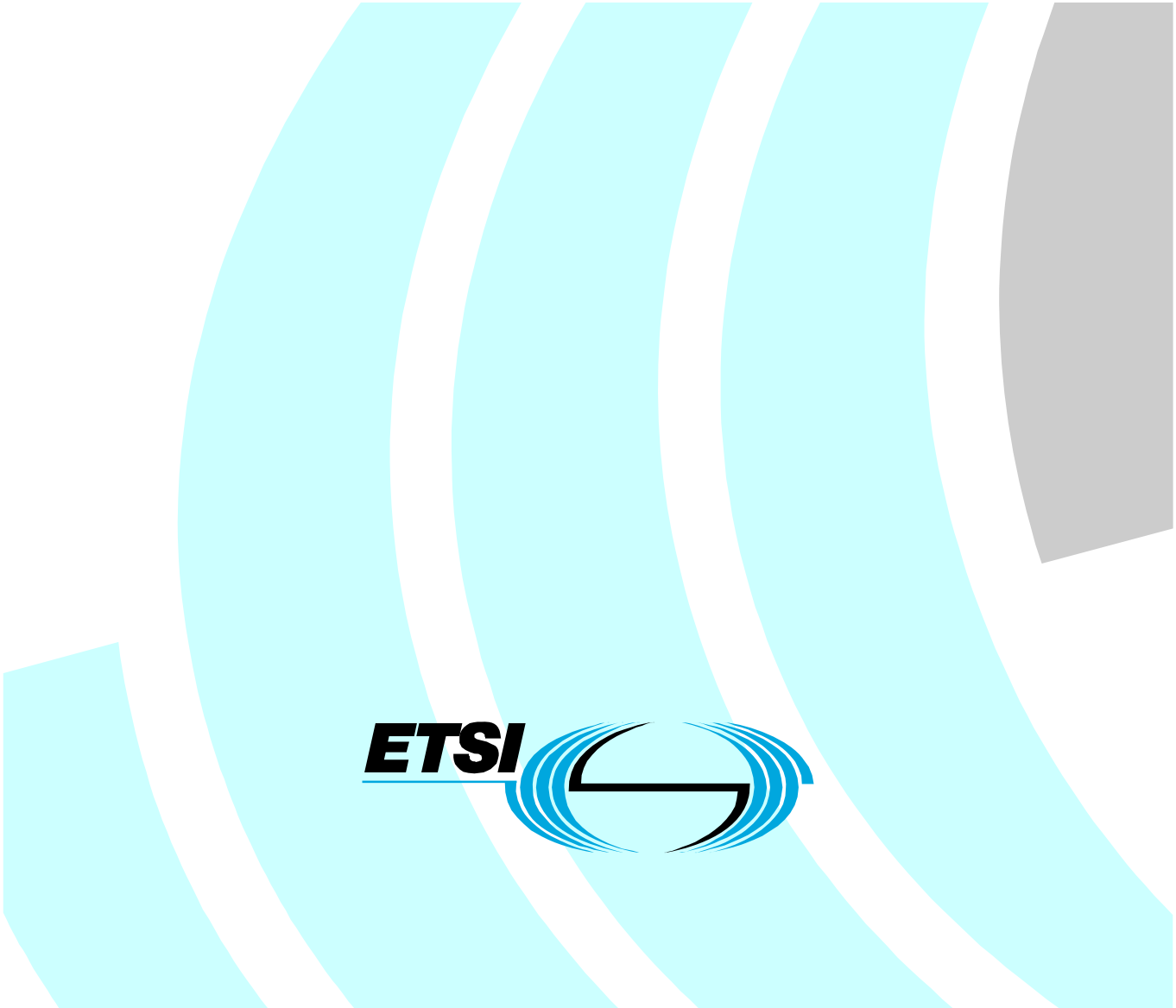
ETSI TR 185 012 V3.1.1 (2010-07)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study of security mechanisms for customer premises networks connected to TISPAN NGN



Reference
DTR/TISPAN-05021-NGN-R3

Keywords
gateway, security

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

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

The present document explores possible solutions to comply to the security requirements of TS 187 001 [i.1].

1 Scope

The present document presents the results of a study into the feasibility of providing security mechanisms to be implemented in a Customer Premises Network (CPN) that allow the CPN to comply with the security objectives and requirements of the CPN. The present document identifies the placement of measures in the Customer Network Gateway (CNG) and in the Customer Network Devices (CNDs) that support the end-to-end security architecture of NGN release 3 as defined in TR 180 001 [i.20] (NGN-R3 release definition) and TS 187 003 [i.18] (security architecture).

The present document completes task 7 of the TVRA method defined in TS 102 165-1 [i.21] with due account of the remainder of the TVRA for CPNs presented in TR 185 008 [i.13] and TR 187 002 [i.17].

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

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 necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 187 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[i.2] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Vocabulary for 3GPP Specifications (Release 7) (3GPP TR 21.905)".

[i.3] ISO/IEC 7498-2: "Information Processing Systems - Interconnection Reference Model - Part 2: Security Architecture".

[i.4] IETF RFC 5209 (June 2008): "Network Endpoint Assessment (NEA): Overview and Requirements".

[i.5] ETSI TS 133 234: "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Wireless Local Area Network (WLAN) interworking security (3GPP TS 33.234 version 9.1.0 Release 9)".

[i.6] ETSI TS 133 203: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Access security for IP-based services (3GPP TS 33.203 version 9.3.0 Release 9)".

[i.7] ETSI TS 133 110: "Universal Mobile Telecommunications System (UMTS); LTE; Key establishment between a UICC and a terminal (3GPP TS 33.110 version 9.0.0 Release 9)".

[i.8] ETSI TS 185 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Services requirements and capabilities for customer networks connected to TISPAN NGN".

[i.9] ETSI TS 185 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Devices architecture and Reference Points".

[i.10] IETF RFC 1827: "IP Encapsulating Security Payload (ESP)".

[i.11] ETSI TR 187 009: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study of prevention of unsolicited communication in the NGN".

[i.12] ETSI TS 185 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Network Gateway (CNG) Architecture and Reference Points".

[i.13] ETSI TR 185 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Analysis of security mechanisms for customer networks connected to TISPAN NGN R2".

[i.14] UPnP Forum: "Internet Gateway Device (IGD) Standardized Device Control Protocol V 1.0".

NOTE: Available at http://www.upnp.org/standardizeddcps/igd.asp.

[i.15] IETF RFC 2663 (1999): "IP Network Address Translator (NAT) Terminology and Considerations".

[i.16] Home Gateway Initiative: "Home Gateway Technical Requirements V 1.0".

[i.17] ETSI TR 187 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN-SEC); Threat, Vulnerability and Risk Analysis".

[i.18] ETSI TS 187 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".

[i.19] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.20] ETSI TR 180 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; Release definition".

[i.21] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.22] IETF RFC 3261: "SIP: Session Initiation Protocol".

[i.23] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[i.24] IEEE 802.16-2009: "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems".

[i.25] Broadband Forum Technical Report TR-069: "CPE WAN Management Protocol v1.1".

[i.26] IEEE 802.1x-2010: "IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control".

[i.27] IEEE 802.1B-1992: "Local and Metropolitan Area Network: LAN/MAN Management".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

authentication: property by which the correct identity of an entity or party is established with a required assurance

NOTE: The party being authenticated could be a user, subscriber, home environment or serving network (see TR 121 905 [i.2]).

authorization: granting of permission based on authenticated identification (see ISO/IEC 7498-2 [i.3])

NOTE: In some contexts, authorization may be granted without requiring authentication or identification e.g. emergency call services.

3.2 Abbreviations

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

AKA	Authentication and Key Agreement
AV	Anti-Virus
B2BUA	Back to Back User Agent
C-BGF	Core-Border Gateway Function
CND	Customer Network Device
CNG	Customer Network Gateway
CPN	Customer Premises Network
DOS	Denial of Services
FTTx	Fiber To The x
HGI	HoMe Gateway Initiative
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IGD	Internet Gateway Device
IGD	Internet Gateway Device
IMS	IP Multimedia Subsystem
IPSEC	Internet Protocol SECurity
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MCF	Media Control Function
MDF	Media Delivery Function
MF	Media Function
MPLS	Multiple Protocol Label Switching
NAC	Network Access Control
NAPT	Network Address and Port Translator
NAT	Network Address Translation
NBA	NASS Bundled Authentication
NEA	Network Endpoint Assessment
NGN	Next Generation Network
NTP	Network Time Protocol
P-CSCF	Proxy-Call Session Control Function
PDA	Personal Digital Assistant
POP3	Post Office Protocol version 3
PUC	Prevention of Unsolicited Communication
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SIP	Session Initiation Protocol
SMTP	Simple Mail Transport Protocol
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer

TCP	Transmission Control Protocol
TLS	Transport Layer Security
TVRA	Threat Vulnerability and Risk Analysis
UC	Unsolicited Communication
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTM	Unified Threat Management
VCR	Video Cassette Recording
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
xDSL	x Digital Subscriber Line

4 General overview

As noted in TR 185 008 [i.13] security problems in the CPN may have two origins:

- internally to the CPN; or
- externally to the CPN.

