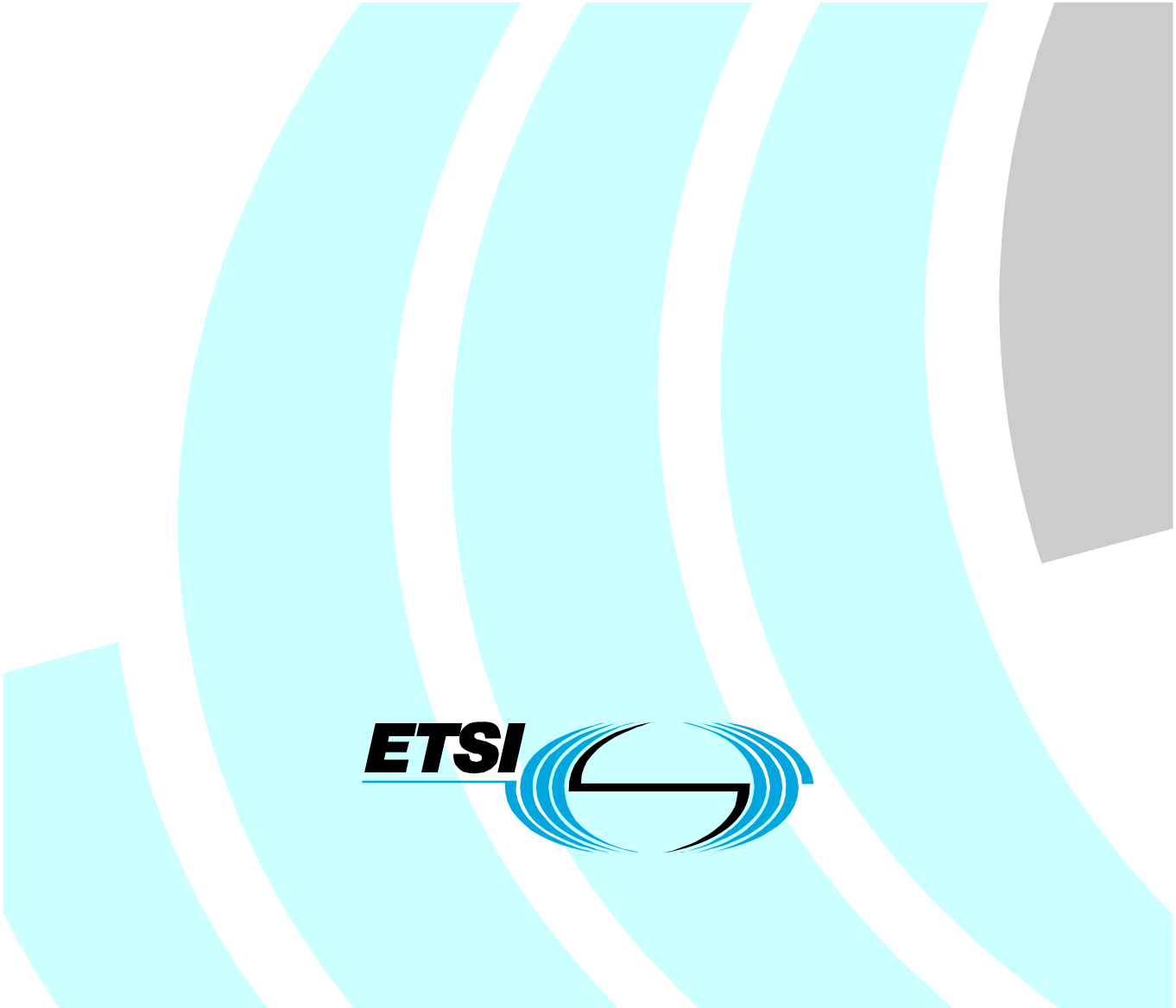
ETSI TR 182 010 V3.1.1 (2010-02)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Peer-to-peer for content delivery for IPTV services: analysis of mechanisms and NGN impacts



Reference
DTR/TISPAN-02075-NGN-R3

Keywords
analysis, IP, TV

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

Introduction

There is an ever growing demand for an ever wider variety of content and content services ("the long tail"). Content may originate from all over the world, both from professional content makers and home-recorded user-generated content. Roaming users may want to access the same content (BC channels and CoD) that they can access when they are not roaming. The number of available "television channels" will explode from several tens to several hundreds and more. The number of available titles in a content-on-demand library will grow from thousands to ten thousands or even more. There will also be a separation between the delivery of the (encrypted) content itself, which is a bulk process, and the trade of viewing rights using conditional access and/or digital rights management.

Peer-to-peer technologies are very effective for the delivery of streaming content further down the "long tail". However, peer-to-peer content sharing also has some drawbacks on network capacity availability, the free cash flow of ISPs and on customer experience due to slowed down throughput of broadband access and internet.

Peer-to-peer mechanisms could be interesting to IPTV providers in various ways.

- IPTV providers could offer peer-to-peer support as a service:
  - caching and distributing content on behalf of the user;
  - content management services for the CNG;
  - session support for peer-to-peer delivery:
    - identity management (UPSF);
    - quality of service control (RACS);
    - service attachment (NASS).
- IPTV providers could also use peer-to-peer mechanisms for distribution of content (optimization):
  - peer-to-peer delivery as alternative to static multicasting;
  - peer-to-peer mechanisms to distribute content over regionally distributed MDF;
  - peer-to-peer mechanism to have content be exchanged directly between UE or CNG, bypassing MDFs;
  - super-peer-based solution architectures for content caching optimization.

The TISPAN Release-2 IPTV architectures (TS 182 027 [i.1] and TS 182 028 [i.2]) do not support peer-to-peer mechanisms for content delivery. The basic assumption of the TISPAN R2 IPTV architectures is that all content originates from an MDF, without any further assumptions how the content gets there in the first place.

TISPAN may develop a broader view on the origins of the content, and define interfaces for content origination for example from:

- content providers;
- other IPTV Services providers; and
- users themselves.

Because of this broader view on the flow of content origins, it was considered useful to have a better understanding of the mechanisms used to handle, distribute and deliver the content, resulting in the present document.

1 Scope

The present document is an ETSI Technical Report which contains only informative elements.

The words "shall" and "must" used in the present document either refer to requirements defined in other documents or propose requirements that could be used later on in a document containing normative provisions such as a Technical Specification or an ETSI Standard.

The present document analyses peer-to-peer technologies for content delivery for IPTV services: use cases, requirements, architecture studies and other aspects.

The scope of the present document includes:

- Use cases and requirements:
  - Types of peer-to-peer mechanisms:
    - delivery of stored/off-line content;
    - delivery of streaming content.
  - Application of peer-to-peer mechanisms:
    - deliver content from IPTV Service Provider to Consumer;
    - share User-Generated Content (UGC) between users via the IPTV solution;
    - acquire content from third-party Content Providers by IPTV Service Provider;
    - manage content within the IPTV solution;
    - customer profiling based on traffic characteristics.
- Architecture studies:
  - topology analysis;
  - super-peer-based solution architectures;
  - impact on TISPAN IPTV network architecture;
  - impact on Customer Premises Network architecture.
- Other aspects:
  - network aspects, transport level;
  - security aspects, risk analysis;
  - legal aspects;
  - charging aspects;
  - indexing aspects ("naming");
  - concatenation of peer-to-peer ("NNI").

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] ETSI TS 182 027: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; IPTV functions supported by the IMS subsystem".

[i.2] ETSI TS 182 028: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN integrated IPTV subsystem Architecture".

[i.3] B. Carlsson; R. Gustavsson: "The Rise and Fall of Napster - An Evolutionary Approach" Proceedings of the 6th International Computer Science Conference on Active Media Technology, 2001.

[i.4] J Liang, R. Kumar and K.W. Ross: "Understanding KaZaA" Technical Report, Polytechnic University, New York, May 2004.

NOTE: Available at http://cis.poly.edu/~ross/papers/UnderstandingKaZaA.pdf.

[i.5] D.Brookshier, D. Govoni, N. Krishnan, J. C. Soto, "JXTA: Java P2P Programming", Sams Publishing, 2002.

[i.6] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker: "A scalable content-addressable network" Proc. of ACM SIGCOMM'01, pages 161-172, August 2001.

[i.7] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, H. Balakrishnan, Chord: "A Scalable Peer-to-Peer Lookup Service for Internet Applications", ACM SIGCOMM'01, 2001.

[i.8] The Gnutella Protocol specification.

NOTE: Available at http://www9.limewire.com/developer/gnutella_protocol_0.4.pdf.

[i.9] I. Clarke, Oskar S, O. Wiley and T. W. Hong, Freenet: "A distributed anonymous information storage and retrieval system", Designing Privacy Enhancing Technologies, Springer, DOI 10.1007/3-540-44702-4-4, 2001.

[i.10] J. Liang, R. Kumar, and K. W. Ross: "The FastTrack Overlay: A Measurement Study", Computer Networks, vol. 50, no. 6, pp. 842-858, Apr. 2006.

[i.11] Y. Chawathe, S. Ratnasamy, L. Breslau, N. Lanham, and S. Shenker: "Making gnutella-like p2p systems scalable" Proc. of ACM SIGCOMM'03, Augustus 2003.

[i.12] A. Rowstron and P. Druschel: "Pastry: Scalable, decentralized object location and routing for large-scale peer-to-peer systems" Proc. of 18th IFIP/ACM Conferenceon Distributed Systems Platforms, November 2001.

[i.13] Y. B. Zhao, J. D. Kubiatowicz, and A. D. Joseph: "Tapestry: An infrastructure for faulttolerant wide-area location and routing" Technical Report UCB/CSD-01-1141, UC Berkeley, April 2001.

[i.14] I. Abraham, A. Badola, D. Bickson, D. Malkhi, S. Maloo and S Ron: "Practical Locality-Awareness for Large Scale Information Sharing" Peer-to-Peer Systems IV, Springer, DOI 10.1007/11558989-16, 2005.

[i.15] M. Schlosser, M. Sintek, S. Decker, W. Nejdl, HyperCuP: "Hypercubes, Ontologies and P2P Networks", Springer Lecture Notes on Computer Science, Vol. 2530, June 2003.

[i.16] M. Castro, M. Costa, and A. Rowstron: "Should we build gnutella on a structured overlay?" ACM SIGCOMM Computer Communication Review, 34(1):131-136, January 2004.

[i.17] J. A. Pouwelse, P. Garbacki, D. H. J. Epema, and H. J.Sips: "The Bittorrent P2P filesharing system: Measurements and analysis", In 4th Int'l Workshop on Peer-to-Peer Systems (IPTPS), Feb 2005.

[i.18] E. Adar and B. A. Huberman: "Free riding on gnutella" Technical report, Xerox PARC, August 2000.

[i.19] N. Christin, A.S. Weigand, and J. Chuang: "Content availability, pollution and poisoning", In ACM E-Commerce Conference. ACM, June 2005.

[i.20] A. Parker: "The true picture of peer-to-peer filesharing", http://www.cachelogic.com, July 2004.

[i.21] S. Seetharaman and M. Ammar: "Characterizing and mitigating inter-domain policy violations in overlay routes", In Proc of ICNP, 2006.

[i.22] H.Xie, A. Krishnamurthy, A. Silberschatz and Y. R. Yang: "P4P: Providing Portal for Applications", In Proc. of Sigcomm 2008.

[i.23] Comcast's ISP Experiences In a P4P Technical Trial, draft-livingood-woundy-p4p-experiences-03.

[i.24] ETSI ES 282 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture".

[i.25] RFC 5693: "Application-Layer Traffic Optimization (ALTO) Problem Statement".

[i.26] EU FP7 Project NAPAwine: "Network-Aware P2P-TV Application over Wise Networks".

[i.27] ETSI TS 182 019: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Content Delivery Network (CDN) architecture - Interconnection with TISPAN IPTV architectures".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AF	Application Function
A-RACF	Access-Resource and Admission Control Function
ARC	Audience Research Collector
BC	BroadCast
BTF	Basic Transport Functions
CDN	Content Delivery Network
CNG	Customer Network Gateway
CoD	Content on Demand
CS	Content Server
CSBF	Capability and Service Binding Function
EPG	Electronic Program Guide
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
IGMP	Internet Group Management Protocol
IMS	IP Multimedia Subsystem
IPTV	IP Television
ISP	Internet Service Provider
MCF	Media Control Function
MDF	Media Delivery Function
MF	Media Function
NASS	Network Attachment SubSystem
NBAC	Network Based Application Control
NGN	Next Generation Network
NNI	Network Network Interface
NPTF	Network Pattern Triggering Function
OTT	Over The Top service
P2P	Peer-To-Peer
PASDF	Pattern Analysis and Service Discovery Function
PVR	Personal Video Recorder
QoE	Quality of Experience
QoS	Quality of Service
RACS	Resource and Admission Control Subsystem
RCEF	Resource Control Enforcement Function
RTSP	Real-Time Streaming Protocol
SIP	Session Initiation Protocol
SN	Super Node
SN-C	Super Node - Core
SN-T	Super Node - Tracker
SP	Service Provider
SPDF	Service-based Policy Decision Function
UE	User Equipment
UGC	User-Generated Content
UPSF	User Profile Server Function
URL	Uniform Resource Locator
VoD	Video on Demand

4 Overview of peer-to-peer

4.1 Network operator involvement in peer-to-peer

As the contributors to ETSI TISPAN are mainly network operators and their vendors, this Technical Report has expectedly a network-operator perspective. During this study, it became clear that there are many different perspectives that a network operator can look at "peer-to-peer". This is illustrated in figure 4.1.1. Notice that the business role of the "Network Operator" at the left gradually changes to "IPTV Service Provider" at the right.

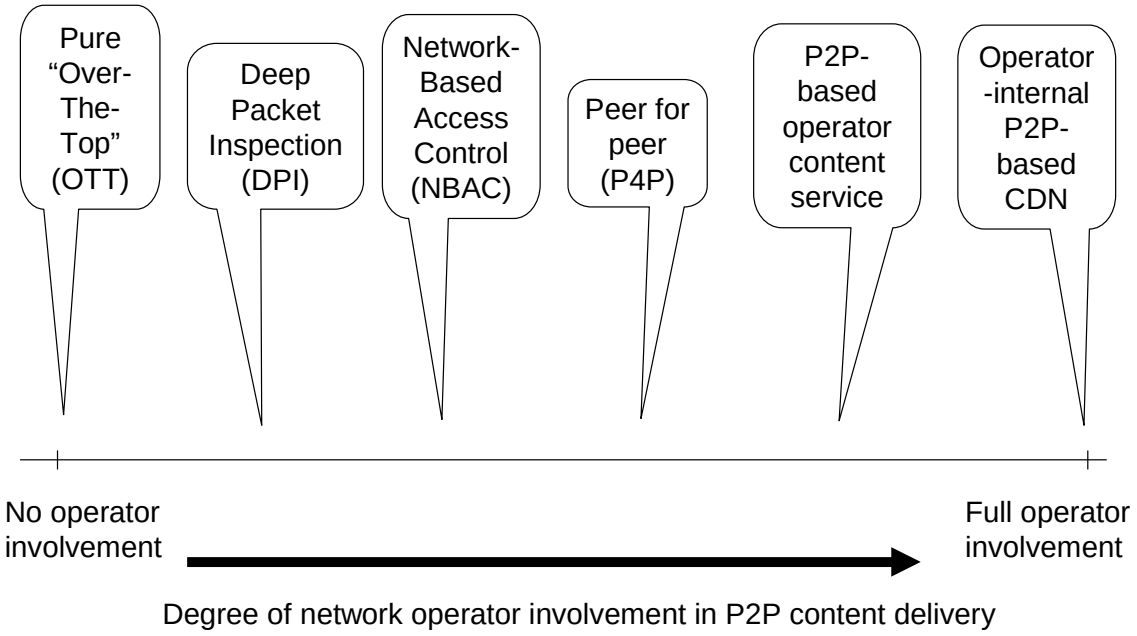


Figure 4.1.1: Many ways for an operator to look at "peer-to-peer"

First of all, P2P can be seen as a content-delivering application that runs over the top (OTT) of an operator network. From the operator perspective, P2P is than merely a use of their best-effort bit pipes.

Some network operators consider over-the-top P2P and other bandwidth-hungry applications as a threat to their network, as the P2P traffic may push aside other traffic and hence deteriorate the Quality of Experience (QoE) of those other services. Throttling the bandwidth-hungry applications by using Deep Packet Inspection is one of the approaches that network operators are considering and using.

The above threat may also be considered as a business opportunity to network operators. End users may be willing to reserve (and pay for) bandwidth guarantees for specific over-the-top applications in order to enhance their QoE. Network-Based Access Control (NBAC) technology is an example of technology in this area. NBAC is extensively described in the present document.

As a next step, network operators may try and get involved in the actual content delivery by the over-the-top application, e.g. by placing caches and stream replicators in the operator network. One initiative in this area is P4P, which is also described in the present document. P4P provides network operators an additional degree of freedom of investment, which can be in transport capacity, but now also in content delivery technologies.

Network operators may also decide to operate their own P2P-based content delivery system, using end-user equipment (UE) to cache and upstream content.

Finally, peer-to-peer technology may be considered a solution to implement large content delivery networks within an operator network. By enabling Media Functions (MF) to exchange mutually content, this reduces the load on the content sources and distributes traffic more evenly over the network.

4.2 Peer-to-peer in a network-operator CDN

In an IPTV system, the large size media contents normally vary from hundreds of megabytes to gigabytes and even above. As a result, network bandwidth and storage capability are facing higher requirements.

Figure 4.2.1 shows a traditional Content Delivery Network (CDN) with a centralized architectures and hierarchical layers. When the edge server receives a request from any UE, it will transfer the UE request to the central server when it exceeds its process capacity. With an increasing number of UEs, the burden on the central server will be becoming even heavier, and user experience will be badly influenced. The system will have to deploy more and more edge servers closer to UEs to provide better service. How to reduce the cost of the IPTV Service Provider, and how to improve user experience becomes crucial.

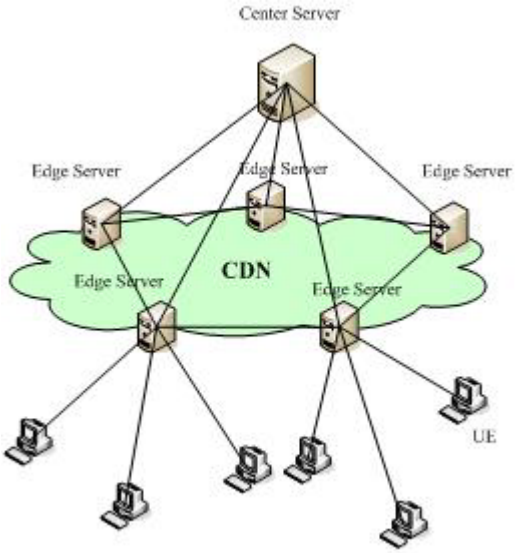


Figure 4.2.1: A traditional Content Delivery Network

Peer-to-peer technology is a way to overcome this problem. By sharing the capacity between different edge servers in a P2P network, more requests can be processed without reaching the central server.

