

IPWorks Technical Description

TECHN PRODUCT DESCR

Copyright

© Ericsson AB 2017–2018. All rights reserved. No part of this document might be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.

Abstract

The purpose of this document is to provide a technical description with an overview of the Base/Value Packages and functions of the Ericsson IPWorks product. Different network scenarios and solutions that IPWorks can be used in are also described. This document does not include engineering specifications, operational, or deployment information for the product.



Contents

1	Introduction	1
1.1	Related Information	2
2	IPWorks Deployment Scenarios	3
2.1	IPWorks Virtualized (VNF) Deployment	3
2.2	SW Architecture View	5
2.3	Data Layered Architecture	7
3	Functionality	9
3.1	IPWorks DNS	9
3.2	IPWorks Internet DNS	10
3.3	IPWorks ENUM	11
3.4	IPWorks ENUM Front-End	13
3.5	ENUM Feature: IMS Interconnect	14
3.6	IPWorks AAA	15
3.7	IPWorks AAA Front-End	26
3.8	AAA Feature: IPWorks PKI authentication	27
3.9	AAA Feature: IPWorks Wi-Fi Mobility	28
3.10	IPWorks DHCP	29
4	Interfaces	33
4.1	Reference Model	33
4.2	Protocols	41
5	Operation, Administration and Maintenance	45
5.1	Provisioning Management	45
5.2	Configuration Management	45
5.3	Backup & Restore	46
5.4	License Management	46
5.5	Fault Management	47
5.6	Performance Management	47
5.7	Security Management	47
5.8	Health Check	48
5.9	Trace	49



6	Redundancy	51
6.1	Traffic Redundancy	51
6.2	Provisioning Redundancy	54
6.3	Storage Redundancy	55
	Reference List	57



1 Introduction

IPWorks 2 is a software system that provides DNS, ENUM, DHCP, and AAA services. IPWorks also includes Element Management System for configuration and control of these services.

- DNS is commonly used to map alphanumeric names to IP addresses and conversely.
- DHCP handles dynamic IP address assignment and configuration.
- ENUM provides E.164 number translation to SIP URI.
- AAA provides Authentication, Authorization, and Accounting service for end user to access to network resources.

IPWorks 2 includes the following new features and enhancements:

- Support of DHCP service
- Support for IPv6 on all interfaces
- Support of DHCP Redundancy and Load Balancing between two DHCP servers located in geographic separated sites, and DHCP provisioned data replication between two IPWorks system
- Support of reference configuration for CEE/HDS8000
- Support of reference configuration for SLES 12 SP2 with KVM/HP DL 380 G10
- Support of P-CSCF restoration
- Support centralized configuration and management of multiple DNS servers at different sites

Scope

This document provides a technical description with an overview of the Base/Value Packages and functions of the Ericsson IPWorks 2 product. Operational, engineering specifications or deployment information are not included in this document. We assume that the reader is familiar with DNS, ENUM, DHCP, AAA, and their normative documents.

- IPWorks deployment and SW architecture are described in Section 2 on page 3.
- IPWorks functionalities with Ericsson SW Model (ESM) are described in Section 3 on page 9.
- Overview of the relevant interface for IPWorks functionalities is described in Section 4 on page 33.



- O&M overview is described in Section 5 on page 45.
- IPWorks redundancy overview is described in Section 6 on page 51.

1.1 Related Information

Trademark information, typographic conventions, and definition and explanation of abbreviations and terminology can be found in the following documents:

- Trademark Information
- Typographic Conventions
- Glossary of Terms and Acronyms



2 IPWorks Deployment Scenarios

The IPWorks 2 is a software delivery that can only be deployed as virtualized SW.

Two deployment scenarios are supported:

- Virtualized deployment

IPWorks 2 supports virtualized deployment on cloud infrastructure with multiple NFVI and HW support.

It is validated on reference configuration of "CEE/BSP (with GEP5/GEP7L)" and reference configuration of "CEE/HDS8000".

- Native deployment

IPWorks 2 supports native deployment using virtualized framework on appropriate HW configuration and hypervisor.

It is validated on reference configuration of "SLES 12 SP2 with KVM / HP DL380 G9 server", and reference configuration of "SLES 12 SP2 with KVM/HP DL380 G10 server".

Notice that not all basic packages are supported on both two deployment scenarios. The IPWorks Internet DNS base package is only applicable to Native deployment scenario.

2.1 IPWorks Virtualized (VNF) Deployment

The overall deployment configuration as virtualized is shown in Figure 1 and Figure 2.

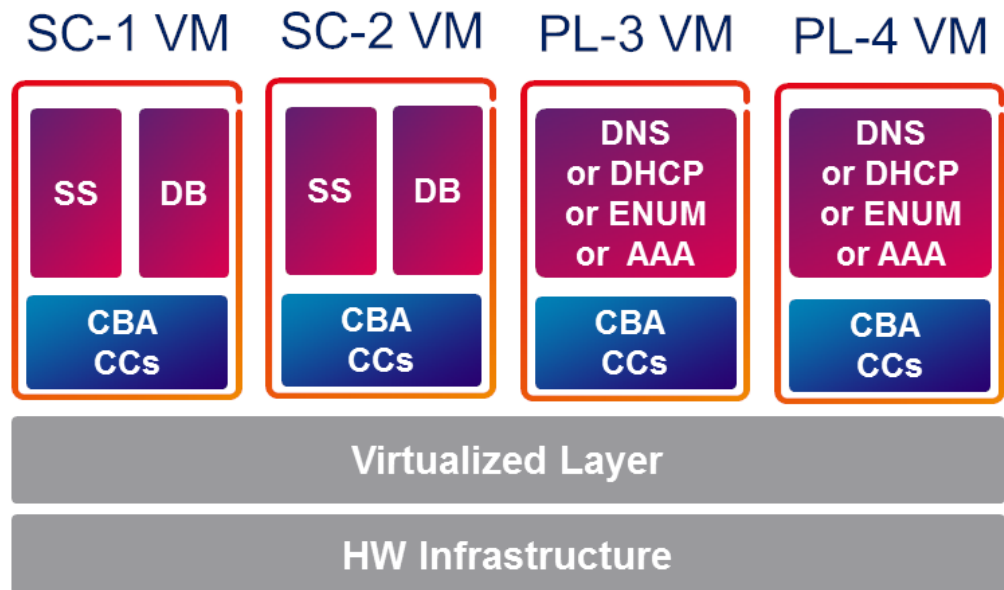


Figure 1 IPWorks VNF Deployment

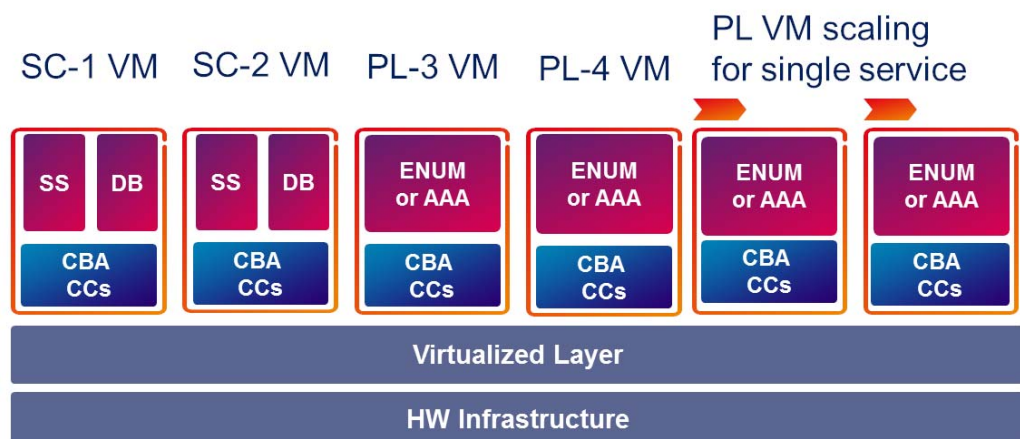


Figure 2 IPWorks VNF Deployment for Single Service with Manual Scalability Support

IPWorks VNF supports two kinds of deployment:

- Flexible deployment for single service, the service can be DNS, ENUM, DHCP, or AAA.
- Standard deployment for single service with manual scalability support, the service can be ENUM or AAA.

For the flexible deployment for single service, IPWorks VNF includes 2 SC VMs + 2 PL VMs (DNS, ENUM, DHCP, AAA). Each VM is allocated with a flexible HW resources.

And the flexible deployment does not support PL VM scaling.



For standard deployment for single service, IPWorks VNF includes 2 SC VMs + 2 PL VMs (ENUM, AAA). The PL VMs can be scaled manually to improve performance and capacity.

Note: The deployment of IPWorks Internet DNS Base Package does not support PL VM scaling.

2.2 SW Architecture View

This section gives the software architecture of the IPWorks.

2.2.1 IPWorks Applications



Figure 3 IPWorks Applications

In IPWorks 2, the IPWorks application contains functions as System Control (SC) and Payload (PL).

System Controller (SC) contains Storage Server (SS) and MySQL NDB Cluster components. It is responsible for cluster control in a Component Based Architecture (CBA) software modeling, providing Service Availability, O&M Interface, Backup Restore, and Performance, Fault Handling, License management functions.

System Control also provides services (DNS, ENUM, DHCP, and AAA) configuration and provisioning function, through "IPWorks CLI" for the network. Provisioned data are stored into MySQL database components.

Payloads are responsible for delivering the services in network, for example, DNS, ENUM, DHCP, and AAA service.

2.2.2 SW Architecture Overview

IPWorks 2 software follows Ericsson Architecture Guide (EAG), implemented in a Component Based Architecture (CBA) framework with reusable components, and offers Ericsson common aligned OAM functions.

IPWorks software architecture is shown in Figure 4:

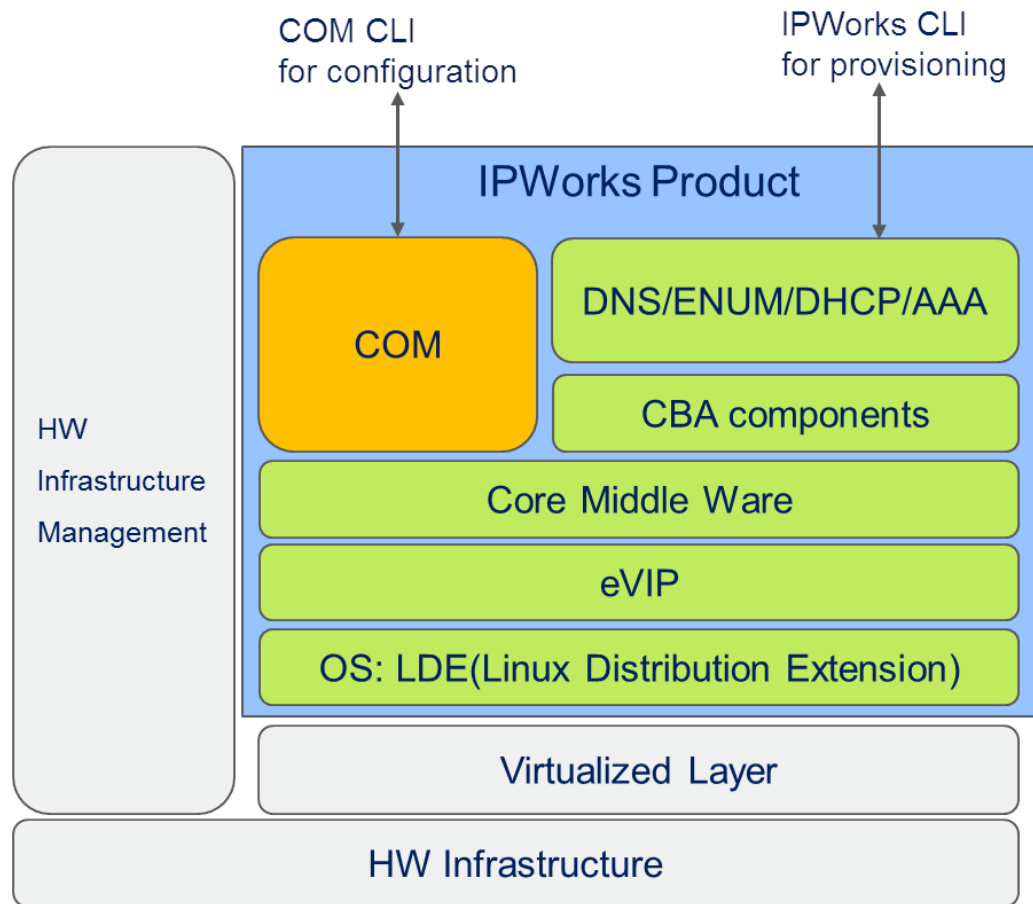


Figure 4 IPWorks SW Architecture Overview

2.2.3 ECIM/IMM Support

The configuration of IPWorks 2 follows Ericsson Common Information Model (ECIM), which achieves a unified Operation and Maintenance using a common model, modelling language, schema, and tool.

The operator manages the system through the Northbound Interface (NBI) by operating on managed object (MO) classes instances in the runtime system.

2.2.4 COM/CLI

Common Operation and Maintenance (COM) provides the operation and maintenance interface. It connects the CBA to the management system through the Ericsson standardized Northbound Interface (NBI).

NBI includes the NETCONF interface for Machine to Machine communications as well as a CLI. Connections for the NETCONF and COM CLI are set up through SSH. Alarms are sent through SNMP.



The SS7 CAF has its own dedicated management system called the Signaling Manager that is used to configure and manage the SS7 stack.

2.2.5 Core Middle Ware

Core Middle Ware (Core MW) is the open Service Application Framework (SAF) based middleware component of CBA.

The AMF (Availability Management Framework) service in Core MW provides High Availability by coordinating redundant resources within the cluster to ensure no single point of failure. For IPWorks virtualized, the 2 SC VMs forms an active-standby redundant pair, providing redundancy for each other. The PL VMs form N-Way active model.

What's more, Core MW also provides Software Management Framework (SMF) including software installation, upgrade, and update management functions.

Other O&M functions such as Performance Management, Fault Management are described in O&M relevant chapters.

2.2.6 DNS/ENUM/DHCP/AAA

DNS/ENUM/DHCP/AAA are the application modules developed in IPWorks. Main functionality is described in Section 3 on page 9.

2.3 Data Layered Architecture

Data Layered Architecture (DLA) is an architecture where data and logic are separated in different layers, which are implemented in different network functional entities.

Application data is stored in a network element so called back-end, and application logic is hosted in a different network element. IPWorks ENUM and AAA (for GPRS and PKI authentication) support DLA deployment.

For example, IPWorks ENUM in DLA includes two layers:

— Application Layer

IPWorks ENUM Front-End provides ENUM application logic interacting with CUDB as Back-End database.