The CPN, consisting of a CNG and a number of CNDs, is connected to the NGN as if it were a single NGN terminal connected for signalling purposes through the Gm reference point. Protection of the NGN interconnection and thus protection of the CPN from NGN attacks is out of scope of the present document but is covered by the following documents TS 187 001 [i.1], TR 187 002 [i.17] and TS 187 003 [i.18].

The CNG offers services to the CNDs within the CPN and the protection of the CNG and its connected CNDs is considered in the present document. However the boundary of the CPN may be compromised by the technologies offered by the CNG and by the CNDs themselves, e.g. a wireless connection between CND and CNG as a broadcast.

The security objectives to be met by the CPN are as follows:

- Confidentiality
    1. Information sent to or from a registered user of a CPN should not be revealed to any unauthorized party.
    2. Information held within the CNG should be protected from unauthorized access.
    3. Details relating to the identity and service capabilities of a CPN user should not be revealed to any unauthorized 3rd party within the CPN or in the wider NGN.
    4. Management Information sent to or from a CPN should not be revealed to any unauthorized party.
    5. Management Information held within a CPN should be protected from unauthorized access.
- Integrity
    1. Information held within the CNG should be protected from unauthorized modification and destruction.
    2. Information sent to or from a registered user of a CPN should be protected against unauthorized or malicious modification or manipulation during transmission.
    3. Management Information held within a CNG should be protected from unauthorized modification and destruction.
    4. Management Information sent to or from a CPN should be protected against unauthorized or malicious modification or manipulation during transmission.

- Availability

    1. Services provided within a CPN should be available only to authorized users of the CPN upon request whether they are attached to an access point within the CPN or to an access point within the wider NGN.

    2. Services provided within a CPN should be accessible and usable on demand only to authorized users of the CPN.

- Accountability

    1. The use of the CPN services should be recorded such that the owner of a CPN should only be billed for legitimate use of chargeable CPN and NGN services.

- Authenticity

    1. It should not be possible for an unauthorized user to pose as an authorized user when communicating with an application or other user of a CPN.

    2. It should not be possible for a CPN to receive and process management and configuration information from an unauthorized user.

    3. Access to and the operation of services by authorized CPN users should not be prevented by malicious activity either in the CPN or in the wider NGN.

- Non-Repudiation

    1. None.

- Reliability

    1. None.

The security functional capabilities for CPN are modelled on the classes of ISO/IEC 15408-2 [i.19] and described in TS 187 003 [i.18]. The security requirements to the CPN are documented in clause 4.19 of TS 187 001 [i.1].

5 Authentication and authorization mechanisms

The basis of identification may be one or more of the following:

- Something the entity knows such as passwords or keys.
- Something the entity possesses such as UICC or hardware token improving the security of authentication mechanisms.
- Something inherent to the entity such as fingerprints or retinal characteristics.

The preferred method for user and service authentication is IMS-AKA. To fully implement the IMS-AKA framework, a UICC is needed into the CPN device which is terminating the IMS security association.

To be compliant with TS 187 001 [i.1], there are other two methods to be considered: Http Digest and NBA.

The mechanisms for the user's authentication in the TISPAN context are enablers for legacy terminals to access the IMS services. In that sense, IMS-AKA and HTTP Digest should be supported by the CNG and may be supported by CNDs. If not supported by CNDs, the CNG can play an active role in completing the procedure, as also described in TS 185 006 [i.9].

5.1 Authentication issues in the Gm'

The Gm' reference point supports the communication between one SIP non-IMS CND (e.g. IETF SIP) and the CNG, e.g. related to registration and session control. The difference between Gm and Gm' is related to the conformance to the IMS and to the need to go through the B2BUA to support local services. Further details about Gm' can be found in the TS 185 003 [i.12] and TS 185 006 [i.9].

In order to strength the security within the CPN, it is necessary to define specific authentication mechanism to be enforced between the CND and the CNG (i.e. Gm'). Threat scenario foresees rogue CND that, violating the local security of the CPN, reaches the IMS through the CNG and could cause security violations such as theft of services, Denial of Services, privacy violations and so on.

5.1.1 Applicability and limitations

Given that IETF SIP protocol mandates the support of Digest authentication (RFC 3261 [i.22]), the main security mechanism to be implemented in the Gm' is the Digest Authentication as described in the RFC 2617 [i.23].
RFC 2617 [i.23] (and its application to the SIP protocol described in the RFC 3261 [i.22]) describes an open framework with different options to be implemented
(e.g. single-way vs. mutual authentication, integrity protection, and others).

The main issue with SIP Digest is the key management, because subscriber-specific information (e.g. SIP key) needs to be installed on the CNDs.

This clause does not contain a complete analysis.

5.1.2 Implementation details

Two main use cases are possible for the CNG in the Gm':

1) The SIP B2BUA is collocated in the CNG; or

2) The CNG has not a SIP B2BUA but it is a SIP proxy from the CND point of view.

The local authentication (between the CND and the CNG) on Gm' could be based at least on the following mechanisms:

- SIP Digest authentication as defined in the RFC 2617 [i.23] (and also in the RFC 3261 [i.22]).
- By extending to the service layer the successful identification/authentication performed at the network (or below) layer, such as IEEE 802.1x [i], MAC address access list or similar layer 2 or 3 mechanisms.

When the SIP B2BUA is available in the CPN (see figure 1), the CNG can perform the IMS authentication on behalf of the CNDs by using its own IMS (UICC or Digest key) credential.

On the Gm the full IMS-AKA is supported (UICC, AKA and IPSEC).

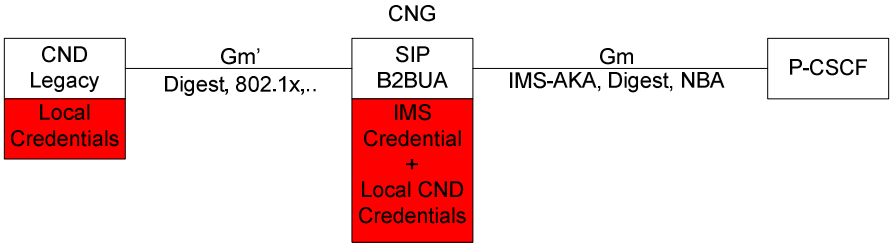


Figure 1: Gm' with a B2BUA in the CNG

When the CNG acts as a SIP Proxy (figure 2) the CNG cannot perform the authentication on behalf of the local CND (because a SIP UA is not available in the CNG) and every CND has to be authenticated directly to the IMS. In such a scenario the SIP non-IMS CND could not authenticate directly to the IMS (e.g. the P-CSCF) by using the TISPAN Digest authentication mechanism but using the NBA only (note that the Sip Digest defined in the [i.6] is a customization of the RFC 2617 [i.23]). Anyway the CNG could authenticate the local CND by using several mechanisms such as Sip Digest (RFC 2617 [i.23]) or access level authentication mechanisms (e.g. MAC address access list, IEEE 802.1x [i] and so on).

To sum up the CNG with a SIP proxy does not register itself to the IMS, letting the CNDs to register themselves to the IMS by using their own user credentials. On Gm', the full IMS-AKA is NOT supported (AKA and IPSEC) and possible restrictions could limit the applicability of TISPAN DIGEST authentication (depending on the SIP Proxy capabilities on the CNG).

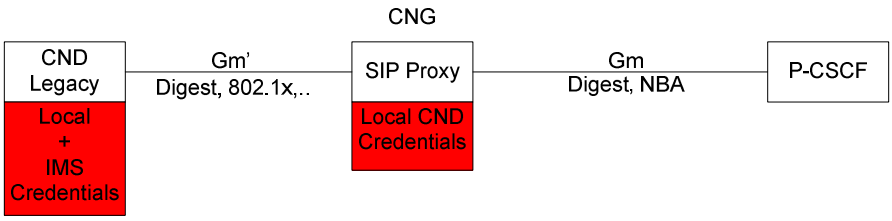


Figure 2: Gm' with a SIP Proxy in the CNG

6 Security Management functionality

CNDs Security management functionality addresses both local and remote access security.

For the local security, it will control all the local exchanges between the devices inside the CPN.

Concerning external security, this will cover the cases of remote management, both from the user (e.g. remote activation of a VCR, remote control of a camera, etc.) or from the network provider (e.g. remote update of the gateway's network data).

These security tasks may be accomplished with the support of additional features, like the authentication features embedded in some chipsets (Trusted Platform Module) or UICC inserted in the CNG that may contain credentials, security algorithms and also other configuration parameters (e.g. some policy rules for the firewall).

7 Firewall

The main mechanism to perform Network Access Control is a firewall, i.e. a system designed to permit, deny or proxy data traffic to or from the customer's network. A firewall is positioned to control all incoming and outgoing traffic; hence the CNG is the perfect candidate to perform the firewall functions.

