

Chapitre 3 Internet Control Message Protocol (ICMP)

Introduction

ICMP complète IPv4 en termes de contrôle et de messages d'erreurs

Présentation

Internet Control Message Protocol (ICMP) est d'une importance cruciale pour la communication au sein des réseaux IP,

L'ICMP pour IPv6 (Internet Control Message Protocol Version 6) fait partie à part entière de l'architecture IPv6 et doit être complètement supportée par toutes les implémentations d'IPv6.

ICMPv6 combine des fonctions antérieurement subdivisées à travers différents protocoles, tels qu'ICMP v4 (Internet Control Message Protocol version 4), IGMP (Internet Group Membership Protocol), et ARP (Address Resolution Protocol), et il introduit quelques simplifications en éliminant des types de messages obsolètes qui ne sont plus utilisés.

Fonctions générales du protocole ICMPv6 est utilisé pour :

- Rapporter des erreurs trouvées dans le traitement de paquets,
- Effectuer des diagnostics réseau : Test (ping)
- Configuration automatique des équipements : Sollicitation de routeur et annonces de routeur,
- Découverte des voisins et des routeurs,
- Rapporter l'appartenance à un multicast : Gestion de groupe Multicast

ICMP n'est pas utilisé pour faciliter l'échange de données entre les systèmes.

ICMP prend en charge le routage IP, les diagnostics et les rapports d'erreurs. Il permet d'échanger des informations sur l'état ou des messages d'erreur des problèmes de connectivité potentiels entre les différents composants d'un réseau (postes, routeurs, imprimantes, switches...).

Le protocole ICMPv6 a le numéro 58.

Le protocole de contrôle d'IP a été revu. Dans IPv4, ICMP (Internet Message Control Protocol) sert à la détection d'erreurs (par exemple : équipement inaccessible, durée de vie expirée,...), au test (par exemple ping), à la configuration automatique des équipements (redirection ICMP, découverte des routeurs). Ces trois fonctions ont été mieux définies dans IPv6. De plus ICMPv6 (RFC 4443) intègre les fonctions de gestion des groupes de multicast (MLD : Multicast Listener Discovery) qui sont effectuées par le protocole IGMP (Internet

Group Message Protocol) dans IPv4. ICMPv6 reprend aussi les fonctions du protocole ARP utilisé par IPv4

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.

ICMPv6 a supprimé les fonctions ICMPv4 qui sont obsolètes et a repris les fonctions des deux principaux protocoles IPv4 IGMP (Internet Group Membership Protocol) et ARP (Address Resolution Protocol) . IGMP et ARP ne sont plus avec IPv6.

⇒ ICMPv6 remplace le protocole ARP et IGMP d'IPv4 et l'affectation automatique des routeurs par DHCP dans Ipv4.

Historique

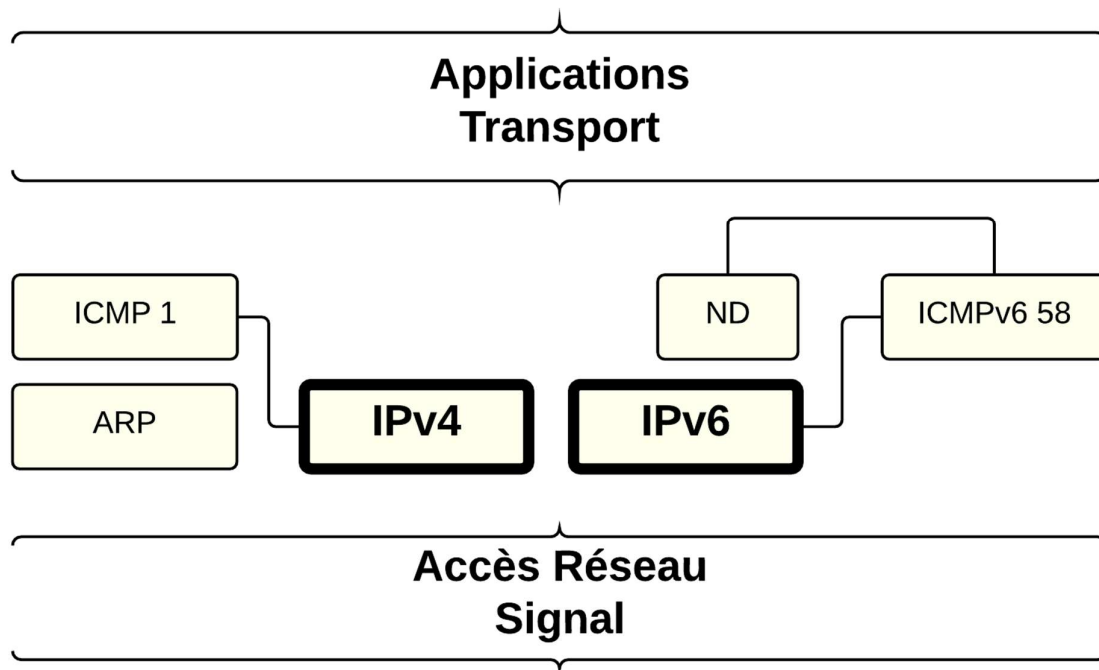
La définition originale de l'ICMP a été esquissée par Jon Postel , qui a contribué massivement et à plusieurs reprises au développement d'Internet, et

Le premier standard d'ICMP a été publié en avril 1981 dans la RFC 777 .

La forme stable de ce protocole a été publiée 5 mois plus tard que sa définition initiale, en septembre 1981, dans la RFC 792, et a également été écrite par Postel.

