NGN Protocol Specifications

Keith Mainwaring
Cisco

Agenda

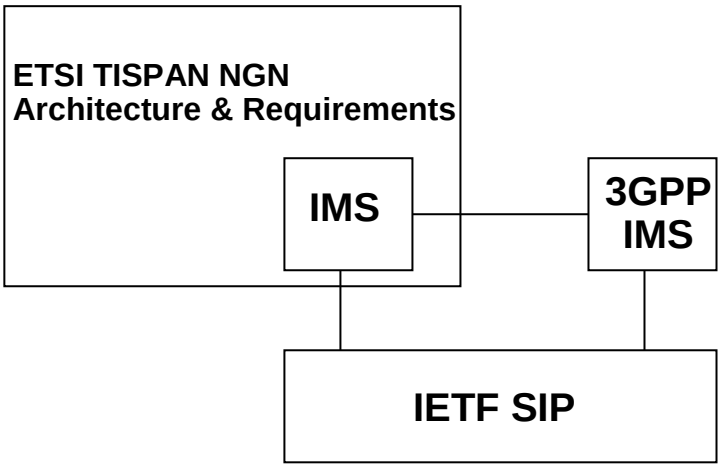
Protocols for:

- Call / Session Control
- Resource and Admission Control
- Data Path & IP infrastructure (IP, TCP, UDP, HTTP, RTP, BGP, OSPF, ENUM, DNS, MPLS, Diffserv, RSVP, Radius, Diameter...)

Produced by:

- ITU-T
- ETSI (European Telecommunications Standards Institute)
- 3GPP (3rd Generation Partnership Project)
- IETF (Internet Engineering Task Force)

ETSI TISPAN NGN IMS



Session Control

IMS
SIP UNI & NNI

IMS Background

- 3GPP application of SIP with modifications to support:
  - GSM business model – subscriber of a ”Home” network operator
  - GSM handset capabilities (SIM for authorisation)
  - Not primarily for voice – this is likely to be supported on the circuit-switched domain for some time – but for presence, IM, push-to-talk....
- ETSI TISPAN NGN IMS
  - Fixed network access with ”nomadicity”
  - Ambition to achieve Fixed Mobile Convergence
- ITU-T
  - Moving to adopt IMS as one element of broad NGN
- PacketCable2.0
  - Moving to adopt IMS model – but tailored to cable requirements

ETSI TISPAN IMS Architecture cf. 3GPP IMS

- The addition of the e2 interface in the TISPAN architecture between the P-CSCF and the NASS (Network Attachment Subsystem) Connectivity Session Location and Repository Function (CLF);
- the use of the Gq’ interface rather than Gq as in the 3GPP architecture; and
- the substitution of the UPSF (User Profile Server Function) for the HSS
  - Equivalent to HSS with HLR stripped out

ETSI TISPAN IMS cf. 3GPP Release 7

Charging

- ETSI TISPAN NGN Release 1 only supports off-line charging.

SIP Protocol

- UEs may support neither ISIM nor USIM.
- Adds NASS bundled authentication.
- Allows a transport mechanism without a security association.
- Inclusion of Gq' interface to P-CSCF.
- Addition of e2 interface.
- Added capability for the Proxy role for "Rejecting anonymous requests in the Session Initiation Protocol (SIP)" and the status code 433 (Anonymity Disallowed).

TISPAN IMS - Supplementary Service Support

- NGN Cdiv
- NGN CONF
- NGN MWI
- NGN OIP/OIR
- NGN TIP/TIR
- NGN CW
- NGN HOLD
- NGN AoC
- NGN CCBS/CCNR
- NGN ACR – CB
- NGN MCID
- NGN Explicit Communication Transfer
- NGN Presence Stage 3

PSTN Emulation & Simulation

- **PSTN/ISDN Emulation**
  - **Mimicking a PSTN/ISDN network from the point of view of legacy terminals (or interfaces) by an IP network, through a gateway. All PSTN/ISDN services remain available and identical (i.e. with the same ergonomics); such that end users are unaware that they are not connected to a TDM-based PSTN/ISDN.**
  - **Softswitch approach: Monolithic architecture**
  - **IMS approach: Re-use (all or part) of the IMS functional architecture to specify the internal structure. Common control platforms, and enables new voice services for all types of subscribers.**
- **PSTN/ISDN Simulation**
  - **The provision of PSTN/ISDN-like services to advanced terminals (IP-phones) or IP-interfaces. There is no strict requirement to make all PSTN/ ISDN services available or identical, although end users expect to have access to the most popular ones, possibly with different ergonomics.**

