

IPWorks CLF NACF a2 Interface

INTERWORK DESCRIPTION

Copyright

© Ericsson AB 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 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	Interface Overview	3
2.1	CLF Failure	3
2.2	NACF Failure	3
2.3	Interface Role	3
2.4	Services	3
2.5	Encapsulation and Addressing	4
3	Communication Model	5
3.1	Synchronous and Asynchronous Modes	5
3.2	PUSH and PULL Modes	6
4	Use Cases	7
4.1	Successful Attach Push Model - Synchronous Mode	7
4.2	Successful Attach Push Model - Asynchronous Mode	8
4.3	Successful Detach Push Model	8
4.4	Successful SIP Register Pull Model	8
4.5	Unsuccessful Attach Push Model	9
4.6	Unsuccessful Detach Push Model	9
4.7	Unsuccessful Pull Model	9
4.8	No Response During Network Attachment Push Model - Synchronous Mode	9
5	Protocol Description	11
5.1	Transport	11
5.2	Message Structure	11
5.3	Primitive Definition	13
5.4	Data Type Definition	20
5.5	Primitive Timer Values	24
6	Communication (Control Mechanism)	25
6.1	Normal State	25
6.2	Control Mechanism	25



6.3	Communication Failure	25
6.4	CLF Failure	26
6.5	NACF Failure	27
7	Security	29
8	Formal Syntax	31
9	Related Standards	33
	Reference List	35



1 Introduction

This document outlines the protocol used between the Connectivity session Location and repository Function (CLF) and the Network Access Configuration Function (NACF). The purpose of the CLF-NACF interface is to exchange the IP address allocated to the Customer Premises Equipment (CPE) and the network location information provided by the NACF.

Scope

It is the IPWorks that offers this interface.

This document covers the following topics:

- Interface Overview
- Interface Role
- Services
- Procedures
- Information Model
- Related Standards

Target Group

This document is intended for operators of the CLF Interface.

1.1 Prerequisites

Not Applicable.

1.2 Related Information

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

- Trademark Information, Reference [1]
- Glossary of Terms and Acronyms, Reference [2]
- Typographic Conventions, Reference [3]





2 Interface Overview

The CLF-NACF interface is used to push the IP context from the NACF toward the CLF. This interface is labeled “a2” in the TISPAN literature and is based on a RADIUS-like proprietary protocol. The NACF is the client while the CLF is the server. The protocol supports an application level heartbeat whose task is to monitor the wellbeing of the CLF application as the transport layer is monitored by the cluster-ware.

2.1 CLF Failure

The interface is designed to support application level heartbeat. The client sends a heartbeat toward the server; the server acknowledges the heartbeat message to signal that its application is functioning properly. In the case of a CLF failure, new IP Context/release will not be pushed toward the CLF. Upon resumption of the CLF node (most likely after a transfer), the IP context push resumes. The users impacted by this failure will be granted access to the network and receive an IP address. If a subsequent request from the SBC requires information for a specific IP address, the interface supports the fetching of the IP context from the NACF through the pull primitive. In the case of a communication failure, the cluster software initiates a transfer toward the standby node. This transfer will cause the current connection toward the A-RACF to be terminated and restarted on the secondary node.

2.2 NACF Failure

In the case of NACF failure, the CLF does not receive the new IP Context. As NACF is the source of IP addresses, there is no impact, as a CPE is required to receive an IP address in order to access the network.

Upon node restoration, the NACF resumes pushing new operations toward the CLF.

2.3 Interface Role

This IWD describes NACF offers services to the CLF and CLF uses services by NACF.

2.4 Services

This section describes the services the offers and uses in the a2 interface.

The services offered by the a2 interface are shown in Table 1.



Table 1 Offered Services

Offered Service	Description
IP Access Context Request:<Requesting service><operation><what>	Example: CLF Request Binding Information.

The user services used by the a2 interface are shown in Table 2.

Table 2 Used Services

Used Service	Description
New IP Access Context:<Requesting service><Method><what>	Example: NACF Send Binding Information.
Release IP Access Context:<Requested service><Method><what><operation>	Example: NACF Notify Binding Information release.

2.5 Encapsulation and Addressing

This section describes what lower level protocol this e2 interface is using.