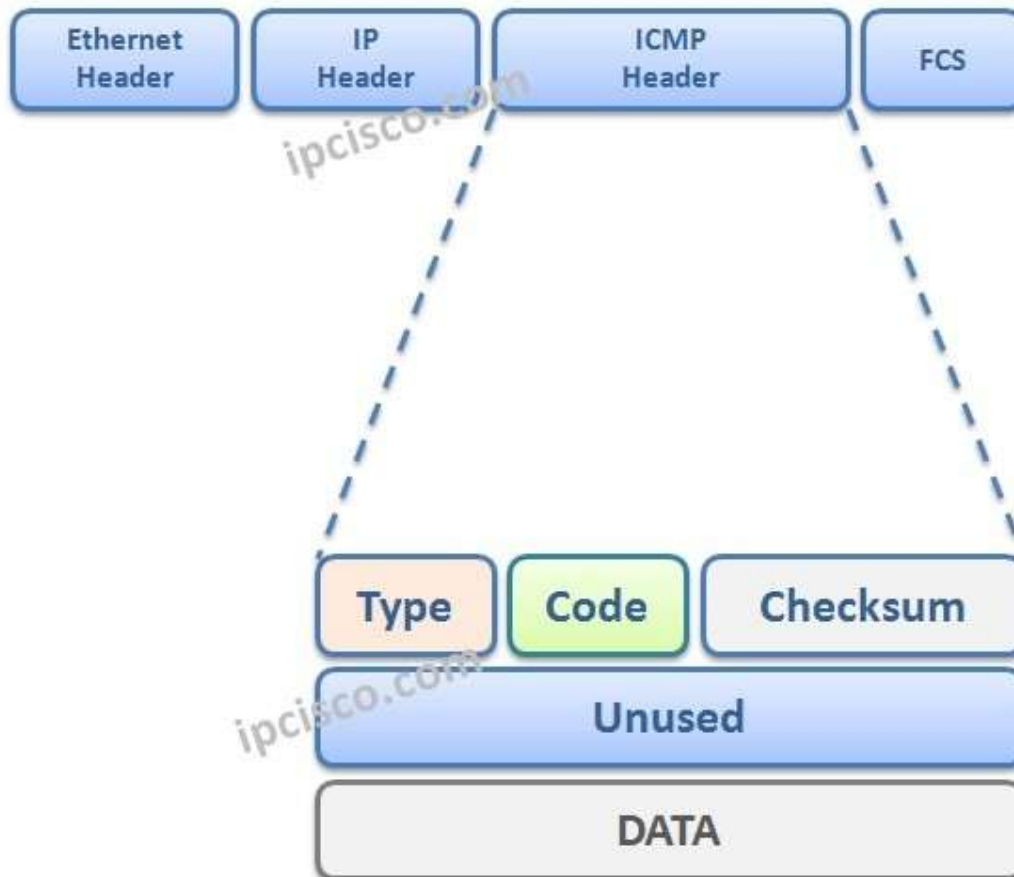
Format de message ICMP et d'en-tête ICMP

C'est un protocole de couche 3.



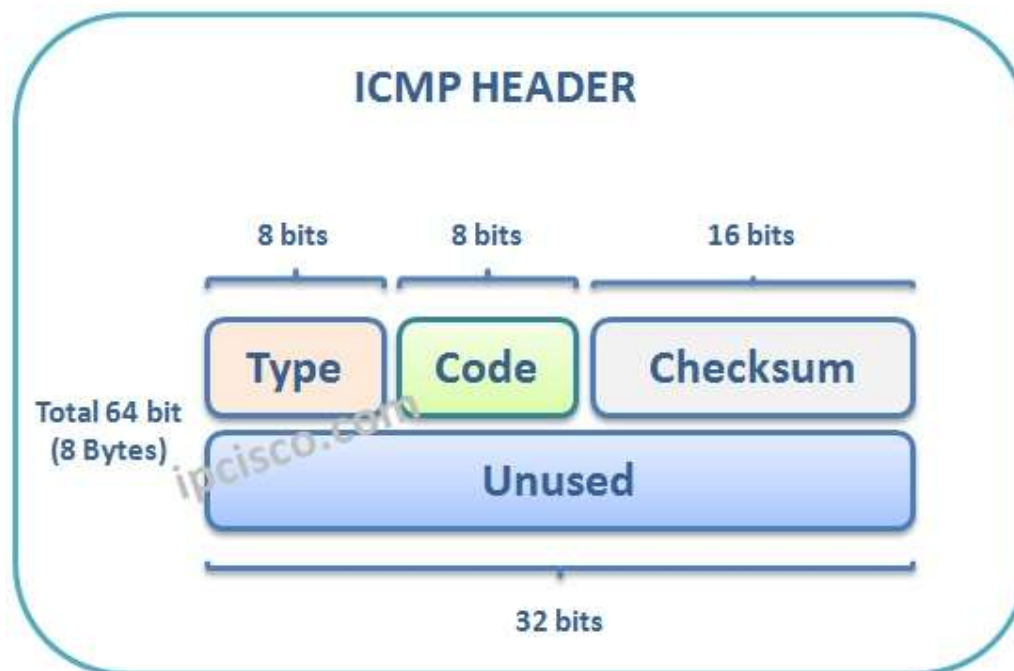
Le message ICMP est encapsulé dans un paquet IP .

Le format générique des paquets ICMPv6 est donné figure Format générique d'un message ICMP :



Dans le message ICMP , il y a d'abord un en- tête ICMP au début . Ce message de protocole de message de contrôle Internet **comprend les zones ci-dessous** :

- **Type** : code la nature du message ICMPv6. Contrairement à IPv4 où la numérotation ne suivait aucune logique, les valeurs inférieures à 127 sont réservées aux messages d'erreur. Les autres valeurs réservées aux messages d'information, parmi lesquels se trouvent ceux utilisés par le protocole découverte des voisins (neighbor discovery) pour la configuration automatique des équipements.
- **Code** : précise la cause du message ICMPv6
- **Somme de contrôle** : permet de vérifier l'intégrité du paquet ICMP. Ce champ est calculé avec le pseudo-en-tête décrit au chapitre Checksum au niveau transport.
- Inutilisé



La taille totale d'un paquet ICMP ne doit pas excéder la taille minimale du MTU (Maximum Transmission Unit) qui est de 1280 octets en IPv6. Cela assure une bonne transmission du message, sans aucune fragmentation, dans toutes les circonstances, ce qui est primordial pour des messages de contrôle.

