 5. Attaches a time stamp to the information to help detect stale reservations in the future.
6. Answers the RAR with a Resource Allocation Answer (RAA) message.

[0041] When the Binding Information is being utilized, and a core network BB receives a QoS reservation request containing the session's SDP from a CSCF server, the core network BB:

- 25 1. Checks whether there is any reservation already made for this session. The BB uses the source and destination IP addresses and the RTP ports extracted

from the SDP (the Binding Information coming from the application layer).

2. If the BB finds another reservation already made for this set of addresses, the BB checks the time stamp to determine whether this reservation is stale. The network operator establishes a time interval as a threshold for considering a reservation stale.

3. The BB may also check for other possible mismatches between the actual request and the reservation already made.

4. If a valid reservation was already made, the BB immediately answers the CSCF's request with a successful reservation.

5. If no valid reservation is found, the BB proceeds with the procedure for reserving the requested QoS.

[0042] The BB maps the type of application and class of service to an SLA. The SLA specifies the characteristics that are needed to carry the packets that belong to a specific application such as the amount of bandwidth, delays, delay variation, and jitter. The BB translates the SLA to a Service Level Specification (SLS). The system must then enforce the SLS to ensure that the right QoS is provided end-to-end.

[0043] Looking specifically at Phase 1, the present invention defines both a Push Policy Mechanism and a Pull Policy Mechanism for ensuring end-to-end QoS. In the push mechanism, the policy is pushed to the routers at session setup while in the pull mechanism, the policy is dynamically retrieved (pulled) at reservation time. FIGS. 4A-4B are portions of a sequence diagram illustrating the implementation of a Push Policy Mechanism for End-to-End QoS for a SIP call during Phase 1 in which the originating network is the Multi-Service Core Network 41, and the terminating network is the Multi-Service Core Network 47 of FIG. 3. The media flows through a single transit network such as Transit Network 17. It is assumed that the originating and terminating users are roaming in their home networks. It is also assumed that the transit network is over-provisioned for handling traffic routed between the originating and terminating networks.

[0044] At step 62, End User (UE-A) 11 sends an Invite message to the Originating P-CSCF-O 44 and includes the A-Name, B-Name, and Proposed Session Description (SDP) (QoS Assured). Guaranteed end-to-end QoS is requested for the session, as indicated by the QoS Assured parameter in the SDP. The Originating P-CSCF-O proxies the Invite message to the home domain of the originating subscriber. To do so, the P-CSCF-O sends a

Domain Name Server (DNS) Request 63 to an originating DNS (DNS-O) 61. The DNS-O sends a Reply at 64 identifying the IP address of an Interrogating CSCF (I-CSCF-A) 65 in the originating network. Following this, the Originating P-CSCF-O sends the Invite message 66 to the I-CSCF-A with the A-Name, B-Name, and Proposed SDP (QoS Assured).

[0045] At 67, the I-CSCF-A 65 requests UE-A's Home Subscriber Server (HSS) 68 to find the Serving CSCF (S-CSCF-A) 69 for UE-A 11. The HSS returns the address of the S-CSCF-A at 71, and the I-CSCF-A sends an Invite message 72 to the S-CSCF-A with the A-Name, B-Name, and Proposed SDP (QoS Assured). At this point, the UE-A is authenticated and the call is authorized. At 73, the S-CSCF-A, in turn, sends an Invite message to an Interrogating CSCF (I-CSCF-B) 74 in the terminating network 47. At 76, the I-CSCF-B requests UE-B's HSS 75 to find the Serving CSCF (S-CSCF-B) 77 for UE-B 12. The HSS returns the address of the S-CSCF-B at 78, and the I-CSCF-B sends an Invite message 79 to the S-CSCF-B with the A-Name, B-Name, and Proposed SDP (QoS Assured). At this point, the UE-B is authenticated and the call is authorized. Therefore, at 81, the S-CSCF-B sends an Invite message to the Terminating P-CSCF-S 51 with the A-Name, B-Name, and Proposed SDP (QoS Assured). At 82, the Terminating P-CSCF-S forwards the Invite message to the UE-B 12 with the Proposed SDP and includes an

Authentication token. The token is used by the SIP client (UE-B) to make the QoS reservation at a later stage, and enables the LER-S to identify the appropriate policy applicable to the session.

5 [0046] At 83, the UE-B 12 sends a SIP 183 response message to the Terminating P-CSCF-S with an indication that the Session Description (SD) is agreed upon. At 84, the Terminating P-CSCF-S 51 requests a QoS Reservation with the Agreed SDP from the BB in the terminating
10 network (BB-S) 48. At 85, the BB-S converts the Agreed SDP to specific SLS-QoS parameters, and then sets up the COPS link to the Policy Server (MPS-S) 49 with a COPS Request (COPS REQ) message 86. A COPS Decision (COPS DEC) message is returned at 87. At step 88, the BB-S 48
15 sends policy instructions to the ingress LER in the terminating network (LER-S) 25 to implement the terminating network's policy instructions. Thus, policy is pushed to the ingress LER-S since the transit network 17 does not include a BB. The policy instruction
20 includes the Binding Information and the token that will be later used by the client to perform the actual reservation. The token enables the LER to identify the policy stored for the client.

[0047] A QoS Reservation Success message 89 is then
25 sent from the BB-S to the Terminating P-CSCF-S 51. The Terminating P-CSCF-S then forwards the SIP 183 response

message 91 to the S-CSCF-B 77 with the Agreed SDP and
codecs. This message is forwarded to the I-CSCF-B 74 at
step 92 which forwards it to the S-CSCF-A 69 in the
originating network at 93. At 94, the S-CSCF-A forwards
5 the 183 message to the Originating P-CSCF-O 44 with the
Agreed SDP and codecs. The Originating P-CSCF-O then
sends a QoS Reservation Request message 95 to the BB in
the originating network (BB-O) 42 with the Agreed SDP and
the Binding Information. At step 96, the BB-O converts
10 the Agreed SD to specific SLS-QoS parameters, and the
process then moves to FIG. 4B.

[0048] At steps 97-98, BB-O 42 sets up the COPS link
to the Policy Server (MPS-O) 43 in the originating
network. At step 99, the BB-O sends policy instructions
15 to the ingress LER in the originating network (LER-O) 21
to implement the originating network's policy
instructions. Thus, policy is pushed to the ingress LER-
O since the transit network 17 does not include a BB.
The policy instruction includes the Binding Information.
20 A QoS Reservation (Success) message 101 is then sent from
the BB-O to the Originating P-CSCF-O 44. The Originating
P-CSCF-O then forwards the SIP 183 response message 102
to the UE-A 11 with the Agreed SDP and token.

[0049] At 103, the UE-A 11 sends a Provisional
25 Acknowledgment (PRACK) message to the UE-B 12, and
receives a SIP 200 OK message in response at 104. At

105, the UE-A sends a Reservation message to the ingress LER-O 21, and receives a Reservation accepted message in return at 106. The Reservation message includes the token, flow specification, and filter specification. The
5 RSVP protocol or other mechanisms are acceptable for performing the bearer reservation by the end user. Likewise, at 107, the UE-B 12 sends a Reservation message to the ingress LER-S 25, and receives a Reservation accepted message in return at 108. Once again, the
10 Reservation message includes the token, flow specification, and filter specification.
[0050] At 109, the UE-B 12 sends a Condition Met (COMET) message to the UE-A 11 indicating that the QoS has been successfully reserved for the direction from UE-B to UE-A. UE-A responds at 111 with a SIP 200 OK
15 message. Likewise, at 112, the UE-A sends a COMET message to the UE-B indicating that the QoS has been successfully reserved for the direction from UE-A to UE-B. UE-B responds at 113 with a SIP 200 OK message. At
20 114, a SIP 180 Ringing message is then sent from the UE-B to UE-A via the Terminating P-CSCF-S 51, the S-CSCF-B 77, and the I-CSCF-B 74 in the terminating network 47, and via the S-CSCF-A 69 and the Originating P-CSCF-O 44 in the originating network 41.
25 [0051] At 115, the UE-A 11 sends a PRACK message to the SIP Client-B 12 in response to the 180 Ringing

message. At 116, the UE-B sends a SIP 200 OK of the PRACK message to the UE-A. At 117, the UE-B sends a SIP 200 OK message to UE-A via the Terminating P-CSCF-S 51, the S-CSCF-B 77, and the I-CSCF-B 74 in the terminating network 47, and via the S-CSCF-A 69 and the Originating P-CSCF-O 44 in the originating network 41. The UE-A responds with an Acknowledgment message at 118, and the process of implementing a Phase 1 Push Policy Mechanism for end-to-end QoS is complete.

[0052] FIGS. 5A-5B are portions of a sequence diagram illustrating implementation of a Pull Policy Mechanism for End-to-End QoS for a SIP call during Phase 1. Again, it is assumed that the originating and terminating users are roaming in their home networks. The sequence is identical to that of FIGS. 4A-4B from steps 62 through 87. At that point, unlike FIGS. 4A-4B, policy is not pushed to the ingress LER. Instead, a QoS Reservation Success message 121 is then sent from the BB-S 48 to the Terminating P-CSCF-S 51. The Terminating P-CSCF-S then forwards the SIP 183 response message 122 to the S-CSCF-B 77 with the Agreed SDP and codecs. This message is forwarded to the I-CSCF-B 74 at step 123 which forwards it to the S-CSCF-A 69 in the originating network at 124. At 125, the S-CSCF-A forwards the 183 message to the Originating P-CSCF-O 44 with the Agreed SDP and codecs. The Originating P-CSCF-O then sends a QoS Reservation

Request message 126 to the BB in the originating network (BB-O) 42 with the Agreed SDP and the Binding Information. The process then moves to FIG. 5B.

[0053] At step 127, the BB-O 42 converts the Agreed SDP to specific SLS-QoS parameters, and at steps 128-129, BB-O sets up the COPS link to the Policy Server (MPS-O) 43 in the originating network. A QoS Reservation (Success) message 131 is then sent from the BB-O to the Originating P-CSCF-O 44. The Originating P-CSCF-O then forwards the SIP 183 response message 132 to the UE-A 11 with the Agreed SDP and token.

[0054] At 133, the UE-A 11 sends a Provisional Acknowledgment (PRACK) message to the UE-B 12, and receives a SIP 200 OK message in response at 134. At 135, the UE-A sends a Reservation message to the ingress LER-O 21, and includes the token, flow specification, and filter specification. The LER-O sends a COPS REQ message 136 to the BB-O 42, and receives a COPS DEC message 137 in response that includes policy instructions and the Binding Information. Thus, policy is dynamically pulled from the BB-O by the ingress LER-O at reservation time. At 138, the LER-O sends a Reservation accepted message back to the UE-A. The RSVP protocol or other mechanisms are acceptable for performing the bearer reservation by the end user.

1000052700

5 [0055] In a similar manner, the UE-B 12 sends a Reservation message 139 to the ingress LER-S 25, and includes the token, flow specification, and filter specification. The LER-S sends a COPS REQ message 141 to the BB-S 48, and receives a COPS DEC message 142 in response that includes policy instructions and the Binding Information. Thus, policy is dynamically pulled from the BB-S by the ingress LER-S at reservation time. At 143, the LER-S sends a Reservation accepted message back to the UE-B.

15 [0056] At 144, the UE-B 12 sends a Condition Met (COMET) message to the UE-A 11 indicating that the QoS has been successfully reserved for the direction from UE-B to UE-A. UE-A responds at 145 with a SIP 200 OK message. Likewise, at 146, the UE-A sends a COMET message to the UE-B indicating that the QoS has been successfully reserved for the direction from UE-A to UE-B. UE-B responds at 147 with a SIP 200 OK message. At 148, a SIP 180 Ringing message is then sent from the UE-B to UE-A via the Terminating P-CSCF-S 51, the S-CSCF-B 77, and the I-CSCF-B 74 in the terminating network 47, and via the S-CSCF-A 69 and the Originating P-CSCF-O 44 in the originating network 41.

20 [0057] At 149, the UE-A 11 sends a PRACK message to the UE-B 12 in response to the 180 Ringing message. At 25 151, the UE-B sends a SIP 200 OK of the PRACK message to

the UE-A. At 152, the UE-B sends a SIP 200 OK message to UE-A via the Terminating P-CSCF-S 51, the S-CSCF-B 77, and the I-CSCF-B 74 in the terminating network 47, and via the S-CSCF-A 69 and the Originating P-CSCF-O 44 in the originating network 41. The UE-A responds with an Acknowledgment message at 153, and the process of implementing a Phase 1 Pull Policy Mechanism for end-to-end QoS is complete.

[0058] FIG. 6 is a simplified block diagram of the preferred embodiment of the Phase 2 BB Architecture of the present invention when there are BBs in every transit network. Thus, FIG. 6 is similar to FIG. 3 except that BBs have been implemented in Transit Network-1 161 and Transit Network-2 162. Within Transit Network-1, BB-T1 163 interfaces with border routers 164 and 165 using the COPS protocol. The BB-T1 also uses the COPS protocol to interface with a Policy Server (MPS-T1) 166. Within Transit Network-2, BB-T2 167 interfaces with border routers 168 and 169 using the COPS protocol. The BB-T2 also uses the COPS protocol to interface with a Policy Server (MPS-T2) 170. All of the network Policy Servers interface with the Clearing House 46 using the OSP protocol.

[0059] In Phase 2, the BBs in the two core networks will behave similarly, with the difference being that their area of control may be extended to consider the BBs

in adjacent networks. However, in scenarios such as when the BB-S 48 in the terminating serving core network sends a request to the adjacent BB-T2 167 in a transit network, the BB-S does not know whether this request is propagated
5 beyond BB-T2 all the way to the BB-O 42 of the originating core network. In the case where there are BBs in all of the intermediate transit networks, then the QoS reservation is propagated all the way to the BB-O in the originating core network. However, if all of the
10 intermediate transit networks do not have a BB, then the originating core network BB-O does not receive the reservation initiated by the BB-S in the terminating core network.

[0060] In Phase 2, the SLA slightly changes its
15 meaning from the perspective of the network playing the "customer" role. Using an analogy to financial markets, it becomes like an option. The customer gets the option to reserve the resources agreed to in the SLA, but the resources are not necessarily used all the time. When
20 the customer wants to reserve some resources it has to send an RAR to the BB of the transit domain, and it will be charged only for the time the reservation is active. The Phase 2 End-to-End QoS mechanisms and the interactions between session layer and transport layer to
25 allow End-to-End QoS evolve from those used in Phase 1.

[0061] FIGS. 7A-7B are portions of a sequence diagram illustrating implementation of a Push Policy Mechanism for End-to-End QoS for a SIP call during Phase 2 when there are BBs in every transit network, as illustrated in FIG. 6. FIGS. 7A-7B illustrate setup with a single transit network such as Transit Network-1 161. It is assumed that the BBs in the multi-service core networks are upgraded with new software that supports the inter-domain BB protocol and the associated BB behavior.

[0062] The sequence is identical to that of FIGS. 4A-4B from steps 62 through 87. At that point, step 171, the BB-S 48 determines the ingress-egress edge routers and BB-T1 163. At 172, the BB-S sends a Resource Allocation Request (RAR) message to the BB-T1 163 indicating a bidirectional session and including the Binding Information. BB-T1 sends a COPS REQ message 173 to its Policy Server (MPS-T1) 166 and receives a COPS DEC message 174 in response. At 175, BB-T1 then determines the ingress-egress edge routers and BB-O 42. At 176, the BB-T1 sends an RAR message to the BB-O indicating a bidirectional session and including the Binding Information. BB-O sends a COPS REQ message 177 to its Policy Server (MPS-O) 43 and receives a COPS DEC message 178 in response. At 179, BB-O then determines the ingress-egress edge routers, and sends a Resource

Allocation Answer (RAA) message 181 to BB-T1 163. The process then moves to FIG. 7B.

[0063] At 182, BB-T1 163 sends the RAA message to BB-S 48. BB-S then sends a QoS Reservation (Success) message 183 to the Terminating P-CSCF-S 51. Policy instructions and Binding Information are then pushed by the BBs in each network to their ingress and egress routers. Thus, at 184 and 185, BB-O 42 sends COPS DEC messages to the ingress LER-O 21 and the egress Rout-O 22. Likewise, BB-T1 163 sends COPS DEC messages 186 and 187 to the ingress Rout-T 164 and the egress Rout-T 165. Likewise, BB-S 48 sends COPS DEC messages 188 and 189 to the ingress LER-S 25 and the egress Rout-S 24.

[0064] The Terminating P-CSCF-S 51 then forwards the SIP 183 message 191 to the Originating P-CSCF-O 44 in the originating network with the agreed SDP and codecs. The 183 message is sent via the S-CSCF-B 77, the I-CSCF-B 74, and the S-CSCF-A 69. After receiving the SIP 183 message, the Originating P-CSCF-O behaves as in Phase 1: it requests the BB-O 42 to perform the bidirectional reservation by sending a QoS Reservation Request message 192 to the BB-O with the agreed SDP and Binding Information. The BB-O first checks at step 193 to determine whether any reservation was already made for this binding. If not, the BB-O proceeds with the QoS reservation. In this scenario, however, the reservation

was already made, so BB-O answers the Originating P-CSCF's request immediately with a QoS Reservation Success message 194. The Originating P-CSCF-O then forwards the SIP 183 response message 195 to the UE-A 11 with the
5 Agreed SDP and token.

[0065] At 196, the UE-A 11 sends a PRACK message to the UE-B 12, and receives a SIP 200 OK message 197 in response. At 198, the UE-A sends a Reservation message to its Ingress LER-O 21, and includes the token, flow
10 specification, and filter specification. The LER-O sends a Reservation Accepted message in return at 199. Likewise, at 201, the UE-B 12 sends a Reservation message to its Ingress LER-S 25, and includes the token, flow specification, and filter specification. The LER-S sends
15 a Reservation Accepted message in return at 202.

[0066] At 203, the UE-A 11 sends a Condition Met (COMET) message to the UE-B 12 indicating that the QoS has been successfully reserved for the direction from UE-A to UE-B. UE-B responds at 204 with a SIP 200 OK
20 message. Likewise, at 205, the UE-B sends a COMET message to the UE-A indicating that the QoS has been successfully reserved for the direction from UE-B to UE-A. UE-A responds at 206 with a SIP 200 OK message. At 207, a SIP 180 Ringing message is then sent from the UE-B
25 to UE-A via the Terminating P-CSCF-S 51, the S-CSCF-B 77, and the I-CSCF-B 74 in the terminating network 47, and

via the S-CSCF-A 69 and the Originating P-CSCF-O 44 in the originating network 41.

[0067] At 208, the UE-A 11 sends a PRACK message to the UE-B 12 in response to the 180 Ringing message. At 209, the UE-B sends a SIP 200 OK of the PRACK message to the UE-A. At 211, the UE-B sends a SIP 200 OK message to UE-A via the Terminating P-CSCF-S 51, the S-CSCF-B 77, and the I-CSCF-B 74 in the terminating network 47, and via the S-CSCF-A 69 and the Originating P-CSCF-O 44 in the originating network 41. The UE-A responds with an Acknowledgment message at 212, and the process is complete for implementing a Push Policy Mechanism for End-to-End QoS for a SIP call during Phase 2 when there are BBs in every transit network.

[0068] FIG. 8 is a simplified block diagram of the preferred embodiment of the Phase 2 BB Architecture of the present invention when there are BBs in some, but not all, transit networks. Although the transit networks will start introducing BB's in Phase 2, it is still possible to have some transit networks with no BB, either because those networks use over-dimensioning to ensure adequate bandwidth, or because the operators want to keep the same philosophy as in Phase 1. Thus, FIG. 8 is similar to FIG. 6 except that no BB has been implemented in Transit Network-1 17.

[0069] FIGS. 9A-9B are portions of a sequence diagram illustrating implementation of a Push Policy Mechanism for End-to-End QoS for a SIP call during Phase 2 when there are BBs in some, but not all, transit networks.

5 The sequence is identical to that of FIGS. 4A-4B from steps 62 through 87. At that point, step 221, the BB-S 48 determines the ingress-egress edge routers and BB-T2 167. At 222, the BB-S sends a Resource Allocation Request (RAR) message to the BB-T2 indicating a
10 bidirectional session and including the Binding Information. BB-T2 sends a COPS REQ message 223 to its Policy Server (MPS-T2) 170 and receives a COPS DEC message 224 in response. At 225, BB-T2 then determines the ingress-egress edge routers.

15 [0070] The bidirectional reservation started by BB-S 48 with the RAR message 222, does not reach the BB-O 42 because Transit Network-1 17 does not have a BB. In Transit Network-2 162, BB-T2 167 knows that there is no BB in Transit Network-1, so it does not attempt to send
20 an RAR towards it. Instead, BB-T2 responds to the RAR 222 received from BB-S by making sure that the SLA with Transit Network-1 accommodates this traffic. BB-T2 then sends an RAA message 226 back to BB-S. The process then moves to FIG. 9B.

25 [0071] At step 227, BB-T2 sends a COPS DEC message to its egress Router 169, and at 228 sends a COPS DEC

message to its ingress Router 168 with policy instructions and the Binding Information for Transit Network-2 162. Thus, policy is pushed to the edge routers of the Transit Network-2. The BB-S 48 then sends
5 a QoS Reservation (Success) message 229 to the Terminating P-CSCF-S 51. At this time, the BB-S also sends a COPS DEC message 231 to its egress Router 24, and sends a COPS DEC message 232 to its ingress LER-S 25 with policy instructions and the Binding Information for the
10 terminating network 47. Thus, policy is pushed to the edge routers of the terminating network. The Terminating P-CSCF-S then forwards the SIP 183 message 233 to the Originating P-CSCF-O 44 in the originating network with the agreed SDP and codecs.
15 [0072] At 234, the Originating P-CSCF-O 44 sends a QoS Reservation Request message to the BB-O 42 with the agreed SDP and the Binding Information. As a result of the request received from the Originating P-CSCF-O, the BB-O checks at step 235 to determine whether there is any
20 reservation already made for that Binding Information. Since no reservation was made, BB-O proceeds with the QoS reservation as in Phase 1. The BB-O sends a COPS REQ message 236 to the MPS-O 43, and receives a COPS DEC message 237 in response. BB-O then sends a COPS DEC
25 message 238 to the egress router 22, and sends a COPS DEC message 239 to the ingress LER-O 21 with policy

instructions and the Binding Information for the
originating network 41. Thus, policy is pushed to the
edge routers of the originating network. For the
scenario described in FIG. 9, the BB-O may be a Phase 1
5 BB.

[0073] At 241, the BB-O 42 answers the Originating P-
CSCF's QoS Reservation request with a QoS Reservation
(Success) message. The Originating P-CSCF-O then
forwards the SIP 183 response message 242 to the UE-A 11
10 with the Agreed SDP and token. At 243, the UE-A 11 sends
a PRACK message to the UE-B 12, and receives a SIP 200 OK
message 244 in response. At 245, the UE-A sends a
Reservation message to its Ingress LER-O 21, and includes
the token, flow specification, and filter specification.
15 The LER-O sends a Reservation Accepted message in return
at 246. Likewise, at 247, the UE-B 12 sends a
Reservation message to its Ingress LER-S 25, and includes
the token, flow specification, and filter specification.
The LER-S sends a Reservation Accepted message in return
20 at 248.

[0074] At 249, the UE-A 11 sends a COMET message to
the UE-B 12 indicating that the QoS has been successfully
reserved for the direction from UE-A to UE-B. UE-B
responds at 251 with a SIP 200 OK message. Likewise, at
25 252, the UE-B sends a COMET message to the UE-A
indicating that the QoS has been successfully reserved

for the direction from UE-B to UE-A. UE-A responds at 253 with a SIP 200 OK message. At 254, a SIP 180 Ringing message is then sent from the UE-B to UE-A via the Terminating P-CSCF-S 51, the S-CSCF-B 77, and the I-CSCF-B 74 in the terminating network 47, and via the S-CSCF-A 69 and the Originating P-CSCF-O 44 in the originating network 41.

[0075] At 255, the UE-A 11 sends a PRACK message to the UE-B 12 in response to the 180 Ringing message. At 256, the UE-B sends a SIP 200 OK of the PRACK message to the UE-A. At 257, the UE-B sends a SIP 200 OK message to UE-A via the Terminating P-CSCF-S 51, the S-CSCF-B 77, and the I-CSCF-B 74 in the terminating network 47, and via the S-CSCF-A 69 and the Originating P-CSCF-O 44 in the originating network 41. The UE-A responds with an Acknowledgment message at 258, and the process is complete for implementing a Push Policy Mechanism for End-to-End QoS for a SIP call during Phase 2 when there are BBs in some, but not all, transit networks.

[0076] Is also possible to have cases with three or more transit networks where the middle networks do not have BB's. In that case, the transit network which is the neighbor to the originating core network may be Phase-2 upgraded with a BB. Then the BB-O should be Phase-2 upgraded. The reservation triggered by the

Originating P-CSCF-O then goes from BB-O, through BB-T1 up to the middle transit network, which has no BB.

5 [0077] It can be seen from the foregoing description that the Binding Information, as described, is being consistently utilized in all scenarios, regardless of the QoS solution deployed in a specific domain.

10 [0078] It is thus believed that the operation and construction of the present invention will be apparent from the foregoing description. While the method, apparatus and system shown and described has been characterized as being preferred, it will be readily apparent that various changes and modifications could be made therein without departing from the scope of the invention as defined in the following claims.

15

WHAT IS CLAIMED IS:

1 1. A method of ensuring a requested Quality of
2 Service (QoS) for a media flow that is routed from a
3 first terminal in an originating network, through at
4 least one transit network, to a second terminal in a
5 terminating network, said originating network including
6 an Originating Bandwidth Broker (BB-O) and an Originating
7 Media Policy Server (MPS-O), said transit network
8 including a Transit Bandwidth Broker (BB-T) and a Transit
9 Media Policy Server (MPS-T), and said terminating network
10 including a Serving Bandwidth Broker (BB-S) and a Serving
11 Media Policy Server (MPS-S), said method comprising the
12 steps of:
13 sending an origination message from the originating
14 network to the terminating network with a proposed
15 session description that identifies the requested QoS;
16 determining by the terminating network that the
17 session description is agreeable;
18 sending a first Bandwidth Broker Protocol Resource
19 Allocation Request (RAR) from the BB-S to the BB-T with
20 binding information that identifies the first and second
21 terminals and the requested QoS;
22 determining by the BB-T whether a Service Level
23 Agreement (SLA) between the transit network and the

24 terminating network allows sufficient resources to be
25 allocated to meet the requested QoS;

26 sending a second RAR from the BB-T to the BB-O with
27 the binding information, upon determining by the BB-T
28 that the SLA between the transit network and the
29 terminating network allows sufficient resources to be
30 allocated to meet the requested QoS;

31 reserving the resources required to meet the
32 requested QoS in the originating network, the transit
33 network, and the terminating network; and

34 setting up a multimedia session to carry the media
35 flow with the requested QoS.

1 2. The method of ensuring a requested QoS for a
2 media flow of claim 1 further comprising, after the step
3 of sending a second RAR from the BB-T to the BB-O with
4 the binding information, the steps of:

5 sending a first Resource Allocation Answer (RAA)
6 from the BB-O to the BB-T;

7 sending a second RAA from the BB-T to the BB-S; and

8 installing by the BB-O, the BB-T, and the BB-S,
9 applicable policies in edge routers to provide the
10 requested QoS in the originating network, the transit
11 network, and the terminating network, respectively.

1 3. The method of ensuring a requested QoS for a
2 media flow of claim 2 further comprising, before the step
3 of reserving the resources required to meet the requested
4 QoS, the steps of:

5 sending a QoS reservation request that includes the
6 agreed session description and the binding information
7 from an Originating Call State Control Function
8 (Originating P-CSCF) to the BB-O;

9 determining by the BB-O whether a previous valid
10 resource reservation exists for the session associated
11 with the binding information; and

12 sending an immediate successful reservation response
13 from the BB-O to the Originating P-CSCF, upon determining
14 that a previous valid resource reservation exists for the
15 session associated with the binding information.

1 4. The method of ensuring a requested QoS for a
2 media flow of claim 3 further comprising the steps of:

3 reserving resources required for the requested QoS,
4 upon determining that a previous valid resource
5 reservation does not exist for the session associated
6 with the binding information.

1 5. The method of ensuring a requested QoS for a
2 media flow of claim 4 wherein the step of determining by
3 the BB-O whether a previous valid resource reservation
4 exists includes the steps of:

5 determining whether a previous resource reservation
6 was made for the session associated with the binding
7 information; and

8 upon determining that a previous resource
9 reservation was made, determining from a time stamp
10 associated with the previous reservation whether the
11 previous reservation is still valid.

1 6. The method of ensuring a requested QoS for a
2 media flow of claim 3 wherein the step of sending the QoS
3 reservation request from the Originating P-CSCF to the
4 BB-O includes sending the QoS reservation request
5 utilizing a Common Open Policy Service (COPS) protocol
6 and a Bandwidth Broker protocol.

1 7. The method of ensuring a requested QoS for a
2 media flow of claim 1 further comprising the step of
3 creating the binding information from a source Internet
4 Protocol (IP) address of the first terminal, an
5 identification of a Real Time Protocol (RTP) port
6 assigned by the first terminal, a destination IP address

7 of the second terminal, and an identification of an RTP
8 port assigned by the second terminal.