ITU-T Signalling Profiles

- NGN NNI Signalling Profile – Q.3401
  - SIP profile
  - Mandatory and optional RFC support (SIP extensions)
  - Codec & packetisation size
- NGN UNI Signalling Profile

NNI - Mandatory RFCs

RFC 2327	SDP: Session Description Protocol
RFC 3261	SIP: Session Initiation Protocol
RFC 3262	Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
RFC 3264	An Offer/Answer Model with the Session Description Protocol (SDP)
RFC 3311	The Session Initiation Protocol (SIP) UPDATE Method
RFC 3323	A Privacy Mechanism for the Session Initiation Protocol (SIP)
RFC 3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
RFC 3326	The Reason Header Field for the Session Initiation Protocol (SIP)
RFC 3966	The tel URI for Telephone Numbers
RFC 4028	Session Timers in the Session Initiation Protocol (SIP)
RFC 4566	SDP: Session Description Protocol

NNI - Optional RFCs

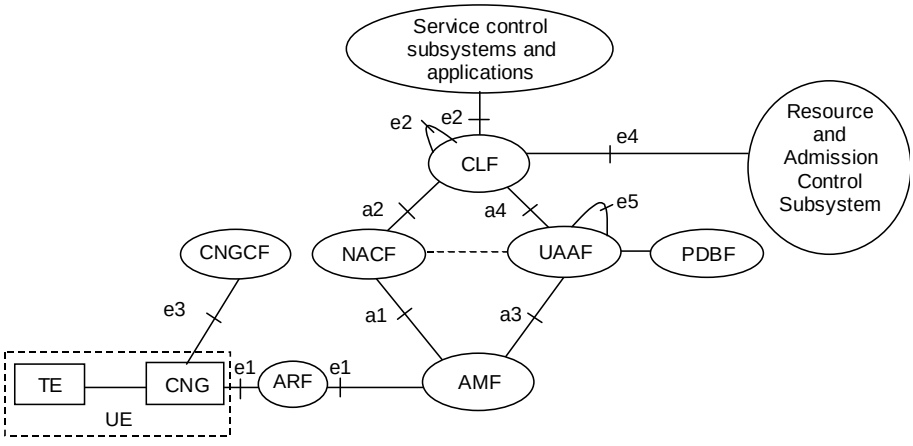
RFC 2046	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
RFC 2976	The SIP INFO Method
RFC 3087	Control of Service Context using SIP Request-URI
RFC 3204	MIME media types for ISUP and QSIG Objects
RFC 3265	Session Initiation Protocol (SIP)-Specific Event Notification
RFC 3312	Integration of Resource Management and Session Initiation Protocol (SIP)
RFC 3324	Short Term Requirements for Network Asserted Identity
RFC 3398	Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping
RFC 3420	Internet Media Type message/sipfrag
RFC 3428	Session Initiation Protocol (SIP) Extension for Instant Messaging
RFC 3455	Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
RFC 3515	The Session Initiation Protocol (SIP) Refer Method
RFC 3824	Using E.164 numbers with the Session Initiation Protocol (SIP)
RFC 3840	Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)
RFC 3841	Caller Preferences for the Session Initiation Protocol (SIP)
RFC 3891	The Session Initiation Protocol (SIP) "Replaces" Header
RFC 3892	The Session Initiation Protocol (SIP) Referred-By Mechanism
RFC 3893	Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format
RFC 3911	The Session Initiation Protocol (SIP) "Join" Header
RFC 3959	The Early Session Disposition Type for the Session Initiation Protocol (SIP)
RFC 3960	Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
RFC 4032	Update to the Session Initiation Protocol (SIP) Preconditions Framework
RFC 4235	An INVITE Initiated Dialog Event Package for the Session Initiation Protocol (SIP)
RFC 4244	An Extension to the Session Initiation Protocol for Request History Information
RFC 4412	Communications Resource Priority for the Session Initiation Protocol (SIP)
RFC 4483	A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages
RFC 4694	Number Portability Parameters for the "tel" URI

