TECHNICAL REPORT

ISO/IEC TR 20002

First edition
2013-12-01

Information technology — Telecommunications and information exchange between systems — Managed P2P: Framework

Technologies de l'information — Télécommunications et échange d'informations entre systèmes — Réseaux pair-à-pair géré: Cadre général

Reference number
ISO/IEC TR 20002:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 20002 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems.*

Introduction

Peer-to-Peer (P2P) is distributed network architecture composed of participants (peer) sharing resources without intervention from the central coordination instances. Due to the advantages of scalability and performance, P2P has emerged as viable service architecture for the large-scale Internet applications such as file distribution, multimedia streaming, etc. By combining the resources of each user devices, P2P network can be automatically self-organized and be adapted to changes in peer populations while providing stable services for content sharing and personal communications. However, the unmanaged characteristics of P2P have caused various technical and social problems such as inefficient use of network, copyright issue, etc.

This technical report suggests approaches to solve such problems by defining manageability and enhanced capability to the P2P through the definition of managed P2P (MP2P). This technical report identifies problems of the P2P, identifies requirements for MP2P, and provides framework for MP2P.

Information technology — Telecommunications and information exchange between systems — Managed P2P: Framework

1 Scope

This Technical Report:

— classifies problems of P2P networking;

— defines taxonomy and concept of managed P2P;

— specifies requirements to support managed P2P;

— specifies framework for managed P2P;

— specifies information flows to support various features of managed P2P.

This Technical Report does not define new P2P protocol or P2P-based applications. This Technical Report does not define manageability features for interoperation with conventional P2P-based applications. The goal of this Technical Report is to define a framework to provide manageability to the conventional P2P-based application.

2 Normative references

None.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
Managed Peer-to-Peer (MP2P)
P2P with manageability features to manage the P2P-based service and P2P network by the P2P participants such as P2P service provider, ISP, and peer

3.2
P2P Service Provider (P2PSP)
service provider providing a P2P-based service

3.3
Peer
equally privileged participant in the P2P network which has the capability to share its resources with other participants

3.4
Peer-to-peer (P2P) networking
distributed networking composed of peers that share portion of the resources to be available to other peers

3.5
Content Fragment
data unit in a content that is exchanged among peers in the P2P network. Content fragment can also be a unit stored in the peer

3.6
Relay Peer
peer relaying data for other peer(s)

3.7
Contributing Peer
peer providing resources to other peer(s)

3.8
Consuming Peer
peer consuming resources from other peer(s)

3.9
Super Peer
peer providing distributed control over P2P network. In general, it has powerful resources compared to other types of peers in the P2P network and is connected to the public network

4 Symbols (and abbreviated terms)

The following acronyms are used in this document.

ALTO	Application-Layer Traffic Optimization
CAN	Content Addressable Network
CAPEX	Capital Expenditure
DHT	Distributed Hash Table
ICE	Interactive Connectivity Establishment
IETF	Internet Expert Task Force
ISP	Internet Service Provider
MP2P	Managed Peer-to-Peer
NAT	Network Address Translation
P2P	Peer-to-Peer
P2PSP	Peer-to-Peer Service Provider
STUN	Session Traversal Utilities for NAT
TURN	Traversal Using Relays around NAT
UPnP	Universal Plug and Play

5 Concept of Peer-to-Peer networking

A peer-to-peer (P2P) networking is a distributed networking that is composed of large number of individual participants (called peers) that make a portion of their resources (such as processing power, disk storage or network bandwidth) directly available to other participants in the P2P network, without the need of the central coordination instances (such as servers or stable hosts). As opposed to traditional client-server architecture, peers in the P2P networking have equal roles and act as a resource provider and a resource consumer. P2P networking protocol provides a method for any two peers to communicate with one another. P2P network is self-organized and is capable of adapting to failures and accommodates transient population of peers, while maintaining acceptable connectivity and performance without requiring intermediation or support from a centralized server or authority. P2P networking is highly distributed, highly scalable, and highly autonomous to large numbers of peers. These characteristics shows advantages in services such as file-sharing, distributed computing, and media streaming.

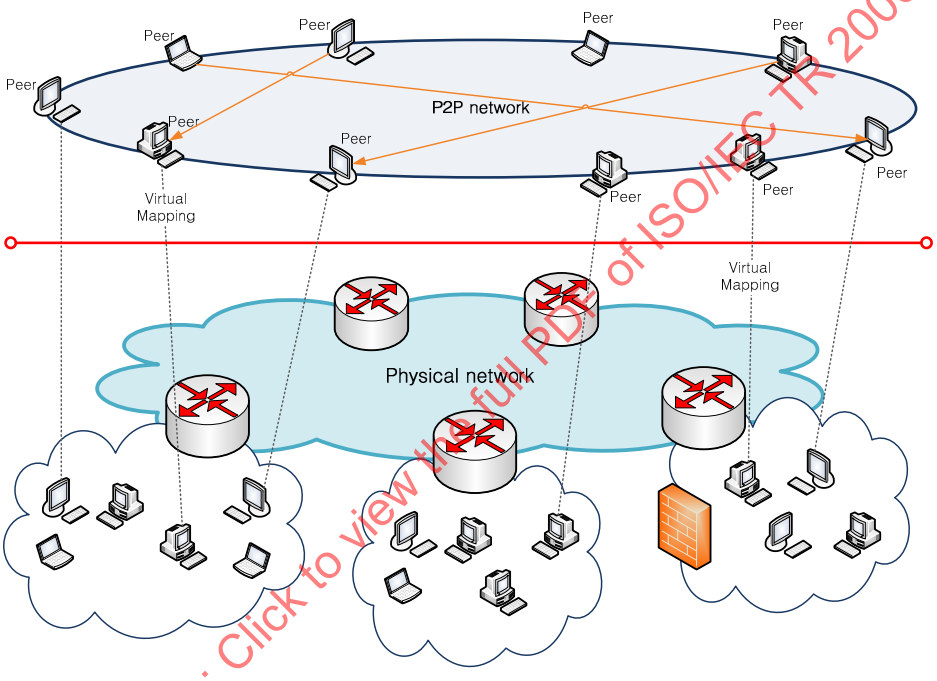

Figure 1 — P2P network

Figure 1 shows a P2P network in which the peers form an overlay network on top of the underlying physical network. The application level routing is used to route data for P2P-based service. The architecture of P2P network allows peers to create new service or application without the intervention from the network infrastructure or central instance.

The peer-to-peer network should not be confused with concept of ad-hoc network, which is a self-configuring infrastructureless network of mobile devices connected by wireless links. Ad-hoc networking involves wireless devices to discover each other within the wireless range and to communicate in peer-to-peer fashion without involving central access points. The P2P network is an application-level overlay network which is independent of the underlying physical network, wired or wireless. The ad-hoc network is out of scope of this document.

5.1 Characteristics of P2P network

This clause describes the characteristics of P2P network.

5.1.1 Distributed resource sharing

P2P architecture is different from the client-server architecture in which the contents or resources are provided by single or small group of server. P2P allows peer to share its resources which includes contents, computing power, connectivity, etc. Peers can participate in content dissemination or distributed computing such as SETI@home. Shared resources are distributed across the network which enables peers to easily utilize the resources.

In P2P, a single peer conducts both client function and server function. It acquires needed resource from multiple peers through client function. It shares its resource with multiple peers through server function.

Since the resource can be found in multiple peers, it is resilient to failure as compared to the server-based architecture. The distributed resources enable distributed parallel processing which leads to increase in throughputs and performances.

5.1.2 Content-based routing

Content-based routing can be realized in the P2P networking, since the target of routing is content or resource not the physical address of the source.

5.1.3 Self-organization and dynamic adaptation

The P2P network is a self-organized network configured by the participating peers without any intervention from the centralized server or authority. The peers participating in the P2P network join and leave the P2P network dynamically. Thus, P2P network enables peer to find other contributing peer when the previous contributing peer abruptly leaves the P2P network. Each node in the P2P network is reorganized autonomously to accomplish dynamic adaptation. Self-organization is realized through this dynamic adaptation feature.

5.1.4 Scalability

P2P network is composed of various types of network devices and accommodates large number of peers without significant decrease in overall performance. In general, the performance of P2P network tends to increase which is proportional to the number of participating peers.

5.1.5 Load distribution

P2P network can provide load distribution through partition tasks or workloads among peers. P2P network shows excellent performance in distributing contents of large volume to large number of peers with much less load concentration compared to client-server system. Contents provider can distribute contents to large number of receivers by providing contents to only a small number of peers in the P2P network. The contents are propagated to rest of the peers over the P2P network.

5.2 Classification of P2P network

5.2.1 Structured P2P network

Structured P2P network, e.g. Tapestry, Chord, CAN, and Kademlia, organizes P2P network according to the predefined structure such as ring topology or two-dimensional coordinate. In order to position peer in appropriate place on the P2P network with the predefined structure, peer uses algorithm based on the distributed hash table (DHT). By use of DHT, the configured P2P network can be optimized in terms of searching and retrieving contents. Although structured P2P network can provide efficient searching and retrieving content, DHT requires global consistency among peers.

5.2.2 Unstructured P2P network

In unstructured P2P network, peers use different algorithm to configure P2P networks. Instead of being configured in the predefined structure, the unstructured P2P network is shaped in varied format according to the peer's activities. The unstructured P2P network is categorized according to the existence of the central server which is as follows.

— Pure P2P network: In pure P2P network such as the early version of Gnutella and Freenet, P2P network consists of peers only. Since there is no central server, peer uses flooding mechanism to acquire contents by sending query messages to all neighbouring peers. Peer with the requested content responds with information for the consuming peer to initiate service connection. Absence of central server helps to prevent the single point of failure but the use of flooding mechanism can impose excessive overhead to the P2P network.

— Centralized P2P network: Centralized P2P network such as Napster, BitTorrent uses a central server to maintain the information of the P2P networks and the information of the participating peers. Peer connects to the central server in order to get the information of the P2P network, especially information of the peers participating in the P2P network. However, the contents itself are directly retrieved from peers participating in the same P2P network. The use of central server can increase manageability of the P2P network or P2P-based service, but it may incur scalability problem and single-point-of-failure issue.

— Hybrid P2P network: In order to overcome problems of the prior two systems, hybrid P2P network, e.g. KaZaA and Skype, exploits a new type of peer called super peer. The central server may not be used in the hybrid P2P network or may be used with minimal functions such as for authentication. Super peers conduct functions for the P2P network on behalf of the central server. Peer may connect to the central server and gets the information of the existing super peers. Then peer connects to super peers to get the list of neighbouring peers or to query contents information. The super peer communicates with other super peers in order to exchange information of peers and resources. The super peer can relay the request to other super peers, if it cannot provide the requested information.

5.2.3 Mapping of contents with P2P network

A P2P network can constructed for a single content or multiple contents. The features and characteristics for each type are as follows.

