rfc3315

DHCPv6

Ce document décrit DHCP pour IPv6, un protocole client/serveur qui fournis une configuration gérée de périphériques.

DHCP peut fournir un périphérique avec des adresses assignées par un serveur DHCP et des informations de configuration, qui sont gérés dans des options. DHCP peut être étendu via la définition de nouvelles options pour gérer les informations de configuration non spécifiées dans ce document.

DHCP est un protocole d'auto-configuration d'adresse à état et let protocole d'auto-configuration à été référré dans la rfc4862.

Les modèles opérationnels et les informations de configuration pour DHCPv4 et DHCPv6 sont suffisamment différents pour que l'intégration entre les 2 services ne soient pas inclus dans ce document.

Protocoles et adressage

Les clients et les serveurs échangent des messages DHCP en utilisant UDP. Le client utilise une adresse de lien-local ou les adresses déterminées via d'autres mécanismes pour transmettre et reçevoir les messages DHCP.

Les serveurs DHCP reçoivent des messages des clients en utilisant une adresse multicast link-scoped. Un client DHCP transmet la plupart des messages à cette adresse multicast réservée, donc ce client n'a pas besoin d'être configuré avec l'adresse des servers DHCP.

Pour autoriser un client DHCP à envoyer un message à un serveur DHCP qui n'est pas attaché au même lien, un relasi DHCP sur le lien du client va relayer les messages.

Une fois que le client a déterminé l'adresse d'un serveur, il peut envoyer les messages directement au serveur en utilisant l'unicast.

Les échanges client-serveur impliquant 2 messages

Quand un client DHCP n'a pas besoin qu'un serveur DHCP lui assigne ses adresses IP, le client peut obtenir des informations de configuration tel qu'une liste de serveurs DNS ou NTP disponibles via un simple échange de message avec le serveur DHCP. Pour obtenir des informations de configuration le client envoie d'abord un message Information-Request à l'adresse multicast All_DHCP_Relay_Agents_and_Servers. Les serveurs répondent avec un message Reply contenant la configuration pour le client.

Cet échange assume que le client ne demande que des informations de configuration et non d'adresses IPv6.

Quand un serveur a des adresses IPv6 et d'autres informations de configuration envoyés à un client, le client et le serveur sont capable d'échanger en utilisant seulement 2 messages, au lieu de 4 comme décris dans la section suivante. Dans ce cas, le client envoie un message Solicit à All_DHCP_Relay_Agents_and_Servers demandant l'assignement des adresses et autres informations de configuration. Ce message inclus une indication que le client accepte un message de réponse immédiat du serveur. Le serveur qui est prêt à envoyer l'assignement d'adresses au client répond immédiatement. Les informations de configuration et les adresses dans la réponse sont ainsi immédiatement disponibles au client.

Chaque adresse assignée au clien a une durée de vie préféré et valide spécifié par le serveur. Pour demander une extension de durée, le client envoie un message Renew au serveur. Le serveur envoye un Reply au client avec la nouvelle durée de vie.

Les échanges client-serveur impliquant 4 messages

Pour demander l'assignement d'une ou plusieurs adresses IPv6, un client localise d'abord un serveur DHCP, puis lui demande l'assignement des adresses et autres informations de configuration. Le client envoie un message Solicit à l'adresse All_DHCP_Relay_Agents_and_Servers pour trouver les serveurs DHCP disponibles. Tout serveur qui répond aux exigences du client répondent avec un message Advertise. Le client choisis ensuite un des serveurs et envoie un message Request au serveur demandant la confirmation de l'assignement. Le serveur répond avec un message Reply qui contient les adresses confirmées et la configuration.

Terminologie DHCP

Approprié au lien Une adresse est approprié au lien quand l'adresse est consistante avec la connaissance du serveur DHCP de la topologie réseau, de l'assignement de préfixe et des stratégies d'assignement d'adresse.

binding Un binding est un groupe d'enregistrement de données serveur contenant les informations du serveur sur les adresses dans un IA ou les informations de configuration explicites assignées au client. Ces informations de configuration qui sont retournées au client via une stratégie ne nécessitent pas de liaison. Une liaison contenant des informations sur un IA est indexé par le triplet <DUID,IA-type, IAID>

Paramètre de configuration Un élément du jeu d'informations de configuration dans le serveur et délivré au client en utilisant DHCP.

DHCP domain Un jeu de liens gérés par DHCP et opéré par une simple entité administrative

DHCP realm Un nom utilisé pour identifier le domain administratif DHCP pour lequel une clé d'authentification DHCP a été sélectionnée

DUID Un DHCP Unique IDentifier pour un participant DHCP. Chaque client et serveur DHCP a exactement un DUID.

Identity Association (IA) Une collection d'adresses assignées à un client. Chaque IA a un IAID associé. Un client peut avoir plus d'un IA assigné ; par exemple, une pour chacune de ses interfaces.

Identity association identifier (IAID) Un identifiant pour un IA choisis par le client. Chaque IA a un IAID unique.

Identity association for non-temporary addresses (IA_NA) Un IA qui gère les adresses assignée qui ne sont pas des adresses temporaire

Identity association for temporary addresses (IA_TA) Un IA qui gères les adresses temporaires

Reconfigure key Une clé fournie à un client par un serveur utilisé pour fournir une sécurité pour les messages Reconfigure

transaction ID Une valeur opaque utilisée pour correspondre aux réponses avec les réponses initiées soit par un client soit par un serveur

Adresses Multicast

DHCP utilise les adresses multicast suivantes :

All_DHCP_Relay_Agents_and_Servers (FF02 : :1 :2) Une adresse multicast utilisée par un client pour communiquer avec les serveurs et agents relais du voisinage

All_DHCP_Servers (FF05 : :1 :3) Une adresse multicast utilisée par un agent relais pour communiquer avec les serveurs, soit pour envoyer des messages à tous les serveurs, soit parce qu'il ne connaît pas les adresses unicast des serveurs.

Ports UDP

Les clients écoutent les messages UDP sur le port 546. Les serveurs et agents relais écoutent sur le port UDP 547.

Types de messages DHCP

DHCP définis les types de messages suivants :

SOLICIT(1) Un client envoie un message Solicit pour localiser les serveurs

ADVERTISE(2) Un serveur envoie un message Advertise pour indiquer qu'il est disponible pour les services DHCP, en réponse à un message Solicit.

REQUEST(3) Un client envoie un message Request pour demander des paramètres de configuration, incluant des adresses IP, à un serveur spécifique.

CONFIRM(4) Un client envoie un message Confirm aux serveurs disponible pour déterminer si les adresse qui lui ont été assignées sont appropriées au lien sur lequel le client est connecté.

RENEW(5) Un client envoie un message Renew au serveur qui lui a fournis les adresses et paramètres de configuration pour renouveler son bail et mettre à jours d'autres paramètres de configuration.

REBIND(6) Un client envoie un message Rebind aux serveurs DHCP pour étendre la durée de vie des adresses assignées et mettre à jours d'autres paramètres de configuration. Ce message est envoyé quand un client n'a pas reçu de réponse à un message Renew

REPLY(7) Un serveur envoie un message Reply contenant les adresses assignée et les paramètres de configuration en réponse à un message du client.

RELEASE(8) Un client envoie un message Release au serveur pour pour indiquer que le client n'utilise plus une ou plusieurs adresses assignées.

DECLINE(9) Un client envoie un message Decline au serveur pour indiquer qu'une ou plusieurs adresse assignée sont déjà utilisées sur le lien.

RECONFIGURE(10) Un serveur envoie un message Reconfigure à un client pour informer le client que le serveur a de nouveaux paramètres de configuration, ou une mises à jours de ceux-ci, et que le client doit initier un Renew/Reply, ou Information-request/Reply.

INFORMATION-REQUEST(11) Un client envoie un message Information-request à un serveur pour demander les paramètres de configuration sans l'assignement d'adresses IP au client.

RELAY-FORW(12) Un agent relay envoie un message Relay-forward pour relayer les messages au serveurs. Le message reçu est encapsulé dans une option dans le messages Relay-forward

RELAY-REPL(13) Un serveur envoie un message Relay-reply pour relayer les messages à un client. Le messages client est encapsulé dans une option dans le message Relay-reply.

Codes de status

DHCPv6 utilise des codes de status pour communiquer le résultat des opérations demandées, et pour fournir des informations additionnelles sur la cause spécifique de l'erreur d'un message.

Paramètres de transmission et retransmission

Cette table de valeur est utilisée pour décrire le comportement de transmission de message des clients et serveurs :

```
Parameter_____Default_____Description
-------------------------
SOL_MAX_DELAY_____1 sec___Max delay of first Solicit
SOL_TIMEOUT_______1 sec___Initial Solicit timeout
SOL_MAX_RT______120 secs__Max Solicit timeout value
REQ_TIMEOUT_______1 sec___Initial Request timeout
REQ_MAX_RT_______30 secs__Max Request timeout value
REQ_MAX_RC_______10 ______Max Request retry attempts
CNF_MAX_DELAY_____1 sec___Max delay of first Confirm
CNF_TIMEOUT_______1 sec___Initial Confirm timeout
CNF_MAX_RT________4 secs__Max Confirm timeout
CNF_MAX_RD_______10 secs__Max Confirm duration
```

```
REN_TIMEOUT______10 secs__Initial Renew timeout
REN_MAX_RT______600 secs__Max Renew timeout value
REB_TIMEOUT______10 secs__Initial Rebind timeout
REB_MAX_RT______600 secs__Max Rebind timeout value
INF_MAX_DELAY_____1 sec___Max delay of first Information-request
INF_TIMEOUT_______1 sec___Initial Information-request timeout
INF_MAX_RT______120 secs__Max Information-request timeout value
REL_TIMEOUT_______1 sec___Initial Release timeout
REL_MAX_RC________5 ______MAX Release attempts
DEC_TIMEOUT_______1 sec___Initial Decline timeout
DEC_MAX_RC________5 ______Max Decline attempts
REC_TIMEOUT_______2 secs__Initial Reconfigure timeout
REC_MAX_RC________8 ______Max Reconfigure attempts
HOP_COUNT_LIMIT__32 ______Max hop count in a Relay-forward message
```

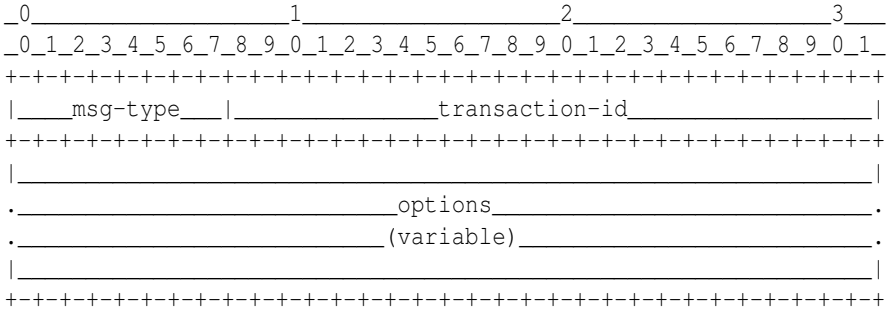
Représentation des valeurs de temps et Infinity

Toutes les valeurs de temp pour les durées de vie, T1 et T2 sont des entiers non-signés. La valeur 0xffffffff signifie infinis.

Formats de message client/serveur

Tous les messages DHCP envoyés entre clients et serveurs partagent un format d'en-tête identique et une zone variable pour les options.

Les options sont stockées en série dans le champ options, sans padding entre les options. Les options sont alignées à l'octet.



