Exonet : ICMPv6

Description

Propriétés	Description
Intitulé long	Comprendre les mécanismes de base d' Ipv6 avec l'étude du protocole ICMPv6
Public concerné	BTS Services informatiques aux organisations
Matière	SISR2 – Conception des infrastructures réseaux
Compétences	Analyser des unités de données de protocole
Savoirs	Technologies et techniques d'adressage et de nommage
Objectifs	Présentation du protocole ICMPv6
Mots-clés	Unicast Multicast Adresse globale Adresse Lien Local Adresse Mac ICMPv6
Auteur(es)	Roger SANCHEZ (avec la très précieuse collaboration d'Apollonie RAFFALLI)
Version	v 1.0
Date de publication	Avril 2009

Contexte de travail

L'entreprise Lapointe envisage une évolution vers le protocole Ipv6. En tant qu'administrateur réseau vous êtes chargé d'étudier ce protocole. Après avoir étudié théoriquement l'adressage Ipv6 (exonet "adressage IPv6") vous avez décidé de mettre en œuvre un réseau IPv6 pour comprendre les mécanismes de base utilisés par ce protocole. Pour cela vous avez capturé des échanges à l'aide d'un analyseur de trames.

Vous trouverez en annexe 1 Les concepts généraux du protocole ICMPv6.
Vous trouverez en annexe 2 Les différentes trames capturées.

Travail à réaliser

Capture 1

1. Donner le libellé correspondant au type ICMPv6.
2. De quel type sont les adresses MAC et IPv6 destination ?
3. Relever l'adresse "target". Comparer cette adresse avec l'adresse IPv6 destination. Expliquer le rôle de cette adresse.
4. Donner l'adresse source IPv6. Expliquer cette adresse.

Capture 2

1. Donner le libellé correspondant au type ICMPv6.
2. De quel type sont les adresses MAC et IPV6 de destination ?
3. Dire quels sont les postes qui liront les paquets adressés à cette adresse.

Capture 3

1. Donner le libellé correspondant au type ICMPv6.
2. De quel type sont les adresses MAC et IPV6 de destination ?
3. Dire quels sont les postes qui liront les paquets adressés à cette adresse.
4. Donner les conséquences sur la configuration des postes après lecture de ce paquet.

Capture 4

1. Donner le libellé correspondant au type ICMPv6.
2. De quel type sont les adresses MAC et IPv6 destination ?
3. Donner l'adresse source IPv6. Dire pourquoi cette adresse est différente de l'adresse source de la capture 1.
4. Expliquer le rôle de l'adresse "Link Layer".

Capture 5

1. Donner le libellé correspondant au type ICMPv6.
2. De quel type est l'adresse MAC destination ?
3. Comparer l'adresse IPv6 de destination de la capture 4 avec l'adresse MAC source de la capture 5. Expliquer.
4. Expliquer le rôle de l'adresse "Link Layer".

Capture 6

1. Donner le libellé correspondant au type ICMPv6.
2. De quel type est l'adresse MAC destination ?
3. Relever le numéro de séquence.

Capture 7

1. Donner le libellé correspondant au type ICMPv6.
2. De quel type est l'adresse MAC destination ?
3. Relever le numéro de séquence et le comparer au numéro de séquence de la capture 6. Expliquer le rôle du numéro de séquence.

Annexes : présentation du protocole ICMPv6

Fonctions générales du protocole ICMPv6

- Détection d'erreurs
- Test (ping)
- Configuration automatique des équipements (découverte des voisins et des routeurs)
- Gestion de groupe Multicast

Usages courants du protocole ICMPv6

- Résolutions d'adresses (remplace ARP)
- Détection d'inaccessibilité des voisins (NUD *neighbor unreachability detection*) (pas d'équivalent IPV4). Permet de mettre à jour les tables de configuration par exemple la table de routage
- Configuration des routeurs (remplace ICMP *router Discovery* de Ipv4)
- Apprentissage des préfixes en fonction des annonces faites par les routeurs
- Détection des adresses dupliquées (équivalent à l'ARP gratuit)
- Découverte des paramètres (notamment le MTU, nombre de sauts avec DHCPv6)
- Redirection (remplace ICMP redirect d'Ipv4 mais dans IPV6 **l'association entre préfixe et réseau local est moins stricte**. On peut imaginer une configuration où l'équipement ne dialogue qu'avec son routeur par défaut qui l'informe des équipements destinataires sur son lien.

