

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

IPWorks DHCPv4 Function Overview

Contents

1	Introduction	3
1.1	Document History	3
1.2	Purpose.....	3
1.3	Scope	3
1.4	Document Structure.....	3
2	Survey of Included Functions.....	3
2.1	Overview	3
2.1.1	DHCPv4 RFC Implementation and Related IPWorks Add-on ...	4
2.1.2	TISPAN NASS NACF Implementation	8
2.1.3	IPWorks DHCPv4 CLI/Server Manager Support.....	8
2.2	List of Actors	8
2.2.1	Actor: DHCP Client/Relay Agent	8
2.2.2	Actor: DNS Server	8
2.2.3	Actor: CLI/Server Manager	8
2.2.4	Actor: CLF (Connectivity Session Location Function).....	9
2.2.5	Actor: DHCP Client from Address Space A/B/C	9
2.3	List of Sub-Functions	9
2.3.1	DHCPv4 Functions Related to IETF RFC's.....	9
2.3.2	TISPAN NASS NACF Function	10
2.3.3	DHCPv4 Server Manager Support Function	10
2.3.4	DHCPv4 Geographic Redundancy Function.....	10
3	Detailed Description	10
3.1	DHCPv4 Functions Related to IETF RFC's.....	10
3.1.1	DHCPv4 Server Standard Function.....	10
3.1.2	DHCPv4 DDNS Function.....	19
3.1.3	DHCPv4 Failover and Load Balancing Function.....	19
3.1.4	Support for Overlapped IP address ranges.....	22
3.2	TISPAN NASS NACF Function	23
3.3	DHCPv4 IPWorks OAM Implementation	25
3.3.1	DHCPv4 CLI/Server Manager Support Function	25
3.4	DHCPv4 IPWorks OAM Implementation	26
4	Operational Conditions	26
4.1	Configurable Parameters	26
4.2	Commands and User Procedures	26
4.3	Charging	27
4.4	Characteristics	27
5	Statement of Compliance.....	27
6	Miscellaneous.....	28
7	Terminology.....	28

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

7.1	Abbreviations	28
7.2	Definitions	28
8	References	28

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

1 Introduction

1.1 Document History

Rev	Date	Sign.	Comment
PA1	2018-01-19	EZGUOZI	Replaces 8/155 17-AVA 901 16 Uen A due to IPWorks 1.14 updates.

1.2 Purpose

The purpose of this document is to specify the DHCPv4 functions realized in IPWorks.

1.3 Scope

The scope of this document is to describe the function of IPWorks DHCPv4 server.

1.4 Document Structure

-

2 Survey of Included Functions

2.1 Overview

For DHCPv4 in IPWorks, there are three types of functions: the functions defined in IETF RFC's and with some IPWorks add-on, TISPAN NASS NACF with IPWorks adaptation, and IPWorks operation/administration/maintenance (OAM) functions for DHCP server. They correspond to different interfaces in Figure - 1: IPWorks DHCPv4 server interfaces overview:

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

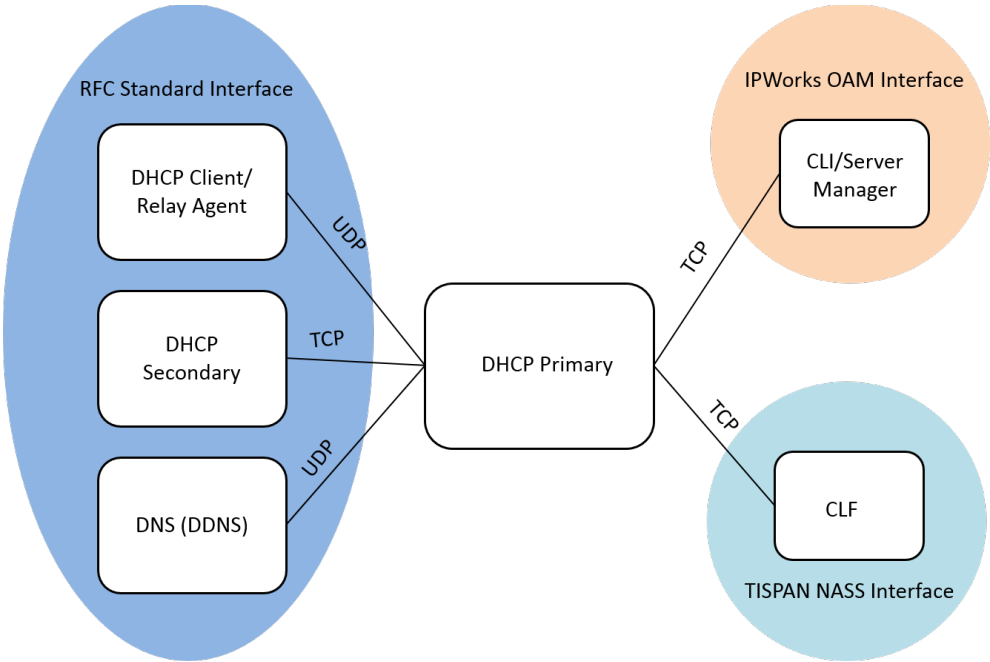


Figure - 1: IPWorks DHCPv4 server interfaces overview

The DHCPv4 server interfaces towards DHCP client, DDNS, interface between primary DHCPv4 server and secondary DHCPv4 server and the corresponding functions fall into the scope of RFC DHCP standards. All other interfaces are IPWorks proprietary.

IPWorks DHCPv4 server supports specifying the lease pools with partial or total overlapping of the IP addresses. We treat this feature as an add-on over the DHCP RFC standard features.

2.1.1 DHCPv4 RFC Implementation and Related IPWorks Add-on

2.1.1.1 DHCPv4 Server Function for DHCP Client/Relay Agent

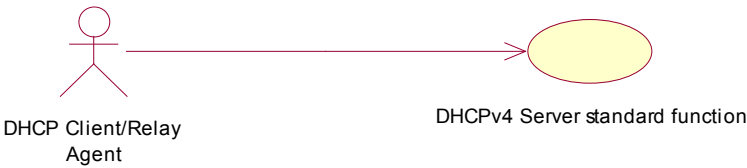


Figure - 2: DHCPv4 Server Function for DHCP Client/Relay Agent

The interface between DHCP client/relay agent and DHCPv4 server provide a mechanism for allocation of network addresses and distributing network configuration parameters from the DHCPv4 server to the client.

- Authentication Protocol

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

Authentication can be enabled between the DHCP clients and DHCP server. The clients can be classified according to the message that is sent from DHCP clients or relay agent to DHCPv4 server. UDP is the protocol used underlying for this interface.

- User ID Provisioning

User ID Provisioning is an IPWorks add-on to the standard interface. IPWorks DHCP server can be configured to extract the Subscriber-ID suboption of Option82, put the suboption information in one of the DHCP options from 224 to 254 upon request, and send it to the client.

- P-CSCF discovery

P-CSCF discovery is used to receive DHCP INFORM message via DHCP option120 SIP Servers.

- ClientClass

In IPWorks DHCPv4 server, ClientClass is a policy object that represents configuration for a group of clients. When the DHCP server receives a request from a client, the contents of the DHCP packet are examined to determine which client classes should be associated with that request. Then further behaviors could be configured for that group of clients like allow/deny, lease limit, IP overlapping, etc.

There are situations where the DHCP option needs to be configured. The IPWorks DHCP server includes a mechanism to configure unsupported options.

Authentication can address issues of Denial of Service attacks, Theft of Services or attempts to establish a Man in the Middle attack through a faulty server or client.

When changes are made to the DHCPv4 Server, the client leases should be renewed with new configuration information. IPWorks DHCPv4 server can be configured to notify clients about this, including the address range changes. DHCPv4 reconfiguration is based on RFC 3203.