— TCP



3 Communication Model

According to the interaction mechanisms, the communication model between NACF and CLF can be described as synchronous and asynchronous modes; according to the information acquisition mechanisms, the communication model can be described as PUSH and PULL modes.

3.1 Synchronous and Asynchronous Modes

— Synchronous Mode

NACF first communicates to CLF before responding to any client request. For example, upon getting a DHCP Request or Release message from CPE, NACF sends the relevant binding information for this CPE to CLF and waits for its response. Once CLF validates this information and responds with ACK or NAK, NACF processes the CPE message accordingly and completes the operation. This also occurs when a lease expires at NACF. NACF notifies CLF and waits for its response before moving the lease to the FREE state.

If CLF replies with ACK, NACF takes the following actions based on the scenarios:

- **DHCP Request for New Lease:** NACF sends an ACK response to the CPE.
- **DHCP Release:** NACF clears out the lease binding information and moves the lease into the FREE state.
- **Expiry of an active lease:** NACF clears out the lease binding information and moves the lease into the FREE state.

If CLF replies with NAK, NACF takes the following actions based on the scenarios:

- **DHCP Request for New Lease:** NACF sends a NAK to the CPE.
- **DHCP Release:** NACF ignores the NAK and clears out the lease binding information and moves the lease into the FREE state.
- **Expiry of an active lease:** NACF ignores the NAK and clears out the lease binding information and moves the lease into the FREE state.

— Asynchronous Mode

NACF does not communicate to CLF prior to serving the CPE request. It first completes the transaction with CPE and then updates CLF. The CLF response makes no difference for NACF since the transaction is already committed irrespective of an ACK or NAK reply from CLF.

NACF behaves in the following ways for an ACK and NAK reply from CLF:



- **DHCP Request for New Lease:** NACF sends an ACK reply to the CPE.
- **DHCP Release:** NACF clears out the lease binding information and moves the lease into the FREE state.
- **Expiry of an active lease:** NACF clears out the lease binding information and moves the lease into the FREE state.

3.2 PUSH and PULL Modes

— PUSH Mode

The PUSH mode consists of having the NACF push the information to the CLF. The PUSH is done during the Network Attach phase when the IP address is assigned to the CPE or during the Network Detachment phase when the IP address is released because of lease expiry in the CPE or the NACF.

— PULL Mode

The PULL mode consists of having the CLF pull the information from the NACF. During the SIP REGISTER, the binding information is pulled from the NACF and stored in the CLF.



4 Use Cases

The scenarios for communications between the NACF and the CLF are described in the following sequence diagrams. The PUSH model is used whenever an IP address is allocated or changed in the NACF, so that CLF always stores the up-to-date and reliable binding information. In addition, the PULL model is a complement in case the binding information is missing due to network error that might occur in the network attachment.

The deployment scenario(s) can apply to a network architecture hosting multiple NACFs to one CLF or one NACF to multiple CLFs. Each NACF and CLF has the configuration data and the message is routed directly to the correct node.

Both Synchronous mode and Asynchronous mode of communication can be used between the NACF and the CLF for the network attachment. The choice of the communication mode is configurable in the NACF depending on the network needs. For example, Synchronous mode should be set when the CLF is mandatory during the SIP session set up.

In the Synchronous mode, the NACF has to wait for a confirmation message from the CLF before it responds to the CPE to assign an IP address. While in the Asynchronous mode, the NACF responds immediately when the request from the CPE is received and doesn't need to wait for confirmation from the CLF.

4.1 Successful Attach Push Model - Synchronous Mode

Whenever a new IP address is reserved for a CPE, the NACF needs to push the binding information with the IP address, IP Addressing Zone (IAZ), Network type, and CLID or Formatted RemoteId to the CLF in the NewIPAccessContext message ; optionally, the terminal type of the CPE is included.

The CLF validates the received parameters. If the CLID (for ATM network type) or Formatted RemoteId (for Gig-Ethernet network type) matches with the provisioned data in the CLF, then it stores the binding information. The NewIPAccessContextAck message is returned to the NACF.

If the received CLID cannot be found in the CLF for the ATM case, the CLF returns the NewIPAccessContextAck message with the error code unrecognized CLID.