1 8. A Multimedia Control Server (MMCS) in a multi-
2 service core network for ensuring a requested Quality of
3 Service (QoS) for a media flow being routed from a first
4 terminal in the core network to a second terminal in a
5 terminating network, said MMCS comprising:

6 an Originating Call State Control Function
7 (Originating P-CSCF) that serves the first terminal;

8 an Originating Bandwidth Broker (BB-O) that manages
9 resources in the originating network;

10 a first interface between the Originating P-CSCF and
11 the BB-O for passing binding information from the
12 Originating P-CSCF to the BB-O, the binding information
13 identifying the first and second terminals and the
14 requested QoS;

15 an Originating Media Policy Server (MPS-O) that
16 provides policy rules regarding allocation of resources
17 in the originating network;

18 a second interface between the MPS-O and the BB-O
19 for passing the policy rules from the MPS-O to the BB-O;
20 and

21 a third interface between the BB-O and a plurality
22 of edge routers that route the media flow into and out of
23 the originating network, said third interface for passing

24 from the BB-O to the edge routers, policy rules
25 applicable to a specific media flow.

26 9. A Multimedia Control Server (MMCS) in a multi-
27 service core network for ensuring a requested Quality of
28 Service (QoS) for a media flow from an application on a
29 first terminal that is transported through a network
30 owned by an administration, said media flow being routed
31 through at least one transit network that is not owned by
32 the same administration, to a second terminal in a
33 terminating network, said MMCS comprising:

34 an Originating Call State Control Function
35 (Originating P-CSCF) that serves the first terminal;

36 an Originating Bandwidth Broker (BB-O) that manages
37 resources in the originating network;

38 a first interface between the Originating P-CSCF and
39 the BB-O for passing a session description and binding
40 information from the Originating P-CSCF to the BB-O, the
41 binding information identifying the first and second
42 terminals and the requested QoS;

43 an Originating Media Policy Server (MPS-O) that
44 provides policy rules regarding allocation of resources
45 in the originating network;

46 a second interface between the MPS-O and the BB-O
47 for passing the policy rules from the MPS-O to the BB-O;

48 a third interface between the BB-O and a plurality
49 of edge routers that route the media flow into and out of
50 the originating network, said third interface for passing
51 from the BB-O to the edge routers, policy rules
52 applicable to a specific media flow; and

53 a fourth interface between the BB-O and a Transit
54 Bandwidth Broker (BB-T) in the transit network for
55 passing the binding information from the BB-T to the BB-
56 O, said binding information having been received by the
57 BB-T from a Serving Bandwidth Broker (BB-S) in the
58 terminating network.

1 10. The MMCS of claim 9 further comprising a fifth
2 interface between the MPS-O and a clearing house that
3 performs as an Authorization, Authentication, and
4 Accounting (AAA) server.

1 11. A system for ensuring a requested Quality of
2 Service (QoS) for a media flow belonging to an
3 application and originating in an originating network
4 owned by an administration, said media flow being routed
5 from a first terminal in the originating network through
6 at least one transit network that is not owned by the
7 same administration, to a second terminal in a
8 terminating network, said system comprising:

9 a first Multimedia Control Server (MMCS) in the
10 originating network comprising:
11 an Originating Call State Control Function
12 (Originating P-CSCF) that serves the first terminal;
13 an Originating Bandwidth Broker (BB-O) that
14 manages resources in the originating network;
15 a first interface between the Originating P-
16 CSCF and the BB-O for passing a session description and
17 binding information from the Originating P-CSCF to the
18 BB-O, the binding information identifying the first and
19 second terminals and the requested QoS;
20 an Originating Media Policy Server (MPS-O) that
21 provides policy rules regarding allocation of resources
22 in the originating network;
23 a second interface between the MPS-O and the
24 BB-O for passing the policy rules to the BB-O;
25 a plurality of originating edge routers that route
26 the media flow into and out of the originating network;
27 a third interface between the originating edge
28 routers and the BB-O for passing policy rules applicable
29 to specific media flows from the BB-O to the originating
30 edge routers;
31 a second MMCS in the terminating network comprising:
32 a Serving Call State Control Function
33 (Terminating P-CSCF) that serves the second terminal;

34 a Serving Bandwidth Broker (BB-S) that manages
35 resources in the terminating network;
36 a fourth interface between the Terminating P-
37 CSCF and the BB-S for passing an agreed session
38 description from the Terminating P-CSCF to the BB-S;
39 a Serving Media Policy Server (MPS-S) that
40 provides policy rules regarding allocation of resources
41 in the terminating network;
42 a fifth interface between the MPS-S and the BB-
43 S for passing the policy rules from the MPS-S to the BB-
44 S;
45 a plurality of serving edge routers that route the
46 media flow into and out of the terminating network;
47 a sixth interface between the serving edge routers
48 and the BB-S for passing policy rules applicable to
49 specific media flows from the BB-S to the serving edge
50 routers;
51 a Transit Bandwidth Broker (BB-T) in the transit
52 network;
53 a seventh interface between the BB-S and the BB-T
54 for passing the binding information from the BB-S to the
55 BB-T in a first Resource Allocation Request (RAR); and
56 an eighth interface between the BB-T and the BB-O
57 for passing the binding information from the BB-T to the
58 BB-O in a second RAR.

ABSTRACT OF THE DISCLOSURE

5 A system and method of ensuring a requested Quality
of Service (QoS) for a media flow that is transported
through multiple transport networks. An interface is
established between a Call State Control Function (P-
CSCF) and a Bandwidth Broker (BB) for the passing of a
session description and Binding Information from the P-
CSCF to the BB. The interface uses the Common Open
Policy Service (COPS) protocol and the Bandwidth Broker
10 (BB) protocol. The Binding Information may be the source
IP address plus Real Time Protocol (RTP) port and the
destination IP address plus RTP port. The Binding
Information is also passed back toward the Originating BB
(BB-O) from a Serving BB (BB-S) in the terminating
15 (serving) network through BBs in adjacent networks using
the BB protocol.

FIG. 1 (PRIOR ART)

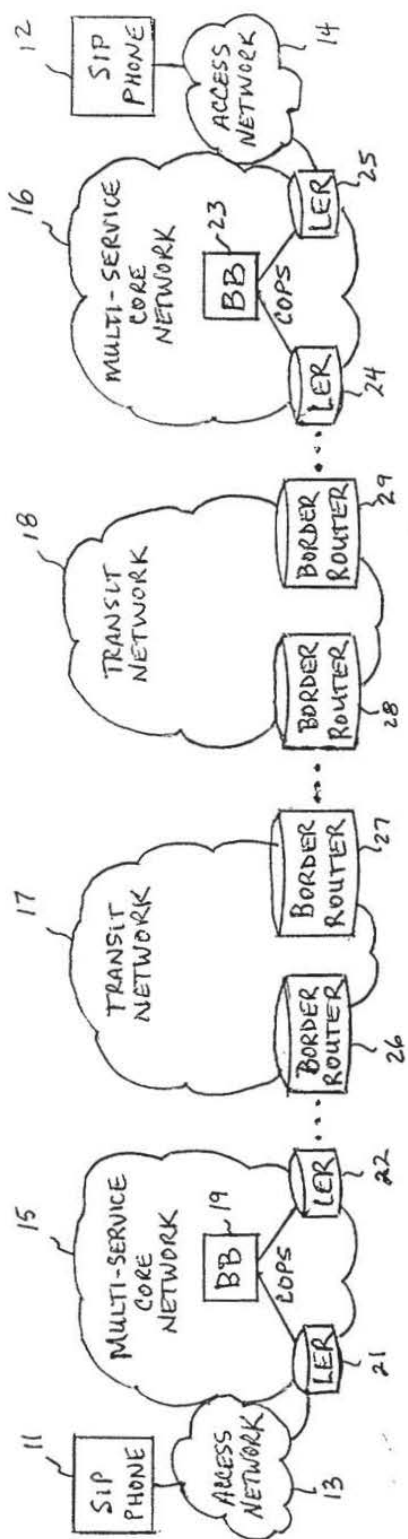


FIG. 1 (PRIOR ART)

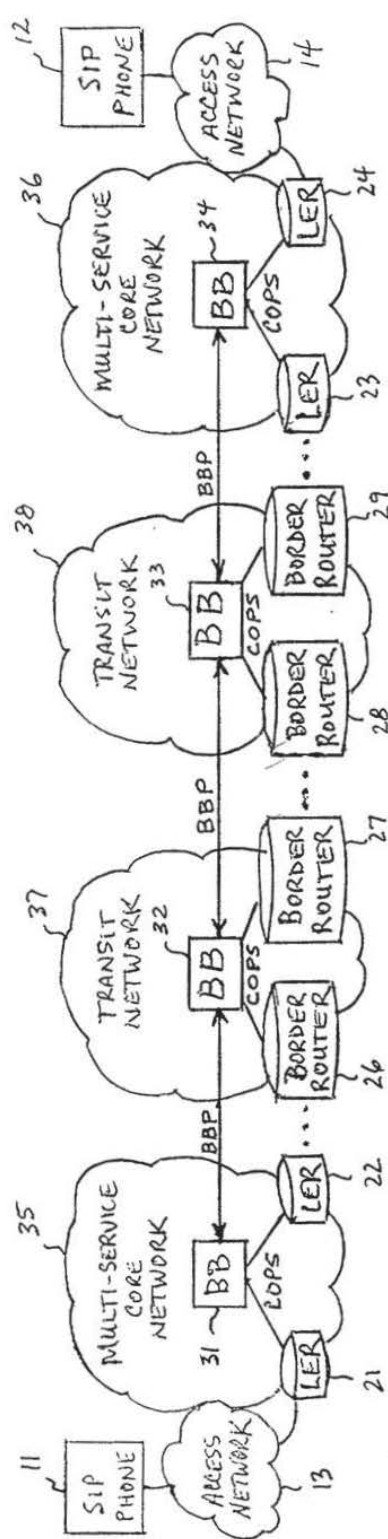


FIG. 2 (PRIOR ART)