2.1.1.2

DHCP DDNS Function



Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

Figure - 3: DHCPv4 Server Function for DDNS

DHCP servers can use the Dynamic DNS (DDNS) updates mechanism (specified in RFC2136 [14]) to update mapping the DNS name to address, and vice versa. So the mappings for DHCP clients are consistent with the IP addresses that the clients acquire via DHCP. UDP protocol is used for this interface as well.

2.1.1.3 DHCP Failover and Load Balancing

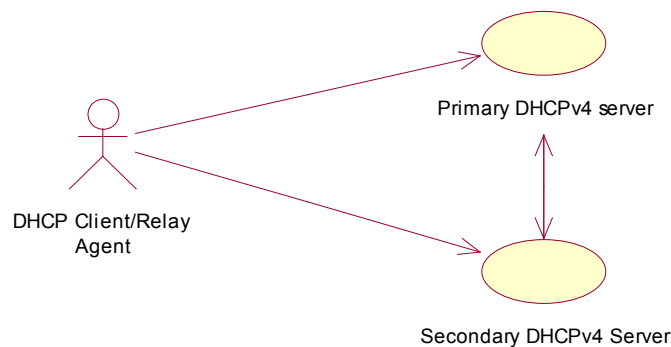


Figure - 4: DHCPv4 Server Failover with Load Balancing

DHCP supports multiple servers operating on a single network to provide redundancy in case of server failure. To work reliably, the cooperating primary and secondary servers must maintain a consistent database of the lease information. This implies that servers need to coordinate any and all lease activity so that this information is synchronized in case of failover. One server is designated as "primary" server, the other is the "secondary" server.

The interface is also used to integrate the failover protocol with the DHCP load balancing approach. To provide reliable and ordered message delivery between the two DHCP servers, TCP protocol is used. Refer to [23] and [24] for standard specifications.

In IPWorks, as an enhancement towards failover protocol, leases that belong to secondary server is possible to be moved to BACKUP state rather than FREE state upon existing EXPIRED state when severe lease imbalance problem happens between primary and secondary servers.

IPWorks only supports one to one mapping for failover protocol. This means in failover configuration, there are two servers: one works as primary and the other one works as secondary. Other configurations specified in failover draft RFC [24] are not supported.

For load balancing, IPWorks supports the following scenarios:

- Between two servers in a failover pair.
- Between two standalone servers/failover pairs.

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

2.1.1.4 Overlapped IP Address Range

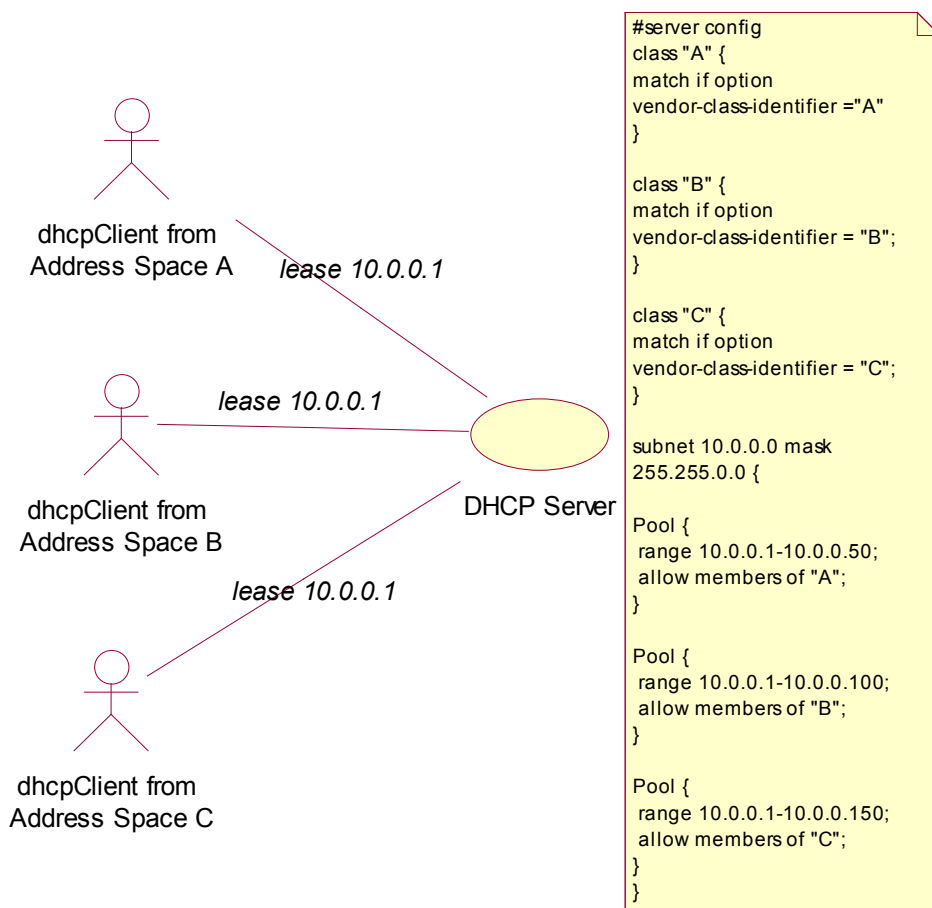


Figure - 5: DHCPv4 Server with Support for Overlapped IP Lease Pools

DHCPv4 server can be configured with overlapping IP addresses. However, the overlapping IP addresses that clients request must belong to different physical/logical layer 2 LAN (local area networks), which are separated by relay agents, routers, or other network devices. That means the clients are in different address spaces. The overlapping pools must also belong to the same logical subnet. Overlapping is applied when many sets of client machines are leased with limited set of address pools.

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

2.1.2 TISPAN NASS NACF Implementation



Figure - 6: DHCPv4 Server as NACF

The IPWorks DHCPv4 server can act as a NACF (Network Access Configuration Function with Dynamic Host Configuration Protocol) server which has interface with CLF (Connectivity Session Location Function) in TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking) NASS (Network Attachment Subsystem) solution.

2.1.3 IPWorks DHCPv4 CLI/Server Manager Support



Figure - 7: IPWorks DHCPv4 Server Manager Support

IPWorks server manager modules are the direct interface to DHCPv4 server. And DHCPv4 server develops a set of IPWorks server manager supporting functions, which perform provisioning and configuration management within IPWorks system architecture via IPWorks CLI.

2.2 List of Actors

2.2.1 Actor: DHCP Client/Relay Agent

DHCP client/relay agent are the network elements that communicate with and receive IP address and network configuration parameters from a DHCP server.

2.2.2 Actor: DNS Server

DNS server accepts RR (Resource Record) update from DHCP server.

2.2.3 Actor: CLI/Server Manager

CLI/server manager performs as the agent for CLI interface to control operations, update DHCPv4 server with the latest configuration data, and retrieve dynamic network or DHCPv4 server data.

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

2.2.4 Actor: CLF (Connectivity Session Location Function)

CLF is a server that interfaces with IPWorks DHCPv4 server (NACF). It connects the users' IP addresses to the network location information in TISPAN NASS solution.

2.2.5 Actor: DHCP Client from Address Space A/B/C

In the network configuration, the clients in different address spaces must not be located in the same layer 2 physical/logical LAN (local area network).

However, within IPWorks DHCPv4 server, clients in different address spaces must belong to different client class group. A client class is a DHCP policy object that represents configuration for a group of clients.

IPWorks operator need to ensure the same IP address assigned to clients in different class group will not conflict with each other in the network.

2.3 List of Sub-Functions

2.3.1 DHCPv4 Functions Related to IETF RFC's

2.3.1.1 DHCPv4 Server Function for DHCP Client/Relay Agent

This function includes IP address allocation, distributing other network configuration parameters to DHCP clients, supporting DHCP options/sub-options and so on.

2.3.1.2 DHCPv4 DDNS Function

With DHCP, Internet addresses are dynamically assigned to clients. These addresses and the associated client's name are dynamically registered to DNS. The IPWorks DHCP server supports the Dynamic DNS update. The most effective way to use DDNS updates is to create a new zone and use only dynamic updates to create the resource records in that zone.