Champs de type et de code ICMP


Comme ICMPv4, **ICMPv6** a également les valeurs Code. Vous pouvez également vérifier les valeurs de code de ces différents types ci-dessous :

Messages d'erreur

Les messages d'erreur ICMPv6 sont similaires à ceux d'ICMPv4. Ils appartiennent à l'une des quatre catégories : Destination non atteignable, Paquet trop gros, Time out, et Problèmes de paramétrage.

0 Destination Unreachable

2 Packet Too Big

 0 Time Exceeded

4 Parameter Problem

ERROR MESSAGES	Type	Code	Description
	Destination Unreachable (Type 1)	0	Destination Unreachable
		1	Source Quence
		2	Redirection
		3	Time Exceeded
		4	Parameter Problem
	Packet Too Big	0	Time Exceeded
	Time Exceed	0	Hop limit exceeded
		1	Fragment reassembly time exceeded
	Parameter Problem	0	Erroneous header field encountered
		1	Unrecognized next header type encountered
		2	Unrecognized IPv6 option encountered

Messages informatifs

L'autre type de messages ICMP est divisé en trois groupes : messages de diagnostic, messages pour la gestion des groupes multicast, et messages de découverte de voisinage. (diagnostic messages, messages for the management of multicast groups, et Neighbor Discovery messages.)

128 Echo Request

129 Echo Reply

INFORMATIONAL MESSAGES	Type	Code	Description
	Echo Request (Type 128)	0	Used to check connectivity, by IPv6 Ping
	Echo Reply (Type 129)	0	IPv6 Ping Reply

Message Source Address Determination

Un nœud qui envoie un message ICMPv6 doit déterminer à la fois les adresses IPv6 de Source et de Destination de l'en-tête IPv6 avant de calculer la somme de contrôle. Si le nœud a plus d'une adresse unicast, il doit choisir l'adresse source du message de la manière suivante :

- (a) Si le message est une réponse à un message envoyé à l'une des adresses unicast du nœud, l'adresse Source de la réponse doit être la même.
- (b) Si le message est une réponse à un message envoyé en multicast ou anycast, d'un groupe dont le nœud est membre, l'adresse de la réponse doit appartenir au groupe.
- (c) Si le message est une réponse à un message envoyé à une adresse n'appartenant pas au nœud, l'adresse source devrait être l'adresse unicast du nœud qui sera la plus utile au diagnostic de l'erreur.
- (d) Dans les autres cas, en fonction de la table de routage.

Types de messages ICMP

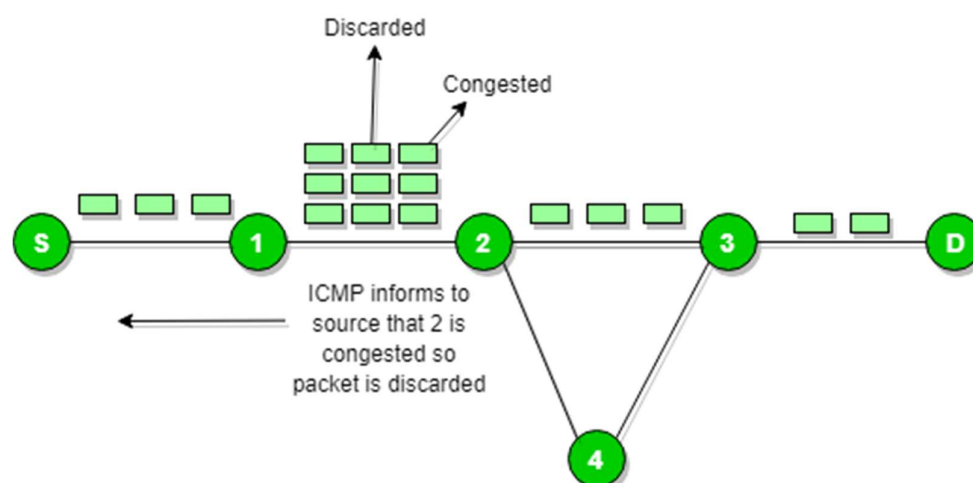
Type	Signification
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem
128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group Membership Reduction
133	Router Solicitation

- 134 Router Advertisement
- 135 Neighbor Solicitation
- 136 Neighbor Advertisement
- 137 Redirect

	Type	Code	Description
NEIGHBOUR DISCOVERY	Router Solicitation (Type 133)	0	Used to check connectivity, by IPv6 Ping
	Router Advertisement (Type 134)	0	Reply to IPv6 Ping
	Neighbour Solicitation (Type 135)	0	Request link-local address of destinationv
	Neighbour Advertisement (Type 136)	0	Reply to Neighbour Solicitation (Type 134)
	Redirect (Type 137)	0	Redirect path to a better next-hop

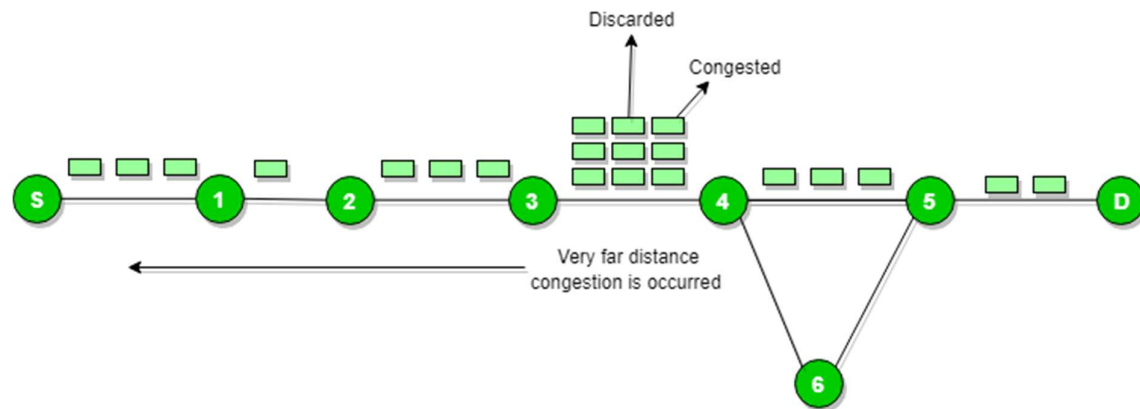
Message d'extinction source :

Le message d'extinction source est une demande de diminution du taux de trafic des messages envoyés à l'hôte (destination). Ou nous pouvons dire que lorsque l'hôte de réception détecte que le taux d'envoi de paquets (taux de trafic) est trop rapide, il envoie le message d'extinction source à la source pour ralentir le rythme afin qu'aucun paquet ne puisse être perdu.