FIG. 3

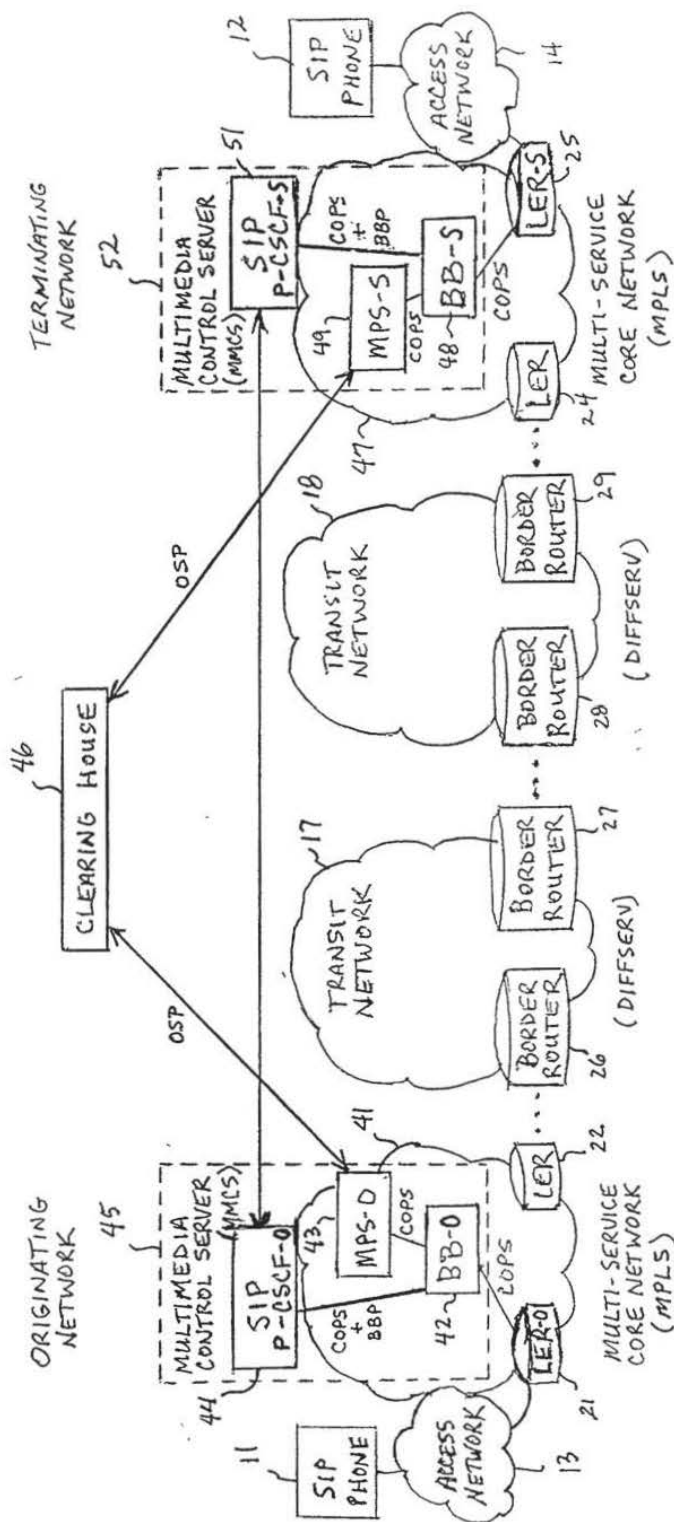


FIG. 3

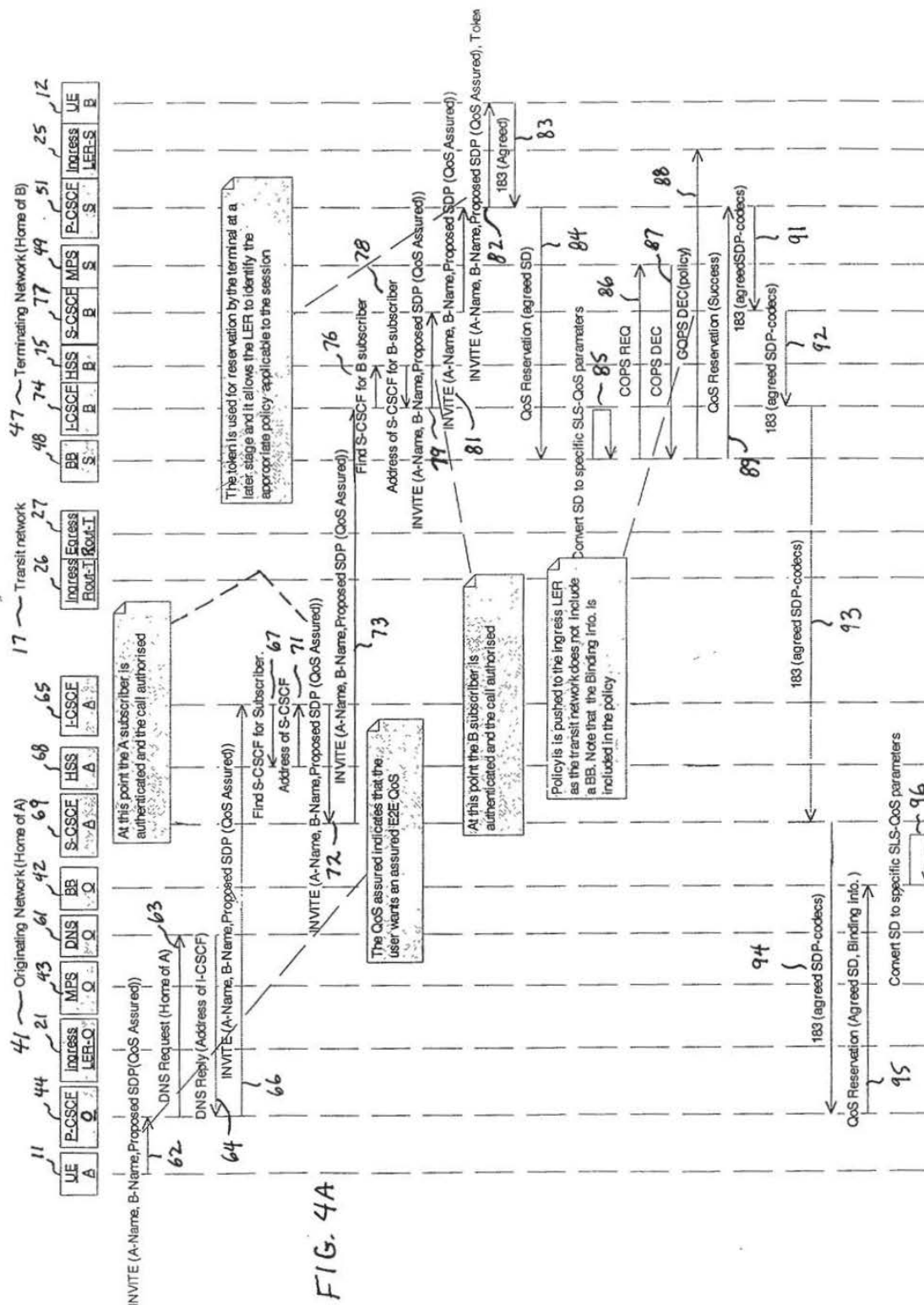


FIG. 4B

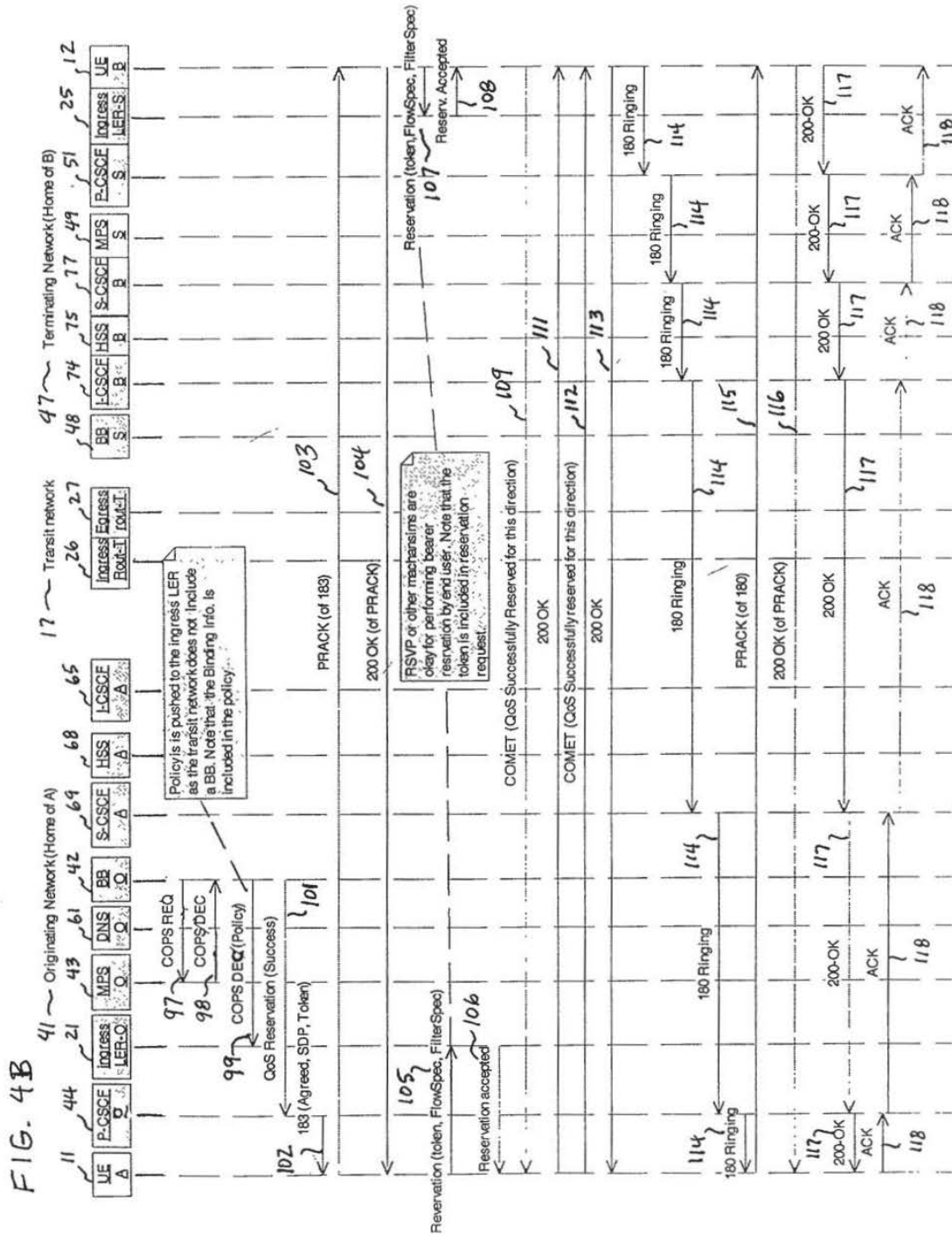


FIG. 5A

FIG. 5A

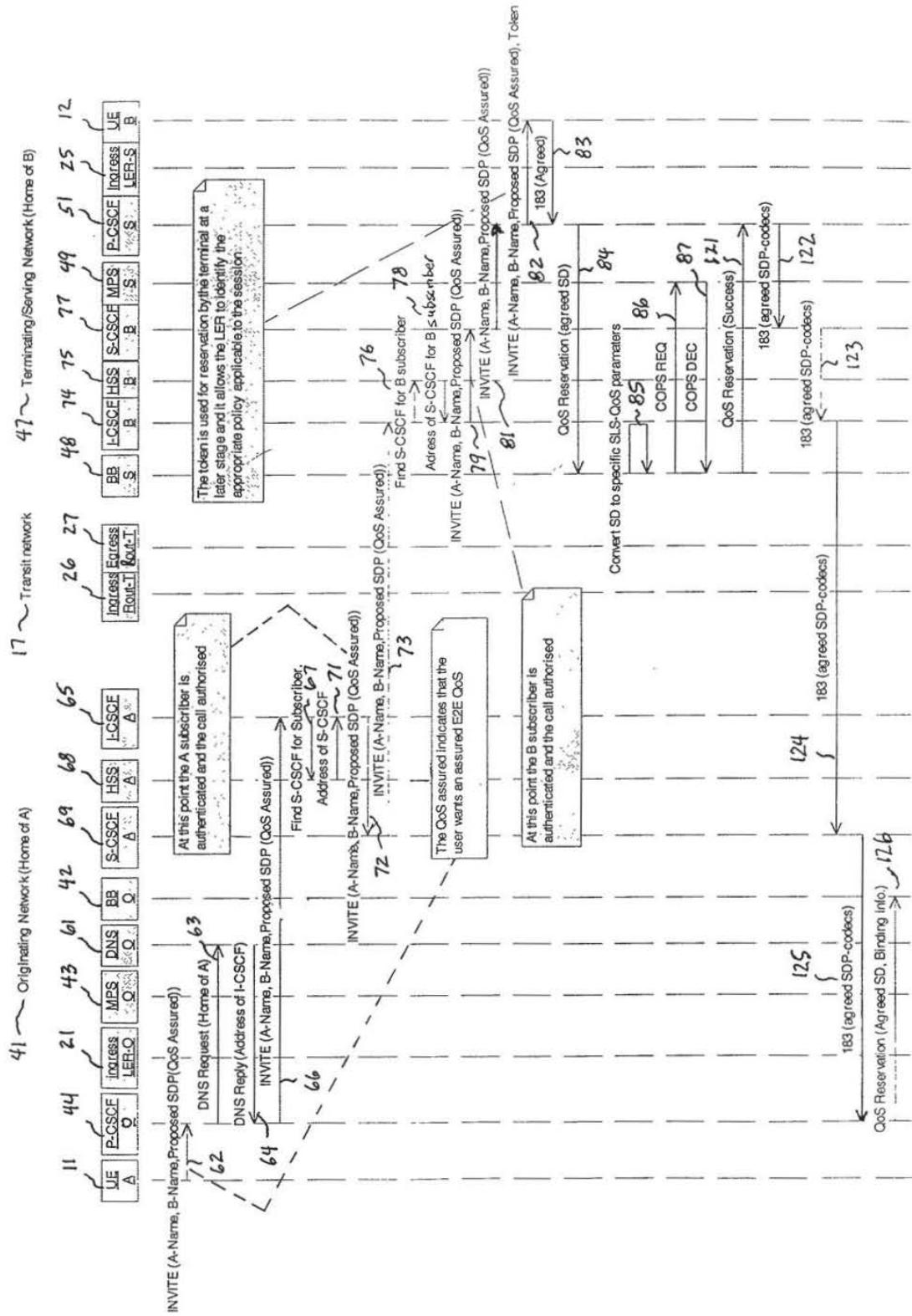


FIG. 5B

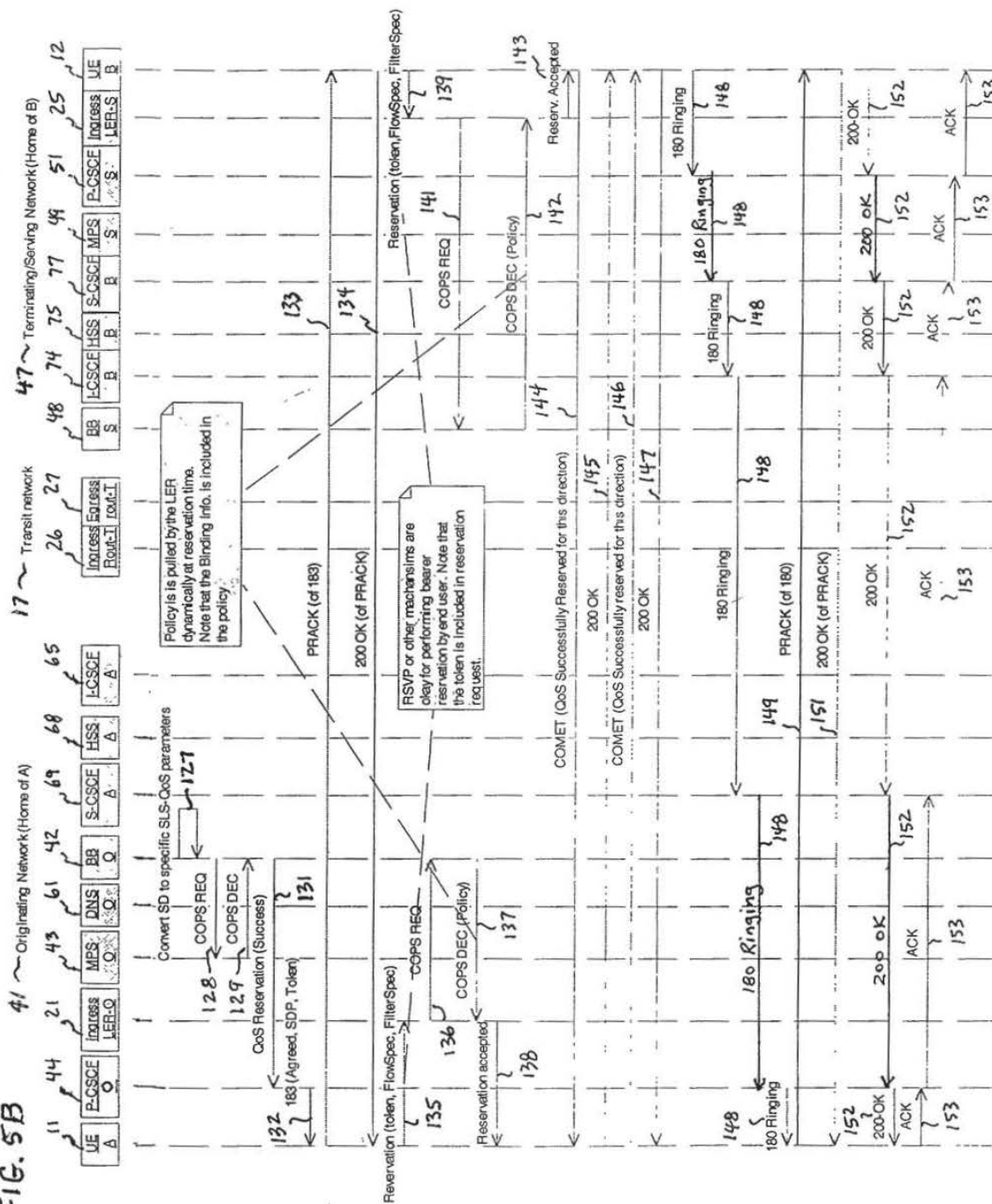


FIG. 6

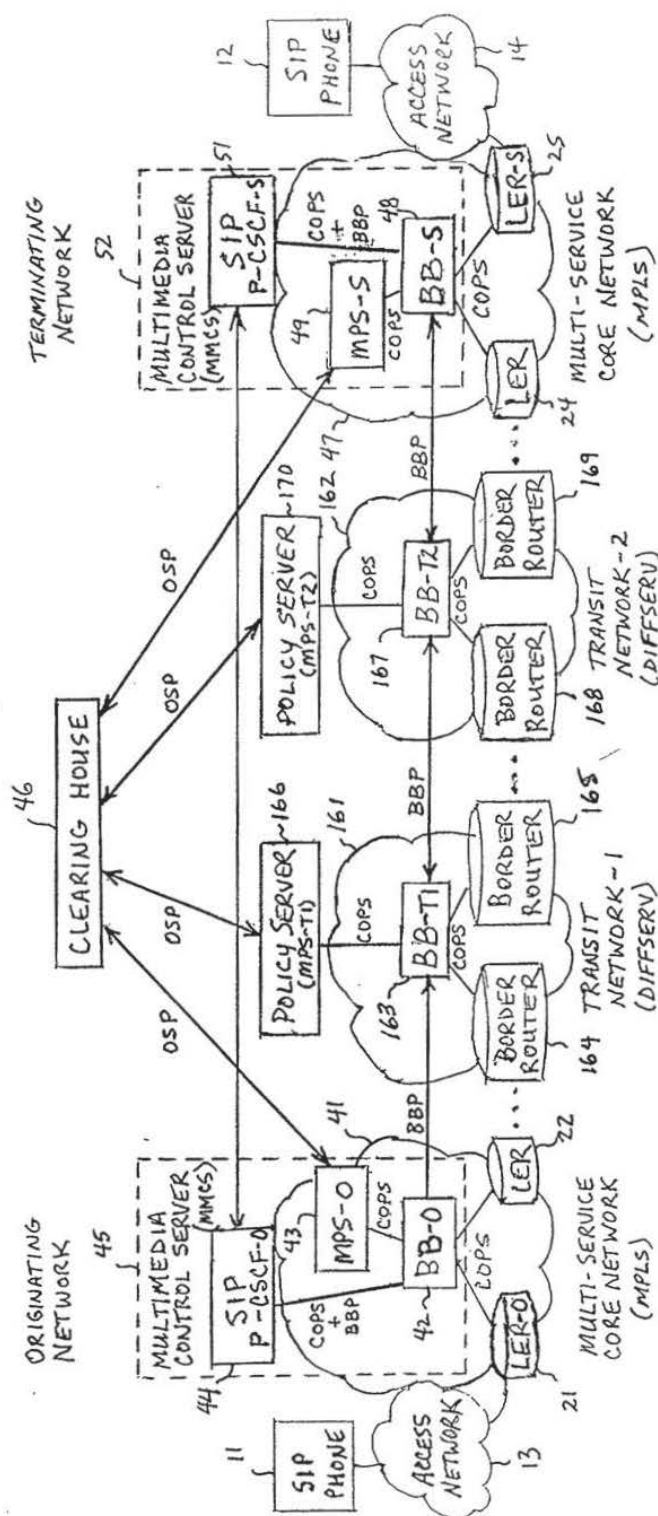
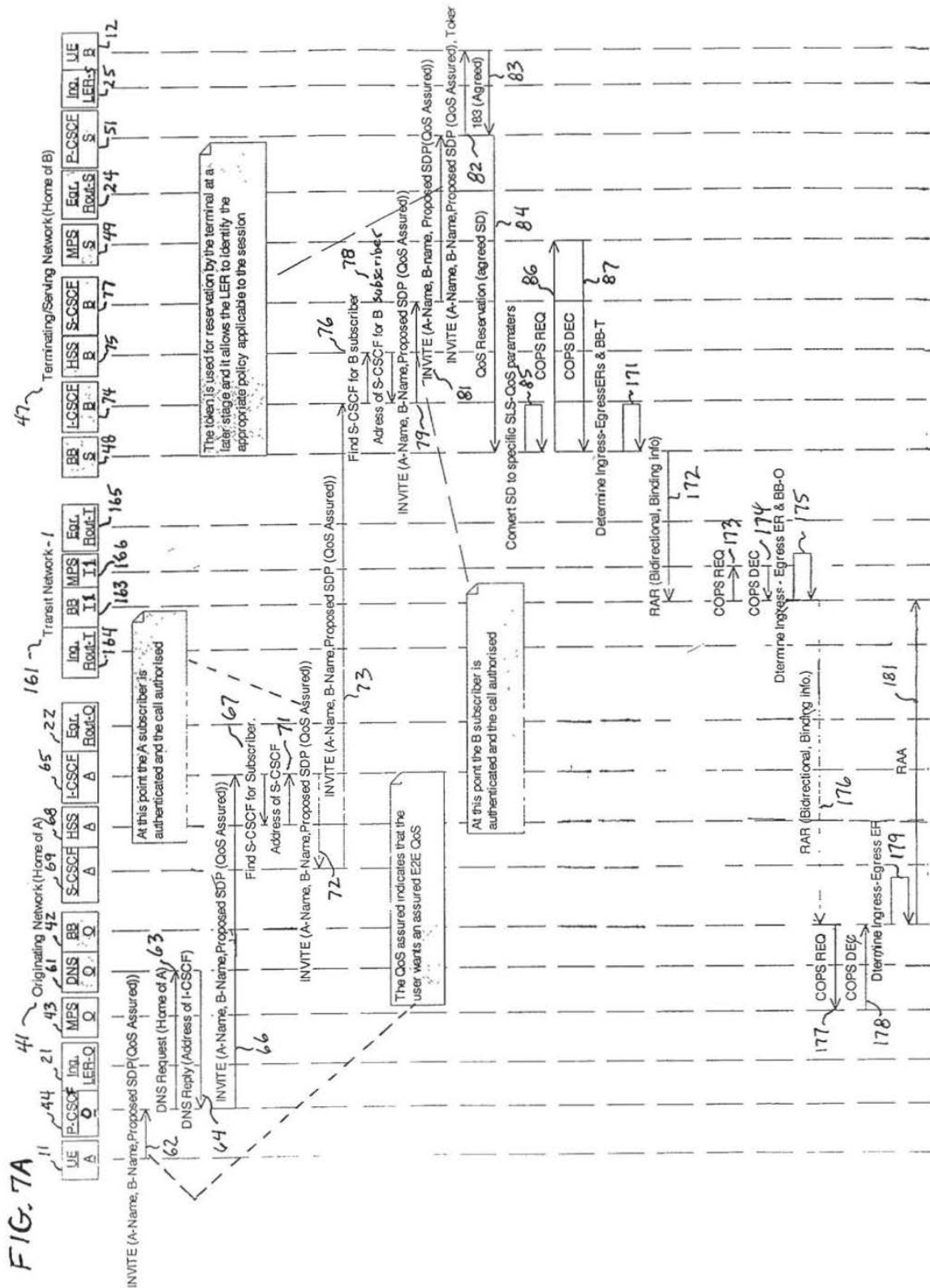
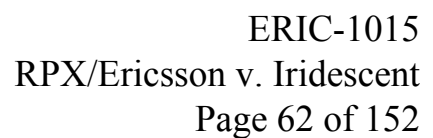


FIG. 6





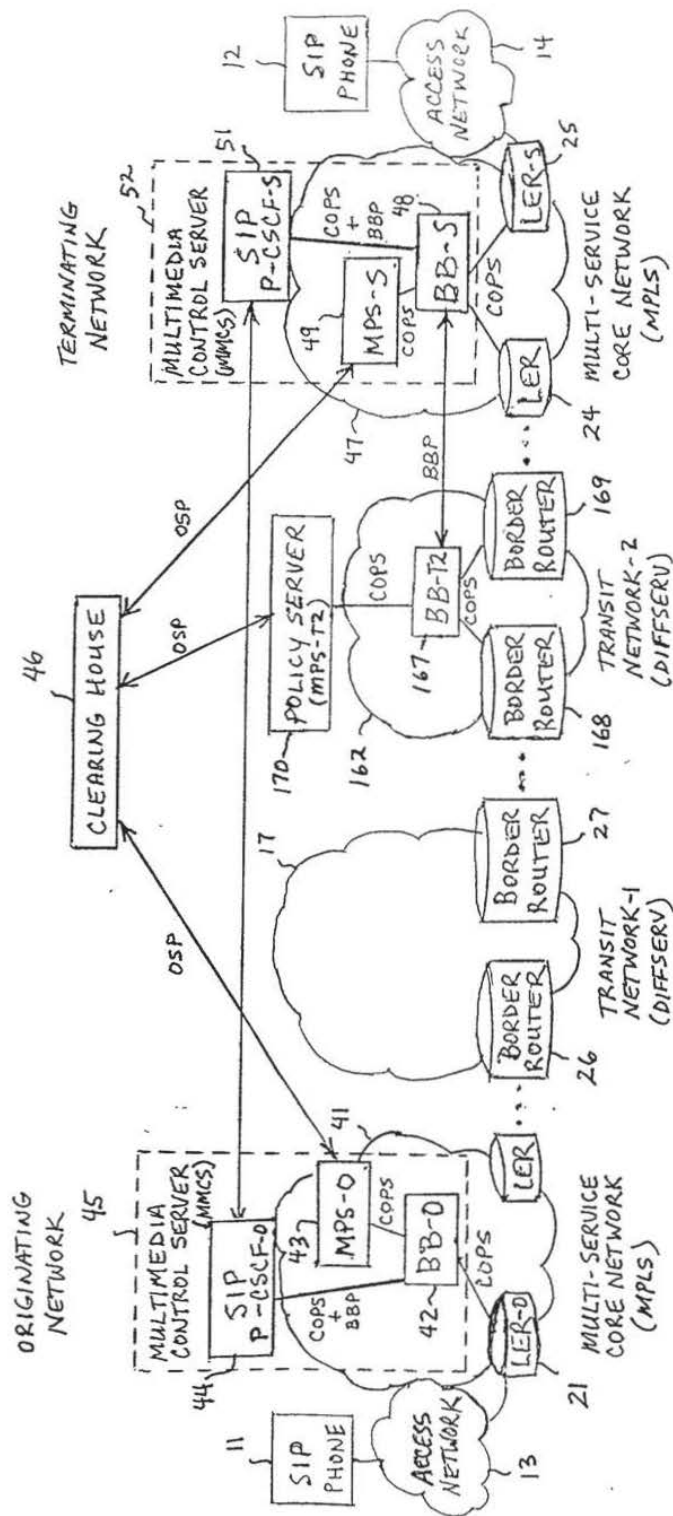
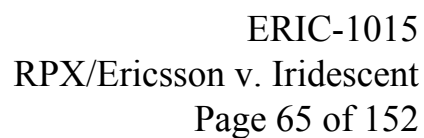


FIG. 8

[illegible]



COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below next to my name; and

I verily believe that I am an original, first, and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled:

**SYSTEM AND METHOD FOR PROVIDING
END-TO-END QUALITY OF SERVICE (QoS) ACROSS
MULTIPLE INTERNET PROTOCOL (IP) NETWORKS**

the specification of which:

X is attached hereto.

— was filed on _____ as Application Serial No. _____ and was
amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Office all information known to me to be material to the patentability of this application as defined in 37 CFR § 1.56.

I hereby claim the benefit under 35 U.S.C. § 119(e) of any previously filed United States provisional patent application(s) listed below which were filed not more than 12 months before the filing of this application, and which disclose the invention of this application in the manner provided by the first paragraph of 35 U.S.C. § 112:

Provisional Application No.

Filing Date

DOCKET NO. 1000-0216

PATENT

I hereby claim foreign priority benefits under 35 U.S.C. § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of any application on which priority is claimed:

| Country | Number | Date Filed | Priority Claimed |
|---------|--------|------------|------------------|
| _____ | _____ | _____ | _____ |
| _____ | _____ | _____ | _____ |

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose material information as defined in 37 CFR § 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

| Application Serial No. | Filing Date | Status (patented, pending) |
|------------------------|-------------|----------------------------|
| _____ | _____ | _____ |
| _____ | _____ | _____ |

I hereby appoint the following attorneys and/or agents to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith: STEVEN W. SMITH, Reg. No. 36,684 and LAWRENCE R. YOUST, Reg. No. 38,795 of the firm of Smith, Danamraj & Youst, P.C., 12900 Preston Road, Suite 1200, LB 15, Dallas, Texas 75230; and STANLEY R. MOORE, Reg. No. 26,958 and GERALD T. WELCH, Reg. No. 30,332 of the firm of Jenkins & Gilchrist, 1445 Ross Avenue, Suite 3200, Dallas, Texas 75202.

Address all telephone calls and correspondence to:

Steven W. Smith
SMITH, DANAMRAJ & YOUST, P.C.
12900 Preston Road, Suite 1200, LB 15
Dallas, Texas 75230-1328
(972) 720-1202

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

| | | | |
|---|--|-----------------------------|--------------------|
| 1 | Sorin Surdila | | |
| | Full Name | Inventor's Signature | Date |
| | 463 Toussaint St. Dorothee Laval, Quebec CANADA H7X 3N3 | | CANADA |
| | Residence | | Citizenship |
| | 463 Toussaint St. Dorothee Laval, Quebec CANADA H7X 3N3 Mailing Address | | |

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

| | | | |
|---|---|-----------------------------|-------------|
| 2 | George Foti | | |
| | Full Name | Inventor's Signature | Date |
| | 163 Mozart Dollard des Ormeaux, Quebec CANADA H9G 2Z8 | CANADA | |
| | Residence | Citizenship | |
| | 163 Mozart Dollard des Ormeaux, Quebec CANADA H9G 2Z8 Mailing Address | | |

United States Patent & Trademark Office
Office of Initial Patent Examination -- Scanning Division



Application deficiencies found during scanning:

☒ Page(s) _____ of Certificate of mailing were not present
for scanning. (Document title)

☐ Page(s) _____ of _____ were not present
for scanning. (Document title)

☐ *Scanned copy is best available.*



UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov



Bib Data Sheet

CONFIRMATION NO. 6405

| | | | | |
|---|---|-----------------------------------|---|---|
| SERIAL NUMBER 09/841,752 | FILING DATE 04/24/2001 RULE | CLASS 370 | GROUP ART UNIT 2661 | ATTORNEY DOCKET NO. 1000-0216 |
| APPLICANTS Sorin Surdila, Laval, CANADA; George Foti, Dollard des Ormeaux, CANADA; | | | | |
| ** CONTINUING DATA ***** | | | | |
| ** FOREIGN APPLICATIONS ***** | | | | |
| IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 06/15/2001 | | | | |
| Foreign Priority claimed <input type="checkbox"/> yes <input type="checkbox"/> no 35 USC 119 (a-d) conditions <input type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> Met after met Allowance Verified and Acknowledged Examiner's Signature Initials | | STATE OR COUNTRY CANADA | SHEETS DRAWING 12 | TOTAL CLAIMS 11 |
| | | | | INDEPENDENT CLAIMS 4 |
| ADDRESS Smith, Danamraj & Youst, P.C. 12900 Preston Road, Suite 1200, LB-15 Dallas, TX 75230 | | | | |
| TITLE System and method for providing end-to-end quality of service (QoS) across multiple internet protocol (IP) networks | | | | |
| FILING FEE RECEIVED 920 | FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following: | | <input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit | |

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

04/27/2001 EHAILE1 00000040 09841752

| | |
|-----------|-----------|
| 01 FC:101 | 710.00 OP |
| 02 FC:102 | 80.00 OP |

PTO-1556
(5/87)

*U.S. GPO: 2000-468-887/39595

PATENT APPLICATION FEE DETERMINATION RECORD

Effective October 1, 2000

Application or Docket Number

1000-0216

CLAIMS AS FILED - PART I

| | (Column 1) | (Column 2) |
|---|---------------|--------------|
| TOTAL CLAIMS | 11 | |
| FOR | NUMBER FILED | NUMBER EXTRA |
| TOTAL CHARGEABLE CLAIMS | 11 minus 20 = | 0 |
| INDEPENDENT CLAIMS | 9 minus 3 = | 1 |
| MULTIPLE DEPENDENT CLAIM PRESENT <input type="checkbox"/> | | |

* If the difference in column 1 is less than zero, enter "0" in column 2

CLAIMS AS AMENDED - PART II

| | (Column 1) | (Column 2) | (Column 3) |
|---|----------------------------------|------------------------------------|---------------|
| AMENDMENT A | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
| Total | * | Minus ** | = |
| Independent | * | Minus *** | = |
| FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/> | | | |

| | (Column 1) | (Column 2) | (Column 3) |
|---|----------------------------------|------------------------------------|---------------|
| AMENDMENT B | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
| Total | * | Minus ** | = |
| Independent | * | Minus *** | = |
| FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/> | | | |

| | (Column 1) | (Column 2) | (Column 3) |
|---|----------------------------------|------------------------------------|---------------|
| AMENDMENT C | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
| Total | * | Minus ** | = |
| Independent | * | Minus *** | = |
| FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/> | | | |

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

SMALL ENTITY TYPE ☐

OR OTHER THAN SMALL ENTITY

| RATE | FEE | | RATE | FEE |
|-----------|--------|----|-----------|--------|
| BASIC FEE | 355.00 | OR | BASIC FEE | 710.00 |
| X\$ 9= | | OR | X\$18= | |
| X40= | | OR | X80= | 80 |
| +135= | | OR | +270= | |
| TOTAL | | OR | TOTAL | 740 |

| RATE | ADDITIONAL FEE | | RATE | ADDITIONAL FEE |
|------------------|----------------|----|------------------|----------------|
| X\$ 9= | | OR | X\$18= | |
| X40= | | OR | X80= | |
| +135= | | OR | +270= | |
| TOTAL ADDIT. FEE | | OR | TOTAL ADDIT. FEE | |

| RATE | ADDITIONAL FEE | | RATE | ADDITIONAL FEE |
|------------------|----------------|----|------------------|----------------|
| X\$ 9= | | OR | X\$18= | |
| X40= | | OR | X80= | |
| +135= | | OR | +270= | |
| TOTAL ADDIT. FEE | | OR | TOTAL ADDIT. FEE | |

| RATE | ADDITIONAL FEE | | RATE | ADDITIONAL FEE |
|------------------|----------------|----|------------------|----------------|
| X\$ 9= | | OR | X\$18= | |
| X40= | | OR | X80= | |
| +135= | | OR | +270= | |
| TOTAL ADDIT. FEE | | OR | TOTAL ADDIT. FEE | |

| CLAIMS ONLY | | | | | | | SERIAL NO. 09841752 | FILING DATE 04-24-01 |
|--------------------|----------|------|------------------------|------|------------------------|------|-------------------------------|--------------------------------|
| | | | | | | | APPLICANT(S) | |
| CLAIMS | | | | | | | | |
| | AS FILED | | AFTER 1st AMENDMENT | | AFTER 2nd AMENDMENT | | | |
| | IND. | DEP. | IND. | DEP. | IND. | DEP. | * | * |
| 1 | / | | | | | | | |
| 2 | | / | | | | | | |
| 3 | | / | | | | | | |
| 4 | | / | | | | | | |
| 5 | | / | | | | | | |
| 6 | | / | | | | | | |
| 7 | | / | | | | | | |
| 8 | / | | | | | | | |
| 9 | / | | | | | | | |
| 10 | | / | | | | | | |
| 11 | / | | | | | | | |
| 12 | | | | | | | | |
| 13 | | | | | | | | |
| 14 | | | | | | | | |
| 15 | | | | | | | | |
| 16 | | | | | | | | |
| 17 | | | | | | | | |
| 18 | | | | | | | | |
| 19 | | | | | | | | |
| 20 | | | | | | | | |
| 21 | | | | | | | | |
| 22 | | | | | | | | |
| 23 | | | | | | | | |
| 24 | | | | | | | | |
| 25 | | | | | | | | |
| 26 | | | | | | | | |
| 27 | | | | | | | | |
| 28 | | | | | | | | |
| 29 | | | | | | | | |
| 30 | | | | | | | | |
| 31 | | | | | | | | |
| 32 | | | | | | | | |
| 33 | | | | | | | | |
| 34 | | | | | | | | |
| 35 | | | | | | | | |
| 36 | | | | | | | | |
| 37 | | | | | | | | |
| 38 | | | | | | | | |
| 39 | | | | | | | | |
| 40 | | | | | | | | |
| 41 | | | | | | | | |
| 42 | | | | | | | | |
| 43 | | | | | | | | |
| 44 | | | | | | | | |
| 45 | | | | | | | | |
| 46 | | | | | | | | |
| 47 | | | | | | | | |
| 48 | | | | | | | | |
| 49 | | | | | | | | |
| 50 | | | | | | | | |
| TOTAL IND. | 4 | ↓ | | ↓ | | ↓ | | |
| TOTAL DEP. | 7 | ← | | ← | | ← | | |
| TOTAL CLAIMS | 11 | | | | | | | |
| 51 | | | | | | | | |
| 52 | | | | | | | | |
| 53 | | | | | | | | |
| 54 | | | | | | | | |
| 55 | | | | | | | | |
| 56 | | | | | | | | |
| 57 | | | | | | | | |
| 58 | | | | | | | | |
| 59 | | | | | | | | |
| 60 | | | | | | | | |
| 61 | | | | | | | | |
| 62 | | | | | | | | |
| 63 | | | | | | | | |
| 64 | | | | | | | | |
| 65 | | | | | | | | |
| 66 | | | | | | | | |
| 67 | | | | | | | | |
| 68 | | | | | | | | |
| 69 | | | | | | | | |
| 70 | | | | | | | | |
| 71 | | | | | | | | |
| 72 | | | | | | | | |
| 73 | | | | | | | | |
| 74 | | | | | | | | |
| 75 | | | | | | | | |
| 76 | | | | | | | | |
| 77 | | | | | | | | |
| 78 | | | | | | | | |
| 79 | | | | | | | | |
| 80 | | | | | | | | |
| 81 | | | | | | | | |
| 82 | | | | | | | | |
| 83 | | | | | | | | |
| 84 | | | | | | | | |
| 85 | | | | | | | | |
| 86 | | | | | | | | |
| 87 | | | | | | | | |
| 88 | | | | | | | | |
| 89 | | | | | | | | |
| 90 | | | | | | | | |
| 91 | | | | | | | | |
| 92 | | | | | | | | |
| 93 | | | | | | | | |
| 94 | | | | | | | | |
| 95 | | | | | | | | |
| 96 | | | | | | | | |
| 97 | | | | | | | | |
| 98 | | | | | | | | |
| 99 | | | | | | | | |
| 100 | | | | | | | | |
| TOTAL IND. | | ↓ | | ↓ | | ↓ | | |
| TOTAL DEP. | | ← | | ← | | ← | | |
| TOTAL CLAIMS | | | | | | | | |

* MAY BE USED FOR ADDITIONAL CLAIMS OR AMENDMENTS

FORM PTO-2022 (1-98)
U.S. DEPARTMENT OF COMMERCE
Patent and Trademark Office



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) EP 0 999 674 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
10.05.2000 Bulletin 2000/19

(51) Int Cl.7: H04L 12/64, H04L 12/56,
H04L 12/24, H04M 7/00,
H04Q 3/00

(21) Application number: 99307282.6

(22) Date of filing: 14.09.1999

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

- Hernandez-Valencia, Enrique
Highlands, New Jersey 07732 (US)
- Sriram, Kotikalapudi
Marlboro, New Jersey 07746 (US)
- Wang, Yung-Terng
Marlboro, New Jersey 07746 (US)
- Yue, On-Ching
Middletown, New Jersey 07748 (US)

(30) Priority: 22.09.1998 US 158694

(71) Applicant: LUCENT TECHNOLOGIES INC.
Murray Hill, New Jersey 07974-0636 (US)

(74) Representative:
Watts, Christopher Malcolm Kelway, Dr. et al
Lucent Technologies (UK) Ltd,
5 Morington Road
Woodford Green Essex, IG8 0TU (GB)

(72) Inventors:
• Doshi, Bharat Tarachand
Homdel, New Jersey 07733 (US)

(54) Method for providing quality of service for delay sensitive traffic over IP networks

(57) A quality of service guarantee for voice and other delay sensitive transmissions within an Internet Protocol (IP) network is provided by identifying the IP network path utilized for IP packet transmission between source and destination edge devices and virtually provisioning IP network path bandwidth for priority voice traffic. Priority for voice packets and admission control of new voice calls (and other delay sensitive traffic) based on the remaining available capacity over the IP network path guarantees that high priority voice (and other delay sensitive traffic) meet stringent delay requirements. A Virtual Provisioning Server is utilized to

maintain bandwidth capacity data for each path segment within the IP network and to forward the bandwidth capacity data to a Signaling Gateway. The Signaling Gateway determines whether to accept or reject an additional delay sensitive traffic component based upon available bandwidth capacity for an IP network path. The Signaling Gateway then signals the originating source edge device as to its determination to accept or reject. Quality of Service guarantees concerning acceptable delay and jitter characteristics for real-time transmission over an IP network are therefore provided without the need to directly signal the individual IP routers over which an IP network path is established.

EP 0 999 674 A1

Description**FIELD OF THE INVENTION**

[0001] The present invention relates to the field of Internet Protocol (IP) networks, and more particularly to the transport of delay sensitive traffic over IP networks.

BACKGROUND OF THE INVENTION

[0002] A global network infrastructure for voice services, using a circuit-switching methodology, is supported by Public Switched Telephone and Private Branch Exchange networks. These networks utilize signaling to establish call connections and routing maps at network switches. The ability to signal during call connection setup provides individual switches with the capability to reject call connection requests when that individual switch does not have the available bandwidth to support a new call connection. Since any switch in a connection path may reject a new call connection request based on available bandwidth limitations, switched voice networks are able to provide guaranteed Quality of Service to established connections. Quality of Service in switched voice networks is guaranteed because the governing precept is that it is preferable to block new call connection attempts rather than allow a new connected call to degrade the performance of established connected calls.

[0003] Explosive growth in Internet Protocol (IP) based Intranets and public Internet has generated a large network infrastructure of IP based routers. Recently, this large IP network infrastructure has begun to be utilized as a vehicle for real-time transmission of voice over the Internet, also known as Internet telephony. Each year, Internet telephony captures a greater share of the telephony market. However, unlike the case of switched voice service networks, routers contained within IP networks are not signaled. Since signaling between source, destination, and intermediate routers is not provided within IP networks, new calls can not be rejected at the IP routers, even if the routers are burdened beyond their respective bandwidth capacities. Therefore, real-time transmission over the Internet is subject to levels of delay and jitter not associated with Public Switched Telephone Networks and Private Branch Exchanges. Rather, transmission over the Internet and other IP networks is accomplished via a best effort transmission mode. Consequently, telephony over IP networks does not currently provide a Quality of Service guarantee for voice and other delay sensitive transmissions.

SUMMARY OF THE INVENTION

[0004] A quality of service guarantee for voice and other delay sensitive transmissions within an Internet Protocol (IP) network is provided by identifying the IP network path utilized for IP packet transmission be-

tween source and destination edge devices and virtually provisioning IP network path bandwidth for priority voice traffic. Priority for voice packets and admission control of new voice calls (and other delay sensitive traffic) based on the remaining available capacity over the IP network path guarantees that high priority voice (and other delay sensitive traffic) meet stringent delay requirements. A Virtual Provisioning Server is utilized to maintain bandwidth capacity data for each path segment within the IP network and to forward the bandwidth capacity data to a Signaling Gateway. The Signaling Gateway determines whether to accept or reject an additional delay sensitive traffic component based upon available bandwidth capacity for an IP network path. The Signaling Gateway then signals the originating source edge device as to its determination to accept or reject. Quality of Service guarantees concerning acceptable delay and jitter characteristics for real-time transmission over an IP network are therefore provided without the need to directly signal the individual IP routers over which an IP network path is established.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] A more complete understanding of the present invention may be obtained from consideration of the following description in conjunction with the drawings in which:

FIG. 1 is a diagram illustrating a voice over IP network between Packet Circuit Gateway edge devices and incorporating a Virtual Provisioning Server, the Virtual Provisioning Server communicating with a plurality of Signaling Gateways, in accordance with an exemplary embodiment of the present invention;

FIG. 2 is a diagram illustrating a voice over IP network between Packet Circuit Gateway edge devices and incorporating a Virtual Provisioning Server, the Virtual Provisioning Server communicating with a Signaling Gateway co-located with one Packet Circuit Gateway, and providing Signaling Gateway functionality to more than one Packet Circuit Gateway within the network, in accordance with an exemplary embodiment of the present invention;

FIG. 3 is a diagram illustrating a voice over IP network between Packet Circuit Gateway edge devices and incorporating a Virtual Provisioning Server, the Virtual Provisioning Server further performing functions as a Virtual Private Network (VPN) Resource Manager, in accordance with an exemplary embodiment of the present invention;

FIG. 4 is a diagram illustrating the bandwidth allocation structure associated with an exemplary embodiment of the present invention; and

FIG. 5 is a flow diagram illustrating one exemplary embodiment of an algorithm for call admission control for a plurality of Virtual Private Networks sharing

a link within a common network, in accordance with the present invention.

DETAILED DESCRIPTION

[0006] FIGS. 1, 2, and 3 are diagrams illustrating various embodiments for IP networks 205 between Packet Circuit Gateway edge devices 215 incorporating a Virtual Provisioning Server 230, in accordance with the present invention. In FIG. 1, the Virtual Provisioning Server 230 communicates with a Signaling Gateway 250 associated with each Packet Circuit Gateway edge device 215. In FIG. 2, the Virtual Provisioning Server 230 communicates with a Signaling Gateway 250 co-located with one Packet Circuit Gateway 215, and providing Signaling Gateway functionality to more than one Packet Circuit Gateway 215 within the network. In FIG. 3, the Virtual Provisioning Server 230 performs additional functions as a Virtual Private Network Resource Manager.

[0007] The present invention is described as being utilized within an environment wherein voice traffic originates and terminates on regular Public Switched Telephone Network circuit switches, such as Synchronous Transfer Mode switches 210, and is carried over paths between routers within an IP network 205. However, these circuit switches may also be implemented as simple access multiplexers or edge vehicles as would be apparent to those skilled in the art. It would also be apparent to those skilled in the art that the present invention may be practiced with any IP datagram traffic (in addition to voice), although the present invention provides the greatest benefit for the transport of delay sensitive IP datagram traffic. Conversion from a circuit signal to IP format occurs at Packet Circuit Gateways (PCGs) 215, which are also alternatively known as Service Access Concentrators (SACs) or Internet Telephone Gateways. In addition to conversion between circuit and IP formats, Packet Circuit Gateways 215 also provide voice compression/decompression, silence suppression/insertion, and other well known functions needed for specific applications.