De fait, ICMPv6 remplace le protocole ARP et IGMP d'IPV4 mais aussi l'affectation automatique des routeurs par DHCP dans Ipv4.

Le protocole ICMPv6 a le numéro 58.

Format d'un message ICMP

- Type : 8 bits
- Code : 8 bits
- Checksum : 16 bits
- Données ICMP (multiple de 32).

Le champ "type" code la nature du message .Les valeurs inférieures à 127 sont des messages d'erreur, les autres valeurs sont des messages d'information.
Le code précise la cause du message.
Le checksum prend en compte le pseudo-entête.

Type	Code	*Nature*/message
		Gestion des erreurs (type < 127)
1		Destination inaccessible (*Destination Unreachable*)
	0	Aucune route vers la destination
	1	La communication avec la destination est administrativement interdite
	2	Hors portée de l'adresse source
	3	l'adresse est inaccessible
	4	Le numéro de port est inaccessible
2		Paquet trop grand (*Packet Too Big*)
3		Temps dépassé (*Time Exceeded*)
	0	limite du nombre de sauts atteinte
	1	temps de réassemblage dépassé

4		Erreur de paramètre (*Parameter Problem*)
	0	champ d'entête erroné
	1	champ d'entête suivant non reconnu
	2	option non reconnue
		information
128		Demande d'écho (*Echo Request*)
129		Réponse d'écho (*Echo Reply*)
		gestion des groupes multicast (MLD RFC 2710)
130		Enquête d'abonnement (*Group Membership Query*)
131		Rapport d'abonnement (*Group Membership Report*)
132		Fin d'abonnement (*Group Membership Reduction*)
		Découverte des voisins (RFC 2461)
133		Sollicitation du routeur (*Router Solicitation*)
134		Annonce du routeur (*Router Advertisement*)
135		sollicitation d'un voisin (*Neighbor Solicitation*)
136		annonce d'un voisin (*Neighbor Advertisement*)
137		Redirection (*Redirect*)
		Renumérotation des routeurs (expérimental RFC 2894)
138		Renumérotation des routeurs (*Router Renumbering*)
	0	Commande
	1	Résultat
	255	Remise à zéro du numéro de séquence
		Recherche d'information sur un nœud (expérimental)
139		Demande d'information (ICMP *Node Information* Query)
140		Réponse d'information (ICMP *Node Information Response*)
		Découverte de voisins inverse
141		Sollicitation (*Inverse Neighbor Discovery Solicitation Message*)
142		Aannonce (*Inverse Neighbor Discovery Advertisement Message*)
		Gestion des groupes multicast
143		Rapport d'abonnement MLDv2
		Mobilité
144		Découverte d'agent mère (requête)
145		Découverte d'agent mère (réponse)
146		Sollicitation de préfixe mobile
147		Annonce de préfixe mobile
		Découverte de voisins sécurisées (RFC 3971)
148		Sollicitation de chemin de certification
149		Annonce du chemin de certification
		Mobilité
150		Protocoles de mobilité expérimentaux

Configuration de l'adresse lien local avec icmpv6

Au démarrage, le poste calcule son adresse lien local puis envoie sur le réseau un message icmpV6 "*neighbor solicitation*" avec sa propre adresse (algorithme DAD) pour vérifier que son adresse n'est pas utilisée sur le lien.

Sollicitation d'un voisin pour un échange

Un poste voulant communiquer avec un autre poste doit récupérer son adresse MAC si celle-ci n'est pas déjà dans son cache. Pour cela il émet sur le réseau un "*neighbor solicitation*", le poste qui reconnaît son adresse dans la demande répond en envoyant un "*neighbor advertisement*".

Remarque : quand un poste s'initialise, il adhère à au moins deux groupes multicast :

- ff02::1 : tous les noeuds sur le lien
- L'adresse multicast sollicitée qui est obtenue en concaténant le préfixe ff02::1:ff00:0/104 aux 24 derniers bits de l'identifiant d'interface.

C'est cette adresse que va utiliser un poste qui connaît l'adresse IPv6 pour rechercher l'adresse MAC correspondante.

Test d'une liaison entre deux postes

Après avoir récupéré l'adresse MAC d'un poste, un poste peut tester la liaison en émettant des "echo request" avec ICMPv6. Le poste destinataire répond à chaque "request" par des "echo reply". L'ordre des différents échanges est géré par un numéro de séquence associé à chaque paquet.

Découverte des routeurs

Un poste IPv6 qui démarre sur un réseau, cherche à découvrir les routeurs présents sur le réseau pour déterminer éventuellement ses préfixes globaux et sa route par défaut. Il émet pour cela une demande ICMPv6 "*router solicitation*".