— Data Layer

CUDB for IPWorks ENUM-FE functionality, where ENUM records are provisioned by Ericsson Dynamic Activation (EDA) and stored in the Back-End. Data storage in CUDB provides High Availability including geographic redundancy and persistent storage.





3 Functionality

This section describes the functionality of the following services:

- IPWorks DNS Base Package, see Section 3.1 on page 9
- IPWorks Internet DNS Base Package, see Section 3.2 on page 10
- IPWorks ENUM Base Package, see Section 3.3 on page 11
- IPWorks ENUM Front-End Base Package, see Section 3.4 on page 13
- IMS Interconnect ENUM-related Value Package, see Section 3.5 on page 14
- IPWorks AAA Base Package, see Section 3.6 on page 15
- IPWorks AAA Front-End Base Package, see Section 3.7 on page 26
- IPWorks PKI authentication AAA-related Value Package, see Section 3.8 on page 27
- IPWorks Wi-Fi Mobility AAA-related Value Package, see Section 3.9 on page 28
- IPWorks DHCP Base Package, see Section 3.10 on page 29

3.1 IPWorks DNS

The Domain Name System (DNS) is a hierarchical, distributed database. It stores information for mapping internet hostnames to IP addresses and conversely, mails routing information, and other data used by internet applications.

The IPWorks DNS server is based on the Internet Systems Consortium (ISC) BIND 9.9.9-P6 DNS server. The Ericsson IPWorks DNS server also includes ActiveSelect DNS (see Section 3.1.1 on page 10).

The IPWorks DNS Server supports the IPv4/IPv6 Dual Stack on traffic interface, which makes it possible to use IPWorks DNS query/responses on IPv6 transport plane.

On the other hand, on traffic plane, the IPWorks DNS Server supports the AAAA Resource Records, IPv6 reverse lookups by PTR Resource Records, DNS Zone Transfer, and View/ACL control functions over IPv6.

IPWorks DNS supports many configuration options supported by BIND. For example, `rrset-order` option, it might be useful to configure the order of the records placed into the response when multiple records are returned in an answer. The `rrset-order` permits configuration of the ordering of the records in a multiple record response.

IPWorks DNS offers solution to separate internal DNS service from external DNS service. "internal" DNS server (iDNS) provides DNS resolution from internal network nodes and external DNS server (eDNS) provides DNS resolution from external network nodes. Both can be managed in same configuration provided that the traffic for iDNS and eDNS topology is separated to achieve the high security demand imposed by the iDNS/eDNS support.

3.1.1 ActiveSelect DNS

ActiveSelect DNS (ASDNS) integrated with element manager is used for load balancing of network resources improving network performance level.

ActiveSelect DNS (ASDNS) is an extension to DNS. This extension makes DNS more dynamic when responding to queries. The IPWorks DNS server with ASDNS uses information sent to it from an ASDNS Monitor so it can make more intelligent decisions about what information to include in certain responses.

ASDNS is able to monitor and report status for DNS A and AAAA records by collecting the status/load of the resources over IPv4/IPv6 transport interface.

For different service nodes, the monitored resources can be different with customized script. IPWorks ASDNS provides scripts for monitoring for example ePDG nodes' status and load, which help balancing the load of the nodes. It can balance the load of the nodes and additionally protect the nodes from overload. For example, if the corresponding monitored node is down or its load exceeds the predefined threshold, ASDNS notifies DNS to remove the overloaded or unavailable nodes from the DNS responses sent to UEs.

For supporting load-balancing for Ericsson nodes, IPWorks ASDNS provides customized scripts for monitoring the nodes' status and load.

ASDNS is useful in cases where:

- Only reachable addresses need to be returned for queries of same domain names.
- Addresses that are close to the source of the query are preferred. Addresses that are close to each other (based on network topology) need to be returned for queries of same domain names.
- Overload protection distributes a load to different nodes based on collected measures.

3.2 IPWorks Internet DNS

IPWorks Internet DNS server offers the DNS and ASDNS functionalities for resolving the public Internet Addresses. The Internet DNS is always deployed as standalone Base Package. It can be deployed in internet scenario working as caching and/or authoritative DNS server.



IPWorks Internet DNS provides the same service as IPWorks DNS, and is applicable on Reference Configuration for SLES 12 SP2 with KVM and HP DL380 G9 only.

Note: IPWorks Internet DNS does not support PL VM scaling.

3.3 IPWorks ENUM

Standard ENUM is defined by RFC 3761. It is based on DNS and uses DNS Naming Authority Pointer (NAPTR) resource records. IPWorks ENUM server is an enhancement towards ISC BIND server. Compared with BIND server, ENUM server has obvious advantages in dealing with large number of NAPTR records:

- ISC BIND uses text file based database. It is not convenient to search or modify a specific DNS record in millions of data. Towards this, ENUM replaces the text file based database with MySQL database. Add/Modify/Delete data is now much faster and safer. Provisioning latency is also reduced from minutes to seconds.
- ISC BIND has a limitation of total number of DNS records. The limitation is the total memory that can be allocated by a single DNS process. ENUM server with scalable configuration can support up to hundreds of millions of ENUM NAPTR records.

Figure 5 shows the ENUM architecture:

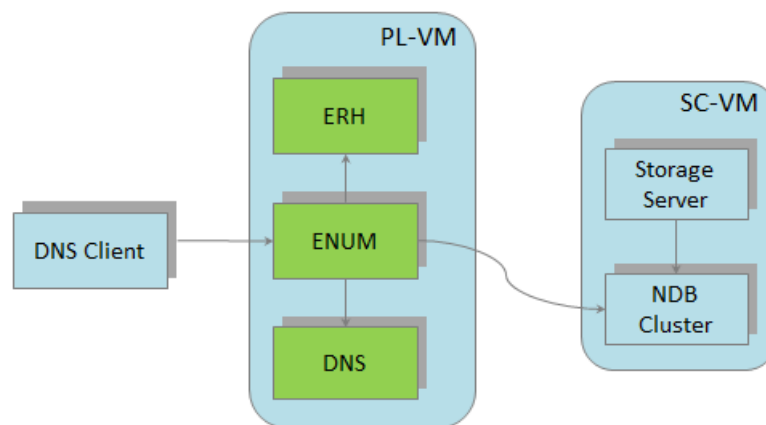


Figure 5 ENUM Server Architecture

IPWorks ENUM Server supports the IPv4/IPv6 Dual Stack on traffic interface, and View/ACL control over IPv6 as well.

3.3.1 Wildcard Options

At most of time, IPWorks ENUM checks QNAME label by label, until the whole QNAME is matched. The corresponding data are then sent back to the client. This is a process called "exact matching".

The wildcard option is an extension to "exact matching". It has two forms:

- QNAME starting with an "asterisk label", such as *.9.3.1.e164.arpa;
- Number range, such as 1391660010 ~ 1391660400.

When all these forms are provisioned in the ENUM database, IPWorks first checks "specific matching", "number range" wildcard option, and then "asterisk label" wildcard option.

- If any of these three criteria is met, IPWorks ENUM discontinues the checking and sends back the corresponding data to the client.
- If none of these criteria is met, IPWorks ENUM sends "NXDOMAIN" to the client.

3.3.2

ERH

External Resolution Handler (ERH) is an extension to the ENUM server to assist lookups in external database. Same as ENUM server, ERH is also responsible for E.164 resolution, such as Number portability resolution.

The difference between ERH and ENUM is, ENUM is used to process query with local data, while ERH is used to process the query with help from other network nodes, for example, NP databases.

Figure 6 shows ERH architecture:

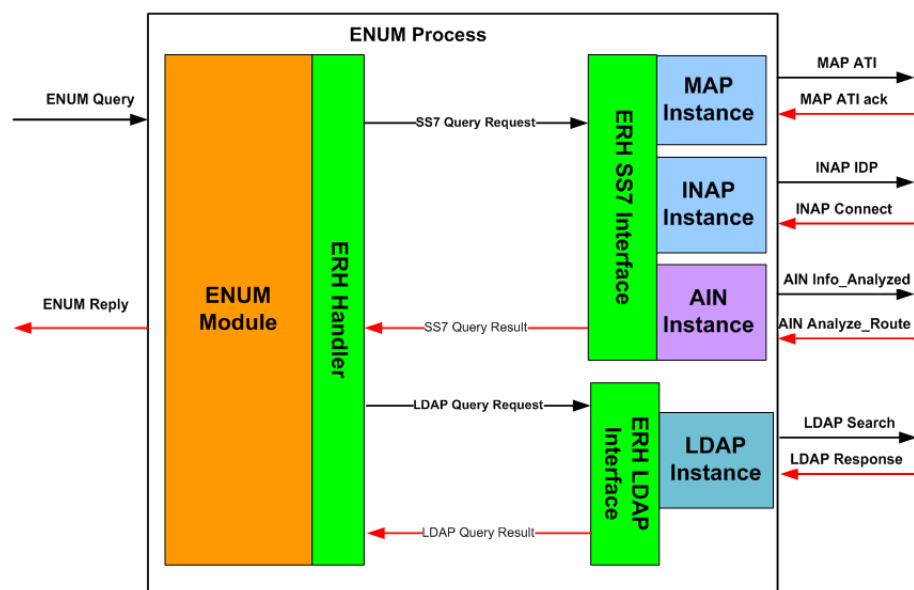


Figure 6 ERH Architecture



IPWorks ERH is able to interact with other nodes by AIN, MAP, or INAP SS7 protocol. MAP and INAP can be supported simultaneously on one machine. However, AIN instance cannot, it must be deployed at another machine.

Figure 7 shows ERH SS7 stack version information:

INAP ETS 300 374-1 v1.1.3 ETSI EN 301 668-1 v1.1.3	MAP 3GPP TS 29.002 (V6.10.0)	AIN GR-1299-CORE Issue 10
ITU TCAP ITU-T rec. Q.771-Q.775 (06/97) ITU-T rec. Q.752 (06/97) ETSI rec. ETS 300 287-1 (11/96) JT-Q.771-JT-Q.774 (1997)		ANSI TCAP ANSI T1.115-1990 ANSI T1.114-1992 ANSI T1.114-1996
ANSI SCCP		

Figure 7 ERH SS7 Stack Overview

IPWorks ERH supports IP (SIGTRAN) as transport layer, and it supports the Number Portability (NP) query/response over IPv6 transport by using SS7 SIGTRAN.

IPWorks ERH is also able to interact with other nodes using LDAP. SS7 and LDAP can be supported simultaneously on one machine.

3.4 IPWorks ENUM Front-End

IPWorks ENUM Front-End is able to deploy as a Front-End interacting with Back-End Database (for example, CUDB).

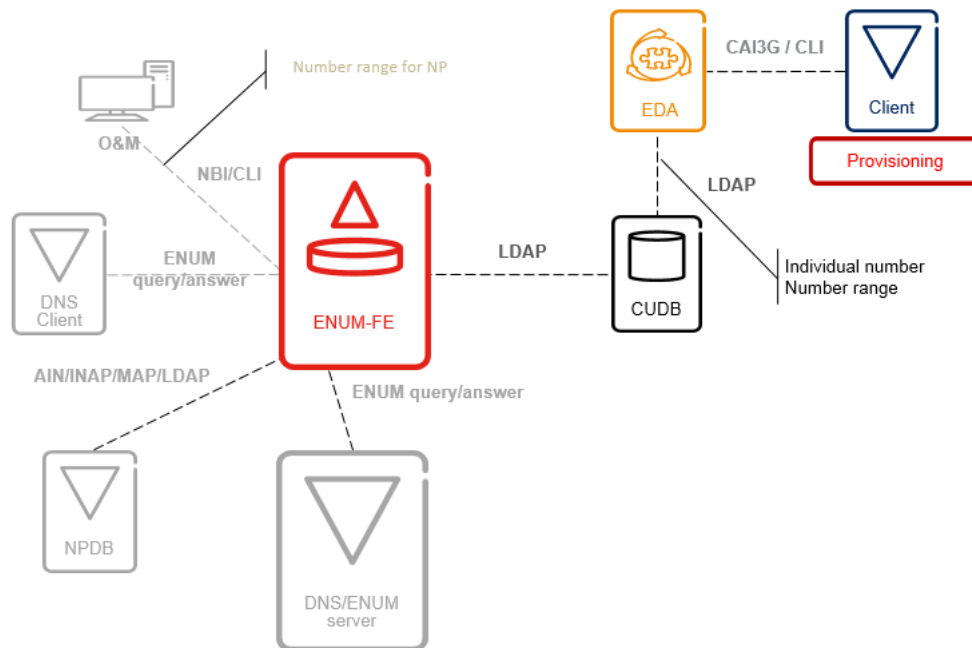


Figure 8 ENUM-FE

The Ericsson Dynamic Activation (EDA) provisions ENUM data to CUDB instead of IPWorks. IPWorks ENUM-FE fetches the ENUM master data from CUDB using LDAP interface.

3.5 ENUM Feature: IMS Interconnect

The ENUM-related Value Package "IMS Interconnect" is applicable to both ENUM and ENUM-FE base packages.

IMS Interconnection, an enhancement of standard DNS/ENUM infrastructure provides the E.164 number resolution in different operator domains. IMS interconnect capability provides a means to secure SIP-to-SIP connectivity for enriched multimedia communication, avoiding fallback to 2G/3G domain. By enabling the IMS Interconnection functionality, the operator benefits the interconnection between IMS services and the number portability across operator domains in both national and international scenarios. The enhanced ENUM architecture is a single root architecture with enhanced Tier 0 and Tier 2 ENUM Server.

Figure 9 shows the traditional and enhanced architectures:

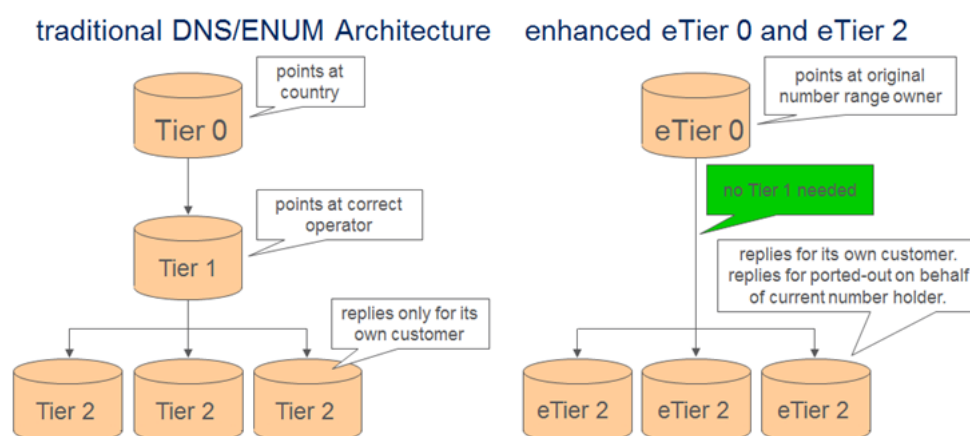


Figure 9 Enhanced Tier0 and Tier2 ENUM Architecture

eTier 0 ENUM Server

The eTier 0 ENUM Server points to an eTier 2 ENUM server operated by a network operator for the number ranges assigned to that operator according to the national numbering plan. The eTier 0 analyses the Country Code as well as the respective Network Codes, and refers to the DNS/ENUM server in the original number range owner.

eTier 2 ENUM Server

The local eTier 2 ENUM Server gets all ENUM queries for the number ranges assigned to it according to the national numbering plan.