[0008] Signaling Gateways 250 are utilized to provide the appropriate interface and interworking between signaling mechanisms and also to determine acceptance or rejection of a new call request originating from an associated Packet Circuit Gateway. Circuit networks, such as Public Switched Telephone Networks, typically use Signaling System 7 (SS7) to communicate requests for connection set-up and tear down. IP endpoints and intermediate routers use ITU-T H.323 or Session Initiation Protocol (SIP) for session management. Therefore, Signaling Gateways 250 provide a higher layer protocol utilized at the Packet Circuit Gateways 215 to facilitate conversions in signaling mechanisms between Public Switched Telephone Networks and IP networks 205. It should be noted that a resident Signaling Gateway 250 is not required at each Packet Circuit Gateway. Rather,

the Signaling Gateway function may be implemented at a single location for all Packet Circuit Gateways with control signals transmitted to corresponding Packet Circuit Gateways from the single Signaling Gateway. For example, FIGS. 1 and 3 illustrate embodiments of the present invention wherein each Packet Circuit Gateway 215 maintains a resident Signaling Gateway 250. However, FIG. 2 illustrates an embodiment of the present invention wherein only PCG#1 maintains a resident Signaling Gateway 250. The Signaling Gateway functions are provided at PCG#2, PCG#3, and PCG#4 by transmission of appropriate control signals between the Signaling Gateway resident at PCG#1 and the remaining Packet Circuit Gateways. Transmission may be over the serviced IP network 205 within a TCP/IP session, an adjunct transmission medium, or any other well known means for data transport.

[0009] One unique feature of the present invention is provided by a Virtual Provisioning Server 230. The Virtual Provisioning Server is utilized to provide the Signaling Gateways 250 with network bandwidth capability information, so that the Signaling Gateways are able to make a determination as to whether to accept or reject a new call request at an associated Packet Circuit Gateway 215. The basis for admission/denial decisions for new calls is made in order to provide assurances that Quality of Service characteristics, such as delay, jitter, and loss of call connections, are maintained below a guaranteed threshold for established voice call connections.

[0010] The Virtual Provisioning Server 230 communicates the network bandwidth capability information to the Signaling Gateways 250 at least once at the commencement of network operation, and episodically whenever the underlying IP network is subject to changes to its link bandwidths due to link failures, new link establishment, addition of bandwidth to existing links, etc. A Network Management System (NMS) is typically associated with an IP network and its functions well known in the art. However, in association with the present invention the Network Management System performs the additional function of apprising the Virtual Provisioning Server of any changes to the link bandwidths as enunciated above.

[0011] FIGS. 1-3 illustrate a network path 255 for the transport of IP packets between PCG#1 and PCG#2. The path 255 is via intermediate components Router #1 and Router #2. Routers 220 are interconnected at the physical layer within the IP network 205 by a plurality of physical layer router transport segments 225. It is over a plurality of these physical layer router transport segments 225 that the illustrated network path 255 is established. A network path 255 is comprised of a plurality of path links established over the plurality of physical layer router transport segments 225. The Virtual Provisioning Server 230, in cooperation with the Public Switched Telephone Network provisioning mechanism and admission control implemented by the Signaling

Gateway 250, provides for a quality guarantee to voice traffic while allowing the remaining capacity in the IP network to be used by other traffic utilizing the well known best effort mode. Similar provisioning can extend the service guarantee to multiple classes of traffic, for example - video conferencing.

[0012] Given that specific STM switches 210 are tied to corresponding Packet Circuit Gateways 215, voice call transport capacity can be easily predicted using standard traffic engineering methods to determine the capacity needed between Packet Circuit Gateways 215. Specific format variables, such as the type of compression method used, the silence suppression capability, etc., determine the network path bandwidth requirements between each pair of Packet Circuit Gateways 215. The Virtual Provisioning Server 230 maintains and manages data corresponding to the transmission capacities of the IP network routers 220 and the physical layer router transport segments 225 between those routers 220. The Virtual Provisioning Server is used, in accordance with the present invention, to determine the capacity requirements over each path between IP network routers 220 to meet the needed bandwidth requirements between Packet Circuit Gateways 215. The capacity requirements over each network element, such as routers 220 and physical layer router transport segments 225 are virtually provisioned within available bandwidth capacity for delay sensitive traffic requirements. In accordance with the present invention, the bandwidth is considered virtually provisioned since the admission/denial of new connected calls is not controlled at each individual router 220, but rather at the Packet Circuit Gateway edge devices 215. Remaining bandwidth capacity over network elements is made available to delay insensitive packet transport only after the provisioning of bandwidth for delay sensitive voice frames or IP packets at the Packet Circuit Gateways 215 is performed. Alternatively, a provisioned minimum bandwidth capacity over each IP network path may be reserved for delay insensitive traffic, with the remaining bandwidth allocated for use by delay sensitive traffic. A Type-of-Service (TOS) field in the IP packet header is utilized to distinguish between delay sensitive and delay tolerant traffic types. Thus, voice packets may be given priority over data packets to ensure that delay and packet loss is in accordance with Quality of Service requirements.

[0013] If IP network routers 220 and physical layer router transport segments 225 utilized for a specific path 255 do not have the necessary bandwidth capacity to meet determined capacity requirements, the Virtual Provisioning Server 230 allocates portions of the bottleneck capacity to the pairs of Packet Circuit Gateways 215 competing for this capacity and messages the associated Signaling Gateway 250 of this allocation. The Virtual Provisioning Server 230 also calculates the need for added capacity within the IP network 205 to meet current and future bandwidth needs. By centrally calcu-

lating and determining required network bandwidth provisioning and messaging the Signaling Gateways 205 within the IP network 205 of the bandwidth allocation, the Virtual Provisioning Server 230 determines the maximum number of voice calls that can be supported simultaneously between any pair of Packet Circuit Gateways 215. Since Signaling Gateways 250 provide the signaling interworking between SS7 and H.323/SIP, they are also able to track the number of connected calls in progress between pairs of Packet Circuit Gateways 215. As shown in the embodiment of the present invention illustrated in FIG. 2, and as previously described, one Signaling Gateway 250 may be utilized to control more than one Packet Circuit Gateway 215 and may also be utilized to track the number of connected calls in progress between other network Packet Circuit Gateways 215 (PCG #2, PCG #3, and PCG #4 in the instant embodiment as illustrated in FIG. 2).

[0014] As previously described, the Virtual Provisioning Server 230 also exchanges data with a Network Management System (NMS) 240. The Network Management System is a well known network controller used to maintain IP network 205 information pertaining to network element capacities, network bandwidth and capacity demand and growth data, link failures, etc. The Network Management System 240 is operable to exchange messages and signals with network routers 220 and to provide and maintain this network information via signaling channels 235. However, the Network Management System 240 does not determine or control admission/denial decisions for new call connections at the Packet Circuit Gateways 215. The Network Management System 240 provides the Virtual Provisioning Server 230 with information about the IP network 205 topology, capacities, failure events, etc. The Virtual Provisioning Server 230 uses this information to update its calculations and signals the Network Management System 240 if changes need to be implemented within the IP network, such as updating routing algorithm weights. Routing algorithm weights are used to determine the routing path for forwarding an IP packet. The use and implementation of such routing algorithm weights is well known in the art of IP networking. When needed capacities cannot be achieved temporarily due to failure events, the Virtual Provisioning Server 230 determines the maximum number of calls that can be supported on affected paths throughout the network and informs the associated Signaling Gateways 250, thereby providing a mechanism to throttle the number of connected calls at the various network Packet Circuit Gateway edge devices 215.

[0015] Although the instant embodiment of the present invention is described in the context of connectivity between PSTN switches and Signaling Gateways 250 to manage signaling conversion and admission control, it may also be used to support telephony between PCs and telephony between a PC and a phone via a PSTN switch. In order to guarantee connection

quality for these connections, it is important to provide messaging from the Virtual Provisioning Server 230 to the Signaling Gateway 250, thus informing the Signaling Gateway about the call capacities for PCG-to-PCG paths for a minimum of telephony traffic originating from PSTN and PCs. In addition, since a network operator may not control the coding rate in this case (i.e. - when calls originate from PCs), a traffic policing function is utilized at the PCG to monitor compliance with the traffic assumptions used in call set-up signaling.

[0016] Voice calls originating from a PC may be assigned lower priority as compared to those originating from a PSTN. Doing so allows the Signaling Gateway 250 to reject PC originated calls based on a lower bandwidth utilization, and rejects the PSTN originated calls at a higher threshold. Therefore, the Signaling Gateway 250 can guarantee call connection quality for voice and other Quality of Service sensitive services by enforcing call admission control at the Packet Circuit Gateways 230 and preferentially awarding priority for PSTN originated voice services over other services. In addition, a service provider may provide a plurality of critical service guarantees to customers and similarly, multiple customers may desire similar critical service guarantees over common paths within an IP network 205. One such example is presented within the context of Virtual Private Networks for voice traffic, wherein a network provider provides wide area services to interconnect corporate users in different locations. The ability to provide multiple Virtual Private Networks along with public service over a common infrastructure is attractive to both the service provider and corporate customers. One critical benefit of providing a Virtual Private Network is that the service provider is able to deliver secure access to the user. A second benefit is the ability to provide a Quality of Service guarantee- comparable to that on leased private lines between customer premises switches (e.g., PBXs).

[0017] Virtual Private Network customers negotiate bandwidth and service quality guarantees from a wide area network operator or service provider. The network operator guarantees this negotiated service level to all Virtual Private Network customers by utilizing the common infrastructure to achieve multiplexing gain. Capabilities available in currently available routers 220 allow the Virtual Provisioning Server 230 to provide these guaranteed services. For example, routers are available which are capable of identifying flows based on the port, source, and destination identifiers, and which categorize group flows into classes and/or super classes according to the level of service and bandwidth guarantees negotiated. These routers are also operable to allocate and manage minimum and maximum bandwidth for each class, super class, etc. Incorporation of buffer and queue management at the routers provides distinction and differentiation of priority treatment among flow classes and super classes. Additionally, statistical multiplexing may be provided for flows within a class and/

or among classes within a super class. A system of Weighted Fair Queuing (WFQ) service provides for management of flow, class, and super class bandwidths. If one of the classes or super classes exceeds a negotiated bandwidth allocation, superior service quality may still be provided if the other negotiated classes or super classes are not completely utilizing their allocated bandwidth. Therefore, only the Quality of Service provided to classes or super classes exceeding their negotiated allocation of bandwidth are affected.

[0018] Referring to FIG. 3, the Virtual Provisioning Server 230 is utilized as a Virtual Private Network Resource Manager. The Virtual Private Network Resource Manager utilizes optimizing algorithms to (i) partition bandwidth between Virtual Private Networks and within Virtual Private Networks if the customer desires a further subclassification of services and (ii) control flow routing within the network. If the network routers 220 utilized have flow partitioning capability, but do not have flexible routing capability, then flow routes are fixed through the IP network 205 and capacities are partitioned in the network by the Virtual Private Network Resource Manager based upon the negotiated Virtual Private Network contract. The Virtual Provisioning Server 230, functioning as a Virtual Private Network Resource Manager, sends this partitioning information to individual routers 220 within the network 205 so that the network routers 220 are able to set algorithm weights, minimum bandwidth, maximum bandwidth, buffer thresholds, etc. Communication between the Virtual Private Network Resource Manager is illustrated over a VPN signaling path 270 between the Virtual Provisioning Server 230 and individual routers, in accordance with FIG 3. The illustrated VPN signaling path 270 is merely illustrative, and any number of other means for signaling routers 220 would also be apparent to those skilled in the art, including communicating through the Network Management System 240. Once partitioning information is received at network routers 220 and partitioning is accomplished, each Virtual Private Network is established with its allocated minimum bandwidth.

[0019] Referring again to FIGS. 1-3, Virtual Private Networks for voice may also be supported using PSTN switches or multiplexers as access vehicles (STM switches 210 in the instant example) and utilizing the IP network 205 as backbone, as was previously described. Advantageously, the instant embodiment for establishing Virtual Private Networks for voice is achieved using network routers 220 with simple priority mechanisms. That is, signaling is not required between the Virtual Provisioning Server 230 and network routers 220 to establish and maintain the Virtual Private Networks. Rather, the Virtual Provisioning Server 230 uses aggregate capacity needed between a pair of gateways to perform virtual provisioning. The Packet Circuit Gateways 215, in conjunction with the Signaling Gateways 250, are utilized to control the acceptance or rejection of new calls from each Virtual Private Network customer utilizing an

acceptance/rejection algorithm residing in the Virtual Provisioning Server 230.

[0020] FIGS. 4 and 5 illustrate and define an exemplary algorithm for performance of the acceptance or rejection of new calls over a Virtual Private Network established between Packet Circuit Gateways 215, in accordance with the present invention. In conjunction with the accompanying description, the following definitions apply:

C = The total link bandwidth 310,
 W = The minimum bandwidth always available for combined traffic supported using Available Bit Rate (ABR) or best effort data service 315,
 $C - W$ = The total bandwidth available for call admission control purposes 320,
 $C - W - D_1$ = An upper threshold for call admission control purpose 325,
 $C - W - D_2$ = A lower threshold for call admission control purpose 330,
 $B_i(n_i)$ = Bandwidth needed to support n_i connections for VPN_i with a specified Quality of Service,
 P_i = Minimum bandwidth contracted for VPN_i ,
 Q_i = Maximum bandwidth contracted for VPN_i , and
 K = Number of Virtual Private Networks with Quality of Service guarantees sharing the link in consideration.

[0021] When a new call set-up request for VPN_i arrives at the Signaling Gateway 250, then the exemplary algorithm associated with FIG. 5 is performed to determine whether to accept or reject the new call, in accordance with step 350. The bandwidth utilized by K Virtual Private Networks (VPN_i ; $i = 1, 2, 3, \dots, K$) is monitored at the Signaling Gateway 250. Referring to step 355 when the VPN_i bandwidth necessary to support an additional call exceeds the maximum bandwidth allocation (Q_i), the requested new call is rejected. However, when the VPN_i bandwidth necessary to support an additional call does not exceed the maximum bandwidth allocation (Q_i), then step 360 is performed. In accordance with step 360, if the VPN_i bandwidth usage would be between the range of zero to $(C - W - D_2)$ after connecting the new call, then the new call is accepted. However, if VPN_i bandwidth usage would be greater than $(C - W - D_2)$ after connecting the new call, then step 365 is performed. In accordance with step 365, if VPN_i bandwidth usage would be between the range from $(C - W - D_1)$ to $(C - W)$, a new call set-up request for VPN_i is accepted only if the bandwidth usage by VPN_i has not exceeded its minimum allocation, P_i , otherwise the call is rejected, in accordance with step 370. If however, the VPN_i bandwidth usage is between the range of $(C - W - D_2)$ to $(C - W - D_1)$, a new call set-up request for VPN_i is accepted or rejected probabilistically based on a sliding scale algorithm in accordance with step 375. Let $q = (1 - p)$ denote the ratio of bandwidth usage in excess of $(C - W - D_2)$ over $(D_2 - D_1)$. A random number x is generated at

the Signaling Gateway 250 to support the probabilistically based algorithm, in accordance with step 380. If the value of x is less than or equal to probability p , then the new call is accepted, in accordance with step 385. For a call that traverses multiple links between its source and destination PCGs, the algorithm of FIG. 4 and FIG. 5 is repeated for each path link used to establish the call. The call is connected between the source and destination PCGs only if the algorithm yields a positive determination (to accept the call) for each link in the path.

[0022] During implementation of the exemplary algorithm of Figure 5, the bandwidth utilization data, $B_i(n_i)$, as a function of the number, n_i , for calls over VPN_i is utilized. If the calls or connections are constant bit rate, then $B_i(n_i)$ is a simple linear function of n_i . However, if the calls or connections are variable bit rate by nature or by design, for example - voice with silence elimination, on/off data sources, etc., then $B_i(n_i)$ is typically a non-linear function of n_i . The non-linear nature of $B_i(n_i)$ is due to the statistical multiplexing of randomly varying variable bit rate sources, as is well known in the art. For example, the specific nature of a $B_i(n_i)$ function, in the context of packet voice multiplexing, is detailed in a publication by K. Sriram and Y. T. Wang entitled "Voice Over ATM Using AAL2 and Bit Dropping: Performance and Call Admission Control," *Proceedings of the IEEE ATM Workshop*, May 1998, pp. 215-224, which is incorporated herein by reference.

[0023] Prior reference to the Virtual Provisioning Server (VPS) is described in the context of an IP network which includes multiple interconnected Open Shortest Path First (OSPF) domains. The present invention may also be implemented within an IP network comprised of multiple interconnected administrative areas, wherein each administrative area is comprised of multiple OSPF domains. Typically, each administrative area is an IP network belonging to an individual internet service provider or carrier, although such a configuration is not required. Such an embodiment of the present invention may be implemented with each administrative area having one gateway VPS. Each respective VPS may be co-located with the gateway router for that respective administrative area, although co-location is not a required aspect of the embodiment. Each pair of respective gateway VPSs determines the capacity requirements between their respective gateway routers. Further, each gateway VPS provides the necessary bandwidth capacity information between pairs of neighboring administrative areas to the VPSs located in each of the OSPF domains within its administrative area. Thus, the signaling gateways anywhere in the larger IP network are adequately provided with the necessary information for admission/denial of calls, including those that originate in one administrative area and terminate in another.

[0024] Numerous modifications and alternative embodiments of the invention will be apparent to those skilled in the art in view of the foregoing description. For example, although the present invention has been de-

scribed in the context of a single Virtual Provisioning Server utilized to service an entire IP network and control all Signaling Gateways within that network, it is also equally applicable for an embodiment of the present invention operable for multi-domain operation. That is, for those instances when call routing is made from a first telephony gateway source connected to a first IP domain and the destination is a second telephony gateway connected through another IP domain, the call processing involves intra-domain routing to the gateway router in the first domain, routing among gateway routers in intervening domains, and intra-domain routing from the gateway router to the telephony gateway in the last domain. Protocols such as Open Shortest Path First (OSPF) determine routing in a domain while a Border Gateway Protocol (BGP) is used for inter-domain routing between gateway domains. In such an embodiment of the present invention, a plurality of Virtual Provisioning Servers are utilized, one for each IP domain. Each Virtual Provisioning Server manages the virtual provisioning of routers within its respective domain, including Gateway Border Routers. Additionally, each pair of interfacing Virtual Provisioning Servers determines the capacity requirements between their respective pair of interfacing Gateway Border Routers. As was true for the single domain embodiment of the present invention, admission/denial control at the originating and terminating Packet Circuit Gateways is enabled without signaling the incorporated routers directly. In the multi-domain embodiment, this capability is attributable to shared knowledge of intra-domain and inter-domain routing protocols among the interfaced Virtual Provisioning Servers and also due to the static nature of router algorithm weights.

[0025] Additionally, the previous description is applicable for embodiments of the present invention in which service guarantees are provided without adding signaling mechanisms between routers and the associated Virtual Provisioning Server. However, the present invention would be equally applicable for those instances in which the Virtual Provisioning Server is operable to directly signal the network routers; although such an embodiment would be more accurately described as having a Server in which the provisioning is more real than virtual (since the provisioning is controlled at the routers instead of at the corresponding originating and terminating gateways). This alternative embodiment utilizes state exchange protocols in Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP), which are extended to provide dynamic topology and capacity information.

[0026] The present invention may also be used in evolving IP networks in which the well-known Multi-Protocol Label Switching (MPLS) is utilized at the network IP routers. In an MPLS based IP network, the Virtual Provisioning Server maintains a knowledge base of possible multiple paths between source-destination pairs of Packet Circuit Gateway edge devices. The Signaling

Gateways receive information from the Virtual Provisioning Server about alternative paths and associated capacities between PCG pairs, and admits a new voice call request if capacity is available over any of the available paths, otherwise, the call request is rejected.

[0027] Accordingly, this description is to be construed as illustrative only and is for the purpose of teaching those skilled in the art the best mode of carrying out the invention and is not intended to illustrate all possible forms thereof. It is also understood that the words used are words of description, rather than limitation, and that details of the structure may be varied substantially without departing from the invention and the exclusive use of all modifications which come within the scope of the appended claims are reserved.

Claims

1. A method for providing a Quality of Service guarantee for delay sensitive traffic conveyed over a path within an Internet Protocol (IP) network having a virtual provisioning server, a source edge device providing an interface for launching said delay sensitive traffic within said IP network, said method comprising the steps of:
 - receiving, at a signaling gateway, a value representing a bandwidth capacity for said path;
 - receiving, at said signaling gateway, a request to establish an additional delay sensitive traffic component over said path;
 - comparing, at said signaling gateway, said value representing said bandwidth capacity for said path with a total bandwidth needed if said additional delay sensitive traffic component is established over said path; and
 - generating, at said signaling gateway, a signal denying said request to establish said additional delay sensitive traffic component if said total bandwidth needed is greater than said value representing said bandwidth capacity for said path.
2. The method in accordance with claim 1 wherein said value representing said bandwidth capacity for said path is transmitted from said virtual provisioning server to said signaling gateway.
3. The method in accordance with claim 1 wherein said request to establish said additional delay sensitive traffic component over said path is conveyed from said source edge device.
4. The method in accordance with claim 3 wherein said source edge device is a packet circuit gateway.
5. The method in accordance with claim 1 further com-

prising the step of conveying said signal denying said request to establish said additional delay sensitive traffic component from said signaling gateway to said source edge device.

6. The method in accordance with claim 1 further comprising the steps of:

generating, at said signaling gateway, a signal authorizing said request to establish said additional delay sensitive traffic component if said total bandwidth needed is less than or equal to said value representing said bandwidth capacity for said path; and
conveying said signal authorizing said request to establish said additional delay sensitive traffic component from said signaling gateway to said source edge device.

7. The method in accordance with claim 1 further characterized in that said signaling gateway monitors and controls a quantity of said delay sensitive traffic over a plurality of paths within said IP network, said plurality of paths within said IP network utilized to convey said delay sensitive traffic from said source edge device to a destination edge device, said method further comprising the steps of:

identifying, at said signaling gateway, at least one of said plurality of paths within said IP network as having a most limiting available bandwidth capacity; and
limiting said quantity of said delay sensitive traffic launched from said source edge device to less than or equal to said most limiting available bandwidth capacity.

8. A method for providing a Quality of Service guarantee for real-time voice transmission traffic conveyed between a source Packet Circuit Gateway and a destination Packet Circuit Gateway over an Internet Protocol (IP) network having a plurality of routers, said source Packet Circuit Gateway providing an interface for launching said real-time voice transmission traffic within said IP network over an IP network path, said method comprising the steps of:

partitioning, from a bandwidth capacity associated with said IP network path, a first provisioned bandwidth capacity for a first Virtual Private Network (VPN), said VPN contracted for said real-time voice transmission traffic conveyed between said source Packet Circuit Gateway and said destination Packet Circuit Gateway;
maintaining, at a Signaling Gateway, a value representing said first provisioned bandwidth capacity for said first VPN;

receiving, at said Signaling Gateway, a request from said source Packet Circuit Gateway to establish a new call connection with said destination Packet Circuit Gateway over said first VPN, in addition to a plurality of presently established call connections;

comparing, at said Signaling Gateway, said value representing said first provisioned bandwidth capacity for said first VPN with a required first VPN bandwidth capacity should said new call connection be established; and
transmitting, from said Signaling Gateway, a signal denying said request to establish said new call connection if said required first VPN bandwidth capacity should said new call connection be established is greater than said value representing said first provisioned bandwidth capacity for said first VPN.

9. The method in accordance with claim 8 further comprising the step of:

transmitting, from said Signaling Gateway, a signal authorizing said request to establish said new call connection if said required first VPN bandwidth capacity should said new call connection be established is less than or equal to said value representing said first provisioned bandwidth capacity for said first VPN.

10. The method in accordance with claim 8 wherein a Virtual Provisioning Server is utilized to provide said Signaling Gateway with said value representing said first provisioned bandwidth capacity for said first VPN.

11. The method in accordance with claim 10 wherein said Virtual Provisioning Server is adapted to maintain a plurality of Virtual Private Networks over said IP network path.

12. The method in accordance with claim 8 wherein said Quality of Service guarantee is established by maintaining delay of said real-time voice transmission traffic conveyed between said source Packet Circuit Gateway and said destination Packet Circuit Gateway below a guaranteed threshold value.

13. The method in accordance with claim 8 wherein said Quality of Service guarantee is established by maintaining jitter of said real-time voice transmission traffic conveyed between said source Packet Circuit Gateway and said destination Packet Circuit Gateway below a guaranteed threshold value.

14. The method in accordance with claim 8 wherein a circuit network switch is utilized to supply and accept said plurality of presently established call connections and said new call connection from said

source Packet Circuit Gateway.

15. The method in accordance with claim 14 wherein said circuit network switch is a Synchronous Transfer Mode (STM) switch. 5
16. The method in accordance with claim 8 wherein at least one of said plurality of routers is operable to support Multi-Protocol Label Switching. 10
17. The method in accordance with claim 10 wherein a plurality of Multi-Protocol Label Switching (MPLS) routers is utilized to establish a plurality of paths between said source Packet Circuit Gateway and said destination Packet Circuit Gateway. 15
18. The method in accordance with claim 17 wherein said Virtual Provisioning Server is further operable to provide said Signaling Gateway with a plurality of values representing bandwidth capacities for each of said plurality of paths between said source Packet Circuit Gateway and said destination Packet Circuit Gateway. 20
19. The method in accordance with claim 10 wherein a plurality of Virtual Provisioning Servers are utilized to service a corresponding plurality of Open Shortest Path First domains. 25
20. The method in accordance with claim 10 wherein a plurality of Virtual Provisioning Servers are utilized to service a corresponding plurality of multiple administrative areas. 30