If the received LineId (in the Formatted RemoteId) cannot be found in the CLF for the Gigabit Ethernet case, the CLF returns the NewIPAccessContextAck message with the error code unrecognized Formatted RemoteId.

If there is a mismatch between the received network type in the IPAccess context and the provisioned network type in the PAL, the CLF returns the NewIPAccessContextAck message with the error code network type mismatch.



If the received IP Access context already exists in the CLF, a positive response is sent back to the NACF. If the IP address is bound to a different CLID/LineId than the received one, the CLF disassociates the old binding, creates a new one over the same CLID/Line Id as the received one, and sends back a positive acknowledgement.

The Synchronous mode is set in the NACF. The NACF returns DHCP Ack with the allocated IP address to the CPE after the NewIPAccessContextAck message is received.

4.2 Successful Attach Push Model - Asynchronous Mode

The Asynchronous mode is set in the NACF. The NACF returns DHCP Ack with the allocated IP address and P-CSCF ID to the CPE immediately after the DHCP Request is received.

This use case is the almost same as 4.1, the only difference being that the NACF does not wait for the CLF response before sending DHCP Ack to the CPE.

4.3 Successful Detach Push Model

Whenever the IP address assigned to a CPE needs to be released, which can be triggered by a client request or a timer expiry in the NACF, the NACF needs to send the message ReleaseIPAccessContext with the IPAddress and IPAddressingZone parameters to notify the CLF.

The CLF searches the stored binding information with the received IP Address and IAZ, clears the stored data, and returns ReleaseIPAccessContextAck to acknowledge the NACF.

In Synchronous mode, the CLF pushes a message to the A-RACF to delete the associated IP Address and QoS profiles. The NACF waits for Release IP Access Context Ack from the CLF prior to cleaning up internal data structures.

In Asynchronous mode, the NACF cleans up the data structures and then informs the CLF. Regardless of a positive, negative, or time-out response received from the CLF, the data structures are cleaned in the NACF.

4.4 Successful SIP Register Pull Model

During SIP Registration, the SBC requests location information from the CLF.

If the CLF cannot find the IP context associated to the bounded Location information with the received IP address, the message IP Access Context Request is sent to the NACF to retrieve the binding information. The NACF returns the IP Access Context Response message to the CLF including Network Type, CLID or Formatted RemoteId and, optionally, terminal type.



The CLF stores the received information, retrieves the associated location information, and returns the location information to the SBC to complete the registration process.

In the CLF configuration, one IAZ can contain more than one NACF node. In this case, the CLF needs to send the IP Access Context Request to each of the NACF nodes and wait for respective responses until the network attach information (which contains the CLID or Formatted RemoteId is received).

4.5 Unsuccessful Attach Push Model

During validation of the received parameters in the message NewIPAccessContext, if there is any syntax error or the received CLID/Remote Id is not provisioned in the CLF, the NewIPAccessContextAck message is returned from the CLF to the NACF with a parameter Error Code indicating the reason of the failure.

The Synchronous mode is set in the NACF. The NACF returns DHCP NACK to the CPE after the NewIPAccessContextAck message is received with the Error Code; consequently the IP address is not assigned to the CPE.

In case of the Asynchronous mode, the NACF returns DHCP Ack with an allocated IP address and P-CSCF ID to the CPE immediately, regardless of the failure result from the CLF.

4.6 Unsuccessful Detach Push Model

During validation of the received parameters in the message ReleaseIPAccessContext, if there is any syntax error or the received IP address and IPAddressingZone doesn't exist in the CLF, the ReleaseIPAccessContextAck message is returned to the NACF with a parameter Error Code indicating the reason of failure. The NACF cleans up its internal data to remove the released or expired lease when there is no response from the CLF or response is negative.

4.7 Unsuccessful Pull Model

During SIP Registration, when the CLF is trying to pull the binding information from the NACF, the NACF returns an Error Code if the binding information associated with the IP address and IPAddressingZone doesn't exist or there is any syntax error in the message.

4.8 No Response During Network Attachment Push Model - Synchronous Mode

The Synchronous mode is set in the NACF. The NACF returns the DHCP Ack to the CPE if the NewIPAccessContextAck message is not received due to communication failure with the CLF.