ICMP prendra l'adresse IP source du paquet rejeté et informe la source en envoyant un message d'extinction de la source.

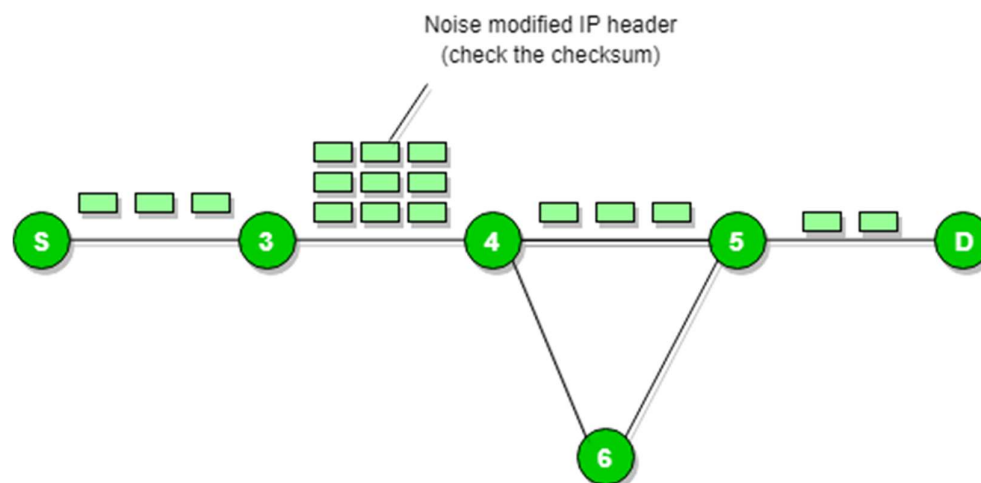
Ensuite, la source réduira la vitesse de transmission afin que le routeur soit exempt de congestion.



Lorsque le routeur de congestion est éloigné de la source, l'ICMP enverra un message d'extinction de la source saut par saut afin que chaque routeur réduise la vitesse de transmission.

Problème de paramètre :

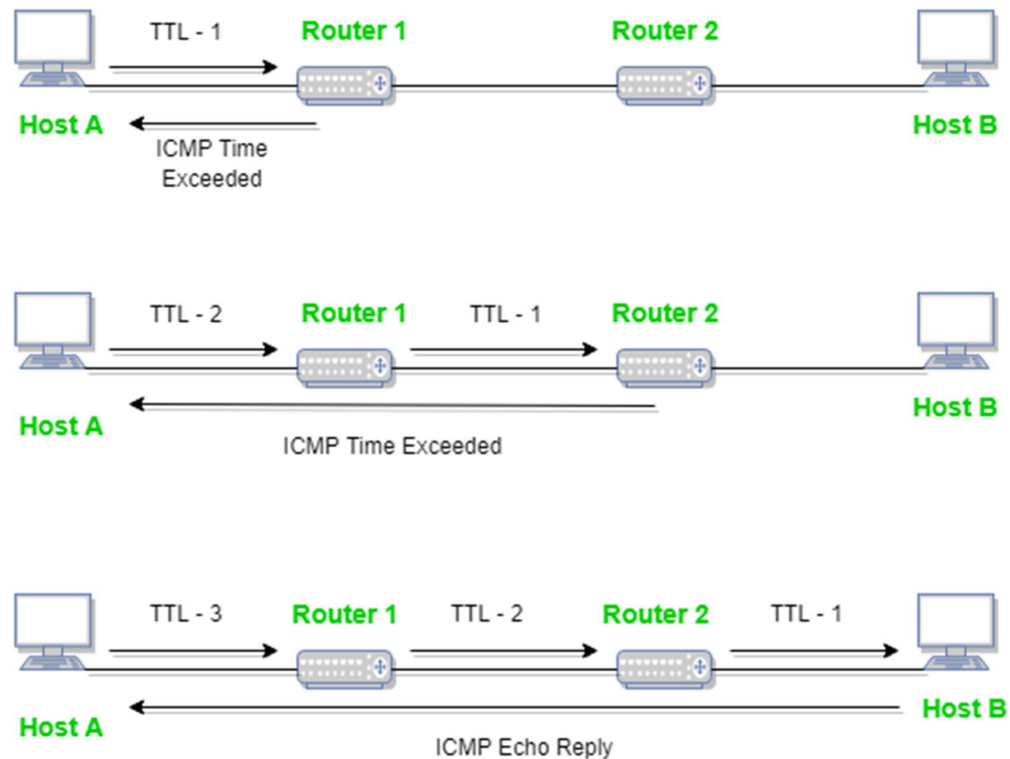
Chaque fois que des paquets arrivent au routeur, la somme de contrôle d'en-tête calculée doit être égale à la somme de contrôle d'en-tête reçue, alors le seul paquet est accepté par le routeur.



S'il y a une discordance, le paquet sera abandonné par le routeur.

ICMP prendra l'adresse IP source du paquet rejeté et informe la source en envoyant un message de problème de paramètre.

