International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

F.746

(06/2012)

SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES

Audiovisual services

Requirements of multimedia optimization control components

Recommendation ITU-T F.746

ITU-T F-SERIES RECOMMENDATIONS

NON-TELEPHONE TELECOMMUNICATION SERVICES

TELEGRAPH SERVICE	
Operating methods for the international public telegram service	F.1–F.19
The gentex network	F.20–F.29
Message switching	F.30–F.39
The international telemessage service	F.40–F.58
The international telex service	F.59–F.89
Statistics and publications on international telegraph services	F.90–F.99
Scheduled and leased communication services	F.100–F.104
Phototelegraph service	F.105–F.109
MOBILE SERVICE	
Mobile services and multidestination satellite services	F.110–F.159
TELEMATIC SERVICES	
Public facsimile service	F.160–F.199
Teletex service	F.200–F.299
Videotex service	F.300–F.349
General provisions for telematic services	F.350–F.399
MESSAGE HANDLING SERVICES	F.400–F.499
DIRECTORY SERVICES	F.500–F.549
DOCUMENT COMMUNICATION	
Document communication	F.550–F.579
Programming communication interfaces	F.580–F.599
DATA TRANSMISSION SERVICES	F.600–F.699
AUDIOVISUAL SERVICES	**F.700–F.799**
ISDN SERVICES	F.800–F.849
UNIVERSAL PERSONAL TELECOMMUNICATION	F.850–F.899
HUMAN FACTORS	F.900–F.999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T F.746

Requirements of multimedia optimization control components

Summary

Recommendation ITU-T F.746 defines multimedia optimization control components (MOCCs), which can provide guidance services to multimedia applications and services in the process of service node selection, traffic optimization, performance enhancement, etc. This Recommendation specifies the MOCC requirements and defines a MOCC functional model. Some typical MOCC deployment scenarios are also described.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T F.746	2012-06-29	16

Keywords

Control component, multimedia applications, multimedia services, optimization.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T F.746

Requirements of multimedia optimization control components

1 Scope

The multimedia optimization control components (MOCCs) defined in this Recommendation are assistance entities which can obtain reliable information from the underlying network. This sort of information can be fed to multimedia applications and services and used as guidance services in the process of service node selection, data traffic optimization and performance enhancement. The MOCC component is located between the multimedia applications and services layer and the network layer. MOCC entities will not be involved in actual data relay and transmission.

The MOCC components can be deployed either in distributed multimedia systems or traditional client-server systems. They can be used in various networks such as NGN [ITU-T Y.2012], internet and other distributed systems.

This Recommendation specifies requirements according to some typical scenarios.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T F.700] Recommendation ITU-T F.700 (2000), *Framework Recommendation for multimedia services*.

[ITU-T F.701] Recommendation ITU-T F.701 (2000), *Guideline Recommendation for identifying multimedia service requirements*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation does not use any terms defined elsewhere.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 supernode: A peer in the overlay network that offers services, including message routing, to other members or clients of the overlay network.

3.2.2 tracker: An index server that can assist in the communication between peers in some peer-to-peer file sharing and multimedia systems by collecting information of file replicas and then providing the corresponding information to the resource demanders to initiate a download.

4 Abbreviations

This Recommendation uses the following abbreviations and acronyms:

AS	Autonomous System
CDN	Content Delivery Network
DOS	Denial of Service
ID	Identity
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
MOCC	Multimedia Optimization Control Component
NAT	Network Address Translation
NGN	Next Generation Network
NLRF	Node Location Resolution Function
P2P	Peer to Peer
PoP	Point of Presence
RASF	Resource Awareness and Statistics Function
TCP	Transmission Control Protocol
VoIP	Voice over Internet Protocol

5 Overview

Due to the evolution of network and multimedia technologies, multimedia services are developing rapidly both on the system scale and on the volume of users, especially for services on the Internet. In contrast with traditional centralized service provision models, more and more services and applications tend to be deployed as distributed models, meaning that the data are transmitted along the paths established among nodes distributed across the whole network. Web content distribution, P2P streaming and P2P file sharing are typical examples of distributed models. For most distributed networks, each node should select one or more service providing nodes from a set of candidates to acquire the desired resources. However, under the end-to-end principle, applications and underlying networks are separated except on the end nodes. Therefore, the "selection" might be random, since the applications may not have the reliable information from transport networks such as topology, congestion status and network address translation (NAT) installation. Sometimes, nodes may cross several network boundaries to fetch the desired resources, thus generating a large amount of costly cross-ISP traffic.

MOCCs defined in this Recommendation are complementary entities that can collect reliable information from the underlying network, analyse it and provide guidance services to the multimedia applications and services (see [ITU-T F.700] and [ITU-T F.701]) in the process of service node selection, data traffic optimization and performance enhancement.

6 Functional architecture

Conceptually, multimedia optimization control components are located between the application and service layer and the network layer. The MOCC functional model is illustrated in Figure 1. It is composed of an MOCC server and MOCC clients.

The MOCC server, which resides on the network side, is responsible for collecting and analysing the information from the underlying transport network, and for providing the processed information to multimedia services and applications and to the MOCC client. The MOCC server consists of an entrance component, a node location resolution function (NLRF) and a resource awareness and statistics function (RASF).

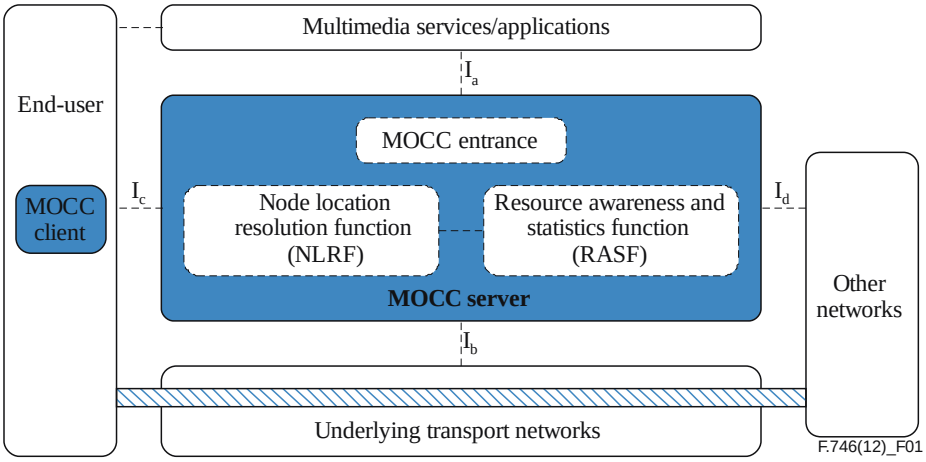


Figure 1 – Functional architecture for multimedia optimization control components

The functions of MOCC server components are as follows:

– **MOCC entrance component**: The MOCC entrance component provides registration and service discovery functions for NLRF, RASF and the MOCC client. NLRF and RASF should register its address, policies, server status and other information with the MOCC entrance component. In order to select the optimum service providing nodes, since there might be multiple MOCC servers in the network, the client should be first authenticated to the MOCC entrance component, which will be responsible for providing the client with the address of the most promising NLRF and RASF. The MOCC entrance component has interfaces with NLRF, RASF, as well as the MOCC clients.