For its own customers, the operator replies with the correct number resolution from its own eTier2 ENUM Server or uses MNP DB to determine Recipient Operator for Ported-out numbers.

If the number does not belong to the operator, the ENUM query is forwarded to the number range owner of the individual number for further resolution.

eTier 2 ENUM Server also has the capability to restrict the replies to ENUM request sent by interconnected partners based on the commercial agreement, and to construct the ENUM/NP URI format based on the local policy.

3.6 IPWorks AAA

IPWorks AAA server realizes Authentication, Authorization, and Accounting (AAA) function to handle user requests for access to network resources.

Radius and Diameter are two major AAA protocols being used today. As a successor of Radius, Diameter provides more flexible, secure, and reliable protocol than RADIUS, and it is adopted as primary protocol of AAA in 3GPP standards. Hence, IPWorks AAA supports both Radius and Diameter protocol, which makes it compliant to legacy scenarios and 3GPP trend proof.

For Radius protocol, IPWorks AAA server can work as a proxy server only, or work as home AAA server only, or work as a proxy server and home AAA server simultaneously. And for diameter protocol, IPWorks AAA server can only work as a home server.

The IPWorks AAA server can act as a Radius proxy server between a Radius client (NAS) and the Home AAA Server. It forwards the authentication, authorization, accounting requests from Radius clients to the target home AAA servers based on the realm, and forwards Change-of-Authorizations (CoA), or Disconnect Messages from the home AAA servers to the corresponding Radius Clients (NAS).

The Realm is used for selecting target home AAA servers; IPWorks Radius AAA can be configured to fetch the realm information from the following specific AVPs according to priority:

- Username
- Called-Station-Id
- NAS-Identifier

The realm can be constructed via a regular expression for AVP format matching as an enhancement. For example, in the Wi-Fi scenario, IPWorks can work as a proxy AAA server for Open SSID user to select the target AAA servers with the constructed realm by AVP Username format based on the configuration; and work as a home AAA server for secure SSID user simultaneously.

3.6.1 AAA for GPRS (Gi Interface, Radius AAA)

The Gi interface, which is standardized in 3GPP TS 29.061, connects a Gateway GPRS Support Node (GGSN) and an external packet data network, enabling the Mobile Stations to exchange IP packets with the external network. IPWorks AAA services are used to authenticate a user, provide subscriber information and accounting to activate back-end services.

IPWorks AAA can also be used for dynamic IP address allocation. The IP address pool selection can be based on user or GGSN.

The following scenarios, which are defined in 3GPP TS 29.061, are supported by IPWorks AAA:

- Authentication and accounting for IP PDP type
- Authentication and accounting for PPP PDP type
- Accounting update
- Accounting mediation, IPWorks AAA supports forwarding accounting message to multiple target server groups based on configuration, and it can be used by regulatory service.
- AAA-Initiated PDP context termination



Figure 10 shows an example of AAA for GPRS (Gi Interface).

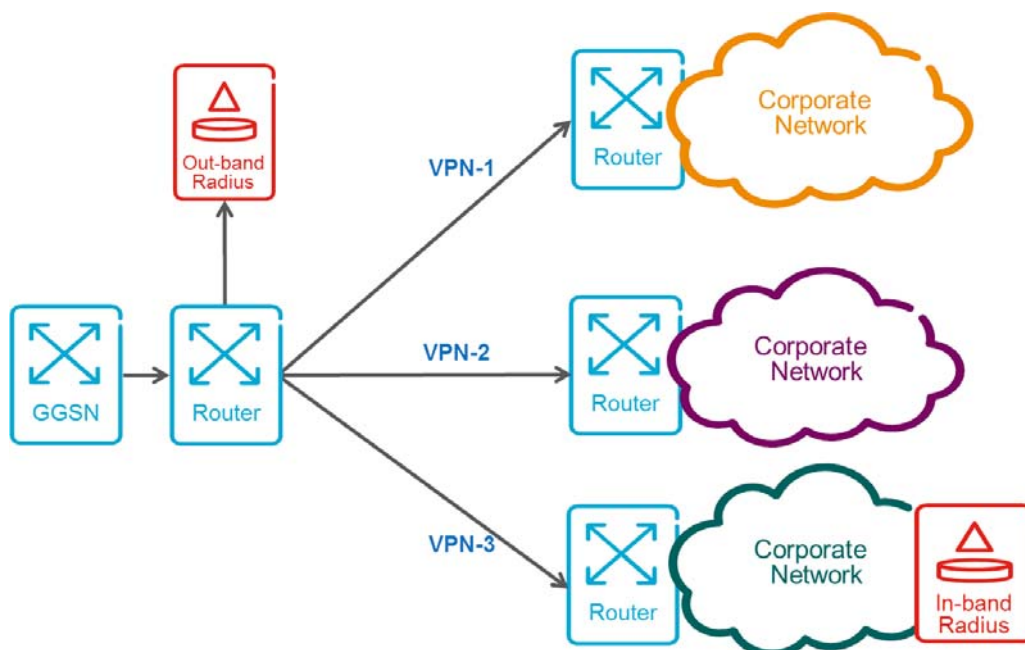


Figure 10 AAA for GPRS (Gi Interface)

In-band and out-band

The definition of an APN using an "in-band RADIUS" server refers to the location of the RADIUS server being physically or logically located, or both. The in-band RADIUS server usually provides AAA functions based on the network policies, access methods, and authentication, which facilitates it to be used in corporate network access in particular.

For those corporations who do not have their own RADIUS server (in-band) for AAA services. The out-band RADIUS server can be used, referred as "shared RADIUS".

3.6.2 AAA for Fixed Access (Radius AAA)

IPWorks AAA supports user Authentication, Authorization, and Accounting for fixed access network based on RFC and BBF standards. eSAPC can be integrated for policy control in the fixed access network scenario.

The following functionalities supported by IPWorks AAA:

- Authentication, Authorization, and Accounting for PPPoX users
- Accounting update
- Accounting mediation, IPWorks AAA supports forwarding accounting message to multiple target server groups based on configuration, and it can be used by regulatory service.

— AAA-Initiated user termination

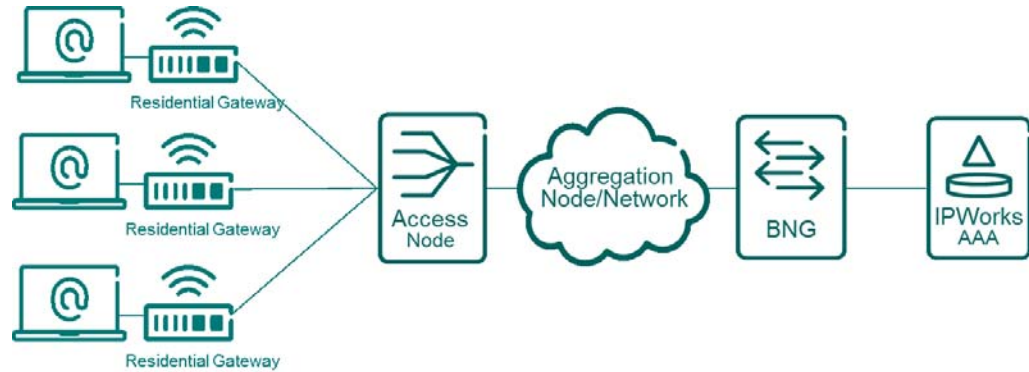


Figure 11 AAA for Fixed Access

For Web-based authentication (Open SSID user accessing internet via fixed network), which needs input Username and password in a web-portal for user authentication. IPWorks AAA integrated with eSAPC can support web-based authentication using PAP/CHAP protocol.

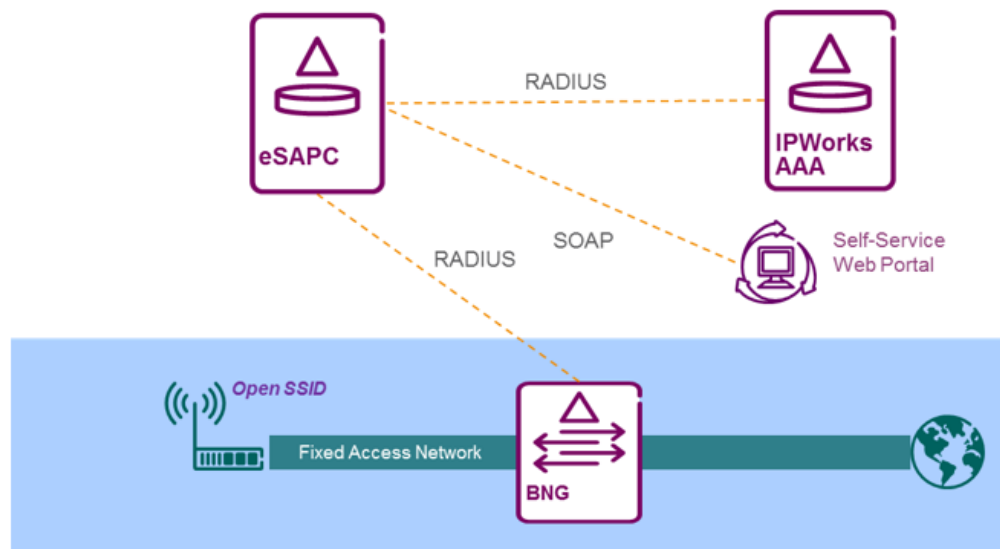


Figure 12 Web-based Authentication Support for Open SSID User

3.6.3 AAA for Wi-Fi Offload (Radius AAA)

Wi-Fi technology builds on IEEE 802.11 standards. A Wi-Fi enabled device such as a personal computer or smart phone can connect to any IP-based network. IPWorks AAA is used to offer mobile users equivalent security levels accessing WLAN than GSM, GPRS and WCDMA network. For SIM-based authentication, access authentication to the WLAN is done using the authentication vectors stored in the HLR for GSM/GPRS/WCDMA authentication. The authentication vectors are retrieved by MAP.

For Wi-Fi offload, SIM-based authentication mechanisms are supported in Wi-Fi Access scenario, which minimizes the interaction from end-user perspective and offloads the traffic data from mobile access to fixed access network.

For SIM-based authentication in Wi-Fi offload scenario, it offers the 3GPP devices the possibility to connect to Internet through Wi-Fi hotspot, and access the 3GPP services (such as mobile internet) through Wi-Fi access. In this scenario, IPWorks AAA can be used for SIM-based devices authentication using EAP-AKA and EAP-SIM.

Figure 13 shows an example of AAA for Wi-Fi solution:

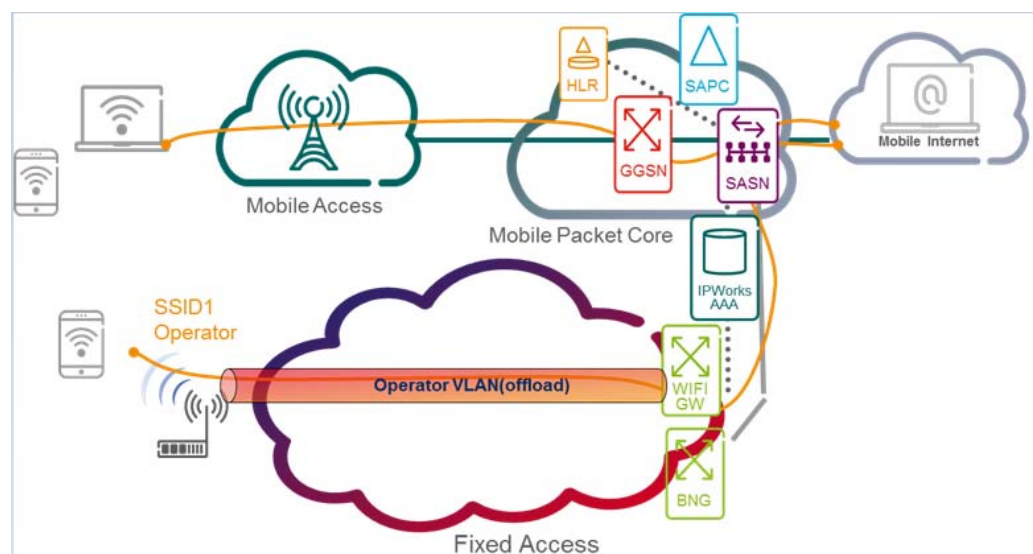


Figure 13 AAA for Wi-Fi Offload

IPWorks AAA implements Wa, Wm, and D'/Gr' reference points as per 3GPP TS 23.234 for SIM-based authentication. For the reference architecture, refer to Figure 12. The following AAA functions are supported by IPWorks:

- EAP-SIM and EAP-AKA authentication mechanism in WLAN AAA Solution.
- EAP-AKA and EAP-SIM full authentication and fast re-authentication procedures.
- EAP-SIM authentication for a 3G user, in this case, if AAA receives quintuplet vectors from HLR within EAP-SIM authentication, it translates it to triplet vectors.
- During the EAP-AKA or EAP-SIM authentication, as the authentication vectors are stored in the HLR Server, IPWorks AAA fetches the authentication vectors from HLR through SS7 MAP protocol.
- WLAN Access authorization for the UE based on the subscriber data received from HLR, if the user has a contract for accessing the WLAN Network, then HLR returns a flag in Operator Determined Barring HPLMN data.

- Receive notifications from HLR about the user status change and according to the notifications contents to decide whether send Disconnect-Request to terminate the accounting session automatically.
- Accounting functions in WLAN scenario.
- To support WLAN user to access 3GPP network, the node SASN initiates the setup of the Gx flow with SAPC. Owing to BRAS today cannot perform double accounting to both AAA and SASN, AAA forwards the accounting message to SASN to trigger the Gx flow between SASN and SAPC. When forwarding the accounting message, AAA inserts UE MSISDN (Calling-Station-ID) and UE IP address (Framed-IP-Address) in the accounting message if they are not included. IPWorks AAA supports forwarding accounting message to multiple target server groups based on configuration, and it can be used by regulatory service.
- Charging characteristics can be included in the user profile sent from HLR to AAA, which can be added in the Radius EAP response message back to Wi-Fi GW to facilitate and differentiate prepaid/postpaid information within the context of ENIW Solution.

3.6.4 AAA for LTE/EPC

AAA for LTE/EPC (3GPP AAA) provides the diameter protocol based procedures supporting Non-3GPP IP Access scenario, which is specified in 3GPP TS 23.402 and 3GPP TS 29.273, IPWorks 3GPP AAA supports the access authentication, authorization from Non-3GPP network such as CDMA2000, WiMAX, Wi-Fi, as well as mobility between these networks and LTE accesses.