There are several approaches to implements firewall functionalities, such as:

- Packet Filtering: the simplest one inspects each incoming or outgoing IP packet permitting, dropping or rejecting it on the basis of simple policies (usually defined as access control list) such as the IP address and the protocol type.
- Stateful Firewall: in addition to a Packet Filter, keeps track on IP packets belonging to the same connection thereby detecting whether a packet is part of an existing connection or a start of a new connection.
- Application Level Gateway: In addition to a stateful firewall can understand the behaviour of some applications and can detect e.g. if an illegal protocol is used for a given application or dynamically open ports for additional sessions belonging to a flow.

Firewalls can divide the network into subnets each one with a different level of security and different security policy as for example a demilitarized zone.

The firewall could have several configuration alternatives:

- A basic/minimum configuration to ensure a minimum level of security.
- One or several default configurations provided and managed by the operator/service provider through a remote management system.
- Additional alternative configurations that can depend on the user (e.g. there can be different configurations for parents and children). These user specific configurations could be managed by the same entity managing the user identity (e.g. the UICC).

7.1 Basic description

In the CPN context, the CNG sits between the NGN and the internal network and this aspect makes the CNG as the perfect candidate to host the firewall functions. Figure 3 shows a typical scenario where the CNG and the Firewall are co-located on the same device. The external interface is the one that is connected to the NGN via e.g. xDSL, IEEE 802.16 [i.24] wireless modem, FTTx, etc., and is often referred to as the unsecure (red) interface. The secure (black) internal interfaces are connected to the CNDs and can be based on ethernet, IEEE 802.1B [i.] and other wired or wireless communication technologies.

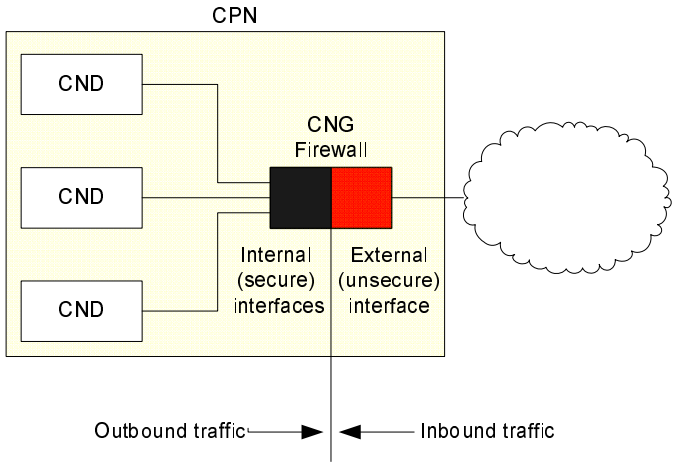


Figure 3: Firewall in the CPN

The advantages of using a Firewall as shown in the picture (i.e. co-located on the CNG) is that the CNG appears to the external network (i.e. NGN) as the only point of contact for the CPN, simplifying the protection of the CNDs against threats that originate on the NGN.

7.2 Applicability and limitations

The Firewall in the CNG should be designed to protect CPN users against threats originating from the external interface, the NGN. The main goal is to provide a baseline intrusion prevention mechanism protecting against scans for information and denying all unsolicited inbound traffic in order to stop or limit security attacks originating from the NGN.

One of the drawbacks related to the Firewalls deployment is that they have typically been difficult to manage and to configure. This point is particularly important in the CPN context and then the firewall should provide a simple but effective security experience for example by providing a simple user interface for managing the security policies. A simple firewall configuration tool should eliminate the configuration problems for end users while still providing flexibility to customize advanced settings.

This clause does not contain a complete analysis.

7.3 Implementation details

For the protection of the CPN, a firewall should support the some basic features, such as security policy definition and enforcing, firewall management, logging functions and so on. The following clause describes in details such features.

7.3.1 Stateful Inspection

TS 185 005 [i.8] requires a stateful inspection firewall to secure the CPN: "*CPN environment shall be protected with a stateful firewall function, which may be implemented in the CNG*". While a packet filter decides whether or not to drop a packet based on few information contained in the packet headers (e.g. addressing information), a stateful packet filter takes its decisions also on the state information that the firewall keeps in memory about all active connections travelling across it.

For connection-oriented protocols, such as TCP, the state of the connection is equivalent to the protocols definition of a connection (e.g. three-way handshake), whereas for a connection-less protocol, such as UDP, the state of the connection is the set of packets that are sent between common endpoints (e.g. source IP address/port and destination IP address/port) without interruption (i.e. the lack of any packets matching that flow for a given period of time e.g. one minute).

The stateful firewall also performs additional structural checks on network packets. These checks include e.g. quickly dropping of malformed packet and enforcing the TCP three-way handshake to establish and teardown network connections.

7.3.2 Communication technologies

The Firewall should be enabled on the local CPN network including all kind of wired and wireless connectivity used on the CPN, as well as remote access connections such as PPP over Ethernet and Virtual Private Network on the WAN side of the CNG. Note however that the firewall cannot be enabled when the CNG acts as a network bridge.

IPv6 firewalling is needed in case the CNG supports IPv6 traffic.

7.3.3 Security Policy

The firewall could have several configuration alternatives. In order to simplify the management of the security policy and still provide a basic level of security to the CPN it is proposed to define one or more security profiles.

As defined by HGI in [i.16] at least the following basic configurations should be supported by the firewall: *HIGH* security configuration and *LOW* security configuration.

The *HIGH* security configuration foresees the following behaviour:

- For the traffic originated from the NGN toward the CPN (inbound): to refuse connections in TCP, UDP and ICMP; to authorize already established connections only (and known by the stateful firewall).
  Based on the Operator/Service Provider local policy, the firewall could accept incoming connections for specific services/ports, such as 5060 for SIP (e.g. inbound SIP calls).

- For the traffic originated from the CPN toward the NGN (outbound): to authorize only well known ports, such as:

  - 25 - SMTP
  - 80 - HTTP
  - 443 - SSL
  - 554 - RTSP
  - 995 - POP3
  - 123 - NTP
  - 5060 - SIP

A second alternative basic firewall configuration should be supported by the firewall, the *LOW* security configuration: all traffic (inbound and outbound) is authorized by default. Anyway the stateful firewall still performs the security check on the TCP/UDP active sessions.

Also Internet Control Message Protocol (ICMP) messages should be managed because these messages can be used in hacking and DOS attacks. The firewall should block or allow specific ICMP options (e.g. Echo Requests, destination unreachable).

Additional alternative configurations can depend on the user preferences and/or Operator/Service Provider local policy.

7.3.4 ALG for standard protocols support

Also a stateful firewall is not effective or could limit specific services with applications that include IP addresses and TCP/UDP port information in the payload (e.g. FTP, SIP protocols, peer to peer applications). To filter these protocols, and at the same time permit the access to such services, the firewall has to be augmented by specific Application Level Gateway.

The firewall should contain support for the NGN standard protocols, such as SIP and RTSP, for the pinholing of the media ports so that the inbound and outbound traffic could flow through the CNG.

Note that when B2BUA is implemented inside the CNG [i.12], it acts as a SIP ALG; in this case the B2BUA needs to interact with the firewall.

7.3.5 Firewall management

The firewall should be manageable from the CPN and by the IPS/Operator and it should enable the ISP/Operator also to upgrade the firewall functionality via download of a new configuration file. To implement this operation, the management centre downloads to the CNG firewall the configuration file. This file integrates the basic firewall configuration that includes the HIGH and LOW configurations. As described by HGI in [i.16], DSL Forum TR-069 [i.25] provides mechanisms for configuration file downloads. However, some additional mechanisms and specifications could be needed to fully support the CPN security requirements, for example OMA device management which supports also the security of the management.

The management features should permit the upgrade of the software firewall, the management of the security policy and the access to the logging information.

7.3.6 Logging

The firewall should have the ability to log network traffic and main security events. Basic logging options should be supported (by default all logging options should be disabled). The logging function should capture at least the following events:

- Log of changes to firewall policy.
- Network connection logs, which include dropped and rejected connections (for both inbound and outbound packets).
- Log of software firewall upgrade events.

The log files should be accessible from the remote management.

NOTE 1: Time synchronization of the device is also important for security reasons (e.g. certification expiration).

NOTE 2: Log storage: It is for further study where to keep/send the log.

8 Network Access Control (NAC)

The Network Access Control (NAC) is a gathering of methods linked to the control of a network's access. In term of security, these methods aim to control access to a network with policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do. The combined tools used are usually enforced authentication, security policies for users, management of network resources, verification tools for security updates, and directory management.

8.1 Basic description

The IETF NEA [i.4] architectures have been defined to assess the "posture" of endpoint devices for the purposes of monitoring compliance to an organization's posture policy and optionally restricting access until the endpoint has been updated to satisfy the posture requirements. Posture refers to the hardware and software configuration of an endpoint and may include knowledge that software installed to protect the device (e.g. patches, anti-virus, firewall, host-based intrusion detection system or any custom software) is enabled and up-to-date.