— Single content on a P2P network: In this relationship, single P2P network is configured for a single content. This type of P2P network does not need to provide content searching because it is configured only for one content. The peer needs to access a separate index server, such as web-based bulletin board, to acquire information of the P2P networks and the metadata of the contents. Based on the acquired information, peers can participate in the P2P network and receive the desired content. BitTorrent is one example for this type of P2P network.

— Multiple contents a P2P network: In this relationship, single P2P network is organized for multiple contents. Peer needs to join the P2P network with the initiation of the P2P-based service. Peer queries to search for content in the P2P network. The peers with the queried contents respond to the querying peer. Consuming peer makes a peer list consisting of contributing peers which can respond to the query. eDonkey is one example for this type of P2P network.

6 Problem statement

Even though P2P networking has various advantages such as high scalability and high throughput, it incurs various problems as well. This clause lists problems caused by P2P networking.

6.1 Problems in the network-side

6.1.1 Disregarding underlying networks

P2P networking does not consider the status of the underlying network in the process of the peer selection. Selected peer has small possibility of being the most appropriate peer from the underlying network perspective. This leads to inefficiency in P2P network. In addition to inefficient use of the network, P2P networking may incur inter-ISP traffic which imposes monetary cost on ISP.

6.1.2 Load concentration on specific peers/networks

In P2P network, resources are not evenly distributed throughout the network which can result in network load concentration on specific peer or specific part of the network. Network status changes frequently from extreme peer dynamics and flash crowd. Unpredictable behavior of peers makes it impossible to predict traffic flows.

6.2 Problems in the service-side

6.2.1 High churn

Peers can join or leave P2P network any time during the service. This dynamic behavior called peer churn may lead to instability of P2P networks and the P2P based services. If the churn rate is too high, P2P based service may suffer from service discontinuity. This indicates that the extreme peer dynamics and flash crowd results in lack of service reliability and robustness.

6.2.2 Illegal distribution of content

P2P network does not have method to prevent illegal distribution of contents. Copyright protection is one of the serious issues in P2P based service.

6.2.3 Absence of distribution control

P2P network is a receiver-oriented system, which the content distribution is controlled by the receiver. P2P network lacks feature for the contents provider to control the distribution. The peer providing contents may want to manage the distributing area (serving region or consuming peers) or to receive report from the consuming peer.

6.3 Problems in the user-side

6.3.1 Absence of authentication

There is lack of verification feature in the P2P system. The participants of P2P network can be peers who are neither verified nor authenticated. It is hard to guarantee the reliability of the contents received from peers, because it may contain viruses, worms, Trojan horses, malware, spyware, etc. There is no adequate penalty to the peers for committing such malicious acts. Also, there is no protection scheme for the innocent victims.

6.3.2 Fairness and differentiation

P2P network is based on voluntary resource sharing among peers. This leads to selfish participants who receive resources from other peers but intentionally do not share its resources. For effective P2P-based service, it is important for the peers to share their resources. An adequate mechanism is needed to prevent or to reduce intentional selfish participants. In order to provide fairness in terms of traffic among peers, P2P networks have their own mechanism, e.g. optimistic unchoking and tit-for-tat, for fairness. However, those mechanisms do not consider network capability of each peer but only reflect the amount of data sent and received. Thus, peers with poor uplink capability cannot receive adequate service even if those peers are not intentional selfish participants. In addition to fairness, appropriate incentive mechanism is needed to provide differentiated service based on peer contribution.

7 Requirements of Managed P2P

Managed P2P (MP2P) is a P2P with manageability features to manage the P2P-based service and P2P network by the participants such as P2PSP, ISP, and peer. It is possible to resolve or reduce various problems of the P2P and to provide new features to enhance P2P-based services through managed P2P. This clause defines requirements of the MP2P. The requirements should be understood with the following conventions.

— The keywords “is required to” indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

— The keywords “is recommended” indicate a requirement which is recommended but which is not absolutely required. This requirement need not be present to claim conformance.

— The keywords “can optionally” indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor’s implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

7.1 Traffic Management

P2P networking constructs P2P network to directly share data among peers without considering the status of the underlying network. P2P traffic without considering underlying network status can cause congestion in the network which leads to degradation of network performance. It is hard to control the P2P traffic directly because the P2P traffics are directly exchanged among peers.

Therefore, if the ISP can provide information of the underlying network to P2P-based application, it is beneficial for both the user and the ISP. This means that the user can experience better service quality compared to the P2P networking not considering the underlying network, and ISP can be relieved from the unnecessary traffic load created by the P2P-based applications.

Prior to P2P traffic control, measuring network traffic should be preceded. The traffic status can be measured through cooperation among ISP, peer, and P2PSP.

P2P networking can provide NAT/Firewall traversal functionalities using a special relay peer such as super peer or relay server. By the use of the relay peer, P2P-based application can control traffic congestion in the application level. Congestion control in the network level is attained by queuing and re-routing traffics in the IP routers. The peer application directly performs P2P traffic control, and it is possible to actively control P2P traffic through cooperation among participating P2P entities.

7.1.1 P2P Traffic Measurement

It is important to recognize the traffic status of P2P network. However, it is impossible to fully comprehend the whole status of P2P network. In the MP2P, each peer should report its traffic status information to the P2PSP, and P2PSP and ISP should cooperate to distribute traffic to perform traffic localization. In the status report, peer can include its network status, preference, and the other characteristics. P2PSP can manage the P2P network based on the information gathered from peer and the ISP.

Network measurement can be divided into active measurement and passive measurement. Active measurement is achieved through probing the network by generating artificial traffic or through observing the network as an active participant. Passive measurement is achieved through monitoring of the network as an observer.

All data stream in P2P network is transmitted directly among peers, so it is useless to perform traffic measurement in the P2PSP. However, P2PSP can use the traffic status information gathered from ISP and peers for managing the P2P network.

In the IETF ALT, ISP, third parties, and user communities participate in measuring the network traffic. ISP can easily measure the traffic based on the information of the network. Third party can collect the information of network independently from the ISP and can be a substitute to the role of ISP in delivering the network information to P2PSP. User communities applies distributed algorithm to analyse the topology of the network.

Req-Traffic-010: P2PSP is required to acquire and maintain information of network status and preference of each peer.

Req-Traffic-020: Peer is required to measure data traffic of its network interface and convey the measured information to the P2PSP.

7.1.2 P2P Traffic Control

MP2P can control the traffic in two ways: direct control and indirect control. P2PSP constructs P2P network with the list of participating peers and indirectly controls the P2P traffic based on the gathered P2P network information. Peer can control its P2P traffic directly through controlling uplink and downlink traffic.

7.1.2.1 Direct P2P Traffic Control by Peer

Peers have ownership of their resources so that they can directly control the uplink/downlink traffic pattern. The activity of peers within P2P network can be controlled by the user's preferences. For example, user can limit the uplink/downlink bandwidth and controls the maximum number of concurrent peers. Furthermore, user can apply those parameters per peer or connection in providing differentiated services to the premium users.

Req-Traffic-030: Peer is required to be able to manipulate its preferences such as traffic pattern and differentiated access control.

Req-Traffic-040: Peer is recommended to control its traffic pattern.

Req-Traffic-050: Peer is recommended to provide differentiated access control.

7.1.2.2 Indirect P2P Traffic Control by P2PSP

P2PSP provides the peer list to the consuming peer in P2P network. Consuming peer can select contributing peer in the peer list to receive contents. During this process, P2PSP can indirectly control the traffic by ordering and filtering peers in the peer list.

Req-Traffic-060: MP2P is required to provide the capability of ordering and filtering for traffic control when providing peer list.

7.1.2.3 Network Level Traffic Control by ISP

ISP can perform traffic engineering in IP layer, but ISP cannot directly restrict or alter the P2P traffic since it could arise some legal issues. In the other hand, ISP can control by applying different QoS to different type of P2P-based services through DPI (Deep Packet Inspection). However, this is not only exhaustive task, but also can damage the performance of the network. Thus, traffic measurement and control in ISP will not be considered in this document.

7.1.3 NAT/Firewall Traversal & Traffic Relay

In general, peer behind NAT/Firewall cannot receive the incoming connection request from peer residing outside the NAT/Firewall. For the peers behind the NAT/Firewall, NAT traversal techniques such as STUN, TURN, ICE, and UPnP are applied to provide end-to-end communication. However, these techniques do not guarantee NAT traversal in every situation.

NAT/Firewall traversal is not a critical issue for delay-tolerant P2P-based services such as file distribution, because traffic does not have to be transferred symmetrically. However, for services such as streaming and real-time communication, it is required to provide NAT/Firewall traversal for peers behind the NAT/Firewall.

Req-Traffic-070: MP2P is recommended to provide NAT/Firewall traversal.

For peers without NAT/Firewall traversal capability, peer can traverse NAT/Firewall by utilizing peer with relaying function such as relay peer.

In the unmanaged P2P networking, it is up to the peer to traverse the NAT/Firewall. In certain occasion, peer needs to build a pinhole through STUN or UPnP in order to use the service. Failing to build such pinhole can result in service failure. This problem can be solved through the use of a relay peer. MP2P can provide NAT/Firewall traversal by maintaining a relay peer. In addition, each relay peer should be managed in order not to be overloaded. If a peer participates as a relay peer, P2PSP should consider an appropriate incentive method for contribution.

Req-Traffic-080: P2PSP is required to manage the contributing peer such as relay peer and super peer in order to keep track of the resource usage by consuming peers.

7.2 Cooperation Management

In non-manageable P2P networking, the peers are not selected based on topology and underlying network status which can cause various problems such as traffic implosion, monetary cost from inter-domain traffic. In order to solve these problems, the information of the underlying network should be considered through the cooperation among peers, P2PSP, and ISP. ISP can provide various network information including network bandwidth, network topology, routing policy, routing metric, distance, etc. Peer can provide own status such as status of the access network, system load, preference, etc. This information can be provided to the P2PSP in controlling P2P traffic, application congestion, and load distribution to improve the performance of the P2P network. By cooperation with the ISP, it is possible to provide better performance to the user through optimized P2P traffic routing and is possible to provide better traffic modelling for the ISP.

7.2.1 ISP-P2PSP Cooperation

P2PSP keeps track of all the peers participating in the P2P network and provides the list of peers that can provide the service to the consuming peer. In order to realize optimized peer selection, P2PSP can make the peer list based upon the information provided by the ISP and the participating peers. The ISP can assign priority on the peers in the peer list that is the most appropriate for the consuming peer based on the underlying networking prospective.

Req-Coop-010: MP2P is required to provide interfaces for cooperation with ISP and P2PSP.

However, it is important to keep the ISP's network information confidentially and should prevent that information from being open to the public, since it can cause problem in the network management and

network security perspective. Thus, it is important that the information exchanged between the ISP and P2PSP should be delivered safely under bilateral agreements.