Figure 14 shows AAA for LTE/EPC:

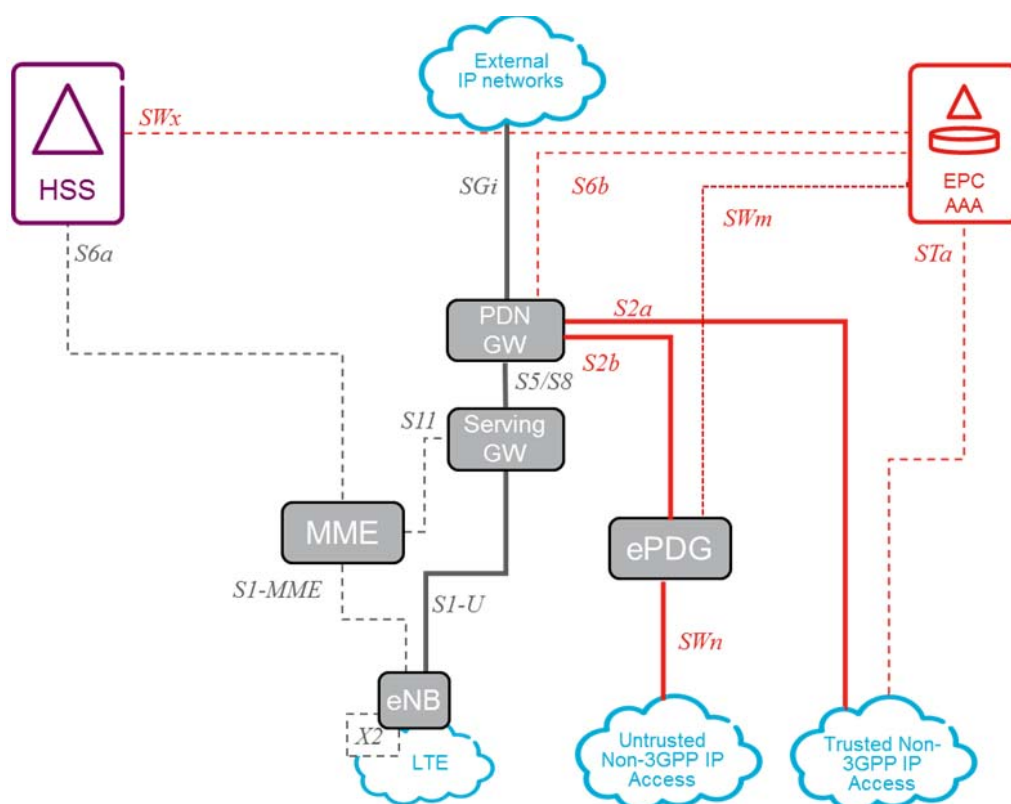


Figure 14 AAA for LTE/EPC

IPWorks 3GPP AAA supports the STa, SWm, S6b, and SWx interfaces as per 3GPP TS 23.402 R12 and 29.273 R12. And it also supports the following functions and procedures for Untrusted and Trusted non-3GPP IP Access scenarios:

- EAP-AKA' as the authentication mechanism during the Trusted non-3GPP Access (STa Procedure).
- EAP-AKA as the authentication mechanism during the Untrusted non-3GPP Access (SWm Procedure).
- Fetch the authentication vectors and user profiles from HSS through SWx interface during EAP-AKA'/AKA authentication.
- Update PDN GW information into the HSS, downloading the QoS Profiles and making the mobility related parameters for non-3GPP Accesses possible.
- Support SLF/HSS failover and load balancing.
- Support user de-registration, and user profile update triggered by HSS via SWx RTR (Registration-Termination-Request) message and SWx PPR (Push-Profile-Request) message. And also support HSS-based P-CSCF restoration procedure triggered by HSS via SWx PPR (Push-Profile-Request).
- Support to include AVP AAA-Failure-Indication in SWx request to notify HSS the previous 3GPP AAA Server is unavailable.

- Support throttling on SWx requests to HSS with configured traffic rate to protect HSS from overloading.

IPWorks 3GPP AAA supports direct connections to EPC nodes (ePDG, HSGW, P-GW, and SLF/HSS), and also supports connections to EPC nodes via Diameter Routing Agent (DRA).

For DRA deployment scenario, IPWorks 3GPP AAA server supports multiple connections to one DRA via TCP and SCTP; and supports load-balancing and failover among multiple DRAs.

Figure 15 shows the scenario for AAA deployment with DRA.

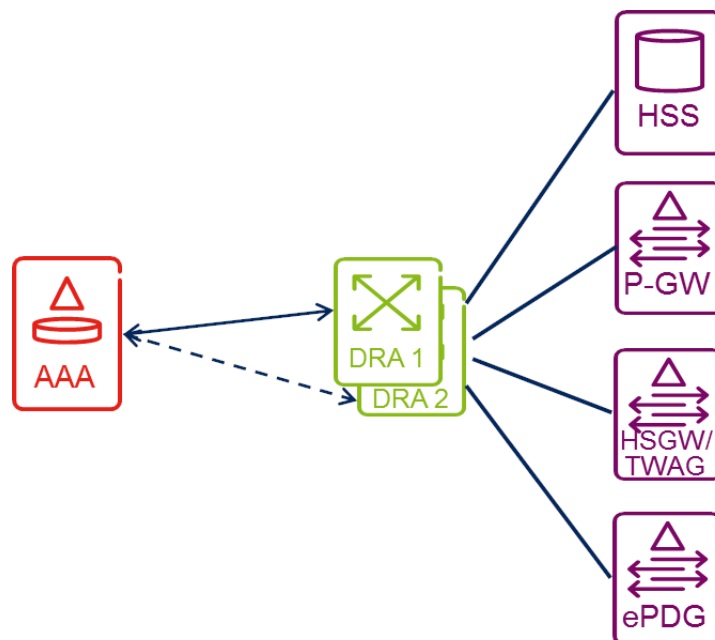


Figure 15 AAA Deployment with DRA

3.6.5 Untrusted Wi-Fi Support

When UE attaches to EPC network through untrusted Wi-Fi access, ePDG triggers the AAA for fetching transport mobility parameters, tunnel authentication and authorization through SWm interface, which is specified in 3GPP TS 23.402 R12 and 3GPP TS 29.273 R12.

IPWorks AAA supports user authentication and authorization, and transports Network Based Mobility (NBM) related mobility parameters in a case the UE attaches to the EPC network through the S2b (based on PMIPv6 or GTPv2) and SWn reference points (for example, IP Mobility Mode Selection information).

When UE attaches to EPC network for an IMS emergency call through untrusted Wi-Fi access, Emergency-Indication shall be included in SWm and S6b request, IPWorks AAA follows user authentication procedure as a non-emergency request,



and applies specific policies for emergency services, as specified in 3GPP TS 23.402 R13 and 3GPP TS 29.273 R13.

To make the authentication procedure more secure in customized solution, UE (SIM or non-SIM Wi-Fi device) can mask the identity using RSA encryption and base64 encoding. And when the DER message with masked identity is sent to the IPWorks AAA by ePDG, the IPWorks AAA is able to RSA decrypt and base64 decode to obtain the native identity and continue authentication process.

Figure 16 shows the Untrusted Wi-Fi Support for SIM user:

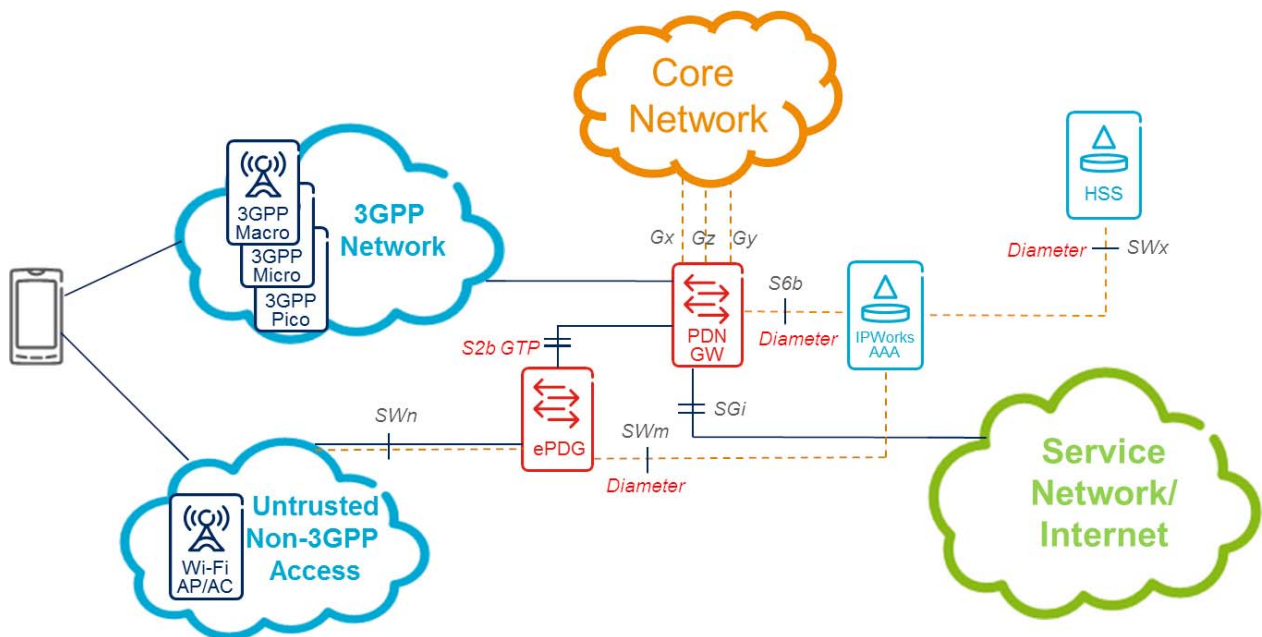


Figure 16 Untrusted Wi-Fi Support Solution

3.6.5.1 Extension for SES authentication

Secure Entitlement Server can use SWm interface to interact with IPWorks AAA server for user authentication, and retrieving user information (MSISDN).

User authentication and profile data can be located in HLR (3G user), and/or in HSS (4G user). IPWorks AAA supports user authentication for SES entitlement, and supports authentication fallback to HLR if user data is not located in HSS.

When SES sends the authentication request to IPWorks AAA, IPWorks AAA attempts to retrieve user authentication and profile data and from HSS first; if HSS returns DIAMETER_ERROR_USER_UNKNOWN, IPWorks AAA contacts HLR to retrieve user authentication data to continue user authentication.

3.6.5.2 IMEI check support

IPWorks AAA supports the control of the devices attempting the connection to the network. IPWorks AAA contacts the Equipment Identity Register (EIR) node for

checking the received/retrieved international mobile equipment's identity (IMEI) status when UE is attached via untrusted non-3GPP access network.

If IMEI check is required by operator policy and configuration, IPWorks AAA server does request the EIR to perform the IMEI check by sending the ME Identity Check Request (ME Identity, IMSI). Upon receiving the ME Identity Check Ack (Response), the IPWorks AAA server determines whether to continue or to stop the authentication and authorization procedure. If IPWorks AAA server determines that the authentication and authorization procedure shall be stopped based on operator policy and configuration, it replies to the WMG/ePDG with a failure message with appropriate cause value (DIAMETER_ERROR_ILLEGAL_EQUIPMENT).

3.6.6 Trusted Wi-Fi Support

Using this functionality, operators can seamlessly connect trusted WLAN access network to 3GPP packet core network, optimize capital expenditures by reusing core network capabilities. Any end-user device with Wi-Fi capability can connect to an operator's Wi-Fi network, and enjoy services available through the packet core network.

Trusted Wi-Fi Support is based on the SIM/USIM authentication, by means of EAP-AKA or EAP-SIM. The trusted Wi-Fi operation is controlled based on the user 2G/3G packet profiles retrieved from HLR. Performing the EAP authentication procedure and profile download processes, IPWorks AAA performs one of the actions:

- Trigger S2a GTP Tunnel setup between Wi-Fi GW (WMG/TWAG) and PDN GW (for example, enabling direct routing of the traffic towards EPC network)
- Trigger the local breakout (for example, resulting to routing of the payload through BNG for services network or internet access directly)
- Reject the request if no Wi-Fi subscription authorization for the user.

Figure 17 shows Trusted Wi-Fi Support solution:

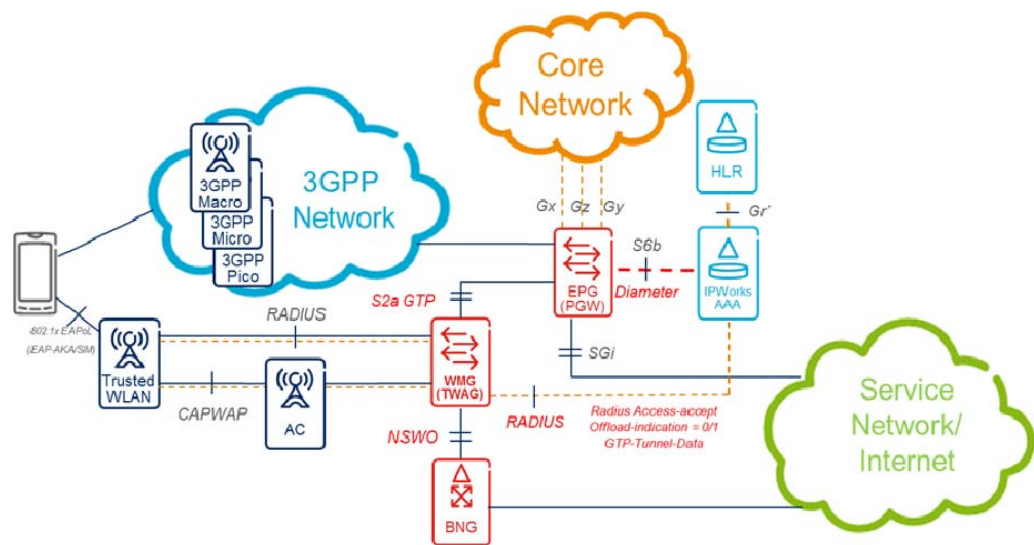


Figure 17 Trusted Wi-Fi Support Solution

Proprietary Traffic Steering for SIM Wi-Fi Device

Proprietary traffic steering for SIM Wi-Fi device is an enhancement in IPWorks AAA. IPWorks AAA includes the proprietary usedRAT-Type “WLAN” in Gr' interface to HLR. HLR does not disconnect the IP connection through 3GPP RAN if UPDATE_GPRS_LOCATION from IPWorks AAA with the proprietary used RAT-Type “WLAN”. The UE has dual IP connections through Wi-Fi and 3GPP RANs, and traffic steering is supported.