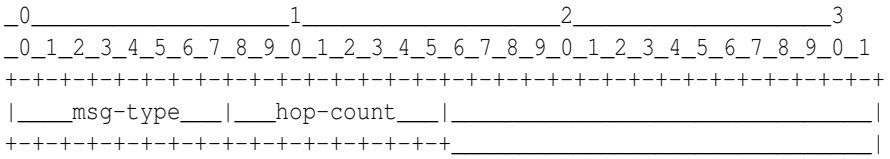
msg-type Identifie le type de message DHCP

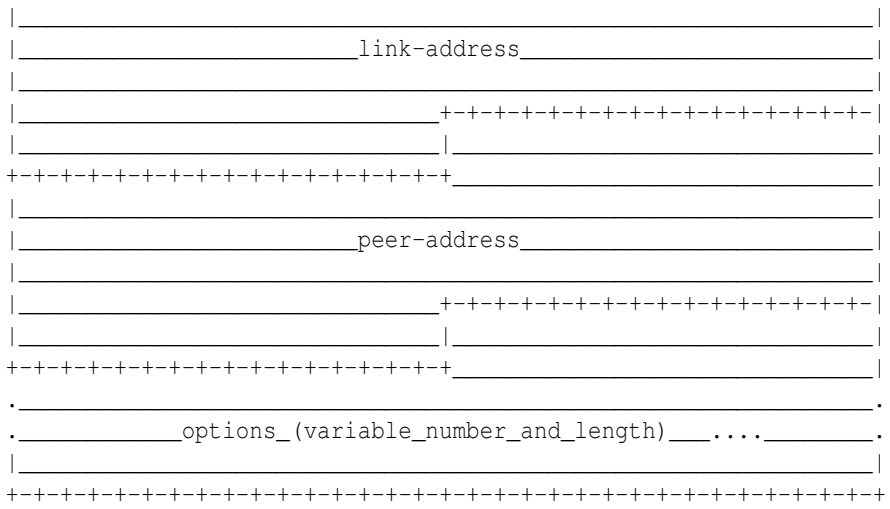
transaction-id L'id de transaction pour cet échange

options Les options dans ce message

Formats de message serveur/agent relais

Les agents relais échangent des messages avec les serveurs pour rejouer les messages entre les clients et les serveurs qui ne sont pas connectés sur le même lien.





Message Relay-forward

msg-type RELAY-FORW

hop-count nombre d'agents relais qui ont relayé ce message

link-address Une adresse globale ou site-local qui sera utilisé par le serveur pour identifier le lien sur lequel le client est localisé

peer-address L'adresse du client ou de l'agent relais depuis lequel le message à relayé a été reçu

options Doit inclure l'option "Relay Message option", et peut inclure d'autres options ajoutées par l'agent relais.

Message Relay-reply

msg-type RELAY-REPL

hop-count Copié depuis le message Relay-forward

link-adress Copié depuis le message Relay-forward

peer-address Copié depuis le message Relay-forward

options Doit inclure l'option "Relay Message option"

Représentation et utilisation des noms de domaine

Un nom de domaine ou une liste de noms de domaine est encodé en utilisant la technique décrite dans la section 3.1 de la rfc1035. Un nom de domaine ne doit pas être stocké sous la forme compressée dans DHCP.

DHCP Unique IDentifier

Chaque client et serveur DHCP a un DUID. Les serveurs DHCP utilisent les DUID pour identifier les clients pour la sélection des paramètres et dans l'association des IA avec les client. Les clients DHCP utilisent les DUID pour identifier un serveur dans les messages où un serveur doit être identifié.

Les clients et serveurs doivent traiter les DUID comme valeurs opaques et doivent seulement comparer les DUID. Les clients et serveurs ne doivent pas interpréter les DUID d'une autre manière. Les clients et serveurs ne doivent pas restreindre les DUID aux types définis dans ce document, vu que d'autres types de DUID peuvent être définis dans le future.

Le DUID est géré dans une option parce qu'il peut être de longueur variable et parce qu'il n'est pas requis dans tous les messages DHCP. Le DUID est conçus pour être unique entre tous les clients/serveurs, et stable pour un client ou un serveur, et ne devrait pas changer dans le temps si c'est possible.

La motivation pour avoir plus d'un type de DUID est que le DUID doit être globalement unique, et doit également être facile à générer. Le trie de l'identifiant globalement unique qui est simple à générer pour un périphérique qui peut différer. Également, certains périphériques peuvent ne pas contenir de stockage persistant, et retenir un DUID généré n'est pas possible, donc le schéma DUID doit s'adapter à de tels périphériques.

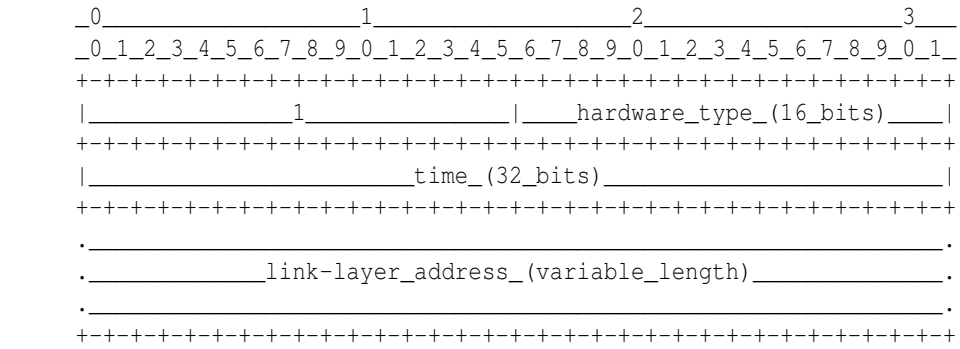
Contenu du DUID

Un DUID consiste d'un code de type à 2 octets, suivis par un nombre variable d'octets. Un DUID ne peut pas dépasser 128 octets de long. Les types suivants sont actuellement définis :

1 Adresse de lien réseau + une date
2 ID unique assigné par le vendeur basé sur le numéro d'entreprise
3 Adresse de lien réseau

DUID type 1 (DUID-LLT)

Ce type de DUID consiste d'un champ type à 2 octets contenant la valeur 1, un code de type hardware à 2 octets, 4 octets contenant une date, suivas par l'adresse de lien-réseaux d'une des interfaces connectée au périphérique DHCP au moment de la génération du DUID. La date est l'heure de génération du DUID, représenté en secondes depuis minuit (UTC), 1er Janvier 2000, modulo 2^32. Le type hardware doit être un type hardware valide assigné par l'IANA comme décris dans la rfc826.



Le choix de l'interface réseau peut être complètement arbitraire, tant que l'interface fournis une adresse de lien réseau unique pour le type de lien, et le même DUID-LLT devrait être utilisé en configurant toutes les interfaces réseau connectées au périphérique, sans regarder quelle interface de lien réseau a été utilisée pour générer le DUID-LLT

Les clients et serveurs utilisant ce type de DUID doivent stocker le DUID-LLT dans un stockage stable, et doivent continuer à utiliser le DUID-LLT même si l'interface réseau utilisée pour génerer le DUID-LLT est supprimée. Les clients et serveurs qui n'ont pas de stockage stable ne doivent pas utiliser ce type de DUID.

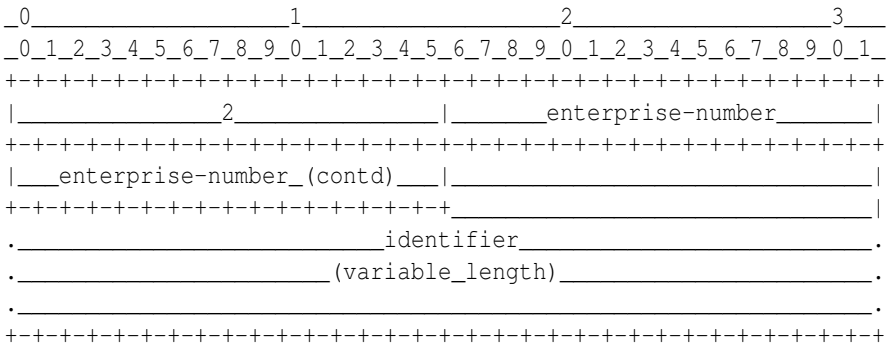
Les clients et serveurs qui utilisent ce DUID devraient tenter de configurer le temps avant de génerer le DUID, si possible, et doivent utiliser une sources de temps (par exemple, RTC) en générant le DUID, même si cette source de temp ne peut pas être configurée avant de générer le DUID. L'utilisation d'une source de temps rend peu probable que 2 DUID-LLT identiques soient générés si l'interface réseau est supprimée du client et qu'un autre client utilise la même interface réseau pour génerer un DUID-LLT.

Cette méthode de génération de DUID est recommandée pour les périphériques courant tels que les postes de travail, imprimantes, routeurs, etc. qui contiennent un stockage non-volatile.

Il est cependant possible que cet algorithme génère un DUID créant une collision. Un client DHCP qui génère un DUID-LLT en utilisant ce mécanisme doit fournir une interface administrative qui remplace le DUID existant avec un nouveaux DUID.

DUID type 2 (DUID-EN)

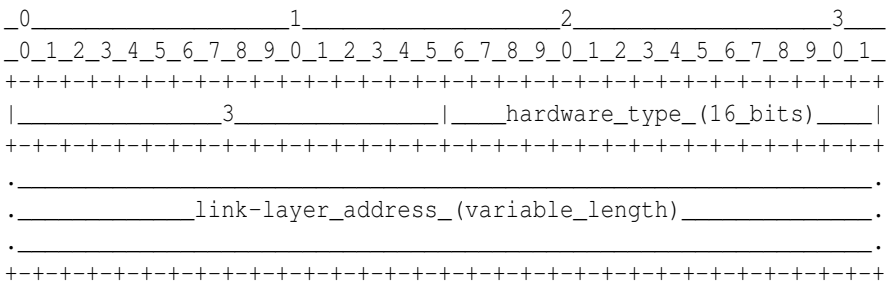
Cette forme de DUID est assignée par le vendeur au périphérique. Il consiste du Private Enterprise Number du vendeur maintenu par l'IANA, suivi par un identifiant unique assigné par le vendeur.



La source de l'identifiant est laissée au vendeur, mais chaque partie de l'identifiant de chaque DUID-EN doit être unique au périphérique, et doit être assigné au périphérique au moment de sa fabrication et stocké dans un stockage non-volatile, et devrait être stocké dans un stockage non-effacable.

DUID type 3 (DUID-LL)

Ce type de DUID consiste de 2 octets contenant le type 3, un code de type hardware à 2 octets, suivi par l'adresse de lien réseau d'une interface connectée au client ou serveur.



Le choix de l'interface réseau peut être complètement arbitraire, tant que cette interface fournis une adresse de lien réseau unique et est attaché en permanence au périphérique qui génère le DUID-LL. Le même DUID-LL devrait être utilisé pour configurer toutes les interfaces réseaux connectées au périphérique, sans regarder qui adresses de lien réseau a été utilisée pour générer le DUID.

DUID-LL est recommandé pour les périphériques qui ont une interface réseau connecté en permanence avec une adresse de lien réseau, et n'a pas de stockage non-volatile. LUID-LL ne doit pas être utilisé par les clients DHCP ou les serveurs qui ne peuvent pas dire si une interface réseau est attachée en permanence au périphérique sur lequel le client DHCP fonctionne.

Identity Association

Un identity-association (IA) est une construction qu'un serveur et un client peut utiliser pour identifier, grouper, et gérer un jeu d'adresses IPv6 liées. Chaque IA consiste d'un IAID et d'informations de configurations associées.

Un client doit associer au moins un IA distinct avec chacune de ses interfaces réseau depuis un serveur DHCP. Le client utilise les IA assignés à une interface pour obtenir des informations de configuration depuis un serveur pour cette interface. Chaque IA doit être associée avec exactement une interface.

Le IAID identifie de manière unique l'IA et doit être choisis pour être unique avec les IAID dans le client. Le IAID est choisis par le client. Pour une utilisation donnée d'un IA par le client, le IAID pour cet IA doit être consistant entre les redémarrages du client DHCP. Le client peut stocker le IAID dans un stockage non volatile ou en utilisant un algorithme qui produira un IAID consistant tant que la configuration du client n'a pas changé.

Les informations de configuration dans un IA consiste d'une ou plusieurs adresses IPv6 avec les temps T1 et T2 pour l'IA. Chaque adresse dans un IA a une durée de vie préférentielle et une durée de vie valide. Les durées de vie sont transmises du serveur au client dans l'option IA. La durée de vie s'applique à l'utilisation des adresses IPv6.