5 Protocol Description

The protocol between the NACF and the CLF follows a Client/Server model where the NACF is the client and the CLF is the server. The mode of communication can be configured to either Synchronous or Asynchronous in the NACF and is non-blocking when the CLF and the NACF are processing the requests from other CPEs. The CLF is able to handle the requests from multiple NACF nodes which are configured in either Synchronous or Asynchronous mode respectively.

5.1 Transport

This protocol uses a socket connection over TCP/IPv4 where each packet utilizes the intrinsic retransmission mechanism to ensure packet delivery. The NACF maintains one TCP/IP connection toward the CLF. All packets are sent in Network Order Byte. The TCP port number 3097 is used for the CLF connection.

5.2 Message Structure

The protocol to exchange the binding information between the NACF and the CLF has the common message format as:

- Version
- Op Code
- Length
- TLV 1..n

The tables below outline the general packet construction. All values are expressed in hexadecimal octets.

Table 3 Header Format

1	1	2
Version	Op code	Length

Version

The version field specifies the version number. The current version is 0x02.

Op Code

This field is a single octet field that ranges from 0x00 to 0xFF. The definition of each Op code is defined further in this document.

Length

This field represents the total message length including version, op code and all TLV attributes.



Table 4 TLV Format

1	2	Variable
Type	Length	Value

Type	The type field signifies the type of the data being sent within the message.
Length	The length of the current TLV has two octets and indicates the attribute including the type, length and value fields.
Value	The Value field is zero or more octets and contains information specific to the attribute. The Type and Length fields determine the format and length of the Value field.

5.2.1 Operation Codes

The following table shows a list of operation codes and their corresponding associated messages to be supported between the NACF and the CLF.

Table 5 NACF-CLF Operation Codes

Operation Code	Message
0x07	Heart Beat
0x08	New IP Access Context
0x09	New IP Access Context Ack
0x0A	Release IP Access Context
0x0B	Release IP Access Context Ack
0x0C	IP Access Context Request
0x0D	IP Access Context Response

5.2.2 Data Type

The following table shows a list of TLV type to be used in the interface messages between the NACF and the CLF.

Table 6 NACF-CLF TLV Data Type

Type Value	Supported Type
0x01	IP Address
0x02	Transaction Id
0x06	Calling Line Identification
0x07	IP Addressing Zone
0x08	Terminal Type



Type Value	Supported Type
0x09	Error Code
0x0A	Network Type
0x0B	Formatted RemoteId

5.3 Primitive Definition

The order of the TLV defined in the primitives is not enforced and can be sent or received in any sequence, except for the Transaction Id TLV, which is assumed to be the first TLV.

5.3.1 New IP Access Context

Sender: NACF

Receiver: CLF

This primitive sends the binding information from the NACF toward the CLF.

Op code = 0x08.

Table 7 TLV Data in New IP Access Context

TLV Name	TLV Type	TLV Length	Optionality	Note
Transaction Id	0x02	4 octets	Mandatory	See Section 5.4.6 on page 22
Calling Line Identification	0x06	Variable octets	Optional	Present when the Network Type = ATM Not present when the Network Type = Gig-E See Section 5.4.1 on page 20



TLV Name	TLV Type	TLV Length	Optionality	Note
Formatted Remote Id	0x0B	Variable octets	Optional	Present when the Network Type = Gig-E Not present when the Network Type = ATM See Section 5.4.8 on page 23
IP Address	0x01	Variable octets	Mandatory	See Section 5.4.3 on page 22
IP Addressing Zone	0x07	Variable octets	Mandatory	See Section 5.4.4 on page 22
Terminal Type	0x08	2 octets	Optional	See Section 5.4.5 on page 22

5.3.1.1 Message Format

The following table represents the layout of the individual octets of data.