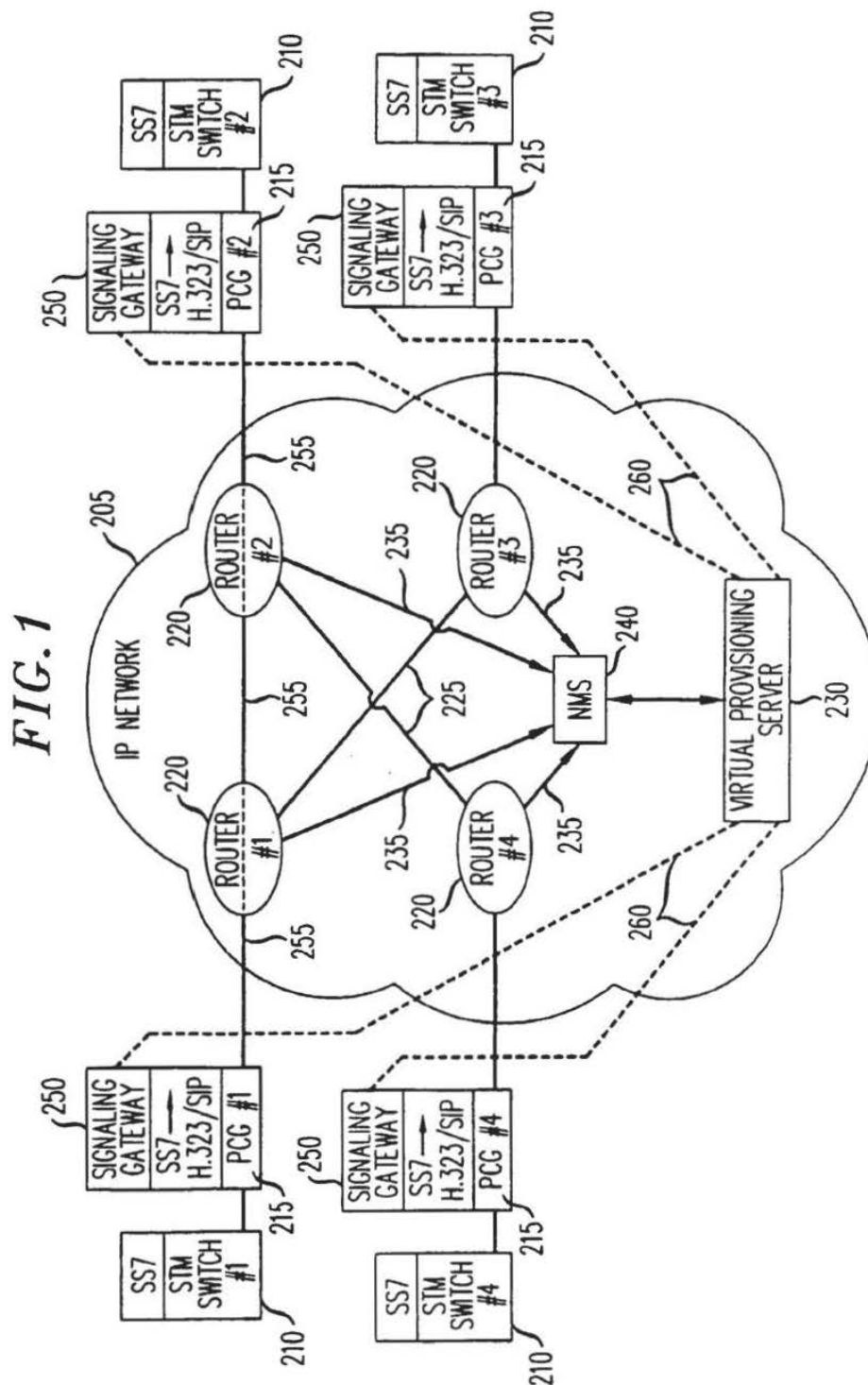
35

40

45

50

55



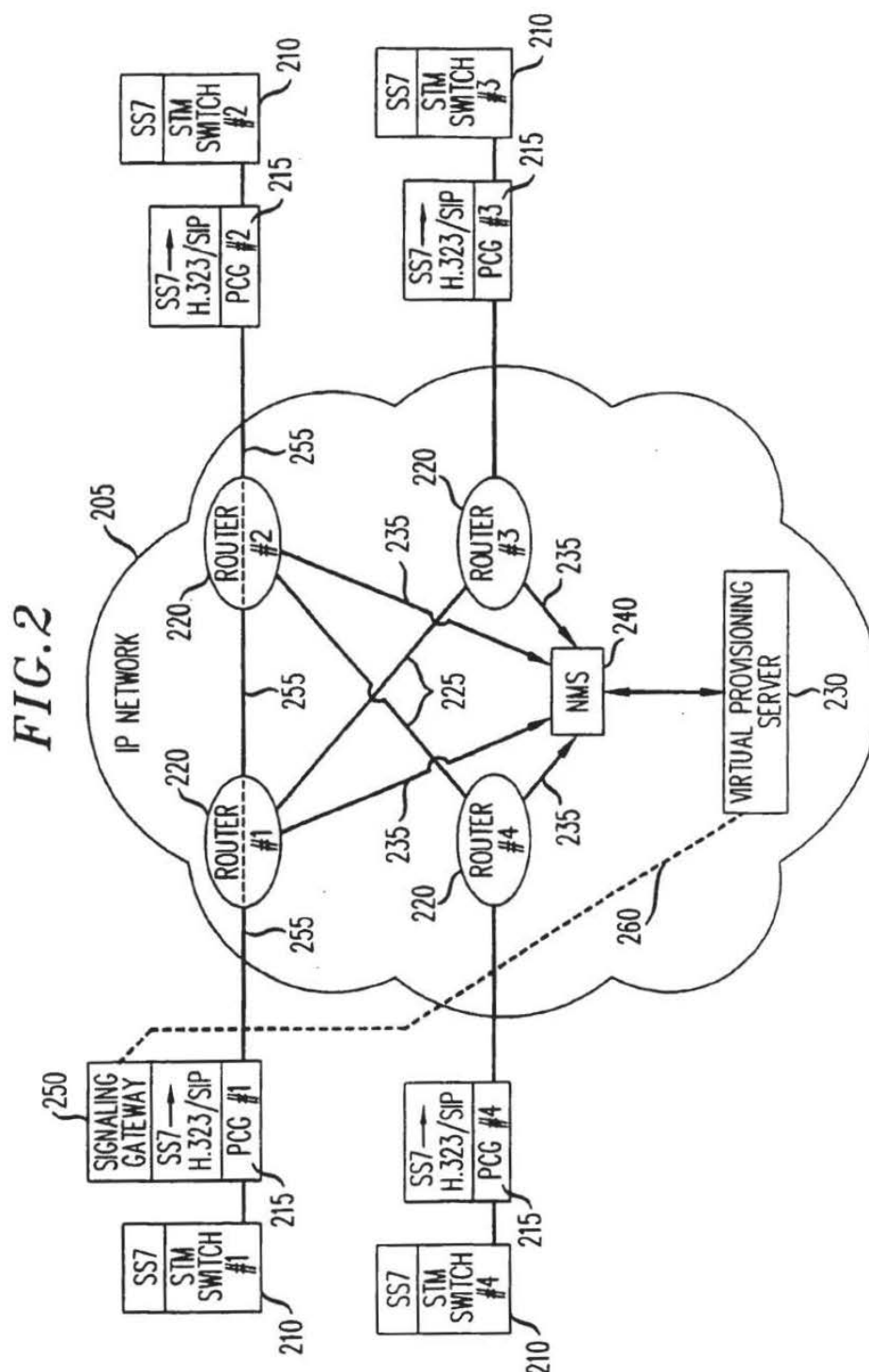


FIG. 3

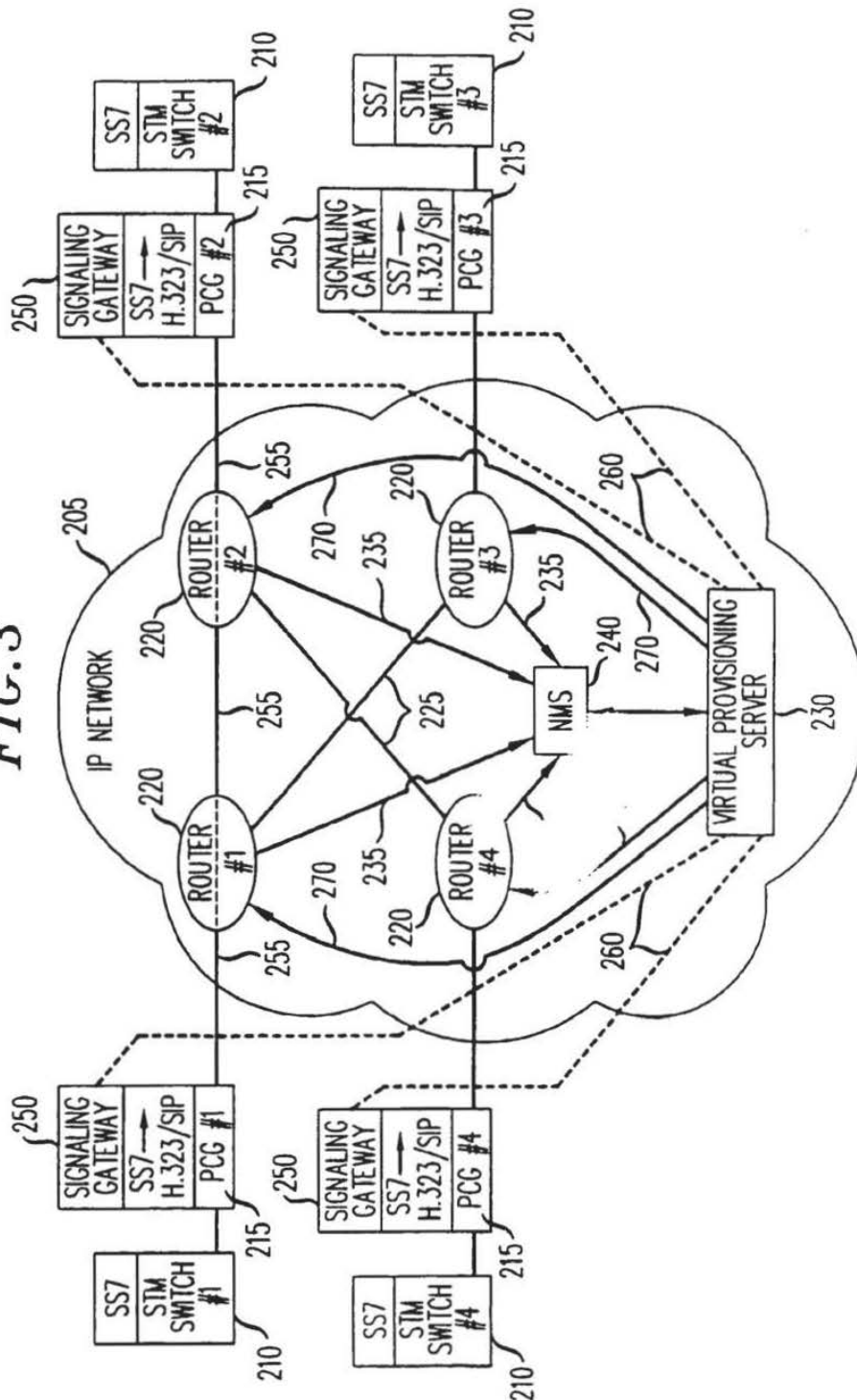


FIG. 4

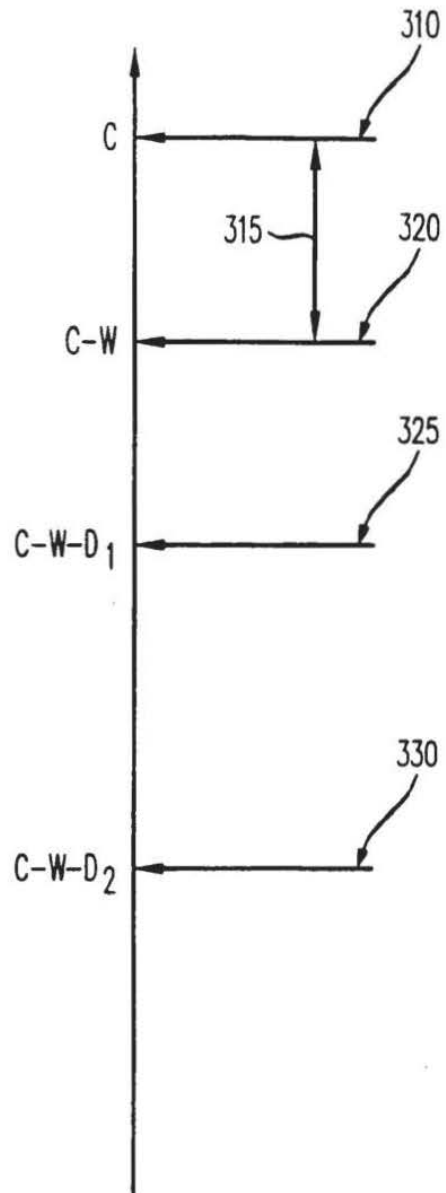
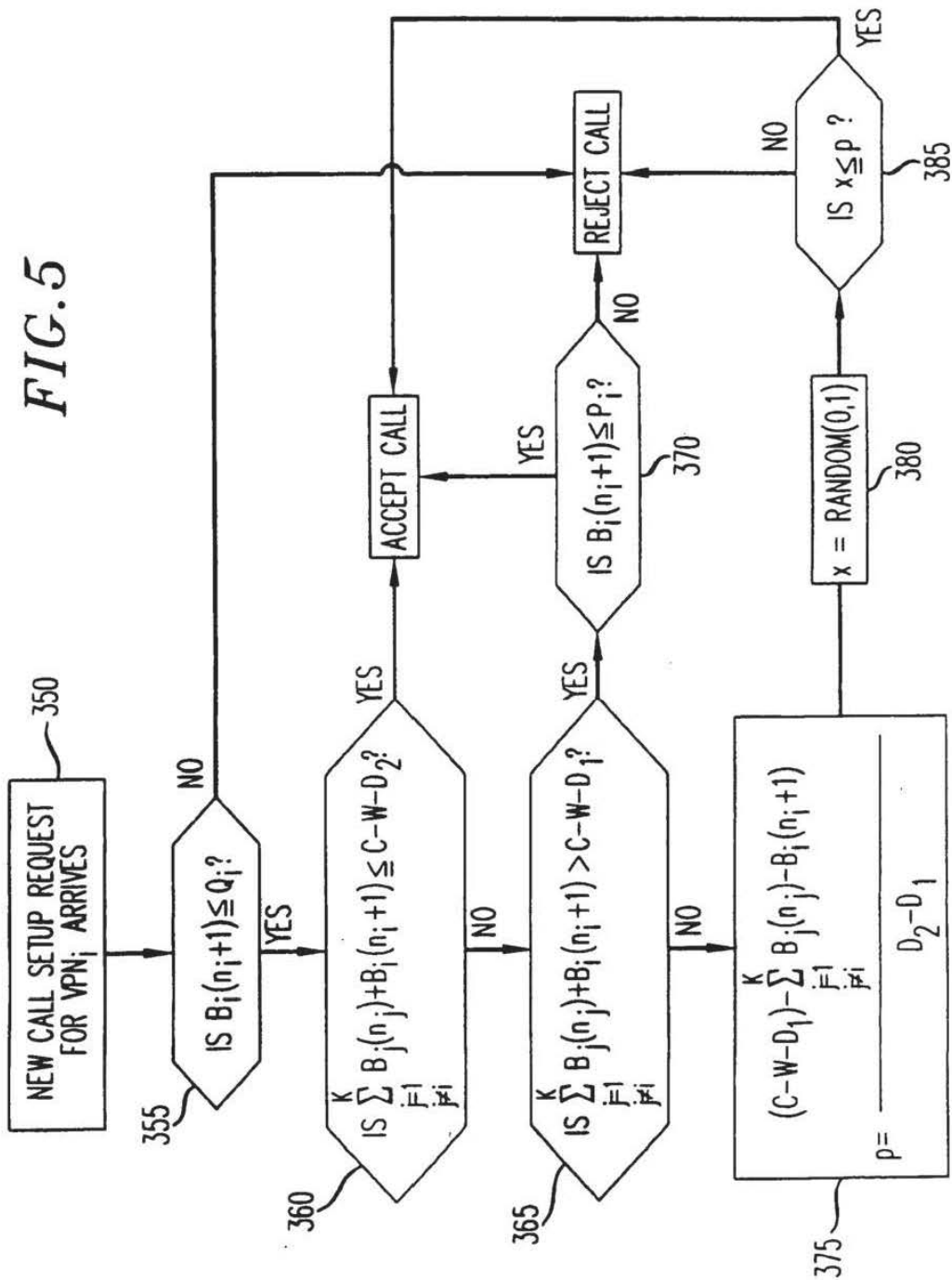


FIG. 5





European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 30 7282

| DOCUMENTS CONSIDERED TO BE RELEVANT | | | |
|--|--|--|---|
| Category | Citation of document with indication, where appropriate, of relevant passages | Relevant to claim | CLASSIFICATION OF THE APPLICATION (Int.Cl.7) |
| A | KOSTAS T J ET AL: "REAL-TIME VOICE OVER PACKET-SWITCHED NETWORKS" IEEE NETWORK: THE MAGAZINE OF COMPUTER COMMUNICATIONS,US,IEEE INC. NEW YORK, vol. 12, no. 1, 1 January 1998 (1998-01-01), pages 18-27, XP000739804 ISSN: 0890-8044 * figure 3 * * page 19, left-hand column, paragraph 3 - right-hand column, paragraph 2 * | 1,8 | H04L12/64 H04L12/56 H04L12/24 H04M7/00 H04Q3/00 |
| A | WHITE P P: "RSVP AND INTEGRATED SERVICES IN THE INTERNET: A TUTORIAL" IEEE COMMUNICATIONS MAGAZINE,US,IEEE SERVICE CENTER. PISCATAWAY, N.J, vol. 35, no. 5, 1 May 1997 (1997-05-01), pages 100-106, XP000657115 ISSN: 0163-6804 * page 100, left-hand column, paragraph 1 - page 101, left-hand column, paragraph 2 * | 1,8 | |
| A | GB 2 317 308 A (KOKUSAI DENSHIN DENWA CO LTD) 18 March 1998 (1998-03-18) * abstract; figure 9A * | 1,8 | |
| The present search report has been drawn up for all claims | | | TECHNICAL FIELDS SEARCHED (Int.Cl.7) |
| Place of search THE HAGUE | | Date of completion of the search 31 January 2000 | Examiner Eraso Helguera, J |
| CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document | | T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document | |

EPO FORM 1503 (3.0.02) (P04001)

ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.

EP 99 30 7282

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

31-01-2000

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---------------------|----------------------------|---------------------|
| GB 2317308 A | 18-03-1998 | JP 10070566 A | 10-03-1998 |

EPC FORM P439

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

QBone Bandwidth Broker Architecture

Work in Progress

STATE OF THE
ART

Abstract

This document is a rewrite of the QBBAC Bandwidth Broker Requirements document (version 0.7) and an attempt to harmonize different ideas and proposals (e.g. see [1] and [10]) that have been made over the past few months within the QBBAC. The goal is to recommend a simple, but adequately capable bandwidth broker architecture for the QBone.

Introduction

The purpose of this document is to establish a minimal set of requirements for network clouds wishing to participate in inter-domain QoS signaling trials across the QBone. In the QBone test bed, each participating network is a differentiated service (DiffServ) domain supporting one or more globally well known forwarding services built from fundamental DiffServ building blocks.

The primary strength of the differentiated service architecture [7,11] is the ability to achieve end-to-end QoS assurances while: 1) allowing for aggregation into a small number of DS behavior aggregates in the core; 2) requiring only bilateral service level agreements (SLAs) between all participating domains; and 3) allowing for maximal flexibility in local resource management decisions.

Any inter-domain DiffServ reservation signaling protocol must not break this model. Only the signaling interfaces between peering QBone domains should be specified and not the details of service level agreements or the underlying means by which individual QBone domains manage their network resources. Indeed, it is anticipated that within the QBone there will be significant variation in the implementations and resource management strategies behind the uniform signaling interface. Finally, because it is important to bootstrap non-trivial QoS deployments, any such protocol must mesh well with the end-to-end signaling capabilities of hosts and must be simple enough to facilitate rapid deployment, while remaining flexible enough to support future performance optimizations and protocol extensions.

Goals

The goals of this document are as follows:

- Define a model of the "bandwidth broker" resource managers to be deployed in the QBone.
- Recommend a deployment phasing for the QBone bandwidth broker work.
- Specify a common interdomain interface for the QBone bandwidth broker.

The technology being discussed here is too new for a complete and definitive analysis of the requirements for the bandwidth broker to take place. Therefore, the best approach is to discuss some of the basic

requirements and basic models and to suggest some candidates for the inter-domain protocol that are likely to prove robust and extendible. This is a stage for experimentation and trying out ideas.

The over-riding principles are:

- Leverage DiffServ model for aggregation and scalability in the forwarding path and keep peering arrangements simple and bilateral
- To keep the design simple to allow for the construction of prototypes and to make inter-operation simpler
- To leave room for future growth. This means building the inter-domain protocol with the flexibility that some developers may include some functions (optionally) which other developers may not want. There should be facilities to pass through or ignore information that a particular bandwidth broker implementation does not support.
- To leave space for different ideas and designs wherever possible. This implies that it is, at this point, better to *under* specify rather than over-specify functions and interfaces. That is, specify the bare minimum needed to inter-operate for the minimum functions, and leave the rest to the discretion of the group(s) building the prototype.

Scope

As just discussed, the scope of this document is limited to the inter-domain protocol. It provides neither a full bandwidth broker design nor a complete requirements analysis. In particular, the details of Service Level Specification (SLS) and SLA negotiation are left to a later time. This is discussed further later on in this document.

It is also generally recognized that policy control, policy-based admission control, accounting, authorization and authentication functions, network management functions and both inter- and intra-domain routing either affect or are (or can be) affected by the bandwidth broker. These are all important issues and should be explored, but are beyond the scope of this document. However, QBone participants should be able to experiment with these issues, and so if there is interest, experimental extensions may be specified in the minimal inter-domain BB protocol to allow for this. The addition of specific experimental TLVs should be discussed within the BBAC.

Further, some of these important issues can be worked out through a combination of additional companion documents generated by the BBAC of QBone and IETF internet drafts in the appropriate workgroups.

Although this document assumes a pure DiffServ environment, where every set of network elements inside a trust domain is considered to be a DS domain, it may be desirable in the future to extend this work to support end-to-end signaling along paths that include non-DiffServ capable domains or elements.

There will be a phased introduction of bandwidth broker functions in QBone:

Phase 0

Initial prototypes without inter-bandwidth broker communication. Note that it is possible in Phase 0 to have only a human "bandwidth broker".

Phase 1

First prototype of the inter-domain bandwidth broker protocol

Phase 2

Later prototypes with possibly "improved" inter-domain bandwidth broker protocol and additional functions

Basic Concepts

In this section, there is an outline of some basic concepts that are the starting point for the bandwidth broker within the QBone project(s).

Services

Summary of QBone Premium Service

QBone Premium Service (QPS) [5] is itself an instance of the Premium Service described in [4]. The fundamental idea is to provide a service with quantitative, absolute bandwidth assurance. The service may be provided entirely within a domain, from domain-edge to domain-edge (within the same domain) or across a number of domains.

An instantiation of QPS requires a number of parameters to be specified (and agreed) between the service provider(s) and the customer(s). These parameters are [5]:

- Start and end times
- Source and destination
- MTU Size
- Peak Rate

The following guarantees are given by the service:

- No loss due to congestion
- No latency guarantees
- Worst-case jitter bounds (ipdv) except in the case of IP route changes.

QPS is unidirectional and "out of profile" traffic is dropped.

This discussion is only about the technical aspects of QPS. A discussion of any financial and legal aspects of the service is **intentionally omitted**. It is important to note that there is *no* specification of how all this is accomplished.

More abstract concept of service

Note that while the initial phases of the BB work concentrate on QPS, the inter-domain BB protocol needs to be flexible enough to handle other services. The design of the inter-domain BB protocol should take this into account, and therefore a slightly more abstract view of service is discussed here.

One can abstract from the above description of QPS to the elements that must be specified, either implicitly or explicitly, for any and every service (in this context).

These elements must first of all fix the service in space and time, i.e. it must be specified between what times the service will be delivered (or can be requested) and the points (in space) at which the service will be delivered (or can be requested). It is assumed, of course, that this specification can be left open-ended, or it can be implied that the service can be requested at all times and at all places where the provider has a

presence.

Likewise, from the customer side, there must be some specification of what the input is. Exactly what must be specified is dependent on the service being requested. Note that although different providers may offer the same service in different ways, for a service that is intended to be global, the same specification should be used at the protocol level. One can expect in general that stricter service requires more specification (as in QPS) whereas a service with fewer guarantees requires much less specification (or none, e.g. Best-effort).

Finally, there has to be a specification of what the service provides (or what it consists of). This may be quantitative (as in the case of QPS) or qualitative, absolute or relative. By qualitative is meant statements like "low loss". By relative is meant statements like "Gold service has delay no worse than Silver service". Note that both absolute and relative may be quantitative or qualitative (this is somewhat different from the terminology in [12]).

The concept of service is end-to-end as fixed by the space coordinates, but the endpoints themselves may be networks and need not only be hosts. Further, in general, the endpoints may be left implicit.

The Diffserv idea

Diffserv is described in [7] in some detail. This is a brief summary for the purposes of understanding the relationship between services and mechanisms, and consequently the relationship between signalling resource reservations and bandwidth broker actions.

The DiffServ architectural model improves the scalability of QoS provisioning by pushing state and complexity to the edges of the network and keeping classification and packet handling functions in the core network as simple as possible. Briefly put, flows are classified, policed, marked and shaped at the edges of a DS domain. The nodes at the core of the network handle packets according to a Per Hop Behavior (PHB) that is selected on the basis of the contents of the DS field in the packet header. The number of DS code points and the number of PHBs is limited and consequently this mechanism allows for a large number of individual (micro-)flows to be aggregated from the point of view of the core router.

A PHB is defined in [7] as a "description of the externally observable forwarding behavior of a DS node applied to a particular DS behavior aggregate". The actual mechanisms causing this behavior are not strictly part of the PHB description. From the description of the behavior supplied by a PHB, it is intended that one can make a service description; at least that part of the service description that says what effect a service has.

The other part of the service description, namely that related to the customer's traffic, is related to the traffic conditioning concepts described in the DiffServ architecture. Traffic conditioning mechanisms include:

- Classification
- Marking
- Metering
- Shaping
- Dropping

and together they make up a traffic conditioning specification. These mechanisms can be set on the basis of the traffic profile usually specified in terms of classification parameters (how to recognize the specific flow

or set of flows), and metering mechanism and parameters (what are the characteristics asserted for the specific flow or set of flows).

QPS is based on the Expedited Forwarding PHB defined by Nichols, Jacobson and Poduri [6] which provides the necessary characteristics (configurable rate allocated to an aggregate independent of any other traffic on the link). With traffic-conditioned input and links in each DS domain configured at or above the specified rate, the service characteristics of QPS can be achieved.

Assuming statically configured SLAs and SLSs between adjacent domains, the service is then realized by the bandwidth broker receiving a resource allocation request and configuring the routers at the edges of (and internal to) its domain with the set of parameters for the PHB mechanisms and the traffic conditioning mechanisms derived from:

- The resource allocation request (RAR)
- The service definition
- The SLA/SLS in place with the peer domains (if applicable)

The further handling of the RAR is the subject of the differences between the Phase 0 and Phase 1 bandwidth brokers.

Bandwidth broker as Oracle

To meet these requirements, it is recommended that each QBone domain be represented by an "oracle" that responds to admissions requests for network resources. Such oracles have become colloquially known as "bandwidth brokers" [8].

The oracle model is as follows: In general, a bandwidth broker may receive a resource allocation request (RAR) from one of two sources: Either a request from an element in the domain that the bandwidth broker controls (or represents), or a request from a peer (adjacent) bandwidth broker. This document does not specify the form of the intra-domain protocol or messages, only the inter-domain protocol.

In any case, the bandwidth broker responds to this request with a confirmation of service or denial of service. This response is known as a Resource Allocation Answer (RAA). The request may have certain side effects also, such as altering the router configurations at the access, at the inter-domain borders, and/or internally within the domain, and possibly generating additional RAR messages requesting downstream resources. These side effects are local to the domain and are not specified here. The mechanism for triggering the response is defined in the protocol specification.

The basic input to the bandwidth broker oracle is what is described in a previous section as necessary for an abstract service; namely, the space-time coordinates of the service, the kind of service (and possibly parameters of the service) and possibly the characteristics of the input. There may, of course, be other input, but this document is only concerned with the minimum necessary input.

Service Level Agreements and Service Level Specifications

Description of SLAs

Service level agreements are concluded between peer domains, presumably (logically) adjacent, where one domain is the service provider and the other domain is the customer. It is possible for the client to be an

individual.

SLAs are assumed to be bilateral, between peer domains, and Bandwidth Brokers are the agents whose (functional) responsibilities include the implementation of the technical aspects of the agreements.

An SLA provides a guarantee that traffic offered by the (peer) customer domain, that meets certain stated conditions, will be carried by the service provider domain to one or more appropriate egress points with one or more particular service levels. The guarantees may be hard or soft, may carry certain tariffs, and may also carry certain monetary or legal consequences if they are not met. They may also include certain non-technical guarantees and issues that do not bear directly on packet handling, which is our main concern here.

The technical conditions and service levels may include policing, shaping and DS PHBs, but in fact may be larger than that in the sense of including matters of the various policies applicable, availability guarantees given, access guarantees given, trouble ticket procedures and response times and so forth.

An SLA, then is a partially technical document that is determined by network administrators, lawyers, and others, and is communicated via means ordinarily appropriate to that sort of agreement. In a sense, it contains the larger context for, and possibly limits to, the technical agreements assumed to be included in the SLA. "Inclusion of technical agreements" should not be taken to mean that all the details must be included in the SLA. What is required is that enough information is included to determine an SLS in sufficient detail, including (but not limited to)

1. PHBs to be applied
2. Traffic conditioners, policers, markers, shapers and their parameters
3. Any applicable policies

An SLA is changed by the (human) parties involved in the agreement. Bandwidth brokers do not involve themselves in SLA negotiation and do not communicate SLAs between peers. Thus SLA (re-)negotiation is not one of the tasks of a bandwidth broker.

This view of the SLA is that it is a human agreement and in fact sets the context and parameters of the behavior of the bandwidth broker with respect to the packet handling service. It may include also bandwidth broker behavior with respect to the application of policies, and other issues which may influence routing, recovery behavior, authorization, authentication and accounting, along with other network management functions.

It is likely that a wide variety of SLAs will flourish to meet a wide variety of technical and contractual requirements. As interesting as the space of potential SLAs (and their components) may be, it is unnecessary for a reservation signaling protocol to refer explicitly to established SLAs.

Description of SLSs

The SLS contains the technical details of the agreement specified by the SLA. An SLS has, as its scope, the acceptance and treatment of traffic meeting certain conditions and arriving from a peer domain on a certain link. More specifically, the SLS asserts that traffic of a given class, meeting specific policing conditions, entering the domain on a given link, will be treated according to a particular (set of) PHB(s) and if the destination of the traffic is not in the receiving domain, then the traffic will be passed on to another domain (which is on the path toward the destination according to the current routing table state) with which a similar (compatible and comparable) SLS exists specifying an equivalent (set of) PHB(s).

A traffic conditioning specification (TCS) specifies classifier rules and any corresponding traffic profiles and metering, marking, discarding and/or shaping rules which are to be applied to traffic aggregates selected by a classifier. The Internet Draft "A Framework for Differentiated Service" [FRAME] gives the following examples of parameters that may be specified by a TCS:

1. Detailed service performance parameters such as expected throughput, drop probability, latency;
2. Constraints on the ingress and egress points at which the service is provided, indicating the 'scope' of the service;
3. Traffic profiles which must be adhered to for the requested service to be provided, such as token bucket parameters;
4. Disposition of traffic submitted in excess of the specified profile;
5. Marking services provided;
6. Shaping services provided;
7. Mapping of globally well-known services DSCP values (not from [FRAME])

It is the responsibility of the service-providing domain (i.e. the receiver of the traffic specified in the SLS) to treat the traffic as specified in the SLS until those packets leave the domain. The SLS represents a commitment to consider certain classes of RARs and to treat the traffic conforming to the parameters of the admitted RARs in a manner consistent with a globally well-known service specification (GWSS). Since services are built from PHBs and the concatenation of PHBs, this is equivalent to handling conforming packets with the appropriate PHB within the domain. If the destination of the traffic is not within the domain itself, then there must be (at least one, but perhaps several) SLS(s) with an adjacent downstream DS domain at an egress point for the traffic that provide(s) a total commitment, over all the egress SLSs that can be used to carry traffic toward that destination, at least as great as that of the SLS on the ingress(es). This can be made precise with requirements on inequalities between the traffic conditioning specifications of the SLSs.