2.3.1.3 DHCPv4 Failover and Load Balancing Function

2.3.1.4 The primary and secondary DHCPv4 servers maintain a consistent database of the lease information. This implies that servers need to coordinate all lease activity so that this information is synchronized in case of failover. They provide both redundancy and load balance via integrating the failover protocol with the DHCP load balancing approach. Support for overlapped IP address ranges

DHCPv4 server can be configured with two or more pools with overlapped address ranges. And the same IP address can be assigned to multiple DHCP clients within different address spaces.

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

2.3.2 TISPAN NASS NACF Function

The standard NACF is responsible for the IP address allocation to the UE. It also distributes other network configuration parameters such as address of DNS server(s), address of signaling proxies for specific protocols. This part is covered in IPWorks DHCPv4 server standard function. NACF focuses on the function needed to interact with CLF: the DHCPv4 server updates the CLF for each new DHCP lease by providing CLF with the CPE IP address and binding information like IP Address Zone, Calling Line Identification (CLID) /RemoteID and Network Type. NACF server also updates the CLF when a lease is released, or when the lease expires. NACF server also services the pull operation initiated by CLF.

2.3.3 DHCPv4 Server Manager Support Function

In IPWorks, nearly all managements for DHCPv4 server are performed through the Server Manager. DHCPv4 server needs to respond to commands like status, reconfigure, fetch, query and so on. From IPWorks system point of view, Server Manager is an agent for CLI /SS which implement the management for DHCPv4 server. A TCP connection is used for the communication between DHCPv4 server and Server Manager.

2.3.4 DHCPv4 Geographic Redundancy Function

Two IPWorks systems can be deployed in two geographically separated sites to prevent disasters. Between the two sites, leasing data are synchronized by DHCP failover protocol. And provisioning data are synchronized by MySQL bin log file. Failover connection is established between the two sites via the service interface which is used by DHCP service on PL servers.

Legacy single site DHCP IPWorks cannot directly transform to Geographic Redundancy DHCP cluster due to the limitation of the protocol. Instead, the legacy IPWorks must be reconfigured.

3 Detailed Description

3.1 DHCPv4 Functions Related to IETF RFC's

3.1.1 DHCPv4 Server Standard Function

The standard DHCPv4 functions include IP address allocation, distributing other network configuration parameters to DHCP clients, DHCP options/sub-options support and so on.

DHCPv4 server supports BOOTP client conforming to RFC [9], [10][11].

DHCPv4 server supports DHCP core protocol conforming to RFC [12] to [24].

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

Table 1 shows all the supported DHCP messages in IPWorks.

Value	Message Type	Reference	IPWorks
1	DHCPDISCOVER	[RFC 2132]	√
2	DHCPOFFER	[RFC 2132]	√
3	DHCPREQUEST	[RFC 2132]	√
4	DHCPDECLINE	[RFC 2132]	√
5	DHCPACK	[RFC 2132]	√
6	DHCPNAK	[RFC 2132]	√
7	DHCPRELEASE	[RFC 2132]	√
8	DHCPINFORM	[RFC 2132]	√
9	DHCPFORCERENEW	[RFC 3203]	√

Table 1:DHCP Messages Supported in IPWorks

For detailed DHCP options support, refer to Table 2: IPWorks DHCP Options Support

Tag	Name	Meaning	Ref	IPWorks
0	Pad	None	[RFC 2132]	√
1	Subnet Mask	Subnet Mask Value	[RFC 2132]	√
2	Time Offset	Time Offset in Seconds from UTC (note: deprecated by 100 and 101)	[RFC 2132]	√
3	Router	N/4 Router addresses	[RFC 2132]	√
4	Time Server	N/4 Timeserver addresses	[RFC 2132]	√
5	Name Server	N/4 IEN-116 Server addresses	[RFC 2132]	√
6	Domain Server	N/4 DNS Server addresses	[RFC 2132]	√
7	Log Server	N/4 Logging Server addresses	[RFC 2132]	√
8	Quotes Server	N/4 Quotes Server addresses	[RFC 2132]	√
9	LPR Server	N/4 Printer Server addresses	[RFC 2132]	√
10	Impress Server	N/4 Impress Server addresses	[RFC 2132]	√
11	RLP Server	N/4 RLP Server addresses	[RFC 2132]	√
12	Hostname	Hostname string	[RFC 2132]	√
13	Boot File Size	Size of boot file in 512 byte chunks	[RFC 2132]	√
14	Merit Dump File	Client to dump and name the file to dump it to	[RFC 2132]	√
15	Domain Name	The DNS domain name of the client	[RFC 2132]	√
16	Sw ap Server	Sw ap Server address	[RFC 2132]	√
17	Root Path	Path name for root disk	[RFC 2132]	√
18	Extension File	Path name for more BOOTP info	[RFC 2132]	√
19	Forw ard On/Off	Enable/Disable IP Forw arding	[RFC 2132]	√
20	SrcRte On/Off	Enable/Disable Source Routing	[RFC 2132]	√
21	Policy Filter	Routing Policy Filters	[RFC 2132]	√
22	Max DG Assembly	Max Datagram Reassembly Size	[RFC 2132]	√
23	Default IP TTL	Default IP Time to Live	[RFC 2132]	√
24	MTU Timeout	Path MTU Aging Timeout	[RFC 2132]	√
25	MTU Plateau	Path MTU Plateau Table	[RFC 2132]	√
26	MTU Interface	Interface MTU Size	[RFC 2132]	√
27	MTU Subnet	All Subnets are Local	[RFC 2132]	√
28	Broadcast Address	Broadcast Address	[RFC 2132]	√

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

Tag	Name	Meaning	Ref	IPWorks
29	Mask Discovery	Perform Mask Discovery	[RFC 2132]	√
30	Mask Supplier	Provide Mask to Others	[RFC 2132]	√
31	Router Discovery	Perform Router Discovery	[RFC 2132]	√
32	Router Request	Router Solicitation Address	[RFC 2132]	√
33	Static Route	Static Routing Table	[RFC 2132]	√
34	Trailers	Trailer Encapsulation	[RFC 2132]	√
35	ARP Timeout	ARP Cache Timeout	[RFC 2132]	√
36	Ethernet	Ethernet Encapsulation	[RFC 2132]	√
37	Default TCP TTL	Default TCP Time to Live	[RFC 2132]	√
38	Keepalive Time	TCP Keepalive Interval	[RFC 2132]	√
39	Keepalive Data	TCP Keepalive Garbage	[RFC 2132]	√
40	NIS Domain	NIS Domain Name	[RFC 2132]	√
41	NIS Servers	NIS Server Addresses	[RFC 2132]	√
42	NTP Servers	NTP Server Addresses	[RFC 2132]	√
43	Vendor Specific	Vendor Specific Information	[RFC 2132]	√
44	NETBIOS Name Srv	NETBIOS Name Servers	[RFC 2132]	√
45	NETBIOS Dist Srv	NETBIOS Datagram Distribution	[RFC 2132]	√
46	NETBIOS Node Type	NETBIOS Node Type	[RFC 2132]	√
47	NETBIOS Scope	NETBIOS Scope	[RFC 2132]	√
48	X Window Font	X Window Font Server	[RFC 2132]	√
49	X Window Manager	X Window Display Manager	[RFC 2132]	√
50	Address Request	Requested IP Address	[RFC 2132]	√
51	Address Time	IP Address Lease Time	[RFC 2132]	√
52	Overload	Overload "sname" or "file"	[RFC 2132]	√
53	DHCP Msg Type	DHCP Message Type	[RFC 2132]	√
54	DHCP Server Id	DHCP Server Identification	[RFC 2132]	√
55	Parameter List	Parameter Request List	[RFC 2132]	√
56	DHCP Message	DHCP Error Message	[RFC 2132]	√
57	DHCP Max Msg Size	DHCP Maximum Message Size	[RFC 2132]	√
58	Renewal Time	DHCP Renewal (T1) Time	[RFC 2132]	√
59	Rebinding Time	DHCP Rebinding (T2) Time	[RFC 2132]	√
60	Class Id	Class Identifier	[RFC 2132]	√
61	Client Id	Client Identifier	[RFC 2132]	√
62	Netware/IP Domain	Netware/IP Domain Name	[RFC 2242]	√
63	Netware/IP Option	Netware/IP sub Options	[RFC 2242]	√
64	NIS-Domain-Name	NIS+ v3 Client Domain Name	[RFC 2132]	√
65	NIS-Server-Addr	NIS+ v3 Server Addresses	[RFC 2132]	√
66	Server-Name	TFTP Server Name	[RFC 2132]	√
67	Bootfile-Name	Boot File Name	[RFC 2132] [RFC 3396]	√
68	Home-Agent-Addrs	Home Agent Addresses	[RFC 2132]	√
69	SMTP-Server	Simple Mail Server Addresses	[RFC 2132]	√
70	POP3-Server	Post Office Server Addresses	[RFC 2132]	√
71	NNTP-Server	Network News Server Addresses	[RFC 2132]	√