Séléctionner des adresses pour l'assignement à un IA

Un serveur séléctionne des adresses à assigner à un IA en accord avec les stratégies d'assignement d'adresse déterminés par l'administrateur serveur et les informations spécifiques déterminés par le serveur pour le client vient d'un combinaison des sources suivantes :

- Le lien via lequel le client est attaché. Le sereur détermine le lien comme suit :
  - Si le serveur reçoit le message directement du client et que l'adresse source dans le datagramme IP dans lequel le message a été reçu est une adresse de lien local, alors le client est sur le même lien que l'interface sur laquelle le message a été reçu.
  - Si le serveur reçoit le message depuis un agent relais, alors le client est sur le même lien que celui avec lequel l'interface, identifié par le champ link-address dans le message de l'agent relais, est attaché.
  - Si le serveur reçoit le message directement du client et que l'adresse source dans le datagramme IP dans lequel le message a été reçu n'est pas une adresse de lien local, alors le client est sur le lien identifié par l'adresse source dans le datagramme IP.
- Le DUID est fournis pas le client
- D'autres informations dans les options fournies par le client

Toute adresse assignée par un serveur qui est basé sur un identifiant EUI-64 doit inclure un identifiant d'interface avec les bits "u" (universal/local) et "g" (individual/group) de l'identifiant d'interface (rfc2373)

Un serveur ne doit pas assigner une adresse qui est réservée pour d'autres utilisations.

Gestion des adresses temporaires

Un client peut demander l'assignement d'adresses temporaires. DHCPv6 gère l'assignement sans faire de différence pour ces adresses temporaires. DHCPv6 n'indique rien sur le détails des adresses temporaires, comme la durée de vie, comment les clients utilisent ces adresses, les règles de génération d'adresses temporaires, etc.

Les client demandent des adresses temporaire et les serveur leur en assigne. Les adresses temporaires sont gérées dans l'option IA pour les adresses temporaires (IA_TA). Chaque option IA_TA contient au moins une adresses temporaire pour chaque préfixe dans le lien sur lequel le client est attaché.

L'espace de nombre IAID pour l'option IA_TÀ est séparé de l'IAID pour l'option IA_NA.

Transmission de messages par un client

Sauf mentionné dans ce document, ou dans un document décrivant comment IPv6 gère un type de lien spécifique, un client envoie les messages DHCP à l'adresse All_DHCP_Relay_Agents_and_Servers

Un client utilise le multicast pour atteindre tous les serveurs ou un serveur individuel. Un serveur individuel est indiqué en spécifiant le DUID du serveur dans l'option Server Identifier dans le message du client.

Fiabilité des échanges initiés par le client

Les clients DHCP sont responsables de la fiabilité de la livraison des messages dans les échanges initiés par le client. Si un client DHCP échoue à recevoir une réponse attendue d'un serveur, le client doit retransmettre son message. Cette section décris la stratégie de retransmission à utiliser par les clients.

Noter que la procédure décrite dans cette section est légèrement modifiée quand utilisée avec le message Solicit.

Le client commence l'échange en transmettant un message au serveur. L'échange se termine qund le client à reçue la réponse appropriée du ou des serveurs, ou quand l'échange est considéré échoué en accord avec le mécanisme de retransmission décris ci-dessous.

Le comportement de retransmission du client est contrôlé et décris par les variables suivantes :

RT Retransmission timeout
IRT Initial retransmission time
MRC Maximum retransmission count
MRT Maximum retransmission time
MRD Maximum retransmission duration
RAND Randomization factor

Avec chaque transmission de message ou retransmission, le client met RT en accord avec les règles données plus bas. Si RT expire avant que l'échange se termine, le client recalcule RT et retransmet le message.

Chaque calcul d'un nouveau RT inclus un facteur aléatoire (RAND), qui est entre -0.1 et +0.1. Ce facteur est inclus pour minimiser la synchronisation des messages transmis par les clients DHCP.

L'algorithme pour choisir un nombre aléatoire n'a pas besoin d'être cryptographique. L'algorithme devrait produire une séquence différente pour chaque invocation d'un client DHCP.

Le RT pour la transmission du premier message est basé sur IRT :

```
RT=IRT + RAND*IRT
```

Le RT pour chaque transmission suivante est basé sur la valeur RT précédente :

```
RT = 2*RTprev + RAND*RTprev
```

Le MRT spécifie une limite maximum de la valeur de RT. Si MRT a une valeur de 0, il n'y a pas de limite maximum. Sinon :

```
if ( RT > MRT )
_RT = MRT + RAND*MRT
```

Le MRC spécifie le nombre de retransmission. Sauf à 0, l'échange échoue quand le client a atteint cette limite de retransmission.

Les MRD spécifie une limite de temps pour la retransmission d'un message. Saux à 0, l'échange échoue une fois ce temps passé à transmettre le message.

Si MRC et MRD ne sont pas à 0, l'échange échoue quand une de ces conditions est atteinte. Si MRC et MRD sont à 0, le client continue à transmettre le message jusqu'à ce qu'il reçoive une réponse.

Validation de message

Les clients et serveurs devraient supprimer tous messages qui contiennent des options qui ne sont pas autorisés à apparaître dans le message reçu. Par exemple, une option IA n'est pas permis dans un message Information-request. Les clients et serveurs peuvent choisir d'extraire les informations d'un tel message si l'information est utile pour le destinataire.

Un serveur doit supprimer les messages Solicit, Confirm, Rebind ou Information-request s'il les reçoit avec une adresse de destination unicast.

Si un serveur reçoit un message qui contient des options qu'il ne devrait pas contenir, que des options sont manquantes, ou n'est pas valide, il peut envoyer un Reply (ou Advertise) avec une option Server Identifier, une option Client Identifier si elle était incluse dans le message et une option Status Code avec le status UnSpecFail.

Utilisation des ID de transaction

Le champ transaction-id maintien une valeur utilisée par les clients et les serveurs pour synchroniser les réponses des serveurs aux message client. Un client devrait générer un nombre aléatoire qui ne peut pas être facilement deviné ou prédit à utiliser comme ID de transaction pour chaque nouveau message qu'il envoie. Un client doit laisser l'ID de transaction inchangé dans les retransmissions d'un message.

Message Solicit

Les clients doivent détruire tous messages Solicit reçus. Les serveurs doivent détruire tous messages Solicit qui n'incluent pas l'option Client Identifier ou qui incluent une option Server Identifier.

Message Advertise

Les clients doit détruire tous messages Advertise qui rencontre une de ces conditions :

- Le message n'inclus pas l'option Server Identifier
- Le message n'inclus pas l'option Client Identifier
- Le contenu de l'option Client Identifier ne correspond pas à la valeur utilisée par le client dans son message Solicit

Les serveurs et agent relais doivent supprimer tous messages Advertise reçus.

Message Request

Les clients doivent détruire tout message Request. Les serveurs doivent détruire tout message Request qui rencontre une de ces conditions :

- Le message n'inclus pas l'option Server Identifier
- Le contenus de l'option Server Identifier ne match pas le DUID du serveur
- Le message n'inclus pas l'option Client Identifier

Message Confirm

Les clients doivent détruire tous message Confirm. Les serveurs doivent détruire tous messages Confirm qui n'incluent pas l'option Client Identifier ou qui n'incluent pas l'option Server Identifier.

Message Renew

Les cients doivent détruire tous messages Renew reçus. Les serveur doivent détruire tous message Renew qui rencontre une de ces conditions :

- Le message n'inclus pas l'option Server Identifier
- Le contenu de l'option Server Identifier ne correspond pas à l'identifiant du serveur
- Le message n'inclus pas l'option Client Identifier

Message Rebind

Les clients doivent détruire tous messages Rebind. Les serveurs doivent détruire tous message Rebind qui n'incluent pas l'option Client Identifier ou qui n'incluent pas l'option Server Identifier.

Messages Decline

Les clients doivent détruire tous messages Decline reçus. Les serveurs doivent détruire tout message Decline qui rencontre une de ces conditions :

- Le message n'inclue pas l'option Server Identifier
- Le contenue de l'option Server Identifier ne correspond par à l'identifiant du serveur
- Le message n'inclue pas l'option Client Identifier

Message Release

Les clients doivent détruire tous messages Release reçus. Les serveurs doivent détruire tout message Release qui rencontre une de ces conditions :

Message Reply

Les clients doivent détruire tout message Reply qui rencontre une de ces conditions :

- Le message n'inclue pas l'option Server Identifier
- Le champ transaction-id dans le message ne correspond par à la valeur utilisée dans le message original

Si le cilent a inclus l'option Client Identifier dans le message d'origine, le message Reply doit inclure une option Client Identifier contentant le DUID du client. Si le client n'a pas inclue l'option Client Identifier dans le message d'origine, le message Reply ne doit pas inclure une option Client Identifier.

Message Reconfigure

Les serveurs et agents relais doivent détruire tous message Reconfigure. Les clients doit détruire tout message Reconfigure qui rencontre une de ces conditions :

- Le message n'a pas été unicast au client
- Le message n'inclue pas l'option Server Identifier
- Le message n'inclue pas l'option Client Identifier qui contient le DUID du client
- Le message ne contient pas l'option Reconfigure Message et le msg-type doit être une valeur valide
- Le message inclue une option IA et msg-type dans l'option Reconfigure Message est INFORMATION-REQUEST
- Le message n'inclue pas d'authentification DHCP :
  - Le message ne contient pas une option d'authentification
  - Le message ne passe pas la validation de l'authentification effectuée par le client.

Message Information-request

Les clients doivent détruire tous message Information-request reçus. Les serveurs doivent détruire tout message Information-request reçus qui rencontre une de ces conditions :

- Le message inclus une option Server Identifier et le DUID dans l'option ne correspond pas au DUID du serveur.
- Le message inclue une option IA

Message Relay-forward

Les client doit détruire tous message Relay-forward reçus

Message Relay-reply

Les clients et serveur doivent détruire tous message Relay-reply reçus.

Sélection d'adresse source client et interface

Quand un client envoie un message DHCP à l'adresse All_DHCP_Relay_Agents_and_Servers, il devrait envoyer le message via l'interface pour laquelle les informations de configuration sont demandées. Cependant, le client peut envoyer le message via une autre interface attachée sur le même lien, si et seulement si le client est certain que les 2 interfaces sont attachées au même lien. Le client doit utiliser une adresse de lien local assigné à l'interface pur laquelle il demande les informations de configuration comme adresse source.

Quand un client envoie un message DHCP directement à un serveur en utilisant unicast (après avoir reçu l'option Server Unicast de ce serveur), l'adresse source dans l'en-tête IP doit être une adresse assignée à l'interface pour laquelle le client souhaite obtenir une configuration et qui est utilisable par le serveur en répondant au client.

Solicitation serveur DHCP

Cette section décris comment un client localise les serveurs qui assignent des adresses aux IA appartenant au client.

Le client est responsable de la création des IA et de la demande à un serveur d'assigner des adresses IPv6 à l'IA. Le client créé d'abord un IA et lui assigne un IAID. Le client transmet un message Solicit contenant une option IA décrivant l'IA. Les serveurs qui peuvent assigner des adresses à l'IA répondent au client avec un message Advertise. Le client initie alors un échange de configuration.

Si le client accepte un message Reply avec l'assignement d'adresse fournis et autres ressources en réponse au message Solicit, le client inclus une option Rapid Commit dans le message Solicit.

Comportement client

Un client utilise le message Solicit pour découvrir les serveurs DHCP configurés pour assigner les adresses ou retourner d'autres paramètres de configuration sur le lien sur lequel le client est attaché.

Création des messages Solicit

Le client définis le champ msg-type à SOLICIT. Le client génère un ID de transaction et l'insert dans le champ transaction-id

Le client doit inclure une option Client Identifier pour s'identifier au serveur. Le client inclus l'option IA pour tous les IA pour lesquelle il souhaite que le serveur assigne des adresses. Le client peut inclure des adresses dans les IA comme adresses préférentielles. Le client ne doit pas inclue d'autres options dans le message Solicit, excepté si spécifiquement permis dans la définition des options individuelles.

Le client utilise les options IA_NA pour demander l'assignement d'adresses non-temporaires et utilise les options IA_TA pour demander l'assignement d'adresses temporaire. Les 2 peuvent être inclus dans les messages DHCP.

Le client devrait inclure une option Option Request pour indiquer les options que le client souhaite reçevoir. Le client peut additionnellement inclure les instances de ces options qui sont identifiées dans l'option Option Request, avec des valeurs pour indiquer ses préférences.