Figure 4.2.2 shows how, when an edge server receives a UE request and it cannot serve it locally, instead of transferring the request to the central server, it searches for the requested content within all edge servers of current layers. It will transfer the request to central server only if none of the neighbouring edge servers do not have the requested content in storage.

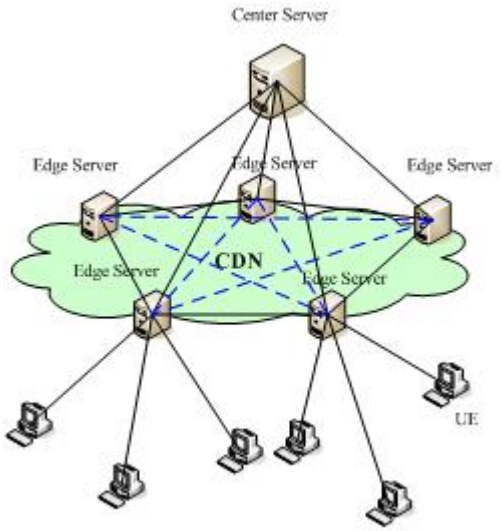


Figure 4.2.2: Using P2P within the CDN

Figure 4.2.3 shows the deployment of P2P technology in the user premises network. UEs can share media contents as well as their aggregate processing capacity, memory and disk storage with each other. This way the UEs can achieve a better Quality of Experience (QoE) for the user.

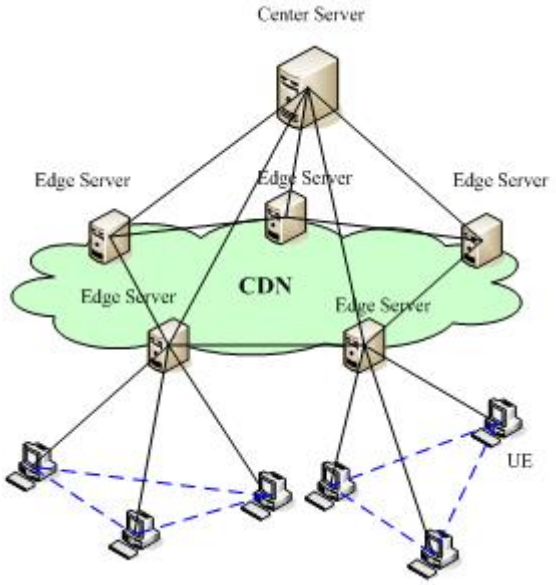


Figure 4.2.3: Using P2P within the user premises networks

5 Use cases and requirements

5.1 Use cases

5.1.1 Delivery of stored/off-line content

Peer-to-peer technology can be used for the delivery of stored/off-line content. As this is a classic P2P use case, it has not been worked out in more detail.

5.1.2 Delivery of streaming content

Peer-to-peer technology can be used for the delivery of real-time streaming content. The following use case is an example of this.

It is Olympic Games time, and millions of people want to watch the live final football game. Gradually, more and more people join the watching queue, but unfortunately, the network provider cannot provide access to multicast functionality. In this scenario, as servers become overloaded, the Quality of Experience (QoE) for the end user deteriorates. An alternative solution to the operator is using application level multicast based on Peer-to-Peer technology. Application level multicast can even improve the QoE with increasing numbers of UEs.

5.1.3 Time-shift TV

Peer-to-peer technology can be used for Time-shift TV. The following use case is an example.

It's 8 o'clock in the evening. Alice is watching a live football game and Rose is watching the same program at the same time. Suddenly the famous football star, Ronaldo contributed an excellent goal. Alice watched the fantastic scene again by using Time-shift TV functionality, almost at the same time that many football fans were also watching again that scene. Everyone can share the hot goal content by using peer-to-peer technology.

NOTE: User consent is required to make recorded content available for retrieval by other users.

5.1.4 Metadata exchange

Metadata is similar to other types of content. P2P solutions may be used to deliver metadata.

5.1.5 Deliver content from IPTV Service Provider to Consumer

An IPTV Service Provider can use a P2P solution to deliver content to Consumers.

5.1.6 Share any type of media/MIME type between users via the IPTV solution

Not only audio or video, but any type of content may be shared and/or distributed through a P2P solution.

5.1.7 Acquire content from other than own third-party Content Providers by IPTV Service Provider

Peer-to-peer technology is not limited to a single administrative domain. Different parties may collaborate to share some of the content-delivery burden. The following use case is an example of this.

A user requests its IPTV Service Provider for some specific IPTV content: broadcast (BC), content-on-demand (CoD) or other. The requested content happens not to be presented in the IPTV Service Provider's own network, but is available at another service provider with which the IPTV Service Provider has a business agreement. The IPTV Service Provider retrieves the requested content from the other service provider and delivers it to the user.

5.1.8 Manage content within the IPTV solution

Content management is an important aspect of content delivery, albeit with or without based on P2P solutions. Content management is not worked out in detail in the present document.

5.1.9 End user contribute capacity to CDN

Peer-to-Peer technology can keep the usage of sever resources stable when the number of UEs increases. The following use case is an example of this.

Current solutions for VoD service use a hierarchical content delivery network (CDN). The bandwidth of these servers constitutes a bottleneck in the system because they can only deliver content to a certain number of UEs at the same time. If the number of VoD requests increases over time, the capacity of these servers needs must to be upgraded to serve all the requests. In addition, if the number of UEs requesting certain content inexpertly, the server may overload.

VoD UEs usually implies a large buffer space at the UE and with P2P technology it can be exploited in order to use this buffer space for direct content distribution among same requests within the users. Compared to a hierarchical approach, a single server can deliver VoD content to more UEs while keeping the same QoE guarantees by using P2P technology among the users.

Overall, this use case does not necessarily imply a replacement of traditional VoD content delivery but rather an enhancement by means of P2P data exchange among UEs in order to achieve serving a higher number of content requests with the same capacity of the CDN in the core network.

5.1.10 Server capacity sharing

Operators deploy several edge servers in one local domain, each responsible for a fixed number of UEs, for example 500. But the content stored in each edge server is not exactly the same. When one UE sends a request to edge server A, edge server A may not contain the required content. Edge server B may contain the required content, but it is lacking processing capacity for streaming. Normally, in such case the request would be refused. However, this changes when the operator applies Peer-to-Peer technology, which enables edge server A to process the content that is stored in edge server B.

5.1.11 Economical use of resources

Most users tend to watch only the beginning of a program. If they do not like it, they may switch to another channel or to other programs. So the first part of content is often more popular than later parts of the content. Operators find it a great waste of bandwidth, storage, etc. if the whole content is delivered to many edge severs. Peer-to Peer technology always segments the full content first, and then transfers the content slice by slice. Operators are interested in this segment mechanism, which enables them to delivery only the first part of some content to most of the edge servers, while delivering other parts of the content to a smaller number of edge servers.

5.1.12 Efficient content delivery

Normally, an operator deploys a hierarchical Content Delivery Network (CDN) to distribute content. When a new content item is published, edge servers should download the full content item from a central server one by one. This procedure is very time consuming. Operators find that the procedure becomes much more efficient by applying Peer-to-Peer technology, which enables edge servers to mutually exchange different parts of the content while independently getting other parts from the central server.

5.1.13 Content delivery in case of low bandwidth

In some remote rural areas where there is a satellite or radio network accesses (usually slow and expensive), the use of P2P technologies can improve the way the operator serves multimedia on-demand content.

A typical use case is a rural area where a small number of users are connected to a broadband network using a number of satellite accesses. For VoD scenarios is probable that the same content could be delivered to several satellite accesses using a high amount of bandwidth. This scenario could be improved if subscribers are connected to a local area network (wired, WiFi, etc.) and P2P technologies could be used.

The network operator can improve the use of the expensive and scarce bandwidth satellite access using a P2P approach. This use case allows two approaches:

- User P2P: where a user serves contents to other users.
- Operator P2P, where all on-demand content requested by a user to the network is stored at a local element property of the operator.

In both cases, when a second remote user asks for the same content, it is delivered inside the local broadband network, instead of using the satellite access.

5.1.14 Flexible distribution of content

Peer-to-peer technology can achieve wide and flexible distribution of content without placing an excessive burden/load on the content source. The following use case is an example of this.

EXAMPLE: *Alice makes a funny home movie and places it on her own small webserver. She sends a reference to the home movie to her friends, among others Bob. Bob really likes the home movie and sends a reference to many of his friends, among others Carl. Carl also likes it and forwards the reference again. In a short period of time, several ten thousand people want to see Alice's home movie. Despite the large demand, Alice's webserver stays up and all interested people can obtain the home movie in a reasonable time.*

5.1.15 Network Based Application Control Use Case

"Network Based Application Control" is the concept based on which the network notifies the NGN control functions through specific triggering mechanisms - about the activity of users accessing some services/applications, enabling new services.

From this point of view, the network traffic becomes an important source of information and permits, thanks to the capabilities/features enrichment, the creation of new services and new business opportunities.

In other words, the network should be able to recognize specific user session's chunks of traffic, to autonomously take decisions, and/or to report towards the control functions. An example of use of this mechanism is the monitoring and the improvement of the offered quality of service, with the purpose of increasing the overall customer satisfaction. This new Network-Triggered control approach could be applied to both trusted services (i.e. services directly provided by the operator) and un-trusted/OTT (Over The Top) services (i.e. Internet TV, Internet VoD, etc.).

The general schema for this approach is the following one:

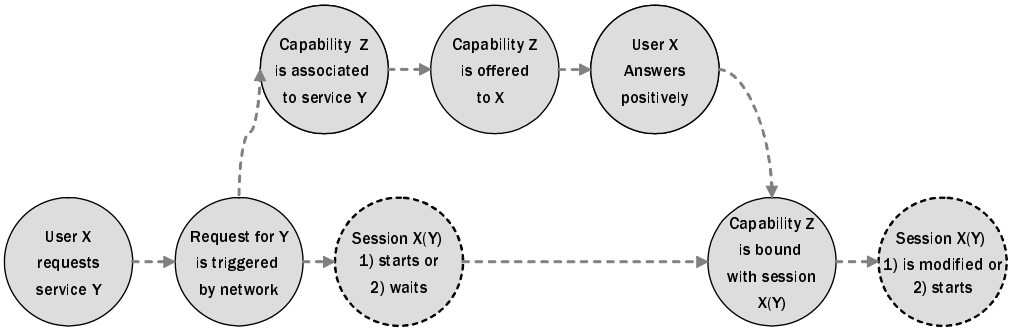


Figure 5.1.15.1: General schema for NBAC

In this model, the role of the control functions is to associate (e.g. using a RACS) the appropriate policies to the specific flow and to install them in the network.

In addition to the traffic originated by legacy services, such as e-mail, FTP and classical Web browsing, in the last years there has been a big growth of traffic associated to services related to the "Web 2.0" phenomenon. These services are based on concepts and technologies like social networking, Wiki, Podcasting, blogging, Web-TV, and so on. Common characteristic for this type of services, and especially for the content-based ones, is the high volume of exchanged traffic, due to their high interactivity grade.

Some famous examples are: video content sharing portal, social networking portal, photos sharing portal, collaborative encyclopedia and content distribution system P2P-based.

The Network Based Application Control mechanism enables the association of network capabilities to a generic user's session. In particular the Network Triggered approach allows to associate an appropriate QoS to particular services including the peer-to-peer services in which operators do not take directly part (OTT services), such as peer-to-peer IPTV services.

From an operator point of view two possible scenarios could be defined.

1) if business relationship exists between the operator and the OTT SP, hence on a partnership base, the network operator can apply the agreed capabilities to the streams coming from the OTT SP's peers, even on a policy base (i.e. notified off-band by the OTT SP) and accordingly with the resources availability.
NBAC applies notifying to RACS any stream coming from OTT SP's peers;

2) if no such business relationship exists, in this case the Network Based Application Control allows to identify single service flows and to notify them to the RACS, enabling the operator to offer a controlled QoS to the customers based on the operator business relationship with the customer.

For example (2nd case), considering a generic content - Over The Top - provider, the Network Based Application Control allows to move from the current "best effort" model, that so far is the only possible solution, to a QoS enabled model.

Using a Network Based Application Control approach, an operator is able to:

- Provide QoS to the user.
- Activate triggering on the services (e.g. content provider) for which the user has subscribed the QoS enable model.
- Perform admission control on triggered events.

Peer-to-peer interaction model can be extended from one-to-one (typical client-server) to many-to-many, where a peer is able to receive/send different parts of the requested content from/to many other peers.

NBAC could be indeed applied even considering the increase of triggering job useful to notify to the RACS the different data streams reaching the peer; specific policies on the RACS, managing the aggregated notifies, will influence the behaviour of the enforcement accordingly to the QoS service interacting with AF.

NOTE 1: Other client-server services can benefit from the use of the Network Based Application Control approach to apply QoS to data flows, for example **Data Management and Backup Services** and **Online gaming and metaworlds**.

NOTE 2: The general scope of the present document is to cover different aspects of peer-to-peer technologies applied to content delivery including network operator involvement. Within this wide spectrum of analysis, the NBAC concept and its network triggered approach is an example of how a network operator may be involved in handling peer-to-peer IPTV services.

5.1.16 Customer Profiling Use Case

During last years a lot of internet advertising companies have been created. Generally they use user Internet navigation tracking systems to build users' profiles based on which they can provide targeted advertising. This particular way of providing advertising, specifically addressed to the user on the basis of its previously traced navigation profile, is generally known as Behavioural Targeting.

Even if these platforms are very complex, they have an intrinsic limit: they can trace the user's navigation only through the sites that are affiliate to their commercial communities, generally known as Advertising Networks.

In this scenario, the "Network Based Application Control" enables to massively collect users' Internet navigation information, thanks to the possibility of tracing the network activity of each single user. In this way, the user profiling coverage overcomes the limits of a specific Advertising Network.

In addition to the browsing activities tracing, Network Based Application Control allows, using Deep Packet Inspection devices, to trace other applications (e.g. Instant Messaging, Email, etc.) and permits a deep analysis of cross-application relationships in a generic user session ("cross-media-user profiling"). Again in this case deep-packet inspection devices are used to recognize a set of protocols and notify events to a system able to aggregate them to profile users individually or by groups.

A particular case of the Customer Profiling is to analyze Web browsing on IPTV services. For In this case it is crucial to refer to the concept of clickstream, as defined in Web Usage Mining environment: clickstream is a sequence of Web Page requests, i.e. of visual rendering of single Web Pages in a specific client environment (e.g. a single instance of Browser) during a specific period of time.

Clickstream detection is a fundamental capability for Network Based Customer Profiling, because within the enormous number of HTTP requests generated throughout the user web activity, it allows to focus only on the interested URLs.

Using ClickStream instead of raw web traffic greatly reduces the number of requests to be analyzed, making the Network Based Customer Profiling a scalable solution.

The user profiling for these services can be done in different ways:

Individually or by groups, according to the type of information that is extracted from the raw data, grouping or not the information obtained for clusters of users, for example with data mining techniques:

- anonymously or explicitly, depending on the opportunity to associate the extracted information to a user's;
- historically or usable in real-time, depending on the retention of data (Data Ware-House) or the possibility to use them in real time.

The customer profiling is a significant source of information for data mining systems.

The mechanism described above may help to answer questions such as:

- Which groups of content are seen by users as a result of a search?
- Which queries have reached the expected result?
- Which contents the user prefers?
- Which are the typical paths of vision?

- Which are the types of content (categories) in the visited sites?
- When is the purchase of a content triggered?
- Which web sites are visited more frequently in searching for contents?

or to provide customer based advertising.

5.1.17 Peer-to-peer Content Download

Peer-to-peer technology can be used for content download. The following use case is an example.

Bob and John live in the same building and both of them like football games every much. One day Bob records the Europe 2008 final football game by C-PVR. John missed that game for some reason. The next day, when John opens his UE to view the game, John's UE can download the game content from Bob's UE quickly if Bob contributes his UE capacities to the peer-to-peer network.

5.1.18 P2P usage for non subscription based services

Beside the dedicated services there are also non subscription based multimedia services (e.g. web platforms to share user generate content) which attract a huge group of users and which is the source of a huge workload on the networks.

To overcome the problem of current deployments provide caching servers in the operator network to serve all the request and provide a good QoE. These traditional caching servers can become quite expensive because they are out of control to the network operator and must scale with the amount of multimedia provided the non subscription based services.

One solution to aid the network based caching is to use P2P technology among the peers, that they can be used as distributed caching entities and distribute the volatile content among each other.

5.2 Requirements

5.2.1 Segmentation

In P2P networks, every peer contributes its aggregate processing, memory and disk storage, and other, so that one peer is able to obtain content from any other peers. For example, there is a media content named "Program A". It is required that the peer must have program A available, in order to be able to distribute it.

The most obvious method is that every peer stores the whole content of Program A independently, so it can work using P2P mechanism. Obviously that is not a smart choice. So we introduce the segmentation mechanism, which splits Program A into different segments, and each peer only stores some of those segments. As a result, one peer can obtain segment 1 from peer A, segment 2 from peer B, etc. until it has obtained all segments.

So the p2p solution should support segmentation.

For CoD services, the Program A is inserted into the IPTV system as a whole. Program A is then segmented into many segments by using P2P technology, and made ready to be delivered to one or several network nodes (peers). Next these segments are shared over several peers. When a user wants to watch and selects Program A, the system will find all segments of the program and presents it to the user.

So the p2p solution should support offline segmentation.

For live services, the content is gathered and inserted into IPTV system in real-time. Segmentation and delivery must be done as quickly as possible. It is different from the offline segmentation, because live services usually use memory storage to store shared segments, whereas CoD services can use disk storage to store shared segments. Memory is more expensive than disk storage. Typically, live services needs more fine segmentation, and it requires a high real-time segmentation mechanism.

So the p2p solution should support real-time segmentation.

5.2.2 Segments indexing

When a Media Function (MF) is using segmentating, a whole media file becomes many segments, and these segments may be distributed and stored in more than one node (peers). When a user wants to see the media program and select it, the MF must decide where the first segment exists, and then MF sends first segment to the UE. Before the first segment is played to the end, the MF must find the next segment and send it to UE when the first segment comes to an end. And so on.

