

IPWorks Security Management

DESCRIPTION

Copyright

© Ericsson AB 2017, 2018. All rights reserved. No part of this document may 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 IPWorks Trademark Information.



Contents

1	Introduction	1
1.1	Prerequisites	1
1.2	Related Information	1
2	Function Survey	3
2.1	IPWorks Security for External Interfaces	3
2.2	List of Sub-functions	6
3	Security on Management and Protocol Interfaces	13
3.1	Security on Management Interfaces	13
3.2	Security on Protocol Interfaces	16
4	Operational Conditions	19
4.1	Configurable Parameters	19
5	Operation and Management	21
5.1	System User Authentication	21
5.2	IPworks Storage Server User Authentication	21
	Reference List	23





1 Introduction

This document describes inherent security features in the IPWorks for interfaces, applications and protocols.

Target Groups

This document is intended for personnel that want to know the security aspects of IPWorks.

1.1 Prerequisites

1.1.1 Documents

Ensure that you read the following documents together with this document:

- For details on the IPWorks product overview, refer to *IPWorks Technical Description*, Reference [6].
- For details on the LDE operating system security hardening, refer to *IPWorks OS Hardening Guide*, Reference [1].
- For details on the security hardening of the IPWorks application components, refer to *IPWorks Application Components Hardening Guide*, Reference [2].

1.2 Related Information

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

- *Trademark Information*, Reference [3]
- *Typographic Conventions*, Reference [4]
- *Glossary of Terms and Acronyms*, Reference [5]





2 Function Survey

This section lists the security features for external interfaces and the sub-functions.

2.1 IPWorks Security for External Interfaces

The detailed description of the inherent security features in IPWorks is given in Section 3.1 on page 13 for the management interfaces and in Section 3.2 on page 15 for the protocol interfaces.

Table 1 and Table 2 list the security features for the management interfaces and protocol interfaces respectively.

Note: Ensure that all the required ports listed in this section must be open.

Table 1 Overview of Security for Management Interfaces

Management Interface	Port	External Interface	Security Feature
CLI	TCP 22 for SSH (SCLI)	From CLI component to administrative user terminal or to other management systems.	SSH (SCLI) supported.
SNMPv3 MIB for alarms Note: IPv4 only.	UDP 162 for traps and alarms	From DNS, DHCPv4, ERH, ENUM, and SS servers to external management systems	SNMPv3 security features (authentication, confidentiality, data integrity protection)
Proprietary protocol (IPWorks API based traffic)	TCP 17071	From IPWorks CLI or IPWorks DNS Management to SS	SSL using Storage Server's certificate and client's user name and password.
ERH and AAA subagent to SS7 stack Operation and Maintenance (OAM)	TCP port 6669	From ERH and AAA subagent to SS7 stack OAM Common Parts manager registration	No inherent security feature



Management Interface	Port	External Interface	Security Feature
Between two SS7 stacks running on two host PSs for redundancy	TCP port 6670	Execution Control Management used for monitoring	No inherent security feature
	TCP port 6671	Execution Control Self used for monitoring	No inherent security feature
	TCP port 8889	Logging daemon	No inherent security feature
Rsyslog	UDP port 514 TCP port 10514	From SS, DNS and ENUM to remote log server	No inherent security feature
OSS	TCP 22 for SSH and SFTP TCP 830 for Netconf, TCP 28080, 28181	From IPWorks to external management systems	No inherent security feature

Table 2 Overview of Security for External Protocol Interfaces

Management Interface	Port	External Interface	Security Feature
DNS	UDP 53, TCP 53. See ⁽¹⁾	From DNS client, or to external DNS server. See ⁽²⁾	
Dynamic DNS (DDNS) Note: IPv4 only	UDP 53, TCP 53. See ⁽¹⁾	From DHCP server, or from external DNS server, to external DNS server. See ⁽²⁾	
ERH & AAA (ERH API)	For example, MAP over SS7, INAP over SS7 or AIN over SIGTRAN (SCTP port 2905)	To external database like HLR, FNR, SCP or other NPDB	No inherent security feature.
DHCPv4	UDP 67 and UDP 68, Failover protocol TCP 647 and 847	To network servers (for example, GGSN, PDSN), failover to an external DHCP server	No inherent security feature.