Req-Coop-020: MP2P is required to construct secure connection between P2PSP and ISP.

7.2.2 ISP-Peer Cooperation

The ISP can provide information on the network status to the peer directly to assist in optimal peer selection.

Req-Coop-030: MP2P is recommended to provide interfaces for cooperating between ISP and Peer.

7.2.3 Peer-P2PSP Cooperation

Peer can provide the information on the preferences, local network status, system load, size of data received, and size of data sent. P2PSP analyses the status of each peer with the information provided. Thus, a unified interface between peer and P2PSP is needed for this interaction.

Req-Coop-040: MP2P is recommended to provide interface for cooperation between the P2PSP and peer.

Req-Coop-050: Peer is required to provide information of its sharable resources to the P2PSP.

Req-Coop-060: P2PSP is required to provide functions to query resource information of the participating peer.

Req-Coop-070: Peer is required to provide its status information to the P2PSP.

Req-Coop-080: MP2P is required to provide method for describing resources and its attributes.

7.3 Contents Management

The traditional P2P networking treats the contents as a merely data, it does not have the capability to classify the contents based on its characteristics including copyright status. Since data can be broken or corrupted during the transmission the consuming peers should be able to confirm the integrity of the received data. Moreover, MP2P needs to provide search engine for contents to enhance usability.

7.3.1 Copyright Protection

One of the major problems of P2P-based service is illegal distribution of copyright contents. It is difficult to stop proliferation of illegal distribution since the contents are located within user's storage. P2PSP may try to stop distribution of contents through removing information of the contents in the index server. This method can prevent new peer(s) from acquiring information to retrieve contents but the contents can still be distributed among peers already participating in the P2P network. Peer(s) can even retrieve the content through the DHT as well, if the P2P network is based on DHT. In some cases, content owner tends to distribute fake contents to prevent illegal distribution. However, this method results in waste of network resources which is not acceptable to the ISP. However, MP2P needs to define method to protected P2P content from copyright infringement and privacy violation.

Req-Content-010: MP2P is required to provide method to stop proliferation of distribution of contents.

Req-Content-020: MP2P is required to provide method to detect illegal distribution of copyright contents.

In order to stop the distribution of illegal contents, P2P network should be audited based on the informational characteristics of contents. The detailed method of auditing contents is out of scope of this document.

7.3.2 Data integrity

In P2P networking, contents are fragmented into multiple fragments. Peer exchanges the fragments with other peer(s), and the collected fragments are merged into a single content. In this process integrity and validation checks are made to the merged content. For integrity and validation checks, most P2P-based applications use hash functions.

Req-Content-030: Peer is required to check the validity of received fragments and contents.

Req-Content-040: Peer is required to send out the report to content provider or to the server if there is an integrity check error from received data.

Req-Content-050: Peer is required to recheck for integrity if there is an error on certain fragments and discard the fragments in order to receive the new fragment of data from other peers.

7.3.3 Contents searching

P2P network can be constructed in two methods. First method is constructing a single overlay network for a single content, and second method is constructing a single overlay network for multiple contents. In the first method, peer can query the index server for the information of the peers with the desired contents. In the second method, peer can flood a query over the P2P network to find the list of peers that has the desired contents or contents are queried to the third party, i.e. index server. No matter how the P2P overlay is constructed, MP2P needs to provide efficient content searching method.

Req-Content-060: MP2P is required to provide a search method to find specific content.

7.4 Service Management

P2P networking is applied to various applications and services. Typical P2P-based application is multimedia streaming service and file sharing services. The core concept is the same, but how the service is provided is somewhat different among the applications or the services based on P2P networking. For instance, P2P networks for file sharing and P2P network for live-streaming have different requirements and need to construct a P2P network adequately according to the requirements. Thus, it is important to find the detailed characteristics of the service and to allocate needed resources in the constructed P2P network.

P2PSP needs to provide the information of the characteristics of the P2P network to the P2P-based application. The P2P-based application can be adjusted to construct the most appropriate P2P networks.

7.4.1 Capability description on P2P network

Service providers should consider whether the service is suitable for selected P2P network before providing the service to the users. For example, services such as file distribution and network storage mirroring require stable and reliable P2P network. On the other hand, interactive services like VoIP requires P2P network with low latency and low jitter rather than reliability.

P2PSP can provide information of the network capability to the peer(s). P2PSP can assist in providing optimal P2P network based on the requirements provided by the P2P-based application/service.

Req-Serv-010: P2PSP is required to provide description on the characteristics of the P2P network

7.4.2 Managing service-specific P2P network

P2PSP can construct a new P2P network or reuse the constructed P2P network based on the requirements from the P2P-based application/service. It is possible to provide service in the separately isolated P2P network or to provide service on the common single P2P network based on the characteristics of application. In addition, it is possible to satisfy the requirements of the P2P-based application by installing cache server or relay server to the adequate position in the P2P network.

Req-Serv-020: MP2P is recommended to configure appropriate P2P network based on the service requirements.

7.5 Resource Management

Unlike the client/server model, resources of the P2P networks are scattered in unmanageable fashion along the multiple user devices. MP2P can provide capability to collect the information of the resources scattered over the P2P network and reorganize the resource to be optimally used in enhancing the P2P performance. MP2P will need to provide standardized method in reserving and utilizing the P2P resources. Thus, MP2P will need to identify the resources and to composite the resources available in the P2P network. Moreover, MP2P needs to provide explicit method expressing the sharing policy based on the user's preference.

7.5.1 Resource and peer identification

P2P needs to identify P2P service user, peer, and resource. One P2P service user can utilize one or more peers. One peer can share one or more resources. Thus, MP2P needs to differentiate each P2P service users, peers, and resources. Management of the P2P service user is in 7.6.1. This clause defines requirements for resource and peer identification.

Resource needs to be identified in order to collect and organize the information of the resources scattered over the P2P network. P2PSP should know the type, location, owner, sharing policy, usage, ratio and current load of the identified resources. P2PSP can assign and organize the resources based on this information.

Req-Reso-010: MP2P is required to provide identification of the resource to identify the resource of each peer in the P2P network.

Req-Reso-020: MP2P is required to gather the information of resources and to organize them based on resource identifier.

Req-Reso-030: MP2P is required to locate resource information with resource identifier.

Req-Reso-040: P2PSP is required to collect and to maintain information of the behavior of each peer.

7.5.2 Resource Composition

Resource composition is a composition of resources which peer can provide. Resource composition provides an abstract layer on top of the distributed physical resources. Peers in the P2P network can contribute resource including contents, network bandwidth, storage, computing power, etc. These resources can be

provided selectively. For example, it is possible to configure virtual network storage by combining contribution of network bandwidth and storage provided by peers.

Req-Reso-050: MP2P is recommended to provide resource composition through composition of resources.

7.5.3 Resource Sharing Policy

Peer can provide network, storage, and contents to other peers in the P2P network. The peer should acknowledge the capacity of the resources by considering the time and system load when sharing its resource selectively. P2PSP may collect this sharing status from each peer and applies this information to manage the P2P network.

Req-Reso-060: MP2P is required to provide method for describing the preference of peers on sharing resources.

Req-Reso-070: MP2P is recommended to provide method for delivering peer's preference on sharing its resources.

P2P service user can adjust a sharing policy of its peer. Peer will need to provide its resource according to the defined sharing policy.

Req-Reso-080: MP2P is required not to exceed the defined policy in sharing resource.

7.5.4 Resource Delegation

In some cases, peer would want to share its contents with other peers in the P2P network, but it does not have time or sufficient network resource to distribute its resource to other peers. In such case, resource delegation can be used. A peer can copy its contents to the dedicated surrogate(s) to be distributed to other peers. The surrogating peer(s) can be used to share contents on behalf of the content owner, even if content owner leaves P2P network.

Req-Reso-090: MP2P is required to provide method to discover appropriate delegate(s).

Req-Reso-110: MP2P is recommended to provide resource delegate(s).

7.6 P2P User Management

Traditional P2P-based service is based on anonymity, so all legal issues like copyright, network abuse, service fairness, and differentiated services are not handled properly. MP2P needs to provide identification method for P2P users in order to solve these problems and provide a framework for P2P-based services.

7.6.1 User Identification

Along with the identification of the resource, there must be identification method for users in the P2P network. Each resource can be mapped to one or more user identifiers. P2PSP will need to keep the information of the activities for each user and provides the information that can be used for accounting and providing incentive. Therefore, MP2P requires the semantics with naming rule to identify the users.

Req-User-010: MP2P is required to provide user identification management.

Req-User-020: P2PSP is required to collect and maintain information of the behavior of each user.

Req-User-030: P2PSP is required to maintain user profile for each user in the MP2P.

7.6.2 Incentive Mechanism

P2P-based service is provided through the sharing resources among the contributing peers. However, selfish user, i.e. user who does not share its resource, may decrease the performance of P2P network and cause problem in the aspect of service fairness. In some P2P-based application, unload/download ratio is measured to provide differentiated service accordingly to the contribution. However, this method is based on unreliable reports from peers, and is difficult to provide differentiated service after the peer has joined the P2P network. It is important to maintain the information of the user activity in the P2P.

Req-User-040: MP2P is recommended to provide incentives to the users who contribute to the P2P network.

Req-User-050: MP2P is required to gather resource utilization information from each peer.

Req-User-060: MP2P is required to provide methods for assuring the integrity of gathered information.

7.7 Distribution Management

P2P network needs to manage the distribution of contents. Since all content distributions are performed between peers, it is hard to provide differentiated services to different level of users. Also, current P2P network is focused on providing benefits to the contents consumer. It does not have any method that provides information to the contents distributors about result of distribution such as statistic report and distribution results. MP2P is capable of providing these types of reports and results.

7.7.1 Distribution Report

In P2P network, data is exchanged directly among peers. P2PSP is not informed of the amount of the exchanged data or of the problems that occurs in the data sharing process. In addition, contents owner does not have the capability to control the delivery method or is informed of the results of the contents distribution.

In MP2P, peers report the delivery results to the P2PSP for the P2PSP to understand the data delivery status and to react quickly to the problems that may occur during the delivery process. P2PSP can provide the content distribution results to the contents distributors.

MP2P can provide mechanisms on distribution reports including reporting frequency and reporting target. During the initiation of the P2P network, peer will receive this reporting policy and the peer will need to behave in accordance with this policy.

Req-Dist-010: MP2P is recommended to report to the content provider on the content distribution result.

Req-Dist-020: MP2P is recommended to report events related to the P2P activities.

7.7.2 Differentiated Distribution

In P2P network, peer can distribute the contents to other peers that are participating in the P2P network. In the distribution process, peers will be requested to send a part of contents and assign a limited resource to the consuming peer. Some P2P networking uses incentive mechanism such as tit-for-tat or give-to-get to provide fairness among the peers, but most of the P2P networking use random scheduling method.