The procedure for an MF to search for the location of a certain segment is called segment indexing. It may be implemented by creating a lookup table in the MF, just like database table, and this lookup table maybe create an index on keywords, for example the program name. It needs effective and efficient methods to create and search this kind of indexing table for real time service.

The p2p solutions should support segments indexing.

5.2.3 RACS requirements

The Network Based Application Control (NBAC) is based on extracting from the service traffic specific signals (e.g. content request, start, stop) and on sending them to the RACS.

For such interactions, the current RACS mechanisms should be extended in order to allow the identification of the correct capability (or set of capabilities) to be activated.

[R.1] The RACS shall be able to associate an appropriate set of capabilities to particular events and derive and install appropriate policies in the network for flows not directly controlled.

5.2.4 Transport processing function requirements

[R.2] Clickstream analysis: Transfer processing functions shall support features based on NBAC to monitor and identify network traffic in a smart way, to detect flows and patterns related to transmission protocols, services and applications.

[R.3] Network triggering: Transfer processing functions shall support the notification of the events generated by the clickstream analysis toward RACS.

5.2.5 Segments switching

5.2.5.1 Background

A media file can be divided into many segments, and these segments may be distributed and stored in more than one node (peer). As shown in the example of figure 5.2.5.1.1, eight segments of one program are distributed among three nodes: the first and second segments are in Node A, the third and fourth segments are in Node B, and the last four segments are in Node C. Here the Node is equal to MF.

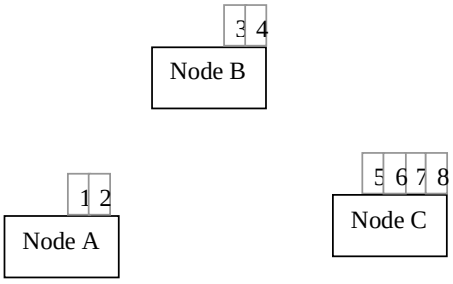


Figure 5.2.5.1.1: Distributed storage of segments

When a user selects media content that he wants to watch, the UE contacts a Media Function, e.g. one of the nodes shown in figure 5.2.5.1.1. This node locates the first two content segments by querying indexing functionality, Node A in this example. When triggered by the UE request to play, Node A sends the first two segments to the UE to play.

Before the first two segments is played to end, the next segment is found in Node B via indexing functionality, and it switches to Node B, so UE can watch the whole program as if it is coming from the same one node.

The following clauses present some possible ways for a UE to obtain the right content segments at the right time. In all figures, the red lines refer to media flows, whereas the blue lines refer to signalling flows.

So the p2p solution should support the switching among segments.

5.2.5.2 Proxy mode

The first way is described in figure 5.2.5.2.1. Before Node A finishes sending the first and the second segments to UE, Node A gets the third and fourth segments from Node B. Right after finish sending the first and the second segments, Node A starts sending the third and fourth segments to the UE. In this case, the Node A acts as a proxy, pulling subsequent content from other nodes and pushing it to UE. The process of pulling and pushing are happening in parallel inside Node A.

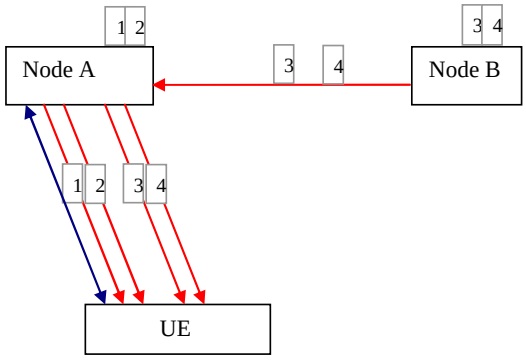


Figure 5.2.5.2.1: Segments switching in proxy mode

5.2.5.3 Server negotiation mode

The second way is described in figure 5.2.5.3.1. Before Node A finishes sending the first and the second segments to UE, Node A notifies Node B to start sending the following content segments to the UE at a certain switching point in time. In this case, maybe Node A and Node B are both sending content segments to UE for a short interval during the process of switching. The signalling channel (e.g. RTSP) between UE and Node A will be kept open during the playing process of the whole program, and any VCR commands are transferred through Node A to Node B. So Node A would act as proxy only for control messages, but not for the content segments.

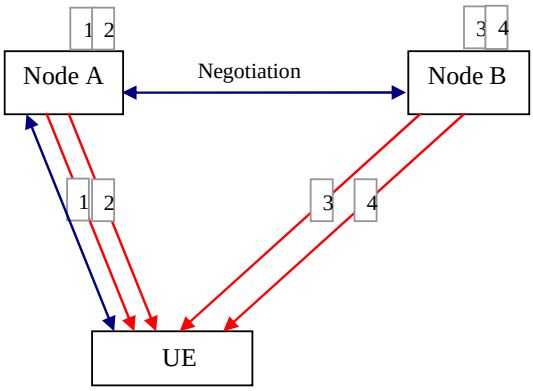


Figure 5.2.5.3.1: Segments switching in server negotiation mode

5.2.5.4 Client involved mode

The third way is described in figure 5.2.5.4.1. Before Node A finishes sending the first and the second segments to UE, Node A tells UE that the following content segments are located in Node B. After that, the UE establishes new signalling and media channels with the Node B. In this case, UE must have the ability of caching contents locally. When Node A stops sending content segments to the UE, the signalling and media channels between UE and Node A will be released.

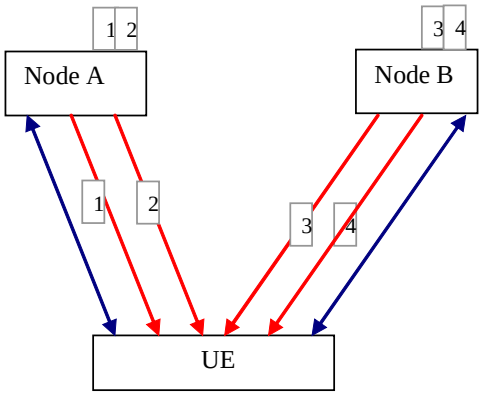


Figure 5.2.5.4.1: Segments switching in client involved mode

5.2.6 Requirement about peer management

In peer-to-peer overlay networks, the peer who acts as client peer must get segments of a content from other peers that act as server peer in the procedure of content distribution or delivery. To select a server peer providing required segments of content, the client peer should not only be aware which server peers contain required segments, but also the status of those server peers. This status includes online/offline, available bandwidth, processing capacity, etc.

The mechanism used to manage status of peers may be different according to the architecture of the peer-to-peer overlay networks. In centralized architecture, each peer may announce its existence to the central index server when it start-up. After that the central index server may interact with these peers to keep an accurate view of status of peers. In a distributed peer-to-peer architecture, the client peer may find on-line peers by itself and makes this kind of interaction with all peers providing contents to itself during the service procedure.

So the peer-to-peer solution shall support effective mechanism(s) to manage the status of peers which includes the discovering their existence, network bandwidth, stored content, etc.

6 Architecture studies

6.1 General

Common for all peer-to peer architectures is that the actual data transfer always takes place between the peer offering the file and the peer requesting it. However, the control plane can be designed and implemented in different manners. According to the degree of their centralization, peer-to-peer networks can be classified as centralized (e.g. Napster [i.3]), super-peer (e.g. KaZaA [i.4]), fully distributed (or "pure") and hybrid (e.g. JXTA [i.5]). Pure peer-to-peer networks do not use central server, except for logging-on to the network. They can be structured (such as CAN [i.6] and Chord [i.7]) or unstructured (like Gnutella [i.8] and Freenet [i.9]). More details on each class of these systems can be found in the remainder of this clause.

6.2 Centralized peer-to-peer architectures

In centralized peer-to-peer architectures, there is a central server facilitating the interaction between peers by maintaining directories of metadata. These directories describe the shared contents stored by the peer nodes. Although the end-to-end interaction and contents exchange may take place directly between two peer nodes, the central servers facilitate this interaction by performing the lookups and identifying the nodes storing the contents.

Obviously, in this scenario, the central server becomes the greatest weakness. This typically makes the whole system poorly scalable.

6.2.1 Description

Figure 6.2.1.1 shows a centralized and hierarchical Content Delivery Network (CDN).

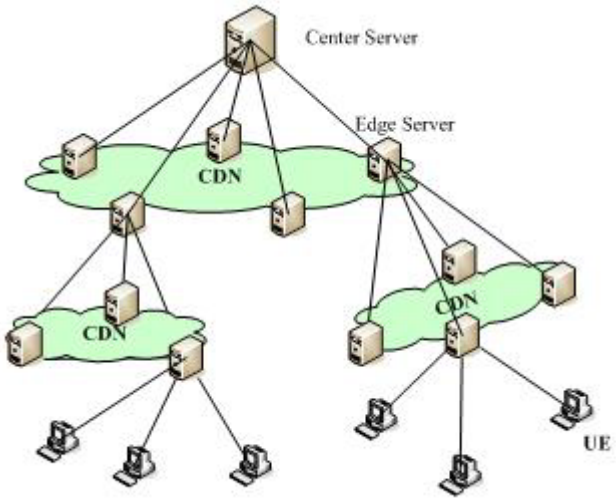


Figure 6.2.1.1: Centralized and hierarchical layers CDN

In order to support the peer-to-peer mechanism, indexing functionality is introduced in each layer. Figure 6.2.1.2 shows this indexing functionality in the different hierarchical layers.

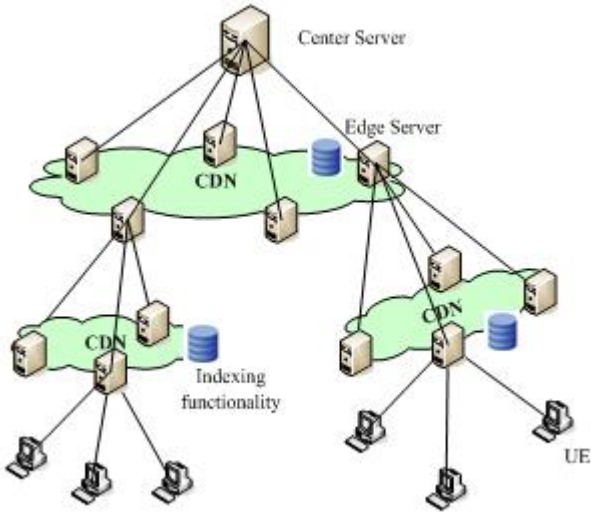


Figure 6.2.1.2: Centralized and hierarchical layers CDN with P2P

Figure 6.2.1.3 shows a single layer for better understanding. The indexing functionality may act as a separated node, or as part of server functionality. The black lines in figure 6.2.1.3 represent the original media content flows between the edge server and its upper edge server, same as in the traditional content delivery networks. The red lines in the figure represent the signalling control flows between peers and indexing functionality. The green lines represent the media content flows between peers. The indexing functionality controls all metadata within the layer, and it is responsible for the entering and exiting of peers in the layer.

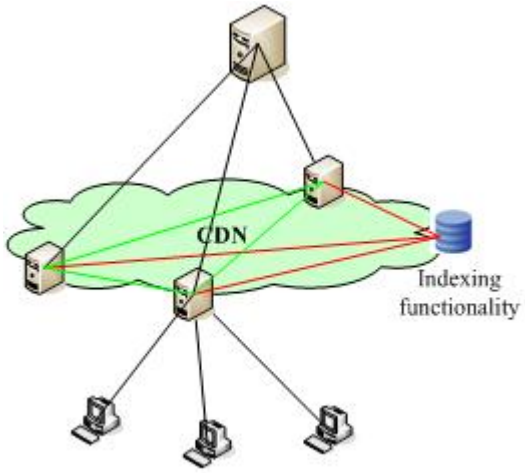


Figure 6.2.1.3: Centralized and hierarchical layers CDN with P2P for single layer

Figure 6.2.1.4 shows using P2P speeds up the content delivery. When the content is delivered from a high layer server, the peers can share their content with each other at the same time. For the traditional CDN network, when a new content is inserted into the system, every lower server has to get one copy from its upper server. However, with P2P technology, some lower server get first part of the whole content and other server gets second part of the content, then they can share with each other.

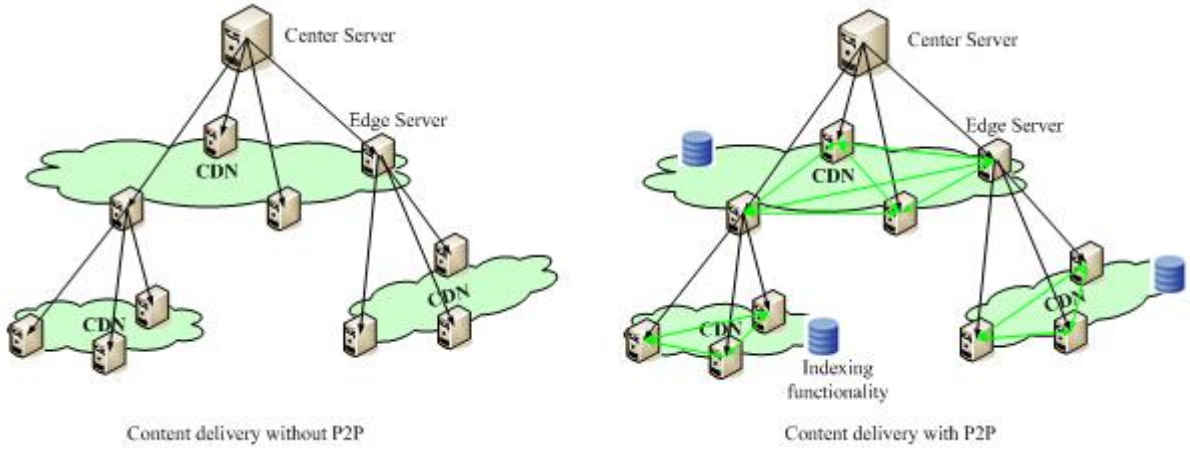


Figure 6.2.1.4: Content delivery flows with P2P and without P2P

Using P2P saves storage space. Each node only needs to store parts of the whole content, and it uses P2P mechanism to share them in the same layer. Only "hot" (very popular) programs are stored in the edge server. For example, most of the users tend to see the beginning of a program. If they do not like it, they may switch to other channels or other programs. There for only the beginning segments need to be stored in each edge server to fit this kind user behaviour.

Figure 6.2.1.5 shows the procedure for content request. When an edge server gets a request from a user about some certain program, it first searches for it itself and it responds to the user at once if it is found. Otherwise, it will use the indexing functionality and try to get the information within all the edge servers of the current layer. Response would be returned to the user once the desired information is found. If none edge servers in the current layer has the program in storage, the request will be transferred to the next high layer. The same process is repeated in that layer.

Comparing with the procedure of content request in the traditional content delivery networks, using P2P reduces the burden of central server.

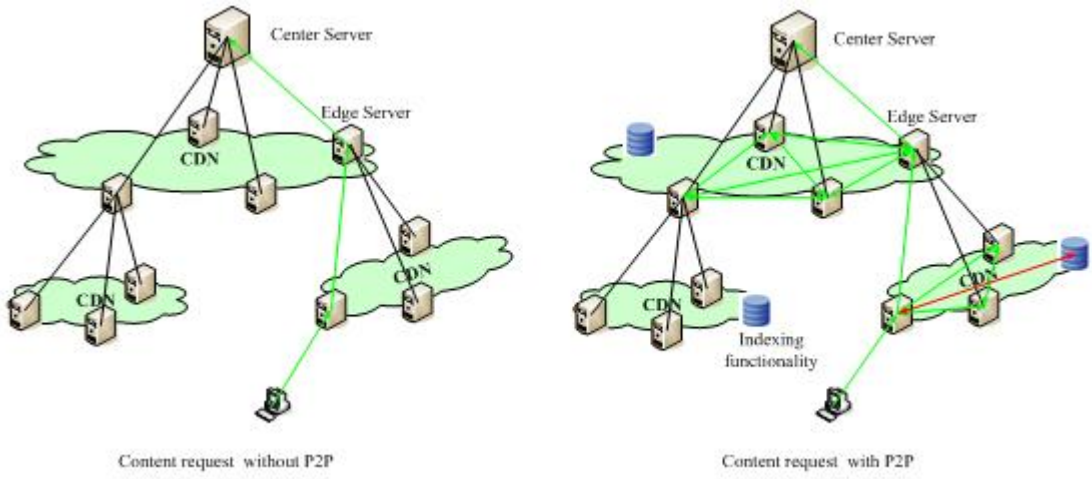


Figure 6.2.1.5: Content request flows with P2P and without P2P

6.2.2 Strong points

Centralized architectures have two strong-points. Firstly, they are easy to control, as all content requests are centralized. Therefore it is easy to apply monitoring and policies on user behaviours. And it is easy to control the content within in the networks. Secondly, they have effective searching. When a peer receives a request for certain content, if it cannot find that content, it only needs to ask the indexing functionality within the P2P networks. For other kinds of P2P architectures, further steps for finding the content will be needed.

6.2.3 Weak points

Centralized architectures also have weak points. The first one is that, when the number of peers is becoming too high, the indexing functionality becomes the bottleneck for the system performance. Then it becomes a problem to scale the network and add more nodes. The second weak point is that the indexing functionality must be high reliable.

6.3 Super-nodes based peer-to-peer architectures

6.3.1 Introduction

In super-nodes based peer-to-peer architectures, there are many domains. Within each domain, the central architecture is adopted. Each domain has a special and more important node named "super nodes", which acts as the local index for contents shared by local peers. And many super nodes from different domains would be connected using a decentralized peer-to-peer architecture network.

6.3.2 Description

Figure 6.3.2.1 shows a super-nodes based peer-to-peer architecture.