The intent is that for any given SLS on the ingress side, that there is sufficient capacity on the egress side to service it. Suppose that you have an SLS on the ingress with a single destination domain for e.g. capacity 10. If you only have one egress in your network that can reach that destination domain then you must have an SLS with the next downstream domain through that router on that interface with capacity at least 10. If you have multiple possible egresses, and you know that the SLS will be realized by reservations for multiple (aggregates of) flows, then you can spread that capacity 10 over those several egresses and no single SLS has to have that capacity by itself (though severally, they have to be able to handle that capacity). If you know that there is a single flow associated with that SLS, then it is questionable whether you can distribute it among several SLSs with downstream domains on the way to the destination because then you will almost certainly cause packets to arrive out of order.

So, the scope of the SLS is through the domain, from ingress point to egress point or destination (if traffic sink is within the domain).

Because full parameterization of SLSs is complex and is currently poorly understood, an SLS establishment and renegotiation protocol should be very minimal and highly extensible. This issue is left for Phase 2 or later. Instead, for Phase 0 and Phase 1, the terms of bilateral SLSs are propagated out-of-band (either through another protocol or manually), so that any two peering bandwidth brokers have a shared understanding of the SLS that exists between them.

Reservations

At this point, we should distinguish a number of concepts. We have already discussed SLAs and SLSs briefly. The SLS is itself not a reservation, but rather a commitment to allow reservations (or a potential for reservations). An analogy can be found in stock options: A stock option is a promise to allow an individual to buy X shares of stock at a given (fixed) price, no matter what the current price of the shares is. When the individual exercises the option, the shares are purchased at the given price and potential profit is realized. In a similar way, an SLS is a promise to allow a certain amount of resource usage and this "option" is exercised by sending an (inter-domain) RAR.

An interdomain reservation depends on sequences of interlocking SLAs and SLSs between DS domains. As pointed out earlier, for an interdomain reservation to succeed, the SLSs and policy requirements of the domains must be compatible and "ripple through" the sequence of agreements between physically adjacent domains. Further, the sequence of agreements must fulfill the service expectations (performance) of the requester.

Actual reservations are accomplished via the protocols described in this document. A reservation represents actually committed resources but not necessarily used resources. As traffic flows, the resource is actually used. How much can be used depends on the type of reservation of course.

Every bandwidth broker must, therefore, track: the SLSs between its DS domain and peering DS domains, the set of established reservations consuming resources in its domain and the availability of all reservable resources in its domain. The SLSs (which we are assuming at this point are not dynamic) are tracked by the bandwidth broker and (shared with) the policy decision and enforcement points. The reservations are tracked by the bandwidth broker and (shared with) the network management system. The actual resource use is tracked by the routers themselves and (possibly) monitored by the bandwidth broker.

Resource Allocation Requests

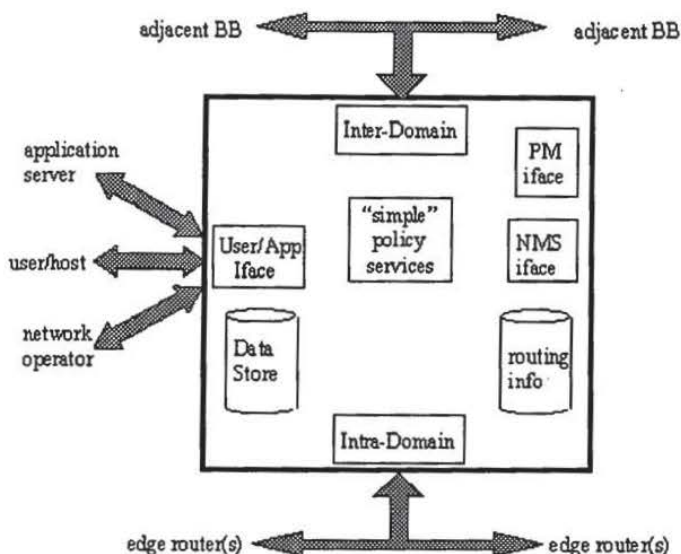
Resource allocation requests (RARs) may succeed or fail depending on the details of an established SLS, details of SLSs along the path, as well as the current state of resource availability along the path. For example (and assume here that all requests are for a specific well-known service), an SLS between an ISP and a customer may specify that all customer RARs for less than 1Mbps will be rejected; or an SLS may specify that the ISP will always make available on one day's notice at least 10Mbps to a specified destination; or an SLS may specify that the customer may request "destination-independent" reservations. There is tremendous flexibility here that is unnecessary to capture or even reveal in the reservation protocol. RARs and their subsequent acknowledgement or rejection are implicitly understood to conform or violate the terms of an existing SLS.

In response to admitted RARs, policers must be reconfigured to admit new DS traffic according to the TCSs in place. An affirmative RAA implicitly acknowledges that this reconfiguration has occurred in whatever manner is consistent with the SLSs and TCSs in place. The space of possible TCSs will inevitably be constrained by the underlying traffic conditioning technologies available on the relevant unidirectional interface. Simple conditioners may only support policing simple behavior aggregates, while more complex conditioners may actually consult route tables to determine classification (e.g. to police according to a profile specific to an ingress-egress pair).

Also unnecessary to the inter-DS-domain signaling protocol are the details behind the admissions control decisions and subsequent traffic conditioner configuration of individual DS domains. These decisions will be based on local resource availability and policy. There will likely be a wide variety of technologies and algorithms for managing the network resources of individual DS domains, but again, this complexity can be obscured behind a uniform admissions control interface.

Nodal Model

A functional decomposition of the bandwidth broker is shown here.



Not all the components will be used by every implementation. It is important to note that since a bandwidth broker touches on a number of functions in the network, including network management, policy control and configuration management, that these functions may in fact be obtained as services from other nodes implementing them, rather than these functions being implemented in the bandwidth broker itself.

The main functional blocks that concern us here are the user/application protocol, the intra-domain communication protocol and the inter-domain peer protocol, and this last is described in some detail later. In this section, we give a short description of the components.

Key Protocols

User/application protocol

This is an interface provided for resource allocation requests from within the bandwidth broker's domain. These requests may be manual (e.g. via a web interface) or they may consist of messages from one or another setup protocol (for example RSVP messages).

Intra-domain protocol

The purpose of this protocol is to communicate BB decisions to routers within the bandwidth broker's domain in the form of router configuration parameters for QoS operation and (possibly) communication with the policy enforcement agent within the router. Current bandwidth broker implementations have a number of different protocols for communicating with routers, including COPS, DIAMETER, SNMP, and vendor command line interface commands.

Inter-domain protocol

The purpose of this protocol is to provide a mechanism for peering BBs to ask for and answer with admission control decisions for aggregates and exchange traffic.

Data Interfaces

Routing Tables

A bandwidth broker may require access to inter-domain routing information in order to determine the egress router(s) and downstream DS domains whose resources must be committed before incoming RARs may be accepted. Additionally, a bandwidth broker may require access to intra-domain routing information in order to determine the paths and therefore resource allocation information within the domain.

Data Repository

This repository contains common information for all the bandwidth broker components. The repository includes some or all of the following information and may be shared with other network components such as policy control and network management.

- SLS information for all ingress/egress routers
- Current reservations/resource allocations
- Configurations of routers
- Service mappings/DSCP mappings
- Policy information
- Network management information
- Monitoring information from routers
- Authorization and authentication databases (for users and peers)

Interfaces to other entities

The bandwidth broker may have interfaces to other functional entities in the network. Alternately, these functions may be implemented or packaged with the bandwidth broker. It is also to be noted that how configuration management functions are split between policy control and network management is the object of some discussion and debate in the IETF.

Phase 0 BB Definition

The Phase 0 bandwidth broker definition does not have an inter-domain peer bandwidth broker protocol. It assumes a globally well-known service specification (QPS) which is statically provisioned and agreed upon by all DiffServ domains involved. This service is provided by statically negotiated bilateral SLSs which are set up via out-of-band protocols (phone or fax, for example). These are concatenated to provide the service. This is possible because the SLSs stretch from ingress router to egress router(s) of a domain. The concatenation runs then from the egress router of the source domain to the ingress router of the destination domain. The reservations for flows that use this service are also set up out-of-band between domains. It should be noted, finally, that the SLSs and reservations are unidirectional.

Within the source and destination domains, there is assumed to exist a protocol which effectively conveys the resource requests to the bandwidth broker in their respective domains. Note that this protocol can be a telephone call to the human "bandwidth broker" for a particular domain.

The bandwidth broker behaves as an oracle with side effects and returns a confirmation or denial of service to the requester. The protocol needed to do this, and the protocol needed to produce the appropriate side effects (if any) is not specified. The current Phase 0 bandwidth broker implementations use various protocols to accomplish this but since they are not communicated between DiffServ domains, they are not

the subject of this document. See the results of the BB operability event.

Inter-domain reservations work as follows [5]: There is a human "bandwidth broker" designated for each DiffServ domain. These bandwidth brokers communicate with a QBone "bandwidth czar" (also human) who maintains centrally a traffic demand matrix collected from bandwidth brokers in the individual domains. The traffic demand matrix is communicated to the QBone transit domains and the czar will request admission control decisions from the affected domains. When the admission control decisions have been coordinated, the reservations are made and the traffic can flow. If sources do not stay within their traffic parameters, border and/or edge routers will automatically condition the incoming traffic by dropping the excess. The bandwidth broker of a DiffServ domain reports this fact to the czar.

There may in addition be a protocol (for example, RSVP) which flows between hosts. This is assumed *NOT* to affect the transit domains lying between the source and the destination systems (see, for example [2]).

Phase 1 BB Definition

The Phase 1 BB definition can be seen as a working-out of the scenario in [8] relating to "Statically defined SLSs with bandwidth broker messages exchanged". The Phase 1 BB specification is attempting to solve two problems: First, how should peer bandwidth brokers communicate with each other? Second, is solving the so-called "last-mile" problem which deals with how to set up reservations end-to-end. While the complete protocol between endpoints and the bandwidth broker is not specified here, the contents of the RAR and RAA messages are specified.

In specifying the Phase 1 bandwidth broker functions, we expressly omit a number of interesting functions and leave them for future development. Among these are dynamic SLS negotiation, most AAA functions and policy functions. The idea is that people can experiment with these in the current framework.

In this phase, RARs flow inter-domain between peer (adjacent) bandwidth brokers, much as described in [8]. The protocol consists of a simple request-response protocol between the bandwidth broker peers, that carries the essential information outlined above for requesting a service in general.

A basic assumption of Phase 1 is that of a pure DiffServ environment, in which heterogeneous networks interoperate at layer 3 and, specifically, achieve QoS interoperability through DiffServ. We make no attempt to solve the intserv/DiffServ integration problem (though there is room to experiment with proposed solutions.) We assume that SLSs are already established (pairwise) between peer bandwidth brokers "out-of-band", that is, without a SLS negotiation protocol. We assume that there are globally well-known services and service IDs referring to those services. The SLSs refer also to these services and in addition, resource allocation requests use the well-known IDs. Further we assume that the BB handles end system requests for its domain, and that BBs may peer directly with non-adjacent BBs. This last is to facilitate the aggregation of service requests and will be explained more fully below.

Lastly, we assume that bandwidth brokers communicate with one another via long-running TCP sessions and that the reliability and flow control provided by TCP are sufficient for this application.

System Design

We describe here how the protocol works end-to-end and discuss some issues that arise in this design.

Following sections contain the definition of the messages.

We assume first, for purposes of description, that the bandwidth broker for a domain is a single entity and accessible to all end systems in the domain. (This is not meant to preclude distributed implementations). Assume that the end systems have implemented the protocol to communicate with the bandwidth broker.

We distinguish several different cases here:

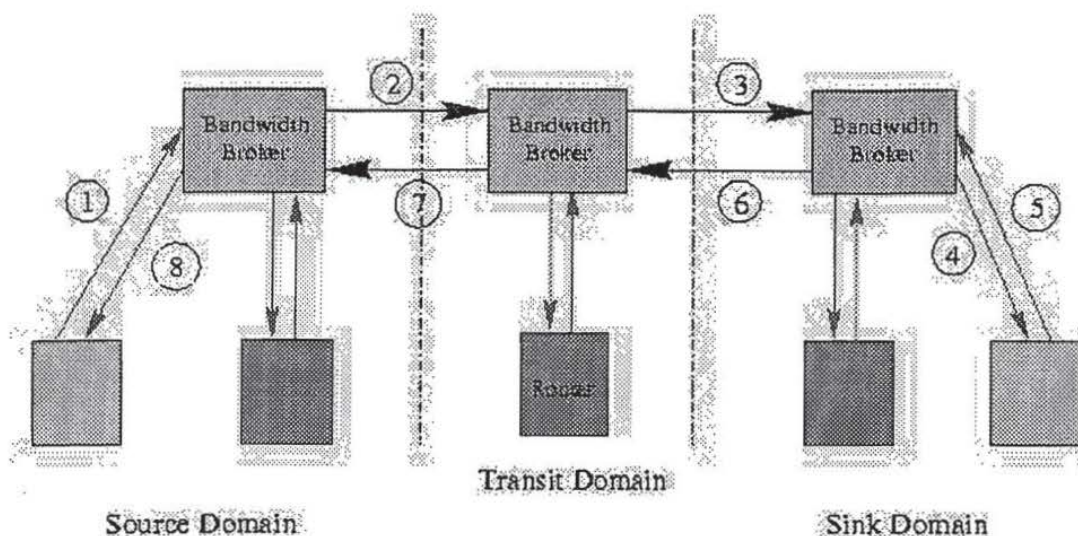
- An end system initiates a request for service with a fully-specified destination address (e.g. /32 for IPv4). The request is thus for service to another end system.
- An end system or a bandwidth broker request service to another domain (that is with a destination prefix that is not fully specified). This is, in effect, a pipe to another domain where the destination is not fully specified.
- A bandwidth broker receives a request for service with fully-specified destination prefix but uses a pipe ("core tunnel") to satisfy the request.

The first scenario shows the basics of inter-domain bandwidth broker communication. We do not expect that the entire mechanism will be used for every request in the network. This would not be especially scalable. The variations in the following scenarios can be used to support aggregation and increase scalability.

The fundamental problem is conveying the knowledge of flows to individual end systems (which might not be in a state to accept the flow) and the need for confirmation that the flow will indeed be accepted.

Case 1: End system initiates a request for service to an end system

The figure below gives an overview of the communication involved in this scenario. It is important to note that the messages are *pairwise*. That is, the request proceeds hop-by-hop and is sent only between "adjacent" entities. In the text that follows, numbers in parentheses, e.g. (1) are keyed to the flows in the figure.



End system request with fully specified destination

- Behaviour of the bandwidth broker in the originating domain

The end system sends an RAR to the bandwidth broker (1). This message includes a globally well-known service ID and an IP destination IP address, a source IP address, an authentication field, times for which the service is requested and the other parameters of the service.

The bandwidth broker makes a number of decisions at this point, including the following:

- Whether the requester is authorized for this service
- The egress router to which the flow may be assigned
- The route through the domain to the egress router
- Whether the flow fits in the SLS of the egress router with the net domain in the path to the destination
- Whether the flow (possibly according to the policies of the domain) may be accepted for the specified service.

If these decisions all have a positive outcome, the bandwidth broker will modify the RAR by including the ID for the domain (e.g. for IPv4 a /x prefix where $x \leq 32$) and sign the request with its own signature (2).

In case these decisions have negative outcomes, then the bandwidth broker returns a Resource Allocation Answer (RAA) to the end system (8). There can be additional information included, such as a reason code for the rejection and hints about what parameters might be acceptable at the moment that the answer is sent.

- Transit domain handling of the request

In this case, the bandwidth broker receives an RAR from an adjacent bandwidth broker with a fully-specified destination address specification (2). The transit bandwidth broker must perform a number of functions:

- a. Authenticate that the request is indeed from a peer bandwidth broker.
- b. Determine egress router (interface) from its (inter-domain) routing tables.
- c. Check that the requested resources fall within the SLS with the sending domain connecting via one of the ingress routers of this domain.
- d. Check that the requested resources fall within the SLS connecting to a successor domain en route to the destination.
- e. Ensure that there are sufficient resources within the domain to support the flow from the ingress border router and (possibly) determine the intra-domain route. This determination may involve the domain's resource allocation strategy.
- f. Determine whether the flow may be accepted (possibly according to the policies of the domain).

In case that all these decisions have positive outcomes, the transit bandwidth broker modifies the RAR as appropriate (e.g. putting its own ID in the sender's ID field and authentication string in the message) and sends it to the bandwidth broker of the following domain en route to the destination IP address (3).

In case that these decisions have negative outcomes, the BB returns an RAA to the sending domain (7). Additional information, such as rejection reason code and hints about acceptable parameters may be returned along with the RAA.

- Behaviour of the bandwidth broker in the destination domain.

In this scenario, the bandwidth broker of the destination domain knows the address of the end system which is to receive the flow. As in the behaviour just described, on the reception of the RAR (3), it makes the following decisions:

- a. Authenticate that the request is indeed from a peer bandwidth broker.
- b. Determine the intra-domain route from the ingress router to the end system and decides whether the resources are available to support the flow.
- c. Check that the requested resources fall within any possible SLS with the end system.
- d. Determine whether the flow may be accepted (possibly according to the policies of the domain).

In case these decisions have negative outcomes, an RAA is sent back (6), possibly with a reason code and hints about acceptable parameters.

In case all these decisions have positive outcomes, the bandwidth broker sends the RAR to the end system with appropriate changes (4). In this case, the end system makes the determination whether it can receive the flow. This is signalled with an RAA to the bandwidth broker of the destination domain (5). The RAA contains authentication of the end system, and parameters for the flow which the end system is willing to accept (which may be different from those received). In case the flow is rejected, the RAA contains a reason code and possibly hints about the set of service parameters that would be acceptable.

Upon receiving the RAA from the end system (5), the bandwidth broker authenticates the answer and forwards the RAA, with appropriate changes to the peer bandwidth broker that sent the RAR (6). At the same time, the bandwidth broker may configure traffic conditioners at the ingress router and possibly at other routers along the intra-domain path to the destination. Note: these are indicated by green arrows in the figure.

- Transit domain processing of the RAA

The RAA received from the peer bandwidth broker (6) is authenticated and the appropriate fields are modified and the RAA is sent to the next bandwidth broker in the chain back to the originating domain (7). Internally to the domain, the bandwidth broker may modify traffic conditioners and PHB parameters in the ingress and egress border routers in the path of the flow (indicated by the green arrows in the figure). In addition, resource allocation internal to the domain may be initiated by the bandwidth broker. This would consist of modifying PHB parameters and traffic conditioners in internal routers.

- Originating domain processing of the RAA

When the bandwidth broker of the originating domain receives the RAA (7) and authenticates it, the bandwidth broker completes any resource allocation actions within the domain, modifies PHB and traffic conditioner parameters at the egress router for the flow and forwards the RAA to the requesting end system (8). This may include setting the marking functions for the flow in the access router serving the requesting end system (indicated by the green arrows in the figure).

The end system receives the RAA and is able to send the flow. Note that there is nothing to prevent the end system from sending the flow earlier; however, the flow will not receive the requested service until the RAA is received and the DSCP of packets sent earlier than this will not be marked consistent with the service.

Case 2: Resource Request for Core Tunnel Services

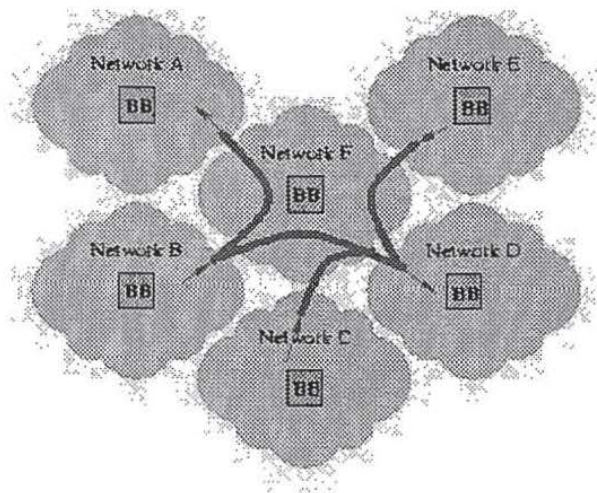
In this section, we handle the setup of a pipe between an origin domain and a destination domain. In this case, the destination prefix is not fully specified (i.e. for IPv4 /X where $X < 32$). In this document, we call such a pipe a *core tunnel*. The following explains this idea.

Tunnel Concept

Tunnel is a term used in this document for an inter-domain reservation where one or both ends of the reservation is not fully specified (i.e. doesn't have a fully specified IP address), not to be confused with IP tunnels or MPLS tunnels. It is a vehicle for aggregating reservations. A tunnel can extend from DS domain to DS domain (i.e. a *core tunnel* or one or the other end can be fully specified. Here we discuss mostly core tunnels, but all the variations are possible.

This kind of request may originate in an end system that knows, for example, that it has a large number of requests for service of a certain kind to send to a destination domain and is prepared to aggregate the resource requests to intermediate domains. The request may also originate with a bandwidth broker, as a result of aggregation algorithms (which may be administratively triggered or could be triggered based on historical data, for example). It is this latter case that we will discuss here, though the same procedures hold for both cases. Also, the same procedures hold where there are **no** transit domains.

The nature of the trigger is not specified in this document and indeed is a research question. The key trade-off here is reserving (possibly idle) bandwidth vs. the number of signalling messages. The research questions include: How large a pipe to request; how much in advance to request a pipe (and on the basis of what?); when to reduce or remove a pipe (and how much to reduce ?); and how often to adjust the reservation (negotiation).

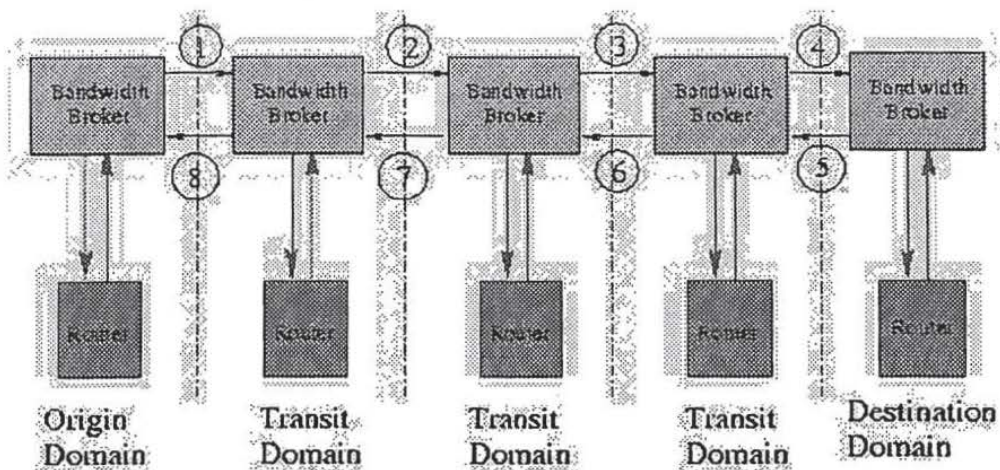


Core tunnels extend from the egress interface of the originating domain to the ingress interface of the destination domain. Note that tunnels as well as reservations are unidirectional. The setting up of a core tunnel involves the intermediate bandwidth brokers, but the use of it for aggregating individual flows does not.

The figure above shows core tunnels extending across several domains. Note the difference between the tunnels and the reservations. The tunnels have origin and destination pairs, while the reservations for several tunnels may be merged at the border router interfaces (shown by the merging of the thick red lines in the figure).

Establishment of the tunnel

Assuming that the establishment of a core tunnel is triggered in the origin bandwidth broker, we have the sequence of the above figure. Note that in the text below, numbers in parentheses are keyed to the circled numbers in the figure.



- Behaviour in the originating domain.

The bandwidth broker in the origin domain creates an RAR which includes the IP prefix of the destination domain along with the normal information required in an RAR (where, extent, when) and an indication that a core tunnel is being requested. This RAR is sent to the bandwidth broker in the next domain (1) in the path on the way to the destination domain.

- Transit domain processing of the RAR

In all transit domains, except for the penultimate domain, the bandwidth brokers behave in exactly the same way as for an RAR with a fully specified destination address. Each transit-domain bandwidth broker performs a number of functions on reception of an RAR from a peer bandwidth broker in an adjacent domain ((1),(2),(3)) among which are the following:

- Authenticate request from peer bandwidth broker
- Determine the egress router from its inter-domain routing table
- Check that the RAR falls within the SLS with the sending domain connecting to one of the ingress routers (interfaces) of this domain.
- Check that the RAR falls within the SLS with the successor domain (determined via the interdomain routing tables) en route to the destination via one of the egress routers (interfaces) of this domain.
- Ensure that there are sufficient resources to support the RAR from the ingress router to the egress router and (possibly) determine the intra-domain route.
- Determine whether the flow may be accepted (possibly according to the policies of this domain).

In case these decisions have positive outcomes, the transit bandwidth broker modifies the RAR by replacing the sender ID and authentication field with its own ID and authentication string. The modified RAR is then sent to the next domain en route to the destination ((2),(3)).

In case these decisions have negative outcomes, the bandwidth broker returns an RAA to the sender indicating failure ((6),(7),(8)). Additional information such as a reason code and hints about acceptable parameters may be included.

- Penultimate domain processing of the RAR

In addition to all the checks outlined in the previous step, the bandwidth broker in the penultimate domain creates, on acceptance of the RAR, a *core tunnel voucher* which contains information about the reservation, ensuring that it fits within the SLS between the penultimate domain and the destination domain. This voucher is added to the RAR and sent to the destination domain (4). It is used later by the origin domain bandwidth broker to refer to the reservation (see next section).

If the reservation is not accepted, the bandwidth broker returns an RAA (6) as above.

- Behaviour in the destination domain

When the bandwidth broker in the destination domain receives the RAR (4), it performs the following functions:

- Authentication that the request is indeed from a peer bandwidth broker.
- Checks that the RAR falls under the SLS with the sending domain connecting via the specified ingress router (interface).
- Checks that there are sufficient resources in the domain to support the RAR. (*Note: this is a research issue.*)

d. Determination of whether the RAR can be accepted (possibly according to domain policies). If the outcomes of these decisions are positive, the destination domain bandwidth broker stores the voucher from the penultimate domain and stores also the identifier of the origin domain. It then returns an RAA (with the voucher) (5) to the penultimate domain.

If the outcomes are negative, then it returns an RAA possibly with a reason code and hints about acceptable parameters (5).

- Transit domain processing of the RAA

In all transit domains (including the penultimate domain) the bandwidth broker authenticates the RAA from the sender ((5),(6),(7) and replaces the sender ID and authentication strings with its own ID and authentication string and then sends the RAA on to the following domain in the direction of the origin domain ((6),(7),(8)).

At the same time, the bandwidth broker may make adjustments to traffic conditioning (shaping, policing, marking, metering) and PHB functions in its affected border routers and (possibly) in the internal routers of the domain. This is indicated by the green arrows in the figure.

- Origin domain processing of the RAA

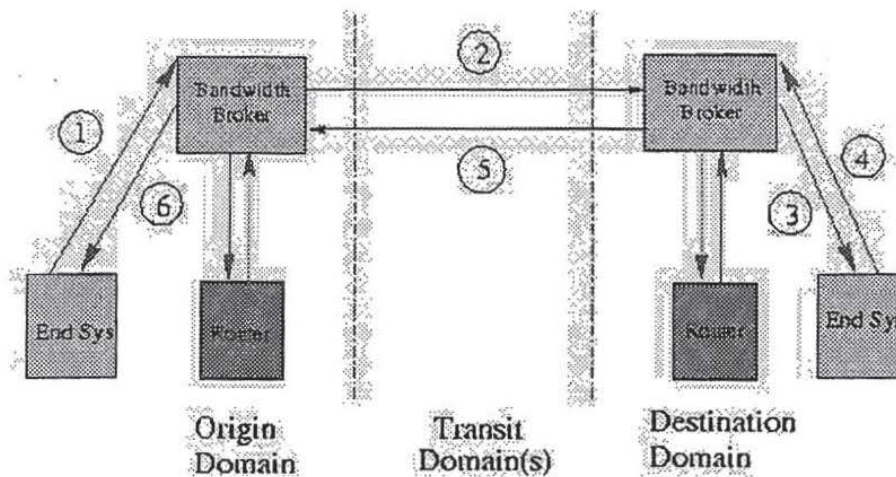
On receiving the RAA for its request (8), the origin bandwidth broker authenticates the RAA and checks the information in it to see whether the request was accepted or not. If the RAR was accepted, the bandwidth broker stores the voucher created in the penultimate domain in the path. At this time, the bandwidth broker may also make adjustments to traffic conditioning and PHB functions in its border router, and it may at this time establish a TCP session with the bandwidth broker in the destination domain (if it has not already done so).

Other Tunnels

In addition to core tunnels, other configurations are possible, for example, where the source address is fully-specified (is an end system) but the destination address is not (*head tunnels*), or where the source address is not fully-specified but the destination address is (*tail tunnels*). Both of these cases can be handled with some minor modifications to this protocol (in the origin and destination domain BBs).