– **NLRF and RASF**: NLRF and RASF can provide the guidance service or node selection service to applications by collecting and analysing the information of the underlying network. In practice, the NLRF and RASF can be implemented in one physical MOCC server. Network operators can deploy multiple MOCC servers with multiple instances of NLRF and RASF. The information of NLRF and RASF can be maintained by the MOCC entrance component. Some policies may be set for the clients to access NLRF and RASF.

By collecting the information of the underlying network in real time, the MOCC servers could obtain reliable information, such as static topology of the whole network (maintained by NLRF) or dynamic network status (maintained by RASF).

– **Network deployment information**: This information is relatively stable, for example, link capacities, node locations and adjacency relationships of the service nodes, and NAT installations. Furthermore, basic information of the service nodes and some policies enforced by the carriers may also be included in network deployment information. This kind of information is collected and maintained by NLRF.

– **Network resource status information**: This information includes bandwidth-related data, congestion status of links, etc. This kind of information is more dynamic than network deployment information and can be used as a basis for load balancing and traffic optimization. This kind of information is collected and maintained by RASF.

The MOCC client is embedded in the end user device and is responsible for communicating with the MOCC server to acquire information (through interface I_c in Figure 1) for multimedia service and application optimization.

Multimedia optimization control components (MOCC server and MOCC client) have interfaces with the multimedia service and application control entities (I_a in Figure 1), by which the multimedia system can acquire the necessary information from the transport network layer. In addition, those components should have interfaces with the transport network layer (I_b in Figure 1), through which they can collect and analyse the transport information according to the requirements of the given service.

7 Requirements

7.1 General requirements

GEN-110: The MOCC can be installed on centralized servers, or can be installed on multiple servers across the whole network. In any case, it should provide an interface to multimedia applications and services. The network information provided by the MOCC component should be accurate and reliable.

GEN-120: Under the P2P application context, according to the particular mechanism, the MOCC server should be able to be queried by the normal peers as well as by the P2P index servers. MOCCs should be suitable for different P2P systems and protocols, a general interface should be defined between MOCC and those applications.

GEN-130: MOCCs should be able to process massive requests from the applications with reasonable and acceptable response time. Specific performance requirements shall be fulfilled. Those requirements may include, amongst others, response time, efficiency, and query precision.

GEN-140: MOCCs are independent from specific multimedia systems and they should not have any impact on the implementation and performance of the multimedia services when guidance services are unavailable or MOCC components fail.

GEN-150: MOCC services provided by different service providers or network operators should be able to interoperate with one another.

GEN-160: Information of the underlying network provided by the MOCC services should be maintained in the local entities of the multimedia system, so as to reduce the network load caused by the frequent queries.

GEN-170: MOCCs should have a mechanism to protect the user privacy, some essential network operator information, and sensitive information collected from the bearer networks. It should also have a mechanism to protect themselves against DOS attacks.

7.2 MOCC service discovery requirements

SDR-110: Public MOCC servers are necessary to help address and policy registration.

SDR-120: MOCC clients should be authenticated before attempting to query MOCC servers.

SDR-130: MOCC clients should cache the replies from MOCC servers and avoid sending replicated query requests. This method helps lowering the processing burden on the MOCC server caused by the translation from IP addresses to network location identification. However, it should be noted that cache may be unreasonable in mobile scenarios.

SDR-140: To clearly define the discovery procedure, specification of discovery interface and corresponding protocol should be standardized.

7.3 Transport information collection requirements

Information of the underlying network that should be collected by MOCC servers includes *inter alia*:

TIC-110: Network topology includes network domain, network location properties, neighbourhood relationship, bandwidth between domains, route costs, etc. Network location properties should include network operator name, AS number, PoP, IP prefix, IP address, etc.

TIC-120: Alternatives of network operator's traffic engineering policy (network policy).

TIC-130: Network static information, such as network capacities, locations and adjacency relationships of the service node and the endpoints, the NAT installations and so on.

TIC-140: Network dynamic information, such as the bandwidth-related information, the congestion status of the links and so on.

7.4 Interaction and information exchange requirements

IIE-110: Information exchanged between the MOCC client and MOCC server may include information such as access authentication, network location search, network distance search, and network capacity search.

IIE-120: In the interaction between MOCC client and MOCC entrance, the MOCC client sends a request including information about itself such as identification or IP address to MOCC server; MOCC entrance replies one or more MOCC server's address to the authorized client.

IIE-130: In the interaction between MOCC server and MOCC entrance, the MOCC entrance should have MOCC server's address and policies information; this should be controlled by the network operator. MOCC entrance should be able to query the MOCC server's status, including busy, failure, and normal.

IIE-140: Within the MOCC server, interaction of information includes transport network information synchronization and client request forwarding.

7.5 Security requirements

SEC-110: MOCC server should keep the network information and content secret, and it should take measures to protect the privacy of the MOCC client end users.

SEC-120: Appropriate methods should be deployed to prevent attacks targeted at MOCC servers.

SEC-130: An authentication mechanism should be used between the MOCC server and network operator in order to establish a trust relationship between these two entities.

Appendix I

MOCC deployment scenarios

(This appendix does not form an integral part of this Recommendation.)

I.1 MOCC deployment in distributed file share services systems

I.1.1 General description

Distributed file sharing applications are very common in the Internet and have developed rapidly in recent years. Their prominent advantages are high efficiency and reliability because the services and resources are distributed across the whole network so that each peer can acquire different file replicas from multiple candidates. Therefore, file exchanging is becoming more flexible than before. Among these file sharing systems, the most prevalent method is to use P2P overlay technologies to implement file sharing applications amongst the peers in networks. Depending on whether the P2P overlay network is used for control message propagation or for data transmission, the P2P file sharing systems can be classified into two categories.