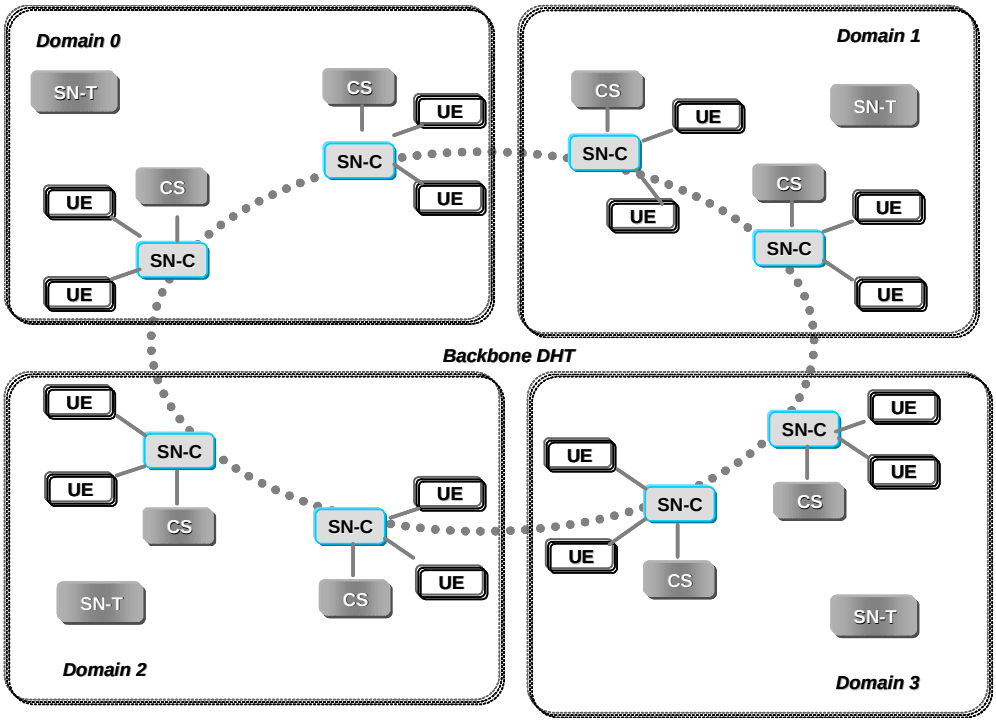


Figure 6.3.2.1: Super-nodes based P2P architecture

The architecture consists of multiple domains. Each domain performs independent management and independent operators. Each domain is constituted by SN-C (Super Node - Core), CS (Content Server), and terminal nodes UE. Each domain performs the storage and discovery of resources index via the DHT constructed by SN-Cs. Domain 0 can be used as a special domain, which performs pre-distribution of content to the CS of other domain by push method. P2P Content sharing within each domain is provided between CS and CS, UE and UE, CS and UE. The content sharing between other domains relies on pull download by local domain CS from other domain CS.

Super node includes core super node SN-C and track super node SN-T (Super Node - Tracker).

The function of SN-C includes:

- Constructing P2P network, storing and querying programs information, achieving global resource sharing.
- Saving the resource status information of local UE and CS, achieving resource discovery and query.
- Directing CS to obtain the content from other domain when the content is not found in local.

The function of SN-T includes:

- Directing SN-C to join service P2P network as a bootstrapping node.
- Managing local SN-C and CS.

The function of CS includes:

- Caching media data of broadcast and VoD services, providing streaming data download and streaming data for local UE. When in broadcast, providing the data transferring function of high speed node. When in VoD, buffering data demand to the local hard disk, so as to reduce the reading pressure of content server.
- Upon receiving a request, providing video data for other domains.
- As a peer, periodically reporting its status information to SN-C.

6.3.3 Super-nodes based peer-to-peer architecture interface description

Below there is a brief description of the interface for super-nodes based peer-to-peer architecture shown in clause 6.3.2.

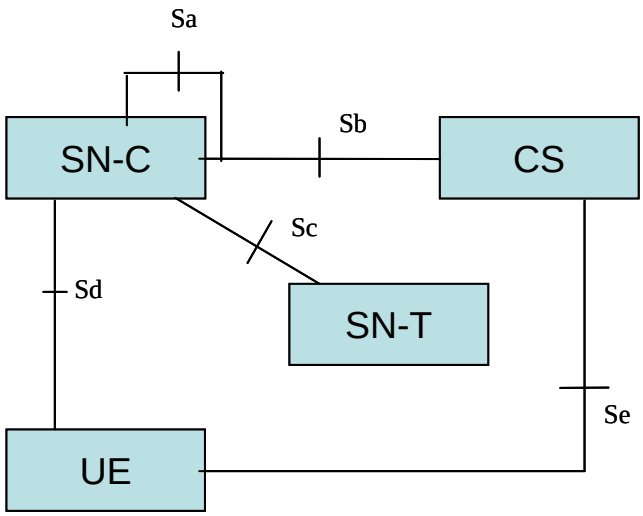


Figure 6.3.3.1: Super-nodes based P2P architecture

The system is illustrated in figure 6.3.3.1. It includes the super node (SN), the user equipment node (UE), and the cache server node (CS). The super node is divided into the core super node SN-C and the track super node SN-T.

The interfaces of system entities are defined as following:

- Sa: the P2P overlay interface between SN-Cs which is used to construct and maintain the P2P overlay network using DHT.
- Sb: the interface between SN-C and CS, realizing the functions of CS status information reporting and media data pull downloading from other domains.
- Sc: the interface between SN-C and SN-T for management and P2P overlay bootstrapping purpose.
- Sd: the interface between SN-C and UE, realizing the functions of UE status information reporting and resource information list obtaining.
- Se: the interface between UE and CS, realizing the functions of downloading media data from CS for UE.

6.3.4 Super-nodes based peer-to-peer architecture service flow diagram examples

Below there is a brief description of the service flow for super-nodes based peer-to-peer architecture shown in clause 6.2.1.

6.3.4.1 P2P media streaming request procedure in intra-domain

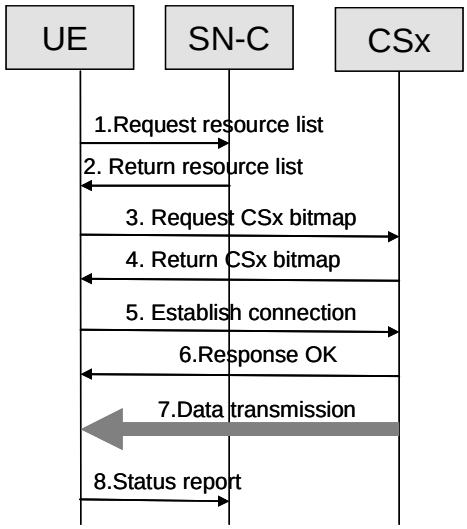


Figure 6.3.4.1.1: P2P media streaming request procedure in domain

1. UE sends request to SN-C to watch its selected video stream.
2. SN-C returns a resource list to the UE including a list of the address (es) of one or multiple CSx.

3.-4. UE sends requests to each CSx and obtains the bitmaps of pieces exchange from CSx respectively.

5.-7. UE downloads resource pieces from CSx after shaking hands with CSx.

8. UE regularly reports resource information and state information to the SN-C.

6.3.4.2 P2P media streaming request procedure between domains

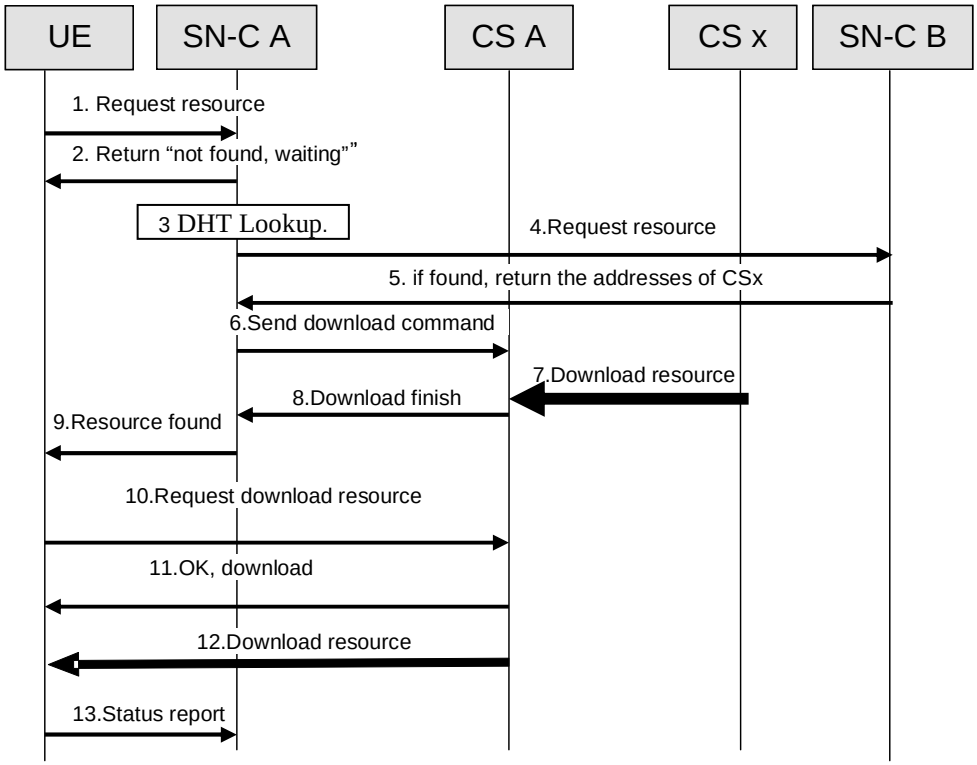


Figure 6.3.4.2.1: P2P media streaming request procedure between domains

1. UE sends request information to the SN-C node within the same domain, querying the node information which owns its request streaming media data.

2. If the information does not exist, it shows that the domain has not the request streaming media data, SN-C returns "resource not found, please wait" message to UE.

3. SN-C sends query request to the core DHT, querying SN-C information which have the current requested streaming media data; After a search process, DHT network returns all or part address list of the SN-C which have the current requested streaming media data to the initial requested SN-C.

4.-5. The initial requested SN-C selects some SN-C to establish a connection, and obtains the address(es) of the corresponding one or multiple CSx in accordance with the information returned by the DHT network.

6.-8. The initial requested SN-C guides the CS within the same domain to download the relevant resources from the remote one or multiple CSx within other domain.

9. SN-C informs the UE that the requested film has found and downloads from local CS.

10.-12. UE establish a connection with and the CS and download resources from the CS.

13. CS sends resource registration information to SN-C, registering its current streaming media information into the SN-C for downloading by other nodes.

6.4 Decentralized peer-to-peer architectures

Decentralized peer-to-peer architectures have not been worked out in the present document.

6.5 Fully distributed peer-to-peer architectures

6.5.1 General

Fully distributed (or pure) peer-to-peer architectures make no use of a central server at all (except for new peers to join the network). In these systems all peers have equal roles and responsibilities. Based on how the participating peers are connected in the overlay network, we can classify pure peer-to-peer networks as unstructured or structured.

6.5.2 Unstructured peer-to-peer networks

An unstructured peer-to-peer network can be easily constructed, as the overlay links are established arbitrarily. Peers are connected in a random graph: a new-coming user joins the overlay by connecting itself to any, randomly chosen, existing node, it copies its existing links and forms its own over time. The main disadvantage of these networks is that the queries are not necessarily resolved. When a peer wants to find a piece of data in the network, the query has to be flooded through the network to find as many peers as possible that share the data. Popular content is likely to be available at several peers and any peer searching for it is likely to find the same thing. But if a peer is looking for rare data shared by only a few other peers, then it is highly unlikely that search will be successful. Since there is no correlation between a peer and the content managed by it, there is no guarantee that flooding will find a peer that contains the desired data. This results in inefficiency, since a large subset of nodes has to be queried for a content not widely distributed to be found. Most of the popular P2P networks such as Gnutella [i.8], Freenet [i.9] and FastTrack [i.10] are unstructured. Despite the considerable efforts made on improving the unstructured overlays (the most recent, Gia [i.11]), as a response to a poor data discovery performance, the structured overlays have emerged.

6.5.3 Structured peer-to-peer networks

Structured peer-to-peer deploy a protocol that efficiently routes a search to some peer that has the desired file, even if that file is rare. Such a guarantee necessitates a more structured pattern of overlay links. These overlays are thus built in a controlled fashion. In these systems, to each data item and to each member a unique logical identifier is assigned. Based on the member's identifier, new members join by attaching to a well defined existing member, resulting in a highly structured graph. But not only is the placement of new members precisely determined, so is the placement of data items. The most common types of structured peer-to-peer systems rely on distributed hash tables (DHTs) to map the key (the identifier of data items) to the node in charge of storing that particular key and that particular data item. This enables efficient search for exact queries, since a data item, given its key, can be found in only O(logN) hops. In addition, the total of only O(logN) neighbors should be maintained per each node. Some well known DHTs are Chord [i.7], Pastry [i.12], Tapestry [i.13], CAN [i.6], and Tulip [i.14]. Not a DHT-approach but a structured peer-to-peer network is HyperCuP [i.15].

6.5.4 Structured versus unstructured

Recent studies have shown that the churn (the rate at which nodes join and leave the network) as well as the heterogeneity of users are high. Many argue that unstructured overlays can handle such an environment more efficiently. In addition, they provide more efficient search for complex queries of popular data items than their structured counterparts. However, structured and unstructured overlays have been compared in [i.16] via detailed simulations. A hybrid system has been designed that constructs a structured graph, however data placement and search mechanisms are the same as those deployed in unstructured overlays. Simulation results based on real-world samples indicated that the hybrid system can support complex queries with lower message overhead while providing higher query success rates and lower response times than systems based on unstructured graphs.

6.6 Challenges with peer-to-peer networks

6.6.1 General

In previous clauses, different peer-to-peer architectures have been described and discussed. Each of those imposes challenges inherent to peer-to-peer systems (as opposed to server-client models) that need to be understood and addressed so that the optimal choice of the peer-to-peer architecture can be made. This clause briefly looks into some of the issues that should consider when making a decision on which of the approaches would be most appropriate for the task at hand.

6.6.2 Availability

Guaranteeing the **availability** of peer-to-peer systems is an essential challenge. The functioning of peer-to-peer networks depends not only on availability of any central component, as the failure of such a component can be disruptive to service, but on the availability of any particular participating peer as well. Taking into account the brief periods of availability of peers (some recent studies [i.17] have shown that less than 4 % of the peers have an uptime of over 10 hours), the availability problem is critical. Proven social incentives such as rewards and social recognition could stimulate users to leave their P2P software running for longer periods, thus improving the overall availability of the network.

6.6.3 Decentralization

Another challenge is **decentralization** of the functionality of a peer-to-peer network across its peers. With the full decentralization the necessity of central elements in the system disappears. This results in the increased robustness of these systems, as central elements must be set up and maintained by some party and may form serious bottlenecks, points of failures, or security threats. However, joining to the network and validating user identities are difficult to implement without any central element. To the best of our knowledge there are no peer-to-peer systems so far in which all functionality is fully decentralized in an efficient manner and without a considerable risk of the integrity loss.

6.6.4 Performance

The **performance** of a P2P system highly depends on the efficiency of the search mechanisms, but also on the willingness of peers to share resources. Autonomous peers are free to decide whether to donate resources or not. Therefore, as the third challenge, in addition to developing efficient search mechanisms, introducing popular incentives to peers is essential in order to stimulate cooperation and, consequently, improve system performance (see [i.18] for more detail).

6.6.5 Integrity

Maintaining the **integrity** of the system and achieving **trust** among peers is the fourth challenge. Peer-to-peer networks inherently use donated resources. It is difficult to maintain the integrity, as donors cannot always be trusted: data can be attacked at several levels, namely system information (e.g. pointers to content), metadata, and the actual content itself (see [i.19] for more detail).

6.6.6 Network transparency

The fifth challenge in peer-to-peer networks is to overcome problems caused by dynamic IP addresses, NAT boxes, and firewalls. Due to these three technologies, peers do not have the freedom to send anything anywhere without the help of another peer acting as a mediator.

6.7 NBAC Analysis and Information Flows

From a purely architectural point of view, the NBAC approach does not introduce new elements into the NGN architecture but it may use elements that already exist, particularly SPDF, A-RACF, RCEF and BTF.

NOTE: An analysis of NBAC impacts on these functional entities is for further study.

These elements host the features that allow the network to trigger events on specific patterns trigger, the control to detect the service involved by these patterns, to select the capabilities appropriate for the service and acting on the service flows opportunely, for forcing the capability.

Some of these features can be obtained by extending existing functionalities, others need new additions inside the elements in order to manage the logics and the interactions resulting from the NBAC.

6.7.1 Generic State Diagram

The phases and the interactions that the NBAC approach requires are represented in the basic scheme below (figure 6.7.1.1): it can be distinguished the additional functional blocks, the optional ones and those already present in the elements of the NGN architecture.

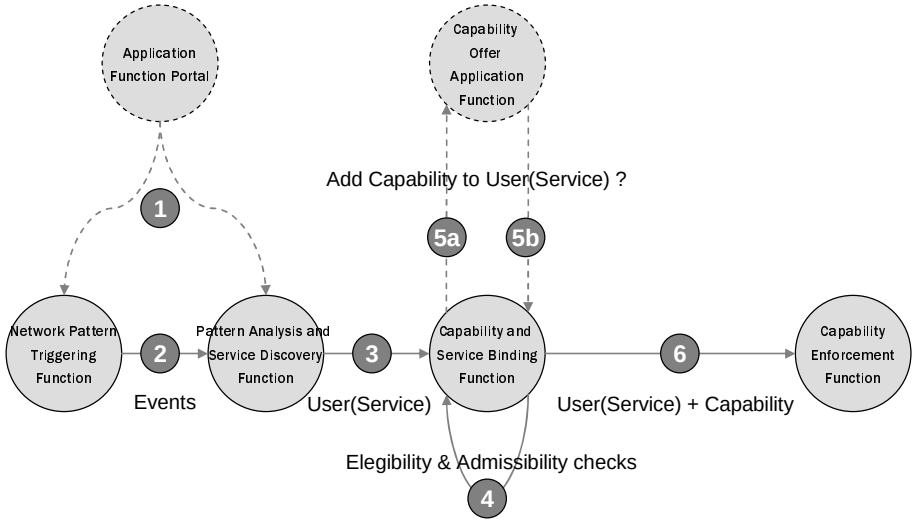


Figure 6.7.1.1: NBAC operation State Diagram

Phases:

1) Network Triggering Activation

2) Network Pattern Triggering

3) Pattern Analysis and Service Discovery

4) Capability and Service Binding

5a) Capability Offer and 5b) Capability Offer response

6) Capability Enforcement

Phase (1) is the Phase that provides the appropriate configuration for the Network Pattern Triggering Function (NPTF) at network level and the "Pattern Analysis and Service Discovery" Function (PASDF) at control level. The Provisioning can start from a specific Application Function, for example with an interaction via a portal a portal. For all use cases, the configuration/provisioning of the N(BTF) can be done either through a pure provisioning interface or via the RACS., see clause 6.7.7.

In this phase are provided the patterns that have to be inspected on the traffic and the associated service templates, which will allow attributing a specific user flow to a specific service.

After the provisioning phase, when a configured pattern is detected on the traffic by NPTF an appropriate event is sent (2) to the PASDF. PASDF analyzes one or more events and, if possible, attributes them to a service. The information User (Service) is then passed (3) to the Capability and Service Binding Function (CSBF)

CSBF selects the appropriate capability that can be potentially bound to User (Service) (4). In this phase CSBF assures also that all the pre-conditions needed for binding the Capability to the User (service) are verified. CSBF can then optionally ask (5a) to a specific application function in order to offer the specific capability to the User for the current Service. In case of positive answer (5b) (or directly if without (5a)), the CSBF requires (6) the enforcement of the capability to the Capability Enforcement Function.