Table 8 New IP Access Context Format

Version=1	Op Code=08	Message Length
Type = 02	Length = 07	Transaction -
ID		Type = 0A
Length = 04	Network Type	Type = 06
Length	Variable Length	
Field, String of Calling Line Identification		
Type = 0B	Length	Variable -
Field, String of Formatted Remote Id		
Type = 01	Length	Variable -
Length Field of IP Address (Length =04 or 16 octets)		
Type = 07	Length	Variable -
Length Field, String of IP Addressing Zone (Maximum 255 characters)		



Type = 08	Length = 5	Terminal
Type		

5.3.2 New IP Access Context Ack

Sender: CLF

Receiver: NACF

This primitive sends the acknowledgement from the CLF toward the NACF.

Op code = 0x09

Table 9 TLV Data in New IP Access Context Ack

TLV Name	TLV Type	TLV Length	Optionality	Note
Transaction Id	0x02	4 octets	Mandatory	See Section 5.4.6 on page 22
Error Code	0x09	1 octets	Optional	See Section 5.4.2 on page 21

5.3.2.1 Message Format

The table below represents the layout of the individual octets of data.

Table 10 New IP Access Context Ack Format

Version=1	Op Code=09	Message Length = 0F	
Type = 02	Length = 07		Transaction -
ID			Type = 09
Length = 04		Error code	

5.3.3 Release IP Access Context

Sender: NACF

Receiver: CLF

The NACF uses this primitive to notify the CLF to release the binding information.

Op code = 0x0A.



Table 11 Release IP Access Context

TLV Name	TLV Type	TLV Length	Optionality	Note
Transaction Id	0x02	4 octets	Mandatory	See Section 5.4.6 on page 22
IPAddress	0x01	16 octets	Mandatory	See Section 5.4.3 on page 22
IPAddressing Zone	0x07	Variable octets	Mandatory	See Section 5.4.4 on page 22

5.3.3.1

Message Format

The table below represents the layout of the individual octets of data.

Table 12 Release IP Access Context Ack Example

Version=1	Op Code=0A	Message Length	
Type = 02	Length = 07		Transaction -
ID			Type = 01
Length		Variable Length -	
Field of IP address (maximum 16 octets)			
...			
Type = 07	Length		Variable -
Length Field of IP Address (Length =04 or 16 octets)			
Type = 07	Length		Variable
Length Field, String of IP Addressing Zone (Maximum 255 characters)			

5.3.4

Release IP Access Context Ack

Sender: CLF

Receiver: NACF

This primitive sends the acknowledgement from the CLF toward the NACF to message Release IP Access Context.

Op code = 0x0B



Table 13 Release IP Access Context Ack

TLV Name	TLV Type	TLV Length	Optionality	Note
Transaction Id	0x02	4 octets	Mandatory	See Section 5.4.6 on page 22
Error Code	0x09	1 octet	Optional	See Section 5.4.2 on page 21

5.3.4.1 Message Format

The table below represents the layout of the individual octets of data.

Table 14 Release IP Access Context Format

Version=1	Op Code=0B	Message Length = 0F
Type = 02	Length = 07	Transaction –
ID		Type = 09
Length = 04	Error code	

5.3.5 IP Access Context Request

This primitive is used in the event that the binding information is missing in the CLF. The CLF requests the NACF to send the binding information that corresponds to the received IP address and IPAddressingZone.

Sender: CLF

Receiver: NACF

Op code = 0x0C.

Table 15 Release IP Access Context Ack

TLV Name	TLV Type	TLV Length	Optionality	Note
Transaction Id	0x02	4 octets	Mandatory	See Section 5.4.6 on page 22
IPAddress	0x01	Variable octets	Mandatory	See Section 5.4.3 on page 22
Error Code	0x07	Variable octet	Optional	See Section 5.4.2 on page 21



5.3.5.1 Message Format

The table below represents the layout of the individual octets of data.

Table 16 IP Access Context Request Format

Version=1	Op Code=0C	Message Length	
Type = 02	Length = 07		Transaction -
ID			Type = 01
Length		Variable Length -	
Field of IP address (Length =04 or 16 octets)			
Type = 07	Length		Variable -
Length Field, String of IP Addressing Zone (Maximum 255 characters)			

5.3.6 IP Access Context Response

Sender: NACF

Receiver: CLF

This primitive is used by the NACF to send the binding information to the CLF upon request.

Op code = 0x0D.