MP2P should provide differentiated service to the peer under the user class. User class can be classified through the policy set by the P2PSP or the level of contribution anticipated by the peers. The classification method of the user class is out of scope of this document.

Req-Dist-030: MP2P is recommended to provide differentiated service according to the user class.

Req-Dist-040: MP2P is recommended to provide mechanism to differentiate users according to service policy.

7.8 P2P Network Management

P2P network is formed by the combination of resources provided by the peers. Since peer can join and leave frequently and unpredictably, it is hard to provide stable service, i.e., stable data delivery rate, over P2P network. In order to provide stable P2P-based services, P2P network should be manageable to be robust, stable, and scalable.

7.8.1 Network maintenance

P2P network is a virtual overlay network located over the physical underlying network. In other words, P2P network is built independently from AS section of ISP. Furthermore, one P2P network can be managed by multiple P2PSP; e.g. multiple tracker servers for one P2P network. Since participants of the P2P network are peers from user-side, it is difficult for the P2PSP to directly control and manage the user-side peers. Therefore, it is complicated to figure out the precise topology of the P2P network. Furthermore, it is even trickier if several P2PSPs are involved.

If the peer does not have any problem in being provided with the P2P-based service, peer does not have to know of the precise topology of the P2P network. That is, peer does not have to know the full topology of the P2P network in order to be provided with reasonable P2P-based services quality. Thus, P2PSP needs to configure and managed P2P network with the status information provided by the ISP and peers.

Req-Net-010: P2PSP is recommended to use the information from ISP and peers to organize and to manage P2P network.

MP2P can provide enhanced QoS/QoE and elevated network performance by using aggregated peer-side information such as network information, behaviour policies, dynamic status information including CPU load, networking status including incoming/outgoing network bandwidth, acceptable number of peers, sharing policy, etc.

Req-Net-020: MP2P is recommended to adjust its behaviours based on aggregated information from peers and on its status. This status information may include CPU load, networking status including incoming and outgoing bandwidth, sharing policies, etc.

7.8.2 Network Robustness and Stability

In P2P network, it is difficult to control the unpredictable behavior of frequent join and leave of peers. The peer list would be inaccurate as with the unexpected leave of the peer. The peer can continue the service with interaction with other peers in the peer list. However, inaccurate peer list can be distributed for some period of time. If the P2PSP is notified of the peer failure or network failure, it will be able to handle such failure according to the notified information. Thus, the stability of the P2P network can be enhanced.

Req-Net-030: MP2P is required to provide mechanism to detect peer failure or network failure.

If the information on the status of P2P network can be attained, peer can determine the most appropriate P2P network. This information may include the number of peers, creation time of P2P network, time of last activity, etc.

Req-Net-040: MP2P is required to provide the information of P2P network to assist in choosing appropriate P2P network.

In order to maintain up-to-date status of the P2P network, P2PSP needs to receive reports from peers. This report includes the information related to interaction between peers. By providing information of the peer failure, P2PSP can construct the most up-to-date P2P network. In addition, P2PSP can convey this information to the peers involved in P2P network.

Req-Net-050: Peer is required to report to P2PSP on detection of interacting peer failure.

Req-Net-060: P2PSP is required to re-organize P2P network in accordance with the failure reports.

7.8.3 Data Integrity

In P2P network, contents are fragmented into multiple fragments, and fragments are exchanged among multiple peers that have no trusted relationship. Thus, these collected fragments needs to be verified prior to merging into the full contents.

Req-Net-070: Peer is required to check the validity of data exchanged among peers.

Data exchanged through P2P network can be corrupted. The stored data itself can be corrupted, or it can be corrupted during delivery process. The receiving peer should be able to identify and to repair the corrupted data before propagating it through the P2P network.

If the contributing peer frequently sends a corrupted data, P2PSP should be notified to take measure. Normally, P2PSP will need to inspect the reported peer and remove it from the P2P network to stabilize the P2P-based service.

Req-Net-080: Peer is required to report the failure of integrity check to P2PSP in order to stop or prevent proliferation of corrupted data.

Req-Net-090: MP2P is recommended to remove peer from P2P network, which sends corrupted data frequently.

7.8.4 Support of Data Caching

If the number of the participating peers is large enough, the robustness and stability of the P2P-based service increases. Even though multiple peers may suddenly leave the P2P network, the remaining peer can still provide P2P-based service to certain quality with sufficient peers remaining in the P2P network. However, if the service quality suddenly decreases to a certain level, P2PSP needs to provide a cache server to keep the quality of service.

Req-Net-100: MP2P is recommended to provide cache server for P2P network.

If the number of peers exceeds a certain threshold, resource of the cache server can be released to be allocated to other emerging P2P network. Figure 2 shows the number of peers participating in a single P2P network. The number of peers is low during service initiation phase. It increases as the service matures and reaches the stable phase. The popularity of the particular P2P network tends to decrease as the service fades out. The cache server can be used during the service initiation phase to support P2P network to rapidly reach the stable phase and during the service termination phase to support service before being completely terminated.

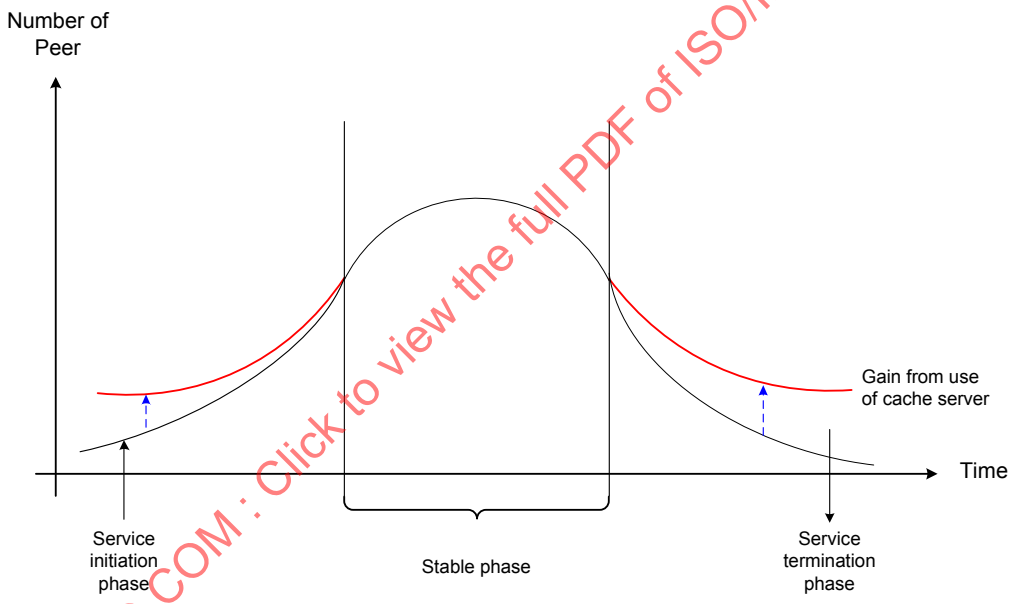

Figure 2 — Service lifecycle and enhancement with cache server

For P2P-based file sharing service, if connection breaks during data delivery, peer should find another peer to retrieve the rest of the contents. If there is adequate number of peers, it is possible to provide the sufficient level of service. However, if there are an insufficient number of peers, then it has to wait until it can find a peer with the required contents.

7.8.5 Support of Data Relay

P2P technology can be used in various services such as real-time communication, multimedia streaming, etc. Some of the participants of these services may reside behind NAT/Firewall, which cause problem in sharing its resources. Peer outside the NAT/Firewall cannot directly establish connection toward the peer behind the NAT/Firewall. This may not be a critical problem for services such as file sharing. But, services which require real-time communications, this can be a critical issue.

MP2P can provide relay service to relay traffic to peer behind NAT/Firewall by establishing and maintaining connection with peer behind NAT/Firewall. The relay service can be provided by the P2PSP server or by a voluntary peer willing to share its resources for the public.

Req-Net-110: MP2P is required to provide relay service for P2P network.

Req-Net-120: MP2P is required to keep track of usage of relay service.

Req-Net-130: MP2P is required to provide interfaces to reserve resource for relay service.

8 MP2P framework

8.1 Domains

The framework of managed P2P is shown in Figure 3. It consists of three domains.

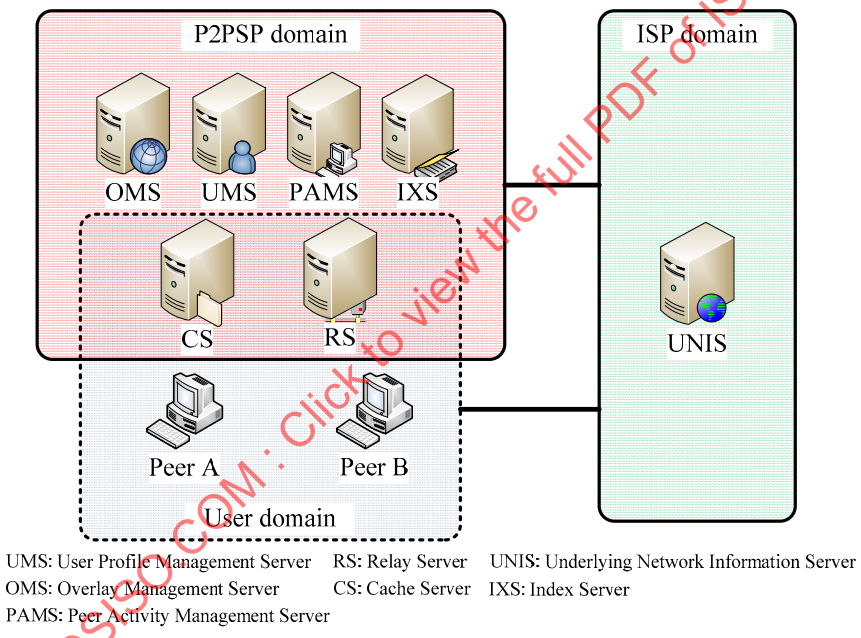

Figure 3 — Framework of managed P2P

8.1.1 P2PSP domain

The P2PSP domain controls and supports the MP2P-based services. It controls services through cooperation of various servers such as OMS, UMS, PAMS, and IXS. It supports services through usage of CS and RS. It cooperates with the ISP domain to enhance MP2P-based services in terms of underlying network efficiency.

8.1.2 ISP domain

ISP domain provides the information of the underlying network i.e., capacity, policies, network distance to other domains (i.e., P2PSP domain, user domain). It is composed of UNIS which is an entity that provides such information.

8.1.3 User domain

User domain consumes the MP2P-based service. It is composed of peers. Peers receive services from other peer(s) or from entities(s) of the P2PSP domain. Also, peer can function as a cache server or as relay server.

8.2 Entities

This clause describes the entities of the MP2P framework. Figure 4 shows the overview of functional architecture. Detailed description for each entity is as follows.