Resource and Admission Control

ETSI TISPAN

ITU-T

TISPAN NASS Architecture



NASS Functions

- CNGCF (Customer Network Gateway Configuration Function) - used during initialization and update of the UE to provide the UE with configuration information (e.g. configuration of a firewall internally in the UE and QoS marking of IP packets) additional to the network configuration data provided by the NACF.
- ARF (Access Relay Function) - relay between the CNG and the NASS that inserts local configuration information.
- AMF (Access Management Function) - translates the network access requests sent by the UE and forwards requests for allocation of an IP address and possibly additional network configuration parameters to/from the NACF and forwards requests to the User Access Authorisation Function (UAAF) to authenticate the user, authorize or deny the network access, and retrieve user-specific access configuration parameters. If PPP is used the AMF terminates the PPP connection and acts as a RADIUS client if the UAAF is implemented in a RADIUS server.
- NACF (Network Access Configuration Function) - responsible for the IP address allocation. Typically implemented as a DHCP or RADIUS server.
- UAAF (User Access Authorisation Function) - performs user authentication and authorisation checking, based on user profiles. Communication between UAAFs in different administrative domains is provided by the e5 interface allowing a UAAF-proxy to request the UAAF-server for user authentication and authorization and allowing the UAAF-proxy to forward accounting data for the particular user session to the UAAF-server.
- PDBF (Profile Database Function) - contains user authentication data (e.g. user identity, list of supported authentication methods, and authentication keys). It may be co-located with UAAF (the interface between them is not to be standardized).
- CLF (Connectivity Session Location and Repository Function) - registers the association between the IP address allocated to the UE and related network location information. The CLF has interfaces to the AF (e.g. P-CSCF) and to the RACS.

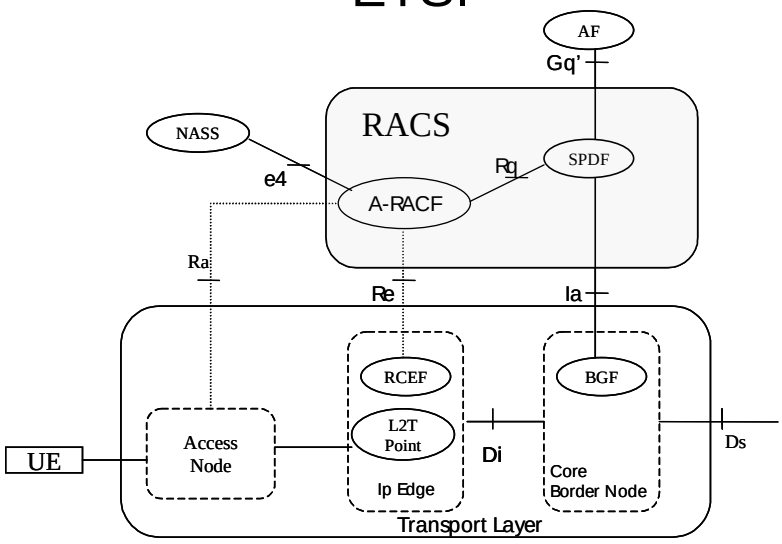
e2 interface

- Enables Application Functions (AF), such as an IMS P-CSCF or a Presence Network Agent (PNA) to retrieve IP-connectivity related session data from the NASS CLF
- Protocol is based on Diameter (RFC 3588)
- The AF can request the following information for a specific subscriber (identified by a globally unique IP address or a subscriber identifier):
  - Subscriber-id;
  - Location information;
  - RACS contact point;
  - Access network type (ATM, Ethernet or Unknown); and
  - Terminal Type.
- Diameter messages over the e2 interface are transported using SCTP (RFC 2960) and use is made of the SCTP checksum method specified in RFC 3309.
- IPSec may be used for secure transport of Diameter messages.
- Accounting functionality is not used on the e2 interface and Diameter sessions are implicitly terminated (i.e. the server does not maintain state information).
- The e2 interface may also be used between a CLF in a visited network and a CLF in a home network in the case in which the P-CSCF resides in the home network.