This function, which for the capability "QoS" can be provided directly by RCEF, provides all the needed configuration for acting on the service flows.

6.7.2 NBAC specific functionalities

Focusing on the functions that are relevant for NBAC, it is possible to distinguish three main roles:

- Network Pattern Triggering Function (NPTF): NPTF inspects the network traffic matching the previously configured patterns. For any matched pattern NPTF provides an "event message" (IP addr, flow tuple, Pattern Id) to the control layer in order to activate the analysis of the detected patterns. The event message can be enriched with parameters spilled out from the traffic (e.g. URL), in order to provide deeper information to the next phases.

- Pattern Analysis and Service Detection Function (PASDF): PASDF analyzes the patterns sent by NPTF and detects, basing on pre-configured service templates, the corresponding service (e.g. P2P TV) the user is connected to. PASDF is able to provide:

  User Info: IP address, other access info

  Service Info: Service Id, Url

- Capability and Service Binding Function (CSBF): CSBF uses the info provided by the PASDF in order to select one or more capabilities (e.g. QoS) that can be potentially bound to the detected service (Eligibility). The selection can incorporate a check for Admissibility of the Capability (e.g. AC for QoS). After these checks, CSBF can optionally ask the user for an explicit consent. CSBF then interacts with Enforcement functions (e.g. RCEF) for activating the capability. In this request CSBF is able to provide:

  User Info: IP address, other access info

  Capability Id: e.g. QoS

  Service Info: Service Id, Url

6.7.3 Out-of-Band QoS with NBAC

This scenario shows how to apply the NBAC functionalities to enforce a certain Quality of Service to an untrusted streaming service.

The user has subscribed for a service that enables the application of QoS when a particular streaming service is accessed. Since the service is untrusted it is not possible to intercept the service request; then the only way to be aware of the service accessed is through the NBAC functionalities.

The network, using the appropriate NBAC functionalities, recognizes the service, and identifies the capability to be applied to the flow, in this case a particular Class of Service.

Before applying the QoS, depending on the user service profile, it may be required to ask an explicit confirmation to the user.

Below an example information flow is depicted. The functionalities responsible for intercepting the flow and trigger a request has been identified in the (N)BTF: the (N)BTF represents a BTF enhanced with NBAC capabilities. The QoS offer AF is intended to be an Application Server.

Phase 1: Network Triggering Activation

This phase is performed via provisioning either through a pure provisioning interface or via the RACS, see clause 6.7.7.

Phase 2: Network Pattern Triggering

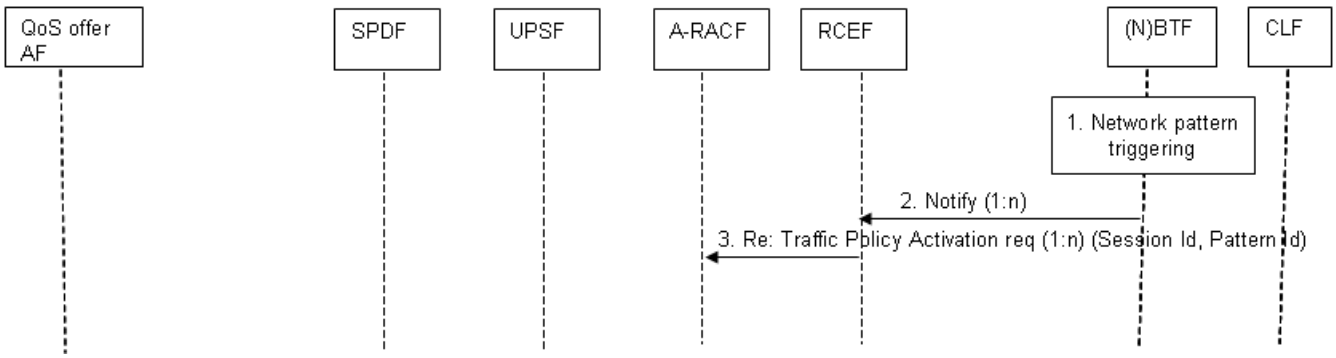


Figure 6.7.3.1: Network Pattern Triggering Information Flow

1. The (N)BTF recognizes the pattern to be triggered.
2. The (N)BTF notifies one or more recognized patterns to the RCEF. This interaction is internal and will not be standardized.
3. The RCEF sends to the A-RACF one or more Traffic Policy Activation Request(s) indicating at least IP addresses, ports and the pattern identifier.

Phases 3 and 4: Pattern Analysis and Service Discovery; Capability and Service Binding

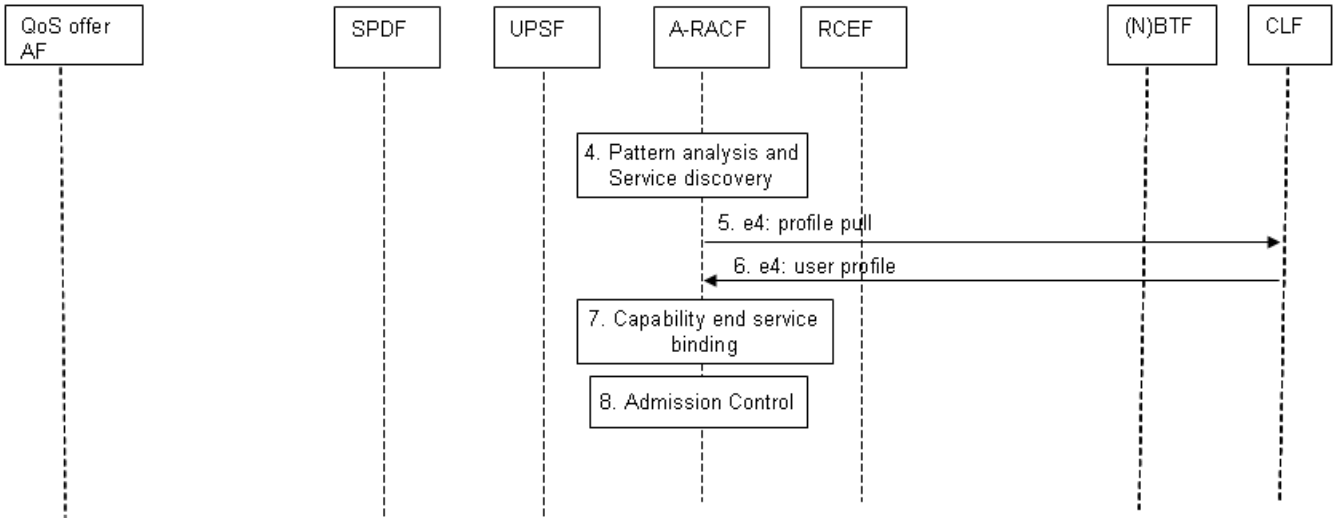


Figure 6.7.3.2: Pattern Analysis and Service Discovery; Capability and Service Binding Information Flow

4. The A-RACF shall be able to collect multiple messages from the RCEF and to analyze the received pattern identifiers in order to recognize the service that the user is accessing (for example video streaming from a particular web site).

5. Optionally, the A-RACF asks the user profile to the CLF. This step is optional because in normal condition the A-RACF already has the user profile.

6. Conditionally, if step 5 occurs, the CLF sends the user profile to the A-RACF.

7. The A-RACF verifies which is the capability (for example to apply a particular class of service to the flow) to be applied to the user for that service.

8. The A-RACF performs the admission control for that capability on the user access.

Phases 5a and 5b: Capability Offer and Capability Offer Response

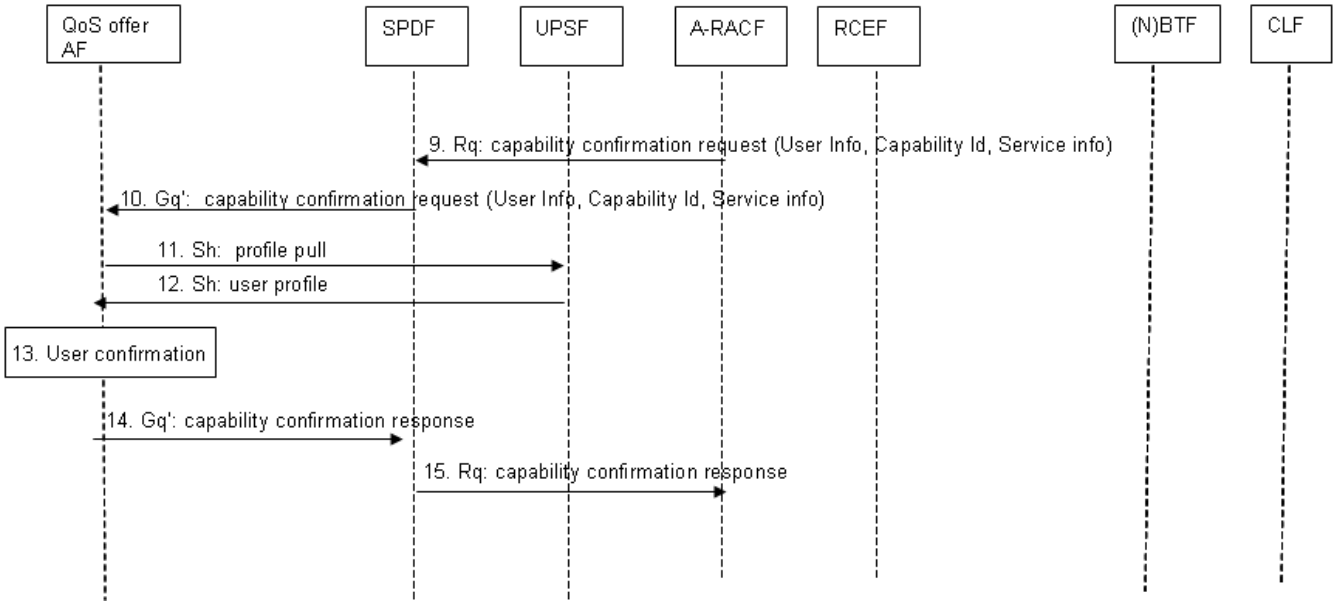


Figure 6.7.3.3: Capability Offer and Capability Offer Response Information Flow

9. The A-RACF sends to the SPDF the information about the service and capability to be applied. The message includes at least the user identifier, capability identifier and possible additional information about the service.

NOTE 1: This interaction is not actually present in RACS stage 2, where the pull mode does not involve the SPDF.

10. The SPDF sends to the QoS offer AF the information about the service and capability to be applied. The message includes at least the user identifier, capability identifier and additional information about the service.

NOTE 2: This interaction is not actually present in RACS stage 2, where the pull mode does not involve the SPDF.

11. The QoS offer AF asks to the UPSF the user service profile in order to verify the user preferences. This allows the AF to verify if the user wants to explicitly confirm the application of the capability and, in that case, which is the preferred way to convey the request (e.g. PC Pop-up, SMS,etc.).

12. The UPSF sends the user service profile to the QoS offer AF.

13. Optionally, the QoS offer AF asks to the user a confirmation on the application of the capability. It is for further study the detail of this interaction.

14. The QoS offer AF forwards the confirmation to the SPDF.

15. The SPDF forwards the confirmation to the A-RACF.

Phase 6: Capability Enforcement

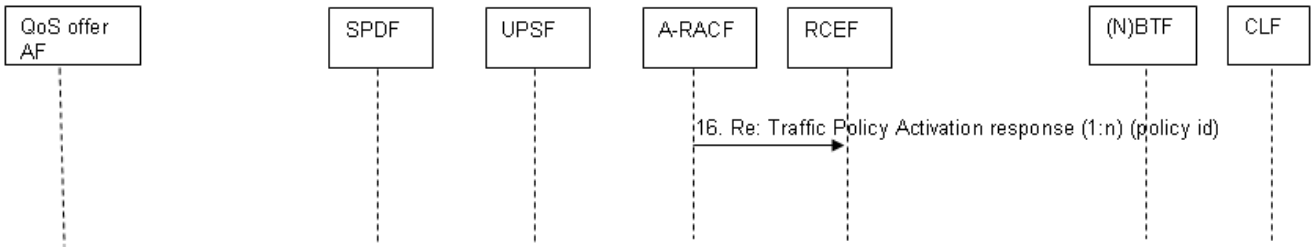


Figure 6.7.3.4: Capability Enforcement Information Flow

16. The A-RACF installs one or more policies into the RCEF. This message includes at least the policy identifier.

6.7.4 Bandwidth boost with NBAC

This scenario shows how to apply the NBAC functionalities to dynamically enable traffic policies to enhance specific untrusted application sessions.

In the following example, the user can enable (e.g. via web portal) a specific application (e.g. FTP) he individually desires to boost.

The network, using the appropriate NBAC functionalities, recognizes the specific traffic session and activates the related policy (e.g. bandwidth enhancement).

For a better understanding of the complete information flow related to this scenario, four main stages have been identified built around the basic NBAC behaviour and operational phases:

Stage 1: Network Triggering Activation

Stage 2: Bandwidth boost "start" based on the sequence of: Network Pattern Triggering ("start"), Pattern Analysis and Service Discovery, Capability and Service Binding, Capability Enforcement

Stage 3: Bandwidth boost "stop" based on the sequence of: Network Pattern Triggering ("stop"), Pattern Analysis and Service Discovery, Capability and Service Binding, Capability Enforcement

Stage 4: Network Triggering de Activation

NOTE 1: The functionalities responsible for intercepting the flow and trigger the policy activation have been identified in the (N)BTF: the (N)BTF represents a BTF enhanced with NBAC capabilities.

NOTE 2: The AF-Portal (e.g. web portal) through which the UE selects the bandwidth boost service is intended to be an application server.

NOTE 3: The relationship between (N)BTF and RCEF is considered to be an internal relationship within the same physical node and will not be standardized as part of the present document.

6.7.4.1 Network Triggering Activation

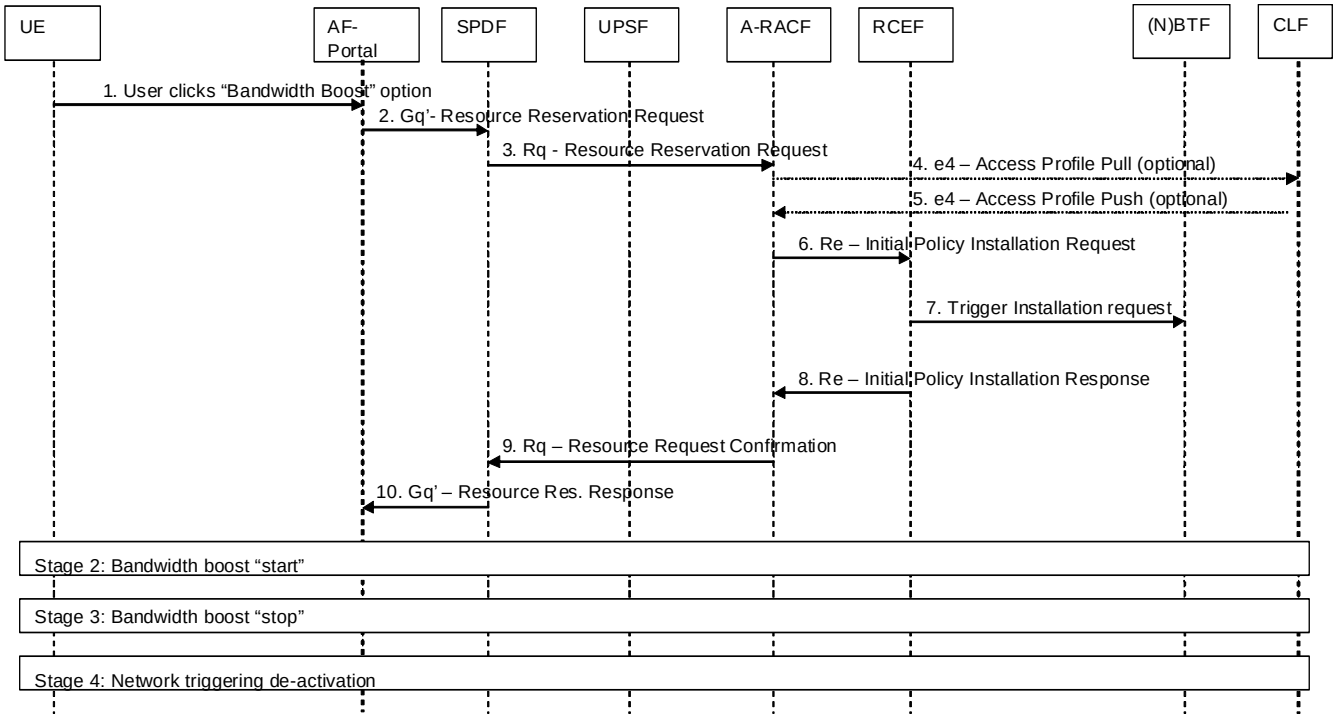


Figure 6.7.4.1.1: Network Triggering Activation Information Flow

1. The User chooses to select the Bandwidth Boost service for a specific application (e.g. FTP). This operation may be implemented through a portal (AF-Portal) either through a pure provisioning interface or via the RACS, see clause 6.7.7.

2. The AF-Portal sends this request through a Resource Reservation Request on Gq' interface. This request contains all information related to how to map this request in terms of policies (to be installed in A-RACF/RCEF) and triggering rules (to be installed on NBTF).

3. The SPDF forwards the message to the A-RACF via Rq interface.

4. (Optional) – The A-RACF sends an Access Profile Pull on e4 interface to the CLF. This operation (and the following one) are only necessary if for some reason A-RACF does not have information related to the user (this info should be already present as a result of the previous authentication/authorization procedure during attachment).

5. (Optional) – The CLF answers with an Access Profile Push (see step 4).

6. The A-RACF installs the proper policy on the RCEF.

7. The patterns to be recognized are provisioned in the (N)BTF.

8. The RCEF sends the confirmation to the A-RACF.

9. The A-RACF generates the confirmation to the SPDF.

10. The SPDF forwards the confirmation to the AF-Portal.

6.7.4.2 Bandwidth boost "start"

This stage involves the following "basic" phases: Network Pattern Triggering (steps 1-3), Pattern Analysis and Service Discovery (step 4), Capability and Service Binding (step 5), Capability Enforcement (step 6).