Le client inclus une option Reconfigure Accept si le client est capable d'accepter les messages Reconfigure du serveur.

Transmission des messages Solicit

Le premier message Solicit du client doit être retardé par un temps aléatoire entre 0 et SOL_MAX_DELAY. Dans le cas d'un message Solicit transmis quand DHCP est initié par IPv6 ND, le délais donne la quantité de temps d'attente après que ND cause le client à invoquer le protocole d'autoconfiguration avec état. Ce délai aléatoire désynchonise les client qui démarrent en même temps.

Le client transmet le message en accord avec la section "Fiabilité des échanges initiés par le client", en utilisant les paramètres suivants :

IRT SOL_TIMEOUT

MRT SOL_MAX_RT

MRC 0

MRD 0

Si le client a inclus une option Rapid Commit dans son message Solicit, le client termine le processus d'attente dès qu'un message Reply avec l'option Rapid Commit est reçu.

Si le client attend un message Advertise, le mécanisme dans la section "Fiabilité des échanges initiés par le client" est modifié comme suit dans la transmission des messages solicit. L'échange de message n'est pas terminé par la réception d'un Advertise avant que le premier RT soit atteinds. Au lieu de celà, le client collecte les messages Advertise jusqu'à ce que le premier RT soit passé. Également, le premier RT doit être sélectionné pour être strictement supérieur à IRT en choisissant RAND pour être strictement supérieur à 0.

Un client doit collecter les message Advertise pendant les RT premières secondes sauf s'il reçoit un message Advertise avec une valeur de préférence à 255. La valeur de préférence est gérée dans l'option Preference. Tout Advertise qui n'inclus pas une option Preference est considérée avec une préférence à 0. Si le client reçoit un Advertise qui inclus une option Preference avec une valeur 255, le client commence immédiatement un échange en envoyant un Request au serveur. Si le client reçoit un message Advertise qui n'inclus pas l'option Preference avec une valeur de 255, le client continue à attendre le RT. Si le premier RT est atteind et que le client a reçu un Advertise, le client doit continue avec un échange en envoyant un Request.

Si le client ne reçoit pas d'Advertise, il commence le mécanisme de retransmission. Le client termine le processus de retransmission dès qu'il reçoit un Advertise, et le client agit sur le message Advertise sans attendre d'autre message Advertise.

Un client DHCP devrait choisir MRC et MRD à 0. Si le client DHCP est configuré avec MRC ou MRD autre qu'à 0, il doit arrêter sa tentative de configurer l'interface si l'échange échoue, puis devrait redémarrer le processus de reconfiguration après un événement externe, tel que l'entrée utilisateur, redémarrage système, ou quand le client est attaché à un nouveau lien.

Réception des Messages Advertise

Le client doit ignorer tout message Advertise qui inclus une option Status Code contenant la valeur NoAddrsAvail, à l'exception que le client peut afficher le message de status associé à l'utilisateur.

Une fois un ou plusieurs messages Advertise valide reçus, le client en séléctionne un ou plus basé sur les critères suivants :

- Les message Advertise avec la valeur de préférence serveur la plus élevé sont préférés.
- Dans un groupe de message Advertise avec la même valeur de préférence serveur, un client peut séléctionner les serveurs dons les message Advertise annoncent des informations d'interêt au client.
- Le cilent peut choisir un serveur moins préféré si ce serveur a un meilleurs jeu de paramètres.

Une fois qu'un client a sélectionne le ou les messages Advertise, le client stocke les informations sur chaque serveur. Si le client doit sélectionner un serveur alternatif dans le cas où un serveur ne répond pas, le client choisis le serveur suivant en accord avec les critères ci-dessus.

Réception d'un message Reply

Si le client inclus une option Rapid Commit dans le message Solicit, il s'attend à un message Reply qui inclus une option Rapid Commit. Le client supprime tous message Reply qui ne contiennent pas l'option Rapid Commit. Si le client reçoit un message Reply valide avec l'option Rapid Commit, il traite le message. S'il ne reçoit pas un tel Reply, le client traite le message Advertise comme décris ci-dessus.

Si le client reçois un message Reply valide qui inclus une option Rapid Commit, il peut :

- Traiter le message Reply comme décris plus bas, et supprimer tous messages Reply reçus en réponse au Request, ou
- Traiter tout message Reply en réponse au Request et supprimer le message Reply qui inclus l'option Rapid Commit.

Comportement serveur

Un serveur envoie un message Advertise en réponse aux messages Solicit valides qu'il reçoit pour annoncer la disponibilité du serveur au client.

Réception des messages solicit

Le serveur détermine les information sur le client et son emplacement, puis vérifie sa stratégie administrative pour répondre au client. Si le serveur n'est pas autorisé à répondre au client, le serveur supprime le message Solicit. Par exemple, si la stratégie administrative du serveur est de répondre uniquement aux clients capable d'accèpter un message Reconfigure, le serveur supprimera tout message Solicit indiquant qu'il n'accepte pas de message Reconfigure.

Si le client a inclus une option Rapid Commit et que le serveur a été configuré pour répondre avec l'assignement d'adresse et autre ressources, le serveur répond avec un Reply comme décris plus bas. Sinon, le serveur ignore l'option Rapid Commit et traite le reste du message comme si l'option n'était pas présente.

Création et transmission des messages Advertise

Le serveur met le champ msg-type à ADVERTISE et copie le contenu du champ transaction-id du message Solicit reçu du client dans le message Advertise. Le serveur inclus son identifiant dans une option Server Identifier et copie le Client Identifier dans le message Advertise.

Le serveur peut ajouter une option préférence. Les implémentations serveur devraient permettre le paramètrage de valeur de préférence serveur par l'administrateur. La valeur de préférence doit être à 0 par défaut.

Le serveur inclus une option Reconfigure Accept si le serveur exige du client qu'il accèpte les messages Reconfigure.

Le serveur inclus les options que le serveur retourne au client dans un message Reply. Les informations dans ces options peuvent être utilisé par le client dans la sélection d'un serveur si le client reçoit plus d'un message Advertise. Si le client a inclus une option Option Request dans le message Solicit, le serveur inclus les options dans le message Advertise contenant les paramètres de configuration pour toutes les options identifiées dans l'option Option Request pour lesquelles le serveur a été configuré pour répondre au client. Le serveur peut retourner d'autres options au client s'il a été configuré pour le faire.

Si le message Solicit du client incluait une ou plusieurs options IA, le serveur doit inclure les options IA dans le message Advertise contenant les adresses à assigner aux IA. Si le client a inclus des adresses dans les IA dans le message Solicit, le serveur les utilise comme préférences pour ce client.

Si le serveur n'assigne pas d'adresse à des IA dans un Request du client, le serveur doit envoyer un message Advertise qui inclus seulement une option Status Code avec le code NoAddrsAvail et un message de status pour l'utilisateur, une option Server Identifier avec le DUID du serveur, et une option Client Identifier avec le DUID du client.

Si le message Solicit a été reçu directement par le serveur, le serveur unicast le message Advertise directement au client en utilisant l'adresse dans le champ adresse source du datagramme IP. Le message Advertise doit être unicast sur le lien sur lequel le message Solicit a été reçus.

Si le message Solicit a été reçu dans un message Relay-forward, le serveur construit un message Relay-reply avec le message Advertise

dans le payload d'une option relay-message. Si le message Relay-forward incluait une option Interface-id, le serveur copie cette option dans le message Relay-reply. Le serveur unicast le message Relay-reply directement à l'agent relay en utilisant l'adresse dans le champ adresse source du datagramme IP.

Création et transmission des messages Reply

Le serveur doit envoyer l'assignement des adresses ou autres informations de configuration avant d'envoyer un message Reply à un client en réponse à un message solicit.

En utilisant un échange Solicit-Reply, le serveur envoie l'assignement des adresses avant d'envoyer le message Reply. Le client peut assumer qu'il a reçu les adresses dans le message Reply et n'a pas besoin d'envoyer un message Request pour ces adresses.

Typiquement, les serveur qui sont configurés pour utiliser l'échange Solicit-Reply sont déployés pour qu'un seul serveur réponde à un message Solicit. Si plus d'un serveur répond, le client utilise seulement les adresses d'un seul de ces serveurs.

Le serveur inclus une option Rapid Commit dans le message Reply pour indiquer que le Reply est en réponse à un message Solicit.

Le serveur inclus une option Reconfigure Accept s'il souhaite que le client accepte les messages Reconfigure.

Échange de configuration DHCP initié par le client

Un client initie un échange de message avec un ou plusieurs serveurs pour obtenir ou mettre à jours sa configuration. Le client peut initier l'échange comme partie du processus de configuration système, quand requis.

Comportement client

Un client utilise les messages Request, Renew, Rebind, Release, et Decline durant le cycle de vie normal des adresses. Il utilise Confirm pour valider les adresses quand il a été déplacé sur un nouveau lien. Il utilise les message Information-Request quand il a besoin d'informations de configuration sans adresses.

Si le client a une addresse source de scope suffisant qui peut être utilisé par le serveur comme adresse de retour, et que le client a reçu une option Server Unicast du serveur, le client devrait unicast tous messages Request, Renew, Release et Decline au serveur.

Création et transmission des messages Request

Le client utilise un message Request pour populer les IA avec des adresses et obtenir d'autres informations de configuration. Le serveur inclus un ou plusieurs options IA dans le message Request. Le serveur retourne les adresses et autres informations sur les IA au client dans les options IA dans un message Reply.

Le client génère un ID de transaction et l'insert dans le champ transaction-id.

Le client doit inclure une option Client Identifier pour s'identifier lui-même au serveur. Le client ajoute toute autre options appropriées, incluant une ou plusieurs options IA.

Le client doit inclure une option Option Request pour indiquer les options que le client souhaite obtenir. Le client peut inclure des options

avec des valeur pour indiquer ses préférences sur ces paramètres.

Le client inclus une option Reconfigure Accept indiquant si le client accèpte les messages Reconfigure du serveur.

Le client transmet le message en utilisant les paramètres suivants :

IRT REQ_TIMEOUT
MRT REQ_MAX_RT
MRC REQ_MAX_RC
MRD 0

Si l'échange échoue, le client prend une action basée sur la stratégie locale du client. Des exemples d'actions que le client peut prendre incluent :

- Sélectionner un autre serveur de la liste de serveurs connus, par exemple, les serveurs qui ont répondu avec un message Advertise
- Initier le processus de découverte de serveur
- Terminer le processus de configuration et reporter une erreur.

Création et transmission des messages Confirm

Un client pouvant être placé sur un nouveau lien, les préfixes des adresses assignées aux interfaces sur ce lien ne sont plus appropriés pour le lien sur lequel le client est attaché. Par exemple :

- Le client redémarre
- Le client est physiquement connecté à une connection filaire
- Le client revient d'un mode veille
- Le client utilise une technologie sans-fil et change de point d'accès

Dans ces situations, quand un client peut avoir changé de lien, le client doit initier un échange Confirm/Reply. Le client inclus les IA assignés à l'interface qui a changé de lien, avec les adresses associées avec ces IA, dans son message Confirm. Tout serveur répondant indique si ces adresses sont appropriées pour le lien pour lequel le client est attaché avec le status dans le message Reply qu'il retourne au client.

Le client met le champ msg-type à CONFIRM. Le client génère un ID de transaction dans le champ transaction-id.

Le client doit inclure une option Client Identifier pour s'identifier lui-même au serveur. Le client inclus les options IA pour tous les IA assignés à l'interface pour laquelle le message Confirm est envoyé. Les options IA incluent toutes les adresses que le client a associé avec ces IA. Le client devrait mettre les champs valid-lifetime dans les options IA Address à 0, vu que le serveur va ignorer ces champs.

Le premier message Confirm du client dans l'interface doit être retardé par un délais aléatoire entre 0 et CNF_MAX_DELAY. Le client transmet le message en utilisant les paramètres suivants :

IRT CNF_TIMEOUT
MRT CNF_MAX_RT
MRC 0
MRD CNF_MAX_RD

Si le client ne reçois pas de réponse avant que le processus de transmission ne se termine, le client devrait continuer à utiliser les adresses IP, en utilisant le dernier lifetime connus pour ces adresses, et devrait continuer à utiliser tout paramètres précédemment utilisés.