Category A: In the first category, the P2P overlay network is only used for control message propagation: Namely, search and response messages are propagated along paths in this overlay network. However, once the search results are available, real data transmission occurs directly between the peers on the underlying physical network, regardless of the overlay network. In this category, searching is the most important architectural issue. According to the different search mechanisms, we can further divide the distributed file-sharing systems in this category into three subtypes:

- **Centralized directory model**: This means that all the files or resources are indexed in a centralized server or a handful of centralized servers.
- **Fully decentralized model**: This means that all the directory services and resources are fully decentralized on every peer of the whole network. Distributed search algorithms often use flooding query method to look for file information.
- **Hybrid model**: This is the combination of the above two types. One implementation is to divide the peers in the network into several groups, and in each group, the node with good performance and high bandwidth will be selected as the directory server, which is typically called a supernode. It is responsible for the maintenance of the whole directory of the group and connects to other supernodes from the overlay network being used for searching.

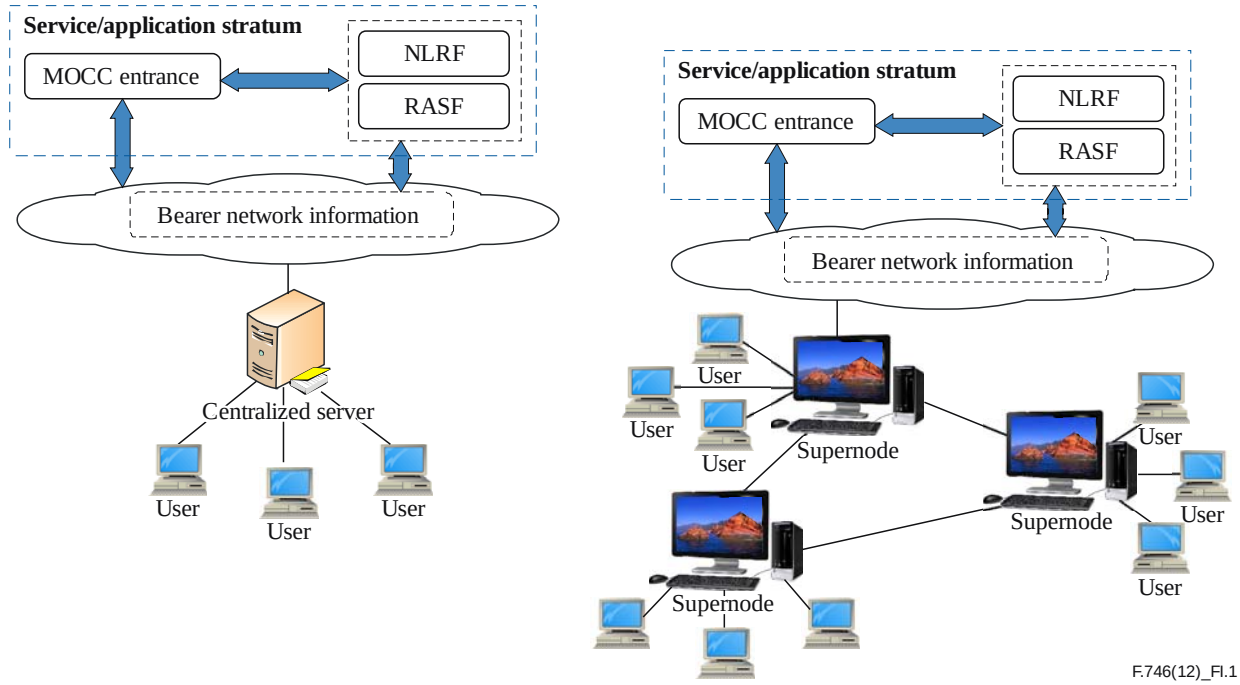
Category B: In the second category, the peers form a cooperative overlay network for data exchange. Data blocks are transmitted along paths in this overlay network.

On the application side, deployment of the MOCC functionalities may happen at different levels. For example, in a completely decentralized network, selection of the best sources is totally up to the user. In Category B P2P systems, central elements such as trackers or servers act as mediators. Therefore, in the former case, improvement would require modification in applications, while in the latter case, it could be implemented just in some central elements. The following clause presents and analyses the scenarios using the different file sharing system types.

I.1.2 Scenario 1: Centralized or hybrid model

Description: The scenario in Figure I.1 fits within either the centralized or the hybrid model, in which the centralized index server or the supernode can serve as mediator for the end users. User A wants to download a resource R. In this scenario, it assumes that the centralized server or the supernodes only provide the index service to the nodes, which won't provide any policies regarding the traffic optimization to the users.

Pre-condition: A number of copies of resource R are scattered in the network. In the centralized model, all the resources are indexed in the centralized server. In the hybrid model, the supernode indexes all the resources located in directly connected non-supernode peers. The centralized server or all the supernodes are authorized to use the MOCC service. NLRF and RASF have already been registered to the MOCC entrance component, which has created the corresponding records in turn.



(a) Centralized model (b) Hybrid model

Figure I.1 – File sharing systems scenario using MOCC service

In this scenario:

1) The centralized server or supernodes send the MOCC matching request to the MOCC entrance component, which includes the addresses of the centralized server or the supernodes. On receiving the requests, the MOCC entrance component will then authenticate them to identify if they are legal clients.

2) After the authentication, the MOCC entrance component will look up for the authorized MOCC servers (RASF, NLRF) for the centralized server or supernodes and then send the addresses and server information in the response messages to the centralized server or supernodes.

3) Upon receiving the messages, the server or the supernodes will cache those MOCC servers' information and then send the access request to the MOCC servers including their addresses and other authentication information until the authentication is succeeded.

4) A user sends a search request to a centralized index server or its responsible supernode, say S.

5) S executes the search (either searches a centralized database in case of the centralized model or initiates a search among the supernodes in the case of the hybrid model) and obtains the list of nodes that can satisfy the search request.

6) S sends the transport network statistics query request to NLRF or RASF including the list of nodes mentioned above as well as the requesting node.

7) NLFR or RASF ranks the list of nodes based on its knowledge of the carrier network status and returns the ranked list of nodes to S.

8) S can return the ranked list of nodes to the requesting user or, alternatively, can choose the top ranked K nodes to return to the user.

9) The user uses the ranked list of nodes to initiate the real file downloading. The user can request different ranges from different nodes to boost the downloading speed.

I.1.3 Scenario 2: Decentralized scenario

Description: The scenario in Figure I.2 illustrates the fully distributed file sharing system model, in which all resources are distributed in every peer of the whole network.