Management Interface	Port	External Interface	Security Feature
CUDB Port	TCP Port 389	CUDB Port	
SOAP Port	TCP Port 8080	SOAP Port	
NTP Port	TCP Port 123	NTP Port	
Radius authentication/authorization	UDP port 1812	Between AAA server/proxy and AAA client/remote AAA	
Radius accounting	UDP port 1813	Between AAA server and AAA client	
Diameter authentication/authorization	TCP/SCTP port 3868	Between EPC AAA server/proxy and AAA client/remote AAA	
Radius Proxy Listening Ports	Dynamic UDP Ports, see ⁽³⁾	Radius Proxy Listening Ports Used for proxy sockets to send the proxy request message to remote site. There are 255 UDP ports at most and the listening number can be configured via control panel. The port is between 10000~10254.	

(1) The default maximum length for UDP is 512 bytes but the maximum length can be increased (negotiated) using the OPT pseudo RR. If truncation occurs the concerned query will be repeated using TCP, which is used always for zone transfers.

(2) DNS queries/responses updates to a local BIND go always via the ENUM server's parser component (EnumIf). The ENUM server itself (EnumArch component) resolves only ENUM queries on a static ENUM zone while the rest is forwarded to BIND.

(3) For ASDNS to monitor the CPU load, the peer status, ping or SNMP can be used. the port depend on the customer configuration. For Radius proxy server, it sends the received UDP packet to the remote radius server. Use proxy server IP to filter the packet.

2.2 List of Sub-functions

This section describes the sub-functions of IPWorks.

2.2.1 Security of Active Select Monitor

Using standard DNS messages, the monitor reports the status and load of systems at configured IP addresses to DNS servers. The monitor calls an external script and processes the response to determine the status of a system at an IP address. The script may use a simple utility such as Internet- Control Message Protocol (ICMP) ping to determine the availability of a system or can do more complex checks (using SNMP) as desired.

Note: No integrity protection is available for ICMP and SNMPv1 interface. It is highly recommended that SNMPv1 is disabled and replaced with a later version.

2.2.2 Split DNS Architecture

A BIND 9 view allows a single DNS server to present one configuration to one set of clients and another configuration to a different set of clients. This is referred as a logically Split DNS architecture or Split Namespace feature. For details, refer to Reference [10].

Typical split DNS architecture is realized by the Internal Name Servers (iDNSs) and External Name Servers (eDNSs). With this architecture, it means:

- The eDNSs:
 - Handle all queries to and from the external domains.
 - Are located on the demilitarized zone (DMZ) in a firewall/security gateway.
 - Do the resolution for all external queries.
 - Face the same threats as any name servers connected to a public DNS infrastructure like the Internet DNS infrastructure.
- The iDNSs:
 - Hide the domains that are not allowed to be visible to the external network.
 - Resolve only the queries from internal hosts.
 - Forward all requests that they cannot resolve to the eDNSs.
 - Are more secure than if connected directly to external networks, reducing the risk of external attacks and impacts on the node due to external network failures.



In a physically split DNS architecture, it is recommended to place the redundant DNS servers on different sites if possible. But at least on different network segments (subnets), reducing the risk of external attacks and impacts on the node due to external network failures.

Full support of BIND 9 views has been added to both the DNS server and to the Element Management system. Views can be used to support both internal and external DNS servers using a single set of servers, for example, an internal DNS view to certain clients, and an external DNS view to the others.

Note: ENUM Views support the Split Namespace feature with the help of wildcard support, but their behavior is different from DNS views. See section 3.2.4 below.

2.2.3

BIND ACLs

Access Control Lists (ACLs), as specified in BIND 9 Administrator Reference Manual, see Reference [10], are address match lists that can be set up and nicknamed in IPWorks as DNS statements and options, such as allow-notify, allow-query, allow-recursion, blackhole, and allow-transfer.

Using ACLs allows a finer control over who can access a name server, without cluttering up configuration files with huge lists of IP addresses. ACLs have been extended to allow TSIG keys also.

ACLs are used to control access to a server. Limiting access to a server by outside parties can help to prevent spoofing and DoS attacks against the server.

2.2.4

ENUM Access Control

ENUM server provides an access control mechanism that permits or denies ENUM queries based on query source IP addresses.