3.6.6.1

HSS Integration

The solution of HSS integration supports the retrievable of the user authentication vectors and profiles from HSS (in case of the LTE/4G user) without changing the existing capability of Wi-Fi Access Network.

Figure 18 shows the integrating with HSS solution:

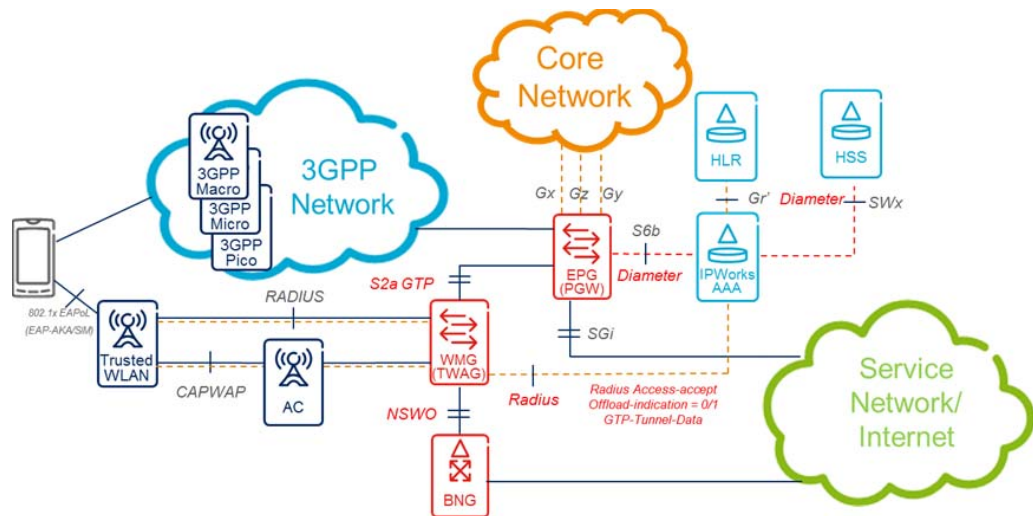


Figure 18 Trusted Wi-Fi Support Solution with integrating with HSS

- For EAP-AKA authentication (3G/4G user), IPWorks AAA contacts HSS through SWx interface for retrieval of user authentication vector and profile data. If no subscription in HSS, IPWorks performs a fallback to HLR for retrieval of user authentication vector and 3G user profile data.
- For EAP-AKA' authentication (4G user), only HSS is selected for retrieving user authentication vector and profile.
- For EAP-SIM authentication (2G/3G user), only HLR is selected for retrieving user authentication vector and profile.
- S6b procedure triggered by PDN GW is supported by AAA for EAP-AKA based authenticated users for trusted Wi-Fi support in HSS.
- Support SLF/HSS failover and load-balancing for HSS integration.
- Support user de-registration triggered by HSS

3.7 IPWorks AAA Front-End

For IPWorks AAA for GPRS and PKI authentication, it can work as Frond-End to retrieve user authentication and profile data from an external back-end database (such as CUDB). The IPWorks AAA-FE provides the same service as IPWorks AAA Classic (Classic deployment Base Package).

AAA-FE acts as a data-less front end with only the dynamic/session data and application logic, the AAA user data is provisioned in the external back-end database (such as CUDB), which can be accessed by the AAA-FE through LDAP interface.

Figure 19 shows the IPWorks AAA-FE for GPRS and PKI authentication in Layered solution:

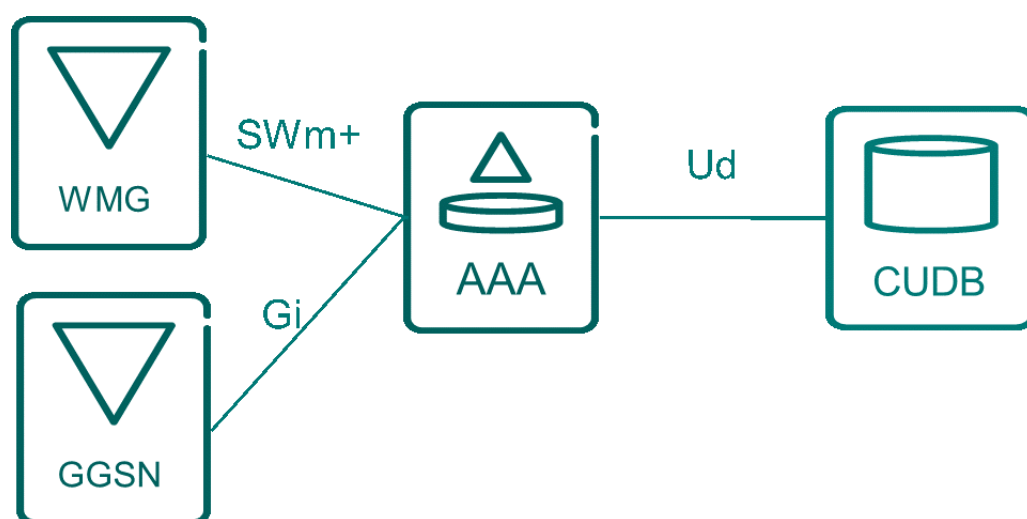


Figure 19 IPWorks AAA-FE for GPRS and PKI Authentication

IPWorks AAA for LTE/EPC can interact with HLR-FE and HSS-FE in a layered solution/deployment. The IPWorks AAA-FE provides the same service as IPWorks AAA Classic (Classic deployment Base Package).

Figure 20 shows IPWorks AAA-FE for LTE/EPC in Layered solution:

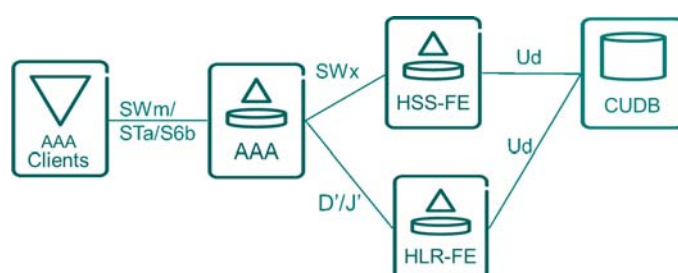


Figure 20 IPWorks AAA-FE for LTE/EPC

3.8 AAA Feature: IPWorks PKI authentication

The IPWorks AAA related Value Package "PKI Authentication" is applicable to IPWorks AAA Base Package only.

IPWorks AAA also supports PKI based authentication for enabling Wi-Fi non-SIM devices to access 3GPP packet core network through untrusted Wi-Fi access. For PKI based authentication, the Wi-Fi user's non-SIM device is associated with a virtual IMSI.

For PKI based authentication for emergency service with Emergency-Indication in SWm+ authentication request, IPWorks follows the authentication procedure as non-emergency request, and apply specific policies for emergency services.

When a connection attempt is received, the IPWorks AAA performs the authentication procedure using EAP-TLS to verify the PKI certificate assigned to the device. IPWorks AAA interacts with Ericsson Certificate Administration Server (ECAS) to check the validity of the certificate status using OCSP.

IPWorks AAA supports the following ways to check the revoked status of UE certificate during PKI authentication procedure.

- Support to check certificate ID with provisioned certificate ID. If the UE certificated Id is provisioned by SEM, IPWorks AAA checks the received certificated ID with the provisioned certificate ID, if it does not match, and the authentication request shall be rejected. It can be disabled or enabled by configuration.
- Support to check the timely revoked status of UE certificate via OCSP. It can be enabled and disabled by configuration.

Figure 21 shows the IPWorks AAA PKI authentication solution.

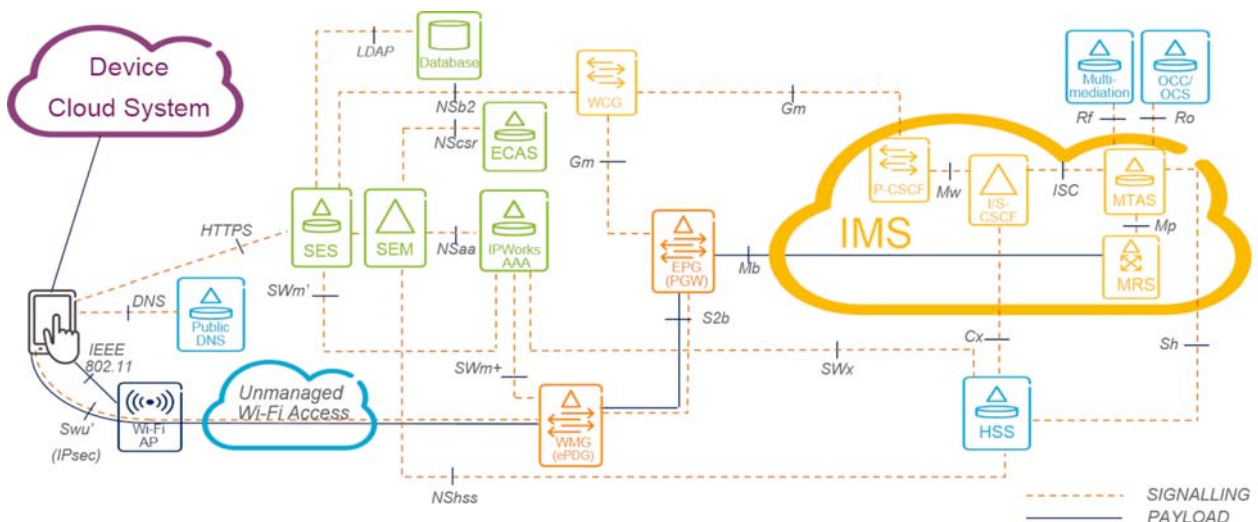


Figure 21 PKI Authentication Solution

3.9 AAA Feature: IPWorks Wi-Fi Mobility

The AAA value package "Wi-Fi Mobility" is applicable to AAA and AAA-FE Base Packages.

When UE attaches to EPC network through untrusted Wi-Fi access, IPWorks AAA supports user authentication and authorization, and transports Network Based Mobility(NBM) related mobility parameters in a case when the UE attaches to the EPC through the S2b (based on PMIPv6 or GTPv2) and SWn reference points (for example, IP Mobility Mode Selection information).

IPWorks AAA can also retrieve UE location information during UE attachment.



IPWorks AAA can obtain UE location by one of the following ways:

- UE IP address received from ePDG/WMG with lookup geographic IP database
- IPWorks AAA contacts HLR for checking registered VLR via MAP ATI request to obtain UE location if UE is registered in CS.

The preference and priority for the two methods can be configured.

If roaming restriction is needed, the VPLMN ID (Visited-Network-Identifier) can be constructed by the UE location country code and sent to HSS for roaming restriction. The roaming restriction policy is defined in HSS.

The UE location information (VPLMN ID) can also be sent to ePDG for charging.

When UE attaches to EPC network for an IMS emergency call through untrusted Wi-Fi access, IPWorks AAA can check the UE location, and decide to reject or accept the attachment. If it is detected UE attachment from location outside home country, the attachment attempt shall be rejected.

3.10 IPWorks DHCP

3.10.1 DHCPv4 Server

The IPWorks DHCPv4 server is based on ISC DHCP 4.3.5 implementation. The DHCPv4 server supports most of standard DHCP server and client options defined in IETF RFCs.

The DHCP server is mainly used for IP address allocation, and also allows for the automatic configuration of IP networking parameters, such as the subnet mask, default router(s), domain names, DNS addresses, and so on. This avoids manual configuration of IP-related parameters on the client or node, which reduces errors, eliminates the need to communicate these parameters through other means, and allows flexible reconfiguration of network resources.

Authentication

Authentication is implemented to address issues of Denial of Service attacks, Theft of Services, or attempts to establish a Man-in-the-Middle service through a rogue server or client.

In the authentication implemented in IPWorks, the administrator needs to configure each client with a unique key and then configure all these keys on the server. The keys, the shared secret between DHCP clients and servers, are the basic means of providing security through authentication. Thus, each client has a unique authentication key and the authentication mechanism (delayed authentication) as per RFC 3118 in DHCPv4.

Authentication is initiated by the client, that is, if the client includes authentication as an option in the message, then the server authenticates the client using the unique key mentioned above.

Client Classing

The IPWorks DHCPv4 Server can be configured to classify clients. Clients can be classified by almost any information that might be sent in a DHCP message. Client classing can be used to assign addresses from specific ranges or to send a specific set of configuration parameters to the group of clients.

Redundancy and Load Balancing

A redundant DHCP service can be set up by enabling the DHCP failover protocol between two DHCP servers according to DHCP failover protocol. The DHCP failover protocol synchronizes a pair of DHCPv4 servers. Under normal conditions, DHCP requests are load-balanced between the two servers according to RFC 3074. If one server fails, the other server takes over the address assignment activities.

Server Reconfiguration

When changes are made to the DHCPv4 server, the client leases must be renewed by using new configuration information. The Reconfiguration "reconfig" command is used to make the server notify clients about the changes, including changes regarding the address range.

The "reconfig" command instructs the server to unicast a FORCERENEW operation (in DHCPv4) to the clients, to renew their leases. When the clients receive these messages, they are requested to renew leases instantly.

IP Overlapping

This function allows the DHCPv4 server to be configured and work with pools having overlapped address ranges. Each pool that has overlapped address ranges serve clients from different subnets.

3.10.2

NACF

The IPWorks DHCPv4 realizes Network Access Configuration Function (NACF) as per TISPAN ETSI ES 282 004. It is responsible for the IP address allocation to the User Equipment (UE). It also distributes other network configuration parameters such as address of DNS server(s), address of signaling proxies for specific protocols (for example, address of the P-CSCF).

It also provides to the UE an access network identifier. This information uniquely identifies the access network to which the UE is attached. With this information, applications are able to locate the CLF.

The essential of NACF is to use DHCP option 82 to carry "relay agent information", which is specified in RFC 3046. A notable feature of IPWorks NACF is that option



82 is configurable. It can satisfy the format requirements of different access devices.

Rule = "^(.*) : ATM ([0-9]{1,2}) / ([0-9]{1,2}) . [0-9]* : ([0-9]{1,3}) . ([0-9]{1,5}) \$"

Output format = "\$1#\$2#\$3#\$4#\$5"

When the server receives the incoming stream, "ERX N+1:ATM 13/12.89542:12.12

Example 1 Option 82 Rule Setup

Rule = "\$1(5):\$2(6):\$3(7):\$4(8):\$5(9.1,9.4):\$6(9.6,9.8):\$7(10):\$8(11,12)"

Output format = "\$1.\$2.\$3.\$4#\$5#\$6#\$7#\$8"

When server receives the incoming stream "01:10:00:11:63:04:01:00:aa:57:01:2

Example 2 Option 82 Rule Setup



4 Interfaces

IPWorks plays an important role in both mobile and fixed networks, for example, 2G, 3G, IMS, LTE/EPC, NASS, and PSTN network solutions. The protocol used by IPWorks follows the IETF, TISPAN, and 3GPP relevant specifications.