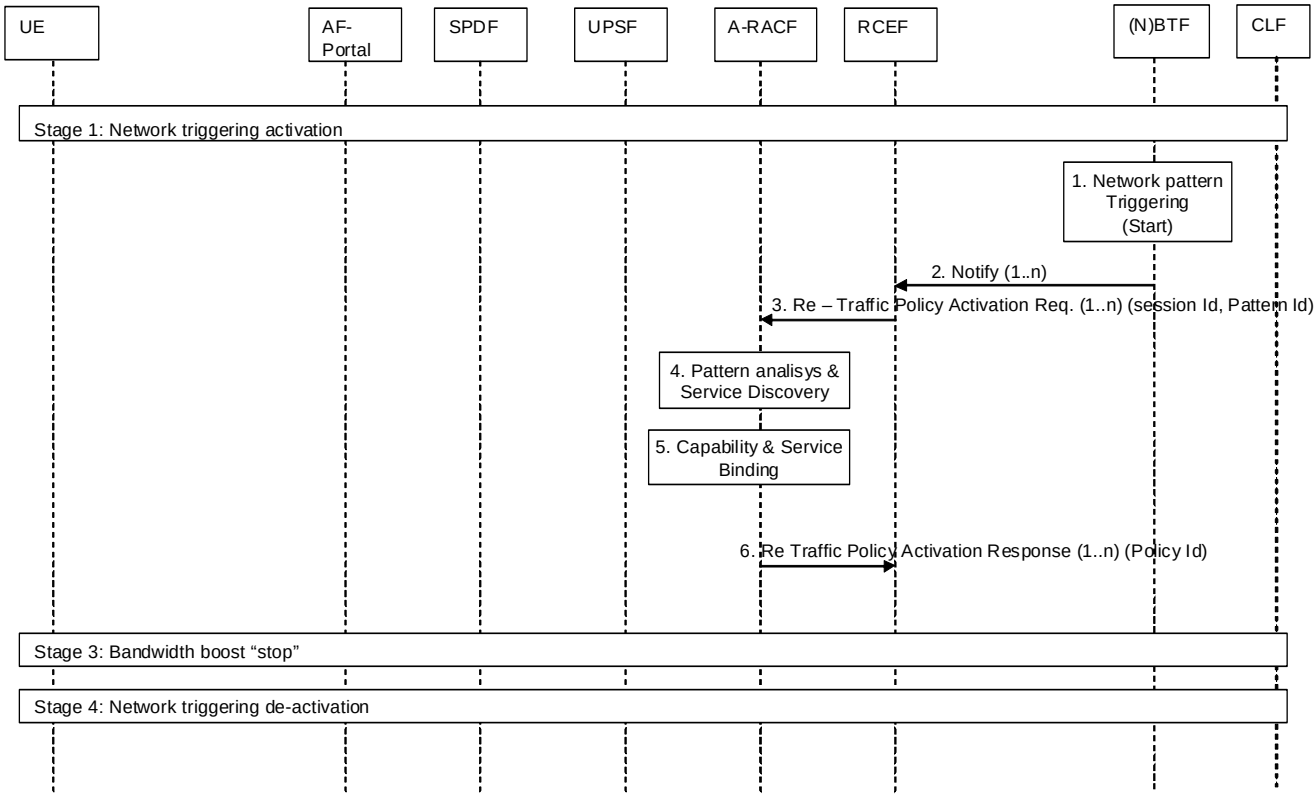


Figure 6.7.4.2.1: Bandwidth boost start Information Flow

1. The (N)BTF recognizes the pattern to be triggered.
2. (N)BTF notifies one or more recognized patterns to the RCEF.
3. The RCEF sends to the A-RACF one or more Traffic Policy Activation Request indicating at least IP addresses, ports and pattern identifier.
4. The A-RACF shall be able to collect multiple messages from the RCEF and to analyze the received pattern identifiers in order to recognize the service that the user is accessing.
5. The A-RACF verifies which is the capability to be applied to the user for that service (e.g. bandwidth boost for a specific FTP session). This step also includes admission control.
6. If step 5 is ok the traffic policy activation response is sent to the RCEF and the "Bandwidth Boost Policy" is enforced in the RCEF.

6.7.4.3 Bandwidth boost "stop"

This stage involves the following "basic" phases: Network Pattern Triggering (steps 1-3), Pattern Analysis and Service Discovery (step 4), Capability and Service Binding (step 5), Capability Enforcement (step 6).

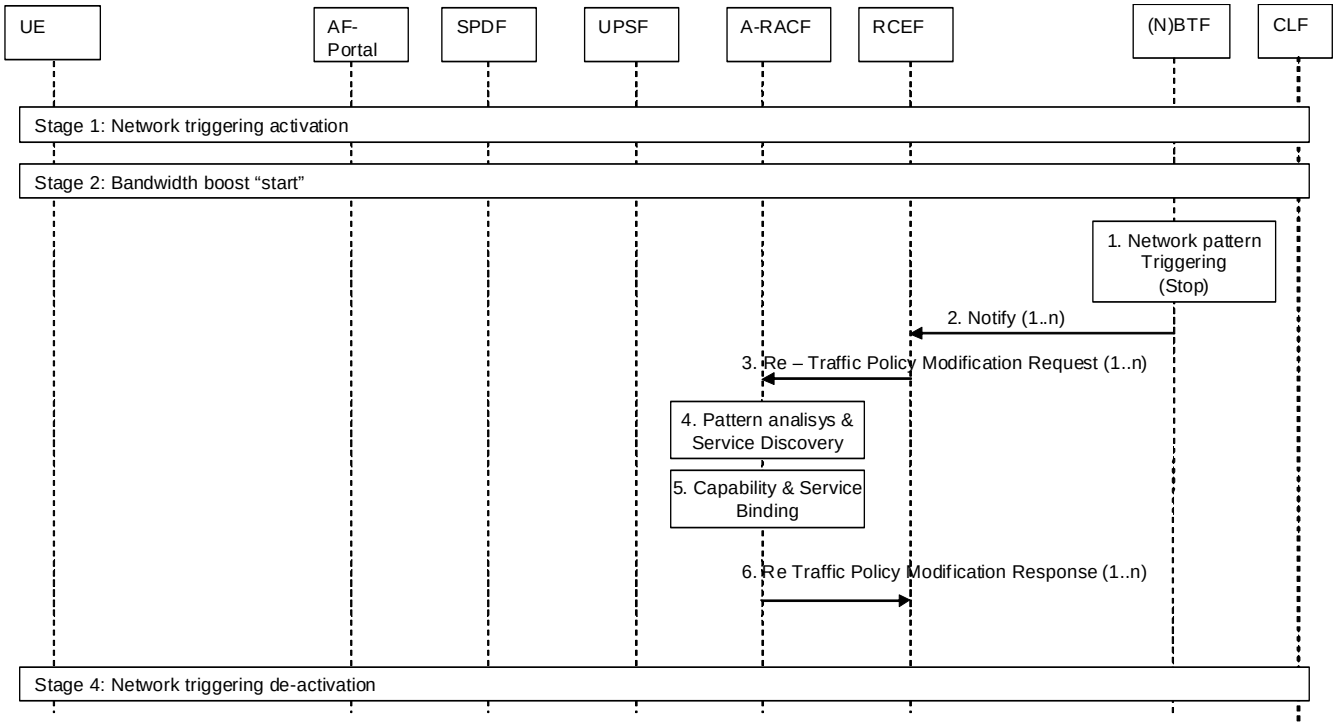


Figure 6.7.4.3.1: Bandwidth boost stop Information Flow

1. The (N)BTF recognizes the pattern (which triggers the de-activation of the current policy) (e.g. de-activates the bandwidth boost policy for a specific FTP session).
2. (N)BTF notifies the recognized patterns to the RCEF.
3. The RCEF sends to the A-RACF the related Traffic Policy Modification Request.
4. The A-RACF collects the messages from the RCEF to analyze the received patterns.
5. The A-RACF verifies which the capability to be applied is (e.g. bandwidth boost de-activation for a specific FTP session). This step also includes the admission control.
6. If step 5 is ok the traffic policy modification response is sent to the RCEF and the "Bandwidth Boost Policy" is de-activated in the RCEF.

NOTE: The De-Activation process does not include any modification in the configuration on (N)BTF. This implies that a new "start" pattern triggering could be notified by (N)BTF and the related bandwidth boost policy will be re-activated.

6.7.4.4 Explicit Network Triggering de Activation

The UE explicitly accesses the AF-portal to disable network triggering function associated to the bandwidth boost service.

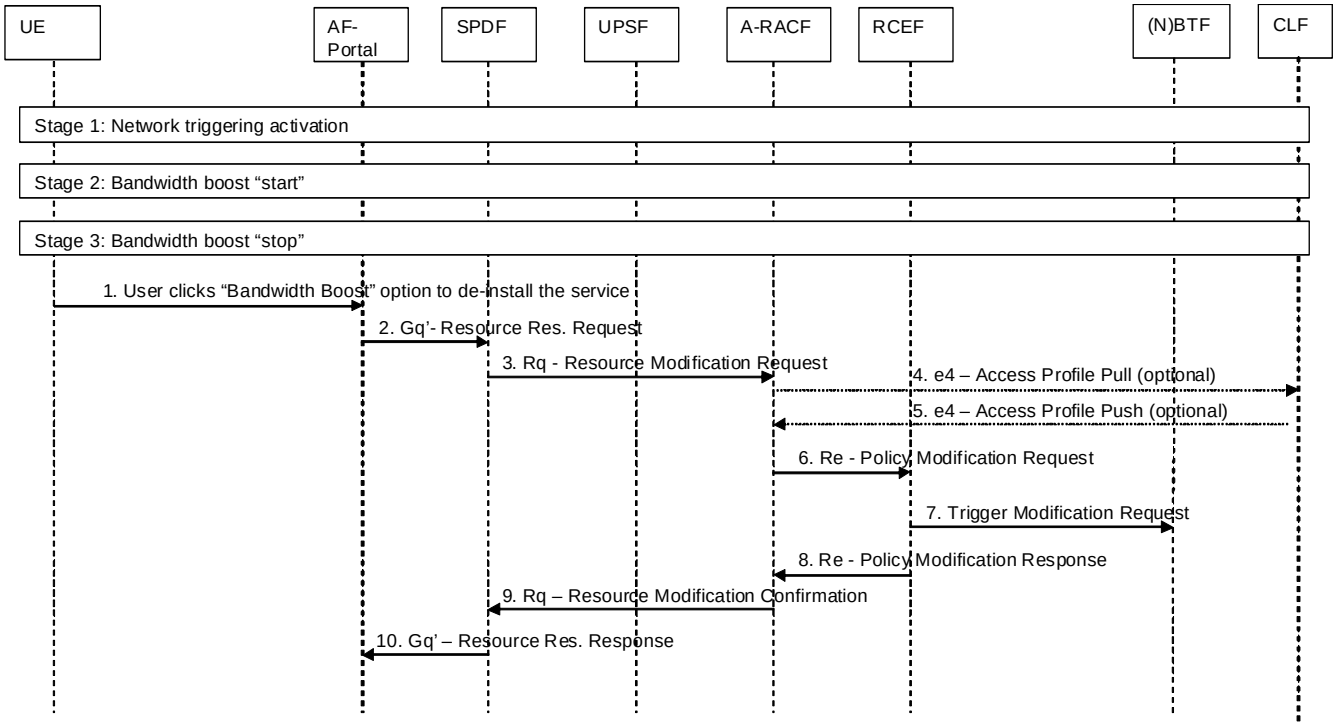


Figure 6.7.4.4.1: Explicit network triggering de-activation Information Flow

1. The UE explicitly requests the de-installation of network triggering function associated to the bandwidth boost service.
2. The AF-Portal sends the related request to the SPDF.
3. The SPDF forwards the request for the policy modification to A-RACF.
4. Optional, the A-RACF asks the user profile to the CLF.
5. Conditionally to step 4 – The CLF sends the user profile to the A-RACF.
6. The A-RACF requests the RCEF to de-install the policy.
7. The RCEF instructs the (N)BTF to disable previously configured triggering patterns.
8. The RCEF sends a confirmation response to A-RACF.
9. The A-RACF forwards the confirmation response to SPDF.
10. The SPDF forwards the result to the AF.

6.7.4.5 Implicit Network Triggering de Activation

If the bandwidth boost service has been selected by the user specifying a "time duration", the policy de-installation may be triggered by A-RACF without manual intervention as shown in the following Information Flow.

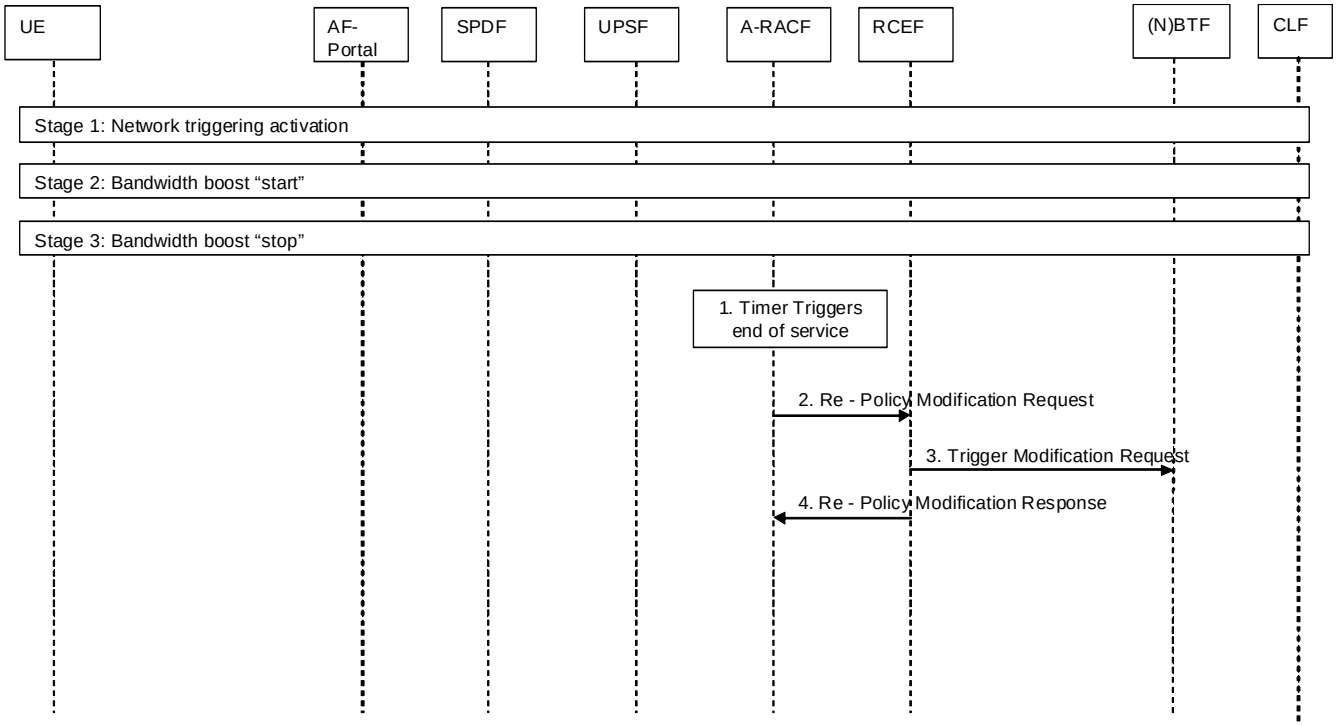


Figure 6.7.4.5.1: Implicit (e.g. timer based) network triggering de-activation Information Flow

1. The timer (internal to A-RACF logic) triggers the de-installation process.
2. The A-RACF requests the RCEF to de-install the policy.
3. The RCEF instructs the (N)BTF to disable previously configured triggering patterns.
4. The RCEF sends a confirmation response to A-RACF.

6.7.5 Peer-to-peer traffic control with NBAC

This scenario shows how to apply the NBAC functionalities to control peer-to-peer traffic. The network, using the appropriate NBAC functionalities, recognizes the specific traffic sessions and activates the related policy; for example, the bandwidth enhancement in case of a commercial web peer-to-peer TV, and the bandwidth limiting in case of a peer-to-peer content sharing the provider has not a deal with.

The policies activations are based on peer-to-peer templates that are preprovisioned in the A-RACF. Peer-to-peer templates are used in order to manage the different flows in terms of type (i.e. web TV), aggregation (i.e. flows of the same stream) and origin (i.e. a particular access network).

In the following figures exemplary information flows are depicted.

The functionalities responsible for intercepting the flow and trigger a request has been identified in the (N)BTF: the (N)BTF represents a BTF enhanced with NBAC capabilities.

Phase 1: Network Triggering Activation

This is performed via provisioning either through a pure provisioning interface or via the RACS, see clause 6.7.7.

Phase 2: Network Pattern Triggering

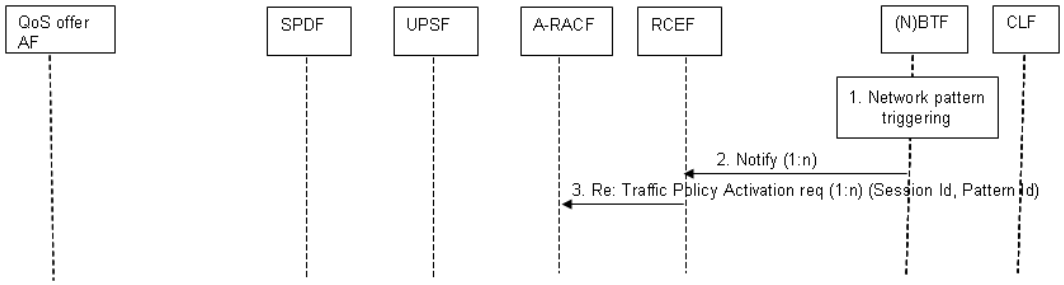


Figure 6.7.5.1: Network Pattern Triggering Information Flow

1. The (N)BTF recognizes the pattern to be triggered.
2. The (N)BTF notifies one or more recognized patterns to the RCEF. This interaction is internal and will not be standardized.
3. The RCEF sends to the A-RACF one or more Traffic Policy Activation Request(s) indicating at least IP addresses, ports and the pattern identifier.