Every ENUM zone is included at least in one view, which is connected to an associated Access Control List (ACL) containing the IP addresses of the DNS clients authorized to access the view and the included ENUM zone data.

Every view is configured with a rank defining the order where the views are searched for a queried ENUM zone that may be included in several views.

ENUM wildcard function brings the possibility to synthesize a range of telephone numbers with a common resource record (RR) set. Split Namespace here means that different configurations can exist for the same number series (range) in different views. The number series can only be in the views to which the ENUM zone belongs. The view to be used for the number series is configurable. If the zone is in the default view, the number series will fit into the default view.

If no view is configured for an ENUM zone, it will be included in the default view without any access control (no ACL is applied).



2.2.5 TSIG

Transaction SIGNatures (TSIG) are part of transaction security in BIND that primarily supports TSIG for server-to-server communication. TSIG is used to provide data origin authentication and data integrity using a shared secret with the HMAC-MD5 integrity algorithm. The communication includes zone transfer, notify, and recursive query messages. For more information, refer to Reference [10].

The IPWorks DNS server supports TSIG as specified in RFC 2845. This feature uses authentication based on shared secrets and one way hashing to sign DNS queries, transfers, updates, and responses. The dynamically created TSIG resource records are generated and verified by DNS clients and servers to ensure that the data has originated from an authorized party and has not been changed in transit.

TSIG and Access Control List (ACL) strengthen DNS server's operations and the service. Usage of ACLs and TSIG is recommended to prevent unauthorized transactions, thereby providing additional security. DNS ACLs are used to allow DNS transactions (like queries and zone transfers) only from certain hosts (co-operating DNS servers and DNS clients). The zone transfers, queries and responses can be transferred confidentially (using shared secrets) under this protection, if the number of involved entities is rather small.

IPWorks DHCP servers support TSIG for dynamic updates. With combination of an ACL and optional TSIG keys, administrators can control which DHCP servers can update DNS servers, thus avoiding invasive updates from rogue servers.

TSIG is not supported by the ENUM server.

2.2.6 Node Hardening

LDE operating system hardening process is performed according to *IPWorks OS Hardening Guide*, Reference [1].

Security hardening for IPWorks application components DNS, DHCP, ENUM, SS, AAA and MySQL database, is performed according to *IPWorks Application Components Hardening Guide*, Reference [2].

When hardening the nodes, the ports and protocols need to be identified. Vulnerability analysis must be performed, and the identified vulnerabilities need to be documented. If applicable, corrective measures must be taken.

2.2.7 Security Audit Logging and Fault Management

IPWorks use Rsyslog to collect security logs, refer to <http://www.rsyslog.com/>.

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, ENUM and SS).



One unified security audit log file is used for all IPWorks components. Tool `ipwsyslog` is introduced to filter security audit log messages. For more detail of log message, refer to *IPWorks Security Log Management Guide*.

2.2.7.1 Start-up the Audit Functions

Start-up the audit functions is logged to the security audit log file for each component of IPWorks. Refer to *IPWorks Security Log Management Guide*.

2.2.7.2 Systematic Checks for Open Services

The open services that are relevant to IPWorks components, are monitored. If any new service is opened, it will be logged to the security audit log file of associated IPWorks components.

2.2.7.3 Security Audit Logging Specific to DNS

The DNS security audit log file provides the administrator with information about Denial of Service (DoS) attacks, approval or denial of requests and any logged alarms or notifications.

The following events are logged for DNS:

- Start-up, Shutdown and Reload of DNS servers
- Alarms if wrong message format queries exceed the limit defined by the administrator in a given granularity period
- Approval or denial of requests due to an ACL
- TSIG key validity failures
- Modification to site info or preference list for ASDNS. At Start-up the list of all the resources configured for DNS is logged to the security audit log file of DNS. After a reload the administrator can compare the old and new resource lists in the security audit log to see if there are any changes.

If the error rate of query failures exceeds the threshold value in a given granularity period, an alarm will be raised and an entry will be logged to the security audit log file.

2.2.7.4 Security Audit Logging Specific to ENUM

The security audit log file specific to ENUM provides the administrator with specific information about ENUM related events including each non-authenticated query attempt due to an ACL.