Table 17 TLV Data in IP Access Context Response

TLV Name	TLV Type	TLV Length	Optionality	Note
Transaction Id	0x02	4 octets	Mandatory	See Section 5.4.6 on page 22
Network Type	0x0A	1 octet	Optional	See Section 5.4.7 on page 23
CallingLineIdentification	0x06	Variable octets	Optional	Present when the Network type=ATM Not present when the Network type=GiG-E See Section 5.4.1 on page 20



TLV Name	TLV Type	TLV Length	Optionality	Note
Formatted Remote Id	0x0B	Variable octets	Optional	Present when the Networktype=GiG-E Not present when the Networktype=ATM See Section 5.4.8 on page 23
TerminalType	0x08	2 octets	Optional	See Section 5.4.5 on page 22
Error Code	0x09	1 octets	Optional	See Section 5.4.2 on page 21

5.3.6.1 Message Format for Positive Response

The table below represents the layout of the individual octets of data when a positive response is received from the NACF.

Table 18 IP Access Context Response Format for Positive Response

Version=1	Op Code=0D	Message Length	
Type = 02	Length = 07		Transaction -
ID			Type = 0A
Length = 04		Network Type	Type = 06
Length		Variable Length -	
Field, String of Calling Line Identification			
Type = 08	Length = 5		Terminal
Type			

5.3.6.2 Message Format for Negative Response

The table below represents the layout of the individual octets of data when a negative response is received from the NACF.



Table 19 IP Access Context Response Format for Negative Response

Version=1	Op Code=0D	Message Length = 0F	
Type = 02	Length = 07		Transaction -
ID			Type = 09
Length = 04		Error code	

5.3.7 Heartbeat

The heartbeat primitive ensures that the application is alive and well. The NACF node uses this primitive to verify at the application level that everything is functioning properly. The NACF sends a heartbeat message with a transaction ID. The CLF, upon receiving this message, verifies the state of the CLF and responds to the heartbeat message with the same transaction ID.

Sender: NACF

Receiver: CLF

Op code = 0x07

Table 20 TLV Data in IP Access Context Response

TLV Name	TLV Type	TLV Length	Optionality	Note
Transaction Id	0x02	4 octets	Mandatory	See Section 5.4.6 on page 22

5.3.7.1 Message Format

The table below represents the layout of the individual octets of data.

Table 21 Heartbeat Format

Version=1	Op Code=07	Message Length = 0B	
Type = 02	Length = 07		Transaction -
ID			

5.4 Data Type Definition

This section provides the definitions of the TLV data.



5.4.1 Calling Line Identification

The Calling Line Identification (CLID) identifies Virtual Circuits used in the ATM network to support IP connection. This parameter contains the DSLAM identifier and data identifying the aggregation path on the DSLAM for the corresponding Virtual Circuit.

The CLID consists of the following information:

- Service Node ID of ECR
- Node Service card number of ECR
- Node Service port number of ECR
- Network VP
- Network VC

The CLID information inserted by the ECR is vendor-dependent and the NACF rearranges and provides the dynamic CLID to the CLF in a uniformed format. The received CLID data is ASCII String and formatted as 'Service Node ID#Node Service card number#Node Service port number#Network VP #NetworkVC'. Each element in the string is delimited by the pound character (#). For example: 'Paris#3#2#114#16'

Type: 0x06

Length: variable octets

Value Range: The network VP ranges from 0 to 255 with a maximum of 3 characters. The Network VC ranges from 32 to 65535 with a maximum of 5 characters.

5.4.2 Error Code

The error code indicates the reason that binding information cannot be created, retrieved or released.

Type: 0x09

Length: 1 octet

Value: integer

Table 22 Value Field Values

Value	Meaning
00	Not used
01	Mandatory parameter missing



Value	Meaning
02	Syntax error
03	Unrecognized CLID
04	Unrecognized IP address
05	Unrecognized IP Addressing Zone
06	System error
07	Network Type mismatch
08	Unrecognized Remote Id
07–255	Reserved

5.4.3 IP Address

This parameter contains the IP address of the CPE allocated by the NACF. Both Ipv4 and Ipv6 format is supported.

Type: 0x01

Length: Variable length. The valid length is either 4 octets or 16 octets. 4 octets indicates Ipv4 format, while 16 octets indicates Ipv6.