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

Tag	Name	Meaning	Ref	IPWorks
72	WWW-Server	WWW Server Addresses	[RFC 2132]	√
73	Finger-Server	Finger Server Addresses	[RFC 2132]	√
74	IRC-Server	Chat Server Addresses	[RFC 2132]	√
75	StreetTalk-Server	StreetTalk Server Addresses	[RFC 2132]	√
76	STDA-Server	ST Directory Assist. Addresses	[RFC 2132]	√
77	User-Class	User Class Information	[RFC 3004]	√
78	Directory Agent	directory agent information	[RFC 2610]	√
79	Service Scope	service location agent scope	[RFC 2610]	√
81	Client FQDN	Fully Qualified Domain Name	[RFC4702]	√
82	Relay Agent Information	Relay Agent Information	[RFC 3046]	√
85	NDS Servers	Novell Directory Services	[RFC 2241]	√
86	NDS Tree Name	Novell Directory Services	[RFC 2241]	√
87	NDS Context	Novell Directory Services	[RFC 2241]	√
90	Authentication	Authentication	[RFC 3118]	√
98	User-Auth	Open Group's User Authentication	[RFC 2485]	√
118	Subnet Selection Option	Subnet Selection Option	[RFC 3011]	√
119	Domain Search	DNS domain search list	[RFC 3397]	√
120	SIP Servers DHCP Option	SIP Servers DHCP Option	[RFC 3361]	√
121	Classless Static Route Option	Classless Static Route Option	[RFC3442]	√
255	End	None	[RFC 2132]	√

Table 2: IPWorks DHCP Options Support

Table 3 lists the supported sub options of DHCP Option82.

Code	Sub-Option Description	Reference	IPWorks
1	Agent Circuit ID Sub-option	[RFC 3046]	√
2	Agent Remote ID Sub-option	[RFC 3046]	√
5	Link Selection Sub-option	[RFC 3527]	√
6	Subscriber-ID Sub-option	[RFC3993]	√

Table 3: DHCP Option82 Sub Options Support

3.1.1.1 User ID Provisioning

Figure - 8 shows how DHCP/NACF server, DHCP relay agent, and Terminal interact with each other for user ID provisioning.

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

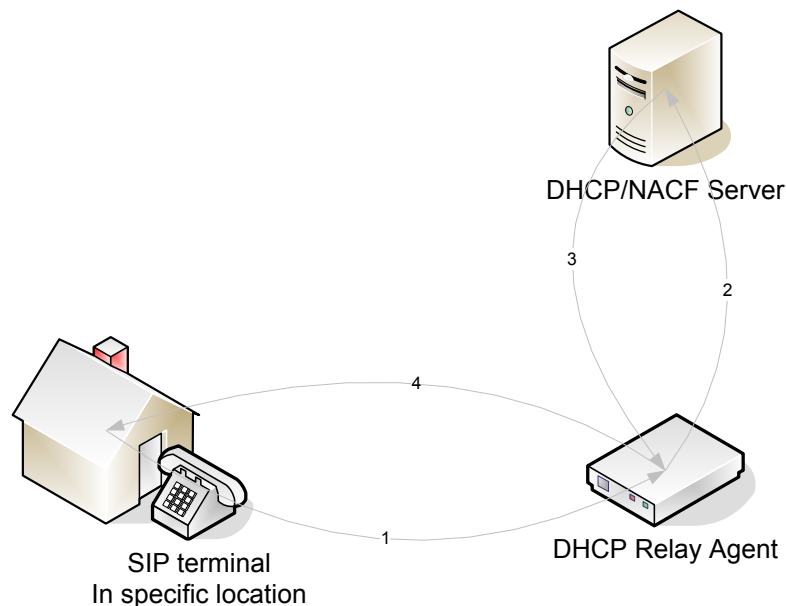


Figure - 8: User ID Provisioning

- 1 SIP terminal issues a request which can be a DHCPDISCOVER to start an IP allocation procedure, or a DHCPREQUEST to renew or rebind IP allocation.
- 2 When DHCP relay agent receives the request, it includes the relay information (Option82 and sub-options) in the request and forward it to DHCP/NACF server.
At this time, the relay agent includes the User ID in sub-option 6 (Subscriber ID).
- 3 If the provision function is enabled, DHCP server can get the User ID information from sub-option and send the User ID information back to DHCP relay agent.
Option between 224 and 254 can be configured to carry the User ID at the server side. If no option is configured to carry User ID, then this function does not work. And the relay information (Option82) returns as same as it received.
- 4 DHCP relay agent (according to RFC 3046) takes away relay information (Option82) and send the rest information back to SIP terminal.

3.1.1.2 P-CSCF Discovery

Figure - 9 shows the message flow among DHCP/NACF server, DHCP relay agent, Home Gateway, and Terminal (notice that Home Gateway and Terminal are in separate box).

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

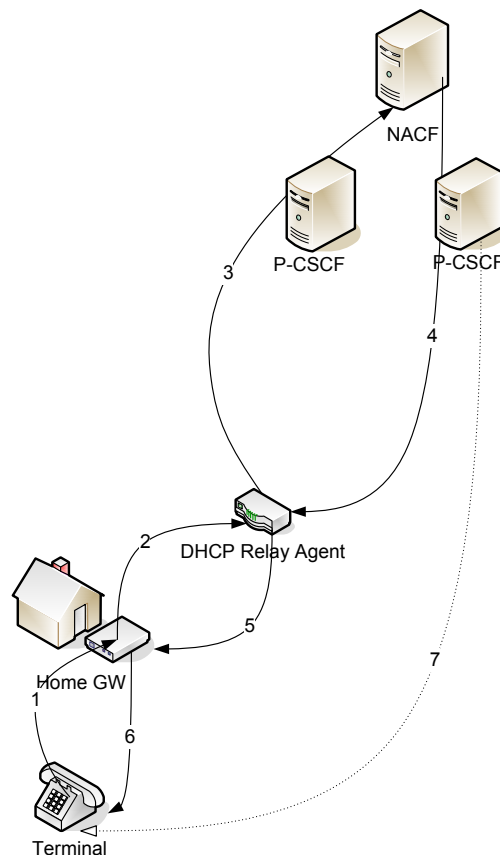


Figure - 9: Message Flow about Fetching P-CSCF via DHCPINFORM

1. Terminal issue DHCP message (Discover/Request) to the Home Gateway.
2. Home Gateway sends DHCPINFORM message to DHCP/NACF. This message requests DHCP/NACF to answer option 120.
3. DHCP relay agent includes relay agent information in DHCPINFORM, then forwards to NACF.
4. DHCP/NACF recognizes the request message, and fetch the SIP server information. Then DHCP sends back the message that includes the address of P-CSCF server by using acknowledge message. DHCP/NACF assigns P-CSCF address base on source IP address and relay agent information.
5. DHCP relay agent takes away relay information and sends the rest information back to Home Gateway.
6. Home Gateway passes the information (option 120) to the terminal, and then the terminal can get the specific P-CSCF address.