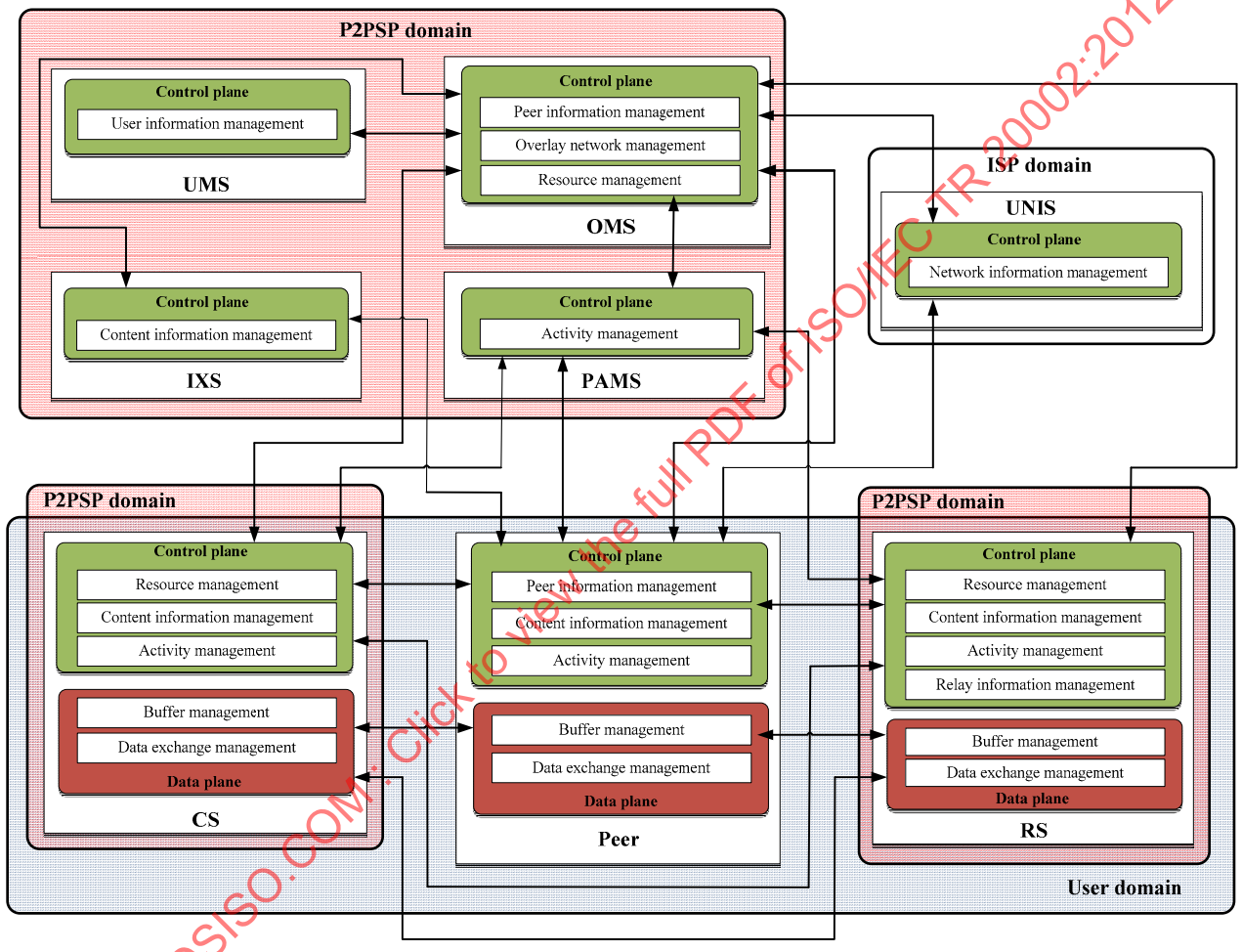

Figure 4 — MP2P functional architecture

8.2.1 Peer

As the provider and consumer of the MP2P-based service, peer is an essential entity of MP2P framework. Each peer shares its resource with other peer(s) by sending and receiving contents with other peer(s), simultaneously.

Peer can be a provider of P2P-based service by acting as a cache server or relay server. A peer acting as a cache server or relay server can be designated by the P2PSP or by voluntary participation.

The function of the peer can be divided into control plane and data plane. The control plane manages the connectivity with other peers (or CS/RS), the subscription for a particular service, and activity status to be used to report its activity information. The data plane manages local buffer, exchange data with other peer (or CS/RS).

8.2.2 User profile Management Server (UMS)

UMS maintains the user information for management purpose. User profile is maintained for each user in the UMS. The user information may include identification, network information, reputation, etc. The UMS provides the information requested by the OMS.

The UMS has only control plane. The control plane manages the user information which is used by the OMS. The control plane interacts with OMS to provide the user information to the OMS.

8.2.3 Overlay Management Server (OMS)

OMS manages the MP2P network and assists peer in joining the MP2P network. In order to maintain the MP2P network, OMS deals with the request of service join and the status information from peer. OMS gives the consuming peer the selected peer list which can provide the requested service. Through interaction with UNIS, OMS can provide peer list suitable for the consuming peer to generate an optimal MP2P network.

The OMS has only control plane. The control plane manages information of the peer, overlay network, and resources. The peer information includes network capability, network status, participating status, shared resources, etc. The overlay network information includes sharing status of the resource(s) and a list of participating peer(s).

8.2.4 Underlying Network Information Server (UNIS)

UNIS is a dedicated device of the ISP which provides the information of the underlying network and network management policies. UNIS can provide the information of the network distance between peer in the P2P network. UNIS can interact with both peer and OMS.

The UNIS has only control plane. The control plane manages information of the underlying network in the ISP perspective. The control plane interacts with OMS to provide the underlying network information to the OMS. The underlying network information can optionally be provided to peer.

8.2.5 Cache Server (CS)

Cache server (CS) is used to cache contents for peers to stabilize the P2P-based service. CS can be a dedicated device (i.e., dedicated CS) provided by the P2PSP or temporary device (i.e., temporary CS) provided voluntarily by a contributing peer. The dedicated CS is normally a trusted device that is controlled by the P2PSP, thus, if a problem occurs to this device, it is required to notify the OMS. The temporary CS is normally a user device which has fewer obligations compared to the dedicated CS. Thus, if a problem occurs to this device, it is recommended to be notified to OMS.

The function of the CS can be separated into control plane and data plane. The control plane manages connectivity with peers (and CS/RS), the subscription for particular service, and activity status to be used to report its activity information. The data plane manages local buffer, exchange data with other peer (or CS/RS).

8.2.6 Relay Server (RS)

Relay server (RS) is used to relay contents to assist the participant behind the NAT/firewall to properly participate in the P2P-based service. RS maintains the connection with the peer behind NAT/firewall to assist peer in establishing connection with the peer behind NAT/firewall. RS can be a dedicated device (i.e., dedicated RS) provided by the P2PSP or temporary device (i.e., temporary RS) provided voluntarily by a contributing peer. The dedicated RS is normally a trusted device that is controlled by the P2PSP, thus, if a problem occurs to this device, it is required to notify the OMS. The temporary RS is normally a user device

which has fewer obligations compared to the dedicated RS. Thus, if a problem occurs to this device, it is recommended to be notified to OMS.

The function of the RS can be separated into control plane and data plane. The control plane manages connectivity with peers (and CS/RS), subscription for a particular service, relay information, and activity status to be used to report its activity information. The data plane manages local buffer, exchange data with other peer (or CS/RS).

8.2.7 Index Server (IXS)

Index Server is used to provide service-specific information. In case of contents distribution, it contains the meta-information of contents. This information may include P2P network ID, descriptions on contents, address of OMS. Index server is also used for contents or service search.

The IXS has only control plane. The control plane manages information of the contents for the peer to retrieve the appropriate information of the desired content. The control plane interacts with OMS to provide the content information to the OMS and peer.

8.2.8 Peer Activity Management Server (PAMS)

PAMS maintains the status information of each participating peers. The status information can be classified into dynamic and static information. The dynamic information may include peer load, traffic status including incoming and outgoing bandwidth, and the acceptable number of concurrent TCP connections. The static information may include peer's resource sharing policies, timely fashioned peer's behaviour and configurations. The status information is reported by the participating peers when appropriate. PAMS also share its aggregated information with OMS to improve performance of the P2P network and P2P-based services.

The PAMS has only control plane. The control plane manages information of the peer activity. The control plane interacts with peer, CS, and RS to provide the information of the peer load status to the OMS.

8.3 High-level information flows

This clause describes the high-level information flows of the MP2P-based service. The interaction among the entities in the MP2P framework is used to provide manageability for the P2P-based service and to enhance the quality of service.

8.3.1 Traffic localization

This clause describes the control flow for traffic localization. Peer will be able to find a local peer that can provide the requesting service.

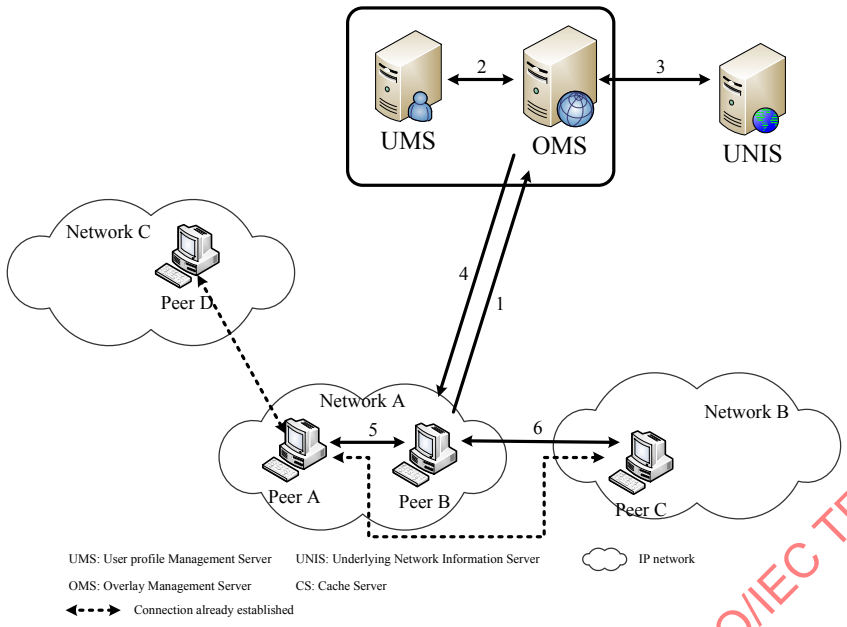

Figure 5 — Control flow for the traffic localization

The control flow for traffic localization is shown in Figure 5. The description of the flow is as follows.

As a presumption, peer A, peer C, and peer D are already participating in the MP2P network. Peer B is a new peer that is willing to join the MP2P network.