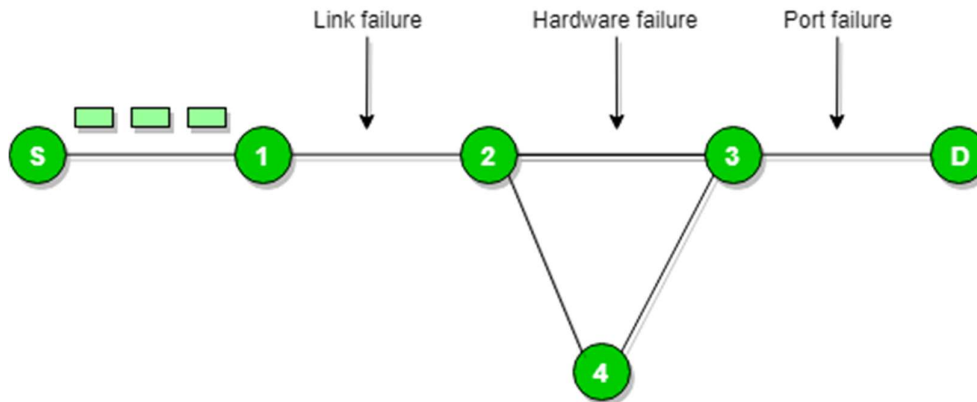
Message de dépassement de temps :



Lorsque certains fragments sont perdus dans un réseau, le fragment détenu par le routeur est supprimé, puis ICMP prend l'adresse IP source du paquet supprimé et informe la source du datagramme supprimé en raison du temps de mise en service atteint zéro, en envoyant le temps dépassé un message.

Destination inaccessible :

La destination inaccessible est générée par l'hôte ou sa passerelle entrante pour informer le client que la destination est inaccessible pour une raison quelconque.



Il n'y a aucune condition nécessaire que le seul routeur donne le message d'erreur ICMP un certain temps, l'hôte de destination envoie un message d'erreur ICMP lorsqu'un type de défaillance (défaillance de liaison, défaillance matérielle, défaillance de port, etc.) se produit dans le réseau.

Message de redirection :

Les paquets de données des requests de redirection sont envoyés sur une autre route. Le message informe un hôte de mettre à jour ses informations de routage (pour envoyer des paquets sur une route alternative).

Ex. Si l'hôte essaie d'envoyer des données via un routeur R1 et R1 envoie des données sur un routeur R2 et il existe un chemin direct de l'hôte vers R2. Ensuite, R1 enverra un message de redirection pour informer l'hôte qu'il existe le meilleur moyen d'atteindre la destination directement via R2 disponible. L'hôte envoie ensuite des paquets de données pour la destination directement à R2.

Le routeur R2 enverra le datagramme d'origine à la destination prévue.

Mais si le datagramme contient des informations de routage, ce message ne sera pas envoyé même si un meilleur itinéraire est disponible car les redirections ne doivent être envoyées que par des passerelles et ne doivent pas être envoyées par des hôtes Internet.

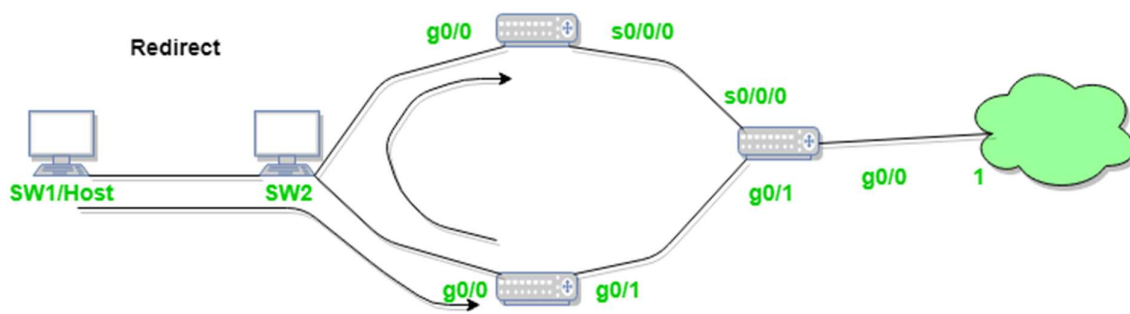


Figure - ICMP redirect Verification CCNP 2.0 100 - 101 (v - 71)

- ✓ ICMP Redirect
- ✓ ICMP Redirect for host
- ✓ ICMP Redirect for network
- ✓ How ICMP redirect work
- ✓ ICMP Redirect verification step by step

Chaque fois qu'un paquet est transmis dans une mauvaise direction plus tard, il est redirigé dans une direction actuelle, alors ICMP enverra un message redirigé.

Protocole de découverte de voisin IPv6

il n'y a pas de protocole de résolution d'adresse (ARP) dans IPv6 et c'est le protocole **IPv6 Neighbor Discovery** qui permet de gérer le processus de résolution de la couche 3 à la couche 2 en **utilisant des messages multidiffusion au lieu d'être diffusés** comme dans IPv4.

Le terme **voisin** ou **nœud voisin** fait référence aux nœuds IPv6 qui se trouvent sur le même segment local ou dans le même domaine de couche 2.

Types de messages

Le protocole IPv6 Neighbor Discovery Protocol définit 5 types de messages qui utilisent l'encapsulation ICMPv6 :

- Sollicitation de routeur (ICMPv6 type 133)
- Annonce de routeur (ICMPv6 type 134)
- Sollicitation de voisins (ICMPv6 type 135)
- Annonce de voisin (ICMPv6 type 136)
- Message de redirection (ICMPv6 type 137)

En comparaison, les messages ARP tels que la requête ARP et la réponse ARP sont encapsulés directement dans une trame Ethernet.

Sollicitation de voisins (NS)

Lorsqu'un nœud doit résoudre l'adresse physique d'une adresse IPv6 connue, il envoie un message de sollicitation de voisin (NS) sur le segment de réseau. Ce message est l'alternative IPv6 à la requête ARP. Il y a peu de changements par rapport à ARP, mais cela rend la sollicitation de voisin **plus sûre et plus efficace**.

Regardons l'exemple illustré à la figure 1 où PC1 veut résoudre l'adresse physique de PC3 - FE80::20C:CFF:FECC:CCCC. PC1 doit envoyer un message de sollicitation de voisin pour cette adresse IPv6 afin de créer un nouveau paquet ICMPv6 de type 135. Le type 135 indique explicitement au côté récepteur qu'il s'agit d'un paquet NS. Dans le champ cible de l'ICMPv6, PC1 met l'adresse IPv6 dont il veut trouver le MAC. Dans notre exemple, il s'agirait de PC3 - FE80::20C:CFF:FECC:CCCC.