The selected P-CSCF server will be used by Terminal.

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

3.1.1.3 ClientClass

With ClientClass, clients are separated into classes and treated differently.. This separation can be done either with a conditional statement, or with a match statement within the class declaration. It is possible to specify a limit on the total number of clients within a particular class or subclass that may hold leases at one time, and it is possible to specify automatic subclass based on the contents of the client packet.

Subclasses can be declared within classes. A subclass is a DHCP policy object that represents the configuration for a subset of the members of a client class.

A spawning class can be declared to automatically produce subclasses based on what the client sends. The reason that spawning classes were created was to make it possible to create lease-limited classes on the fly. The envisioned application is a cable-modem environment where the ISP wishes to provide clients at a particular site with more than one IP address, but does not wish to provide such clients with their own subnet, nor give them an unlimited number of IP addresses from the network segment to which they are connected.

Many cable modem head-end systems can be configured to add a Relay Agent Information option to DHCP packets when relaying them to the DHCP server. These systems typically add a circuit ID or remote ID option that uniquely identifies the customer site.

Refer to [2] for IPWorks DHCPv4 server ClientClass related configuration.

3.1.1.4 User Defined Option

In IPWorks DHCPv4 server, unsupported options can also be configured. Using this option requires the knowledge about numeric tag associated with the option. All standard options in DHCP have a numeric tag associated with them. This tag is the number that is sent in the DHCP packets when the options are sent to a client.

Once the numeric tag is known for the option to be configured, the value for that option can be set by using the custom option. This is a special option that has two arguments, which are separated by white space: the first argument is the numeric tag, the second argument is the value to send to the client. This value must be specified in hex.

3.1.1.5 Authentication

In IPWorks, the operator needs to configure each client with a unique key on a DHCP server. These keys are the shared secrets between DHCP clients & servers. These keys are stored in the dhcpkey.conf file that is uploaded to the DHCP configuration directory.

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

Thus, each client has a unique authentication key and the authentication mechanism (delayed authentication) is as per RFC 3118 in DHCPv4.

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

The server, has three settings, called Authentication Levels (0-2):

- 0: Unsupported authentication
- 1: Mandatory authentication
- 2: Optional authentication

Unsupported Authentication

When the authentication level is set to 0, the server does not support authentication at all. That means, the server responds with unauthenticated messages irrespective of whether the client uses authentication option or not. Listed below are the scenes:

- If the client sends unauthenticated DHCP message, the server responds with unauthenticated message.
- If the client sends DHCP message with invalid authentication option, the server ignores the option and responds with unauthenticated message.
- If the client sends DHCP message with valid authentication option, the server still ignores the option and respond with unauthenticated message.

If the client needs authentication, then a configuration of Authentication Levels 0 is not appropriate. Because the server does not check for authentication and reverts with an unauthenticated message. In this case, the client receives an unauthenticated response, which can be interpreted as either the server does not support authentication, or the authentication failed.

Mandatory Authentication

When the authentication level is set to 1, all the clients need to have their authenticity validation passed by the server. The client-server communication modes and corresponding server behaviors are as follows:

- If the client sends unauthenticated DHCP message, the server drops the packet and does not respond.
- If the client sends DHCP message with invalid authentication option, the server drops the packet and does not respond.

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

- If the client sends DHCP message with valid authentication option, the server responds with authenticated message.

In this case, a client with authentication option can conclude from the server response (or lack of response), that the authentication is failed. If the client does not include the authentication option and receives no response, then it can be concluded that authentication is mandatory on this server.

Optional Authentication

When the authentication level is set to 2, the server handles all messages. It responds to client requests in two different ways based on 2 scenarios as below:

- If the client request includes the authentication option and the authentication is successful, the server sends an authenticated response.
- If the client request does not include the authentication option, or authentication fails, the server returns an unauthenticated message.

In optional authentication, the client is sure of the server authentication level only when the message from server includes the authentication option. In response:

- The client receives an authenticated response upon successful authentication.
- The client receives an unauthenticated response and determine the authentication failed.
- When authentication is optional, if the client does not include the authentication option, the server preference about authentication is unknown.

If a `dhcpkey.conf` file is available at the time of starting up the server, the server reads it irrespective of the Authentication level set in the ECLI. The reading (or loading) of the keys depends on the file being available; not on the ECLI setting. This is because, the setting can be changed at runtime.

If no authentication file is available (that is, it was not uploaded from the CLI during DHCP configuration update), then the server logs an error and starts up. This is not the case with the `dhcpd.conf` file: if that is missing, the server does not start up.

This distinction is important because it can lead to a situation where authentication is required but the `dhcpkey.conf` file is not available.

The operator must ensure that when the authentication level is 1 or 2, `dhcpkey.conf` file is in the configuration directory. Otherwise, the authentication fails.

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

3.1.1.6 Dynamic Reconfiguration

When changes are made to the DHCPv4 server, the client leases should be renewed with new configuration information. The “reconfig” command is used by the server to notify clients about configuration changes, including address range changes. DHCPv4 reconfiguration is based on RFC 3203.

The “reconfig” command instructs the server to unicast a FORCERENEW message to the clients, and instructs the clients to renew their leases. When the clients receive these messages, they request for lease renewal instantly. Only the clients that were served before the server shutdown and their leases are active after the server restart will receive this message.

To apply reconfiguration, the server needs to stop and restart after changing the configuration. For example, a client's lease is active until 21:00. The server is configured at 20:30, and restarts at 21:10. Then no message is sent to the client. If a client's lease expired at 20:25, before the server reconfiguration at 20:30, then the lease is not renewed.

The client is updated with the changes in configuration when the lease is renewed. Retransmission of the FORCERENEW command is attempted 3 times.

3.1.2 DHCPv4 DDNS Function

With DHCP, Internet addresses are dynamically assigned to clients. These addresses and the associated client's name are dynamically registered to DNS. The IPWorks DHCP server supports the DDNS update. The most effective way to use DDNS updates is to create a new zone and use only dynamic updates to create the resource records in that zone.

The IPWorks DHCP server can be configured to use TSIG transaction security in conjunction with dynamic updates to a TSIG enabled DNS server, such as an IPWorks DNS Server. To enable this feature, the secure-ddns option is configured (set to true). Then the TSIGKey used for the DNS Server should be created by creating a DnsContact object. A DnsContact is an object that defines the information using in contacting a DNS server. The server that is being contacted does not need to be an IPWorks managed server.

Refer to [14] for DHCPv4 DDNS IETF specifications and [2] for IPWorks DHCPv4 server DDNS configuration.

3.1.3 DHCPv4 Failover and Load Balancing Function

The DHCPv4 failover protocol provides synchronization between the two servers. So when one server is failed or become unreachable, the other can take over. And the servers need to coordinate all lease activity to maintain the lease database in case of failover. One server is designated as the "primary" server, the other is the "secondary" server. They provide both redundancy and load balance via integrating the failover protocol with the DHCP load balancing approach.

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

The failover configuration provides redundancy, high availability, and has no limit of multiple independent servers. The available address pool is dynamically synchronized between the two servers. So when one server is down, the other server still has all shared address.

Generally, each failover partner responds to a client subset. When a server assigns a new lease to a client, it first gives a lease for the length of time specified by MCLT (defined by option failover-mclt which is much less than the normal lease time) and sends lease information to its partner. After both servers negotiate successfully, the server will give the client a lease with the desired lease interval when the client renews its lease next time (see Figure - 10 for the flow). Then each server sends updates about its leasing activities to the partner. In this way two copies of the lease database are maintained, and each server has up-to-date information. Also, during normal operation, the servers work to distribute the available addresses (addresses not leased to clients) between them.