Création et transmission des messages Renew

Pour étendre la durée de vie des adresses associées aux IA, le client envoie un message Renez au serveur. Le client inclus les options IA Address dans l'option IA pour les adresse associées avec l'IA. Le serveur détermine les nouvelles durées de vie pour les adresses dans l'IA en accord avec la configuration administrative du serveur. Le serveur peut également ajouter de nouvelles adresses à l'IA. Le serveur peut supprimer les adresses de l'IA en définissant les durées de vie préférrés et valide de ces adresses à 0.

Le serveur contrôle le temps auquel le client contacte le serveur pour étendre la durée de vie des adresses assignées via les paramètres T1 et T2.

Au temps T1 pour un IA, le client initie un échange Renew/Reply pour étendre la durée de vie des adresses dans l'IA. Le client inclus une option IA avec toutes les adresses actuellement assignées à l'IA dans son message Renew.

Si T1 ou T2 est à 0 (pour un IA_NA) ou s'il n'y a pas de T1 ou T2 (pour un IA_TA), le client peut envoyer un message Renew ou Rebind, respectivement, à la discretion du client.

Le client met msg-type à RENEW. Le client génère un ID de transaction dnas transaction-id. Le client place l'identifiant du serveur de destination dans une option Server Identifier.

Le client doit inclure une option Client Identifier pour s'identifier lui-même au serveur. Le client ajoute toutes options appropriées, incluant une ou plusieurs options IA. Le client doit inclure une liste d'adresse que le client a associé avec les IA dans le message Renew.

Le client doit inclure une option Option Request pour indiquer les options que le client souhaite reçevoir. Le client peut inclure des options avec des valeurs comme indicateur au serveur que le client souhaite avoir en retour.

IRT REN_TIMEOUT

MRT REN_MAX_RT

MRC 0

MRD Remaining time until T2

L'échange est terminé quand le temps T2 est atteind, auquel cas le client commence un échange Rebind.

Création et transmission des messages Rebind

Au temps T2 pour un IA, le client initie un échange Rebind/Reply avec un serveur disponible. Le client inclus une option IA avec toutes les adresses actuelement assignées à l'IA dans son message Rebind.

Le client met msg-type à REBIND. Le client génère un ID de transaction dans le champ transaction-id. Le client doit inclure une option Client Identifier, et ajoute les options appropriées, incluant une ou plusieurs options IA. Le client doit incluer la liste des adresses associées avec l'IA dans le message REBIND.

IRT REB_TIMEOUT

MRT REB_MAX_RT

MRC 0

MRD Temps restant jusqu'à ce que la durée de vie de toutes les adresses aient expirées.

L'échange est terminé quand les durées de vie de toutes les adresses assignées à l'IA ont expirée. À ce moment le client a plusieurs alternative :

- Le client peut utiliser un message Solicit pour localiser un nouveau serveur DHCP et envoyer un Request pour l'IA expiré à un nouveau serveur.
- Si le client a d'autres adresses dans d'autres IA, le client peut choisir de supprimer l'IA expiré et d'utiliser les adresses dans les autres IA.

Création et transmission des messages Information-request

Le client utilise un message Information-request pour obtenir des informations de configuration sans assigner d'adresses. Le client met msg-type à INFORMATION-REQUEST. Le client génère un ID de transaction dans le champ transaction-id.

Le client devrait inclure une option Client Identifier pour s'identifier au serveur. Si le client n'inclus pas cette option, le serveur ne sera pas capable de retourner d'options spécifiques au client, ou le serveur peut choisir de ne pas répondre du tout. Le client doit inclure cette option si le message Information-Request est authentifié.

Le client doit inclure une option Option Request pour indiquer les options que le client souhaite reçevoir. Le client peut inclure des options avec des valeurs comme préférences.

Le premier message Information-request du client dans l'interface doit être retardé par un délay aléatoire entre 0 et INF_MAX_DELAY. Le client transmet le message avec les paramètres suivants :

IRT INF_TIMEOUT
MRT INF_MAX_RT
MRC 0
MRD 0

Création et transmission des messages Release

Pour libérer une ou plusieurs adresses, un client envoie un message Release au serveur. Le client met msg-type à RELEASE et génère un ID de transaction dans le champ transaction-id.

Le client place l'identifiant du serveur qui a alloué les adresses dans une option Server Identifier. Le client doit inclure une option Client Identifier pour s'identifier au serveur. Le client inclus les options contenant les IA contenant les adresses à libérer.

Le client ne doit pas utiliser les adresses qu'il a libéré. Parce que les message Release peuvent être perdus, le client devrait retransmettre le message s'il ne reçoit pas de réponse. Cependant, il y a des scénarios où le client peut ne pas vouloir attendre (ex : extinction). Les implémentations devraient retransmettre une ou plusieurs fois, mais peuvent choisir de terminer la retransmission plus tôt.

IRT REL_TIMEOUT
MRT 0
MRC REL_MAX_RC
MRD 0

Si les adresses sont libérées mais la réponse est perdue, le client va retransmettre le message Release, et le serveur peut répondre avec un Reply indiquant le status NoBinding.

Création et transmission des messages Decline

Si un client détecte qu'une ou plusieurs adresses assignées par le serveur sont déja utilisées par un autre nœud, le client envoie un message Decline au serveur pour informer que l'adresse est suspecte.

Le client met msg-type à DECLINE. Le client génère un ID de transaction dans le champ transaction-id, et place d'identifiant du serveur qui a alloué la ou les adresses dans une option Serveur Identifier.

Le client doit inclure une option Client Identifier pour s'identifier au serveur. Le client inclus les options contenant les IA pour les adresses qu'il décline. Les adresses qu'il décline doivent être incluses dans les IA. Les autres adresses que le client souhaite continuer à utiliser ne doivent pas être ajoutées dans les IA.

Le client ne doit pas utiliser les adresses qu'il décline. Le client transmet le message en utilisant les paramètres suivants :

IRT DEC_TIMEOUT
MRT 0
MRC DEC_MAX_RC
MRD 0

Si des adresses sont déclinées mais le Reply du serveur DHCP est perdu, le client retransmet le message Decline, et le serveur peut répondre avec un Reply indiquant un status NoBinding. Donc, le client ne traite pas un message Reply avec un status NoBinding dans un échange Decline vu qu'il indique une erreur.

Réception des messages Reply

Une fois reçu un message Reply valide en réponse à un message Solicit (avec l'option Rapid Commit), Request, Confirm, Renew, Rebind ou Information-request, le client extrait les informations de configuration contenues dans la réponse.

Le client devrait effectuer une détection d'adresses dupliquée sur chaque adresse dans les IA qu'il reçoit dans le message Reply avant de les utiliser. Si une des adresses est utilisée sur le lient, le client envoie un message Decline au serveur.

Si le Reply a été reçu en réponse à un message Solicit (avec l'option Rapid Commit), Request, Renew ou Rebind, le client met à jours les informations qu'il a enregistré sur les IA depuis les options IA contenus dans le Reply :

- Enregistre les temps T1 et T2
- Ajoute toute nouvelle adresse dans l'option IA à l'IA enregistrée par le client
- Met à jours la durée de vie des adresses dans l'option IA
- Supprime toute adresses de l'IA, enregistré par le client, qui ont une durée de vie de 0 dans l'option IA Address
- Laisse toute information inchangée sur les adresses que le client a enregistré dans l'IA mais n'était pas inclus dans l'IA reçu du serveur.

La gestion des informations de configuration spécifique est détaillée dans la définition de chaque option plus bas dans ce document.

Si le client reçoit un message Reply avec un code de status contenant UnspecFail, le serveur indique qu'il n'est pas capable de traiter le message à cause d'une condition non spécifiée. Si le client retransmet le message original au même serveur pour retenter la même opération, le client doit limiter le taux de retransmission du message et limiter la durée de retransmission.

Quand le client reçois un message Reply avec un code de status UseMulticast, le client enregistre le message et envois les messages suivants au serveur via l'interface sur laquelle il a reçus le Reply. Le client renvoie le message original en utilisant le multicast.

Quand le client reçoit un status NotOnLink du serveur en réponse à un message Confirm, le client effectue une solicitation de serveur, et une configuration initié par le client. Si le client reçois un message Reply qui n'indique pas un status NotOnLink, le client peut utiliser l'adresse dans l'IA et ignorer tous messages qui indiquent un status NotOnLink.

Le client examine le code de status dans chaque IA individuel. Si le code de status est NoAddrsAvail, le client n'a pas reçus d'adresses utilisatble dans l'IA et peut choisir de tenter d'obtenir des adresses pour l'IA depuis d'autres serveurs. Le client utilise les adresses et autres informations des IA qui ne contiennent pas le code NoAddrsAvail. Si le cient ne reçoit pas d'adresses dans aucun IA, il peut soit tenter d'utiliser un autre serveur, ou utiliser un Information-request pour obtenir d'autres informations de configuration.

Quand le client reçoit un message Reply en réponse à un Renew ou un Rebind, le client examine chaque IA indépendamment. Pour chaque IA dans le message Renew ou Rebind original, le client :

- Envoie un message Request si l'IA contenait une option Code Status avec le status NoBinding (et n'envoie pas de messages additionnels)

- Enovie un Renew/Rebind si l'IA n'est pas dans le message Reply
- Sinon accept l'information dans l'IA

Quand le client reçoit un message Reply valide en réponse à un message Release, le client considère l'événement Releas complété, sans regarder l'option Status Code retourné par le serveur.

Comportement du serveur

Dans la plupart des instances, le serveur envoie un Reply en réponse à un message client. Ce Reply doit toujours contenir l'option Server Identifier contenant le DUID du serveur et l'option Client Identifier correspondant au message reçu du client s'il était présent.

Dans la plupart des messages Reply, le serveur inclus les options contenant les informations de configuration pour le client. Le serveur doit connaître les recommandations des tailles de paquet et l'utilisation de la fragmentavtion. Si le client a inclus une option Option Request dans son message, le serveur inclus les options dans la résponse contenant les paramètres de configuration pour toutes les options identifiées à retourner au client. Le serveur peut retourner d'autres options au client s'il a été configuré pour celà.

Réception des messages Request

Quand le serveur reçoit un message Request via unicast d'un client auquel le serveur n'a pas d'option unicast, le serveur détruit le Request et réponds avec un message Reply contenant un status UseMulticast.

Quand le serveur reçoit une message Request valide, le serveur créé les liaisons avec ce client en accord avec la stratégie du serveur et les informations de configuration et enregistre les IA et autres information demandées par le client.

Le serveur doit inclure une option Server Identifier et Client Identifier. dans le message Reply.

Si le serveur trouve que le préfixe d'une ou plusieurs IP dans un IA dans le message du client n'est pas approprié pour le lien, le serveur doit retourner l'IA au client avec un code de status NotOnLink.

Si le serveur ne peut pas assigner des adresses à un IA dans le le message du client, le serveur doit inclure l'IA dans le Reply sans adresses et un status dans l'IA contenant le status NoAddrsAvail.

Pour tout IA auquel le serveur peut assigner des adresses, le serveur inclus l'IA avec les adresses et autres paramètres de configuration, et enregistre l'IA comme nouvelle liaison cliente.

Le serveur inclus l'option Reconfigure Accet si le serveur souhaite que le client accepte les messages Reconfigure.

Le serveur inclus d'autres options contenant des informations de configuration à retourner au client.

Si le serveur trouve que le client a inclus un IA dans la requête pour lequel le serveur a déjà une liaison associée avec le client, le client a renvoyé un message Request pour lequel il n'a pas reçus de message Reply. Le serveur renvoie un message Reply précédemment mis en cache, ou envoie un nouveau message Reply.

Reception des messages Confirm

Quand le serveur reçoit un message Confirm, le serveur détermine si les adresses dans le message Confirm sont appropriés pour le lien auquel le client est attaché. Si toutes les adresses dans le message Confirm ont passé ce test, le serveur retourne un status Success. Si une des adresse ne passe pas ce test, le serveur retourne un status NotOnLink. Si le serveur n'est pas capable d'effectuer ce test, où s'il n'y a pas d'adresses, le serveur ne doit pas envoyer de réponse au client.