Value: integer

5.4.4 IP Addressing Zone

The IAZ is defined in the NACF corresponding to specific ranges of IP address.

The data type of IAZ is ASCII String and the format refers to the Internet Domain name definition described in RFC1035.

Type: 0x07

Length: variable octets. Maximum length is 255 octets.

5.4.5 Terminal Type

This parameter is not supported and will be defined upon future request.

Type: 0x08

Length: 2 octets

Value Range: 1-65535



5.4.6 Transaction Id

A locally unique number chosen by the client or server associates messages and responses between a client and a server.

Type: 0x02

Length: 4 octets

Value Range: 1-4294967295

5.4.7 Network Type

The network Type indicates the type of access aggregation network where the messages are coming from.

Type: 0x0A

Length: 1 octet

Table 23 Network Type Values

Value	Meaning
0	Not used
01	ATM Aggregation network
02	Gigabit Ethernet Aggregation network

5.4.8 Formatted RemoteId

Remote ID identifies the physical links used in the Gigabit Ethernet aggregation network to support IP connection. It is inserted by the DHCP Relay in the Gigabit Ethernet DSLAM. The Formatted remote Id is used between the NACF and the CLF. The NACF formats the remote Id received from DHCP Option 82.

Type: 0x0B

Length: variable octets

Value range: the Formatted Remote Id is a string. The maximum length of the Formatted RemoteId is 63 characters.

The syntax of the Formatted Remote Id is as follows:

Formatted remotted=<LineId>!<ServiceId>

where,

LineId is a line identifier associated with a Physical Access Line. It is an alphanumeric code.



ServiceId is an identifier associated with the list of services configured on the Circuit.

The LineId and ServiceId are delimited by "!". For example:

Example 1 Formatted Remote Id

where,

LineId="a1s3fs3f379f42er3g34"

ServiceId="312sg25t4gf323"

"

5.5 Primitive Timer Values

The following table provides a summary of the timers used for primitives between the NACF and the CLF. The timer values specified in this table are default values only and can be configured in each node.

Table 24 NACF-CLF Primitive Timer Values

Timer	Default (sec.)	Started when	Normally stopped when
NIACT (New IP Access Context Timer)	3	New IP Access Context is sent	New IP Access Context Ack is received
RIACT (Release IP Access Context Timer)	3	Release IP Access Context is sent	Release IP Access Context Ack is received
IACRT (IP Access Context Request Timer)	3	IP Access Context Request is sent	IP Access Context Response is received
HBT (Heart Beat Timer)	3	Heartbeat is sent	Heartbeat is received



6 Communication (Control Mechanism)

The application protocol uses a single persistent TCP connection between each NACF client and its corresponding CLF server. The NACF is responsible for initiating the TCP connection and the CLF listens on the defined TCP port number.

6.1 Normal State

The normal state consists of the NACF communicating normally with the CLF. The Network Attach or Detach triggers the NACF sending the binding information to the CLF. The CLF is able to pull the binding information from the NACF when it is not stored in the CLF.

6.2 Control Mechanism

The heartbeat message is used to ensure that the CLF is present. Each heartbeat message is sent periodically according to a configurable timer (typically 5 seconds). The NACF sends the Heart Beat message to the CLF and the CLF must echo it back. The timer needs to be reset in the NACF when a Heart Beat message is received from the CLF. The Heart Beat message is resent to the CLF if no response is received when the Heart Beat message timer defined in Table 20 expires.

The CLF is considered not functioning when the maximum retry limit of the Heart Beat message is reached and the TCP connection is then discontinued by the NACF. The number of maximum retries are configurable (typically 3 times).

6.3 Communication Failure

The CLF has a High Availability (HA) mechanism and publishes one logical IP address to the external nodes. The NACF maintains one persistent TCP/IP connection toward the CLF. If the NACF detects the communication failure with the CLF or receives a disconnect socket message, the NACF closes the existing connection and tries to re-establish a TCP connection. The retry interval is configurable and the default is 3 seconds. On the CLF side, the Ack message is dropped if there is no TCP connection when the CLF is trying to respond to the messages pushed by the NACF. For the PULL messages from the CLF, the NACF is treated as not available if there is no TCP connection active. During that reconnect mode, all transactions destined to the CLF are buffered in the NACF for later transmission when the CLF becomes available. When the CLF receives a request of TCP connection set up from an NACF client, it determines if there is an existing connection for that client based on the received source IP address. It abandons the existing connection before the new one is established because the client has decided that the old TCP connection is unusable.