4.1 Reference Model

4.1.1 IMS Reference Model

This section provides an overview of DNS in IMS, interfaces, and protocols.

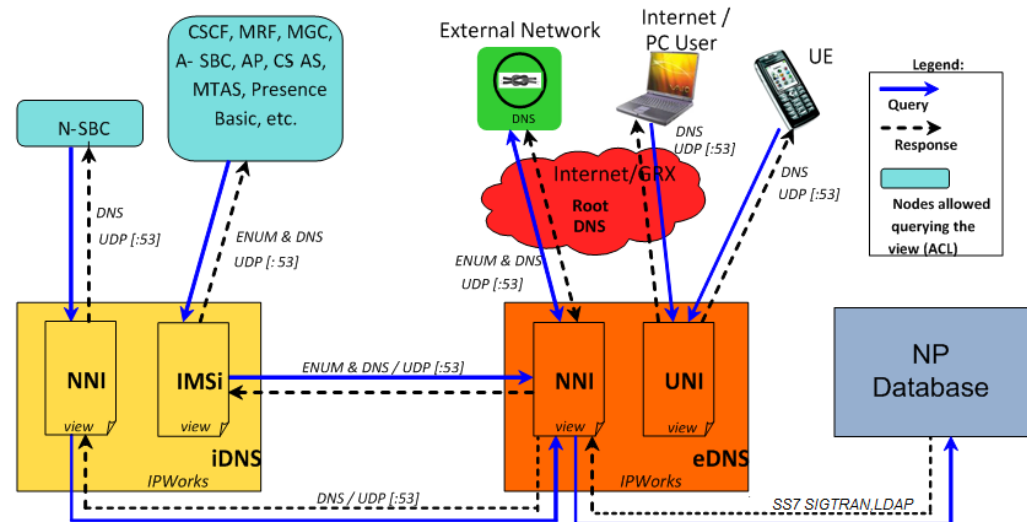


Figure 22 DNS Overview in IMS, Interfaces, and Protocols

IPWorks DNS in IMS is similar to the DNS for general Internet use, and it is based on the IETF specification, there is no 3GPP specific reference point defined on DNS in IMS solution.

The DNS is split into two parts for security reasons: one part is the internal DNS that is only used by the internal IMS System clients; the other is the external DNS that is used by the UE and nodes in external networks.

4.1.1.1 IPWorks IMS Reference Points

DNS Interface

A UE might query the external DNS to obtain the IP address of P-CSCF in the case the hostname of P-CSCF is configured in the UE. The IP address of P-CSCF can also be discovered in the PDP context activation procedure, and then DNS is not used.

A UE queries the external DNS to resolve the configured XCAP Root URL to an IP address of the AP.

External nodes might query the external name server to obtain an IP address of the SBG or an I-CSCF in the case SBG is not used.

The CSCF, MTAS, MRFC, Presence Server, SBG, and MGC use the internal DNS.

ENUM Interface

ENUM interface is used for the ENUM (NAPTR) queries, such as, for resolving E.164 address to SIP Identity (for example, "+461231" is mapped to "sip:user@domain.com").

eDNS might receive ENUM queries from cooperating networks over the NNI that interfaces with ENUM through the DN4 interface.

The interface is also used for queries related to the Number Portability.

SS7 Interface

The SS7 Interface is used between the ENUM and the external SS7 databases to retrieve Number Portability information. The SS7 interface interacts with the outside SS7 databases using AIN, MAP, or INAP protocol.

LDAP Interface

The LDAP interface is used between the ENUM and CUDB to retrieve ENUM record for ENUM-FE functionality.

The LDAP interface is used between the ENUM/ERH and the external LDAP NPDB to retrieve Number Portability information.

4.1.2 3GPP PDN Access Reference Model

Figure 23 shows the relationship between the MS, its terminal equipment, and the PLMN network in the non-EPC-based overall Packet Domain environment.

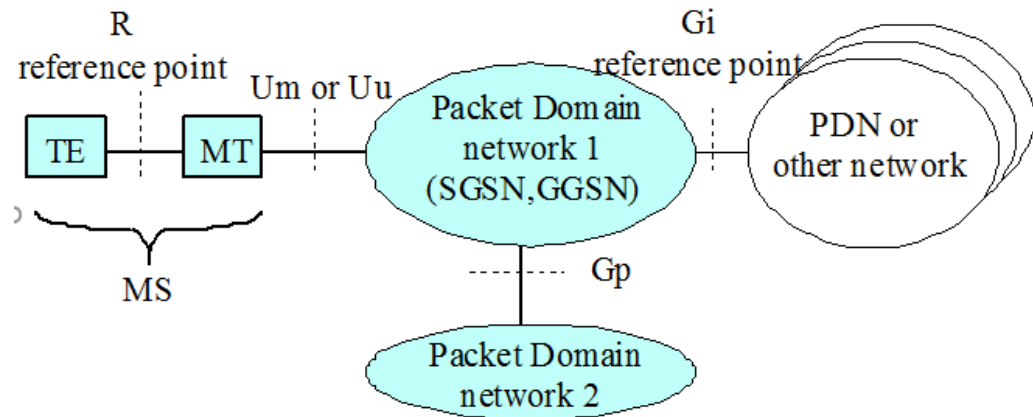


Figure 23 Packet Domain Access Interfaces and Reference Points

A GGSN might, on a per APN basis, use RADIUS authentication to authenticate a user and RADIUS accounting to provide information to an AAA (Authentication, Authorization, and Accounting) server.

AAA Server is placed in the APN Network (so called "in-band RADIUS"), for those corporation networks that do not have the RADIUS Server, the out-band RADIUS Server could be placed outside, also it is named as "shared RADIUS", which means it could be shared by multiple APN Networks.

4.1.2.1

IPWorks AAA on Gi Interface

IPWorks AAA Server supports the Radius over Gi Interface according to the 3GPP TS 29.061, for more detailed information, see Reference [35].

In essence, it can be used in Authentication, Authorization, and Accounting operations as described below:

- PAP/CHAP Authentication for the mobile subscribers to access corporation networks or internet.
- Obtain L2TP parameters for L2TP tunnel establishment between GGSN and "L2TP Network Server in a Corporate Network".
- RADIUS assisted APN Selection, the purpose of the RADIUS-assisted APN selection is to base the APN selection on subscription information. That is, the selection is based on the APN included in the created PDP context request, if RADIUS-assisted APN selection is enabled on the GGSN for that APN.
- RADIUS initiated session deactivation, such as RADIUS Disconnect Message support.
- IPv4 Address allocation, IPWorks can assign an IPv4 address to a user after a user is successfully authenticated.

- Access Control Support, if access control over RADIUS is configured, it provides a list of authorized and possibly unauthorized services to GGSN at PDP context activation.
- RADIUS Accounting Support as per RFC 2866.

4.1.3 3GPP I-WLAN Reference Model

IPWorks AAA can be used for the WLAN Access scenario (see Figure 24), the interworking between WLAN Access Network and 3GPP Network is specified in 3GPP TS 23.234 (see Reference [38]).

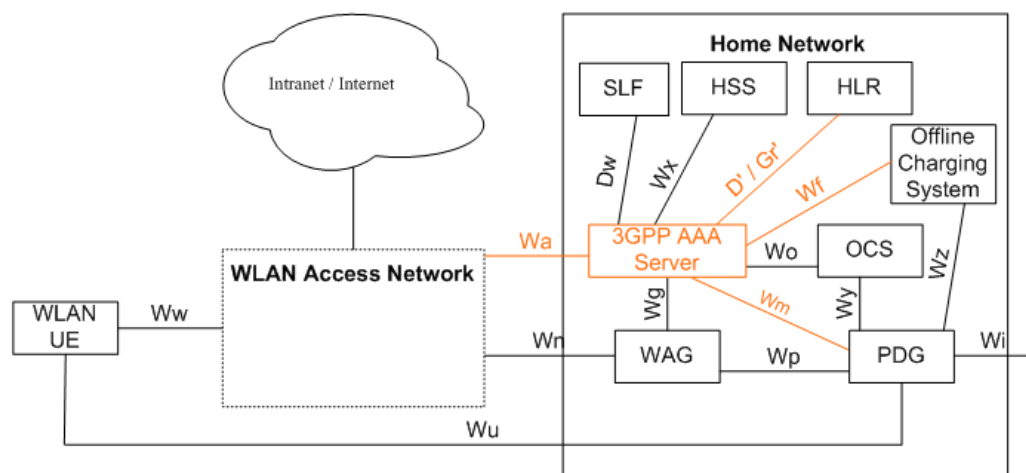


Figure 24 3GPP I-WLAN AAA Reference Model

4.1.3.1 IPWorks I-WLAN Reference Points

Wa Reference Point

Wa reference points connect 3GPP AAA to WLAN and Packet Data Gateway (PDG) respectively.

The Wa reference point is to transport authentication, authorization, and charging-related information in a secure manner. EAP authentication is transported over the Wa reference point and protocol should be Diameter or RADIUS based. Currently, IPWorks AAA server uses RADIUS protocol to convey the EAP-AKA/SIM authentication message.

The reference point supports the following procedures:

- EAP-AKA full authentication
- EAP-SIM full authentication
- EAP-AKA fast re-authentication
- EAP-SIM fast re-authentication



- Accounting
- Session disconnection through Disconnect-Request message

D'/Gr' Reference Point

The D'/Gr' Reference Point is the 3GPP compliant SS7 interface over SIGTRAN transport protocol used between the AAA Server node and Home Location Register (HLR) node, only SIGTRAN is supported.

D'/Gr' interfaces use the Mobile Application Part (MAP) protocol to obtain the authentication vector and other information from HLR. MAP is an SS7 protocol, which provides an application layer for various nodes in GSM and UMTS mobile core networks and GPRS core networks. With the application layer, the various nodes communicate with each other to provide services to mobile phone users.

For D' interface, IPWorks AAA simulates the part behaviors of VLR interaction with HLR; and for Gr' interface, IPWorks AAA simulates the part behaviors of SGSN interaction with HLR, the proprietary used RAT-Type “WLAN” in Gr' interface is supported for proprietary traffic steering mechanisms between Wi-Fi and 3GPP RAN.

The reference point is used for:

- Retrieval of authentication vectors, such as, for USIM authentication, from HLR
- Registration of the 3GPP AAA Server of an authorized WLAN user in the HLR
- Indication of change of subscriber profile within HLR (for example, indication for service termination)
- Purge procedure between the 3GPP AAA server and the HLR
- Fault recovery procedure between the HLR and the 3GPP AAA server

Retrieval of service-related information (such as APNs that might be selected by the WLAN UE) including indications of whether the service is to be supported by the HPLMN or by an identified VPLMN.

Following MAP signaling is used in Wi-Fi authentication scenario:

- MAP_SEND_AUTHENTICATION_INFO
- MAP_RESTORE_DATA
- MAP_UPDATE_GPRS_LOCATION
- MAP_INSERT_SUBSCRIBER_DATA
- MAP_DELETE_SUBSCRIBER_DATA
- MAP_CANCEL_LOCATION

- MAP_RESET
- MAP_PURGE_MS

Wm Reference Point

The Wm Reference Point between AAA Server and PDG is based on RADIUS. It is used during establishment of the secure tunnel using the EAP-AKA/SIM authentication procedures with the RADIUS operations as described in Wa reference point.

Wf Reference Point

The Wf reference point is used between AAA Server and Offline Charging System, IPWorks AAA supports to generate the Accounting CDRs locally and provides to Offline Charging System the FTP/SFTP interface for uploading or fetching the CDR data.

4.1.4 3GPP EPS Reference Model

Figure 25 illustrates the EPS architecture and its interfaces for non-3GPP Accesses. For more information about the architecture for the Non-3GPP accesses, see Reference [40].

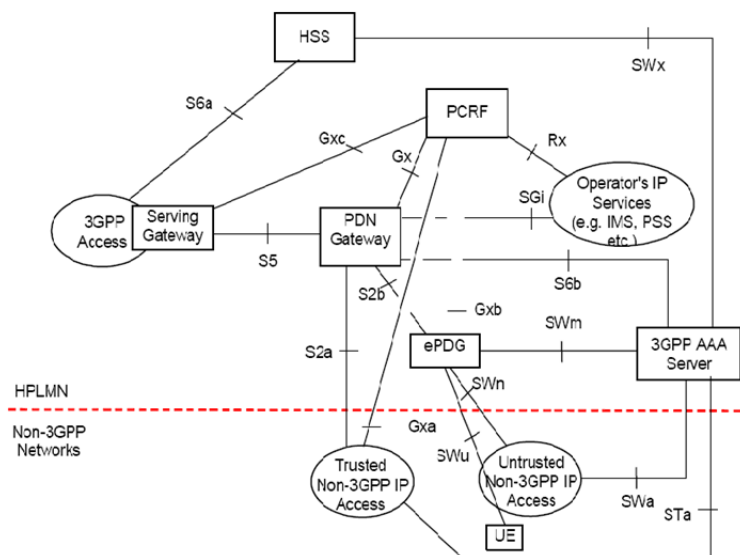


Figure 25 Non-Roaming Architecture within EPS using S5, S2a, S2b

4.1.4.1 IPWorks EPC Reference Points

IPWorks 3GPP AAA supports following procedures in STa, SWm, S6b, and SWx interfaces separately as specified in 3GPP TS 29.273. For more information, see Reference [40].



STa reference points

STa connects the Trusted non-3GPP IP Access (such as CDMA2000 Access Network) with the 3GPP AAA Server/Proxy and transports access authentication, authorization, mobility parameters, and charging-related information in a secure manner.

The STa authentication procedure is based on EAP-AKA', which is defined in RFC 5448. The EAP message is transported over Diameter message as specified in RFC 4072.

For STa interface, the following processes are supported:

- Non-3GPP IP Access Network initiated full authentication and authorization
- Non-3GPP IP Access Network initiated Re-Authentication (including Fast Re-Authentication) and Re-Authorization
- Non-3GPP IP Access Network initiated Re-Authorization
- Non-3GPP IP Access Network initiated session termination
- 3GPP AAA initiated session termination
- 3GPP AAA initiated Re-Authorization

SWm reference points

SWm is the reference point located between 3GPP AAA Server/Proxy and ePDG, and is used for transport of mobility parameters, authentication, and authorization data when user is attached EPC through Untrusted non-3GPP IP Access network.

The SWm authentication procedure is based on EAP-AKA, which is defined in RFC 4187. The EAP message is transported over Diameter message as specified in RFC 4072.