Le serveur ignore les champs T1 et T2 dans les options IA et les champs preferred-lifetime et valid-lifetime dans les options IA Address.

Le serveur construit un message Reply en mettant msg-type à REPLY, et copie le transaction-id depuis le message Confirm.

Le serveur doit inclure les options Server Identifier et Client Identifier. Les server inclus une option Status Code indiquant le status du message Confirm.

Réception des messages Renew

Quand le serveur reçoit un message Renew via unicast d'un client auquel le serveur n'a pas envoyé d'option unicast, le serveur répond avec un code de status UseMulticast.

Quand le serveur reçoit un message Renew qui contient une option IA d'un client, il localise la liaison du client et vérifie que les informations client dans l'IA correspondent au informations stockées.

Si le serveur ne peut pas trouver d'entrée cliente pour l'IA, le serveur retourne l'IA ne contenant aucune adresse avec un Status NoBinding.

Si le serveur trouve les adresses dans l'IA pour le client, e serveur renvoie l'IA au client avec de nouveaux temps T1/T2. Le serveur peut choisir de changer la liste des adresses et les durées de vie des adresses dans les IA qui sont retournés au client.

Le serveur construit un message Reply en mettant msg-type à REPLY, en copiant le transaction-id depuis de message Renew, inclus les options Server Identifier et Client Identifier, et inclus d'autres options contenant des informations de configuration.

Réception des messages Rebind

Quand le serveur reçoit un message Rebind qui contient une option IA d'un client, il localise la liaison du client et vérifie que les information dans l'IA correspondent aux informations stockées.

Si le serveur ne peut pas trouver d'entrée client pour l'IA et que le serveur détermine que les adresses dans l'IA ne sont pas appropriés pour le lien sur lequel l'interface client est attachée, en accord avec la configuration du serveur, le serveur peut envoyer un message Reply au client contenant l'IA du client, avec les durées de vie pour ces adresses à 0. Ce Reply constitue une notification explicite au client que les adresses dans l'IA ne sont plus valides. Dans cette situation, si le serveur n'envoie pas de message Reply, il supprime silencieusement le message Rebind.

Si le serveur trouve qu'une des adresses n'est plus appropriée pour le lien auquel le client est attaché, le serveur retourne l'adresse au client avec une durée de vie de 0.

Si le serveur trouve les adresses dans l'IA pour le client, le serveur devrait retourner l'IA au client avec les nouvelles durées de vie et les temps T1 et T2.

Le serveur construit un message Reply en définissant msg-type à REPLY, et en copiant le transaction-id du message Rebind.

Le serveur doit inclure une option Server Identifier et l'option Client Identifier.

Le serveur inclus d'autres options contenant les informations de configuration à retourner au client.

Réception des messages Information-Request

Quand le serveur reçoit un message Information-Request, le client demande des informations de configuration qui n'incluent pas l'assignement d'adresses. Le serveur détermine tous les paramètres de configuration appropriés au client, basé sur la stratégie de configuration du serveur.

Le serveur construit un message Reply en définissant msg-type à REPLY, et en copiant le transaction-id.

Le serveur doit inclure l'option Server identifier, et si le client l'a fournis, l'option Client Identifier.

Le serveur inclus les options contenant les informations de configuration à retourner au client.

Si le message Information-request reçus du client n'inclus pas l'option Client Identifier, le serveur devrait répondre avec un Reply contenant tous les paramètres de configuration qui ne sont pas déterminés par l'identité du client. Si le serveur choisis de ne pas répondre, le client peut continuer de retransmettre le message Information-request indéfiniment.

Réception des messages Release

Quand le serveur reçoit un message Release via unicast depuis un client auquel le serveur n'a pas envoyé d'option unicast, le serveur supprime le message et répond avec un status UseMulticast, une option Server Identifier et l'option Client Identifier.

À la réception d'un message Release valide, le serveur examine les IA et les adresses dans les IA. Si les IA dans le messages sont dans une liaison pour le client, et que les adresses dans les IA ont été assignées par le serveur à ces IA, le serveur supprime les adresse des IA et les rend de nouveau disponible. Le serveur ignore les adresses non assignées à l'IA, bien qu'il peut choisis de logger les erreurs.

Une fois toutes les adresses traitées, le serveur génère un message Reply et inclus le status Success, Server Identifier et Client Identifier. Pour chaque IA dans le message Release pour lequel le serveur n'a pas de liaison, le serveur inclus un status NoBinding dans l'option IA. Aucune autre option n'est incluse dans l'option IA.

Un serveur peut choisir de garder un enregistrement des adresses assignées et des IA après que les durées de vie aient expirées pour permettre au serveur de réassigner les adresse précédemment assignées à un client.

Réception de messages Decline

Quand le serveur reçoit un message Decline via unicast depuis un client auquel le serveur n'a pas envoyer d'option unicast, il répond avec un status UseMulticast.

À la réception d'un message Decline valide, le serveur examine les IA et les adresses dans les IA. Si les IA dans le message sont dans une liaison pour le client, et que les adresses dans les IA ont été assignés par le serveur pour ces IA, le serveur supprime les adresses depuis les IA. Le serveur ignore les adresses non assignées à l'IA.

Le client a trouvé toutes les adresses dans le message Decline comme étant déjà utilisé sur son lien. Cependant, le serveur devrait marquer les adresses déclinée par le client pour que les adresses ne soient pas assignées à d'autres clients, et peut choisir de créer une notification indiquant que ces adresses ont été déclinées. La stratégie locale du serveur détermine quand les adresses identifiées dans un message Decline peuvent être disponible pour l'assignement.

Une fois toutes les adresse traitées, le serveur génère un message Reply et inclus une option Status Code avec la valeur Success, d'option Server Identifier, et Client Identifier. Pour chaque IA dans le message Decline pour lequel le serveur n'a pas d'information de liaison, le serveur ajoute une option IA pour laquelle le serveur n'a pas d'information de liaison, avec un status NoBinding. Aucune autre option n'est incluse dans l'option IA.

Transmission des messages Reply

Si le message original a été reçu directement par le serveur, le serveur unicast le message Reply directement au client en utilisant l'adresse source du message reçu. Le message Reply doit être unicasté via l'interface dans laquelle le message original a été reçu.

Si le message original a été reçu dans un message Relay-forward, le serveur construit un message Relay-reply avec le message Reply dans le payload d'une option Relay Message. Si les messages Relay-forward incluaient une option interface-id, le serveur copie cette option dans le message Relay-reply. Le serveur unicast le message Relay-reply directement à l'agent relay en utilisant l'adresse source du message Relay-forward.

Échange de configuration initié par le serveur

Un serveur initie un échange de configuration pour forcer les clients DHCP à obtenir de nouvelles adresses IP et d'autres informations de configuration. Par exemple, un administrateur peut utiliser un échange de configuration initié par le serveur quand les liens dans le domain DHCP doivent être rénumérotés. D'autres exemples incluent les changements d'emplacement des services d'annuaire, l'ajout de nouveaux services tels que l'impression, et la disponibilité de nouveaux logiciels.

Comportement du serveur

Un serveur envoie un message Reconfigure pour forcer un client à initier immédiatement un Renew/Reply ou un échange Information-request/Reply avec le serveur.

Création et transmission de messages Reconfigure

Le serveur met msg-type à RECONFIGURE. Le serveur met le champ transaction-id à 0. Le serveur inclus une option Server Identifier, et une option Client Identifier dans le message Reconfigure.

Le serveur peut inclure une option Option Request pour informer le client des informations qui ont été changés ou les nouvelles informations qui ont été ajoutées. En particulier, le serveur spécifie l'option IA dans l'option Option Request si le serveur souhaite que le client obtienne une nouvelle adresse. Si le serveur identifie l'option IA dans l'option Option Request, le serveur doit inclure une option IA qui ne contient pas d'autres sous-options pour identifier chaque IA qui doit être reconfigurée dans le client.

À cause du risque d'attaques DDOS contre les client DHCP, l'utilisation d'un mécanisme de sécurité est obligatoire dans les messages Reconfigure. Le serveur doit utiliser l'authentification DHCP dans le message Reconfigure.

Le serveur doit inclure une option Reconfigure Message pour sélectionner si le client répond avec un message Renew ou un message Information-request.

Le serveur ne doit pas inclure d'autres options dans le Reconfigure excepté si spécifiquement permis dans la définition des options individuelles.

Un serveur envoie chaque message Reconfigure à un simple client DHCP, en utilisant une adresse unicast de scope suffisant. Si le serveur n'a pas d'adresse à laquelle envoyer le message Reconfigure directement, le serveur utilise un message Relay-reply et envoie le message Reconfigure à un agent relais qui va relayer le message au client. Le serveur peut obtenir l'adresse du client et de l'agent relais si requis, via l'information du serveur sur les clients qui sont en contact avec le serveur, ou via un agent externe.

Pour reconfigurer plus d'un client, le serveur unicast un message séparé à chaque client. Le serveur peut initier la reconfiguration de plusieurs clients simultannément ; par exemple, un serveur peut envoyer un message Reconfigure à des clients additionnels pendant que

d'autres échanges de reconfiguration sont en cours.

Le message Reconfigure force le client à initier un échange Renew/Reply ou Information-request/Reply avec le serveur. Le serveur interprète la réception d'un message Renew ou Information-request du client comme satisfaisant le message Reconfigure.

Timout et retransmission des messages Reconfigure

Si le serveur ne reçoit pas de message Renew ou Information-Request du client dans les REC_TIMEOUT ms, le serveur retransmet le message Reconfigure, double de temps REC_TIMEOUT et attend de nouveau. Le serveur continue ce processus jusqu'à REC_MAX_RC tentative infructueuse, auquel cas le serveur devrait annuler le processus de reconfiguration pour ce client.

Réception des messages Renew

Le serveur génère et envoie un message Reply au client, incluant les options pour les paramètres de configuration. Le serveur peut inclure des options contenant les IA et de nouvelles valeurs pour d'autres paramètres de configuration dans le message Reply, même si ces IA et paramètres ne sont pas demandés dans le message Renew du client.

Réception des messages Information-request

Le serveur génère et envoie un message Reply au client, incluans les options pour les paramètres de configuration. Le serveur peut inclure des options contenant de nouvelles valeurs pour d'autres paramètre même si ces paramètres n'ont pas été demandé par le client.

Comportement client

Un client reçoit des messages Reconfigure envoyés au port UDP 546 sur les interfaces pour lesquelles il a acquis les informations de configuration via DHCP. Ces messages peuvent être envoyés à tout moment. Vu que le résultat d'une reconfiguration peut affecter les programmes de la couche application, le client devrait logger ces événements, et peut notifier les programmes des changements.

Réception des messages Reconfigure

À la reception d'un message Reconfigure valide, le client répond avec soit un message Renew soit un message Information-request. Le client ignore le champ transaction-id dans le message Reconfigure. pendant que la transaction est en progression, le client supprime silencieusement tout message Reconfigure reçus.

Création et transmission des messages Renew

En répondant à un Reconfigure, le client créé et envoie le message Renew exactement de la même manière que décris dans la section "création et transmission des messages Renew", à l'exception que le client copie l'option Option Request et les options IA du message Reconfigure dans le message Renew.

Création et transmission des messages Information-request

En répondans à un message Reconfigure, le client créé et envoie le message Information-request exactement comme dans la section "création et transmission des messages Information-request", à l'exception que le client inclus une option Server Identifier avec l'identifiant du message Reconfigure.

Timeout et retransmission des messages Renew et Information-request

Le client utilise les même variables et algorithmes de retransmission qu'avec les messages Renew et Information-request générés par un échange initié par le client. Si le client ne reçoit pas de réponse du serveur à la fin du processus de retransmission, le client ignore et supprime le message Reconfigure.

Réception des messages Reply

À la reception d'un message Reply valide, le client traite les options et définis ou réinitialise les paramètres de configuration. Le client enregistre et met à jours la durée de vie des adresse spécifiées dans les IA dans le message Reply.

Comportement de l'agent relais

L'agent relais peut être configuré pour utiliser une liste d'adresses de destination, qui peut inclure des adresse unicast, l'adresse All_DHCP_Servers, ou d'autres adresses sélectionnées par l'administrateur réseau. Si l'agent relais n'a pas été expicitement configuré, il doit utiliser l'adresse All_DHCP_Servers. Si l'agent relais relaye les messages à l'adresse All_DHCP_Servers ou d'autres adresses multicast, il définis le champ Hop Limit à 32.