Phases 3 and 4: Pattern Analysis and Service Discovery; Capability and Service Binding

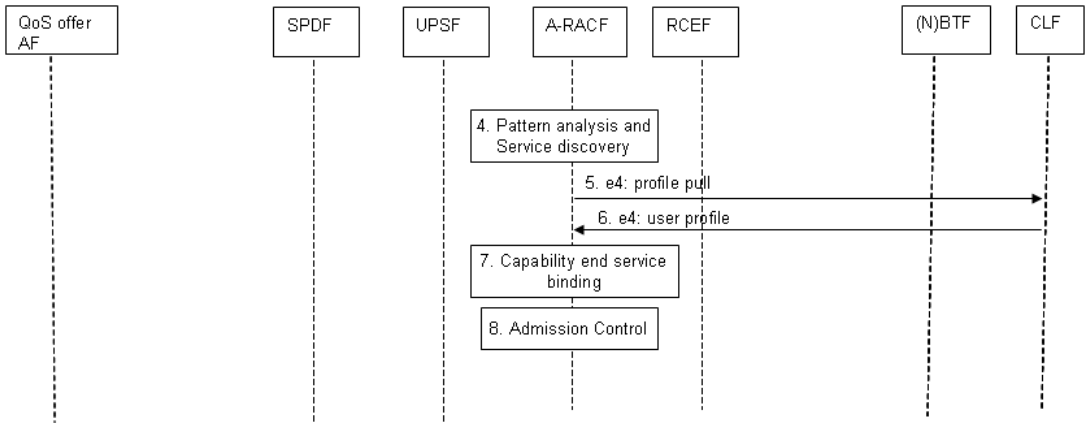


Figure 6.7.5.2: Pattern Analysis and Service Discovery; Capability and Service Binding Information Flow

4. The A-RACF shall be able to collect multiple messages from the RCEF and to analyze the received pattern identifiers.
5. Optionally, the A-RACF asks the user profile to the CLF. This step is optional because in normal condition the A-RACF already has the user profile.
6. Conditionally, if step 5 occurs, the CLF sends the user profile to the A-RACF.
7. The A-RACF verifies which is the capability to be applied to the user for that service (i.e. the peer-to-peer template that best fits to the pattern identified).
8. The A-RACF performs the admission control for that capability on the user access.

Phases 5a and 5b: Capability Offer and Capability Offer Response

These phases are not included in this scenario.

Phase 6: Capability Enforcement

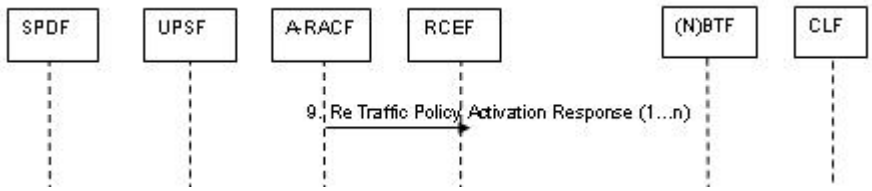


Figure 6.7.5.3: Capability Enforcement Information Flow

9. The A-RACF installs one or more policies into the RCEF. This message includes at least the policy identifier.

6.7.6 Audience Research with NBAC

This scenario shows how to apply NBAC functionalities to Audience Research, an example of the customer profiling use-case (refer to clause 5.1.16). Audience Research mainly applies to IPTV streaming services including web browsing on IPTV services.

As already remarked in previous clauses the NBAC approach can be applied to different kind of services both trusted (i.e. services directly provided by the operator) and un-trusted/OTT (Over The Top) (i.e. Internet TV, Internet VoD, etc.).

For this specific use-case, the purpose is to collect measures (or metrics) covering IPTV audience metrics (e.g. broadcast, CoD, PVR Contents), access and navigation (e.g. Content Guide), interactive applications (e.g. rating) in order to target Personalized Advertising, Content Recommendation, etc.

This process may be enabled only after user's consent. And with respect of the user privacy (further information on legal aspects related to customer profiling can be found in clause 13.2).

Audience data can be collected across networks, platforms, type of services and service providers. Within the scope of this clause only data passing across the transport processing functions (N)BTF will be considered.

For the purpose of the present document it can be assumed that these events could be used advantageously by an Audience Research Collector (ARC) for creating/updating the profile of the IPTV user: with this level of detail and an appropriate data mining it can be:

- measured the number of advertising impression and advertising skips;
- tracked the selection paths on EPG for the preferred channel;
- evaluated the interest for specific (portion of) content (replay, skip, forward);
- tracked the user interaction during a content streaming.

How these data are further processed by specific Application Functions (e.g. Audience Research Collector) is out of the scope.

In the following figures exemplary information flows are depicted.

Phase 1: Network Triggering Activation

This phase is performed via provisioning either through a pure provisioning interface or via the RACS, see clause 6.7.7. Examples of network pattern triggers include:

- IPTV Service Access Triggers: include all the patterns related to basic interaction for getting a broadcast video or an on Demand video: e.g. igmp join/leave, rstp Play/Stop. In this category of patterns can be included also more detailed patterns related to trick play events for detecting for example user action like Pause, FW, RW operations (e.g. RTSP Pause/FF/RW).
- Service Interaction Triggers: include all the patterns related to other interactive/hybrid services that can be associated to an IPTV content: like rate, vote, gamble, comment, click-to-call etc.

Phase 2: Network Pattern Triggering

1. The (N)BTF recognizes the pattern to be triggered.
2. The (N)BTF notifies one or more recognized patterns to the RCEF. This interaction is internal and will not be standardized.
3. The RCEF sends to the A-RACF one or more Event Notification Indication(s).

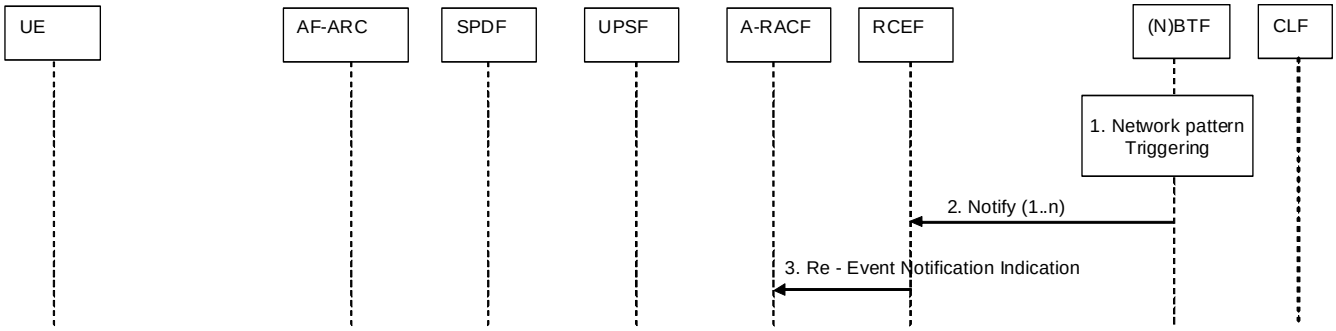


Figure 6.7.6.1: Network Pattern Triggering Information Flow

Phases 3 and 4: Pattern Analysis and Service Discovery; Capability and Service Binding

4. The A-RACF shall be able to collect multiple messages from the RCEF and to analyze the received pattern identifiers in order to recognize the service that the user is accessing.
5. Optionally, the A-RACF asks the user profile to the CLF. This step is optional because in normal condition the A-RACF already has the user profile.
6. Conditionally, if step 5 occurs, the CLF sends the user profile to the A-RACF.
7. The A-RACF verifies that the user has provided his consent to be tracked.
8. If previous step is "Yes" the A-RACF forwards to the SPDF the received information in one or more Event Notification Indication(s).
9. Finally, the SPDF forwards to the Audience-Research-Collector AF the received information.

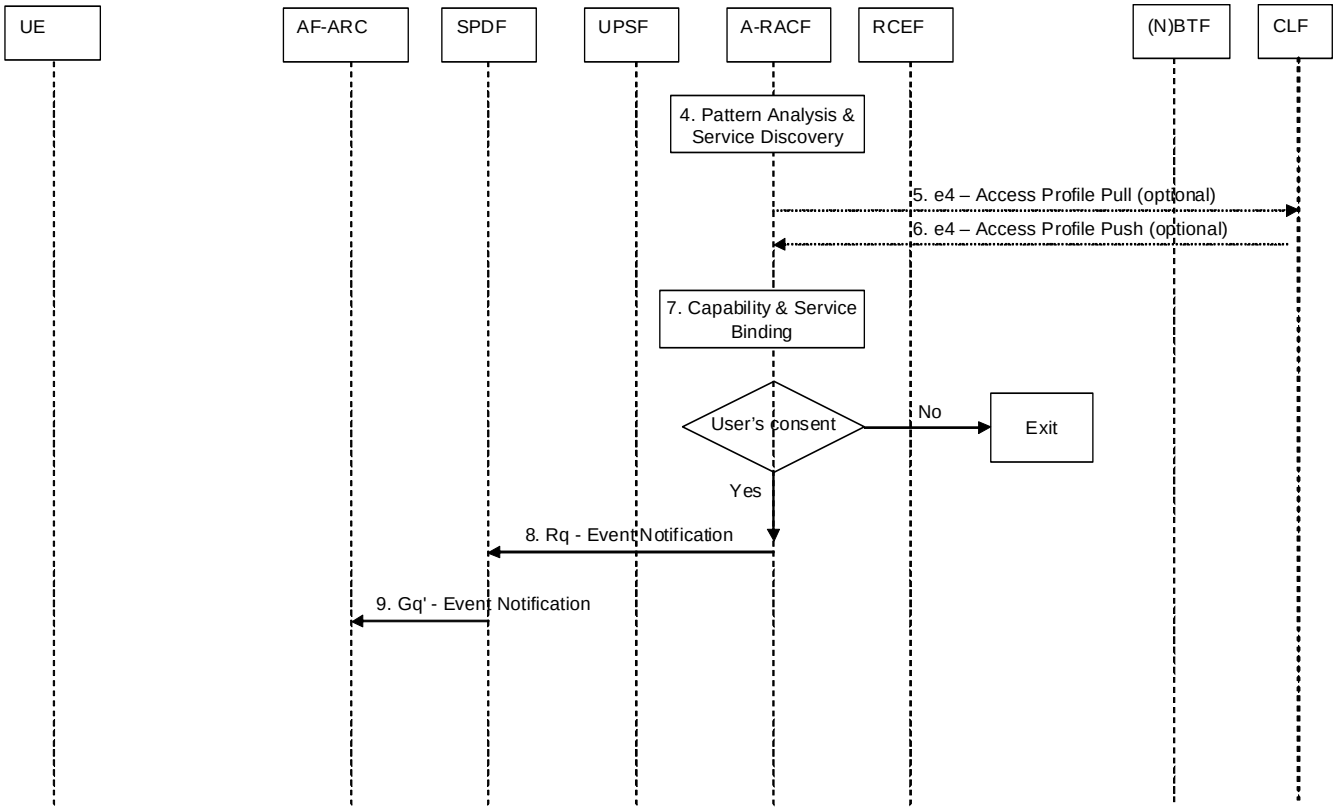


Figure 6.7.6.2: Pattern Analysis and Service Discovery; Capability and Service Binding Information Flow

6.7.7 Network Triggering Activation

The previous clauses mention that Network Triggering Activation is performed via provisioning. This clause works out this provisioning in more detail in several scenarios.

In scenario A, the user selects the over-the-top (OTT) service from a list from a list provided by the Application Function Portal (AF Portal), see figure 6.7.7.1. This scenario assumes a knowledgeable user and the service being present on the list.

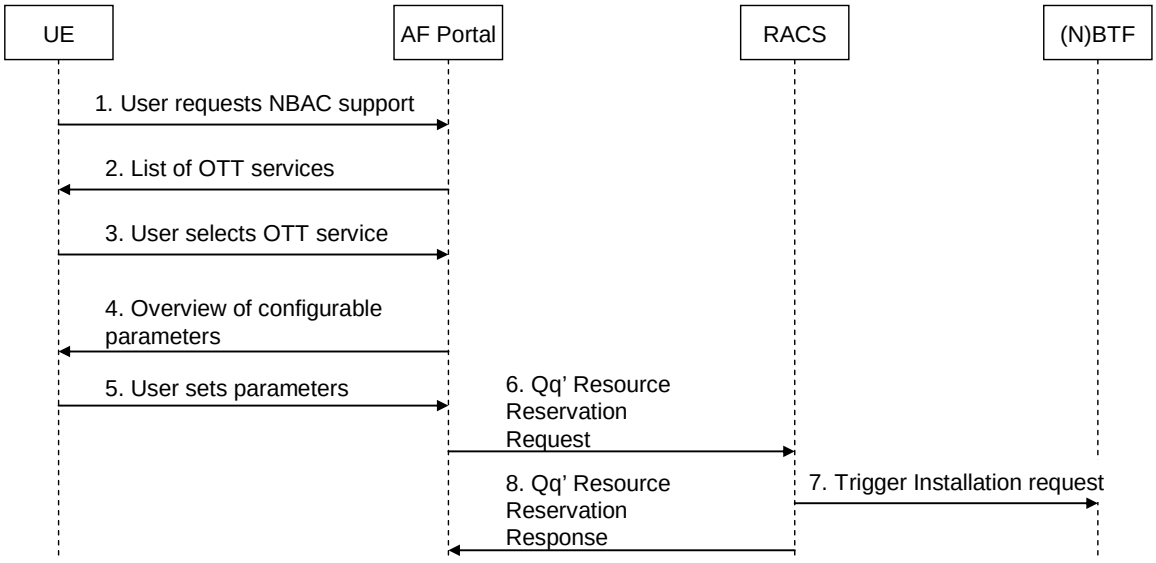


Figure 6.7.7.1: Scenario A, Network Trigger Activation by selecting service from a list

1. UE sends a request for NBAC support to AF Portal.
2. AF Portal responds with a list of supported OTT services.
3. UE selects the OTT service for which NBAC support is needed.
4. AF Portal confirms the selection and provides an overview of configurable parameters, e.g. bandwidth.
5. UE sets the parameters.
6. AF Portal makes a Resource reservation request to the RACS, including a Traffic Policy, based on the selected OTT service and configured parameters. This flow is similar to flows 2-6 from figure 6.7.4.1.1.
7. RACS sends a Trigger Installation request to (N)BTF for the selected OTT service.
8. RACS sends a resource reservation response to AF Portal, similar to flows 8-10 from figure 6.7.4.1.1.

Using this trigger, the (N)BTF activate the Service Template which will allow attributing a specific user flow to the specific OTT service.

In scenario B, the user requests NBAC support for "this OTT service". The (N)BTF functionality is used to learn what the user means by "this", see figure 6.7.7.2. This self-learning approach minimizes the intellectual efforts required from the user.

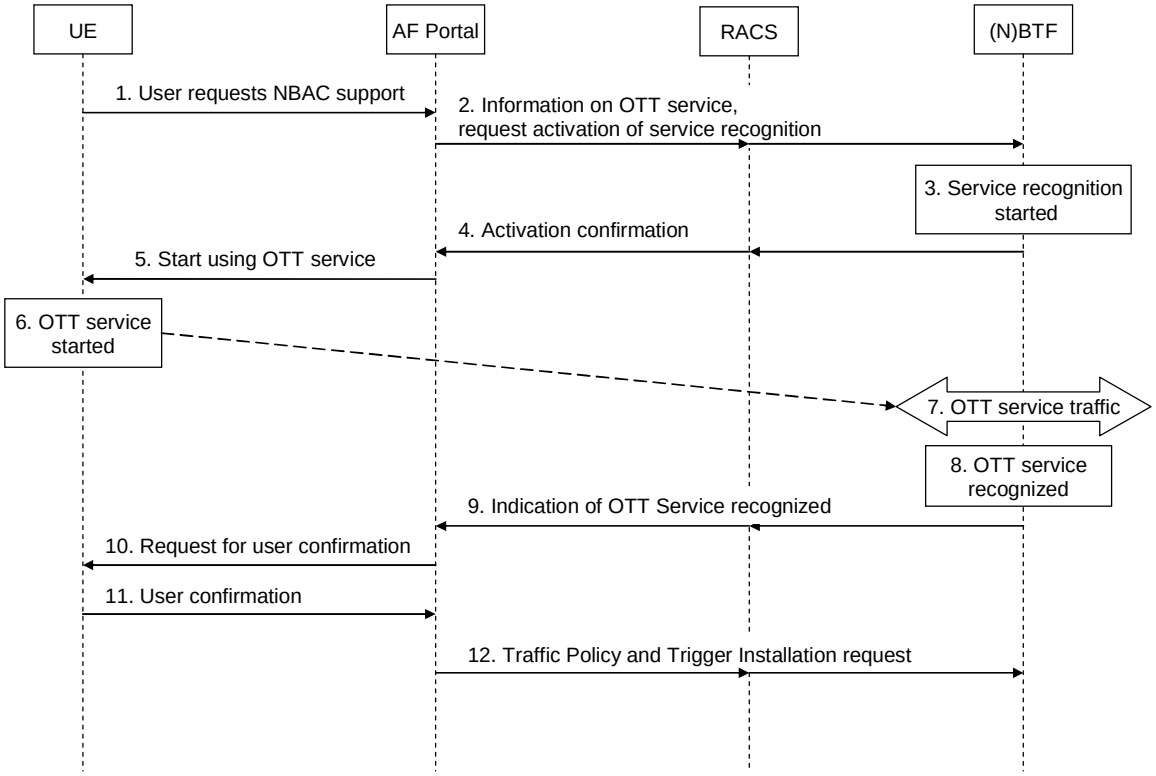


Figure 6.7.7.2: Scenario B, Network Trigger Activation by traffic recognition

1. UE sends a request for NBAC support to AF Portal.
2. AF Portal requests (N)BTF via RACS to activate the service recognition functionality and start trying to detect new traffic from/to the identified user. This flow is similar to flows 2-6 from figure 6.7.4.1.1.
3. De (N)BTF makes a snapshot of the traffic types currently running to/from the user, and starts looking for new traffic.
4. (N)BTF confirms to AF Portal via RACS, similar to flows 7-10 from figure 6.7.4.1.1.
5. AF Portal requests UE to start the OTT service for which NBAC support is needed. It may also request the user to suspend all other services in order to aid the service recognition process.

6. UE starts the OTT service.
7. This results in OTT service traffic from and to the UE, passing the (N)BTF.
8. (N)BTF recognizes the OTT service traffic, and stops detection.

NOTE 1: A wide variety of parameters may be used to identify the OTT service, which include user info (IP address, other access info), service info (IP addresses, port numbers, URLs, service identification, protocol identification), specific protocol info (e.g. carried in sip invite, igmp join/leave and rstp Play/Stop messages), etcetera.

9. (N)BTF indicates via RACS to AF Portal which OTT service was recognized.
10. AF Portal notifies UE and optionally request confirmation from UE.
11. UE confirms to AF Portal.
12. AF Portal sends a Trigger Installation request via RACS to (N)BTF for the selected OTT service.

Scenario C is the most advanced scenario. In this scenario, the user wants to add an OTT service for NBAC support that is not previously known to the NBAC system. A combination of configuration by the user and self-learning is used, see figure 6.7.7.3. This scenario helps the user and the network provider to extend the list of OTT services that are supported by NBAC. The scenario requires an advanced, motivated user.