Case 3: Core tunnel handling of a request with fully-specified destination

In this case, the service request has a fully specified destination address, but a separate reservation in the core network(s) is not made. Instead this service request is aggregated into a *core tunnel* assumed in this case to be previously set up. Note that only the origin and destination bandwidth brokers and the end systems are involved in this communication.



Note that in the text below, numbers in parentheses are keyed to the circled numbers in the figure.

- Originating domain processing the RAR

The bandwidth broker in the origin domain receives an RAR (1) from an end system in its control. According to its own algorithms, it chooses to aggregate this request with others in an existing core tunnel. The bandwidth broker checks the following:

- Whether the requester is authorized for this service
- The route through the domain to the egress router. It was assumed that in setting up the core tunnel, the bandwidth broker would check to ensure that the resources to support it were available in the domain. However, that check could be delayed to, or repeated at this point.
- Whether the flow fits in the core tunnel
- Whether the flow (possibly according to the policies of the domain) may be accepted for the specified service.

If the outcomes of these decisions are positive, the bandwidth broker replaces the sender ID and authentication string in the RAR with its own ID and authentication string, and places the Core Tunnel Voucher TLV for the core tunnel into the message and sends the RAR directly to the bandwidth broker of the destination domain (2).

If the outcomes are negative, then the bandwidth broker returns an RAA to the end system (6) indicating failure along with a reason code and possibly hints about acceptable parameter values.

- Destination Domain processing the RAR

When the destination bandwidth broker receives the RAR (2), it checks the following:

- Authenticate that the request is indeed from a peer bandwidth broker.
- Authenticate the Core Tunnel TLV
- Check that the requested resources fit in the core tunnel
- Determine the intra-domain route from the ingress router to the end system and decides whether the resources are available to support the flow.
- Determine whether the flow may be accepted (possibly according to the policies of the domain).

In case these decisions have negative outcomes, an RAA is sent back (5), possibly with a reason code and hints about acceptable parameters.

In case all these decisions have positive outcomes, the bandwidth broker sends the RAR to the end system with appropriate changes (3). In this case, the end system makes the determination whether it can receive the flow. This is signalled with an RAA to the bandwidth broker of the destination domain (4). The RAA contains authentication of the end system, and parameters for the flow which the end system is willing to accept (which may be different from those received). In case the flow is rejected, the RAA contains a reason code and possibly hints about the set of service parameters that would be acceptable.

Upon receiving the RAA from the end system (4), the bandwidth broker authenticates the answer and forwards the RAA, with appropriate changes to the origin bandwidth broker (5). At the same time, the destination bandwidth broker may configure traffic conditioners at the ingress router and possibly at other routers along the intra-domain path to the destination. Note: these are indicated by green arrows in the figure.

- Origin processing of the RAA

When the bandwidth broker of the originating domain receives the RAA (5) and authenticates it, the bandwidth broker completes any resource allocation actions within the domain, modifies PHB and traffic conditioner parameters at the egress router for the flow and forwards the RAA to the requesting end system (6). This may include setting the marking functions for the flow in the access router serving the requesting end system (indicated by the green arrows in the figure).

The end system receives the RAA and is able to send the flow.

Takedown

Either of the endpoints of a QBone reservation may release the reservation, or the BBs in the endpoint domains (if they are not holders of the endpoint of the reservation) may do so. It is assumed that intermediate bandwidth brokers who are aware of a reservation (i.e. one representing a tunnel, not made within a tunnel) also know their peer bandwidth brokers both upstream and downstream with respect to the reservation.

Note that a QBone reservation set up by the SIBBS protocol may have an exact end time specified. In this case the reservation is removed automatically by all parties involved without the need for a takedown message to be sent.

We propose a semi-soft state mechanism for backup of the takedown procedure. This is a refresh of the reservation RAR with a fairly long time constant (on the order of minutes) that is there in case a number of unlikely events cause the takedown messages and retries to be lost. More details of this mechanism will be in the next version of this document.

Takedown is accomplished via the RAR/RAA pair. A node wishing to release the reservation sends an RAR indicating a release of the reservation (or part of it). A complete release should result in a 0 reservation. A negative adjustment that is not a complete release may only be sent by the initiator of the reservation (or its bandwidth broker).

The following conditions and behaviours are defined for reservation takedown:

1. Unless there is some error or internal inconsistency in the RAR, a reduction/takedown always succeeds.
2. A release of a reservation is indicated in one of the following ways:
 - a. *decrease* and *delta* are indicated in the flag field of the RAR and the reservation parameter values are equal to the currently held reservation. If the absolute value of the values in the RAR are greater than the reservation currently held by the bandwidth broker, the entire reservation is released and a notification TLV is included in the RAR/RAA.
 - b. *decrease* and *absolute* are indicated in the flag field of the RAR. A release is indicated by 0 values in the RAR. A reduction is indicated by non-zero values in the RAR (but "less than" the value of the currently held reservation, where "less than" has a special meaning when applied to a multi-valued object like a reservation). An inconsistent condition occurs if *decrease* and *absolute* are indicated but the values in the RAR are "greater than" the currently held reservation. In this case, the reservation is retained and the RAR should be treated as an error.
3. Since either end can send a takedown, messages may cross. If a takedown arrives at a BB for a reservation that no longer exists, it is by definition successful and receives a positive RAA. It is not, however, forwarded since there may be multiple paths to the origin or destination domains and it would not be known to which peer BB the message should be forwarded.
4. Since in general (except as noted above) a release will always succeed, an RAA can be sent immediately to the sender of the RAR. In this case, however, the BB sending the RAA is responsible for forwarding the RAR to its peer in the next downstream domain.

Failure Conditions

Message Formats

The following subsections give the message formats for the Phase 1 BB protocol.

RAR

The following table outlines the RAR message format. Note that not all of the fields are used in an RAR sent between end systems and bandwidth brokers (i.e. intra-domain).

| Field | Explanation |
|---------------------------------------|--|
| Version | Bandwidth broker protocol version ID (current version is 1) |
| RAR ID | Unique RAR ID (perhaps IP address + sequence number) generated by initial RAR sender and propagated forward; may be used for bookkeeping purposes by any intermediate BB; must be returned in matching RAA message |
| Sender ID | Identifier of the DS domain that sent the RAR; rewritten by intermediate domains; used to authenticate the RAR. For RARs sent to or from end systems, this field is not used. |
| Sender Signature | Each RAR message should be signed with the public key of the sending DS domain; this field in conjunction with the Sender ID allows the RAR receiver to authenticate that the RAR is from a peer DS domain and to reference internal state on the SLS in place with that domain |
| Source Prefix | IP address prefix for source terminus of the service request |
| Destination Prefix | IP address prefix for destination terminus of service request |
| Ingress Router ID | IP address of the interface between two domains for which the sending domain is requesting service. This field is replaced in the message by each sending bandwidth broker. When sent by an end-system, this field contains the IP address of the access router interface through which the flow will pass (for example, the default router) en route to the destination. When sent from a bandwidth broker to an end system, it contains the IP address of the access router interface over which the flow will be forwarded. |
| Start Time | now specific future time |
| Stop Time | indefinite as long as possible specific future time |
| Flags | <p>The following flags are defined:</p> <ul style="list-style-type: none"> • receiver pays (collect call) • probe (determine parameters/acceptance but do not commit resources) • establish Core Tunnel • renegotiation • delta/absolute values for Service Parameterization Object (SPO) • increment/decrement values for SPO |
| GSID | Globally well-known service ID |
| Service Parameterization Object (SPO) | Service specification parameters dependent on the particular GWS indicated by the GSID. |
| Additional TLVs | Core Tunnel Voucher |

RAA

Corresponding to each RAR generated, is an RAA message, each having the following format:

| Field | Explanation |
|---------------------------------------|--|
| Version | Bandwidth broker protocol version ID (current version is 1) |
| RAR ID | Unique RAR ID (perhaps IP address + sequence number) generated by initial RAR sender and propagated forward; may be used for bookkeeping purposes by any intermediate BB; must be returned in matching RAA message |
| Sender ID | Identifier of the DS domain that sent the RAR; rewritten by intermediate domains; used to authenticate the RAR. For RARs sent to or from end systems, this field is not used. |
| Sender Signature | Each RAR message should be signed with the public key of the sending DS domain; this field in conjunction with the Sender ID allows the RAR receiver to authenticate that the RAR is from a peer DS domain and to reference internal state on the SLS in place with that domain |
| Source Prefix | Copied from RAR |
| Destination Prefix | Copied from RAR |
| Ingress Router ID | Copied from RAR as received by this bandwidth broker |
| Start Time | Copied from RAR |
| Stop Time | Copied from RAR. If 'as long as possible' was specified in the RAR, then this may be set to a specific future time. |
| Flags | <p>The following flags are defined:</p> <ul style="list-style-type: none"> • RAR Accepted <p>If this bit is set (on) then the RAR has been accepted and the learned service parameters may be found in the SPO; if this bit is off, the RAR was rejected and the SPO may optionally be rewritten to reflect the "nearest match" reservation that would have been accepted. Additionally, a reason code TLV may be included following the SPO.</p> <ul style="list-style-type: none"> • Core tunnel set up <p>This bit indicates that a core tunnel was set up as a result of the associated RAR and that there is a 'voucher' TLV contained in this message.</p> |
| GSID | Copied from the RAR |
| Service Parameterization Object (SPO) | Service specification parameters dependent on the particular GWS indicated by the GSID; parameters that were left blank in the RAR may be completed in the RAA or rewritten to reflect a renegotiation hint as described in the "Flags" field above. |
| Additional TLVs | <ul style="list-style-type: none"> • Reason Code TLV • Core Tunnel Voucher TLV |

Additional Objects (TLVs)

The SPO

The final parameter of both message types, the Service Parameterization Object (SPO), merits further discussion. This parameter is intended to be a service-specific specification of requested or learned service parameters. Depending on the service in question, this may be a simple parameter (e.g. bits-per-second of bandwidth) or may be quite complex (full TSpec, trTCM configuration, etc.).

In the case of the QBone Premium Service (QPS) [5], QPS reservations are defined by the tuple: {source, dest, route, startTime, endTime, peakRate, MTU, jitter}. Analogously, the QPS SPO should have the following format:

| Field | Explanation |
|----------|--|
| Route | TLV describing the per-DS-domain route along which service is requested. |
| PeakRate | QPS peakRate in bytes per second |
| MTU | QPS MTU in bytes |
| Jitter | QPS jitter bound in microseconds |

SPO formats must allow for a service to be "ramped up" as well as to be "ramped down" and downright "torn down". Therefore, there must exist at least one field that quantifies the service (e.g. PeakRate), rather than parameterizing the assurance (e.g. Route, Jitter). The numerical SPO parameters are taken to be a delta if the "delta" flag in the Flags field of the RAR is on. Additionally, these parameters are added if the "increment" flag is on, and subtracted otherwise. So, for example, if the *renegotiation* flag is on, together with the *absolute* flag, then the value in the SPO replaces the entire current reservation.

Reason Code TLV

The Reason Code TLV is sent anytime an RAR is rejected. It contains information allowing the receiver to diagnose the rejection. The format is as follows:

| Field | Explanation |
|------------------|---|
| Domain/System ID | TLV indicating a unique identifier (e.g. IP address) of the entity rejecting the RAR. |
| Reason Code | <p>Among the possible reason codes are:</p> <ul style="list-style-type: none"> • Policy rejection: The RAR was rejected because of policy in the rejecting domain or system. • Parameter rejection: The RAR was rejected because the parameters requested could not be honored. Appropriate parameters may be contained in the SPO returned with the RAA. • Sender not authenticated: The sender of the RAR could not be authenticated. • No SLS: The required SLS for the service did not exist. |
| RAR | TLV containing the offending RAR (or parts thereof) |

Core Tunnel Voucher TLV

The Core Tunnel Voucher TLV is created by the last bandwidth broker in the chain making up the tunnel and is a permission or certificate that shows that the originator has a reservation for a specific service. The format of the Core Tunnel Voucher is as follows:

| Field | Explanation |
|----------------|--|
| Generator ID | Domain ID of the bandwidth broker creating the voucher. |
| Destination ID | Domain ID of the bandwidth broker in the destination domain of the tunnel. |
| Voucher | <p>A field signed with the public key of the last bandwidth broker in the tunnel and consisting of the following fields:</p> <ul style="list-style-type: none"> • Global Well-known Service ID • Ingress router ID (i.e. the ingress to the destination domain) • Domain ID of the originating bandwidth broker • SPO of the reservation requested |

Unrecognized TLVs

The TLVs defined in this document (and perhaps some others in revisions of it) are regarded as base. That is, all QBone BB implementations are required to recognize these TLVs. However, for future and experimental TLVs, we need to have a mechanism for nodes not recognizing non-required TLVs to handle them. Our design is the following: We define a base TLV named **Unrecognized TLV received**.

| Field | Explanation |
|------------------|--|
| Flags | <ul style="list-style-type: none"> • Found in RAR • Found in RAA |
| Unrecognized TLV | The TL values that were not recognized by this node's message parser. |
| IP address | The IP address of the node reporting the condition |

The behaviour of a node receiving an unrecognized vector is as follows:

- The node creates a subfield consisting of the Flags, the unrecognized TL value and its own IP address.
- If the **Unrecognized TLV Received** is not present in the RAR/RAA, then it creates one and inserts it together with the relevant information into the RAR/RAA.
- If the **Unrecognized TLV Received** is present, the node inserts its information at the *end* of the vector and adjusts the length field.
- The node forwards all received vectors and the **Unrecognized TLV Received** onward in the RAR/RAA.
- The **Unrecognized TLV Received** from an RAR must be placed in the corresponding RAA.

[Optimization]An additional optimization we can make is to divide the code space of the TLVs into 2 parts so that one part of the space applies only to TLVs for functions relating to bandwidth brokers in the endpoint domains or the end systems and the other part applies only to functions that must (or should) be supported at intermediate nodes. With a slight change to the rules above, we can reduce the number of unrecognized TLVs reported.

Contributors

The following people have contributed heavily to this and earlier versions of this document:

- Larry Dunn, Cisco

- Rüdiger Geib, Deutsche Telekom
- Susan Hares, Merit
- Rob Neilson, BCIT
- Francis Reichmeyer, IP Highway
- Dave Spence, Merit
- Andreas Terzis, UCLA
- Jeff Wheeler, Nortel

Terminology

Diffserv Terms

Downstream DS domain

The DS domain downstream of traffic flow on a boundary link.

DS boundary node

A DS node that connects one DS domain to a node in another DS domain or in a domain that is not DS-capable.

DS domain

A DS-capable domain; a contiguous set of nodes which operate with a common set of service provisioning policies and PHB definitions.

DS egress node

A DS boundary node in its role of handling traffic as it leaves a DS domain.

DS ingress node

A DS boundary node in its role of handling traffic as it enters a DS domain.

Service

The overall treatment of a defined subset of a customer's traffic within a DS domain.

Service Level Agreement (SLA)

A service contract between a customer and a provider that specifies the forwarding service a customer should receive. A customer may be a user organization (source domain) or another DS domain (upstream domain).

Service Provisioning Policy

A policy that defines how traffic conditioners are configured on DS boundary nodes and how traffic streams are mapped to DS behavior aggregates to achieve a range of services.

Upstream DS domain

The DS domain upstream of traffic flow on a boundary link.

"New" Terms

In addition to the terms from [RFC2475], we define the following:

Bandwidth Broker (BB)

A bandwidth broker (BB) manages network resources for IP QoS services supported in the network and used by customers of the network services. A BB may be considered a type of policy manager (see Policy Manager definition below) in that it performs a subset of policy management functionality.

Connection Admission Control (CAC)

Connection admission control refers to the process, performed by the BB, of admitting connection requests to the network based on available resources in the network. The determination of available resources may be done on a static or dynamic basis.

Domain

A domain typically refers to DiffServ domain - see *DS domain* above, from [RFC2475].

Edge Router (or Edge Device)

We use the terms edge router, edge device, and boundary node interchangeably. See *DS boundary node* above, from [RFC2475].

Inter-Domain Communication

Inter-domain communication refers to the protocol messages and control data that are exchanged between BBs in adjacent domains.

Intra-Domain Communication

Intra-domain communication refers to the protocol messages and control data that are exchanged between a BB and the nodes (usually edge devices) within that BB's domain.

Peer Domains

Two domains are peer domains if they are adjacently connected.

Per Hop Behavior (PHB)

The externally observable forwarding behavior applied at a DS-compliant node to a DS behavior aggregate. Note that while each service is mapped to a PHB (and specific DS Code Point(s)), it is not possible to identify a service by its PHB (e.g. AF).

Policy Manager (PM) or Policy Server (PS)

A policy manager (PM) or policy server (PS) typically manages the access of users to network policy services. As part of the process of admitting users to access policy services, a PM may employ a BB for CAC, as described above.

Premium Service

Premium Service refers to a quantitative differentiated service which provides a guaranteed low loss and jitter over a DS region. The Premium Service often is also described as "Virtual Leased Line (VLL)" Service. The exact service specification may be found in [QBONEARCH].

Resource Allocation Request (RAR)

A RAR refers to a request for network resources (or service) from an individual user to the BB of that user's domain. If the request includes network resources for outside of the user's local domain, the admission control may be performed based on the SLS(s) in place with adjacent domains. Accepted RARs may result in service provisioning policy (see above) installed in edge devices by a BB.

Service

Service is the overall treatment of a defined subset of a customer's traffic within a DS domain or end-to-end [RFC2475]. In this document, the [RFC2475] service definition will also be applied for traffic treatment between two domains. This leads to unilateral, bilateral and end-to-end service specifications. Whenever "service" is used as stand alone term in the following, bilateral and end-to-end services are meant.

Each "service" is mapped to a PHB identified by its DS Code-Point(s) (DSCPs). By this definition a "SERVICE" IS IDENTIFIED BY ITS "DSCPs" within a DS domain as well as between two adjacent DS domains in the following. The IETF does only standardize PHB's. IETF specifications usually DO NOT LINK DSCPs TO SPECIFIC SERVICES. While each service is mapped to a PHB (and specific DS Code Point(s)), it is not possible to identify a service by its PHB (e.g. AF).

Unilateral Service

Unilateral service is used to refer to "service" as defined in DiffServ [RFC2475] (above).

Service Level Agreement (SLA)

See SLA in [rfc2475] which defines SLA as "a service contract between a customer and a service

provider that specifies the forwarding service a customer should receive. A customer may be a user organization (source domain) or another DS domain (upstream domain). A SLA may include traffic conditioning rules which constitute a Traffic Conditioning Agreement (TCA) in whole or in part."

Service Level Specification (SLS)

An SLS refers to the particular information relative to the BB and the network devices in order to support a SLA in that network. Information in an SLS is generally on the level of aggregate data flows and the resources/bandwidth provisioned for those flows. An SLS is typically applied at the endpoints of a link connecting adjacent domains and reflects traffic that will be sent from the upstream domain to the downstream domain.

Service Users

End systems users and other entities that can generate RARs. It could as well be an operator that does the RARs (e.g. after being contacted by end-users).

Subnet Bandwidth Manager (SBM)

A Subnet Bandwidth Manager (see [15]) is in charge of the resource allocation requests for a subnet. All users on a variety of hosts on a subnet would defer to the Subnet Bandwidth Manager to negotiate the bandwidth with the bandwidth broker within a domain. The communication path to request resources would be the host signaling the SBM that it needs premium service. The SBM will send an RAR to the BB within the domain. An SBM can also be pre-configured with the ability to requests certain bandwidth resources.

Virtual Leased Line (VLL)

See Premium Service.

References

1. Multidomain Bandwidth Broker Model, Memo to the QBBAC, September 1999, D. Spence
2. Integrated Services Operation over Diffserv Networks, <draft-ietf-issll-diffserv-rsvp-03.txt> Internet Draft, Bernet, Yavatkar, Ford, Baker, Zhang, Speer, Braden, Davie, June 1999, Work in progress
3. A conceptual model for DiffServ routers, <draft-ietf-diffserv-model-00.txt>, Internet Draft, Bernet, Smith, Blake, June 1999, Work in progress
4. A Two-bit Differentiated Services Architecture for the Internet; K. Nichols, V. Jacobson, L. Zhang, 1998
5. QBone Architecture (v1.0), Ben Teitelbaum et al. Internet 2 QoS Working Group Draft, August 1999, Work-in-progress
6. An expedited forwarding PHB, V. Jacobson, K. Nichols, K. Poduri, RFC 2598, IETF proposed standard, June 1999
7. Architecture for Differentiated Services, S. Blake, D. Black, M Carlson, E. Davies, Z. Wang, W. Weiss, RFC 2475, December 1998
8. A Two-bit Differentiated Services Architecture for the Internet. K. Nichols, V. Jacobson, L. Zhang, July 1999, RFC 2638, Informational.
9. Aggregation of RSVP for IPv4 and IPv6 Reservations, <draft-ietf-issll-rsvp-aggr-00.txt> Fred Baker, Carol Iturralde, Francois Le Faucheur, Bruce Davie, work in progress.
10. SIBBS: Simple Interdomain Bandwidth Broker Signalling, Ben Teitelbaum, Note to the BBAC mailing list, September 1999.
11. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, K. Nichols, S. Black, F. Baker, D. Black, RFC 2474, Standards track, December 1998.
12. Y. Bernet, J. Binder, S. Blake, M. Carlson, B. Carpenter, S. Keshav, E. Davies, B. Ohlman, D. Verma, Z. Wang, W. Weiss, "A Framework for Differentiated Services", Internet Draft,

draft-ietf-diffserv-framework-02.txt, February 1999.

13. R. Guerin, S. Blake, S. Herzog, "Aggregating RSVP-based QoS Requests", Internet Draft, draft-guerin-aggreg-rsvp-00.txt, November 1997.
14. J. Wroclawski, "The Use of RSVP with IETF Integrated Services", Request for comments, rfc 2210, (proposed standard), Internet Engineering Task Force, September 1997.
15. Raj Yavatkar, Don Hoffman, Yoram Bernet, Fred Baker, Michael Speer "Subnet Bandwidth Manager: A protocol for RSVP-based Admission Control over 802-style networks" Internet Draft (work in progress) draft-ietf-issll-is802-sbm-09.txt

Appendix 1: Alternative System Model

System Model

This model follows along the lines of [2] and is shown in Figure X. (It is not exactly the model of [2], though.)

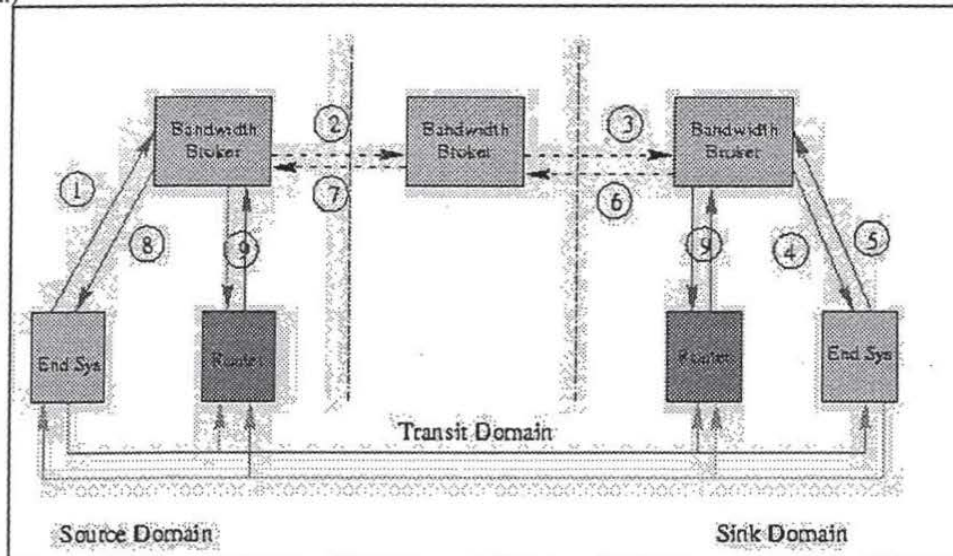


Figure X: System model 2

In this model, bandwidth broker communication takes place in addition to end-to-end communication between the end systems via RSVP. The RSVP protocol between the end systems could be tunneled through the transit domains and the PDUs re-appear at the endpoint domains. There are several designs possible in this case, some of them outlined in [2]. Figure X shows one of them.

The general approach is that the BB is concerned with edge-to-edge resource reservation, but not necessarily with the reservations in the source and sink domains. The RSVP messages sent by the end systems cause resource reservations (intserv) to be made both in the end systems themselves and in the path from the border router of the domain to the end system.

Here we describe in overview, the operation of the system, assuming that the source and sink domains are RSVP-aware, and that the transit domain(s) are not aware of the RSVP messages flowing through them.

- (As noted in [2] there are several different ways to handle this, but we will stay with the simplest case.) This implies that the PATH and RESV messages originating in the source and sink domains are tunneled or otherwise masked from the transit domains (which may also have RSVP-aware routers for other purposes).

System operation

1. The end system, A in the source domain sends a request (RAR) to its bandwidth broker A whose job it is to do resource allocation and make admission control decisions. Bandwidth broker A then checks whether the request fits into the SLSs that it currently has with adjacent domain(s) in the direction of domain C. Note that this implies a sufficiently long prefix to enable BB A to determine this.
2. Assuming that the request can be handled, BB A sends an inter-domain RAR to BB B. Note that BB A may aggregate this with other requests. It is not necessarily the case that each request received by a BB results in an inter-domain request.
3. BB B receives the inter-domain request from BB A, may again perform some level of aggregation and sends the request further on to BB C. Further, if domain B is multi-homed, then enough has to be known of the routing of the requests through domain B to determine the egress interface and SLS with domain C.
4. BB C makes the determination, again based on existing SLSs, whether to admit the reservation and responds to BB B. NOTE: This may involve further communication with the end system -- flows (4) and (5) in the diagram -- but this is not strictly necessary.
5. BB B notes the success or failure of the reservation and forwards the information back to BB A.
6. BB A notes the success or failure of the reservation and forwards the results back to the hosts.
7. The BBs in the source and sink domains may adjust the parameters in the (border) routers in their domains as a result of the reservation.

The end systems can then send the RSVP messages end-to-end which nails up the reservation.

*Ben Teitelbaum
ben@internet2.edu*

*Phil Chimento
chimento@ctit.utwente.nl*

The work of Phil Chimento was supported by SURFnet contract Number 3365

Last modified: Mon Feb 28 14:14:27 MET 2000



UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

| APPLICATION NUMBER | FILING/RECEIPT DATE | FIRST NAMED APPLICANT | ATTORNEY DOCKET NUMBER |
|--------------------|---------------------|-----------------------|------------------------|
| 09/841,752 | 04/24/2001 | Sorin Surdila | 1000-0216 |

CONFIRMATION NO. 6405

FORMALITIES LETTER



OC00000006191281

Smith, Danamraj & Youst, P.C.
12900 Preston Road, Suite 1200, LB-15
Dallas, TX 75230

Date Mailed: 06/18/2001

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION


FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is unsigned.
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(e) of \$130 for a non-small entity, must be submitted with the missing items identified in this letter.
- **The balance due by applicant is \$ 130.**

*A copy of this notice **MUST** be returned with the reply.*


Customer Service Center
Initial Patent Examination Division (703) 308-1202
PART 3 - OFFICE COPY



Section 118
#3

PATENT APPLICATION
DOCKET NO. 1000-0216

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:

Sorin Surdila et al.

Serial No.: 09/841,752

Filed: April 24, 2001

§
§
§
§
§
§

Group No.: 2661

Examiner: Unknown

For: SYSTEM AND METHOD FOR PROVIDING END-TO-END QUALITY OF SERVICE
(QoS) ACROSS MULTIPLE INTERNET PROTOCOL (IP) NETWORKS

BOX MISSING PARTS
Commissioner for Patents
Washington, D.C. 20231

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to:
Commissioner for Patents, Washington, D.C. 20231

on June 20, 2001 by Steven W. Smith

Signature *Steven W. Smith*

**RESPONSE TO NOTICE TO FILE MISSING PARTS OF
NONPROVISIONAL APPLICATION**

In response to the Notice to File Missing Parts of Nonprovisional Application, dated June 18, 2001, to which a response is due by August 18, 2001, a signed declaration is hereby submitted.

A check in the amount of \$130.00 is enclosed for payment of the surcharge set forth in 37 CFR 1.16(e).

Dated: June 20, 2001

SMITH, DANAMRAJ & YOUST, P.C.
12900 Preston Road, Suite 1200, LB-15
Dallas, Texas 75230-1328
(972) 720-1202, ext. 229

Respectfully submitted,

Steven W. Smith

Steven W. Smith
Registration No. 36,684



UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

| APPLICATION NUMBER | FILING/RECEIPT DATE | FIRST NAMED APPLICANT | ATTORNEY DOCKET NUMBER |
|--------------------|---------------------|-----------------------|------------------------|
| 09/841,752 | 04/24/2001 | Sorin Surdila | 1000-0216 |

CONFIRMATION NO. 6405

FORMALITIES LETTER



OC00000006191281

Smith, Danamraj & Youst, P.C.
12900 Preston Road, Suite 1200, LB-15
Dallas, TX 75230

Date Mailed: 06/18/2001

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is unsigned.
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(e) of \$130 for a non-small entity, must be submitted with the missing items identified in this letter.
- **The balance due by applicant is \$ 130.**

A copy of this notice MUST be returned with the reply.