Relayer un message client ou un message Relay-forward

Un agent relais relaye les messages des client et les messages Relay-forward depuis d'autres agents relais. Quand un agent relais reçoit un message valide à relayer, il construit un nouveau message Relay-forward. L'agent relais copie l'adresse source de l'en-tête IP du message reçus dans le champ peer-address du message Relay-forward. L'agent relais copie le message DHCP reçu dans une option Relay Message dans le nouveau message. L'agent relais ajoute d'autres options s'il est configuré pour les inclure.

Relayer un message du client

Si l'agent relais reçoit le message à relayer depuis un client, il place une adresse de scope globale ou de site avec un préfixe assigné au lien sur lequel le client devrait reçevoir une adresse dans le champ link-address. Cette adresse sera utilisée par le serveur pour déterminer le lien sur lequel le client devrait reçevoir une adresse et d'autres informations de configuration. Le Hop-Count est mis à 0.

Si l'agent relais ne peut pas utiliser l'adresse dans le champ link-address pour identifier l'interface via laquelle la réponse au client sera relayé, l'agent relais doit inclure une option Interface-id dans le message Relay-forward. Le serveur inclus l'option Interface-id dans son message Relay-reply. L'agent relais remplissent le champ link-address tel que décris dans le paragraphe précédent sans regarder s'il inclus une option Interface-id dans le message Relay-forward.

Relayer un message depuis l'agent relais

Si le message reçus par l'agent relais est un message Relay-forward et le hop-count est supérieur ou égal à HOP_COUNT_LIMIT, l'agent relais supprime le message.

L'agent relais copie l'adresse source de l'en-tête IP dans lequel le message a été reçus du client dans le champ peer-address dans le message Relay-forward et met le hop-count à la valeur du champs hop-count du message reçu, incrémenté de 1.

Si l'adresse source de l'en-tête IP du message reçus est une adresse global ou de site, l'agent relais met le champ link-address à 0 ; sinon l'agent relais met le champ link-address à l'adresse global ou de site assigné à l'interface sur laquelle le message a été reçu, ou inclus une option Interface-ID pour identifier l'interface sur laquelle le message a été reçu.

Relayer un message Relay-reply

L'agent relais traite les options incluses dans le message Relay-reply en plus de l'option Relay Message, puis supprime ces options.

L'agent relais extrait le message de l'option Relay Message et le transmet à l'adresse contenu dans le champ peer-address du message Relay-reply.

Si le message Relay-reply inclus une option Interface-ID, l'agent relais transmet le message du serveur au client sur le lien identifié. Sinon, si le champ link-address n'est pas à 0, l'agent relais transmet le message sur le lien identifié par le champ link-address.

Construction des message Relay-reply

Un serveur utilise un message Relay-reply pour retourner une réponse à un client si le message original du client a été relayé au serveur dans un message Relay-forward ou pour enoyer un message Reconfigure au client si le serveur n'a pas d'adresse utilisable pour envoyer le message directement.

Une réponse au client doit être relayée via le même agent relais que le message original. Le serveur créé un message Relay-reply qui inclus une option Relay Message contenant le message pour l'agent relais suivant dans le chemin de retour au client. Le message Relay-reply contient une autre option Relay Message à envoyer au prochain agent relais, et ainsi de suite. Le serveur doit enregistrer le contenu des champs peer-address dans le message reçu pour construire le message Relay-reply approprié.

Par exemple, si le client C envoie un message relayés par l'agent relais A au relais B puis au serveur, le serveur envoie le message Relay-reply à l'agent relais B :

msg-type : RELAY-REPLY
hop-count : 1
link-address : 0
peer-address : A
Relay Message option, contenant :
  msg-type : RELAY-REPLY
  hop-count : 0
  link-address : address from link to which C is attached
  peer-address : C
  Relay Message option : <response from server>

En envoyant un message Reconfigure à un client via un agent relais le serveur créé un message Relay-reply qui inclus une option Relay Message contenant le message Reconfigure pour le prochain agent relais dans le chemin de retour au client. Le serveur met le champs

peer-address dans l'en-tête du message Relay-repy à l'adresse du client, et met le champ link-address tel que requis par l'agent relais pour relayer le message Reconfigure au client. Le serveur obtient les adresses du client et de l'agent relais avant l'intéraction avec le client ou via un mécanisme externe.

Authentification des messages DHCP

Certains administrateurs réseaux peuvent souhaiter fournir l'authentification de la source et du contenu des messages DHCP. Par exemple, les client peuvent être sujets à des attaques par refus de service via l'utilisation de serveurs faux DHCP, ou par des serveurs mal configurés. Les administrateurs réseau peuvent souhaiter contraindre l'allocation des adresses aux hôtes autorisés pour éviter les attaques DOS.

Sécurité des messages envoyés entre les serveurs et agents relais

Les agents relais et les serveurs qui échangent des messages sécurisés utilisent les mécanismes IPsec pour IPv6. Si un message client est transféré via plusieurs agents relais, chaque agent relais doit avoir une relation de confiance établis. Les agents relais et les serveurs utilisent IPsec sous les conditions suivantes :

Selectors Les agents relais sont manuellement configurés avec les adresses de l'agent relais ou serveur auxquels les messages DHCP sont forwardés. Chaque agent relais et serveur qui utilise IPsec pour sécuriser les messages DHCP doit également être configuré avec une liste d'agents relais auxquels les messages sont transmis. Les sélecteurs pour les agents relais et serveurs échangent des messages DHCP sur les port UDP 546 et 547.

Mode Les agents relais et les serveurs utilisent le mode transport et ESP. Les informations dans les messages DHCP ne sont généralement pas considérés confidentiels, donc le chiffrement n'est pas utilisé.

Gestion de clé Parce que les agents relais et les serveurs sont utilisés dans une organisation, les schémas à clé publique ne sont pas nécessaires. Parce que les agents relais et les serveurs doivent être configurés manuellement, la gestion de clé manuelle peut suffire, mais n'offre pas de défense contre les messages rejoués. IKE avec des clé pré-partagés devraient être supportés. IKE avec des clés publiques peut être supporté.

Stratégie de sécurité Les messages DHCP entre les agents relais et les serveurs devraient seulement être acceptés des paires DHCP tel qu'identifié dans la configuration locale

Authentification Les clés partagées, indexées à l'adresse IP source du message DHCP reçus, sont adéquats dans cette application

Disponibilité Les implémentations IPsec appropriées sont disponibles pour les serveurs et agents relais dans des périphériques plus récents dans l'entreprise.

Sommaire de l'authentification DHCP

L'authentification des messages DHCP est accomplis via l'utilisation de l'option Authentication. Les informations d'authentification dans cette option peuvent être utilisées pour identifier de manière fiable la source d'un message DHCP et pour confirmer que le contenu du message DHCP n'a pas été altéré.

L'option Authentication fournis un framework pour plusieurs protocoles d'authentification. 2 sont définis ici. Tout message DHCP ne doit pas inclure plus d'une option Authentication.

Le champ protocole dans l'option Authentication identifie le protocole spécifique utilisé pour générer les informations d'authentification dans l'option. Le champ algorithm identifie un algorithme spécifique dans le protocole d'authentification ; par exemple, le champ algorithm spécifie l'algorithme de hashage utilisé pour générer le MAC dans l'option authentication. Le champ Replay Detection Method (RDM) spécifie le type de détection utilisé.

Détection de répétition

Le champ Replay Detection Method (RDM) détermine le type de détection de répétition utilisé dans le champ Replay Detection.

Si le champ RDM contient 0x00, le champ Replay Detection doit être mis à la valeur d'un compteur monotonique incrémental. Utiliser un compteur, tel que la date courante, peut réduire le risque d'attaques. Cette méthode doit être supporté par tous les protocoles.

Protocole d'authentification retardé

Si le champ protocole est 2, le message utilise le mécanisme "delayed authentication". Dans l'authentification retardée, le client demande une authentification dans son message Solicit, et le serveur répond avec un message Advertise qui inclus l'authentification. Cette information d'authentification contient une valeur nonce générée par la source comme un MAC pour fournir une authentification du message et de l'entité. L'utilisation d'une technique particulière basée sur HMAC en utilisant MD5 est définis ici.

Option Authentication dans le protocole Delayed Authentication

Dans un message Solicit, le client remplis les champs protocol, algorithm et RDM dans l'option Authentication avec les préférences du client. Le client met le champ replay detection à 0 et omet le champ authentication information. Le client met le champ option-len à 11.

Dans tous les autres messages, les champs protocol et algorithm identifient la méthode utilisée pour construire le contenu du champ authentication information. Le champ RDM identifie la méthode utilisée pour construire le contenu du champ replay detection. Le format de Authentication information est :

DHCP realm Le royaume DHCP qui identifie la clé utilisée pour générer la valeur HMAC-MD5

key ID L'identifiant de clé qui identifie la clé utilisée pour générer la valeur HMAC-MD5

HMAC-MD5 Le MAC généré en appliquant un MD5 au message DHCP en utilisant l'identifiant de clé par le DHCP realm, client DUID, et key ID.

L'émeteur calcule le MAC en utilisant l'algorithme de génération HMAC et la fonction de hashage MD5. Tout de message DHCP, incluant l'en-tête et les options, sont utilisé comme entrée dans la fonction de calcul MD5

Validation du message

Tout message DHCP qui inclus plus d'une option authentication doit être détruit.

Pour valider un message entrant, le receveur vérifie d'abord que la valeur dans le champ replay detection est acceptable en accord avec la méthode spécifiée dans le champ RDM. Ensuite, le reçeveur calcule le MAC. Tout le message est utilisé en entrée de la fonction MAC, en mettant le champ MAC à 0. Si le MAC calculé ne correspond pas avec celui reçu, le reçeveur détruit le message DHCP.

Utilisation de clé

Chaque client DHCP a un jeu de clés. Chaque clé est identifié par <DHCP realm, client DUID, key id>. Chaque clé a également une durée de vie. La clé ne peut pas être utilisé avant la fin de sa durée de vie. Les clés du client sont initialement distribuées au client via un mécanisme tiers. La durée de vie pour chaque clé est distribuée avec la clé.

Le client et le serveur utilise une des clés du client pour authentifier les messages DHCP durant une session (jusqu'au prochain message Solicit envoyé par le client).

Considération client pour le protocole d'authentification retardé

Le client annonce son intention d'utiliser l'authentification DHCP en incluant une option Authentication dans son message Solicit. Le serveur séléctionne une clé pour le client basé sur le DUID du client. Le client et le serveur utilisent cette clé pour authentifier tous les messages DHCP échangés durant la session.

Envoyer des messages Solicit

Quand le client envoie un message Solicit et souhaite utiliser l'authentification, il inclus une option Authentication avec le protocole désiré, l'algorithme et RDM. Le client n'inclus pas replay detection ni authentication information dans l'option Authentication.

Recevoir les messages Advertise

Le client valide tous message Advertise contenant une option Authentication spécifiant le protocole d'authentication retardé en utilisant le teste de validation.

Le comportement de client si aucun message Advertise n'inclus d'information d'authentification ou ne passe le test de validation, est contrôlé par sa stratégie locale.

Un client doit être configurable pour supprimer les messages non-authentifiés et devrait être configuré par défaut pour les supprimer si le client a été configuré avec une clé d'authentification.

Envoyer des messages Request, Confirm, Rebind, Decline ou Release

Si le cilent a authentifié le message Advertise avec lequel le client a séléctionné le serveur, le client doit générer les informations d'authentification pour les messages suivants. Quand le client envoie un message, il doit utiliser la même clé utilisée par le serveur pour générer les informations d'authentification.

Envoyer des messages Information-request

Si le serveur a séléctionné une clé pour le client dans un échange précédent, le client doit utiliser la même clé durant la session.

Reçevoir des messages Reply

Si le client a authentifié le Advertise qu'il accepte, le client doit valider le message Reply associé depuis le serveur. Le client doit détruire le Reply si le message échoue le test de validation et peut logger l'erreur. Si le Reply échoue le test, le client doit redémarrer le processus

de configuration DHCP en envoyant un message Solicit.