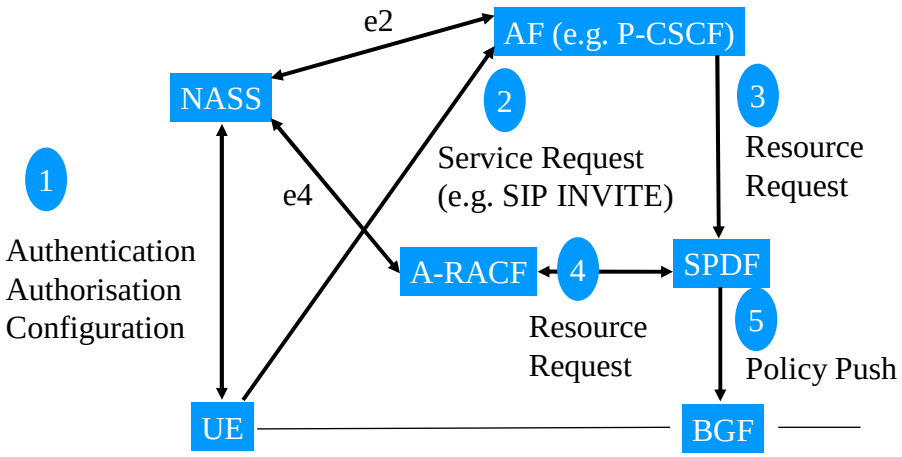
e4 interface

- Enables the exchange of IP-connectivity related session data between the NASS CLF and the Access -RACF in the RACS
- The protocol is based on Diameter
- The following information can be transferred from the CLF to the A-RACF:
  - Initial Gate Setting
  - List of allowed destinations
  - Up-Link Subscribed Bandwidth
  - Down-Link Subscribed Bandwidth
  - QoS Profile Information
  - Transport service class
  - Media-Type
  - Up-Link Subscribed Bandwidth
  - Down-Link Subscribed Bandwidth
  - Maximum Priority
  - Requestor Name
- The Access Profile is “pushed” from the CLF to the A-RACF when an IP address has been allocated to a subscriber or in the case of a modification occurring on a profile that has already been pushed to the RACS and “pulled” by the A-RACF from the CLF after a restart or upon reception of a resource reservation request associated with an IP-Address for which no record is stored.
- The CLF can also report the loss of IP connectivity enabling the RACS to remove the access profile from its internal data base. This occurs when the allocated IP address is released (e.g. DHCP leased timer expiry) or due to the release of the underlying layer 2 resources.
- As on the e2 interface: the Diameter messages over the e4 interface are transported using SCTP; use is made of the SCTP checksum method specified in RFC 3309; IPSec may be used for secure transport; Accounting functionality is not used; and Diameter sessions are implicitly terminated.

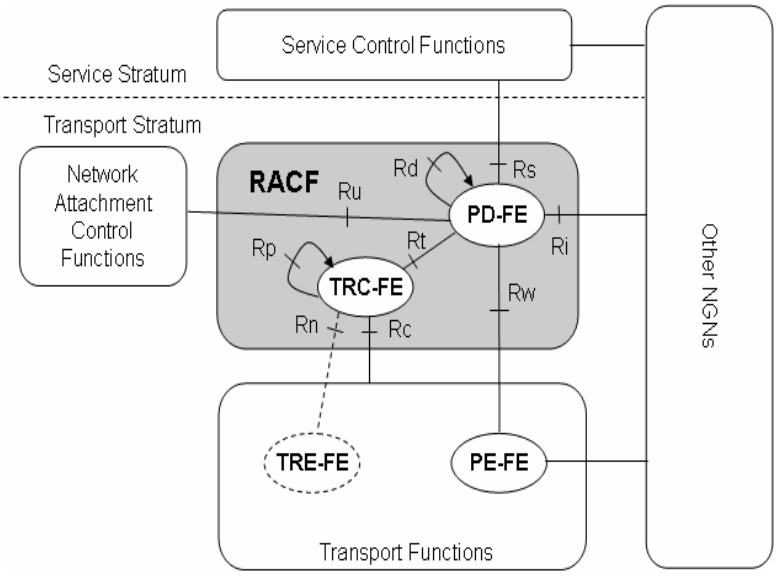
Resource and Admission Control ETSI



Outline of NGN QoS Control



ITU-T Resource Control – Y.2111



IP Infrastructure

IETF

IP Network Specifications

- Very many RFCs
  - IP, TCP, UDP, HTTP, RTP, BGP, OSPF, ENUM, DNS, MPLS, Diffserv, RSVP etc