Te H S Youst
Customer Service Center

Initial Patent Examination Division (703) 308-1202

PART 2 - COPY TO BE RETURNED WITH RESPONSE

06/27/2001 BNGUYEN1 00000142 09841752

01 FC:105

130.00 OP

**COMBINED DECLARATION AND POWER OF ATTORNEY**

As a below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below next to my name; and

I verily believe that I am an original, first, and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled:

**SYSTEM AND METHOD FOR PROVIDING
END-TO-END QUALITY OF SERVICE (QoS) ACROSS
MULTIPLE INTERNET PROTOCOL (IP) NETWORKS**

the specification of which:

___ is attached hereto.

X was filed on 04/24/01 as Application Serial No. 09/841,752 and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Office all information known to me to be material to the patentability of this application as defined in 37 CFR § 1.56.

I hereby claim the benefit under 35 U.S.C. § 119(e) of any previously filed United States provisional patent application(s) listed below which were filed not more than 12 months before the filing of this application, and which disclose the invention of this application in the manner provided by the first paragraph of 35 U.S.C. § 112:

Provisional Application No.

Filing Date

DOCKET NO. 1000-0216

PATENT

I hereby claim foreign priority benefits under 35 U.S.C. § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of any application on which priority is claimed:

| Country | Number | Date Filed | Priority Claimed |
|---------|--------|------------|------------------|
| _____ | _____ | _____ | _____ |
| _____ | _____ | _____ | _____ |

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose material information as defined in 37 CFR § 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

| Application Serial No. | Filing Date | Status (patented, pending) |
|------------------------|-------------|----------------------------|
| _____ | _____ | _____ |
| _____ | _____ | _____ |

I hereby appoint the following attorneys and/or agents to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith: STEVEN W. SMITH, Reg. No. 36,684 and LAWRENCE R. YOUST, Reg. No. 38,795 of the firm of Smith, Danamraj & Youst, P.C., 12900 Preston Road, Suite 1200, LB 15, Dallas, Texas 75230; and STANLEY R. MOORE, Reg. No. 26,958 and GERALD T. WELCH, Reg. No. 30,332 of the firm of Jenkins & Gilchrist, 1445 Ross Avenue, Suite 3200, Dallas, Texas 75202.

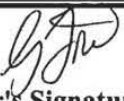
Address all telephone calls and correspondence to:

Steven W. Smith
SMITH, DANAMRAJ & YOUST, P.C.
12900 Preston Road, Suite 1200, LB 15
Dallas, Texas 75230-1328
(972) 720-1202

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

| | | | |
|---|--|-----------------------------|--------------------|
| 1 | Sorin Surdila | <i>Surdila</i> | 25/04/01 |
| | Full Name | Inventor's Signature | Date |
| | 463 Toussaint St. Dorothee Laval, Quebec CANADA H7X 3N3 | | CANADA |
| | Residence | | Citizenship |
| | 463 Toussaint St. Dorothee Laval, Quebec CANADA H7X 3N3 Mailing Address | | |

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

| | | | | |
|---|---|---|--|--------------------|
| 2 | George Foti |  | | 2001/04/25 |
| | Full Name | Inventor's Signature | | Date |
| | 163 Mozart Dollard des Ormeaux, Quebec CANADA H9G 2Z8 | | | CANADA |
| | Residence | | | Citizenship |
| | 163 Mozart Dollard des Ormeaux, Quebec CANADA H9G 2Z8 Mailing Address | | | |



PATENT APPLICATION
Attorney Docket No. P14655US

RECEIVED

MAR 01 2002

Technology Center 2600

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

2661

#5

| | | | |
|------------------------------|----------------|---|----------------------|
| In re Patent Application of: | SURDILA et al. |) | |
| | |) | |
| Serial No.: | 09/841,752 |) | Group Art Unit: 2661 |
| | |) | |
| Filed: | 2001-04-24 |) | Examiner: Unknown |
| | |) | |

For: SYSTEM AND METHOD FOR PROVIDING END-TO-END QUALITY OF
SERVICE (QoS) ACROSS MULTIPLE INTERNET PROTOCOL (IP) NETWORKS

Assistant Commissioner for Patents
Washington, D.C. 20231



REVOCATION OF POWER OF ATTORNEY AND CHANGE OF MAILING
ADDRESS

Dear Sir:

The Applicants hereby request that the Power of Attorney for SMITH, DANAMRAJ & YOST, P.C., be revoked, and hereby appoint Sandra Beauchesne, Reg. No. 43,422, and Alex Nicolaescu, Reg. No. 47,253 as agents of record for the above-mentioned application.

Please now send all further correspondence to the following address:

Ericsson Canada Inc.
LMC/UP IPR Section
8400 Decarie Blvd
Montreal, QC
H4P 2N2
CANADA

For more information, the undersigned can be reached at (514) 345-7900 ext.:
5612.

Respectfully submitted,

Date: February 26, 2002

S. Beauchesne
Sandra Beauchesne
Registration: No. 43,422



UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

| APPLICATION NUMBER | FILING DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|--------------------|-------------|-----------------------|------------------------|
| 09/841,752 | 04/24/2001 | Sorin Surdila | 1000-0216 |

27902
ERICSSON RESEARCH CANADA
8400 DECARIE BLVD.
MONTREAL, QC H4P 2N2
CANADA

CONFIRMATION NO. 6405



OC000000007633007

#6

Date Mailed: 03/13/2002

NOTICE REGARDING POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/28/2002.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

KENNETH A DAVIS
2600 (703) 306-3337

OFFICE COPY



UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

| APPLICATION NUMBER | FILING DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|--------------------|-------------|-----------------------|------------------------|
| 09/841,752 | 04/24/2001 | Sorin Surdila | 1000-0216 |

CONFIRMATION NO. 6405



OC000000007632997

Smith, Danamraj & Youst, P.C.
12900 Preston Road, Suite 1200, LB-15
Dallas, TX 75230

Date Mailed: 03/13/2002

NOTICE REGARDING POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/28/2002.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

KENNETH A DAVIS
2600 (703) 306-3337

OFFICE COPY



UNITED STATES PATENT AND TRADEMARK OFFICE

Feb

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--|-------------|----------------------|-----------------------|------------------|
| 09/841,752 | 04/24/2001 | Sorin Surdila | 1000-0216 | 6405 |
| 27902 | 7590 | 06/30/2005 | EXAMINER | |
| ERICSSON RESEARCH CANADA 8400 DECARIE BLVD. MONTREAL, QC H4P 2N2 CANADA | | | NGUYEN, PHUONGCHAU BA | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2665 | |

DATE MAILED: 06/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | | |
|------------------------------|------------------------|---------------------|--|
| Office Action Summary | Application No. | Applicant(s) | |
| | 09/841,752 | SURDILA ET AL. | |
| | Examiner | Art Unit | |
| | Phuongchau Ba Nguyen | 2665 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 April 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-11 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4 and 6-11 is/are rejected.
- 7) ☒ Claim(s) 5 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 April 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892). | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Information Disclosure Statement

1. The information disclosure statement filed 4-24-1 fails to comply with 37 CFR 1.98(a)(1), which requires the following: (1) a list of all patents, publications, applications, or other information submitted for consideration by the Office; (2) U.S. patents and U.S. patent application publications listed in a section separately from citations of other documents; (3) the application number of the application in which the information disclosure statement is being submitted on each page of the list; (4) a column that provides a blank space next to each document to be considered, for the examiner's initials; and (5) a heading that clearly indicates that the list is an information disclosure statement. The information disclosure statement has been placed in the application file, but the information referred to therein has not been considered. For example, the PTO-1449 is not found in the original disclosure.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting

directly or indirectly from an international application filed before November 29, 2000.

Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

1. Claims 1-4, 6-7 are rejected under 35 U.S.C. 102(e) as being anticipated by Teitelbaum (Outline of Bbroker Architecture).

Regarding claim 1:

Teitelbaum (Outline of Bbroker Architecture) discloses Qbone Bandwidth Broker Architecture, *a method of ensuring a requested Quality of Service (QoS) (RAR-Resource Allocation Request, see page 8) for a media flow that is routed from a first terminal (end system, see the figure in page 13) in an originating network (source domain, see the figure in page 13), through at least one transit network (transit domain, see the figure in page 13), to a second terminal (end system) in a terminating network (sink domain), said originating network (source domain) including an Originating Bandwidth Broker (BB-O) (bandwidth broker) and an Originating Media Policy Server (MPS-O) (policy of the source domain-not shown, see step e in page 13), said transit network (sink domain) including a Transit Bandwidth Broker (BB-T) (bandwidth broker) and a Transit Media Policy Server (MPS-T) (policy of the transit domain-not shown, see step f in page 14), and said terminating network (sink domain) including a Serving Bandwidth Broker (BB-S) (bandwidth broker) and a Serving Media Policy Server (MPS-S) (policy of the sink domain-not shown, see step d in page 14), said method comprising the steps of:*

sending an origination message (RAR) from the originating network (source domain, see the figure in page 13) to the terminating network (sink domain) with a proposed session description that identifies the requested QoS (see lines 2-4, page 13);

determining by the terminating network (the bandwidth broker in the destination/sink domain) that the session description is agreeable (see behavior of bandwidth broker in destination domain, step d, page 14);

sending a first Bandwidth Broker Protocol Resource Allocation Request (RAR) from the BB-S to the BB-T with binding information that identifies the first and second terminals and the requested QoS (see lines 31-40, page 14);

determining by the BB-T whether a Service Level Agreement (SLA) between the transit network and the terminating network allows sufficient resources to be allocated to meet the requested QoS (see lines 1-7, page 15);

sending a second RAR from the BB-T to the BB-O with the binding information, upon determining by the BB-T that the SLA between the transit network and the terminating network allows sufficient resources to be allocated to meet the requested QoS (see lines 1-7, page 15);

reserving the resources required to meet the requested QoS in the originating network, the transit network, and the terminating network (see lines 8-13, page 15); and

setting up a multimedia session to carry the media flow with the requested QoS (see lines 14-17).

Regarding claim 2:

Teitelbaum discloses sending a first Resource Allocation Answer (RAA) from the BB-O to the BB-T (see line 13, page 13 to line 11, page 14); sending a second RAA from the BB-T to the BB-S (see lines 12-15, page 14); and installing by the BB-O, the BB-T, and the BB-S, applicable policies in edge routers to provide the requested QoS in the originating network, the transit network, and the terminating network, respectively (see routers in the figure on page 13).

Regarding claim 3:

Teitelbaum discloses sending a QoS reservation request (RAR) that includes the agreed session description and the binding information from an Originating Call State Control Function (Originating P-CSCF) to the BB-O (see lines 1-12, page 13); determining by the BB-O whether a previous valid resource reservation exists for the session associated with the binding information (see lines 9-12, page 13); and sending an immediate successful reservation response from the BB-O to the Originating P-CSCF, upon determining that a previous valid resource reservation exists for the session associated with the binding information (see lines 13-15, page 13).

Regarding claim 4:

Teitelbaum discloses reserving resources required for the requested QoS, upon determining that a previous valid resource reservation does not exist for the session associated with the binding information (see lines 9-12 & 16-17, page 13).

Regarding claim 6:

Teitelbaum discloses wherein the step of sending the QOS reservation request (RAR) from the Originating P-CSCF to the BB-O includes sending the QoS reservation request utilizing a Common Open Policy Service (COPS) protocol and a Bandwidth Broker protocol (see lines 1-12, page 13).

Regarding claim 7:

Teitelbaum discloses creating the binding information from a source Internet Protocol (IP) address of the first terminal, an identification of a Real Time Protocol (RTP) port assigned by the first terminal, a destination IP address of the second terminal, and an identification of an RTP port assigned by the second terminal (see lines 1-12, page 13).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 8-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teitelbaum (Outline of Bbroker Architecture) in view of Donovan (6,366,577).

Regarding claim 8:

Teitelbaum discloses a Multimedia Control Server (MMCS) in a multi-service core network for ensuring a requested Quality of service (QoS) for a media flow being routed from a first terminal (source terminal at source domain, see figure on page 13) in the core network (source domain) to a second terminal (end terminal at sink domain, see figure on page 13) in a terminating network (sink domain), said MMCS comprising:

- an Originating Call State Control Function (Originating P-CSCF) that serves the first terminal (the function for sending RAR from send system to bandwidth broker via (1), see the figure on page 13, lines 2-4 of page 13);

- an Originating Bandwidth Broker (BB-O) that manages resources in the originating network (Bandwidth Broker in source domain, the figure in page 13);

- a first interface (1) between the Originating P-CSCF and the BB-O for passing binding information from the Originating P-CSCF to the BB-O, the binding information identifying the first and second terminals and the requested QoS (see lines 2-4, page 13);

- a third interface (connection lines) between the BB-O and a plurality of edge routers (routers in source domain, transit domain, and sink domain, see the figure in page 13) that route the media flow into and out the originating network, said third interface for passing from BB-O to the edge routers, policy rules applicable to a specific media flow (see lines 11-12, page 13).

Teitelbaum (Qbone Bandwidth Broker Architecture-Work in Progress) discloses all the claimed limitations, except (1) an Originating Media Policy Server (MPS-O) that

provides policy rules regarding allocation of resources in the originating network; (2) a second interface between the MPS-O and the BB-O for passing the policy rules from the MPS-O to the BB-O.

However, in the same field of endeavor, Donovan (6,366,577) discloses an Originating Media Policy Server (MPS-O) 140-fig.1 that provides policy rules regarding allocation of resources in the originating network (see col.5, lines 16-40) (corresponding to (1)); a second interface (COPS-not shown in fig.1) between the MPS-O and the BB-O for passing the policy rules from the MPS-O to the BB-O (col.5, lines 20-24) (corresponding to (2)). Therefore, it would have been obvious to an artisan to apply Donovan's teaching to Teitelbaum's system with the motivation being to provide an acceptable QoS during an IP communication across the Internet.

Regarding claim 9:

Teitelbaum discloses a Multimedia Control Server (MMCS) in a multi-service core network for ensuring a requested Quality of service (QoS) for a media flow from an application on a first terminal that is transported through a network owned by an administration, said media flow being routed through at least one transit network that is not owned by the same administration, to a second terminal in a terminating network, said MMCS comprising:

an Originating Call State Control Function (Originating P-CSCF) that serves the first terminal (the function for sending RAR from send system to bandwidth broker via (1), see the figure on page 13, lines 2-4 of page 13);

an Originating Bandwidth Broker (BB-O) that manages resources in the originating network (Bandwidth Broker in source domain, the figure in page 13);

a first interface (1) between the Originating P-CSCF and the BB-O for passing binding information from the Originating P-CSCF to the BB-O, the binding information identifying the first and second terminals and the requested QoS (see lines 2-4, page 13);

a third interface (connection lines) between the BB-O and a plurality of edge routers (routers in source domain, transit domain, and sink domain, see the figure in page 13) that route the media flow into and out the originating network, said third interface for passing from BB-O to the edge routers, policy rules applicable to a specific media flow (see lines 11-12, page 13); and

a fourth interface (7-see the figure in page 13) between the BB-O and a Transit Bandwidth Broker (BB-T) in the transit network for passing the binding information from the BB-T to the BB-O said binding information having been received by the BB-T from a Serving Bandwidth Broker (BB-S) in the terminating network.

Teitelbaum (Qbone Bandwidth Broker Architecture-Work in Progress) discloses all the claimed limitations, except (1) an Originating Media Policy Server (MPS-O) that provides policy rules regarding allocation of resources in the originating network; (2) a

second interface between the MPS-O and the BB-O for passing the policy rules from the MPS-O to the BB-O.

However, in the same field of endeavor, Donovan (6,366,577) discloses an Originating Media Policy Server (MPS-O) 140-fig.1 that provides policy rules regarding allocation of resources in the originating network (see col.5, lines 16-40) (corresponding to (1)); a second interface (COPS-not shown in fig.1) between the MPS-O and the BB-O for passing the policy rules from the MPS-O to the BB-O (col.5, lines 20-24) (corresponding to (2)). Therefore, it would have been obvious to an artisan to apply Donovan's teaching to Teitelbaum's system with the motivation being to provide an acceptable QoS during an IP communication across the Internet.

Regarding claim 10:

Teitelbaum disclose all the claimed limitations, except (1) a fifth interface between the MPS-O and a clearing house that performs as an Authorization, Authentication, and Accounting (AAA) server.

However, in the same field of endeavor, Donovan discloses a fifth interface (connection between Policy 1 and clearing house-fig.1) between the MPS-O and a clearing house that performs as an Authorization, Authentication, and Accounting (AAA) server (see col.5, line 62-col.6, lines 7) (corresponding to (1)). Therefore, it would have been obvious to apply Donovan's teaching to Teitelbaum's system with the motivation being to provide authorization for QoS, a collector of usage reports, and settlement between service providers.

Regarding claim 11:

Teitelbaum discloses a system for ensuring a requested Quality of Service (QoS) for a media flow belonging to an application and originating in an originating network owned by an administration, said media flow being routed from a first terminal in the originating network through at least one transit network that not owned by the same administration, a second terminal in a terminating network, said system comprising:

- a first Multimedia Control Server (MMCS) in the originating network comprising:

- an Originating Call State Control Function (Originating P-CSCF) that serves the first terminal (the function for sending RAR from send system to bandwidth broker via (1), see the figure on page 13, lines 2-4 of page 13);

- an Originating Bandwidth Broker (BB-O) that manages resources in the originating network (Bandwidth Broker in source domain, the figure in page 13);

- a first interface (1-figure in page 13) between the Originating P-CSCF and the BB-O for passing a session description and binding information from the Originating P-CSCF to the BB-O, the binding information identifying the first and second terminals and the requested QoS (see lines 2-4, page 13);

- a plurality of originating edge routers (router at source domain) that route the media flow into and out of the originating network;

- a third interface (connection lines) between the originating edge routers (routers in source domain, transit domain, and sink domain, see the figure in page 13) and the

Art Unit: 2665

BB-O for passing policy rules applicable to specific media flows from the BB-O to the originating edge routers (see lines 11-12, page 13);

- a second MMCS in the terminating network comprising:

- a Serving Call State Control Function (Terminating P-CSCF) that serves the second terminal (the function for sending RAR from send system to bandwidth broker via (1), see the figure on page 14, lines 32-37 of page 14);

- a Serving Bandwidth Broker (BB-S) that manages resources in the terminating network (Bandwidth Broker in sink domain, the figure in page 13);

- a fourth interface (5-figure in page 13) between the Terminating P- CSCF and the BB-S for passing an agreed session description from the Terminating P-CSCF to the BB-S (lines 32-37, page 14);

- a plurality of serving edge routers (routers in sink domain-figure on page 13) that route the media flow into and out of the terminating network (sink domain);

- a sixth interface (connection) between the serving edge routers (router-figure on page 13) and the BB-S (bandwidth broker-figure on page 13) for passing policy rules applicable to specific media flows from the BB-S to the serving edge routers;

- a Transit Bandwidth Broker (BB-T) in the transit network (bandwidth broker in transit domain);

- a seventh interface (6-figure on page 13) between the BB-S and the BB-T for passing the binding information from the BB-S to the BB-T in a first Resource Allocation Request (RAR); and

an eighth interface (7-figure on page 13) between the BB-T and the BB-O for passing the binding information from the BB-T to the BB-O in a second RAR.

Teitelbaum (Qbone Bandwidth Broker Architecture-Work in Progress) discloses all the claimed limitations, except (1) an Originating Media Policy Server (MPS-O) that provides policy rules regarding allocation of resources in the originating network; (2) a second interface between the MPS-O and the BB-O for passing the policy rules from the MPS-O to the BB-O; and (3) a Serving Media Policy Server (MPS-S) that provides policy rules regarding allocation of resources in the terminating network; (4) a fifth interface between the MPS-S and the BB-S for passing the policy rules from the MPS-S to the BB-S.

However, in the same field of endeavor, Donovan (6,366,577) discloses an Originating Media Policy Server (MPS-O) 140-fig.1 that provides policy rules regarding allocation of resources in the originating network (see col.5, lines 16-40) (corresponding to (1)); a second interface (COPS-not shown in fig.1) between the MPS-O and the BB-O for passing the policy rules from the MPS-O to the BB-O (col.5, lines 20-24) (corresponding to (2)); and (3) a Serving Media Policy Server (MPS-S) 141-fig.1 that provides policy rules regarding allocation of resources in the terminating network; (4) a fifth interface (COPS-not shown in fig.1) between the MPS-S and the BB-S for passing the policy rules from the MPS-S to the BB-S (col.5, lines 20-24).

Therefore, it would have been obvious to an artisan to apply Donovan's teaching to Teitelbaum's system with the motivation being to provide an acceptable QoS during an IP communication across the Internet.

Allowable Subject Matter

5. Claim 5 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.


6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Phuongchau Ba Nguyen whose telephone number is 571-272-3148. The examiner can normally be reached on Monday-Friday from 10:00 a.m. to 2:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Huy Vu can be reached on 571-272-3155. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



STEVEN NGUYEN
PRIMARY EXAMINER



Phuongchau Ba Nguyen
Examiner
Art Unit 2665

| | | | |
|-----------------------------------|---------------------------------------|--|-------------|
| Notice of References Cited | Application/Control No. 09/841,752 | Applicant(s)/Patent Under Reexamination SURDILA ET AL. | |
| | Examiner Phuongchau Ba Nguyen | Art Unit 2665 | Page 1 of 1 |

U.S. PATENT DOCUMENTS

| * | | Document Number Country Code-Number-Kind Code | Date MM-YYYY | Name | Classification |
|---|---|--|-----------------|--------------------|----------------|
| X | A | US-6,366,577 B1 | 04-2002 | Donovan, Steven R. | 370/352 |
| X | B | US-2002/0041590 | 04-2002 | Donovan, Steven R. | 370/352 |
| X | C | US-6,594,277 | 07-2003 | Chiang et al. | 370/230 |
| X | D | US-6,141,686 | 10-2000 | Jackowski et al. | 709/224 |
| X | E | US-2004/0106403 | 06-2004 | Mori et al. | 455/452.2 |
| X | F | US-2004/0177107 | 09-2004 | Qing et al. | 709/200 |
| X | G | US-2002/0046284 | 04-2002 | Brabson et al. | 709/228 |
| | H | US- | | | |
| | I | US- | | | |
| | J | US- | | | |
| | K | US- | | | |
| | L | US- | | | |
| | M | US- | | | |

FOREIGN PATENT DOCUMENTS

| * | | Document Number Country Code-Number-Kind Code | Date MM-YYYY | Country | Name | Classification |
|---|---|--|-----------------|---------|------|----------------|
| | N | | | | | |
| | O | | | | | |
| | P | | | | | |
| | Q | | | | | |
| | R | | | | | |
| | S | | | | | |
| | T | | | | | |

NON-PATENT DOCUMENTS

| * | | Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages) |
|---|---|---|
| | U | |
| | V | |
| | W | |
| | X | |

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

BIBDATASHEET

CONFIRMATION NO. 6405

Bib Data Sheet

| | | | | |
|-----------------------------|---------------------------------------|--------------|------------------------|-------------------------------------|
| SERIAL NUMBER 09/841,752 | FILING DATE 04/24/2001 RULE | CLASS 370 | GROUP ART UNIT 2665 | ATTORNEY DOCKET NO. 1000-0216 |
|-----------------------------|---------------------------------------|--------------|------------------------|-------------------------------------|

APPLICANTS

Sorin Surdila, Laval, CANADA;
 George Foti, Dollard des Ormeaux, CANADA;

** CONTINUING DATA ***** *NA*

** FOREIGN APPLICATIONS ***** *NA*

IF REQUIRED, FOREIGN FILING LICENSE GRANTED
 ** 06/15/2001

| | | | | |
|---|--|-------------------------------|-----------------------|----------------------------|
| Foreign Priority claimed <input type="checkbox"/> yes <input checked="" type="checkbox"/> no | STATE OR COUNTRY CANADA | SHEETS DRAWING 12 | TOTAL CLAIMS 11 | INDEPENDENT CLAIMS 4 |
| 35 USC 119 (a-d) conditions met <input type="checkbox"/> yes <input checked="" type="checkbox"/> no <input type="checkbox"/> Met after Allowance | EXAMINER'S SIGNATURE <i>[Signature]</i> | INITIALS <i>[Initials]</i> | | |

Verified and Acknowledged

ADDRESS

AIR MAIL

27902
 ERICSSON RESEARCH CANADA
 8400 DECARIE BLVD.
 MONTREAL, QC
 H4P 2N2
 CANADA

TITLE

System and method for providing end-to-end quality of service (QoS) across multiple internet protocol (IP) networks

| | | |
|------------|---|--|
| FILING FEE | FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT | <input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) |
|------------|---|--|

<http://neo:8000/PrexServlet/PrexAction>

10/12/04

| | | |
|-----------------|--------------------------|--|
| RECEIVED 920 | No. _____ for following: | <input type="checkbox"/> 1.18 Fees (Issue) |
| | | <input type="checkbox"/> Other _____ |
| | | <input type="checkbox"/> Credit |

Search Notes

Application/Control No.

09/841,752

Examiner

Phuongchau Ba Nguyen

Applicant(s)/Patent under
Reexamination

SURDILA ET AL.

Art Unit

2665

SEARCHED

| Class | Subclass | Date | Examiner |
|-------|--|-----------|----------|
| 370 | 236, 351-352, 354,356, 389,401, | 5/16/2005 | PN |
| 379 | 90.1 | 5/16/2005 | PN |
| 709 | 226-227 | 5/16/2005 | PN |
| 709 | 224,237 | 5/16/2005 | PN |
| 455 | 452.2 | 5/16/2005 | PN |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

INTERFERENCE SEARCHED

| Class | Subclass | Date | Examiner |
|-------|----------|------|----------|
| | | | |
| | | | |
| | | | |
| | | | |

**SEARCH NOTES
(INCLUDING SEARCH STRATEGY)**

| | DATE | EXMR |
|------|-----------|------|
| east | 5/16/2005 | PN |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--|-------------|----------------------|-----------------------|------------------|
| 09/841,752 | 04/24/2001 | Sorin Surdila | 1000-0216 | 6405 |
| 27902 | 7590 | 05/02/2006 | EXAMINER | |
| ERICSSON RESEARCH CANADA 8400 DECARIE BLVD. MONTREAL, QC H4P 2N2 CANADA | | | NGUYEN, PHUONGCHAU BA | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2616 | |

DATE MAILED: 05/02/2006


Please find below and/or attached an Office communication concerning this application or proceeding.


| | | | |
|------------------------------|----------------------|----------------|--|
| Notice of Abandonment | Application No. | Applicant(s) | |
| | 09/841,752 | SURDILA ET AL. | |
| | Examiner | Art Unit | |
| | Phuongchau Ba Nguyen | 2616 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

This application is abandoned in view of:

1. ☒ Applicant's failure to timely file a proper reply to the Office letter mailed on 30 June 2005.
 - (a) ☐ A reply was received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply (including a total extension of time of _____ month(s)) which expired on _____.
 - (b) ☐ A proposed reply was received on _____, but it does not constitute a proper reply under 37 CFR 1.113 (a) to the final rejection. (A proper reply under 37 CFR 1.113 to a final rejection consists only of: (1) a timely filed amendment which places the application in condition for allowance; (2) a timely filed Notice of Appeal (with appeal fee); or (3) a timely filed Request for Continued Examination (RCE) in compliance with 37 CFR 1.114).
 - (c) ☐ A reply was received on _____ but it does not constitute a proper reply, or a bona fide attempt at a proper reply, to the non-final rejection. See 37 CFR 1.85(a) and 1.111. (See explanation in box 7 below).
 - (d) ☒ No reply has been received.
2. ☐ Applicant's failure to timely pay the required issue fee and publication fee, if applicable, within the statutory period of three months from the mailing date of the Notice of Allowance (PTOL-85).
 - (a) ☐ The issue fee and publication fee, if applicable, was received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the statutory period for payment of the issue fee (and publication fee) set in the Notice of Allowance (PTOL-85).
 - (b) ☐ The submitted fee of \$_____ is insufficient. A balance of \$_____ is due.
The issue fee required by 37 CFR 1.18 is \$_____. The publication fee, if required by 37 CFR 1.18(d), is \$_____.
 - (c) ☐ The issue fee and publication fee, if applicable, has not been received.
3. ☐ Applicant's failure to timely file corrected drawings as required by, and within the three-month period set in, the Notice of Allowability (PTO-37).
 - (a) ☐ Proposed corrected drawings were received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply.
 - (b) ☐ No corrected drawings have been received.
4. ☐ The letter of express abandonment which is signed by the attorney or agent of record, the assignee of the entire interest, or all of the applicants.
5. ☐ The letter of express abandonment which is signed by an attorney or agent (acting in a representative capacity under 37 CFR 1.34(a)) upon the filing of a continuing application.
6. ☐ The decision by the Board of Patent Appeals and Interference rendered on _____ and because the period for seeking court review of the decision has expired and there are no allowed claims.
7. ☐ The reason(s) below:


DORIS H. TO
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600


Phuongchau Ba Nguyen
AU 2616

Petitions to revive under 37 CFR 1.137(a) or (b), or requests to withdraw the holding of abandonment under 37 CFR 1.181, should be promptly filed to minimize any negative effects on patent term.

U.S. Patent and Trademark Office
PTOL-1432 (Rev. 04-01)

Notice of Abandonment

Part of Paper No. 20060417