In the CPN context, the NEA architecture could be used to allow only compliant and trusted Customer Network Devices (CND), such as PCs, IP-phone, and PDAs, onto the network, restricting or blocking the access (at the network layer) of noncompliant devices, and thereby limiting the potential damage from security threats and risks. Then NEA allows operators and service providers to enforce specific security policies on all CND as they enter the customer premises network, regardless of their access methods, ownership, device types, application configurations, etc.

The general NEA architecture is a client-server architecture, where the server component evaluates the posture of an endpoint device and provides network authorization decisions. Moreover the NEA server interacts with the NEA client (i.e. CND) by means of a specific software agent installed on each managed element. Usually such agents have a small footprint and low impact on the CND activities. In the CPN context, the Customer Network Gateway (CNG) is the natural candidate to perform the NEA server role.

Figure 4 shows the general NAC architecture for a CPN environment. Depending on the business model and on the technologies adopted to implement the NAC services, different scenarios are possible. The main points to highlight are the following:

- CND controlled by means of a specific agent (called NAC client in the figure) able to check the local posture and enforce the policy locally. The agent could be both, installed permanently on the CND (e.g. at subscription time, the customer installs the agent on his CNDs such as PC, laptop and so on) or on demand and temporary installed by means e.g. of Java applet of other mobile code system.

- CND without any agent (permanent or temporary). Usually such devices cannot be managed by an agent because of their legacy/closed operative system (e.g. printer) or because explicitly required by the business model of the NAC service. Without an agent, it is necessary to assess the posture of the CND remotely by checking for vulnerability to attacks from the network. For example the CNG could be equipped with specific software able to look for open TCP/UDP ports, detect the Operative System type and detect applications running on a target system (i.e. the CND to be assessed). It is also necessary to define a separate enforcing point, e.g. on the GNG.

- NAC server implemented within the CPN e.g. in the CNG. In this case the NAC server is responsible for the security of the local CPN and checks the posture of the local CNDs depending on the policies locally defined by the customer or centrally defined by the Service Provider/Operator.

- The NAC server can reside inside the Operator's management network (e.g. in the NGN outside the CPN) and no specific software has to be installed on the CNG.

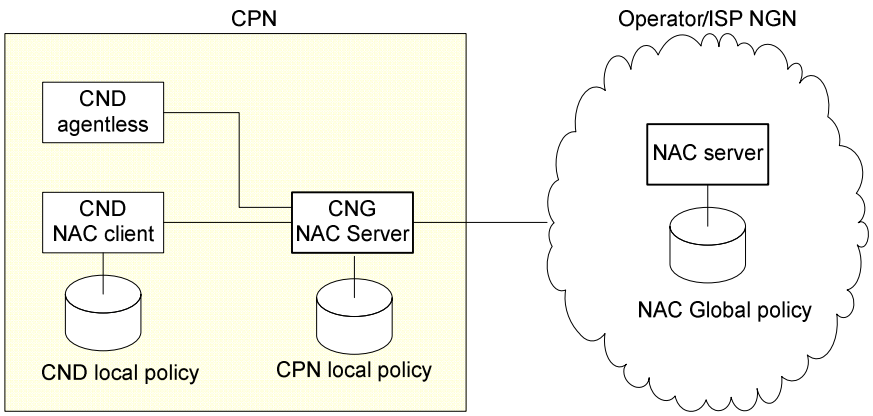


Figure 4: CPN NAC architecture

8.2 Applicability and limitations

NAC (and NEA) frameworks could provide significant benefits to the security of the CPN environments, among them the following are the most relevant:

- Assessment and identification of non-compliant CNDs.
- Centralized security policies definition.
- Monitoring of the CND's compliance over time.

In the CPN context the main issues are related to the implementation of the remediation process and the enforcement mechanisms. The implementation of a NAC service raises the expectation that some legitimate CNDs will be denied access to the CPN resources. Hence it is required a mechanism to remediate the CNDs vulnerabilities found during the assessment phase. There are at least two strategies for remediation: quarantine networks and captive portals. A quarantine network is a restricted IP network providing access only to certain hosts and applications (e.g. Antivirus server where the CND can download the latest signatures). Captive portals intercept access to web pages, redirecting users to a web application that provides instructions and tools for updating their devices. The enforcement point in the CPN can be implemented e.g. by defining specific security policy for the network firewall running in the CNG.

8.3 Implementation details

Figure 5 shows a sequence diagram related to a CND managed by means of a specific agent (i.e. NAC client). Such an agent could be permanent or temporary installed. The figure shows the NAC server implemented outside the CPN (e.g. in the Operator's network operation centre) but the same behaviour (with minimal changes) also apply to the scenario where the NAC server is implemented in the CNG.

On step 1, the NAC process begins e.g. at CND boot time when the agent starts its assessment process. It sends a request to the NAC server in order to retrieve the latest version of the security policy defined the specific CND. This step permit the alignment of the local policy to the centrally defined ones and it is optional (e.g. because the geographic link could be down whereas the local network services are still working).

On Step 2, the NAC server checks the latest version of the policy and, if an alignment is required, send to the NAC agent the new NAC policy.

After receiving the latest version of the policy (if available), the NAC agent begins to check the posture of the CND (e.g. by checking the presence of a properly configured personal firewall, up to date antivirus engine, up to date operative system patching and so on).

On step 3, depending on the posture evaluation result, the CND can finally access the CPN network resources or "quarantined" until a proper remediation action (not shown in the figure). The security policy is enforced by the NAC client.

On step 4, the NAC client sends (optional) the results of the evaluation process to the NAC server, in order to update the centralized database with the status of the managed CND.

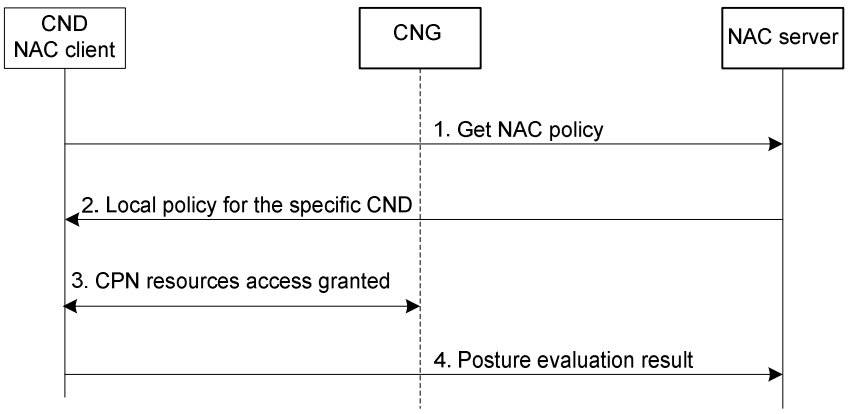


Figure 5: Agentful CND posture assessment process

Figure 6 show a possible implementation when the CND has not an agent installed and it is not possible to use a mobile agent (e.g. Java applet). In this scenario the CNG will play a fundamental role as locally policy enforcer and eventually as a local assessment device. The figure describes the scenario where the CNG acts also as a local NAC server.

On step 1, the CNG/local NAC server collects the MAC/IP address of the locally connected CNDs and detects the activities performed by a CND not yet assessed.

On step 2, once the CND has been recognized as an agentless CND, the local NAC server starts a network scanning in order to assess the posture of the CND. As an alternative strategy, it is possible to use a whitelist; mechanism of authorized CNDs. Whenever the MAC address of the agentless CND has been detected, if that MAC address is contained in the whitelist, than the corresponding device is automatically allowed to access the CPN resources.

On step 3, the CPN enforces the policy decision, for example it could allow the CND to access all the local resources, otherwise it could block any connection attempt originated form that CND.

On step 4, the NAC client sends (optional) the results of the evaluation process to the global NAC server, in order to update the centralized database with the status of the managed CPN.

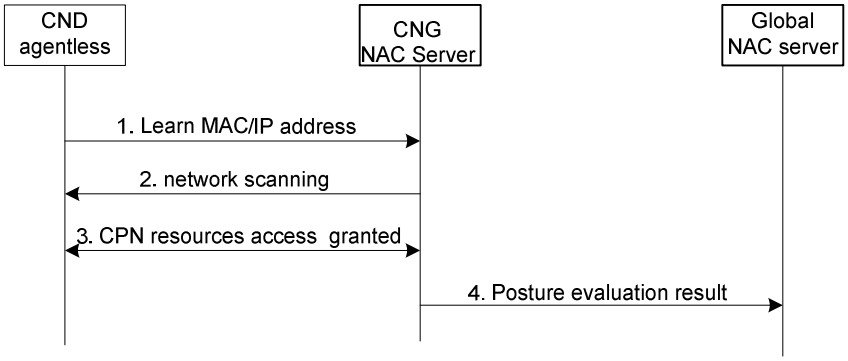


Figure 6: Agentless CND posture assessment process

9 Antispoofing

Spoofing is a technique consisting in using the IP address of a device in order to take over its identity. This technique allows the creation of IP packets with a source IP address belonging to someone else and can be used to tackle networks while being recognized as someone else and makes it possible to carry out DoS or unauthorized service access. Antispoofing functionality could help the protection of the NGN from attacks originated from the customer network.