For SWm interface, the following processes are supported:

- Full authentication and authorization procedure
- Re-Authentication (including Fast Re-Authentication) and Re-Authorization procedure
- Re-authorization procedure
- ePDG initiated session termination
- 3GPP AAA initiated session termination
- 3GPP AAA initiated Re-Authorization

S6b reference points

S6b is the reference point between PDN GW and 3GPP AAA server for mobility-related authentication if needed. The PDN GW can use this interface to deal the authorization and update the PDN GW information into HSS. This reference point might also be used to retrieve static QoS profile for a UE for non-3GPP access in case dynamic PCC is not supported.

For S6b interface, the following procedures are supported:

- PDN GW initiated authorization procedure
- PDN GW initiated session termination procedure
- 3GPP AAA initiated Re-Authorization

SWx reference points

SWx reference point is located between 3GPP AAA Server and HSS and is used for transport of authentication vectors and user profiles from HSS, register, and deregister user into HSS and also update the PDN GW information into HSS.

For SWx interface, the following procedures are supported:

- Authentication procedure
- Download user profile procedure
- UE Registration and deregistration procedure
- Update the HSS with PDN GW information procedure
- Error notification to HSS
- HSS initiated user De-registration
- HSS initiated update of user profile

Reference point between 3GPP AAA Server or 3GPP AAA Proxy and EIR

- The reference point between the 3GPP AAA Server or 3GPP AAA Proxy and the EIR is used to check the mobile equipment's identity status (for example to check that it has not been stolen, or, to verify that it does not have faults).
- For the reference point interface, the following procedure is supported:
 - ME Identity Check procedure

4.1.5 3GPP UDC Reference Model

The 3GPP UDC reference model is based on the 3GPP specifications. The following figure shows the User Data Convergence (UDC) architecture and its interfaces. It includes the most relevant entities and interfaces in the 3GPP standard. For more information about the UDC, see Reference [41] and Reference [42].



IPWorks ENUM-FE and AAA-FE play the role of Application Front-end in the UDC architecture.

Figure 26 shows the 3GPP UDC reference architecture:

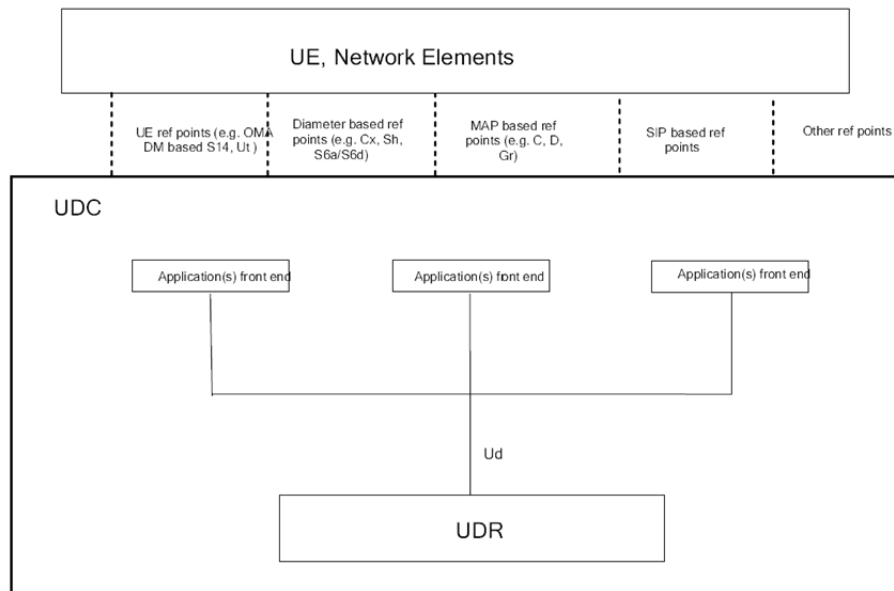


Figure 26 3GPP UDC Reference Architecture

4.1.5.1 IPWorks UDC Reference Points

The ENUM-FE and AAA-FE implement the 3GPP Ud interface to the BE-DB (for more details, see Reference [42]) based on LDAP protocol to read the user data in the BE-DB.

4.2 Protocols

4.2.1 Protocols Supported on Traffic Interfaces

IPWorks has the following protocols supported on **traffic interfaces**:

- AIN

IPWorks uses the Advanced Intelligent Network (AIN) Protocol to communicate with the SCF nodes to perform Local Number Portability (LNP) and Toll-free Queries requesting the Number Portability information.

- MAP

The Mobile Application Part (MAP) protocol can be used between IPWorks and Mobile Number Portability Signaling Relay Function (MNP SRF) node for Mobile Number Portability (MNP) information retrieval.



IPWorks supports MAP over SS7 SIGTRAN transport layer.

— INAP

The Intelligent Network Application Protocol (INAP) is used between IPWorks and Service Control Function (SCF) node for Number Portability (NP) information retrieval.

The InitialDP operation in Intelligent Network Capability Set 1 (CS1) is used by IPWorks to interrogate the SCF to retrieve portability information for a subscriber number. One of the INAP messages, Connect, Continue, Release, or certain InitialDP negative response message is replied from SCF.

— DNS

The Domain Name System (DNS) provides the information for mapping internet hostnames to IP addresses and conversely, mails routing information, and other data used by internet applications, IPWorks DNS is used for IMS, GPRS, and general IP Networks.

— Diameter

IPWorks supports the Standard Diameter protocol as specified in RFC 6733 for EPC AAA.

Diameter is an extensible base protocol, to provide Authentication, Authorization, and Accounting services. Diameter protocol is transported over SCTP or TCP where multiple TCP connections might be optionally used.

— RADIUS

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized access Authentication, Authorization, and Accounting management for people or computers to connect and use a network service. For IPWorks, it is used for Authentication, Authorization, and Accounting relevant to PDN and WLAN accesses.

— DHCP

The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks. DHCPv4 is now supported by IPWorks.

— LDAP

The Lightweight Directory Access Protocol (LDAP) is supported on IPWorks AAA Front End and ERH. IPWorks AAA Front End in DLA uses LDAP protocol to read the user data in the back-end database (BE-DB), and ERH use LDAP protocol to read Number Portability data in the external LDAP NPDB.



4.2.2 Protocols Used for OAM

The following protocols are used for **OAM**:

- SSH (CLI)

Secure Shell (SSH) is a network protocol that allows data to be exchanged using a secure channel between two networked devices, IPWorks SC VMs communicate with the administrative terminals through CLI command, and the CLI connection is protected by using SSH over TCP port 22.

- FTP/SFTP

The Secure File Transport Protocol (Secure FTP) and FTP allows transfer of files to and from the IPWorks. IPWorks enables SNMP Manager (OSS) to fetch its performance management (PM) statistics data in XML files over FTP or SFTP.

- SNMP

The Simple Network Management Protocol (SNMP) allows management information for a network element to be inspected or altered by logical remote users. The IPWorks supports SNMPv2 and SNMPv3 for fault management and performance management.

- NETCONF

NETCONF is an XML-based protocol that defines operations for accessing and updating a configuration data store. IPWorks NBI includes NETCONF interface for Machine to Machine configuration.





5 Operation, Administration and Maintenance

5.1 Provisioning Management

IPWorks DNS, ENUM, DHCP, and AAA server provisioning is realized by the IPWorks Command-Line Interface (IPWorks CLI) which is implemented inside SC-VM.

IPWorks DNS GUI is also used for IPWorks DNS sever provisioning.

For the provisioning for IPWorks DNS, ENUM, DHCP and AAA service, the provisioning data includes user data and service policy configuration for each service.

- DNS data is provisioned using IPWorks CLI or DNS GUI. For more information, refer to [IPWorks DNS, ASDNS, ENUM Parameter Description](#).
- DHCP data is provisioned through IPWorks CLI, the DHCP data includes DHCPv4 objects configurations (DHCP Policy objects configuration, DHCPv4AuthKey configuration, DHCPv4 options configuration, option 82 configuration, and so on). For more information, refer to [IPWorks DHCP Parameter Description](#).
- ENUM data is provisioned through IPWorks CLI, then ENUM data includes EnumACL, EnumZone, EnumDnRange, EnumDnsched, and so on. For ENUM layered deployment, ENUM data (only EnumDnShced and EnumDnRange) is provisioned to CUDB through LDAP interface by EDA/PG. For more information, refer to [IPWorks DNS, ASDNS, ENUM Parameter Description](#).
- AAA data is provisioned through IPWorks CLI. The provisioning data includes AAA user data and AAA service policy. For AAA layered architecture, AAA user data is provisioned to CUDB through LDAP interface by EDA/PG. For more information, refer to [IPWorks AAA Parameter Description](#).

IPWorks CLI is used to interrogate and configure different components of IPWorks, such as importing and exporting data; adding, deleting, or modifying objects; or updating servers. The CLI provides simple but powerful commands that are entered at a shell prompt. The CLI runs interactively or in batch mode.

For more information about IPWorks CLI, refer to [Command Line Interface User Guide for IPWorks SS](#).

5.2 Configuration Management

IPWorks Configuration Management (CM) is a set of management functions that allows the user to manage and control the configuration of IPWorks applications. The Managed Element (ME) provides a machine-machine interface



based on the IETF NETCONF standard, the Ericsson NETCONF interface, and a human-machine user interface, the Ericsson Command-Line Interface (ECLI).

Both interfaces are model-driven, which means that the configuration data of the ME is represented as a set of Managed Objects (MOs). The complete set of MOs and their relationships are described in a Managed Object Model (MOM). The MOM is exposed through the Ericsson NETCONF interface and the ECLI, and provides a consistent view of the configuration and state data.

Check [IPWorks Configuration Management](#) for IPWorks configuration details. Check [Managed Object Model \(MOM\)](#) for all supported configuration parameters.

IPWorks uses MySQL database for data storage, and MySQL CLI is used for such configurations. Refer to [Configure MySQL NDB Cluster](#) for detail configurations on MySQL NDB Cluster.

If ENUM Number Portability functionality requires NPDB query through SS7 signaling, the “Signaling Manager” is used to configure SS7 link. Refer to [Configure SS7 for ENUM Number Portability and Signaling Manager User Guide](#) for details.

5.3 Backup & Restore

The IPWorks virtualized supports Backup and Restore procedures for the VMs through the CBA service component of Backup and Restore Framework (BRF).

Two types of backup are supported:

- A “System Data Backup” contains the entire software and configuration
- A “User Data Backup” contains all the user data such as IPWorks configuration or configuration and provisioning data both.

Backups can be exported to and imported from an external storage system through SFTP.

For more information, refer to [Backup and Restore](#).

5.4 License Management

IPWorks implements CBA component of License Management (LM) for licensing service. Besides, IPWorks follows the license format defined in Ericsson License Manager (ELIM) License Key File (LKF).

When the License Manager is first installed, it automatically enters Integration Unlock mode. While operating in Integration Unlock mode, License Manager is able to function with and without access to licenses. This mode can allow operators to use the system without license keys for maximum 60 days.



The license manager components are deployed on SC VMs with redundancy, while the license clients are distributed in all PL VMs. In this way, a “cluster locking” on licenses is achieved.

All IPWorks license keys are ordered from the Ericsson software supply organization. Each license is identified by a license name and version number. License keys are contained in a license key file. Each license key file is customer-specific and fingerprinting is used to lock the key file.

IPWorks operates using soft license handling, enabling the continuous operation serving the traffic even when the license limit is superseded. Consequently, the emergency unlock capability are not applicable for IPWorks system.

Check details in [License Management](#) and relevant OPIs.

5.5 Fault Management

CBA component Core MW provides fault management functions for IPWorks.

IPWorks supports SNMP traps that capture alarms and events. These can be sent to SNMP-based network monitoring stations as notifications for procession and further action.

For more information, refer to [Fault Management](#) and [IPWorks Alarm List](#).

5.6 Performance Management

CBA component Core MW provides performance management, in which the performance report is created with defined collection of data, at defined time intervals, during a specified period. The files created are collected by the management system, using SFTP.

For more information, refer to [Performance Management](#), [IPWorks Performance Measurements](#), and [IPWorks Measurement List](#).

5.7 Security Management

Files residing in IPWorks are protected by UNIX file permissions, which are restrictive.

5.7.1 Authentication and Encryption

IPWorks user authentication supports both remote and local authentication method on the interface of NETCONF, ECLI and SFTP over SSH. For more information, refer to [IPWorks Authentication User Guide](#).



OAM (provisioning and configuration management activities) and traffic interfaces are possible by the following secure interfaces:

- In general, all socket-based communication between IPWorks components is based on IPSec.
- The Command-Line Interface (CLI) is protected by SSH
- DNS messages can be either protected by IPSec or TSIG-based DNSSec
- SNMPv3 is used for OSS/NMS monitoring functions
- Password is encrypted

5.7.2 Security Logs

Security audit logging involves recognizing, recording, and storing the information of security events. In IPWorks, this means providing a log of all critical security events for the IPWorks components (DNS, ASDNS Monitor, ENUM). Separate security audit log files are maintained for each IPWorks component apart from the general log files.

For more information, refer to [IPWorks Security Management](#).

5.7.3 IP Filtering

IPWorks supports the IP packet filtering on any network interface implementing IP, which is able to filter the IP packets according to the value of specific fields of the protocol (such as IP, TCP, UDP, ICMP) headers for both incoming and outgoing traffics. When the filter rule is matched, it applies permit, reject, or drop actions.

The actions of IP filtering are possible to be logged into the syslog, and it contains the information such as time-stamp, permit/reject/drop status, source/destination address and port, network element information and so on.

IPWorks IP filtering can apply on both IPv4 and IPv6 packet.

5.8 Health Check

IPWorks provides a facility to execute automated health checks on the node. The automated procedure generates reports based on key aspects of IPWorks configuration, settings, and values. The information is output in user-friendly reports which make the manual analysis quick and easy.

The automated health check takes a short time to execute. It can be performed on daily basis, or before or after an upgrade.



5.9 Trace

For Diameter and Radius AAA, IPWorks can provide the capability to trace user authentication, authorization, and accounting transaction encompassing related protocol messages that traverse IPWorks AAA.

With the trace feature, the operator can define traced user list and trace profiles for fault finding and localization of potential issues.

This feature can be used for troubleshooting, interoperability testing, and so on, with the benefit of improved Total Cost of Ownership (TCO).

It is also possible with commands to, in real time, print the user data that is handled in the AAA for the traced user (Username or IMSI).

The trace output files can be transferred to Network Management System for offline processing.





6 Redundancy

6.1 Traffic Redundancy

In IPWorks, local traffic redundancy is supported by PL VMs running in an N-Way active mode.

VIP is configured for the IPWorks DNS/ENUM/AAA service, the service shall be taken over by active servers for one server failure.

IPWorks system can be deployed at different sites for traffic geo-redundancy.

6.1.1 DNS/ENUM

For DNS/ENUM service, traffic redundancy is provided by N-Way active mode. Both active servers are able to provide network service. DNS/ENUM client preconfigures at least two server addresses: primary and secondary. If the primary server is unreachable, the client forwards the request to alternative server.