1. Peer B requests OMS to join the MP2P network.
2. OMS forwards the information of peer B to UMS to produce the user profile on peer B. The user profile may be created or updated in this process.
3. OMS may need to query UNIS for the network related information to find more appropriate peer in the network perspective that can provide the requested service.
4. OMS provides a peer list to peer B sorted in the order that is more appropriate for peer B. In order to assist peer B in choosing optimal peer(s), peer(s) in the local network will have the highest priority. In Figure 5, the sorted order is peer A, peer C, and peer D.
5. Based on the peer list received from OMS, peer B makes a connection with peer A which is in the same local network.
6. If peer B needs to make another connection, peer B selects peer C according to the peer list and establishes a connection with peer C.

MP2P framework can provide the traffic localization through interaction among UNIS, UMS, and OMS.

8.3.2 Load balancing

This clause describes the control flow for load balancing. A specific peer can suffer from load due to the automaticity of the peers in MP2P network. The OMS needs to balance the load of the contributing peer by considering the load of each peer.

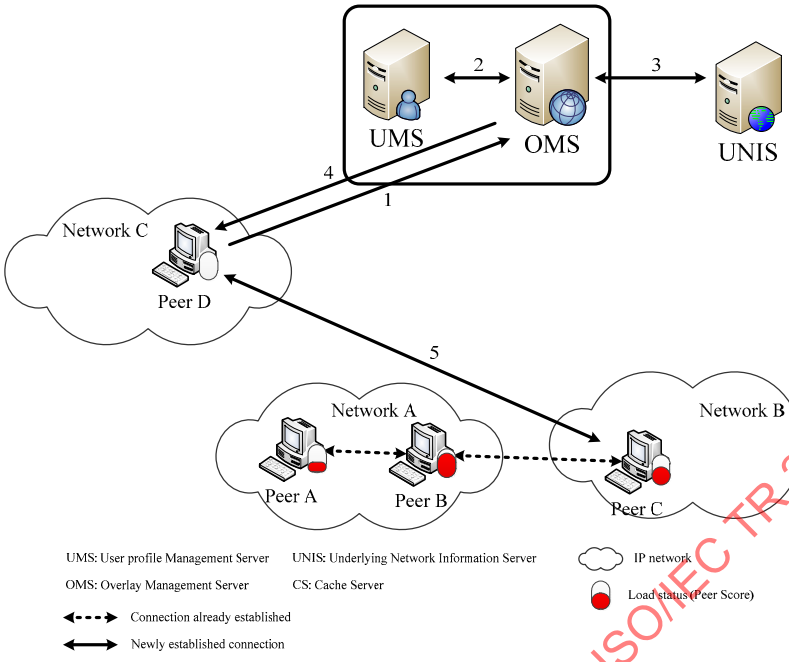

Figure 6 — Control flow for load balancing

The control flow for load balancing is shown in Figure 6. The description of the flow is as follows.

As a presumption, peer A, peer B, and peer C are already participating in the MP2P network. Peer D is a new peer that is willing to join the MP2P network. In addition, peer B is suffering from overload.

1. Peer D requests OMS to join the MP2P network.

2. OMS forwards the information of peer D to UMS to produce the user profile on peer D. The user profile may be created or updated in this process.

3. OMS may need to query UNIS for the network related information to find more appropriate peer in the network perspective that can provide the requested service.

4. OMS creates a peer list sorted in the order that is appropriate for peer D. The OMS check the peer list to check if there are any peers that is being overloaded. The overloaded peer can be removed from the peer list or be assigned with lower priority. In Figure 6, peer B is overloaded, thus, the sorted order is peer A, peer C, and peer B.

5. Based on the peer list received from OMS, peer D makes a connection with peer C.

In summary, MP2P framework can provide the load balancing through interaction among UNIS, UMS, and OMS.

8.3.3 NAT/firewall traversal

This clause describes the control flow for NAT/firewall traversal. A peer can be under NAT/firewall. P2PSP needs to provide MP2P-based services to peer under NAT/firewall.

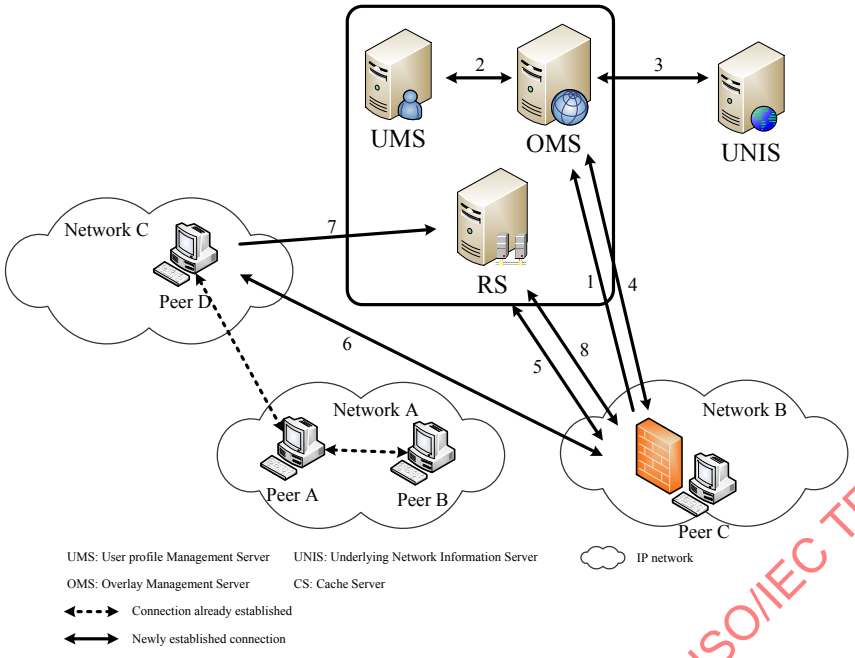

Figure 7 — NAT/Firewall traversal in MP2P network

The control flow for NAT/Firewall traversal is shown in Figure 7. The description of the flow is as follows.

As a presumption, peer A, peer B, and peer D are already participating in the MP2P network. Peer C is a peer behind NAT which is willing to join the MP2P network.

1. Peer C requests OMS to join the MP2P network. Peer C informs the OMS that it is behind NAT/firewall.
2. OMS forwards the information of peer C to UMS to produce the user profile on peer C. The user profile may be created or updated in this process.
3. OMS may need to query UNIS for the network related information to find more appropriate peer in the network perspective that can provide the requested service.
4. OMS provides peer C with information of RS to be used for NAT/firewall traversal.
5. Peer C establish a connection with RS and maintains the established connection.
6. Peer C initiates connection with peers outside the NAT/firewall.
7. Peer outside the NAT/firewall initiates connection with peer C through RS.
8. RS relays the received request to peer C. After the connection is established, RS relays data between peers outside the NAT/firewall with peer C.

In summary, MP2P framework can provide the NAT/firewall traversal through interaction among UNIS, UMS, OMS, and RS.

8.3.4 Forced stop of illegal distribution

This clause describes the control flow to stop illegal distribution of copyright contents.

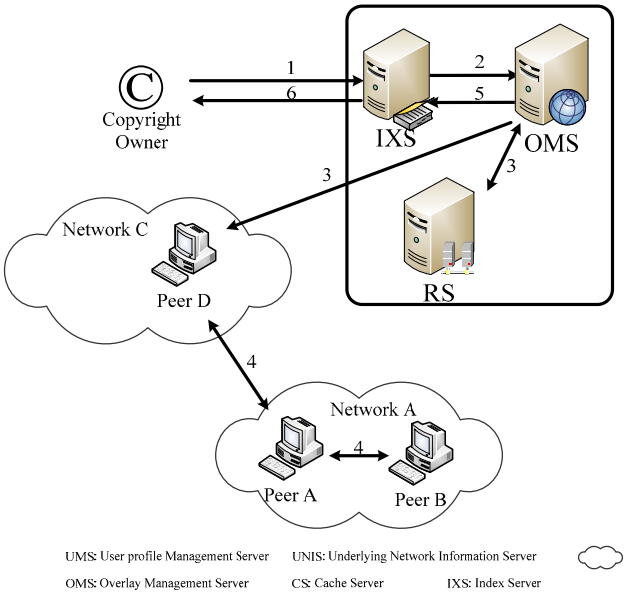

Figure 8 — Forced stop of illegal distribution

The control flow for forced stop of contents distribution is shown in Figure 8. The description of the flow is as follows.

As a presumption, there is an interface between IXS and copyright owner. This interface is out of scope this document.

1. Copyright owner requests IXS to stop distributing certain copyright contents. This procedure can be done through online or offline.

2. IXS deletes contents information from internal database and notifies to OMS to stop distribution.

3. OMS sends request to connected peers to stop distributing and release RS resource that is allocated for content distribution.

4. When a peer receives this message from OMS, it relays the stop distribution message to its connected peers, which is propagated to the rest of the peers in the MP2P network.

5. OMS informs IXS of the result of the forced stop of distribution and remove the information of the peer list for that contents.

6. IXS sends the received reports to the copyright owner. This procedure also can be done online or offline.

8.3.5 Content searching and retrieval

This clause describes the control flow for content searching and retrieval.

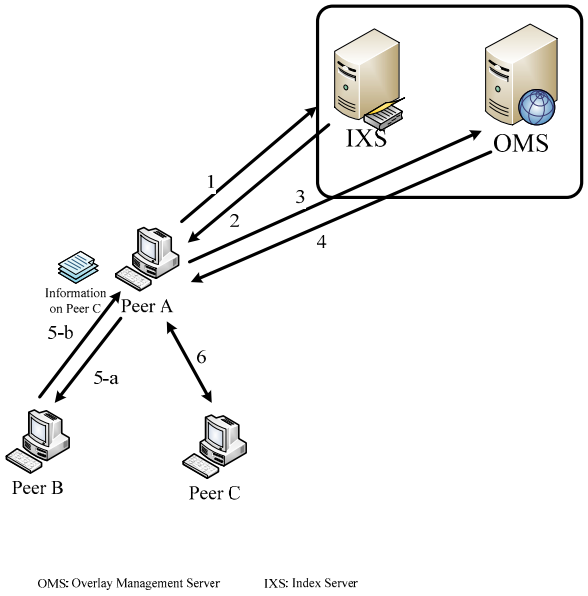

Figure 9 — Content searching and retrieval

The control flow for content searching and retrieval is shown in Figure 9. The description of the flow is as follows.

As a presumption, a single MP2P network is constructed for a single content and Peer A wants to receive content X.

1. Peer A connects to IXS to find MP2P network for content X.
2. IXS responds with the information of the MP2P network, such as overlay ID, which can provide the requested contents.
3. Peer A connects to OMS to join the MP2P network for content X.
4. OMS sends information of the peers that are participating in the MP2P network for content X. In this case, OMS sends information of Peer B, only.
5. Based on the information received from OMS, Peer A makes connection with Peer B. During this procedure, Peer B can give the information on Peer C to Peer A.
6. Peer A can learn of Peer C based on the information received from Peer B. If needed, Peer A can make connection with Peer C.