Packet filtering is one defence against IP spoofing attacks. The gateway to a network usually performs ingress filtering, which is blocking of packets from outside the network with a source address inside the network. This prevents an outside attacker spoofing the address of an internal machine. Ideally the gateway would also perform egress filtering on outgoing packets, which is blocking of packets from inside the network with a source address that is not inside. This prevents an attacker within the network performing filtering from launching IP spoofing attacks against external machines.

It is also recommended to design network protocols and services so that they do not rely on the IP source address for authentication.

Some upper layer protocols provide their own defence against IP spoofing. For example, Transmission Control Protocol (TCP) uses sequence numbers negotiated with the remote machine to ensure that arriving packets are part of an established connection. Since the attacker normally cannot see any reply packets, he has to guess the sequence number in order to hijack the connection. The poor implementation in many older operating systems and network devices, however, means that TCP sequence numbers can be predicted.

10 VPN capabilities

A Virtual Private Network (VPN) is a communications network tunnelled through another network, and dedicated for a specific network. A VPN enables corporations or service providers to extend their services to employees and partners without the risk of compromising their integrity and confidentiality.

Different technologies (standard and proprietary solutions) can be adopted for VPN implementation such as encryption (IPSEC, Secure RTP (SRTP) to protect the payload, TLS, etc.) or traffic separation (e.g. MPLS).

Key management aspects have to be considered for further study.

10.1 VPN Capability Based on IPsec

IPsec can be used to create Virtual Private Networks (VPN), through its two different modes:

- transport mode (end-to-end).

  Only the transferred data of the IP packet is encrypted and/or authenticated. The routing is intact (as the IP header is not modified/encrypted), but when the authentication header is used, the IP addresses cannot be translated. Transport mode is used for host-to-host communications.

- tunnel mode (portal-to-portal).

  The entire IP packet (data plus the message headers) is encrypted and/or authenticated then encapsulated into a new IP packet for routing to work. Tunnel mode is used for network-to-network communications (secure tunnels between routers) or host-to-network and host-to-host communications over the Internet.

NOTE: In IPv6 it is mandated to support IPsec but optional to deploy, and it is optional to deploy IPsec for use with IPv4.

Reference to "WLAN 3GPP IP Access" of TS 133 234 [i.5], i.e. scenario 3, may provide basis for this VPN functionality.

10.1.1 Remote access case

The payload traffic that goes between the CPN and a remote access device is not protected in the remote access service context. In TS 133 203 [i.6], IMS-AKA and IPsec together provide authentication and integrity protection but only for the signalling traffic between the CNG and NGN. With HTTP Digest only authentication protection is provided. Therefore, there is also a need of integrity and confidentiality protection for the payload traffic.

IPsec might be used to establish an encrypted communication channel between the CNG and a remote access device. IPsec provides both integrity and confidentiality protection for IP datagram according to RFC 1827 [i.10]. In addition IMS-AKA requires IPsec support in the Gm interface between UE and P-CSCF for integrity protection.

Remote access services that might benefit from such an encrypted communication channel include:

- home surveillance;
- uploading content (files, photos or video clips) from a remote device to a home server;
- downloading content from a home server to a remote device;
- Home-to-Home communication (see [i.7], clause 4.1.8).

10.2 Tunnelling using SSL/TLS

SSL/TLS used either for tunnelling the entire network stack, as in the OpenVPN project, or for securing what is, essentially, a web proxy. SSL is a framework more often associated with e-commerce, but it has been built-upon by a number of vendors to provide remote access VPN capabilities. A major practical advantage of an SSL-based VPN is that it can be accessed from the locations that restrict external access to SSL-based e-commerce websites only, thereby

preventing VPN connectivity using IPsec protocols. SSL-based VPNs are vulnerable to trivial Denial of Service attacks mounted against their TCP connections because latter are inherently unauthenticated.

10.3 OpenVPN

OpenVPN is an open standard VPN. It is a variation of SSL-based VPN that is capable of running over UDP. Clients and servers are available for all major operating systems.

10.4 VPN Quarantine

The client machine at the end of a VPN could be a threat and a source of attack; this has no connection with VPN design and is usually left to system administration efforts. There are solutions that provide VPN Quarantine services which run end point checks on the remote client while the client is kept in a quarantine zone until healthy.

11 Anti-Virus

Customer devices should be provided with an easy-to-use Anti-virus (AV) Engine to defend them from malicious code and viruses hidden inside files, e-mail or on the Web pages. Automatic real-time and off line scanning is essential to protect devices from potential threats that can occur for example during software download.

The CNG could be part of the anti-virus architecture, for example by taking into consideration the AV Relay function. An AV Relay has all the functionality to interact between the AV facility in the customer devices and the Security Operation Centre supplying the AV service. The AV Relay is able to synchronize the AV clients with the latest more updated AV signature file.

An AV engine can work with different detection methods, like:

- Comparison with a known virus signature list. This list needs to be regularly updated, and stored in a secured way (e.g. in the UICC) to avoid any unauthorized access to modify it.
- Various detection algorithms that can compare behaviours with usual or unusual viruses' behaviours, allowing detection of yet unknown viruses.

The CNG could also be equipped with an AV engine, in order to perform a real time scan of all the traffic passing through it. Considering strong implementation issues, this additional functionality can be considered only for non-residential scenarios, which is out of scope of the present document.

12 URL/URI filtering and prime user control

The possibility of denying a list of URLs/URIs or URLs/URIs that contain a specific pattern, to prevent another person from sending or receiving information (usually on the web) and mainly to restrict access to unsuitable/questionable material. This function is especially useful to implement parental control services directly inside the CNG.

13 Unsolicited communication prevention

Unsolicited Communication (UC) can apply on different types of communication in the NGN:

- Bulk (recorded) text messages (aka SPAM).
- Bulk (recorded) other multimedia messages (aka SPIT).
- More advanced attack scenarios (can be found in TR 187 009 [i.11]).

As defined in TR 187 009 [i.11] the NGN should provide the ability of identifying and preventing UC in the network. This can be done in a two step approach:

1) Detection and marking in a system wide approach (i.e. global blacklist, call-rate analysis, etc.).

2) Detection and handling in a personalized way (i.e. redirect to Junk-mail or decline call).

Only the second step is in the scope of this WI where a user should be able to directly interact with a UC prevention system at his premises (e.g. the CNG). This UC prevention entity should be able to filter in a personalized way the UC attempts (i.e. by personalized blacklists, call-rate or more advanced filtering) and may even handle/prevent UC attempts by e.g. redirect to Junk-mail or decline call). This UC Prevention Entity should also interpret system-wide marking of calls, if such a system is implemented.

The advantage of this approach would be that the user has direct control over the UC rating and handling, and final responsibility for call acceptance/rejection remains ultimately with the user (and not the operator).

For more information please go to TR 187 009 [i.11] (Feasibility study of prevention of unsolicited communication in the NGN).

13.1 Basic description

As identified in TR 187 009 [i.11], Unsolicited Communication (UC) is a complex threat that can become a harassment to the NGN. Methods on a technical level are needed for the Prevention of Unsolicited Communication (PUC) in the NGN. The biggest challenge for PUC is the definition of what kind of communication is unsolicited since this is based on highly personal and subjective sensations. To avoid legal issues and to provide most effective results for PUC, it is mandatory to involve the customer/end user as the last decision point for identification and handling of UC. Thus, the devices in the CPN, e.g. the CNG, need to play an important role in an end-to-end framework.

13.2 Applicability and limitations

This clause does not contain a complete analysis.

13.3 Implementation details

PUC can be broken up in three functional entities:

1) **Identification:** technical means to identify UC, e.g. black-lists/white-lists, statistical analysis or Turing tests.

2) **Marking** of UC to convey UC information over the network:
This can be done downstream (i.e. towards the callee) to address several PUC nodes for identification and handling and also upstream as feedback from the callee back to a node in charge of identification rules and handling procedures.

3) **Handling** of UC: Based on marked communication call-routing schemes gets applies e.g. decline or reroute

These Functional Entities (FEs) can be distributed along the communication path in different network segments.

The FE for identification can be composed of one or many identification modules which cooperate to achieve a common UC marking. Depending on the intrusiveness of the modules they need access to the signalling and also to the media path of the communication.