Ce message ICMPv6 est ensuite encapsulé dans un paquet IPv6. Pour l'adresse source au niveau de la couche 3, PC1 définit sa propre adresse lien-local FE80:20A:AFF:FEAA:AAAA. L'adresse de destination est la clé de l'amélioration de la sécurité et de l'efficacité par rapport au protocole ARP dans IPv4. Pour l'adresse de destination dans le paquet IPv6, PC1 définit un type spécial d'adresse de multidiffusion appelée multidiffusion **de nœud sollicité**. Pour chaque adresse IPv6 configurée, chaque nœud rejoint un groupe de multidiffusion identifié par l'adresse FF02::1:FF XX:XXXX où XX:XXXX sont les 6 dernières valeurs hexadécimales de l'adresse unicast IPv6. Par conséquent, pour chaque adresse de monodiffusion configurée, qu'elle soit lien-local ou global, l'hôte rejoint le groupe de multidiffusion **de nœud sollicité** généré automatiquement respectif.

Dans notre exemple, PC1 veut envoyer le message NS au nœud avec l'adresse IP FE80::20C:CFF:FE CC:CCCC. En gardant à l'esprit la logique ci-dessus, le nœud qui a cette adresse IPv6 doit avoir joint le groupe de nœuds sollicités généré à partir de cette adresse - FF02::1:FF CC:CCCC.

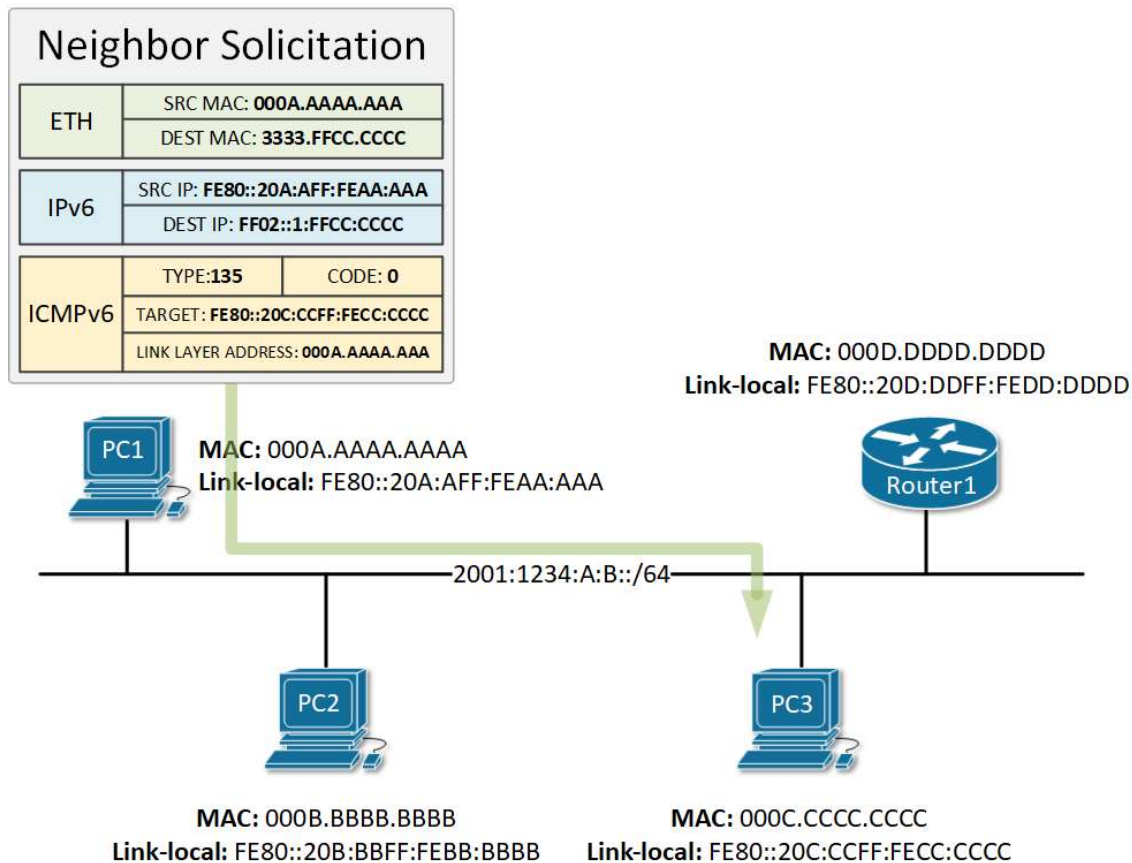


Figure 1. Message de sollicitation de voisin IPv6

Une fois l'en-tête IPv6 rempli, le paquet est encapsulé dans une trame Ethernet. Pour l'adresse MAC source, PC1 définit sa propre adresse physique gravée. L'adresse MAC de destination est définie sur un MAC de multidiffusion généré à partir de l'adresse IPv6 de multidiffusion dans l'en-tête de couche 3 à l'aide de la formule suivante. 3333. XXXX.XXXX où XXXX:XXXX sont les 8 derniers chiffres hexadécimaux de l'adresse IPv6 de multidiffusion. Dans notre exemple, cela se traduira par l'adresse physique 3333.FFCC.CCCC car ce sont les 8 derniers chiffres hexadécimaux de l'adresse de destination FF02::1 : FFCC:CCC.

Lorsque PC1 envoie ce message Sollicitation de voisin sur le réseau, il y a deux scénarios possibles :

- Si les commutateurs du segment local exécutent un protocole appelé IPv6 Multicast Listener Discovery Snooping (MLD), ils sauront que seul PC3 est abonné au groupe de multidiffusion FF02::1:FFCC:CCC et commuteront la trame uniquement sur PC3.
- Si les commutateurs du segment local n'exécutent pas MLD, ils diffuseront la trame à chaque nœud du segment de la même manière qu'une trame ARP dans IPv4. Cependant, seul PC3 traitera le paquet, car seul PC3 est abonné à ce groupe de multidiffusion. Tous les autres nœuds qui reçoivent ce paquet NS le rejeteront, car ils n'écoutent pas cette adresse de nœud sollicité FF02::1:FFCC:CCC.