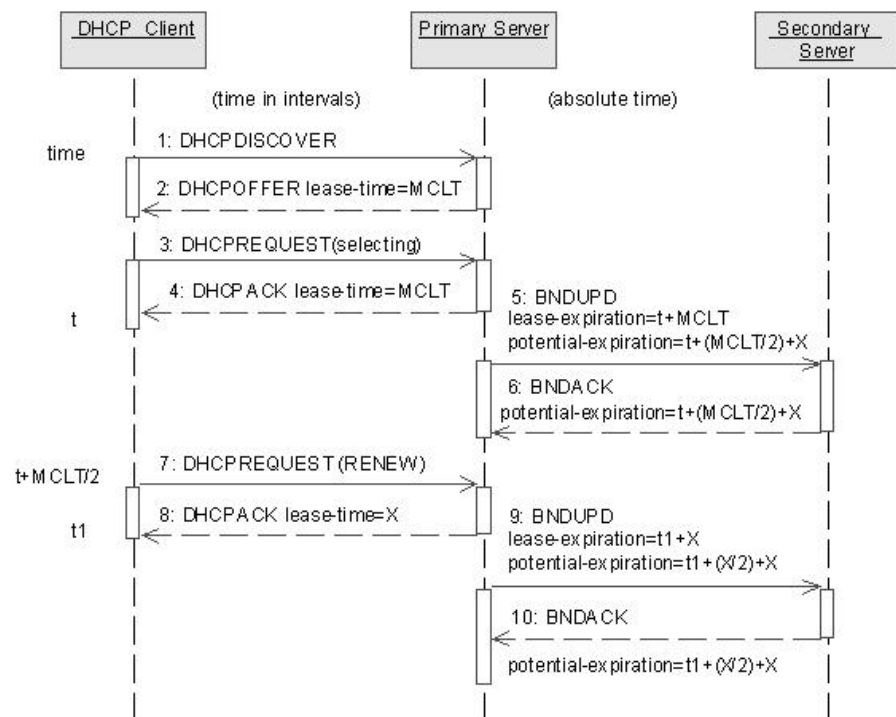


Figure - 11: DHCPv4 Server Failover Update Message Traffic

If one of the servers goes offline, the remaining server takes over all leasing activity, issues new leases and renews existing leases. Each server has an available portion of the distributed addresses to assign to new clients. Existing clients can continue to renew the leases on the assigned addresses by either server. Once the offline server returns, the remaining server updates all the lease activities with the return one. So both have up-to-date information. The servers also redistribute the available addresses.

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

If a network element fails and disables communication between the two servers, each starts servicing all clients (new and renewal requests). Each server has a portion of the available addresses that can be assigned to new clients, and each can continue to renew leases on addresses previously leased by either server. Once the network is repaired and communication resumes, the servers update the lease activities with each other and return to normal.

There are three aspects about the two servers handle leases and their communication that makes up failover protocol:

- An expired or renewed lease is not assigned to a new client until both servers have placed the address in an available state by exchanging messages.
- Each server allocates addresses for new leases from separate address pools. The server periodically redistributes the available addresses between them, based on leasing activity.
- All new leases have a relatively short fixed time, called the maximum client lease time (MCLT), until the desired lease time is successfully negotiated between both servers. Renewals use the full desired lease time once both servers are able to negotiate the desired lease time.

Failover also provides a mechanism for the remaining server to take over all addresses when the offline server is unavailable for an extended period of time. This is called partner-down mode. While in partner-down mode, the server runs as if it were running standalone, and periodically checks if the partner server is online. This means, the server - after the MCLT has expired - own the entire lease pool and does not need to negotiate with the offline server for lease times.

Refer to [21] and [22] for IETF DHCPv4 load balance and failover specifications.

Each server can extend leases given out by the other server.

Load balancing allows each failover server that is in normal communication to process a subset of the clients. Load balancing is disabled when the servers are not in communication, since the other server can be down or the network can be disconnected.

The failover pair is able to initiate an IP resource pool rebalance procedure. Pool rebalance events can happen on schedule and/or the pool is severely misbalanced in the peer's favor.

In IPWorks as an enhancement towards failover protocol, leases that belong to secondary server is possible to be moved to BACKUP state rather than FREE upon existing EXPIRED state.

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

The IPWorks DHCPv4 servers can also be part of a server farm. A load balancing mechanism is implemented in the IPWorks DHCPv4 servers, which can balance the load between two DHCP servers or between DHCP failover pairs

Load balancing is implemented on the server level, which means if the server is a part of a failover pair, that pair have the same hash mask (HBA) to handle. When starting up a server and there is no server-level HBA, one HBA is created and each bit of the HBA is default set to "1".

Figure - 12 shows a server farm concept is sharing the load (50 percent) between two failover pairs. The mask for load balancing (ghba) is on the top of the DHCP Primary server in both DHCP1 and DHCP2. In the Failover pair is the Failover load balancing (lbhba) active, which can be seen in the respective DHCP Primary and Secondary.

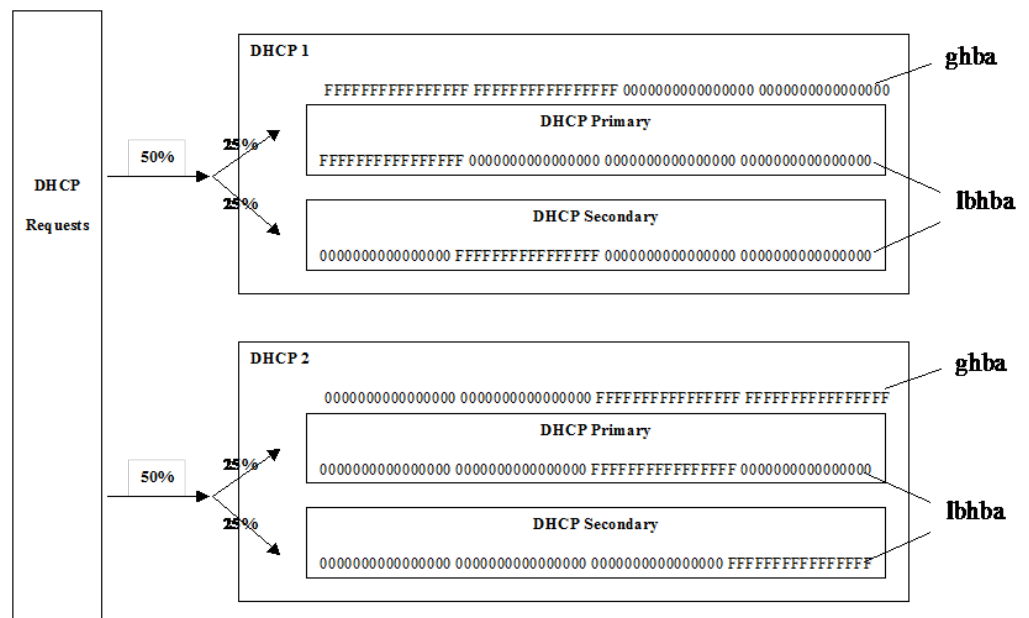


Figure - 13: Load balance between two DHCPv4 failover pairs

3.1.4

Support for Overlapped IP address ranges

In IPWorks, the operator can specify the lease pools (IP address ranges) with partial or total overlapping of the IP addresses. But it can lead to a conflict when multiple network elements from a given address space are served by the DHCPv4 server with the same IP address (from different pools with overlapped address ranges). In IPWorks DHCPv4 server, the pools with overlapped IP address ranges are uniquely available for a given address space via configuring different ClientClass (refer to section 3.1.1.3) for different IP lease pools.

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

ClientClass classifies the clients and specifies a pool to serve the clients of particular class. Meanwhile, it avoids all the other pools with overlapped address range serving this client class. This is the only way to avoid collision in IP address assignment while dealing with duplicated address range.

