La Supervision – 21/10/22 - Compte-rendu

Valentin MALO

Consignes :

Protocole ICMP

1. Recherche sur tous ce que l'on peut faire à base de « ping » ou du protocole « icmp »
2. Recherche d'outils, de package autour de ce protocole
    a. 1.Exemples : fping

Quand on fait un ping sur un équipement, regarder les informations que l'on peut sortir juste avec un simple ping

Lien : *http://igm.univ-mlv.fr/~dr/XPOSE2010/IPSLA/presentation.html*

Qu'est-ce que le Ping ?

Le ping est une commande utilisée sur plusieurs systèmes d'exploitation différente. Son but est d'essayer d'atteindre un hôte cible en passant par le réseau et grâce à son adresse IP cible.

Comment fonctionne le Ping ?

Avec la commande ping suivi de l'adresse IP de destination et l'argument que l'on utilise, on peut voir différentes informations.

La commande ping a elle seule permet de réaliser un test du lien établi entre 2 services ou 2 postes sur un même serveur ou pour faire du dépannage réseaux. Dans le cas suivi, je réalise un ping un des serveurs DNS de google, sur son adresse IPv4 : 8.8.8.8.

On peut voir dans la capture ci-dessous, que mon poste a envoyé 3 paquets et que les 3 paquets ont bien été réceptionnés par le serveur (l'hôte cible) car il n'y a eu aucune perte. C'est un échange de paquet entre le serveur local et le serveur distant (je lui envoie un paquet, il la réception avant de le renvoyer puis je le réceptionne à nouveau).

Comme indiqué, il est marqué « Réponse de 8.8.8.8 » qui montre bien que c'est un retour après l'envoie de notre paquet.

La commande permet aussi d'afficher le temps de latence entre l'envoie et la réception finale des paquets (25 ms).

Le partie octets, indique la taille de notre paquet, par défaut 32 sous Windows (et plus gros, 64 octets sous Linux).

On peut voir aussi la durée de vie d'un paquet (TTL = Time to Live). Chaque fois qu'un paquet passe par un service, ce paquet se trouve dégrader et perd en durée de vie. S'il atteint 0, le paquet sera

alors ignoré. C'est une valeur propre à un paquet ICMP, ce qui a pour but d'empêcher le paquet de se propager à l'infini.

```
C:\Users\ValentinMALO>ping 8.8.8.8

Envoi d'une requête 'Ping'  8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=25 ms TTL=246
Réponse de 8.8.8.8 : octets=32 temps=26 ms TTL=246
Réponse de 8.8.8.8 : octets=32 temps=25 ms TTL=246

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 25ms, Maximum = 26ms, Moyenne = 25ms
```

Dans le cas où le temps de réponse est long ou élevé, il se peut qu'il y soit un problème sur la ligne (problème de routage, débit du transfert de données ou encore équipement déconnecter ou défectueux).

Format des messages Ping

Byte 0	Byte 1	Byte 2	Byte 3
Type (8 = IPv4, ICMP; 128 = IPv6, ICMP6)	Code	En-tête de vérification	
Identificateur		Numéro de séquence	
Payload			

Exemples de syntaxes de Ping

-I (i)	Spécifie la valeur du champ Durée de vie (TTL) dans l'en-tête IP pour les messages de demande d'écho envoyés. La valeur par défaut est la valeur TTL par défaut de l'hôte. La *durée de vie* maximale est de 255.
-n	Nombre de demandes d'écho à envoyer
-a	Résout les adresses en noms d'hôtes
-4	Force l'utilisation d'IPv4
-w	Délai d'attente pour chaque réponse, en ms

Qu'est-ce que ICMP et à quoi il sert ?

ICMP = Internet Control Message Protocol, est un protocole utilisé pour le diagnostique des problèmes de communication du réseau, par les équipements réseaux.

Utilisé principalement pour déterminer si les données (paquets) atteignent l'hôte distant en temps voulu. Et il est indispensable pour le signalement d'erreurs et les tests.

ICMP est important pour la communication au sein des réseaux IP, ce protocole est aussi utilisé par les routeurs.

L'objectif principale est de signaler les erreurs sur le réseau. Lorsque 2 périphériques se connectent sur Internet, l'ICMP génère des erreurs à partager avec le périphérique émetteur dans le cas où certaines données n'ont pas atteint la destination prévue.

Dans le cas où un paquet est trop volumineux pour un routeur, ce dernier abandonne le paquet et renvoie un message ICMP à la source originaire des données.

Exemples d'utilitaire/outils qui utilise le protocole ICMP

PingInfoView : PingInfoView - Ping to multiple host names/IP addresses (nirsoft.net)

Utilitaire qui permet d'envoyer facilement un ping à plusieurs hôtes cibles et adresses IP. Les résultats apparaissent sous forme de tableau.

L'outil envoie automatique des commandes Ping à tous les hôtes chaque seconde et affiche le nombre de pings réussis et échoués, ainsi que le temps de ping moyen (latence en ms).

PingICMP : Outil Ping ICMP - FRAMEIP.COM

Apporte autant d'information que l'outil PingInfoView sur les différents pings effectués.

Comme la latence ou le temps de réponse inférieur en ms.

Le changement des adresse IP source.

Il permet aussi l'envoie massif afin de permettre d'atteindre des débits hauts tel que ~65 Mbps sur une carte de 100 Mbps.