VIP is configured for DNS/ENUM service, two or more DNS/ENUM servers work as one cluster, if one server is unreachable, the service can be taken over by other active servers.

Figure 27 illustrates the local redundancy solution for DNS/ENUM:

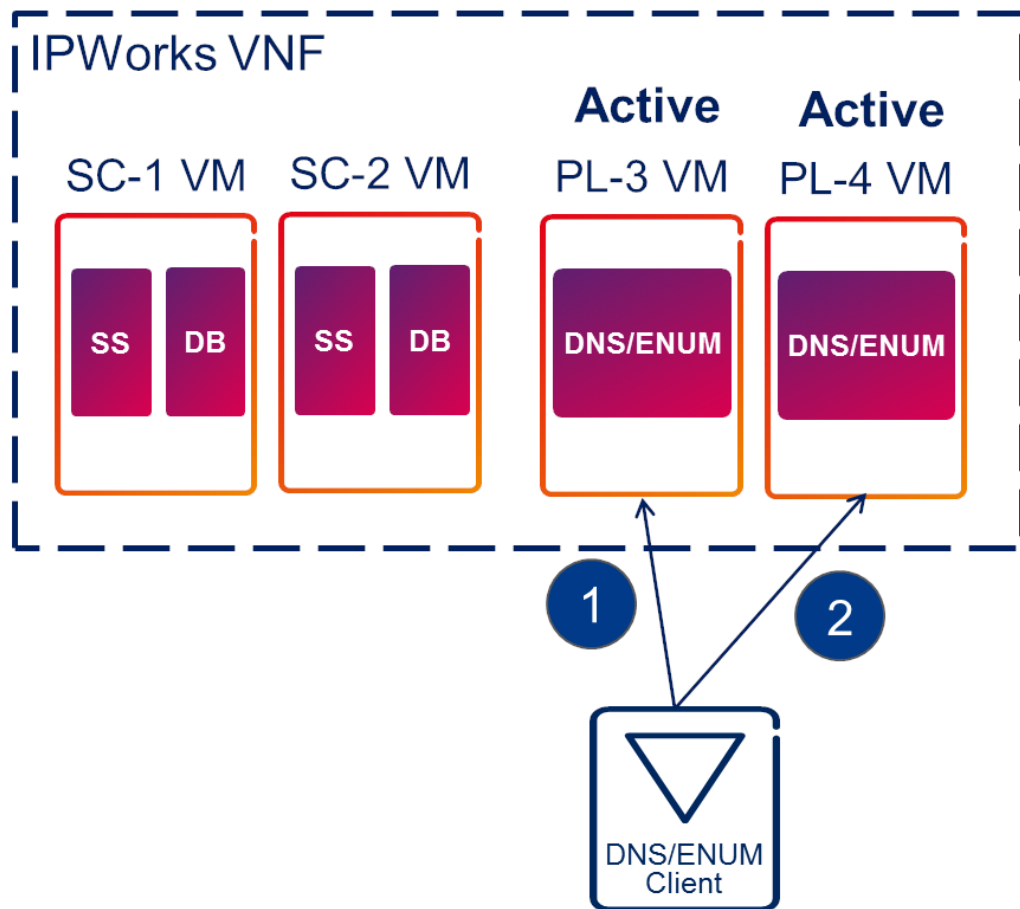


Figure 27 Local Redundancy Solution for DNS/ENUM

In ENUM-FE function, the ENUM-FE sync model which preserves ENUM data from CUDB, is working as active/stand-by mode.

For traffic geo-redundancy, two IPWorks DNS/ENUM systems can be deployed in two sites to support traffic geo-redundancy. For more information, refer to IPWorks Geographic Redundancy.

6.1.2

AAA

For AAA service, traffic redundancy is provided by N-Way active mode. Both active servers are able to provide network service. AAA client preconfigures at least two servers: primary and secondary. If the primary server is unreachable, the AAA client forwards the request to alternative server.

VIP is configured for AAA service, two or more AAA servers work as one cluster, if one server is unreachable, the service can be taken over by other active servers.

Figure 28 illustrates the AAA local redundancy solution:

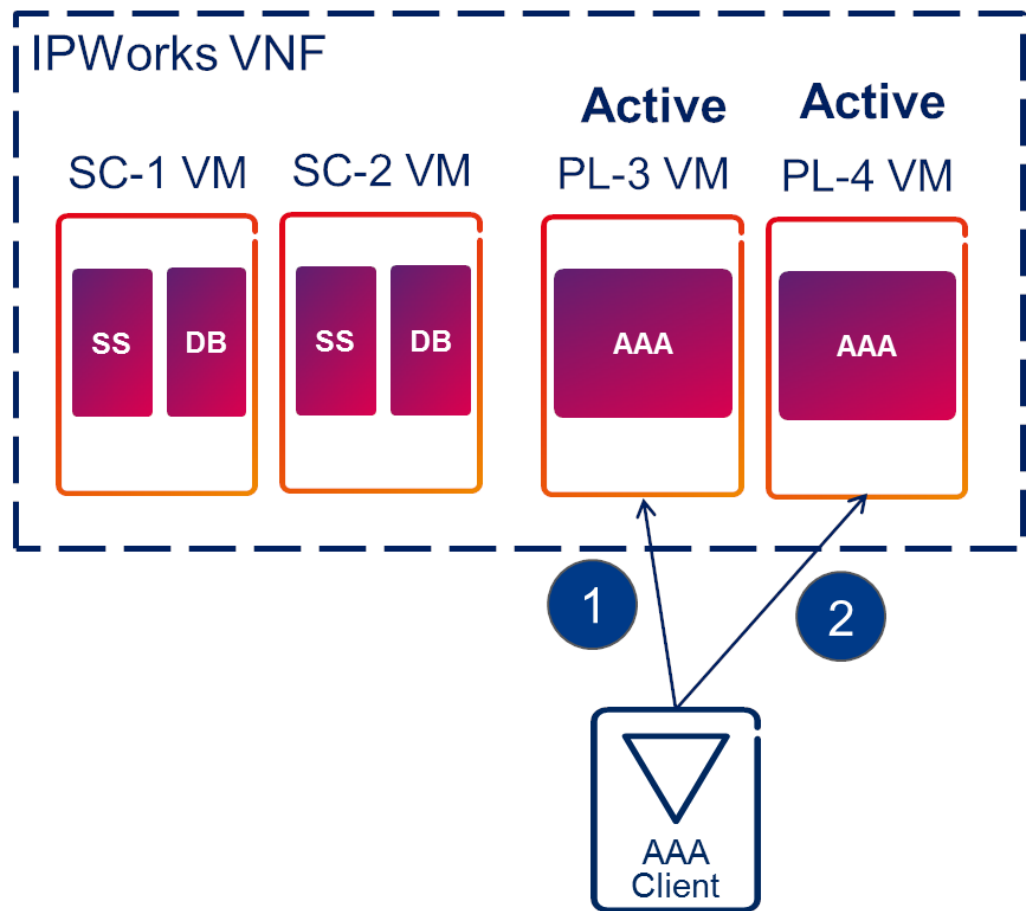


Figure 28 Redundancy Solution for AAA

For traffic geo-redundancy, two IPWorks AAA systems can be deployed in two sites to support traffic geo-redundancy. For more information, refer to *IPWorks Geographic Redundancy*.

6.1.3

DHCPv4

For DHCP service, DHCPv4 traffic redundancy is provided by active/active mode. DHCP differs from the mode of DNS/ENUM and AAA, it does not require its client to actively select DHCP server. DHCPv4 server and client follow DHCP failover protocol to select "alive" server to continue the IP lease management.

For more information about DHCP failover protocol, refer to *draft-ietf-dhc-failover-12.txt*.

Figure 29 illustrates the redundancy solution for DHCP:

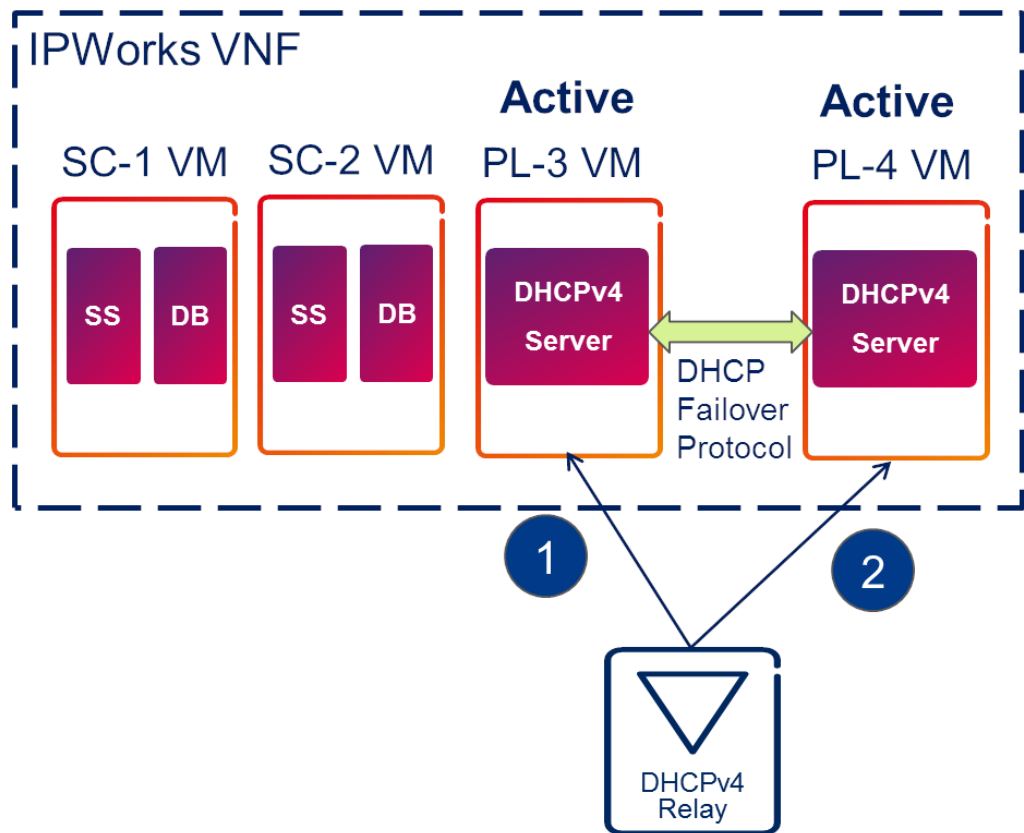


Figure 29 Redundancy solution for DHCP

For traffic geo-redundancy, two IPWorks DHCP systems can be deployed in two sites to support traffic redundancy and load-balancing between two DHCP servers located in two geographic separated sites. For more information, refer to [IPWorks Geographic Redundancy](#).

6.2 Provisioning Redundancy

In IPWorks 2, SS application in two SC VMs that is responsible for IPWorks provisioning is working in active/standby mode. When SS application in one SC VM is unreachable, the SS application in the other SC VM takes the provisioning traffic to maintain high availability upon SS application failure or VM failure.

Whereas, Geographic Redundancy on provisioning solution allows the deployment of IPWorks nodes with geographical redundancy to ensure that the IPWorks system can still function normally in case of one node or site failure because of disasters or some other reasons. In this case, one solution is using EDA dual provisioning. EDA performs the double provisioning to the IPWorks systems in two separated sites, so to guarantee the identical user data in two geographic separated sites.



For ENUM or AAA geographic redundancy, another solution is provisioning data replication between two geographic separated sites. For more information, refer to [IPWorks Geographic Redundancy](#).

For DHCP redundancy and load-balancing between two servers located in geographic separated sites, IPWorks supports DHCP provisioning data replication between two geographic separated sites. For more information, refer to [IPWorks Geographic Redundancy](#).

6.3 Storage Redundancy

System Control function uses persistent storage while the Payload does not.

Within System Control inside, guest operating system --LDE is the layer that interacts with the disks and configures these into a usable set of partitions for the cluster. The biggest part of the disks is set up in a Distributed Replicated Block Device (DRBD) pair. Because of this, every byte of data in the DRBD partition (`/cluster`) is actually stored two times (one time on each disk) on the two disks of SCs.





Reference List

IPWorks Library Document

- [1] Trademark Information
- [2] Typographic Conventions
- [3] Glossary of Terms and Acronyms
- [4] Command Line Interface User Guide for IPWorks SS
- [5] Ericsson Command-Line Interface User Guide
- [6] Fault Management
- [7] IPWorks Alarm List
- [8] IPWorks Configuration Management
- [9] IPWorks DNS, ASDNS, ENUM Parameter Description
- [10] IPWorks DHCP Parameter Description
- [11] **IPWorks AAA Parameter Description**
- [12] Configure MySQL NDB Cluster
- [13] Configure DNS and ENUM
- [14] IPWorks Geographic Redundancy
- [15] Diameter Stack Configuration Guide
- [16] Configure SS7 for ENUM Number Portability
- [17] Configure SS7 for AAA
- [18] Signaling Manager User Guide
- [19] Performance Management
- [20] IPWorks Performance Measurements
- [21] IPWorks Measurement List
- [22] IPWorks Security Management
- [23] Backup and Restore

- [24] License Management
- [25] IPWorks Manual Health Check
- [26] IPWorks Auto Health Check

PCAT and Other Ericsson Documents

- [27] IPWorks 2 Characteristics, 155 02-FGC 101 3568
- [28] IPWorks Dimensioning Guideline, 1/192 02-FGC 101 3568
- [29] IPWorks Statement of Compliance Overview, 1/174 02-FGC 101 3568

Standards

- [30] [Dynamic Updates in the Domain Name System \(DNS UPDATE\)](#)
- [31] [The E.164 to Uniform Resource Identifiers \(URI\) Dynamic Delegation Discovery System \(DDDS\) Application \(ENUM\)](#)
- [32] [Diameter Base Protocol](#)
- [33] [Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement \(EAP-AKA\)](#)
- [34] [Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement \(EAP-AKA'\)](#)
- [35] [Interworking between the Public Land Mobile Network \(PLMN\)](#)
- [36] [RFC2865, Remote Authentication Dial In User Service \(RADIUS\)](#)
- [37] [RFC2866, RADIUS Accounting](#)
- [38] [3GPP system to Wireless Local Area Network \(WLAN\) interworking](#)
- [39] [Architecture enhancements for non-3GPP accesses](#)
- [40] [Evolved Packet System \(EPS\); 3GPP EPS AAA interfaces](#)
- [41] [User Data Convergence \(UDC\); Technical realization and information flows; Stage 2](#)
- [42] [User Data Convergence \(UDC\); User data repository access protocol over the Ud interface; Stage 3](#)

Other Reference

- [43] DNS and BIND, 4th Edition, Paul Albitz & Cricket Liu, O'Reilly
ISBN, 0-596-00158-4



- [44] The DHCP Handbook, Second Edition, Ralph Droms & Ted Lemon, Sams Publishing.
ISBN, 0-672-32327-3