TECHNICAL REPORT

ISO/IEC TR 20002

First edition
2012-12-01

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 20002:2012(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 iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols (and abbreviated terms) 2

5 Concept of Peer-to-Peer networking 3
5.1 Characteristics of P2P network 3
5.2 Classification of P2P network 4

6 Problem statement 5
6.1 Problems in the network-side 6
6.2 Problems in the service-side 6
6.3 Problems in the user-side 6

7 Requirements of Managed P2P 7
7.1 Traffic Management 7
7.2 Cooperation Management 9
7.3 Contents Management 10
7.4 Service Management 11
7.5 Resource Management 12
7.6 P2P User Management 13
7.7 Distribution Management 14
7.8 P2P Network Management 15

8 MP2P framework 18
8.1 Domains 18
8.2 Entities 19
8.3 High-level information flows 21

Annex A (informative) **There are various types of P2P-based service and applications. This annex describes some major P2P-based applications and use cases for managed P2P** 33

Bibliography 42

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.

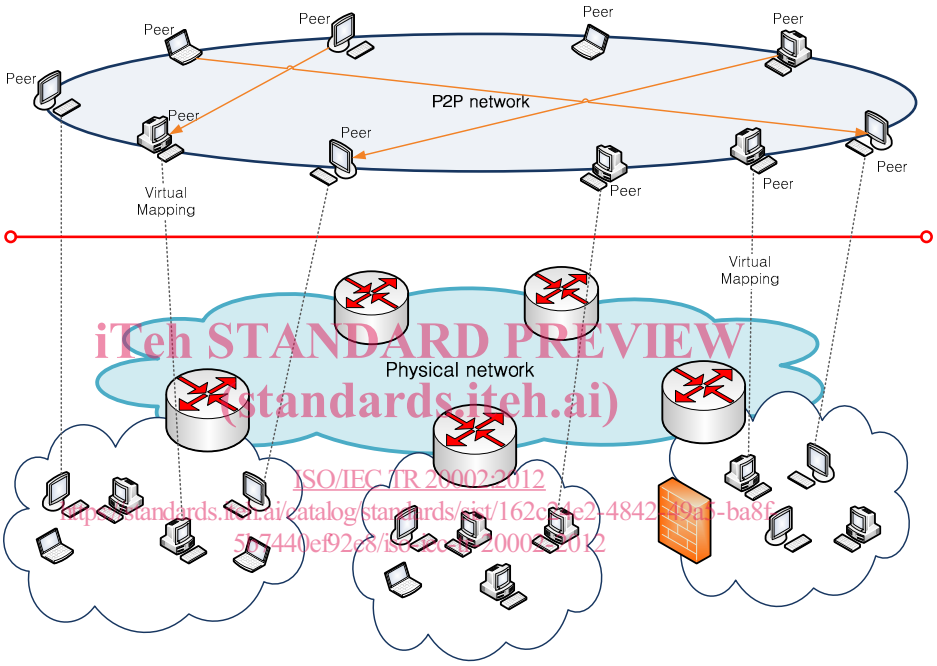

Figure 1 — P2P network

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