Pre-condition: A number of copies of resource are scattered in the network. There is no centralized indexing server to index the resources. User A wants to download a resource R. All or a part of the users are authorized to use the MOCC service. NLRF and RASF have already been registered to the MOCC entrance component, which has created the corresponding records in turn.

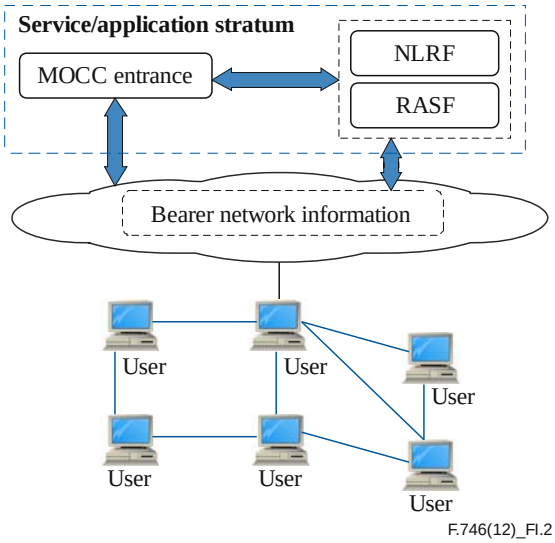


Figure I.2 – File sharing systems scenario using MOCC service in the fully distributed model

In this scenario:

1) The user sends the MOCC matching request to the MOCC entrance component, which includes its address, etc. On receiving the request, the MOCC entrance component will then authenticate the user to identify if they are legal clients.

2) After the authentication, the MOCC entrance component will look up for the authorized MOCC servers (RASF, NLRF) for the user, and then send the addresses and server information in the response messages to the user.

3) Upon receiving the messages, the user will cache those MOCC servers' information and then send the access request to the MOCC servers, which include its address and other authentication information until the authentication is succeeded.

4) The user initiates a search request to the system.

5) The system returns a list of nodes that can satisfy the search request to the user.

6) The user sends the transport network statistics query request to NLRF or RASF, including the list of nodes mentioned above.

7) NLRF or RASF ranks the list of nodes based on its knowledge of the carrier network status, and returns the ranked list of nodes to the user.

8) The user uses the ranked list of nodes to initiate the real file downloading. The user can request different ranges from different nodes to accelerate the downloading speed.

I.1.4 Scenario 3: P2P with real data exchange among peers

Description: The scenario in Figure I.3 illustrates file downloading in P2P system with data exchange among peers. User 1 is looking for the "seed" for a particular movie in this kind of P2P network. Trackers 1 and 2 are connected to the MOCC service. Since the algorithms and mechanisms vary in different kinds of hybrid file sharing systems, the tracker capabilities in those systems are diversified. This scenario assumes that Trackers 1 and 2 only provide the collection and index services to the nodes, which will not provide any policies regarding the traffic optimization to the users.

Pre-condition: The "seed" (.torrent) file has been already published and the file information has been registered in Trackers 1 and 2. Trackers 1 and 2 are responsible for the maintenance of status of all the peers in its group and nodes-selection of the given resources. All the trackers in Category B P2P system are authorized to use the MOCC service. NLRF and RASF have already registered with the MOCC entrance component, which has in turn created the corresponding records. Trackers 1 and 2 are authorized to use the MOCC services to optimize their node selection.

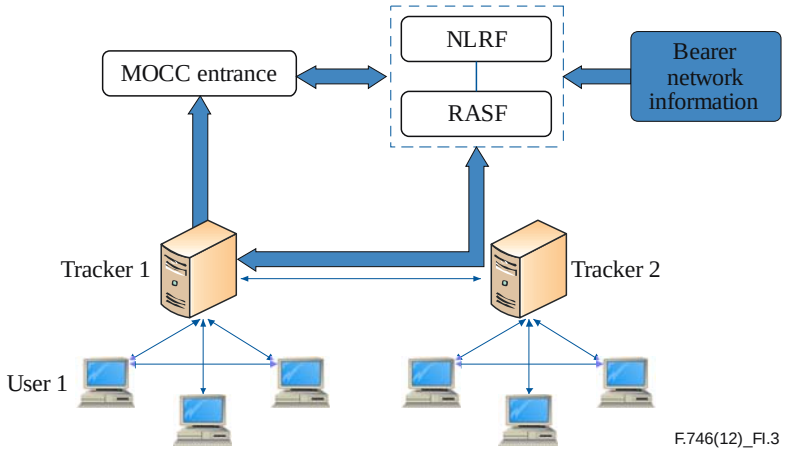


Figure I.3 – File sharing application optimization scenario using MOCC services

In this scenario:

1) Trackers 1 and 2 send the MOCC matching request to the MOCC entrance component, which includes the Tracker ID, addresses, etc. On receiving the requests, the MOCC entrance component will try to authenticate those trackers to identify if they are legal clients.

2) After the authentication, the MOCC entrance component will look up for the authorized MOCC servers (RASF, NLRF) for those trackers, and then send the addresses and server information in the response messages to the trackers.

3) Upon receiving the messages, Tracker 1 and 2 will cache that MOCC server information and then send an access request to the MOCC servers until the authentication is successful. The access request includes tracker ID, address and other authentication information.

4) User 1 gets one "seed" (.torrent) of the movie, which includes the available tracker information. User 1 sends the connect attempts to those trackers on the list one by one until one successful connection has been established between it and a tracker, say Tracker 1.

5) Corresponding to the given movie, Tracker 1 retrieves a huge list of candidate peers, which are recorded storing one or more replicas. In the normal Category B P2P operation, the tracker will send the list to User 1, who will then randomly choose some of the candidate peers. However, with the aid of the MOCC server, that selection can be optimized.

6) Tracker 1 will send the transport network statistics query request, which includes the information of those candidate peers. The type of request can be one or a combination of: network location query request, network distance query request and network resources status query request. Those requests are preceded by NLRF and RASF, respectively.

7) According to the different query requests, NLRF and RASF will then inquire about the bearer network information services, which can be implemented by the MOCC itself or can be provided by some practical entities such as RACF. In some cases, within certain policy boundaries, network information services can be provided by the network operators.

8) MOCC servers send the results to the trackers to initiate the node selection optimization.

9) The tracker sends the optimized node list to User 1.

10) User 1 will send a TCP connect request to the nodes on the list. After successful connections have been established, a handshake procedure will be performed among those peers. After that, those peers use "interested", "not interested", "choke", "unchoke" to exchange the attitude of resource sharing.

11) The Category B P2P file transfer begins.