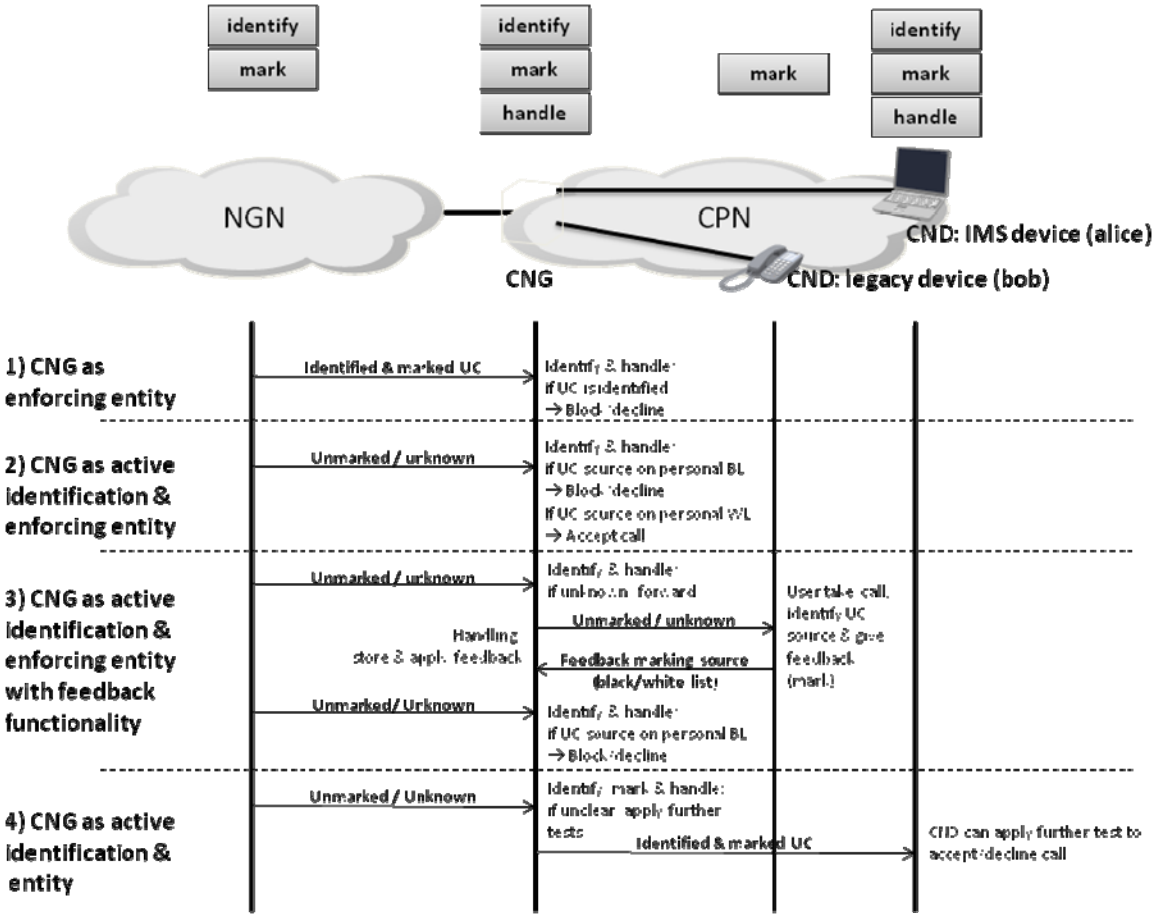


Figure 7: Sample set of PUC for CPNs

1) The example scenarios shown above should visualize on a high level a possible distribution of the FEs in the CPN and the central role of the CNG in this scenario. If the NGN provides the service for identification and marking of UC, and if there is a trusted relationship between the CPN owner and the NGN PUC service, the CNG could act as a simple enforcing point for PUC.

2) If the NGN does not provide UC information or if the end-user wants to apply personalization to the general NGN filtering, he can use the PUC information provided by the NGN in his CNG to apply personalized filtering.

3) In the case that the CNG support PUC for legacy devices (e.g. POT telephones), the CNG should provide the ability to interact with the legacy device to retrieve feedback from the end-user. This could be done by e.g. providing a web-interface where the user can configure his settings e.g. his personal blacklist or by providing a mean to give feedback by number-codes or an IVR system provided at the CNG.

4) In the case of the support of PUC-enabled UEs, the CNG can act as further PUC identification and marking node and convey this information further down to the CND, where the handling policy gets applied.

14 Intrusion Detection System

An Intrusion Detection System (IDS) monitors data traffic inside a network segment in order to reveal malicious traffic. It complements a firewall by introducing more thorough inspection mechanisms than a firewall. Typically an IDS is able to detect protocol anomalies, malicious traffic patterns etc. More advanced systems are called Intrusion Prevention Systems that can also drop traffic that is violating the security policy and Unified Threat Management (UTM) Systems that can also perform anti-virus operation and spam filtering.

IDS monitors network traffic for suspicious activity alerting the network administrator of possible security problems. IDS system should be placed at strategic points inside the network to monitor traffic to and from all devices in the network, such as the border between the private, secure, LAN and the public insecure network (Internet) where the IDS system can scan all inbound and outbound traffic. In this sense the Customer Network Gateway would be a suitable location for the IDS function.

The most suitable IDS technology for the customer environment is the "signature based" one, where the system monitors packets on the network and compares them against a database of signatures taken from known malicious threats. Hence it is very important that the database of signatures is always up to date.

In case of tentative intrusion, there can be the need of alerting a particular entity. Alerts and actions can be configurable.

Strong implementations issues at the CNG level have to be considered.

15 Network Address Translation (NAT)

Network address translation (NAT) is a technique for the translation of an Internet Protocol address used within one network to a different IP address within another network through a device that re-writes the source and/or destination IP addresses of the traversing packets. When NAT involves also the translation of the Port information contained in the UPD/TCP layers, it is also known as Network Address and Port Translator (NAPT). For more details about NAT terminologies see RFC 2663 [i.15].

The main reason of using NAT is to enable multiple hosts on a private network to access the Internet using a single globally routable IP address, but it is also widely used in order to improve the security of a private network (e.g. the CPN) because it limits the visibility of the private hosts.

NAT is a popular tool for alleviating the IPv4 address shortage. For example, NAT allows to enable multiple hosts on a private network to access the Internet using a single public IP address.

NAT involves re-writing the source and/or destination IP addresses, and usually also the TCP/UDP port numbers of IP packets as they pass through the NAT. Checksums (both IP and TCP/UDP) need also to be rewritten to take into account the changes. A NAT which also rewrites the ports is called a NAPT (Network Address Port Translation). NAPT is the most widely used NAT mechanism in the CNG, so there is often a mix between NAPT & NAT in that context (and it will be the case in the present document).

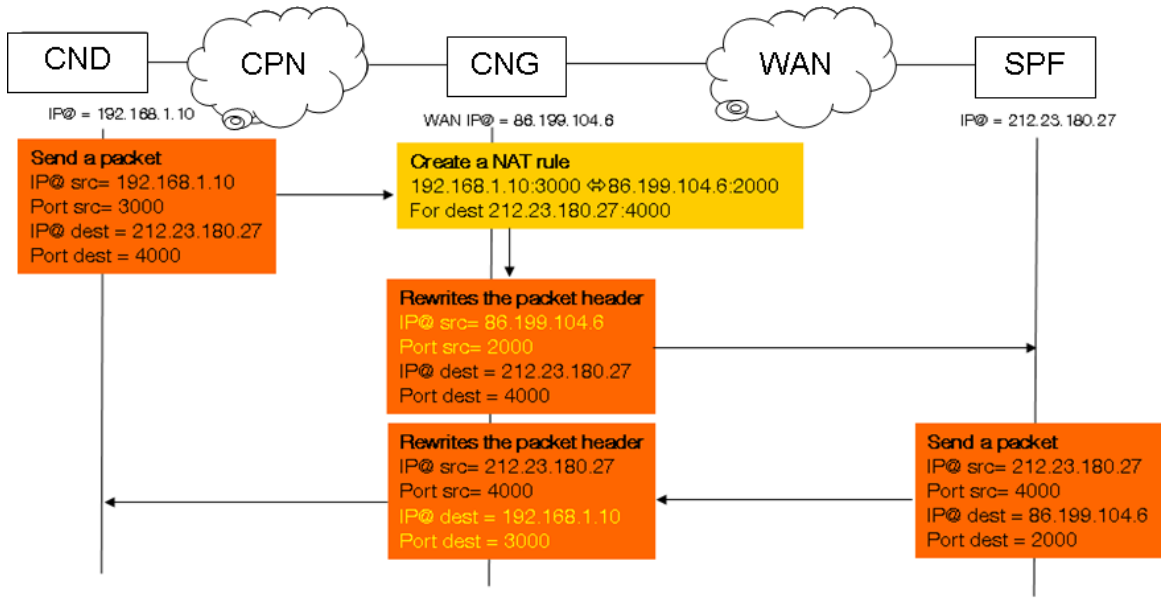


Figure 8: NAT is an IP address translator

Even if this solution is largely used in the routers which access the NGN Network, it does not solve all the problems.

There are some remaining issues like:

- **Expiration of the mapping timer:** In order to manage its resources, a NAT destroy a NAT rule after a period of inactivity between the internal client and the remote host.
- **IP addresses carried in payloads:** Protocols like SIP, H323, SNMP do not respect the layered model, and they re-use the IP packet's address in their payload. The issue is the private IP addresses in the payload are no longer valid once packet crosses the NAT.
- **Issues with bundled session applications:** Bundled session applications are applications which use a control connection to establish a data flow (cf. FTP, H.323, SIP and RTSP for example). In the example below, (1) the softphone contacts a host on the NGN (i.e. another softphone here), and this remote host is responsible for establishing the session on another port (2). No CNG NAT binding is performed for the session, as it is initiated by the remote host (3). It does not work because there is no NAT binding for the requested session.