2.2.7.5 Security Audit Logging Specific to Storage Server

Security audit logging involves recognizing, recording and storing the information of security events. The resulting audit records can be examined to determine which events took place and who is responsible for them. All the security events related to IPWorks OAM are logged in by Rsyslog.

The security events that are logged include the following:

- Any authentication and login attempt and its result
- Five consecutive unsuccessful login attempts during a single session
- Each logout or session termination (whether remote or console)
- Modification to Access controls
- Failures of communications, and operations
- Information of Account Locking and Unlocking

2.2.8 IP Filtering

IP filtering software is included in the Linux OS in the iptables software by netfilter.org.

Iptables is a generic table structure for the definition of rulesets. Each rule within an IP table consists of a number of classifiers (iptables matches) and one connected action (iptables target).

The iptables packet filtering framework enables basic packet filtering (IPv4), stateful packet filtering (IPv4) and network address (and port) translation (NAT/NAPT, only for IPv4).

Ip6tables is the corresponding software for IPv6 filtering.

For more information, refer to *IPWorks IPTables Service Configuration*.

2.2.9 NDB Cluster

It provides nearly linear scalability the NDB cluster, Cluster SQL Node and Cluster Management Node are collocated with the SS Server in the Control Server (SC) machine.

The transport protocol ports used at the servers for any communication are configurable.



2.2.10

AAA

IPWorks AAA server realizes authentication and authorization function to handle user requests for access to network resources. Authentication identifies the user. Authorization implements policies that determine which resources and services a valid user may access.

The IPWorks AAA server is based on the Remote Authentication Dial In User Service (RADIUS). Radius is a security protocol for carrying authentication, authorization and configuration information between a Network Access Server (NAS) and a shared Authentication Server. For more detailed information on the Radius protocol see RFC 2865, RFC 2866 and RFC 5176.

Diameter is an authentication, authorization and accounting protocol like RADIUS. As a successor to RADIUS, it extends the base protocol by adding new commands and attributes. Diameter relies on connection oriented protocols (TCP, note that SCTP is not used for Diameter in IPWorks) that are more secure and reliable than the connectionless protocol UDP used by RADIUS. Diameter protocol is specified in IETF RFC 3588. The IPWorks AAA server is responsible for receiving user connection requests, authenticating the user and then returning all configuration information necessary for the client to deliver service to the user.

The IPWorks AAA server is also responsible for receiving accounting requests and returning a response to the client. Transactions between the client/NAS and the AAA server are authenticated through the use of a shared secret, which is never sent over the network. The shared secret is stored in the AAA server in such a way that access to it is as limited as possible. Additionally, any user passwords are sent encrypted between the client and Radius server, and the user passwords are stored in the MySQL database in a secure way together with other user information.

The 3GPP AAA server, which is defined in 3GPP TS 29.273, is used to authenticate the UE from non-3GPP IP access network. IPWorks EPC AAA is an implementation of 3GPP AAA, and it also provides support for mobility between non-3GPP and LTE access. Diameter protocol is supported for this.

The IPWorks AAA-FE runs on the SUSE Linux Enterprise Server (SLES). Harden OS first and then harden the application components.

2.2.11

SNMP

IPWorks SNMP applications support SNMPv1, SNMPv2c and SNMPv3 versions but only the last one (v3) includes reasonable security mechanisms while the first two rely on using clear text Community Strings for access control.

SNMPv3 provides a User-Based security Model (USM) and a View-based Access Control Model (VACM) employing DES and AES encryption and MD5 message authentication. It is strongly recommended that only SNMPv3 is used.



2.2.12 Redundancy

For more information on redundancy in the IPWorks, refer to the section *Redundancy and Scalability in IPWorks Technical Description*.



3 Security on Management and Protocol Interfaces

This section describes the security features for the management and protocol interfaces in detail.

3.1 Security on Management Interfaces

The communication between the management interface components and the IPWorks SS can be configured to use authentication and encryption. The specific security protocol used for IPWorks management interfaces depends on the IPWorks component as shown in Figure 1.

The third party products, like OpenSSL, are either integrated with the IPWorks or installed together with IPWorks installation. IPWorks supports SNMPv3 for IPv4.