Annonce des routeurs

Dans IPv6 un routeur a deux rôles :

- router les paquets (il doit être configuré pour cela)
- donner des éléments de configuration aux postes de travail

Un routeur émet un "*router advertisement*" pour permettre aux postes présents sur les liens locaux sur lequel il est connecté, de configurer leurs préfixes globaux et leur route par défaut. Le routeur émet ce message soit en réponse à une sollicitation, soit périodiquement en fonction de son paramétrage.

Annexe 2 : capture d'échanges ICMPv6

Capture 1

```
Ethernet II, Src: 00:03:ff:1e:ef:1e, Dst: 33:33:ff:1e:ef:1e
   Destination: 33:33:ff:1e:ef:1e (IPv6-Neighbor-Discovery_ff:1e:ef:1e)
   Source: 00:03:ff:1e:ef:1e (Microsof_1e:ef:1e)
   Type: IPv6 (0x86dd)
Internet Protocol Version 6
   Version: 6
   Traffic class: 0x00
   Flowlabel: 0x00000
   Payload length: 24
   Next header: ICMPv6 (0x3a)
   Hop limit: 255
   Source address: ::
   Destination address: ff02::1:ff1e:ef1e
Internet Control Message Protocol v6
   Type: 135
   Code: 0
   Checksum: 0x9da9 (correct)
   Target: fe80::203:ffff:fe1e:ef1e
```

Capture 2

```
Ethernet II, Src: 00:03:ff:1e:ef:1e, Dst: 33:33:00:00:00:02
   Destination: 33:33:00:00:00:02 (IPv6-Neighbor-Discovery_00:00:00:02)
   Source: 00:03:ff:1e:ef:1e (Microsof_1e:ef:1e)
   Type: IPv6 (0x86dd)
Internet Protocol Version 6
   Version: 6
   Traffic class: 0x00
   Flowlabel: 0x00000
   Payload length: 16
   Next header: ICMPv6 (0x3a)
   Hop limit: 255
   Source address: fe80::203:ffff:fe1e:ef1e
   Destination address: ff02::2
Internet Control Message Protocol v6
   Type: 133
   Code: 0
   Checksum: 0x9eac (correct)
   ICMPv6 options
      Type: 1 (Source link-layer address)
      Length: 8 bytes (1)
      Link-layer address: 00:03:ff:1e:ef:1e
```

Capture 3

```
Ethernet II, Src: 02:00:4c:4f:4f:50, Dst: 33:33:00:00:00:01
   Destination: 33:33:00:00:00:01 (IPv6-Neighbor-Discovery_00:00:00:01)
   Source: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50)
   Type: IPv6 (0x86dd)
Internet Protocol Version 6
```

Version: 6
Traffic class: 0x00
Flowlabel: 0x00000
Payload length: 96
Next header: ICMPv6 (0x3a)
Hop limit: 255
Source address: fe80::4cff:fe4f:4f50
Destination address: ff02::1
Internet Control Message Protocol v6
Type: 134
Code: 0
Checksum: 0x8a71 (correct)
Cur hop limit: 0
Flags: 0x00
0... .... = Not managed
.0.. .... = Not other
..0. .... = Not Home Agent
...0 0... = Router preference: Medium
Router lifetime: 0
Reachable time: 0
Retrans time: 0
ICMPv6 options
Type: 1 (Source link-layer address)
Length: 8 bytes (1)
Link-layer address: 02:00:4c:4f:4f:50
ICMPv6 options
Type: 5 (MTU)
Length: 8 bytes (1)
MTU: 1500
ICMPv6 options
Type: 3 (Prefix information)
Length: 32 bytes (4)
Prefix length: 64
Flags: 0xc0
1... .... = Onlink
.1.. .... = Auto
..0. .... = Not router address
...0 .... = Not site prefix
Valid lifetime: 0xffffffff
Preferred lifetime: 0xffffffff
Prefix: 2001:688:1f80:2000::
ICMPv6 options
Type: 3 (Prefix information)
Length: 32 bytes (4)
Prefix length: 0
Flags: 0x80
1... .... = Onlink
.0.. .... = Not auto
..0. .... = Not router address
...0 .... = Not site prefix
Valid lifetime: 0xffffffff
Preferred lifetime: 0xffffffff
Prefix: ::