For failover protocol, the overlapped IP addresses are shared between the Primary and Secondary servers like other non-overlapped IP addresses, and stored in the way described above.

Dynamic updates to DNS server (with PTR and/or A record) is done with the existing data from the DHCPv4 server. This is possible because even for the overlapped IP addresses, the A record and the PTR records have the same IP address but different domain names. And DNS server is able to store them independently. The queries to DNS server are made with the domain names (URL) which are different from each client. But as the queries for PTR records are made by specifying the IP addresses, and the IP addresses are duplicated / overlapped, so there are multiple PTR records in the DNS zone database with same IP address. Hence, a query to DNS server for PTR record with single IP address can have a feedback with multiple domain names. The operator needs to pick up the correct domain.

3.2 TISPAN NASS NACF Function

3.2.1.1 General Description

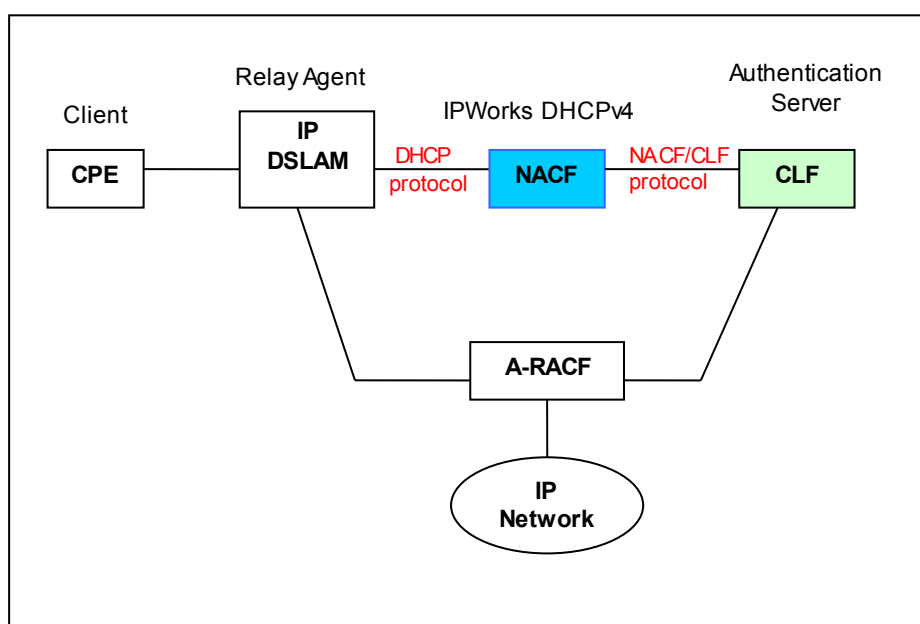


Figure - 14: DHCPv4 Server Works as NACF Server

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

The Network Access Configuration Function (NACF) is a DHCPv4 server that interacts with another network element called Connectivity Session Location Function (CLF). This interface is to exchange the binding information of the IP address exchanges allocated to the Customer Premises Equipment (CPE) and the network location information provided by the NACF. Each IP addressing zone contains multiple topology zones. CPEs across the topology zones are connected to NACF through routers. And each topology zone maintains its own router.

NACF and CLF communicate over a TCP connection where NACF acts as TCP client and CLF as the TCP server. During start-up, NACF initiates the connection towards CLF. If CLF is available, it accepts the connection and thus a TCP link established between these NACF and CLF. However, CLF cannot be activated or deactivated during server's run-time. If the user needs to change the states of CLF, the server must be rebooted.

Once the connection is established, NACF and CLF start exchanging heart beat messages to ensure the integrity of the link. NACF is the sender of the heart beat messages, and CLF, as receiver, acknowledges the reception of the same to NACF. NACF periodically transmits the heart beat messages as long as the interface exists.

3.2.1.2 Communication Protocol Between IPWorks DHCPv4 Server (NACF) and CLF

This protocol between the NACF and the CLF follows a client/server model in which 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 the communication is non-blocking when the CLF and the NACF are processing the requests from other CPEs.

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

For detailed description about the communication protocol, refer to [7].

3.2.1.3 Flexible Option82

Usually, there are DHCP relay agent equipment from many vendors. And every vendor has their own format definition for the information contained in suboptions of DHCP Option82. NACF needs to be able to parse the information required by CLF from option 82.

IPWorks DHCPv4 server offers a flexible mechanism to extract the input data stream from Option82 based on the predefined input formats of virtual circuits or physical links. And convert the CLID or Remoteld to the new one based on the predefined output formats. Then the reformatted CLID or Remoteld are sent to CLF.

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

It is configurable to build remote ID or circuit ID for CLF from sub option of option 82.

IPWorks DHCPv4 NACF function supports parsing of ASCII characters set.

IPWorks DHCPv4 NACF function supports parsing of bit stream.

IPWorks DHCPv4 NACF function handles Option82 from different types of DHCP relay agent using different parsing rules.

3.3 DHCPv4 IPWorks OAM Implementation

3.3.1 DHCPv4 CLI/Server Manager Support Function

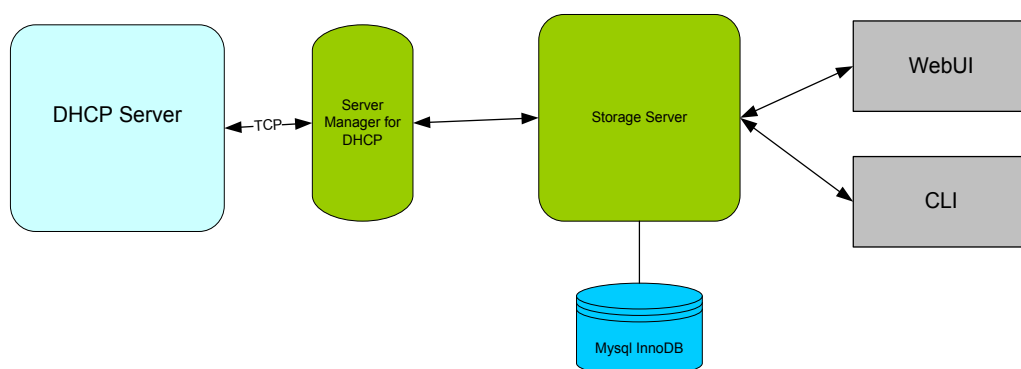


Figure - 15: DHCPv4 Server Integration with Server Manager

The IPWorks DHCPv4 server and Server Manager communicate with non-blocking messages. When the IPWorks DHCPv4 server starts, it sends a message to the Server Manager. The Server Manager then retrieves the current configuration information from the Storage Server (SS) if available. The Server Manager places this information in ASCII based configuration files on the IPWorks DHCPv4 server's local file system. If the SS is not available or cannot retrieve the configuration, an error is logged and the DHCPv4 server loads the previous configuration.

The SS stores only static configuration information, to minimize management traffic and to reduce the number of transient entries in the database. The IPWorks DHCPv4 server stores all dynamic DHCP lease information locally. The SS can retrieve real-time lease information for export, reporting or viewing from one of the IPWorks user interfaces.

A TCP connection is used for the Server Manager to DHCP communication. The DHCPv4 server listens on a port on the loopback address and the SM establishes a TCP connection. The port value is 34464.

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

When a TCP connection is first established, the Sever Manager sends a request to the server either use SSL or not. The DHCPv4 server responds with one byte indicating no SSL. The following messages are then exchanged over the TCP connection without SSL.