8.3.6 Configuration of MP2P service overlay network

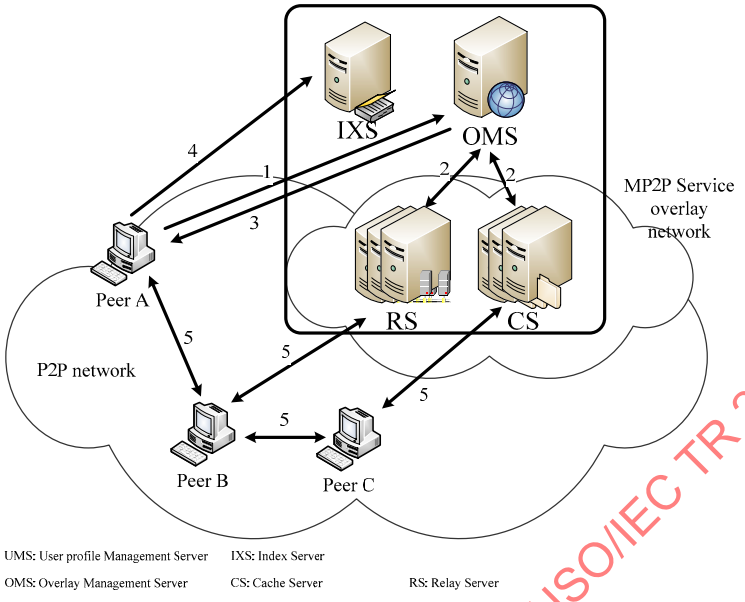

Figure 10 — Configuration of MP2P service overlay network

MP2P framework supports configuration of MP2P network according to the service requirements. An example configuration of MP2P network according to service requirements is described as follows.

1. Peer A wants to distribute a content through MP2P network. Peer A requests OMS to construct a new MP2P network to provide its content distribution services.

2. According to the service requirement from Peer A, OMS constructs an appropriate MP2P network. In order to achieve service requirements, OMS may reserve resources of P2PSP, such as RS and CS.

3. After construction of appropriate MP2P network, OMS notifies Peer A of successful creation of MP2P network to provide a new service.

4. In order to advertise its service, Peer A requests IXS to register its service.

5. Other peers, Peer B and Peer C, can participate in the MP2P network for content distribution service provided by Peer A. Other peers may receive service through Peer A or through P2PSP-side resources which are reserved for providing service of Peer A.

8.3.7 Resource delegation

This clause describes the control flow for resource delegation. In case of mobile terminal, the network access cost and high battery consumption is an issue to participate in normal P2P activities. Hence, it is desirable to use resource delegator to surrogate the role of peer for the mobile terminal. In this case, a CS(Cache Server) can act as a resource delegator for the mobile terminal to provide storage, network, etc.

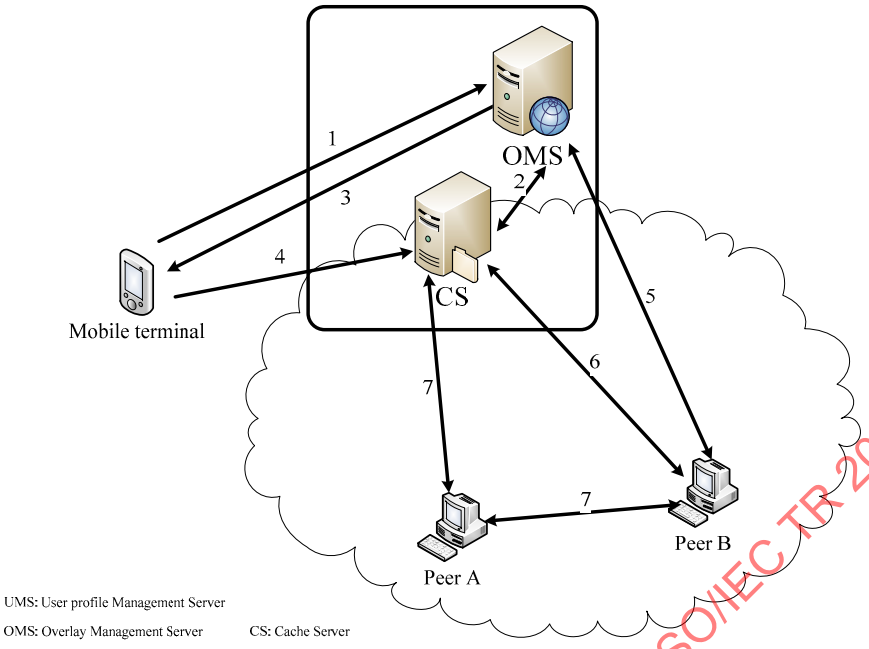

Figure 11 — Flows for resource delegation

The control flow for resource delegation is shown in Figure 11. The description of the flow is as follows.

1. Mobile terminal requests OMS to allocate resources for delegating mobile terminal's activity for distributing mobile terminal's contents.
2. OMS reserves resources of CS for mobile terminal.
3. OMS responds to mobile terminal with the information of CS for resource delegation. This information may include network address, description on reserved resources.
4. When mobile terminal receives a confirm message from OMS, it begins to send contents data to CS.
5. ~7. Contents from mobile terminal can be shared among peers and CS.

8.3.8 Distribution report

This clause describes the control flow for distribution report. This report contains information whether distribution was successful. If the distribution ends in errors, peer sends report to OMS with appropriate error message. If the distribution is successful, peer sends distribution status report to UMS. The information aggregated in the UMS will be used in providing incentives for contributing users. The methods for providing the incentives are dependent on the P2PSP incentive policies.

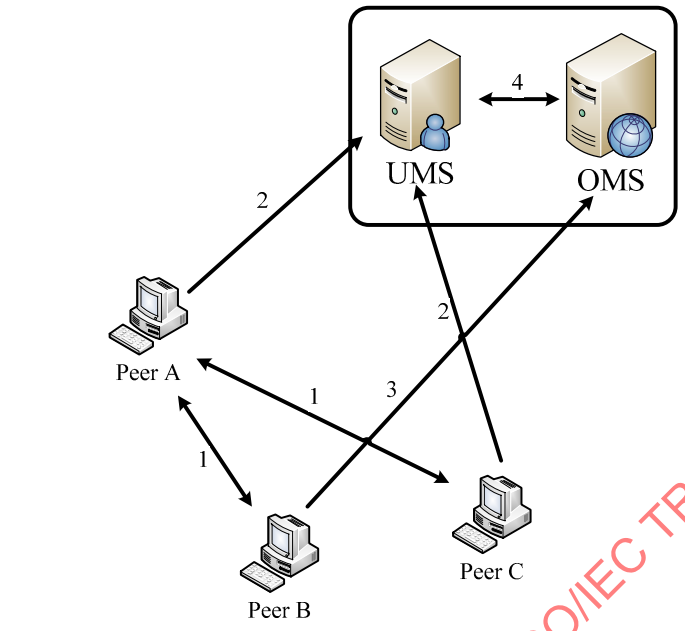

Figure 12 — Flows for Distribution Report

As a presumption, peers already know the information of UMS and OMS, and this flow begin with data exchange among peers for simplicity.

The control flow for distribution report is shown in Figure 12. The description of the flow is as follows.

1. Peer A,B,C shares contents.

2. After successful exchange of contents, Peer A and C send report to UMS. In this report, it may include how much data has been exchanged and the index number of fragments. Even though, there are some errors between Peer A and B, Peer A sends successful report to UMS, if transmission to Peer B has been completed.

3. When Peer B detects some error on received data/contents, it reports to OMS.

4. OMS interacts with UMS for maintaining consistency of information that is received from each peers.

It is possible for each peer to report of reception of single fragment, but this would leads to heavy load to OMS and UMS. Hence, it should be also possible to report aggregated information for pre-specified interval. By using aggregated report on UMS, P2PSP can provide incentives to resource contributors. How to use the information for providing incentives are dependent to the policy of P2PSP. MP2P framework provides capability for aggregating raw data that can be used in incentive policy.

If the OMS receives distribution error reports from multiple peers, OMS will need decides whether the peer is distributing polluted data. If OMS decides that a specific peer is corrupting the MP2P network, it can expel the troublesome peer from the MP2P network.

8.3.9 Differentiated service for user class

This clause describes one example for confirming the user class of consuming peer to provide the differentiated service according to the user class. The actual methods of providing differentiated service are service dependent. For example in streaming service, peer can send the streaming data block in the order of the peer class with peer of higher class receiving the most recent data.

One important factor in providing differentiated service is for the peer to confirm the user class of the consuming peer. The new peer can inform the neighbouring peers of its class which will need to be confirmed by the P2PSP. The flow of confirming user class is shown in Figure 13.

As a presumption, peers already know the information of UMS and OMS. Peer B and Peer C are new to Peer A and are requesting P2P-based service from Peer A.

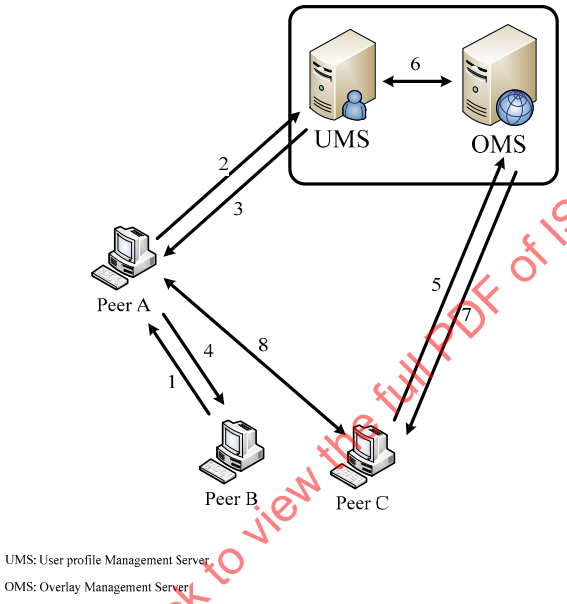

Figure 13 — Confirming user class from P2PSP domain

This clause describes two methods in confirming user class from P2PSP. The first method is when Peer A asks UMS for the actual class for Peer B.

1. Peer B requests Peer A for the P2P-based service. Peer B informs the Peer A of its user class. If Peer B declares of being the lowest class and no other confirmation is needed, Peer A may omit step 2 ~ 3 and move to step 4.

2. Peer A asks for the actual class of Peer B from UMS. This process may also be used to confirm other information such as the qualification of the Peer B in using the pertaining P2P-based service.

3. UMS confirms the class of Peer B along with other information needed in providing this service.

4. Peer A provides Peer B with service as accordingly to the specified class.

The second method is when Peer C asks the OMS for a passkey to verify its class to Peer A.