Capture 4

Ethernet II, Src: 00:03:ff:18:ef:1e, Dst: 33:33:ff:4f:4f:50
Destination: 33:33:ff:4f:4f:50 (IPv6-Neighbor-Discovery_ff:4f:4f:50)
Source: 00:03:ff:18:ef:1e (Microsof_18:ef:1e)

Type: IPv6 (0x86dd)
Internet Protocol Version 6
Version: 6
Traffic class: 0x00
Flowlabel: 0x00000
Payload length: 32
Next header: ICMPv6 (0x3a)
Hop limit: 255
Source address: fe80::203:ffff:fe18:ef1e
Destination address: ff02::1:ff4f:4f50
Internet Control Message Protocol v6
Type: 135)
Code: 0
Checksum: 0xb4e8 (correct)
Target: fe80::4cff:fe4f:4f50
ICMPv6 options
Type: 1 (Source link-layer address)
Length: 8 bytes (1)
Link-layer address: 00:03:ff:18:ef:1e

Capture 5

Ethernet II, Src: 02:00:4c:4f:4f:50, Dst: 00:03:ff:18:ef:1e
Destination: 00:03:ff:18:ef:1e (Microsof_18:ef:1e)
Source: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50)
Type: IPv6 (0x86dd)
Internet Protocol Version 6
Version: 6
Traffic class: 0x00
Flowlabel: 0x00000
Payload length: 32
Next header: ICMPv6 (0x3a)
Hop limit: 255
Source address: fe80::4cff:fe4f:4f50
Destination address: fe80::203:ffff:fe18:ef1e
Internet Control Message Protocol v6
Type: 136
Code: 0
Checksum: 0x5807 (correct)
Flags: 0x60000000
0... .... = Not router
.1.. .... = Solicited
..1. .... = Override
Target: fe80::4cff:fe4f:4f50
ICMPv6 options
Type: 2 (Target link-layer address)
Length: 8 bytes (1)
Link-layer address: 02:00:4c:4f:4f:50

Capture 6

Ethernet II, Src: 00:03:ff:18:ef:1e, Dst: 02:00:4c:4f:4f:50
Destination: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50)
Source: 00:03:ff:18:ef:1e (Microsof_18:ef:1e)
Type: IPv6 (0x86dd)
Internet Protocol Version 6
Version: 6
Traffic class: 0x00
Flowlabel: 0x00000
Payload length: 40

Next header: ICMPv6 (0x3a)
Hop limit: 128
Source address: fe80::203:ffff:fe18:ef1e
Destination address: fe80::4cff:fe4f:4f50
Internet Control Message Protocol v6
Type: 128
Code: 0
Checksum: 0x4c42 (correct)
ID: 0x0000
Sequence: 0x01db
Data (32 bytes)

Capture 7

Ethernet II, Src: 02:00:4c:4f:4f:50, Dst: 00:03:ff:18:ef:1e
Destination: 00:03:ff:18:ef:1e (Microsof_18:ef:1e)
Source: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50)
Type: IPv6 (0x86dd)
Internet Protocol Version 6
Version: 6
Traffic class: 0x00
Flowlabel: 0x00000
Payload length: 40
Next header: ICMPv6 (0x3a)
Hop limit: 128
Source address: fe80::4cff:fe4f:4f50
Destination address: fe80::203:ffff:fe18:ef1e
Internet Control Message Protocol v6
Type: 129
Code: 0
Checksum: 0x4b42 (correct)
ID: 0x0000
Sequence: 0x01db
Data (32 bytes)

Proposition de correction

Capture 1

1. Donner le libellé correspondant au type ICMPv6.

Type: 135 (Neighbor solicitation)

2. De quel type sont les adresses MAC et IPv6 destination ?

Ce sont des adresses multicast.

3. Relever l'adresse "target". Comparer cette adresse avec l'adresse MAC source. Expliquer le rôle de cette adresse

Target: fe80::203:ffff:fe1e:ef1e. C'est l'adresse lien local du poste (prefix FE80). Elle est déduite de l'adresse MAC du poste. Le poste teste l'unicité de son adresse autoconfigurée.

4. Donner l'adresse source IPv6. Expliquer cette adresse.

L'adresse source :: correspond à l'adresse tout à zéro. C'est l'adresse indéterminée. Elle est utilisée ici car le poste teste l'adresse qu'il a autoconfiguré et ne peut donc encore l'utiliser.
S'il n'y a pas de réponse, le poste utilisera cette adresse sinon une intervention manuelle est nécessaire.

.