12) The TCP connections tear down among the peers after the file has been fully downloaded.

I.2 MOCC deployment in the streaming services systems

I.2.1 General description

The conventional centralized client/server-based streaming media system has some inherent limitations that make it impossible to be widely deployed, such as server performance bottleneck and single point of failure. Comparing to the client/server-based system, streaming media systems based on distributed content delivery networks can somehow improve the service capability. However, there are still issues (such as expensive hardware deployment, high bandwidth cost and complicated device management and scalability) that add to the complexity and cost of implementations.

Another radical way to improve the scalability of the streaming services is based on P2P technology. However, systems based on P2P-based streaming services cannot guarantee user experience. Factors include long start-time, topology inconsistency, instability induced by fast user turn-over ("churn") and NAT-deployment issues.

The deployment of MOCC in P2P networks is to some extent helpful for solving those inherent problems. For example, RASF can record every resource contained by the node and NLRF can give the location information about the resource requested by any node.

I.2.2 Scenario for P2P streaming media systems

P2P file sharing systems have become common in the Internet. P2P technologies bring revolutionary changes to the network content distribution model and make it possible that the comprehensive streaming media applications become practical in the Internet.

P2P streaming media systems use P2P technologies to alleviate the server load and optimize the service capability. Based on the type of data distribution method, most of the P2P streaming systems can be classified into two subtypes:

– **Tree-based system**: This kind of P2P streaming system implements a tree-based content distribution, and the tree is in the application layer and rooted at the content sources. In principle, each node receives data from a parent node, which might be the source or a peer. If peers do not change frequently, then the systems require little message overhead since the packets are forwarded from node to node without the need for extra messages. However, in high-churn environments (i.e., fast turnover of peers in the tree), the tree must be continuously destroyed and rebuilt, which produces considerable control message overhead.

– **Mesh-based system**: In this kind of P2P streaming system, each node contacts a subset of peers to obtain a number of chunks. Every node needs to know which chunks are owned by its peers and explicitly "pulls" the chunks it needs. This type of scheme involves overhead, due in part to the exchange of buffer maps between nodes (i.e., nodes advertise the set of chunks they have) and in part to the "pull" process (i.e., each node sends a request to receive the chunks). Each node relies on multiple peers to retrieve content and as a consequence mesh-based systems offer good resilience to node failure.

Both tree-based and mesh-based systems have advantages in particular scenarios, but neither can completely overcome the challenges of the dynamic peer-to-peer environments. A strong advantage for mesh-based systems is their simplicity, but they have a trade-off between overhead and latency: if nodes choose to send notifications upon every segment arrival, then the overhead will increase; on the other hand, periodic notifications containing buffer maps reduce the overhead but increase latency. A tree-based system does not suffer from this trade-off, but has to face the inherent instability of dynamic environments and bandwidth underutilization.

The deployment of MOCC in P2P streaming media systems can make the node acquire the information about the overlay network and its neighbours, which is useful to determine the status of the network and the correlative peers so as to make the right data schedule and relationship selection.

I.2.2.1 Scenario for tree-based systems

Tree-based systems have well-organized overlay structures (typically trees) for delivering data, with each data packet being disseminated using the same structure. Nodes on the structure have well-defined relationships, such as "parent-child" relationships in trees. Tree-based systems are typically push-based, i.e., when a node receives a data packet, it also forwards the copies of the packet to each of its children. Since all data packets follow this structure, it becomes critical to ensure that the structure is optimized to offer good performance to all receivers. Furthermore, the structure must be well-maintained, as nodes randomly join and leave the group. In particular, if a node crashes or otherwise stops performing adequately, all of its children in the tree will stop receiving packets, and the tree must be repaired. In addition, loop avoidance is an important issue that must be addressed when constructing tree-based structures in the streaming services system.

Description: The scenario in Figure I.4 illustrates a tree-based system in which there is an application layer streaming tree with ten peers. In this scenario, it assumes that there are two peers at level 1 and receiving video directly from the server, four peers at level 2 receive video from their parents at level 1, and three of them forward received video to four peers at the bottom level.

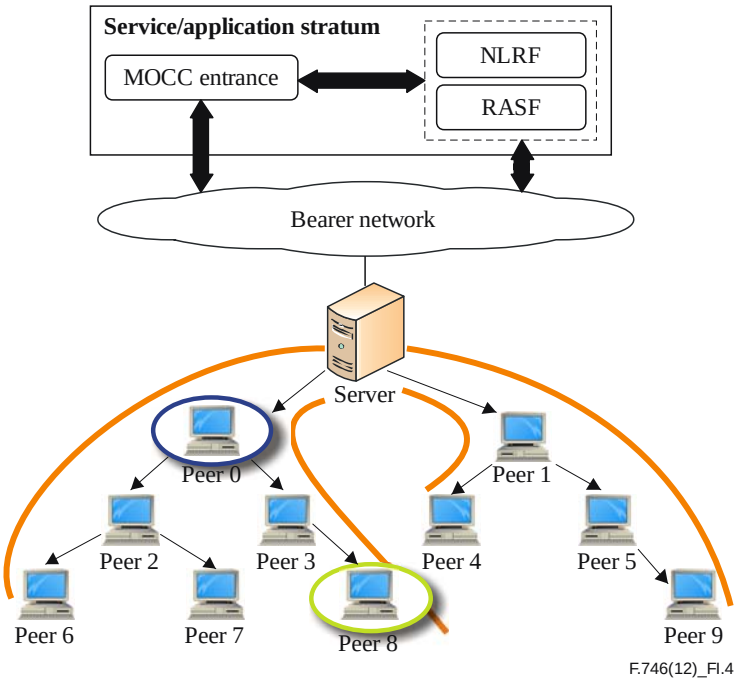


Figure I.4 – Tree-based system scenario using MOCC service with a single application layer multicast tree

Pre-condition: The video files are sent along the established tree for the server to the last level peer. In this scenario, every peer will periodically send its overlay information to RASF, which includes next level peers, upper level peers, multicast tree ID, upload and download bandwidth, level ID, etc. The server or all the tree member peers are authorized to use the MOCC service. NLRF and RASF have already been registered to the MOCC entrance component, which has created the corresponding records in turn.

In this scenario:

– The MOCC servers are distributed in the network; therefore, each node who wants to use the MOCC functions should get access to the corresponding ones for the topologies information querying.