5. Peer C asks for a passkey to OMS to verify its class. This process can occur during the initial access of the Peer C to the P2P network.

6. OMS asks the UMS for the user class information of Peer C.

7. OMS informs the Peer C of the passkey to be used in identify itself during the P2P-based service,

8. Peer C provide a passkey to Peer A along with the P2P request.

8.3.10 Peer activity managements

This clause describes the control flow for aggregating peer's activity information. Peer activity information includes dynamic and static information. The activity information can be retrieved from peers by event-driven notification or request/response between P2PSP and peers.

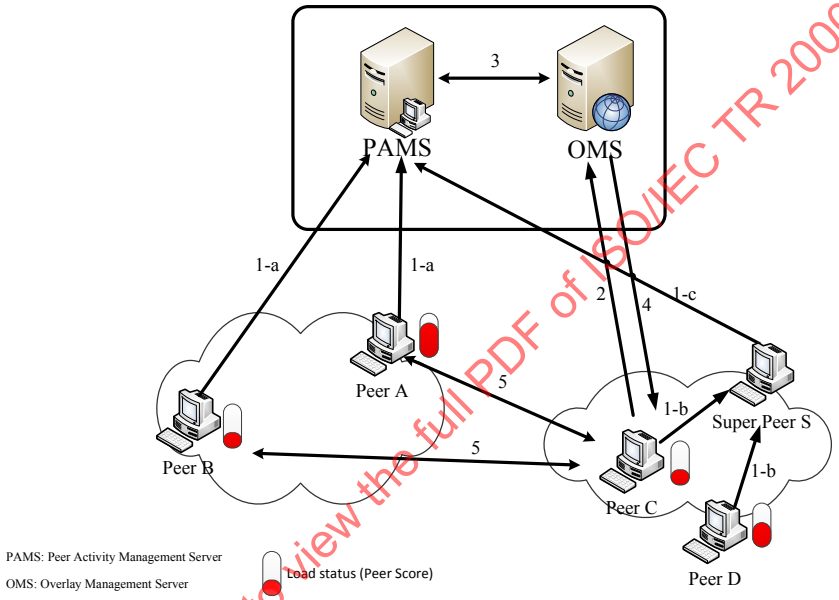

Figure 14 — Control flow for Peer Activity Management

The control flow for peer activity management is shown in Figure 14. The description of the flow is as follows.

As a presumption, peer A, peer B are already participating in the MP2P network, and Peer C is a new peer that is willing to join the MP2P network. Peer C and peer D are under control of super peer S.

1. Each peer reports its status to PAMS or super peer S. Peers that are under control of super peer S sends their reports to super peer S.
   a. Peer A and peer B sends its status information to PAMS directly
   b. Peer C and peer D sends its status information to super peer S
   c. Super peer S sends aggregated status information to PAMS
2. Peer C request OMS to join MP2P network.
3. OMS constructs peer list for the requested MP2P network and query status information of each peers in the list to PAMS.

4. OMS reconstructs peer list with each peer's status information and send it to peer C. This message contains peer list and status information of each peer.

5. Based on the peer list and status information received from OMS, peer C selects the most appropriate peers.

In summary, MP2P framework can provide the peer activity management through interaction among PAMS, OMS and peers.

Annex A
(informative)

Use Case for managed P2P

There are various types of P2P-based service and applications. This annex describes some major P2P-based applications and use cases for managed P2P.

A.1 P2P-based File distribution

The peers share files or contents by distributing files/contents across the P2P network. The P2P based file distribution is different from file distribution in client-server fashion. P2P-based file distribution such as *BitTorrent* can exploit downlink bandwidth of each peer for faster file distribution. In addition, P2P-based file distribution can provide better scalability than client-server based file distribution.

However, in the P2P based file distribution, peers are scattered over the Internet incurring numerous inter-ISP traffic that imposes monetary cost to the ISP. In addition, peer cannot choose the most appropriate peer in terms of link capacity since the peer makes selection based on the round-trip time (RTT). Copyright infringement is also a problem. It is hard to stop the distribution of illegal contents in P2P-based file distribution.

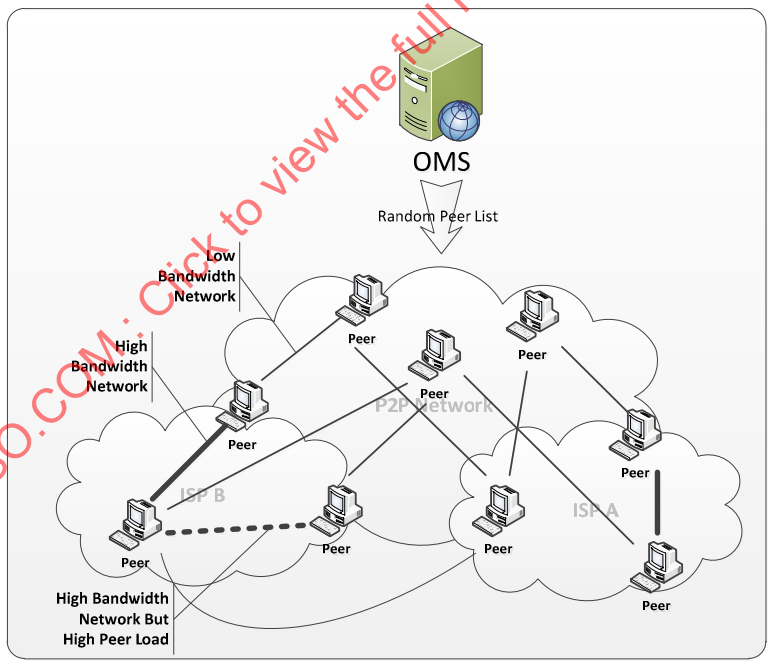

Figure A.1 — A.Use case of file distribution in P2P

The Figure A.1 shows the use case of P2P file distribution. As shown in Figure A.1, OMS returns random-ordered peer list to the joining peer because it has no information on peer status or underlying network information. Even though a peer is able to choose a local peer, the end user will not have the expected QoS/QoE when the local peer is overloaded.

Through managed P2P, traffic between peers can be localized and optimized since each peer can obtain information of the most appropriate peers from OMS by cooperation between P2PSP and ISP. Furthermore, peer can choose the most optimal peers with the support of PAMS.

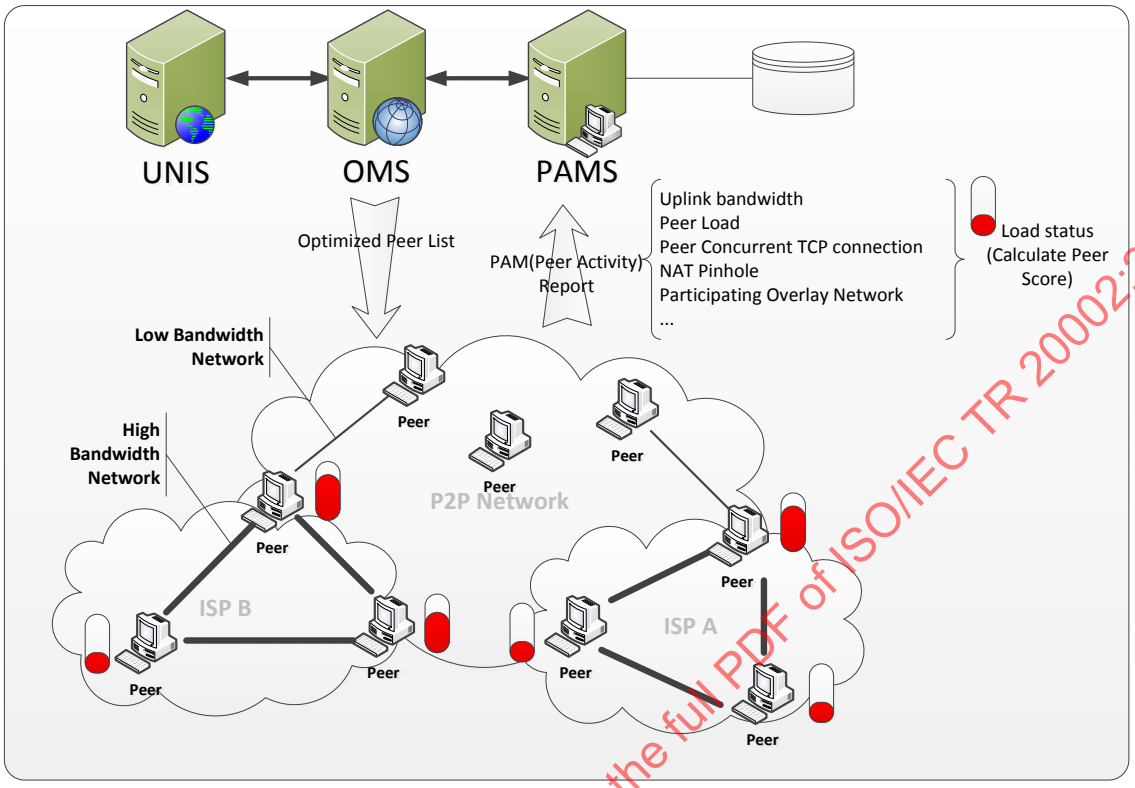

Figure A.2 — Use case of file distribution in MP2P

Figure A.2 shows the use case of file distribution in the MP2P network. Each peer has connection with the peers in the local network which can deliver data at high speed. The peer is able to recognize the load of each peer which it enables to choose the most appropriate peers. When a peer request OMS for the peer list, OMS interacts with the UNIS and PAMS to create a peer list ordered as most appropriate for the requester. Peer list contains underlying network information and status information for of each peer. The underlying network information is provided by UNIS. The status information is provided by PAMS which is aggregated from the report by each peers. The report may contain unlink/downlink bandwidth, load, the number of servicing peers, and the list of participating P2P network. Before providing the status of peer, agreement by the user of each peer should be preceded for privacy concern.

There are two methods in providing status information by each peer. The first method is to provide peer activity information along with the peer list. In this case, if a consuming peer requests for a peer list of a specific P2P network, it is provided with the contributing peer list containing detailed peer status. Consuming peer selects the most appropriate peer based on its necessity. The second method is to provide peer activity score rather than the precise status information. Before OMS sends the peer list to the consuming peer, it request PAMS to send the score of each peer within the peer list. By applying MP2P framework, each peer can retrieve contents from the most appropriate peers which construct an optimized P2P network.

A.2 Multimedia or Voice over IP

MP2P framework can provide infrastructures for multimedia communication services such as VoIP. Traditional ITSP (Internet Telephony Service Provider) provides voice communications service using UDP datagram. It uses a proxy server to locate the address of the callee. This may cause bottleneck to proxy server when massive number of call requests are made, or is vulnerable to the DoS(Denial of Service) attacks. Another