Publicité de voisin (NA)

Lorsque PC3 reçoit le message Sollicitation de voisin de PC1, il examine le champ Cible dans l'en-tête ICMPv6 et le compare à ses propres adresses IPv6 configurées. L'adresse cible correspond à l'adresse lien-local de PC3, de sorte que **PC3 répondra à PC1 avec un message appelé Neighbor Advertisement**. Ce message est l'alternative IPv6 à la réponse ARP en IPv4.

Examinons en détail toutes les valeurs du message. Dans l'en-tête ICMPv6, PC3 définit le champ Type sur 136, ce qui signifie qu'il s'agit d'un message NA. Dans le champ *Target*, PC3 définit l'adresse IPv6 et dans le champ *Link-local Address*, il définit l'adresse physique de l'interface configurée avec cette IPv6.

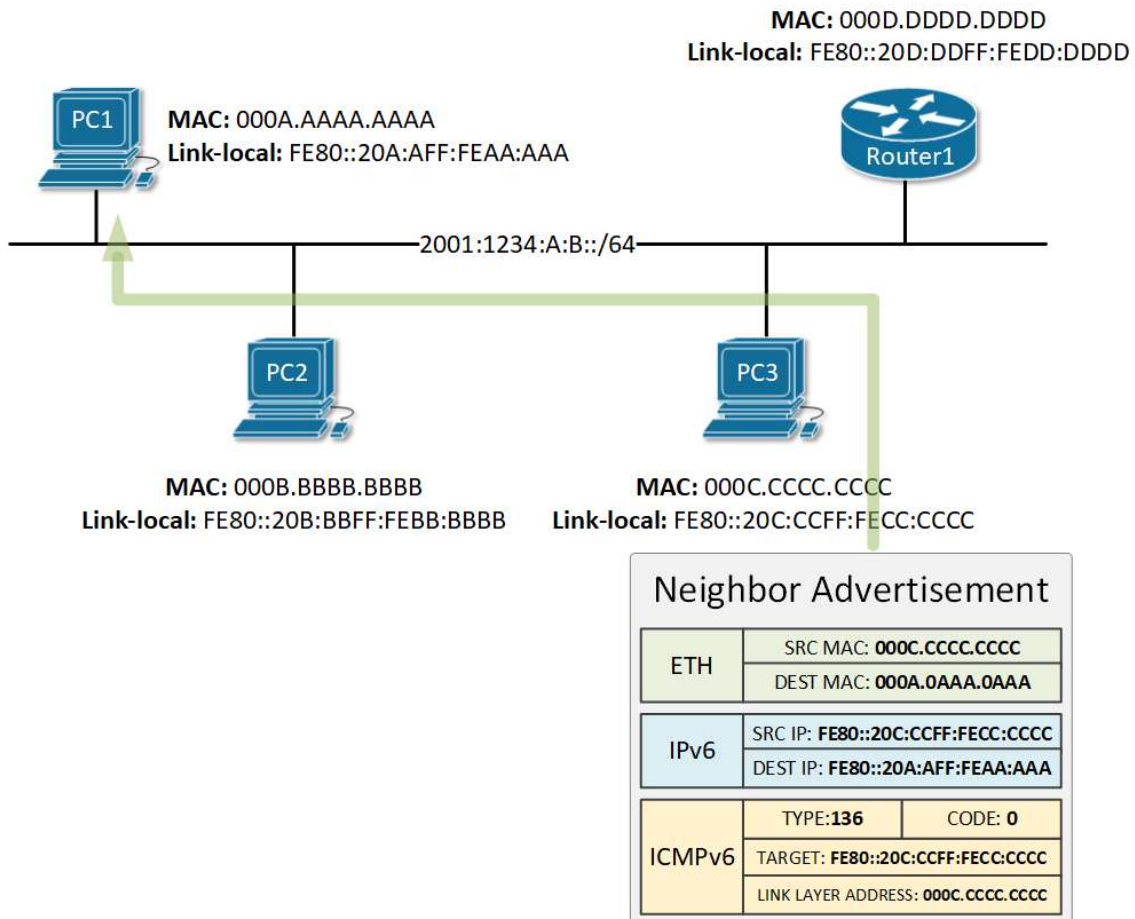


Figure 2. Message d'annonce de voisin IPv6

Dans l'en-tête IPv6, PC3 définit l'adresse IPv6 source comme étant son adresse lien-local et la destination comme étant l'adresse lien-local de PC1.

Dans l'en-tête Ethernet, PC3 définit sa propre adresse physique comme source MAC et l'adresse physique de PC1 comme destination MAC. Notez que **l'annonce de voisin est un message unicast**.

Annnonce de routeur (RA)

Les routeurs IPv6 attachés à un segment local annoncent périodiquement leur présence via un message ICMPv6 appelé **Router Advertisement (RA)**. Le message est destiné à l'adresse de multidiffusion de **tous les nœuds** FF02 :: 1, ce qui signifie que chaque nœud du segment le reçoit et le traite. Les messages RA contiennent le **préfixe** et la **longueur** du préfixe utilisés sur ce segment ainsi que d'autres paramètres tels que le MTU. Les routeurs Cisco annoncent leur présence sur un segment toutes les **200 secondes** par défaut.