ERH API is implemented in the ENUM server which is used for External Resolution Handler (ERH). The ERH interacts with the external SS7 databases to get Number Portability (NP) information.

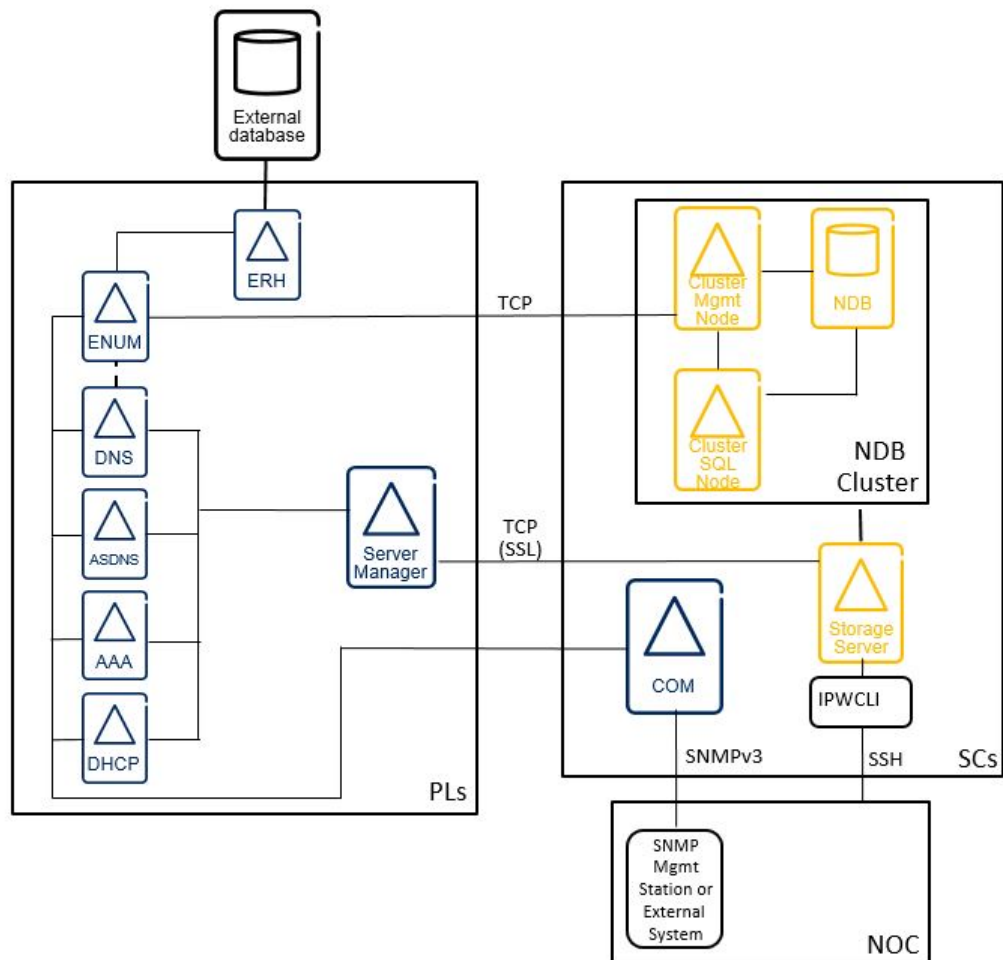


Figure 1 IPWorks Management Interfaces



Note: Depending on the deployed configuration, some of the external connections presented in Figure 1 turn to machine internal connections.

Figure 1 represents the management interfaces of IPWorks internal/external components .

- The sockets used in IPWorks Element Management are all TCP Sockets except for the SNMP which uses UDP Sockets.
- The Storage Server communicates with the user interface components CLI and the Server Managers using the default port 17071 over a proprietary protocol supported by the IPWorks API. The port number is configurable. The communication with the Storage Server can be configured to use SSL for authentication and encryption.
- The interface between the Server Managers and the Storage Server can be protected by SSL.
- The DNS Server, ActiveSelect DNS Monitor, DHCPv4 Server, ENUM Server and AAA Server communicate with the SS using the internal interface through the Server Managers.
- The connections from NOC to IPWorks can be confidentiality and integrity protected by SSH on the TCP port 22.
- BIND 9 provides the rndc tool for stopping, starting and reloading the named daemon. The rndc tool and the DNS server communicate over TCP port 953. The named daemon is administered locally or remotely, with command line statements. The rndc program uses the `/etc/rndc.conf` file for its configuration options, which can be overridden with command line options.