– Together with the server, users belonging to the same session form an application-level multicast tree which is called a base tree, and the whole video file contained by the server is called a base stream. The members of the base tree periodically send the necessary information to MOCC entities, such as its parent and children, bandwidth, base stream information, etc. to renew the topology-related information for each one. When a new client wants to join the tree, for example, Peer 8, it will query the MOCC servers on the most suitable tree member (using some parent selection algorithm), and then it will join this tree.

– Furthermore, if e.g., Peer 0 wants to leave the tree, it can send notification to the MOCC servers, in turn, the MOCC entities will notify Peer 0's parent and children and start to direct the repair for the tree.

I.2.2.2 Scenario for mesh-based systems

In a mesh-based P2P streaming system as illustrated in Figure I.5, peers are not confined to a comparative static topology. Instead, the peer relationships are established or terminated based on the content availability and bandwidth availability on peers. In the mesh-based structure, peers will dynamically connect to a subset of random peers in the system and will periodically exchange information about their data availability. Video content is pulled by a peer from its neighbours who have already obtained the content. Since multiple neighbours are maintained at any given moment,

mesh-based video streaming systems are highly robust to peer churns. However, users may suffer from video playback quality degradation ranging from low video bit rates, long start-up delays, to frequent playback freezes because different data packets may traverse different routes to reach the users (this will also make it difficult to predict the variation of dynamic peer relationships).

Description: Similar to P2P file sharing systems like Category B P2P, a mesh streaming system has a tracker to keep track of the active peers in the video session. Trackers 1 and 2 are all connected to the MOCC service. In this scenario, Trackers 1 and 2 provide index service for peers.

Pre-condition: The video file has been already published and the file information has been registered in Trackers 1 and 2. Trackers 1 and 2 are responsible for the track of status of all the peers in its group and nodes-selection of the given resources. All the trackers in this system are authorized to use the MOCC service. NLRF and RASF have already registered to the MOCC entrance component, which have created the corresponding records in turn. Trackers 1 and 2 are authorized to use the MOCC services to optimize their nodes selection.

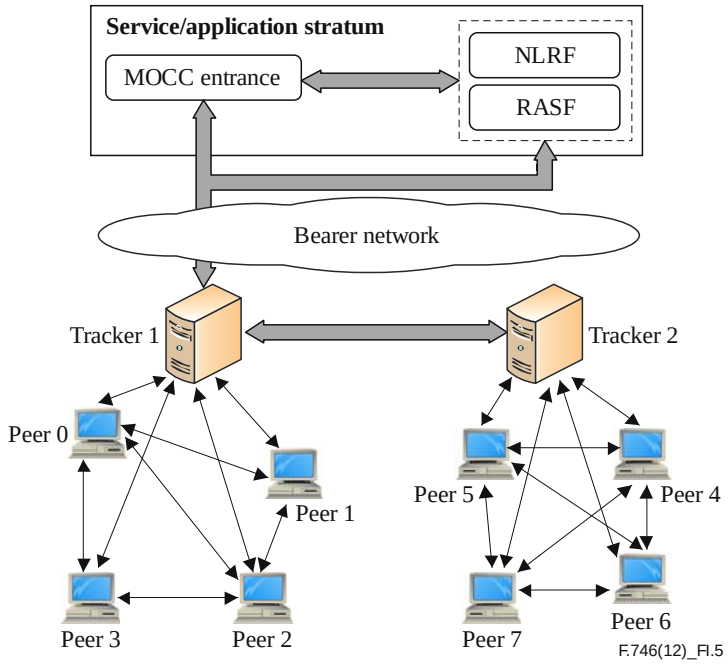


Figure I.5 – Scenario of the mesh-based system using MOCC service

In this scenario:

– The MOCC servers are distributed in the network; therefore, each tracker who wants to use the MOCC functions should get access to the corresponding ones for the topologies information querying.

– When one peer (for example Peer 3) joins the streaming session, Tracker 1 can query the network statistics information from the MOCC servers, which can be one or a combination of: network locations, network distance, network resources status query, etc. Tracker 1 then accordingly makes optimized active peers selections with the aid of the topologies information NLRF & RASF have been provided. After receiving an initial list of active peers, Peer 3 tries to make connections to some remote peers on the list and, after obtaining enough neighbours, Peer 3 will then start to exchange video content with its neighbours.

I.3 MOCC deployment in NAT traversal and media relay

I.3.1 General description

Many real-time communication services are using the distributed model, which can allow the users to establish direct media flows such as video, audio, text, etc. Unlike the client-server model, every host in a P2P network can act at the same time as server and client, and its peers are more or less equal. Therefore, the main problem for P2P applications in a NAT environment is that NATed peers are usually not reachable for arbitrary peers. Unsolicited connection requests from outside are denied by the NAT device because the requests are sent to the public internet address of the gateway and the NAT device has no clue to which internal address the request should be forwarded.