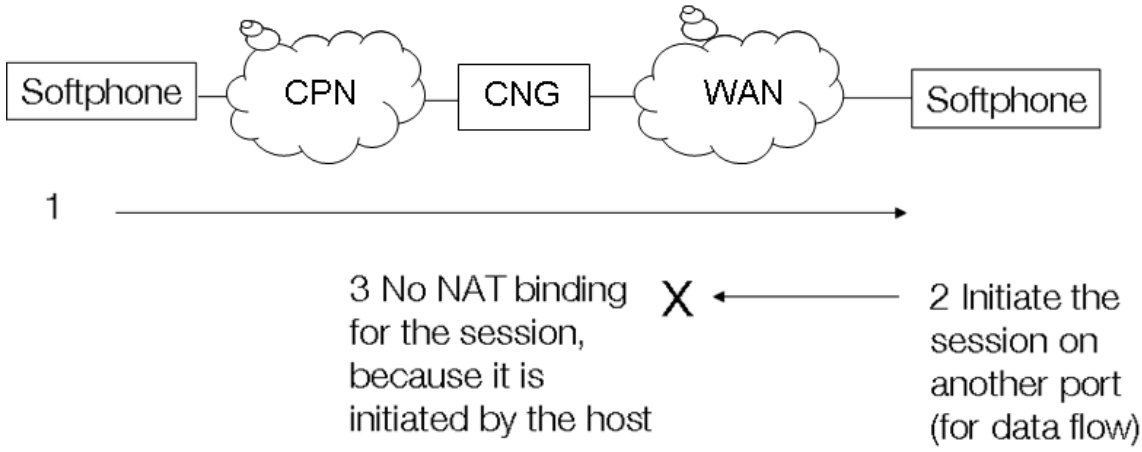


Figure 9: NAT issue with bundled session applications

Different technologies (standard and proprietary solutions) can be adopted for NAT-T, each one with different impacts on the performance and the security of the final solution.

UPnP IGD provides a mechanism to solve the NAT traversal issues.

15.1 UPnP IGD V 1.0

The Universal Plug and Play (UPnP) IGD architecture had been designed for the discovery, configuration, and management of an Internet Gateway Device (IGD). An IGD is an IP addressable device typically residing at the edge of a home or small-business network. An IGD interconnects at least one LAN with a WAN interface for Internet/public network access. An IGD also provides local addressing and routing services between one or more LAN segments and to and from the external network.

UPnP is a set of computer network protocols promulgated by the UPnP Forum and its scope is quite large. The UPnP architecture addresses a number of general issues, not only the NAT-T issue, and it is designed to allow simple configuration of small networks. For the scope of the present clause only the NAT-T scenario will be taken into consideration.

15.1.1 Basic description

With UPnP IGD routers and/or firewalls (i.e. CNG) expose themselves as Internet Gateway Devices, allowing any local UPnP controller (e.g. the CND) to perform a variety of actions, including retrieving the external IP address of the device, enumerate existing port mappings, and adding and removing port mappings. By adding a port mapping, a UPnP controller behind the IGD can enable traversal of the IGD from an external address to an internal client.

Hence UPnP IGD v1 [i.14] can enable NGN applications (e.g. a SIP IMS application) to manage the presence of a NAT device in the path between the CND and the network server deployed on the NGN (e.g. P-CSCF). In particular with IGD v.1 it is possible to perform the following tasks:

- Learning public IP address.
- Enumerating existing port mappings.
- Adding and removing port mappings.
- Assigning lease times to mappings (optional capability in the UPnP IGD v1.0 [i.14]).

In the CPN context the IGD role can be assigned to a CNG, whereas the CND acts as a UPnP controller.

15.1.2 Applicability and limitations

The main issues related to the UPnP solution as a NAT-T mechanism are:

- Security: UPnP relies on the NAT opening pinholes to the outside world (i.e. the network outside the CPN) under the dynamic control of the UPnP client or controller (e.g. a Sip phone). This capability is usually contrary to most security policies and therefore may not be accepted by Service Providers and Telecom Operators. Moreover, all UPnP device implementations lack authentication mechanisms, and by default assume local systems and their users are completely trustworthy.

NOTE: UPnP forum is currently working (at the time of creating this version, August 2009) to a secure version to address most security issues associated with IGD.

- The mechanism does not work if the NAT is operated outside the CPN boundary, or more than one NAT devices are on the path between the CND and the NGN server, as UPnP IGD can only control the first NAT closest to the CND.
- Several options are open in the specification.

The main advantages related to the UPnP solution as a NAT-T mechanisms are:

- It works for all kind of services and protocols (SIP, RTSP, RTP, IMS based services and non IMS based such as dedicated IPTV subsystem), even if for SIP applications other solutions can be more relevant, like a SIP ALG in the CNG for instance. Indeed there is a need for a UPnP/SIP interface if UPnP IGD used.
- Standardized (by the UPnP Forum) solutions and widely available (although usually deactivated).

15.1.3 Implementation details

The sequence diagram shows in figure 10 describes an example of the main steps involved in the UPnP NAT-T mechanism:

1) The CND discovers in the CPN any IGD devices, e.g. the CNG; UPnP works with the 239.255.255.250 multicast address (on port 1900) for discovering devices; The IGD device (CNG) may offer different subprofiles to the UPnP controller (e.g. CND), including the WANIPConnection (e.g. IP router) or WANPPPConnection subprofiles (e.g. ADSL modem). On the WANIPConnection or WANPPPConnection subprofiles of the IGD device the CND may issue the remote calls to configure the NAT port mapping (the control messages are formatted in XML and use SOAP.

2) The CND asks for the external IP address of the CNG by means of the GetExternalIPAddress() command. The CNG (step 2.a) responds with its external address (e.g. the IP address assigned to the WAN interface). That information could be used to check if the CND is behind a NAT mechanism and to generate the outgoing packets correctly (e.g. to fill in accordingly the headers values of the SIP/SDP protocol with the external CNG IP address).

3) A new portmap entry will be added by using the AddPortmapEntry() call. The following parameters need to be passed: RemoteHost (option in UPnP IGD v1.0, e.g. a video server address), ExternalPort, PortMappingProtocol, InternalPort, InternalClient, PortMappingDescription, PortMappingLeaseDuration.
The tuple (RemoteHost, ExternalPort, PortMappingProtocol) needs to be unique across any entry present in the port mapping table.
RemoteHost may be used to restrict the port mapping for just one external host (0.0.0.0 to indicate any host), the PortMappingProtocol parameter needs to be TCP or UDP and the ExternalPort is used to specify the TCP or UDP port on the WAN side of the IGD device to be used for the portmap. The InternalPort parameter specifies the port on a client machine to which all traffic coming in on external port should be forwarded to. The InternalClient parameter sets the client machine that traffic should be sent to.

4) The information received from the IGD device needs to be used by the CND to access the NGN service, generating the outgoing packets accordingly and to process incoming packets (e.g. the device can use directly the external IP address and the allocated port in the SIP/SDP signalling payload).

5) When the portmap is no longer needed, the CND should delete a port mapping entry by using the DeletePortMapping (RemoteHost, ExternalPort, PortMappingProtocol) command.

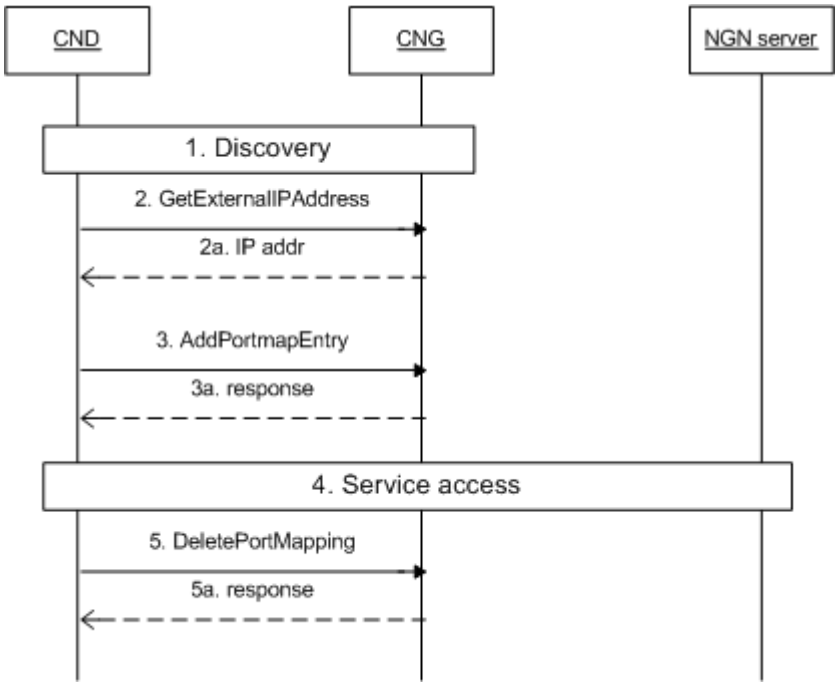


Figure 10: Flow Diagram for UPnP IGD v 1.0 NAT-T usage

Since the UPnP forum specification foresees several options, it is possible to define different use cases and scenarios. The detailed procedures of UPnP IGD V 1.0 Port Mapping are described in [i.14].