Capture 2

1. Donner le libellé correspondant au type ICMPv6.

Type: 133 (Router solicitation)

2. De quel type sont les adresses MAC et IPV6 de destination ?

Ce sont des adresses multicast.

3. Dire quels sont les postes qui liront les paquets adressés à cette adresse.

Ces adresses multicast correspondent aux routeurs. Les postes qui démarrent sur le réseau contactent les routeurs présents sur le lien local pour configurer leurs préfixes globaux et leur route par défaut.

Capture 3

1. Donner le libellé correspondant au type ICMPv6.

Type: 134 (Router advertisement)

2. De quel type sont les adresses MAC et IPV6 de destination ?

Ce sont des adresses multicast.

3. Dire quels sont les postes qui liront les paquets adressés à cette adresse.

L'adresse multicast correspond à tous les postes présents sur le lien local. Ceux-ci liront l'annonce ICMPv6 envoyé par le routeur.

4. Donner les conséquences sur la configuration des postes après lecture de ce paquet.

Les postes vont configurer un prefixe global égal à 2001:688:1f80:2000, et une route par défaut grâce au préfixe ::.

Remarque : Ces trois premières captures correspondent à l'initialisation d'un poste sur le réseau

Capture 4

1. Donner le libellé correspondant au type ICMPv6.

Type: 135 (Neighbor solicitation)

2. De quel type sont les adresses MAC et IPv6 destination ?

Ce sont des adresses multicast.

3. Donner l'adresse source IPv6. Dire pourquoi cette adresse est différente de l'adresse source de la capture 1.

Source address: fe80::203:ffff:fe18:ef1e. Il ne s'agit pas ici de tester l'adresse autoconfigurée mais de demander sur le lien local à quelle adresse MAC correspond l'adresse IPv6.

4. Expliquer le rôle de l'adresse "Link Layer".

L'adresse Link layer correspond à l'adresse MAC de l'émetteur. Le poste qui fait une requête "neighbor sollicitation" fournit son adresse MAC pour que la réponse se fasse en unicast.

Capture 5

1. Donner le libellé correspondant au type ICMPv6.

Type: 136 (Neighbor advertisement)

2. De quel type est l'adresse MAC destination ?

C'est une adresse unicast qui correspond à l'adresse du poste demandeur "neighbor solicitation".

3. Comparer l'adresse IPv6 de destination de la capture 4 avec l'adresse MAC source de la capture 5. Expliquer.

Destination address (capture4) : ff02::1:ff4f:4f50 : c'est une adresse multicast sollicitée qui est dérivée de l'adresse IPv6 de destination : les 24 derniers bits correspondent aux 24 derniers bits de l'adresse IPv6 et donc, en règle générale, aux 24 derniers bits de l'adresse MAC recherchée.
Source (MAC capture 5) : 02:00:4c:4f:4f:50 : un poste écoute sur tous ses groupes multicast. Le poste ayant reconnu une de ses adresses IPv6 répond et envoie son adresse MAC dont les 24 derniers bits sont identiques à l'adresse multicast sollicitée.

4. Expliquer le rôle de l'adresse "Link Layer".

L'adresse Link layer correspond à l'adresse MAC de l'émetteur. Le poste répond à une requête "neighbor solicitation". Il fournit son adresse MAC.

Capture 6

1. Donner le libellé correspondant au type ICMPv6.

Type: 128 (Echo request)

2. De quel type est l'adresse MAC destination ?

C'est une adresse unicast. L'écho se fait après avoir obtenu l'adresse MAC du destinataire. Soit cette adresse a été obtenue par un "neighbor solicitation" soit cette adresse était en cache.

3. Relever le numéro de séquence.

Sequence: 0x01db

Capture 7

1. Donner le libellé correspondant au type ICMPv6.

Type: 129 (Echo reply)

2. De quel type est l'adresse MAC destination ?

C'est une adresse unicast. Le reply se fait après avoir obtenu l'adresse MAC du destinataire. Soit cette adresse a été obtenue dans le cadre d'un "neighbor solicitation" soit cette adresse était en cache.

3. Relever le numéro de séquence et le comparer au numéro de séquence de la capture 6. Expliquer le rôle du numéro de séquence.

Sequence: 0x01db. C'est le même numéro que dans le paquet ICMP précédent. Ce numéro permet d'associer l'écho avec son reply.

Remarque : Ces 4 dernières captures correspondent à un ping. L'équivalent IPv4 est une demande ARP suivi de l'échange ICMP, en IPv6 le protocole ICMPv6 remplace le protocole ARP.