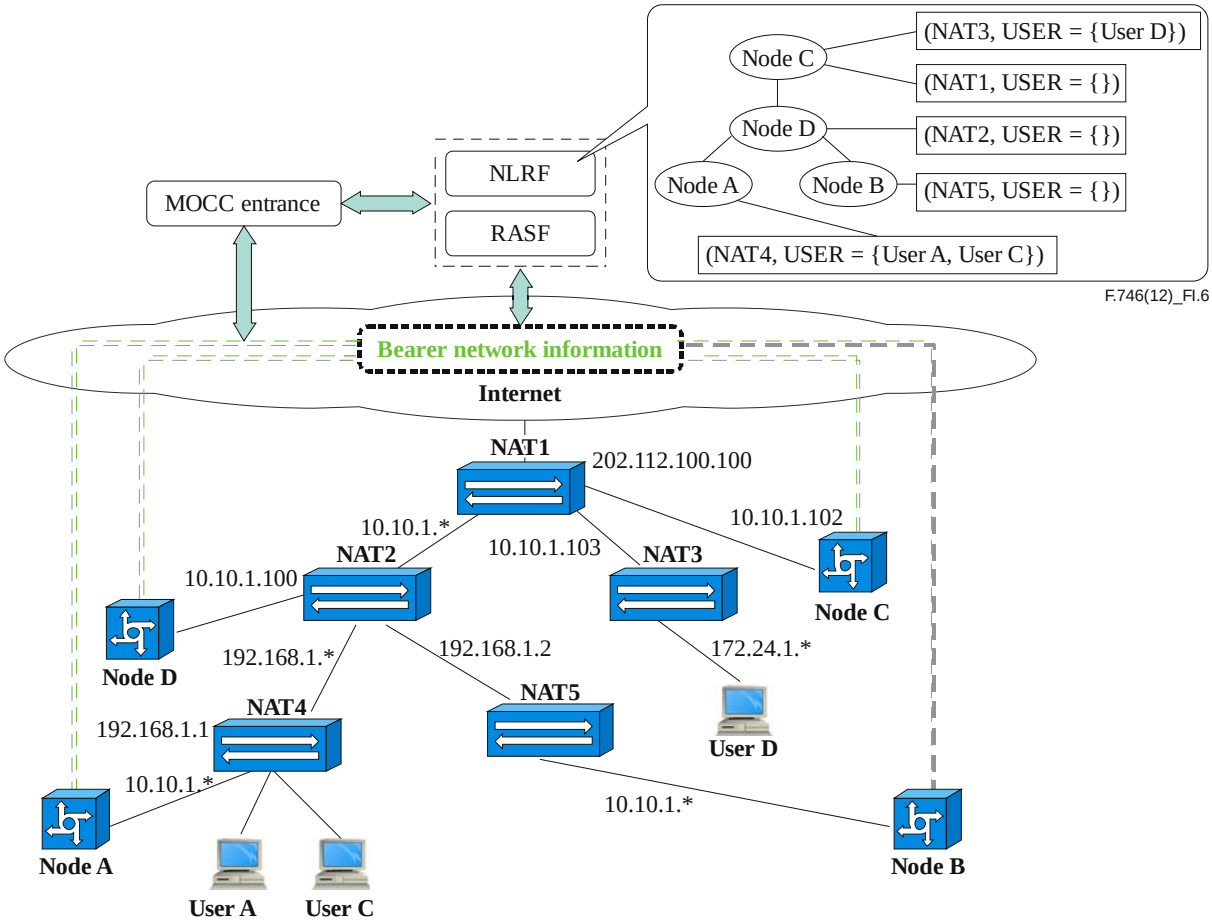


Figure I.6 – Illustration of MOCC deployed in the hierarchical NATed environment

On the other hand, the peer-selecting methods in some P2P algorithms are somewhat random, which does not take the topology issues into consideration. This is especially the case when there are many NAT devices in the network and it is hard to get accurate estimation of those NATed peers connected to the Internet. Therefore, it might happen that in some systems the traffic is iteratively routed or takes a detour in case of the same-root NAT.

In a general sense, the network resource controlled by one single NAT is within the boundary from its internal interface to the external interface of the lower-level NAT connected to it. There are no other NAT devices within this area, which is defined as the current network in this Recommendation. Regarding one NAT, the upper-level network, current network and lower-level network can be regarded as the directed edges, which compose the topology of the multi-level NATs deployment in a network. The NAT device whose external interface was configured with the global unique public address is called the root NAT (NAT1) as shown in Figure I.6. Along the edge, if there is one path from NAT1 to NAT2, then NAT1 can be called the same-root upper level NAT

of NAT2; and meanwhile if there is another path from NAT1 to NAT3, then NAT2 and NAT3 are called same-root NAT to one another.

According to the ownership of the NAT devices, the same-root NAT scenario can be divided into the following three categories:

Scenario 1: In this scenario, all the NAT devices are deployed and maintained by the network operators, and the end users are not allowed to connect their own NATs to the network. One example of this scenario is the enterprise network.

Scenario 2: In this scenario, there is one or more same-root NAT deployed, among which the lowest-level NATs are deployed by some users at liberty. This is very common in the campus network or public internet.

Scenario 3: This scenario can be found in some broadband access provider network. There are some third-party NAT devices deployed in the operators' network, by which it can provide the access services to the end-users. In this scenario, users can deploy their own NAT devices as well.

This clause discusses the above three scenarios respectively, which is illustrated with the example of the P2P VoIP system.

The network deployment information collected by MOCC can provide assistance to solve this problem. For example, the address-related information of NAT can be used to implement the NAT traversal. On the other hand, to enhance the performance, it can help to find the best relay path, such as by minimizing the NATs in the path or discovering the same-root NATs.

I.3.2 Scenario 1: Unified NAT deployment by the network operators

Description: The scenario in Figure I.7 illustrates the deployment of MOCC functionalities into one P2P VoIP system. In this scenario, User D wishes to establish a call with User A. MOCC functionalities have been deployed into this system.

Pre-condition: The P2P nodes in this system are authorized to use the MOCC service. NLRF and RASF have already registered to the MOCC entrance component, which has created the corresponding records in turn. User A and User D are registered to its corresponding bootstrapping servers.

In this scenario:

1) User D wants to establish a call with User A. First, it will send the location query request to its service node to acquire the address of User A.
2) According to the UserID carried in the request message, the service node will then retrieve the IP address and NodeID of User A. The service node will then send the response message to User D, which includes the necessary information of User A.
3) User D sends the session initiate request to the service node, which carries the address of User A.
4) The simplest way for the service node to process this request is to choose some nodes along the path from User D to User A for the media relay. One possible path may be User D → Node C → Node D → User A. However, with the aid of the MOCC server, that selection can be optimized.
5) The service node will send the network topology query request to the NLRF, which includes the information of those candidate nodes.
6) NLRF will then inquire about the bearer network information services, which can be implemented by the MOCC itself or be provided by some practical entities such as RACF, or in some cases, within certain policy boundaries, those information services can be provided by the network operators, and then send the result to the service node.

7) From the topology information, it was found that Node A and User A are under the same NAT, therefore the path can be established from User D → Node A → User A.