The NACF maintains two separate TCP/IP connections toward the CLF. If the NACF receives a disconnect socket message, the NACF retries for a number of minutes (configurable ranging from –1 Infinite to 1440, for example, one day). During that reconnect mode, all transactions destined to the CLF are sent over via the other network interface. If both interfaces fail, all transactions are buffered in the NACF for later transmission when the CLF becomes available.

6.3.1 Retry Mechanism when Communication Fails

The NACF and the CLF nodes need to implement the retry mechanism to ensure that application message is delivered successfully when the destined node is active. For the node that originates the messages, if there is no response from the destined node when the message timer expires, the node retries sending the same message several times. The retry time is configurable in the node. Value 0 indicates no retry is needed.

The message is discarded and a time-out treatment starts if all the retries fail.

If all the retries fail, the originating node tries the same process over the secondary interface.

The CLF and the NACF node can receive messages with duplicated transaction IDs because of the retransmission. They treat each message as if it was a new one and they send back the response for each of them.

6.3.2 Protocol Errors

In the case where the Version or Opcode in the message header is incorrect, the received message is discarded and the TCP connection is closed.

In the case where the Transaction ID in the TLV is incorrect or it is not the first TLV received, the received message is silently discarded, but the TCP connection is not dropped.

If a node receives any invalid TLV except Transaction ID, the Syntax error is returned.

If a node receives a request and the capacity license is reached by producing the request, the System error is returned.

6.4 CLF Failure

This section provides information on CLF failures and how data can be recovered if a failure occurs.



6.4.1 Communication Failure

The CLF binding information is saved to disk and reloaded in case of a CLF failure. During the failure period, when the CLF application has a communication problem or the CLF node is down, the following events can happen in the NACF:

- Initial DHCP request: In the Synchronous mode, since the NACF assigns the IP Address to the CPE when there is no response from the CLF, the Network Attachment can be still successful but the new binding information is not pushed to the CLF. In the Asynchronous mode, the Network Attachment can be done between the NACF and the CPE, resulting in the corresponding new binding information missing in the CLF.
- DHCP release: The IP address in the CPE and the NACF can be released without notifying the CLF. The data recovery mechanism used in the event of this failure is described in the next section.

6.4.2 Data Recovery

- Data synchronization by the NACF: The NACF is the master database of the IP address allocation, which stores the accurate information when an IP address is reserved or released. When the NACF tries to push the New IP Context message to the CLF to update the IP access context, if there is no response from the CLF, the NACF does not buffer the messages not delivered. When the NACF tries to push the New IP Context message to the CLF to remove the IP access context, if there is no response from the CLF, the NACF needs to buffer the messages not delivered and resend them when the CLF is up. The data in the CLF will not be consistent with that in the NACF since the NACF only buffers the release IP Access Context messages during the failure period. However, the missing binding information in the CLF is recovered from the NACF when the SBC queries the CLF, thus reducing the total number of messages to be buffered.
- Data Recovery in the CLF: For the new IP binding information missing during the failure period of the CLF node, the data can be retrieved when the SBC queries the CLF and then is created in the CLF by querying the NACF with the IP Access Context request message.

6.5 NACF Failure

The NACF must ensure the integrity of its data after a NACF failure. When the NACF application has no communication with the CLF, it needs to resend all the binding information updated during the failure period to the CLF.

When the NACF application completely fails or the NACF node is down, no network attachment or detachment is occurring. However, the data stored in the CLF is still reliable and the SIP Registration and Invite can be processed normally.





7 Security

This protocol is not secure; however, the security of the network access can be achieved by the deployment and site configuration.





8 Formal Syntax

Not Applicable.





9 Related Standards

Not Applicable.





Reference List

Ericsson Documents

- [1] Trademark Information
- [2] Glossary of Terms and Acronyms
- [3] Typographic Conventions