In order to prevent unauthorized users in other systems from controlling BIND on a server, a shared secret key method is used to explicitly grant privileges to particular hosts. In order for rndc to issue commands to any named, even on a local machine, the keys used in `/etc/named.conf` and `/etc/rndc.conf` must match.

- SNMPv3 uses UDP port 162 for traps/alarms.
- IPWorks has a specified interface for O&M. In IPWorks, the regular DNS server has no external interface which uses the conventional UDP and TCP ports 53. Instead, these ports are connected to the ENUM server, which forwards all the regular DNS queries to BIND using the port 5300 on the loop-back address. A dedicated physical interface exists for DHCP traffic (UDP port 67 and 68 DHCP v4) towards the protocol servers. ActiveSelect DNS Monitor and ActiveSelect NAT-PT Monitor may also use SNMP for checking the status of IP addresses, in addition to the ICMP ping..



3.2 Security on Protocol Interfaces

The DNS protocol uses port 53 for communication between DNS resolvers and servers, servers (for zone transfers), and ActiveSelect DNS monitors and servers.

The DHCP (IETF RFC 1541) is an extension to BOOTP (IETF RFC 1542), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

The DHCPv4 protocol uses UDP ports 67 and 68.

The DHCPv4 Failover protocol uses TCP ports 647 and 847, by default. The DHCP Failover protocol is required between two DHCPv4 servers to enable a redundant DHCP service.

Note: When only DNS server is used, both TCP and UDP 53 are connected to DNS server.

When both DNS server and ENUM server are used, TCP 53 and UDP 5300 are connected to DNS server, UDP 53 is connected to ENUM server.

UDP is primarily used, but the default maximum length of a DNS query or response is 512 bytes. A longer length can be negotiated by using the OPT pseudo RR DNS extension. If the response is truncated, the client may repeat the query using TCP. TCP is also used for zone transfers between servers. Diagnostic tools such as nslookup are also resolvers. See Figure 2.