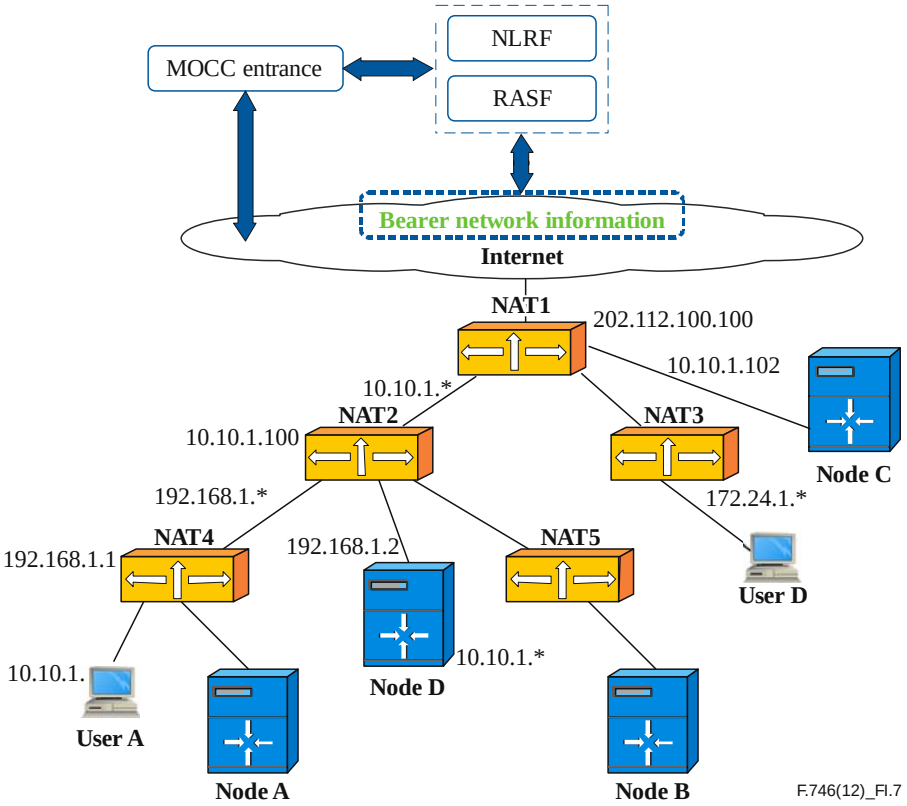


Figure I.7 – Scenario of P2P Application NAT traversal using MOCC service

I.3.3 Scenario 2: The lowest-level NATs are connected and owned by the users

Description: The scenario in Figure I.8 illustrates the deployment of MOCC functionalities in a P2P VoIP system. MOCC functionalities have been deployed into this system. NAT-U1/U2/U3/U4 are owned and connected by the end-users, which remain unknown to the network operators.

Pre-condition: The P2P nodes in this system are authorized to use the MOCC service. NLRF and RASF have already registered to the MOCC entrance component, which have created the corresponding records in turn. All the users are registered to its corresponding bootstrapping servers.

In this scenario:

1) The bootstrapping server is deployed in each level of this NAT topology, from the root NAT to the operator's lowest-level NATs, to which the user-owned NAT are connected. In this way, the NLRF can collect all the topology information of the end users.

2) User A, User C and User D send the register request to the bootstrapping server in the current network of NAT2.

3) Upon receiving those messages, the bootstrapping server will compare the address information carried in the IP headers and message payloads. If the information doesn't match, then it will determine that those users are behind the unknown NAT devices. And meanwhile it will store the address mapping information and send the message upwards level by level, until it reached the bootstrapping server in the public network.

4) According to the topology information stored in each bootstrapping server, the topology view will be computed and generated by the NLRF component.

5) User C wants to establish a call with User A. First, it will send the location query request to its service node to acquire the address of User A.

6) The service node will send the network topology query request to the NLRF, which includes the information of User A and User C.

7) NLRF will then query the bearer network information services, from the topology information. If it is found that User A and User C are under the same NAT, Node A can be selected as the optimum service node to assist the communication between User A and User C.

8) After the path optimization, the media can be established from User A to User C.

9) In this way, the unwanted traffic in the P2P system can be reduced, and the resources of the corresponding service node can be optimized as well.

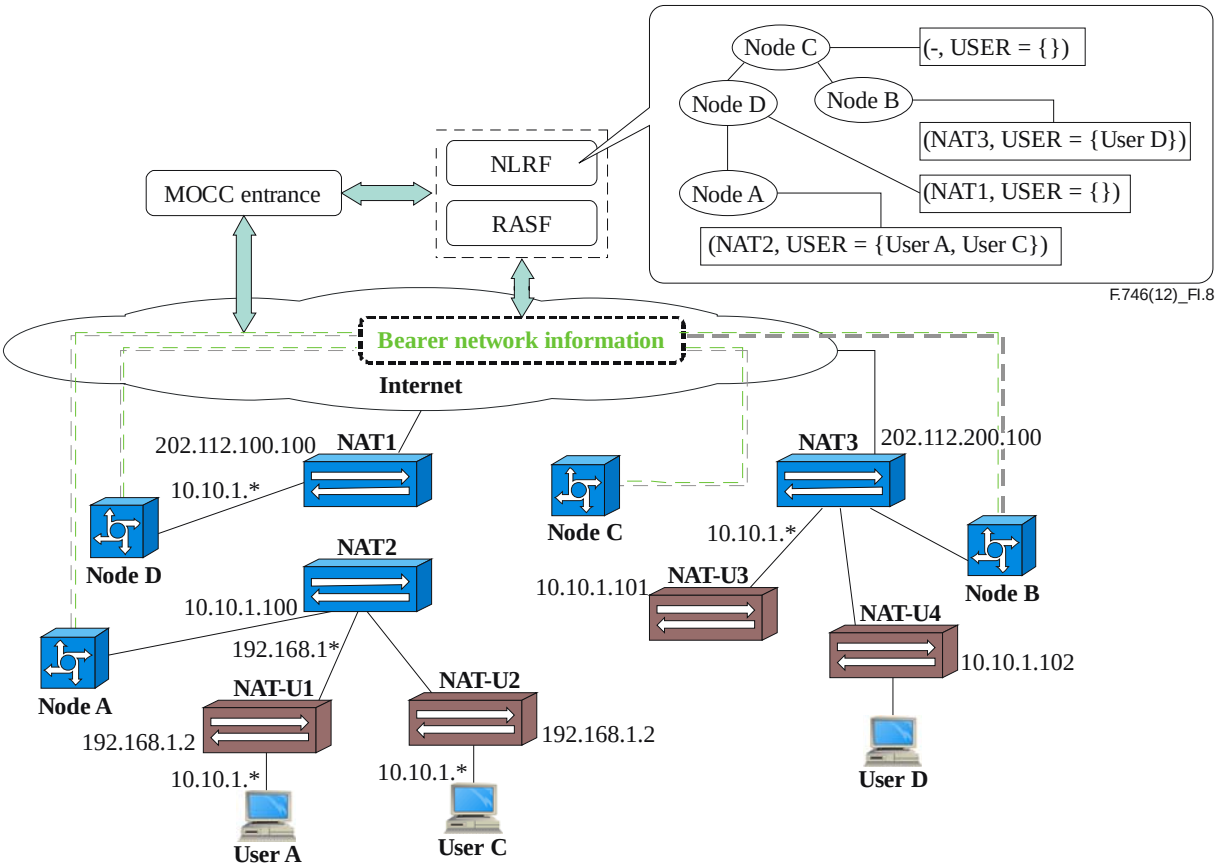


Figure I.8 – The lowest-level NATs are connected and owned by the users

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	**Non-telephone telecommunication services**
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013