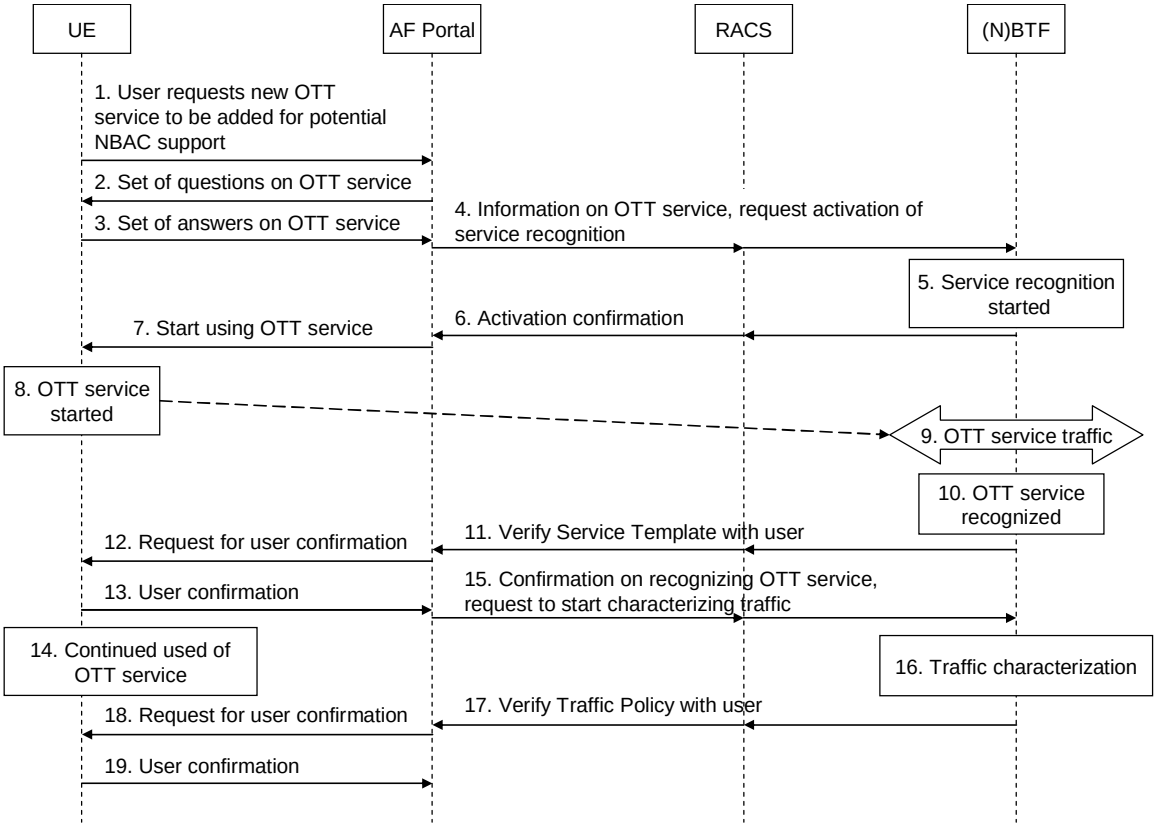


Figure 6.7.7.3: Scenario C, adding a new OTT service for NBAC support

Scenario C starts at the point where scenarios A and B have failed, and the conclusion has been made that the specific OTT services is not yet recognized or supported by the NBAC system ("It is not on the list").

1. UE sends a request to AF Portal to add a new OTT service for potential NBAC support.
2.-3. In a series of Q&E, UE characterizes the OTT service to the AF Portal. This may include the following aspects.
    a. Naming the OTT services for the context of NBAC.

b. Providing parameters to create a Service Template that can be used to recognize traffic from the OTT service.

c. Providing parameters that characterize the traffic, to be used to create a Traffic Policy for the OTT service (QoS parameters, like bandwidth, delay or jitter).

If the user input is sufficiently complete to create the Service Template and Traffic Policy for the new OTT service, then these are created and stored, and the scenario ends. Assuming incomplete input, self-learning by the (N)BTF may be used to complete the process.

4. AF Portal requests (N)BTF via RACS to activate the service recognition functionality and start trying to detect new traffic from/to the identified user.

5. De (N)BTF makes a snapshot of the traffic types currently running to/from the user, and starts looking for new traffic.

6. (N)BTF confirms to AF Portal via RACS.

7. AF Portal requests UE to start the OTT service for which NBAC support is needed. It may also request the user to suspend all other services in order to aid the service recognition process.

8. UE starts the OTT service.

9. This results in OTT service traffic from and to the UE, passing the (N)BTF.

10. (N)BTF creates and stores a Service Template based on the passing OTT service traffic. This Service Template can be used by the (N)BTF to recognize traffic from the specific OTT service.

11. (N)BTF sends the Service Template via RACS to the AF Portal for verification.

12. AF Portal provides feedback to UE on the Service Template and request conformation (and possible modification).

13. UE sends a confirmation to the AF Portal. Consequently, AF Portal provisions the NBAC system with the new Service Template.

At this point, the NBAC system knows how to recognize traffic from the new OTT service. However, it may not yet know the properties of the OTT service traffic and the associated Traffic Policy. Also this may be obtained through a self-learning process.

14. UE continues using the OTT service.

15. AF Portal confirms the Service Template for recognizing the OTT service traffic, and requests (N)BTF via RACS to start characterizing the traffic.

16. (N)BTF characterizes the traffic and creates a Traffic Policy.

NOTE 2: (N)BTF could e.g. measure the average bandwidth consumed, the variability of the bandwidth consumed, and typical times between up- and downstream messages of the OTT service to get an indication of the required responsiveness.

17. (N)BTF sends the Traffic Policy via RACS to the AF Portal for verification.

18. AF Portal provides feedback to UE on the Traffic Policy and request conformation (and possible modification).

19. UE sends a confirmation to the AF Portal. Consequently, AF Portal provisions the NBAC system with the new Traffic Policy.

From this point, the NBAC service knows how to recognize the new OTT service traffic (Service Template) and it knows what Traffic Policy should be applied. Now, the user can request NBAC support for the new OTT service using scenarios A or B.

6.8 Peer-4-peer initiative

Peer-to-peer traffic is growing dramatically. Some recent estimates have indicated that the aggregated traffic of P2P applications contributes to approximately 50 % to 80 % of Internet traffic (see [i.20]). This tremendous volume poses significant challenges to network traffic control, i.e. to the efficient utilization of the network resources owned by network providers. In addition to the volume, it is also the network-oblivious characteristic of p2p traffic that causes the problem as well. P2P traffic connects random peers, and, therefore, can unnecessarily traverse multiple links within a provider's network, leading to much higher load on some backbone links. While some connections are formed within an ISP, most P2P connections are to and from the rest of the Internet, resulting in high cost and bandwidth pressure on ISP peering and transit links with other networks [i.21], which may lead to serious disruption of ISP economics. In order to handle this problem, ISPs can either extend their infrastructure (which is cost inefficient) or deploy different tactics to manage their bandwidth, in response to which the P2P networks take steps to conceal their networks from management tools, leading to an unproductive back-and-forth between the P2P networks and the ISPs.

Therefore, some believe that it would be more effective to focus on cooperative approaches to address this challenge, which is how Proactive network Provider Participation for P2P (P4P) emerged [i.22].

The objective of P4P technology is to interconnect local peers as much as possible. P4P neither substitutes nor controls P2P networks. P4P allows the P2P networks to optimize traffic within each ISP, which not only reduces the volume of data traversing the ISP's infrastructure, but also creates a more manageable flow of data. This is achieved by providing additional information regarding network topology that P2P networks may choose to utilize to optimize network data delivery. P4P works by having an ISP deploy an "iTracker", that provides information on the network configuration of the ISPs. P2P client software (tracker) queries the i-Tracker to obtain the information on the preferred data routes, and on the connections to be avoided, which varies according to the time of day. The P2P software can then co-operatively connect to peers that are closer or cheaper for the ISP, selectively favouring peers instead of choosing peers randomly. In addition to the network topology information, information on the observed peer data transfer rates can also be utilized, so that a P2P network has a choice between a "nearby" peer that is slow, and a "far" peer that is fast. Because implementation of P4P is entirely voluntary on the part of both the ISPs and the P2P networks, it will only be adopted if it is mutually beneficial.

Recently, several ISPs and Universities performed a first major P4P trial [i.23]. The first results indicated that, when compared to a random swarm, the use of any iTracker provided substantial speed boosts to network users, ranging from 57 % to 85 % above default behaviour. Furthermore, the field tests have shown that P4P leads to a huge reduction in data delivery average hop count (from 5,5 to 0,89), resulting in significantly lower cost to ISPs. Furthermore, total external (peering) link load dropped by as much as 42 % (outbound) and 35 % (inbound). Finally, normalized load on internal backbone links dropped by as much as 71 % on average.

6.9 IETF Application-Layer Traffic Optimization (ALTO)

The ALTO working group designs and specifies an Application-Layer Traffic Optimization (ALTO) service that will provide applications with information to perform better-than-random initial peer selection. ALTO services may take different approaches at balancing factors such as maximum bandwidth, minimum cross-domain traffic, lowest cost to the user, etc.

Related documents:

- A "problem statement" document providing a description of the problem and a common terminology.
  Which is published as RFC 5693 [i.25].

- A requirements document that will list requirements for the ALTO service, identifying, for example, types of information P2P applications may need for optimizing their choices.
  Which is currently work in progress as draft-ietf-alto-reqs.

In the context of the work in TISPAN this concept can be used to create managed P2P overlay networks which can suite the requirements of an operated overlay network by utilizing the benefits of the P2P topology.

6.10 Peer-to-Peer Session Initiation Protocol (p2psip)

The Peer-to-Peer (P2P) Session Initiation Protocol working group (P2PSIP WG) is chartered to develop protocols and mechanisms for the use of the Session Initiation Protocol (SIP) in settings where the service of establishing and managing sessions is principally handled by a collection of intelligent endpoints, rather than centralized servers as in SIP as currently deployed.

Related documents:

- A SIP Usage for RELOAD
  Which is currently work in progress as: draft-ietf-p2psip-sip
- REsource LOcation And Discovery (RELOAD) Base Protocol.
  Which is currently work in progress as: draft-ietf-p2psip-base
- P2PSIP Overlay Diagnostics
  Which is currently work in progress as: draft-ietf-p2psip-diagnostics

This ongoing work is based on the SIP protocol which is the protocol for the TISPAN NGN usage. These studies and concept can be adapted to the required functionality within the TISPAN needs for P2P usage.

6.11 Network-Aware P2P-TV Application over Wise Networks (NAPAwine)

Within this EU project a managed IPTV distribution system is investigated which relies on P2P technology with at the same time a network aware control mechanism of steering the peers in creating the overlay [i.26].

TV services over the Internet can be provided by a variety of ways, e.g. exploiting IP multicast functionalities, relying on a pure end-to-end (P2P) approach, using adaptive streaming and CDN either exploiting IP multicast functionalities or relying on a pure end-to-end (P2P) approach. The first technique unfortunately, will only work on a network infrastructure controlled by a single broadband operator due to limitations of IP multicast facilities. On the contrary, the P2P approach has been successfully exploited to overcome these limits and can potentially offer a scalable planetary infrastructure. Recently, several P2P-TV systems started to show up, with the last generation offering High Quality TV (P2P-HQTV) systems, providing a ubiquitous access to the service. These same potentialities of P2P-TV systems constitute a worry for network carriers since the traffic they generate may potentially grow without control, causing a degradation of quality of service perceived by Internet users or even the network collapse (and the consequent failure of the P2P-HQTV service itself!).

With the NAPAwine concept these problems can be resolved by having a network aware mechanism to assist the peers in their overlay creation. This allows active control of the P2P service by providing input by e.g. the network/service operator.

Detailed information can be found on: http://www.napa-wine.eu.

7 Customer profiling legal aspects

Regarding legal aspects of customer profiling, there are two different issues that are involved:

- Navigation data collection process
- The association of collected data to customer's identity

Navigation data collection can silently operated but the solution must be able to ensure a level of anonymity such that the navigation data extracted from the network are never bind to the user identity without his explicit consent. In any case the solution must guarantee a confidentiality level of managed information higher than the one imposed by existing legislation on privacy.

8 For further study

The following areas are not addressed in this Technical Report and remain for further study.

- Network management
  - Traffic management
  - OAM and troubleshooting
  - Routing in the overlay network
- Security
- Business models
  - Charging
- Numbering and addressing
  - Naming and indexing
- Interconnection
  - Concatenation of peer-to-peer ("NNI")
- Legal aspects
  - Naming and indexing

9 Epilog

This clause is looking towards possible future ETSI TISPAN activities related to IPTV P2P.

As shown in the introduction, the present document covers a wide range of application of P2P technology, varying from a fully IPTV-Service-Provider-internal approach to Content Delivery Networks to having no Service Provider or Network Operator involvement at all. Therefore, this epilog differentiates its considerations consequently.

9.1 P2P for IPTV SP internal content delivery

Clauses 6.2 and 6.3 show P2P-based architectures for provider-internal content delivery. The two main variations are caching without or with UE involvement.

9.1.1 P2P for IPTV SP internal CDN

ETSI TISPAN document TS 182 019 [i.27] specifies a Content Delivery Network (CDN). Application of P2P in this architecture would involve direct exchange of content between Content Delivery Functions (CDF).

So this type of functionality could be introduced in a Work Item related to TS 182 019 [i.27], or in a future release.

9.1.2 P2P for in a IPTV SP CDN involving UE

The concept of actively loading and caching content on User Equipment (UE) has already been specified with the concept of the Client Personal Video Recorder (C-PVR) in ETSI TISPAN documents TS 182 027 [i.1] and TS 182 028 [i.2]. However, the C-PVR functionality in the UE, controlled by the network, focuses on (pre-)loading/recording/storing/caching content for the specific user of that C-PVR.

Using UEs as distributed caches for IPTV Service Provider content delivery is new to ETSI TISPAN. Several aspects of this approach remain to be studied:

- Digital rights. How can IPTV Service Provider guarantee that the digital rights of the Content Provider are not violated?
- User control and social networking. What degree of control can the user have on the storing and distribution of content on his/her UE? What role could social networking play, e.g. support of storing and delivery of content for friends?

So any further activity on CDN functional elements instantiated in the UE would likely require a new or expanded Work Item.

9.2 Active IPTV SP support of user-to-user P2P

Clause 6.8 introduced the Peer-for-Peer (P4P) initiative, which enables network operators to actively support P2P content exchanges between its users. This support could involve caching of content, indexing of content and other support to achieve more efficient routing of content. The rationale behind this approach is that more efficient use of the network would postpone or reduce network capacity investments.

There are no ETSI TISPAN activities related to user-to-user P2P at the time of writing of the present document. More study would be needed to discover what (if anything) ETSI TISPAN should do in this area.

9.3 Network-Based Access Control (NBAC)

Clause 6.7 provides an extensive description of Network-Based Access Control (NBAC). NBAC technology enables users to reserve bandwidth for specific Over-The-Top (OTT) applications, which include P2P exchange of content. NBAC can be seen as an extension of the NGN RACS subsystem, as described in ES 282 003 [i.24], but a detailed description of the NBAC system could require a new document.

The specification of NBAC functionality may be performed in one or more new Work Items.

Annex A:
Network Based Application Control flow diagram example

Below there is a brief description of the interactions between the systems, according to the previous example, we assume that user has subscribed to the proposed service, that allows to watch contents with QoS; The service is, for example, a prepaid time-based service and the user must accept it on a per-content basis:

1. The user asks for a content using a browser.
2. The content provider server sends the content to the user.
3. The NBAC enabled device triggers the flow (analyzing the HTTP signalling protocol) and notifies to RACS that the user has asked for a content. The user's request can be put in a wait status using a controlled redirection (e.g. HTTP 3xx) towards a proper web server, or temporarily forwarded in a best effort mode.
4. RACS performs admission control on the flow and, in case the result is positive, it reserves the necessary resources.
5. RACS notifies to an AF the resource reservation for that specific user.
6. The "prepaid QoS service" AF asks to the user to confirm that he wants to receive the content with quality.
7. The user confirms or refuses.
8. The service logic notifies the user's response to RACS.
9. RACS commits the reservation and enforces a policy for that particular flow.
10. The content continues (or restarts, if it was in wait status) to flow in the assigned QoS.

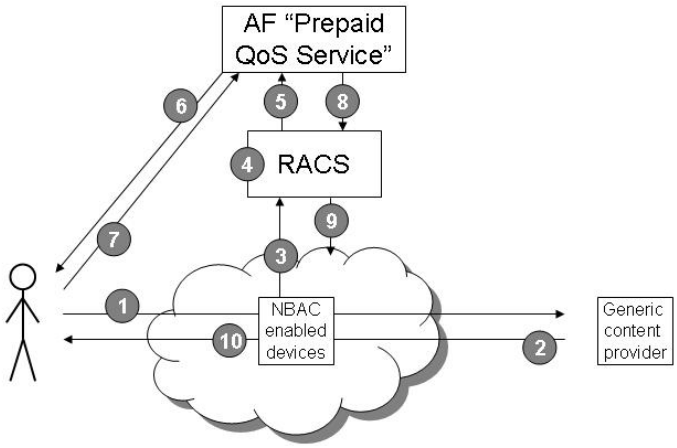


Figure A.1: Network Based Application Control flow diagram example

As "prepaid" is intended a commercial offer regarding a generic service (in this case QoS) where the service is paid for in advance gaining a credit that will be deducted based on one or more fee/charges (i.e. prepaid phone cards).

Annex B: Bibliography

Stephanos Androutsellis-Theotokis and Diomidis Spinellis: A survey of peer-to-peer content distribution technologies. ACM Computing Surveys, 36(4):335–371, December 2004 (doi:10.1145/1041680.1041681).

X. Hei, C. Liang, J. Liang, Y. Liu and K.W. Ross: "A Measurement Study of a Large-Scale P2P IPTV System", IEEE Transactions on Multimedia Volume: 9, Issue: 8 pp. 1672-1687 (2006).

Rowstron A., Druschel P.: Pastry. "Scalable, Distributed Object Location and Routing for Large-scale Peer-to-Peer systems", In 18th IFIP/ACM International Conference on Distributed Systems Platforms Heidelberg, (2001).

Siddhartha Annapuredd, Saikat Guha, Christos Gkantsidis: Is HighQuality VoD Feasible using P2P Swarming?, WWW 2007.

History

Document history		
V3.1.1	February 2010	Publication