3.4 DHCPv4 IPWorks OAM Implementation

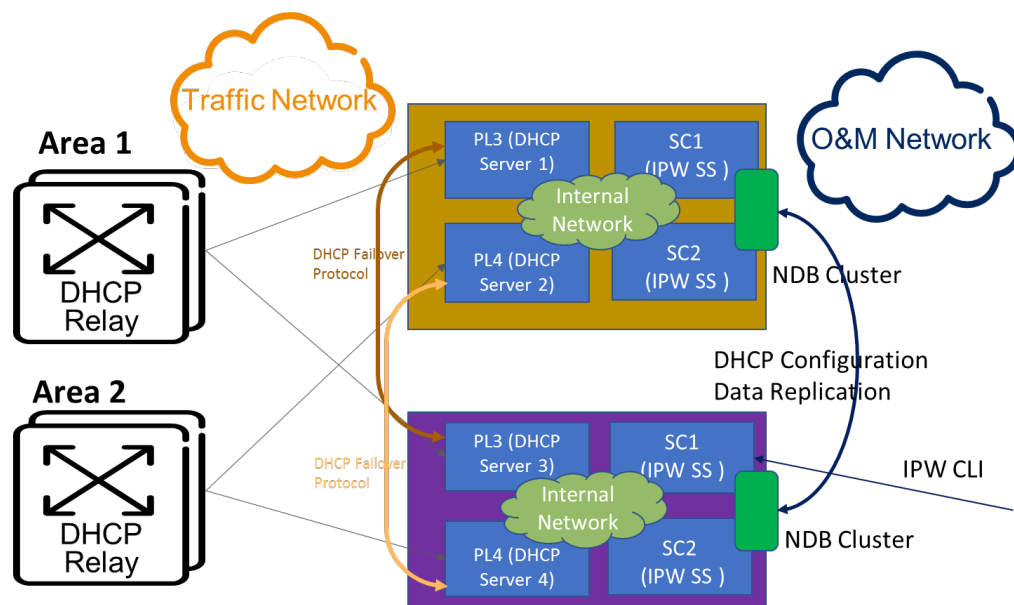


Figure 15: DHCPv4 Geographic Redundancy

- Configuration could be performed at any of the two sites which participated the geographic redundancy deployment. Configuration data can be automatically replicated to another site.
- Operations as "update", "show status", and "partnerdown" should be performed at the site which the destination DHCP server resides. See section 3.3.1 for the CLI/SM Support Function.

4 Operational Conditions

4.1 Configurable Parameters

DHCP server can be configured through IPWorks CLI and ECLI. Refer to [2] and [4] for detailed information.

4.2 Commands and User Procedures

Refer to [2] and [3] for IPWorks CLI commands about DHCPv4 server.

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

4.3 Charging

-

4.4 Characteristics

-

5 Statement of Compliance

RFC Number	RFC Name	Statement of Compliance	Comments
RFC951	BOOTSTRAP PROTOCOL	FC	
RFC1542	Clarifications and Extensions for the Bootstrap Protocol	FC	
RFC1534	Interoperation Between DHCP and BOOTP	FC	
RFC2131	Dynamic Host Configuration Protocol	FC	
RFC3203	DHCP reconfigure extension	FC	
RFC2132	DHCP Options and BOOTP Vendor Extensions	FC	
RFC3396	Encoding Long Options in the Dynamic Host Configuration Protocol	FC	
RFC2242	NetWare/IP Domain Name and Information	FC	
RFC3004	The User Class Option for DHCP	NC	
RFC2610	DHCP Options for Service Location Protocol	FC	
RFC3046	DHCP Relay Agent Information Option	FC	
RFC2241	DHCP Options for Novell Directory Services	FC	
RFC3118	Authentication for DHCP Messages	FC	
RFC4388	Dynamic Host Configuration Protocol (DHCP) Leasequery	NC	
RFC2485	DHCP Option for The Open Group's User Authentication Protocol	FC	
RFC2937	The Name Service Search Option for DHCP	NC	
RFC3011	The IPv4 Subnet Selection Option for DHCP	FC	
RFC3397	Dynamic Host Configuration Protocol (DHCP) Domain Search Option	FC	
RFC3361	Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers	FC	
RFC3925	Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)	FC	
RFC3074	DHC Load Balancing Algorithm	FC	
RFC 3527	Link Selection sub-option for the Relay Agent Information Option for DHCPv4	FC	
RFC 3993	Subscriber-ID Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option	FC	
RFC 4701	A DNS Resource Record (RR) for Encoding Dynamic Host Configuration Protocol (DHCP) Information (DHCID RR)	FC	
RFC 4702	The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option	FC	
RFC 4703	Resolution of Fully Qualified Domain Name (FQDN) Conflicts among Dynamic Host Configuration	FC	

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

	Protocol (DHCP) Clients		
draft-ietf-dhc-failover-12	DHCP Failover Protocol	FC	Load Balance algorithm has been improved.

6 Miscellaneous

7 Terminology

7.1 Abbreviations

<Abbr>	<Explanation>
CPE	Customer Premises Equipment
DSLAM	Digital Subscriber Line Access Manager
NACF	Network Access Configuration Function
A-RACF	Access Resource and Admission Control Function
CLF	Connectivity Session Location Function
CLID	Calling Line Identification
DDNS	Dynamic Domain Name System
CP	Control Panel

7.2 Definitions

Primary Server	A DHCP server configured to provide primary service to a set of DHCP clients for a particular set of subnet address pools.
Secondary Server	A DHCP server configured to act as backup to a primary server for a particular set of subnet address pools.
HBA	Hash Bucket Assignments

8 References

[1]	The DHCP Handbook second edition	ISBN 0-672-32327-3	
[2]	IPWorks Configuration Management	6/1551-AVA 901 33/3	C
[3]	Command Line Interface	2/1553-AVA 901 33/3	B

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

User Guide for IPWorks SS

[4]	Ericsson Command-Line Interface User Guide	6/1553-CAA 901 2587/7	B
[5]	IPWorks CLF NACF a2 Interface	43/155 19-AVA 901 16	A
[6]	Bootstrap Protocol	RFC 951	
[7]	Interoperation Between DHCP and BOOTP	RFC 1534	
[8]	Clarifications and Extensions for the Bootstrap Protocol	RFC 1542	
[9]	Dynamic Host Configuration Protocol	RFC 2131	
[10]	DHCP Options and BOOTP Vendor Extensions	RFC 2132	
[11]	Dynamic Updates in the Domain Name System (DNS UPDATE)	RFC 2136	
[12]	DHCP Options for Service Location Protocol	RFC 2610	
[13]	The User Class Option for DHCP	RFC 3004	
[14]	The IPv4 Subnet Selection Option for DHCP	RFC 3011	
[15]	DHCP Relay Agent Information Option	RFC 3046	
[16]	Authentication for DHCP Messages	RFC 3118	
[17]	DHCP reconfigure extension	RFC 3203	
[18]	Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers	RFC 3361	
[19]	Encoding Long Options in	RFC 3396	

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

the Dynamic Host
Configuration Protocol
(DHCPv4)

- [20] DHC Load Balancing Algorithm RFC 3074
- [21] DHCP Failover Protocol draft-ietf-dhc-failover-12.txt
- [22] The DHCP Client FQDN Option draft-ietf-dhc-fqdn-option-13.txt
- [23] Resolution of FQDN Conflicts among DHCP Clients draft-ietf-dhc-ddns-resolution-12.txt
- [24] A DNS RR for Encoding DHCP Information (DHCID RR) draft-ietf-dnsext-dhcid-rr-13.txt
- [25] The DOCSIS (Data-Over-Cable Service Interface Specifications) Device Class DHCP (Dynamic Host Configuration Protocol) Relay Agent Information Sub-option RFC 3256
- [26] DHCP Options for Novell Directory Services RFC 2241
- [27] NetWare/IP Domain Name and Information RFC 2242
- [28] DHCP Option for The Open Group's User Authentication Protocol RFC 2485
- [29] The Name Service Search Option for DHCP RFC 2937
- [30] Dynamic Host Configuration Protocol (DHCP) Domain Search Option RFC 3397
- [31] Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4) RFC 3925
- [32] Dynamic Host RFC 4388

Prepared (also subject responsible if other) EZAIYUA		No. 56/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-09-19	Rev D	Reference

Configuration Protocol
(DHCP) Leasequery