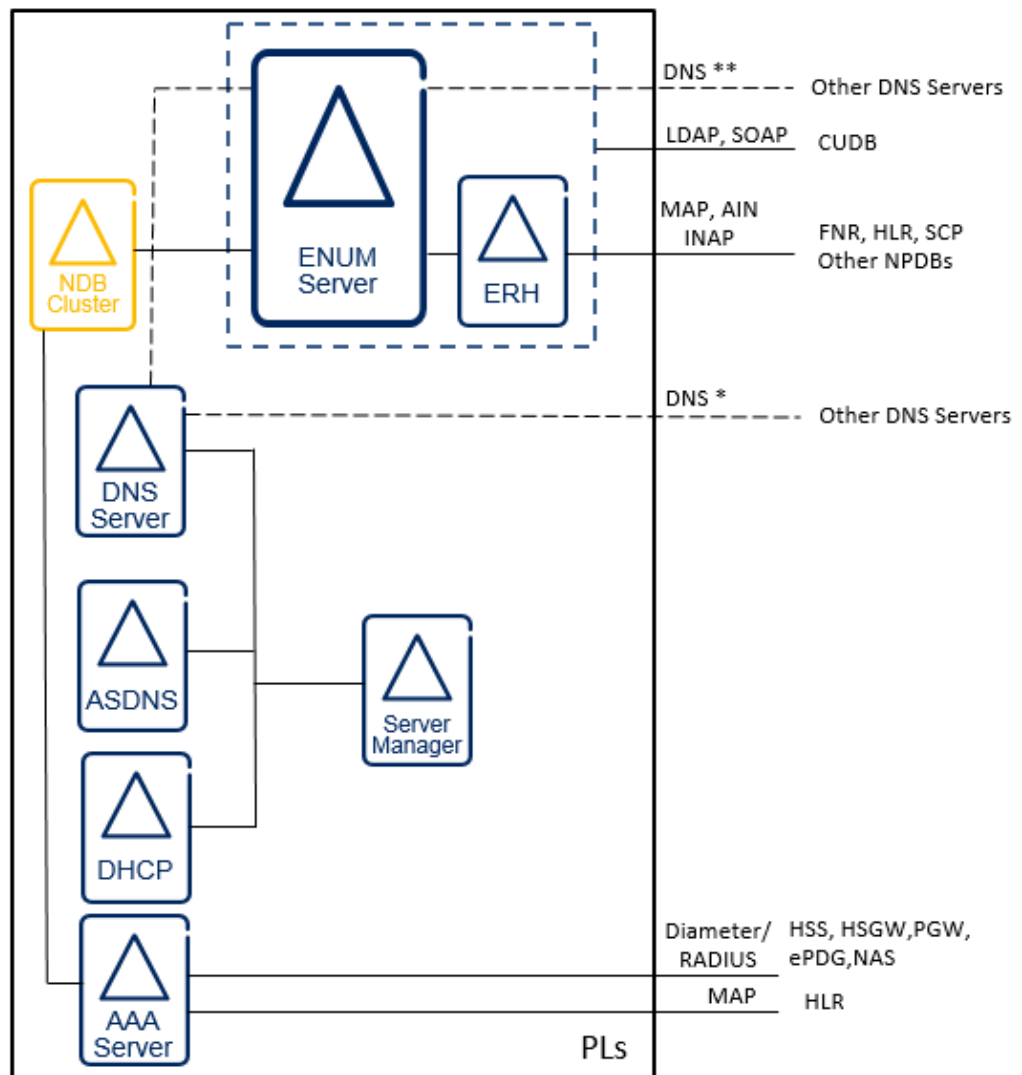


Figure 2 IPWorks Protocol Interfaces

Typically, DHCP traffic does not cross firewall boundaries. A DHCP relay is typically used to relay DHCP broadcast traffic across networks between the client and server. DHCP Relay Agent Information Option (RFC 3016) function can be used to give additional protection against: IP spoofing, client identifier spoofing, MAC address spoofing and DHCP address exhaustion.

The ENUM interfaces with the external CUDb using LDAP and SOAP.

The ERH interacts with the external SS7 databases like HLR, FNR, SCP or other NPDB to get number portability (NP) information. The connection to external SS7 databases is established using SIGTRAN. The ERH interacts with the external NP databases using AIN, MAP or INAP protocol according to the predefined number series rule and return the NP information to the ENUM via the ERH API.



IPWorks AAA server uses RADIUS protocol with listening port 1812 for authentication/authorization and listening port 1813 for accounting.

IPWorks AAA server uses Diameter protocol with listening port 3868 for authentication/authorization.



4 Operational Conditions

This section describes the configurable parameters and OAM.

4.1 Configurable Parameters

The security relies on DNS ACLs and several other configurable parameters. These parameters can be used to configure for IP filtering, SSL, SSH and SNMPv3.





5 Operation and Management

This section gives an overview of the OAM of access control.

Only authorized users are permitted to login and do O&M operations. Access and configuration management activities are limited and controlled by the security functionality of the IPWorks.

5.1 System User Authentication

The operator can manage the IPWorks user authentication. For more detail, refer to *IPWorks Authentication User Guide*.

5.2 IPworks Storage Server User Authentication

The IPWorks Storage Server has own user authentication and password policy includes the following functions:

- The user is forced to change the password on the first login after the account has been established.
- The user is forced to change the password on the first login after the password has been reset.
- The user is forced to select a strong password.
- The user is forced to change the passwords at predefined intervals.
- The passwords are stored encrypted.
- It is possible to configure the number of failed login attempts a user can perform before the account is locked, and also the interval for changing the passwords.

An inactivity timer for login sessions is supported. It is possible to configure the inactivity timer for management sessions.





Reference List

Ericsson Documents

- [1] *IPWorks OS Hardening Guide*
- [2] *IPWorks Application Components Hardening Guide*
- [3] *Trademark Information*
- [4] *Typographic Conventions*
- [5] *Glossary of Terms and Acronyms*
- [6] *IPWorks Technical Description*
- [7] *IPWorks IPTables Service Configuration*
- [8] *IPWorks Security Log Management Guide*
- [9] *Security Management for ECLI, NETCONF, and SFTP Users*

Other Reference

- [10] [BIND 9 Administrator Reference Manual](#)