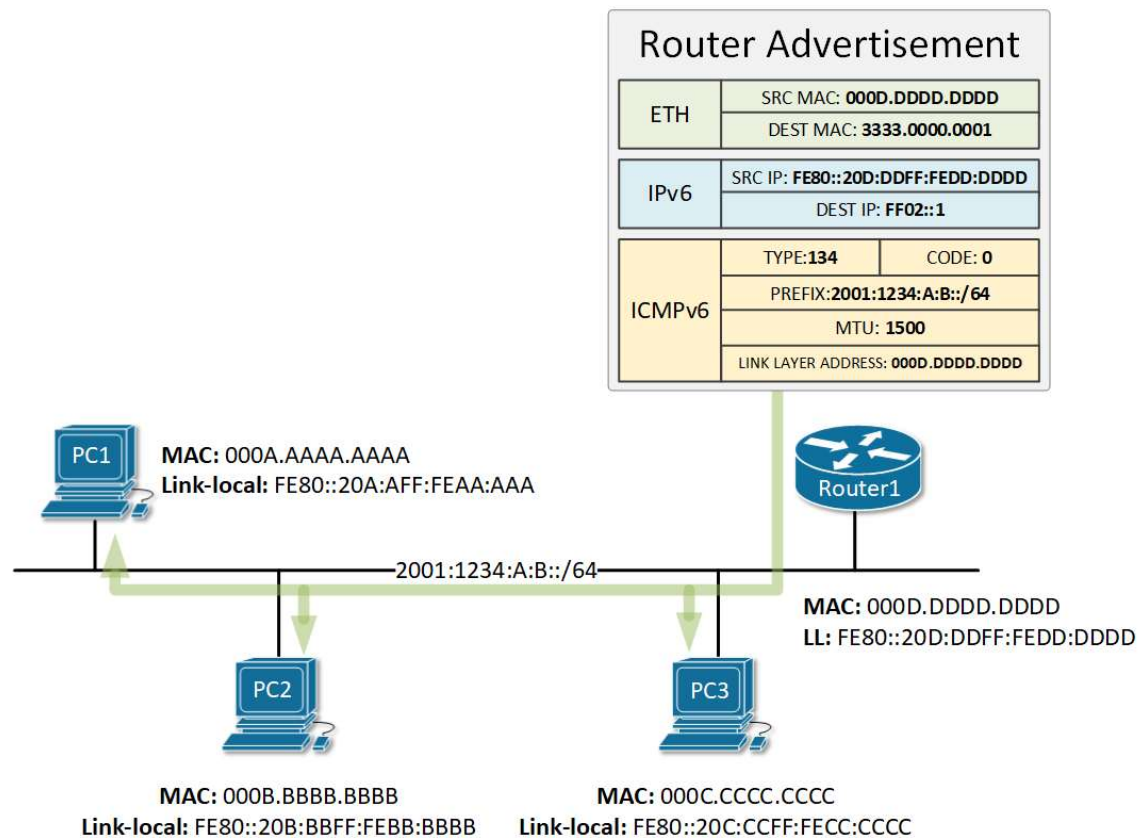


Figure 3. Message d'annonce du routeur IPv6

Sollicitation de routeur (RS)

Les routeurs Cisco envoient par défaut des messages d'annonce de routeur toutes les 200 secondes. Cependant, lorsqu'un nœud est connecté à un segment local, il envoie un message appelé Neighbor Solicitation qui demande que les routeurs génèrent des annonces de routeur (RA) immédiatement plutôt qu'à leur prochaine heure planifiée.

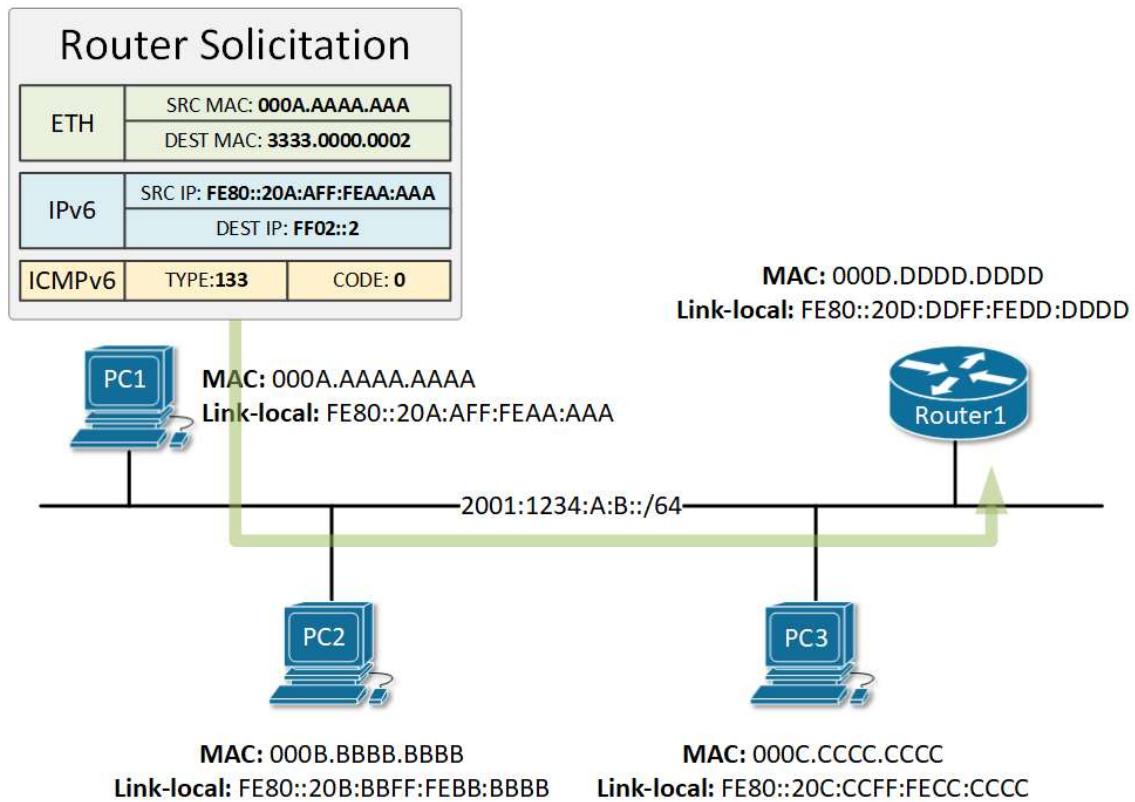


Figure 4. Message de sollicitation du routeur IPv6

Comme vous pouvez le voir dans l'exemple de la figure 4, le message de sollicitation de routeur est destiné à l'adresse de multidiffusion de **tous les routeurs**, ce qui signifie que seuls les routeurs du segment local traiteront ces messages RS.