Considération serveur

Une fois reçus un message Solicit qui contient une option Authentication, le serveur détecte une clé pour le client, basée sur le DUID du client et la stratégie de sélection de clé. Le serveur identifie la clé séléctionnée dans le message Advertise et utilise la clé pour valider tous les autres messages reçus.

Réception de Solicit et envoie de Advertise

Le serveur séléctionne une clé pour le client et inclus les informations d'authentification dans le message Advertise retourné au client. Le serveur doit enregistrer l'identifiant de la clé séléctionnée pour le client et utilise cette clé pour valider tous les autres messages échangés avec le client.

Réception de Request, Confirm, Renew, Rebind, Release et envoie de Reply

Le serveur utilise l'identifiant de clé dans le message et valide le message. Si le message échoue le test ou le serveur ne connaît pas l'identifiant de clé, le serveur doit détruire le message et peut logger l'erreur.

Si le message passe le test, le serveur répond au message en incluant les informations d'authentification générées en utilisant la clé identifiée dans le message reçu.

Protocole de reconfiguration de clé d'authentification

Ce protocole fournis une protection contre les mauvaises configurations d'un client causé par un message Reconfigure envoyé par un serveur DHCP malicieux. Dans ce protocole, un serveur DHCP envoie un Reconfigure Key au client dans l'échange initial. Le client enregistre le Reconfigure Key à utiliser pour authentifier les messages Reconfigure suivants de ce serveur. Le serveur inclus un HMAC calculé depuis le Reconfigure Key dans les messages Reconfigure suivants.

Le Reconfigure Key envoyé par le serveur et le HMAC dans les messages Reconfigure suivants sont gérés dans une option Authentication. Le protocole Reconfigure Key est utilisé seulement si le client et le serveur n'utilisent pas d'autres protocole d'authentification et que le client et le serveur ont négocié l'utilisation des messages Reconfigure.

Les champs suivants sont mis dans une option Authentication pour le protocole d'authentification Reconfigure Key :

protocol 3

algorithm 1

RDM 0

Le format des informations d'authentification pour le Reconfigure Key Authentication Protocol contient un champ Type sur 1 octet contenant le type dans le champ Value (1=Reconfigure Key, utilisé dans la réponse,2=HMAC-MD5 du message, utilisé dans un message Reconfigure). Le champ Value contient les données.

Considérations serveur pour le protocole Reconfigure Key

Le serveur séléctionne un Reconfigure Key pour un client durant un échange Request/Reply, Solicit/Reply ou Information-request/Reply. Le serveur enregistre le Reconfigure Key et transmet cette clé au client dans une option Authentication dans le Reply. Le Reconfigure Key fait 128bits de long, et doit être un nombre aléatoire cryptographiquement fort.

Pour fournir l'authentification pour un message Reconfigure, le serveur sélectionne une valeur replay detection en accord avec le RDM séléctionné par le serveur, et calcul un HMAC-MD5 du message Reconfigure en utilisant le Reconfigure Key pour le client. Le serveur calcul le HMAC-MD5 sur tout le message Reconfigure, incluant l'option Authentication ; le champ HMAC-MD5 est mis à 0. Le serveur inclus le HMAC-MD5 dans le champ authentication information dans une option Authentication inclus dans le message Reconfigure envoyé au client.

Considérations client pour le protocole Reconfigure Key

Le client reçoit un Reconfigure Key du serveur dans le message Reply initial du serveur. Le client enregistre le Reconfigure Key à utiliser dans les messages Reconfigure suivants.

Pour authentifier un message Reconfigure, le client calcul un HMAC-MD5 du message DHCP en utilisant le Reconfigure Key reçus du serveur. Si le HMAC-MD5 calculé correspond avec la valeur dans l'option Authentication, le client accepte le message Reconfigure.

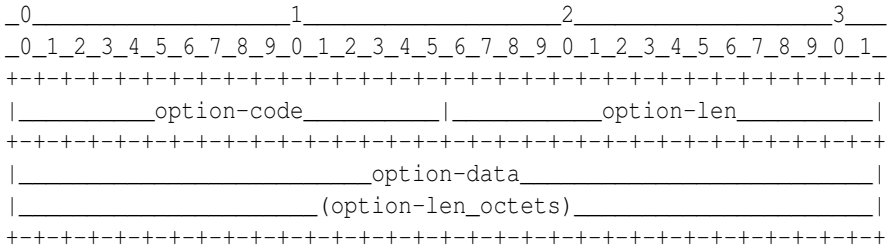
Options DHCP

Les options sont utilisées pour qérer des informations additionnelles et paramètres dans les messages DHCP. Toutes les options partagent une base commune. Ce document décris les options DHCP de base de la spécification DHCP. D'autres options peuvent être définies dans des documents séparées.

Sauf mention, chaque option peut apparaître seulement dans la zone d'options et peut apparaître seulement une seule fois.

Format des options

Le format des options DHCP est :



option-code Un entier non-signé identifiant le type d'option.

option-len Un entier non-signé donnant la longueur du champ option-data

option-data Les données pour l'option

Client Identifier

L'option Client Identifier est utilisé pour spécifier un DUID identifiant un client.

option-code OPTION_CLIENTID (1)
option-len Longueur du DUID en octets
DUID Le DUID du client.

Serveur Identifier

L'option Serveur Identifier est utilisé pour spécifier un DUID identifiant un serveur.

option-code OPTION_SERVERID (2)
option-len Longueur du DUID en octets
DUID Le DUID du serveur

Identity Association for Non-temporary Addresses

Gère un IA_NA, les paramètres associés et les adresses non-temporaires associées.

option-code OPTION_IA_NA (3)
option-len 12 + longueur du champ IA_NA-options
IAID Identifiant unique pour cet IA_NA.
T1 Temps auquel le client contacte le serveur auprès duquel l'IA_NA a été obtenus pour étendre la durée de vie, exprimée en secondes
T2 Temps auquel le client contacte un serveur disponible pour étendre la durée de vie des adresses assignée.
IA_NA-options Options associées avec cet IA_NA

Noter qu'un IA_NA n'a pas de durée de vie associée. Dans un message envoyé par le client, les temps T1 et T2 sont les préférences du client.

Identity Association for Temporary Addresses

Gère un IA_TA, les paramètres associés et les adresses temporaire associées.

option-code OPTION_IA_TA (4)
option-len 4 + longueur du champ IA_TA-options
IAID Identifiant unique pour cet IA_TA
IA_TA-options Options associées avec cet IA_TA

Quand la durée de vie de toutes les adresses dans un IA_TA ont exprirés, l'IA peut être considéré comme expiré.

IA Address

L'option IA Address est utilisée pour spécifier les adresses IPv6 associées avec un IA_NA ou un IA_TA. Cette option doit être encapsulée dans le champ Option pour une option IA_NA ou IA_TA.

option-code OPTION_IAADDR (5)
option-len 24 + longueur du champ IAaddr-options
IPv6 address Une adresse IPv6
Preferred-lifetime Durée de vie préférrée pour l'adresse, en secondes
valid-lifetime Durée de vie valide pour l'adresse, en secondes
IAaddr-options Options associées avec cette adresse

Option Request

Utilisé pour identifier une liste d'options dans un message entre un client et un serveur.

option-code OPTION_ORO (6)
option-len 2*nombre d'options demandées
requested-option-code-n Le code d'option demandé.

Preference

Cette option est envoyée par un serveur à un client pour affecter la sélection d'un serveur par le client.

option-code OPTION_PREFERENCE (7)
option-len 1
pref-value La valeur de préférence pour le serveur dans ce message

Elapsed Time

option-code OPTION_ELAPSED_TIME (8)
option-len 2
elapsed-time Durée depuis que le client a commencé sa transaction DHCP. exprimé en centièmes de secondes

Relay Message

Transporte un message DHCP dans un message Relay-forward ou Relay-reply

option-code OPTION_RELAY-MSG (9)
option-len Longueur du DHCP-relay-message
DHCP-relay-message Le message DHCP à relayer.

Authentication

Gère les informations d'authentification pour authentifier l'identité et le contenu des messages DHCP.

option-code OPTION_AUTH (11)
option-len 11 + Longueur du champ information
protocol Protocole utilisé
algorithm Algorithme utilisé
RDM Méthode de détection de rejeu.
Replay detectsion Information de détection pour le RDM
authentication information L'information d'authentification tel que spécifié par protocol et algorithm

Server Unicast

Le serveur envoie cette option à un client pour indiquer que le client est autorisé à unicast les messages au serveur.

option-code OPTION_UNICAST (12)
option-len 16
server-address L'adresse IP où envoyer les messages

Status Code

Retourne le status lié au message ou l'option dans laquelle elle apparaît.

option-code OPTION_STATUS_CODE (13)
option-len 2 + longueur du status-message
status-code code de status
status-message Chaîne UTF-8 à afficher à l'utilisateur. ne doit pas se terminer par une NULL.

Rapid Commit

Utilisé pour signaler l'utilisation d'un échange 2 messages.

option-code OPTION_RAPID_COMMIT (14)
option-len 0

User Class

Utilisé par un client pour identifier le type ou la catégorie d'utilisateur ou d'applications qu'il représente

option-code OPTION_USER_CLASS (15)
option-len Longueur du champ user-class-data
user-class-data Classes utilisateur envoyé par le client

Vendor Class

Utilisé par un client pour identifier le vendeur du hardware sur lequel le client fonctionne.

option-code OPTION_VENDOR_CLASS (16)
option-len 4 + longueur de vendor-class-data
enterprise-number Enterprise Number du vendeur
vendor-class-data Configuration hardware de l'hôte

Vendor-specific Information

Utilisé par les clients et serveur pour échanger des informations spécifiques au client

option-code OPTION_VENDOR_OPTS (17)
option-len 4 + longueur de option-data
enterprise-number Enterprise Number du vendeur
option-data object opaque interprété par le code spécifique au vendeur

Interface-Id

L'agent relais peut envoyer l'option Interface-Id pour identifier l'interface sur laquelle le message client a été reçu.

option-code OPTION_INTERFACE_ID (18)
option-len longueur de interface-id
interface-id Valeur opaque générée par l'agent relais pour identifier un de ses interfaces.

Reconfigure Message

Un serveur inclus une option Reconfigure Message dans un message Reconfigure pour indiquer au client si le client réponds avec un message Renew ou un message Information-request.

option-code

option-len

msg-type

Reconfigure Accept

Un client utilise cette option pour annoncer au serveur qu'il accept les messages Reconfigure, et le serveur l'utilise pour indiquer au client s'il accepte les message Reconfigure.

option-code OPTION_RECONF_ACCEPT
option-len 0

Adresses Multicast

All_DHCP_Relay_Agents_and_Servers address FF02 : :1 :2
All_DHCP_Servers address FF05 : :1 :3

Types de messages DHCP

SOLICIT 1
ADVERTISE 2
REQUEST 3
CONFIRM 4
RENEW 5
REBIND 6
REPLY 7
RELEASE 8
DECLINE 9
RECONFIGURE 10
INFORMATION-REQUEST 11
RELAY-FORW 12
RELAY-REPL 13

Options DHCP

OPTION_CLIENTID 1
OPTION_SERVERID 2
OPTION_IA_NA 3
OPTION_IA_TA 4
OPTION_IAADDR 5
OPTION_ORO 6
OPTION_PREFERENCE 7
OPTION_ELAPSED_TIME 8
OPTION_RELAY_MSG 9
OPTION_AUTH 11
OPTION_UNICAST 12
OPTION_STATUS_CODE 13
OPTION_RAPID_COMMIT 14
OPTION_USER_CLASS 15
OPTION_VENDOR_CLASS 16
OPTION_VENDOR_OPTS 17
OPTION_INTERFACE_ID 18
OPTION_RECONF_MSG 19
OPTION_RECONF_ACCEPT 20

Codes de status

Success 0 Succès

UnspecFail 1 Erreur, raison non spécifiée

NoAddrsAvail 2 Le serveur n'a pas d'adresses disponible à assigner aux IA

NoBinding 3 Enregistrement client non disponible

NotOnLink 4 Le préfix pour l'adresse n'est pas approprié pour le lien sur lequel le client est attaché

UseMulticast 5 Indique au client d'utiliser multicast.