The recommended security requirements for implementing IGD on the CNG connected to the TISPAN NGN are:

- UPnP IGD control point should not be able to query or set sensitive information on the CNG.
- CNG Management parameters need to be kept inaccessible from IGD.
- UPnP IGD NAT rules need to be visible to the user.
- User need to be able to delete rules created via UPnP IGD.
- Rules created via IGD need not be persistent and they need to be removed as soon as the portmap is no longer needed.

NOTE: Security requirements are also going to be elaborated by UPnP forum.

15.2 Hosted-NAT solution for RTSP based services

Hosted Nat traversal for TISPAN IMS access is specified in ETSI TS 282 003. The mechanism has been defined to solve the NAT issue for the SIP based services (e.g. voice call) and it is based on an ALG collocated inside the P-CSCF and mandates the usage of the C-BGF in the access network. The C-BGF allocates and releases transport addresses according to the request coming from the ALG function of the P-CSCF. It ensures proper forwarding/binding of media packets coming from or going to the CND.

The Hosted Nat mechanism works also when the SIP packets are encapsulated inside an IPSEC tunnel.

The same (similar) mechanism can be used for the NAT traversal of the RTSP protocol (and related media flows), used in the IPTV IMS-based or in the dedicated subsystem.

15.2.1 Basic description

When the RTSP protocol passes through the NAT device (e.g. CNG), the embedded address and port in the "transport" header will be translated in order for the connection to be successful (e.g. SETUP message). These issues could be managed by an ALG placed in the Operator Network (e.g. MFC in the IPTV context). The main steps involved in the NAT traversal procedure are the following:

- The ALG in the server entity (e.g. MCF) have to detect the presence of NAT comparing the client's external IP address with the source IP address in the IP header of the SETUP message (e.g. by checking the IP address in the "destination" field).
- The ALG requests the C-BGF to set up the media relay binding (IP and Port to be allocated for the media stream).
- The ALG send the (C-BGF) port information to the media server (e.g. by modifying the corresponding parameters inside the RTSP setup message) and then will forward to the CND the IP address and port that the C-BGF have been allocated for the media session.
- The CND, in order to receive the media flow (e.g. using the PLAY message) begins to send the keep-alive messages to the C-BGF port. Keepalive messages are used to punch the hole in the FW/NAT (e.g. CNG) and to aid the BGF for port binding and address mapping.

15.2.2 Applicability and limitations

The main issues related to the Hosted Nat solution as NAT traversal mechanisms for the RTSP are:

- The mechanism could impose some constraints on the server side of the TISPAN NGN (e.g. performance).
- The CNDs need to support symmetric media in order for NAT and PAT mechanism to work on the CNG. Symmetric RTP means the device uses the same port for sending and receiving.
- The CND has to punch specific holes in the CNG in order to let the media (RTP packets) enter into the CPN by using keep-alive messages (to be defined).

The main advantages related to the Hosted Nat solution as a NAT-T mechanisms are:

- Even if the mechanism have been designed for the SIP services, it works also for other kind of services and protocols, including RTSP independently of the transport layer adopted (UDP vs. TCP).
- Minimal changes are required to the current TISPAN (r1 and r2) architecture, since it reuses the same interface used for the SIP Host Nat mechanism (e.g. Gq').
- It works also when the RTSP is protected with TLS (or IPSEC) and then it could support different level of security.
- It works in the environment with cascaded NAT routers (whereas UPnP cannot work).

15.2.3 Implementation details

The sequence diagram in figure 11 describes an example of the main steps involved in the proposed Hosted Nat mechanism for RTSP. The scenario described foresee a CND (e.g. a STB) accessing the NGN IPTV dedicated subsystem. The CNG and the NAT device are collocated in the same device. In order to simplify the scenario (e.g. because the Xp reference point is not yet defined), also the MCF and MDF are collocated and seen as a single entity called Media Function (MF):

1) The CND sends the RTSP SETUP message with appropriate SDP description (or other session description mechanism) of the media request to the Media Function in order to receive the desired media channel (the RTSP server IP address could be obtained, for example, through HTTP communications - not shown in the figure). The CNG changes the sender IP address and TCP port of the RTSP packet and forwards it to the destination address (the IP address of the RTSP server, the MCF). It is worth to mention that the RTSP can be transported over TLS without any changes needed to the present solution. Anyway it is assumed that the RTSP is transported over TCP.

2) The MF detects the presence of a NAT device in the network between the CND and requests (on Gq') the allocation of specific addresses and ports on C-BGF for the RTP media flows; this information is used to update the IP and port address information in the SDP message that describes the RTP flow.

3) The MF generates a RTSP 200 OK message where the SDP contains the BGF address and port reserved for this media flow during the step 2; the RTSP message is sent back to the CND inside the TCP connection opened during the step 1 (the NAT device keeps the hole opened because the TCP is connection oriented).

4) When the IPTV customer wants to see the content, it sends the RTSP PLAY message to the MF.

5) The MF starts to send the media traffic to the address and port allocated by the C-BGF. That traffic is then discarded by the BGF because it does not yet know the actual address of the CND.

6) The CND starts sending keep alive messages that could consist of empty RTP packet with a payload type of 20 to the destination address and port contained in the 200 OK (i.e. the C-BGF); The frequency of the keep-alive should also be defined; the keepalive message opens the hole in the CNG and reaches the C-BGF.

7) The C-BGF learns the IP address and port where to send the RTP traffic from the keep-alive messages and starts to forward the media traffic to the CNG. The NAT device finally delivers the flow to the CND by using its internal NAT table.

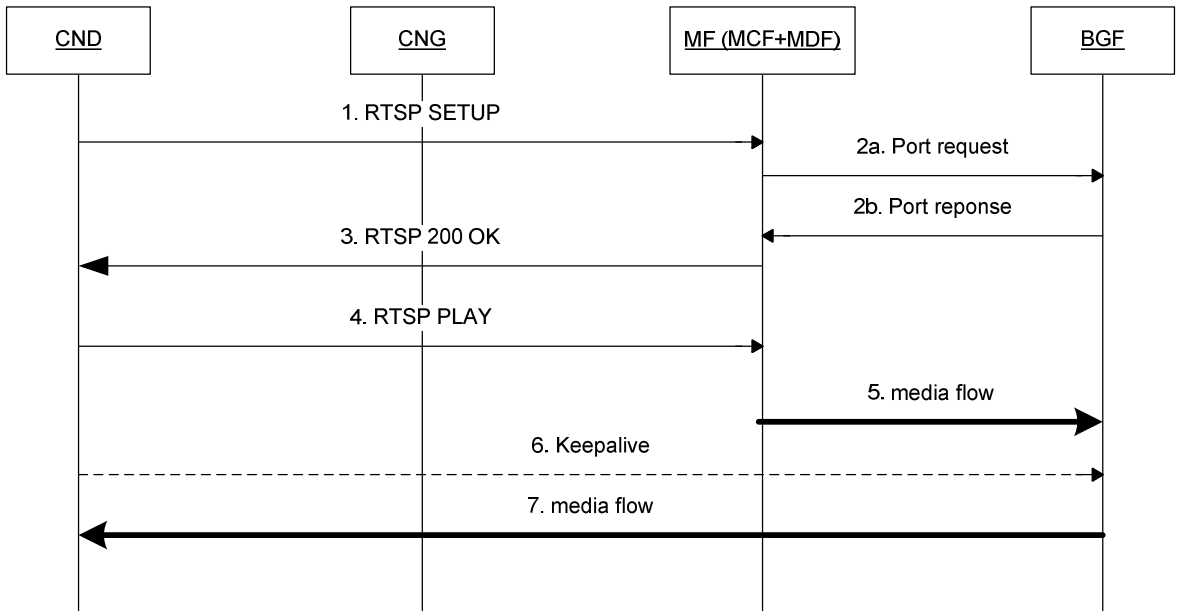


Figure 11: RTSP Hosted Nat Flow Diagram

It is also possible to adapt the described solution to a scenario where the C-BGF is missing. In such a scenario the MF needs to support directly the symmetric NAT capabilities of the C-BGF.

Annex A: Bibliography

ETSI TS 133 246: "Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS) (3GPP TS 33.246 version 9.0.0 Release 9)".

ETSI TR 187 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NAT traversal feasibility study report".

IEEE 802.11a: "IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz band".

IEEE 802.11b: "IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band".

IEEE 802.11i: "IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements".

IEEE 802.11g: "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher Data Rate Extension in the 2.4 GHz Band".

ETSI TS 185 009: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) Architecture and reference points of a customer network device for IMS based IPTV services".

ETSI TS 123 228: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228 Release 9)".

History

Document history		
V3.1.1	July 2010	Publication