ICMP

Rappel et approfondissement

1

Ce document rappelle et approfondie les éléments sur le protocole ICMP et ses déclinaisons dans les outils de base.

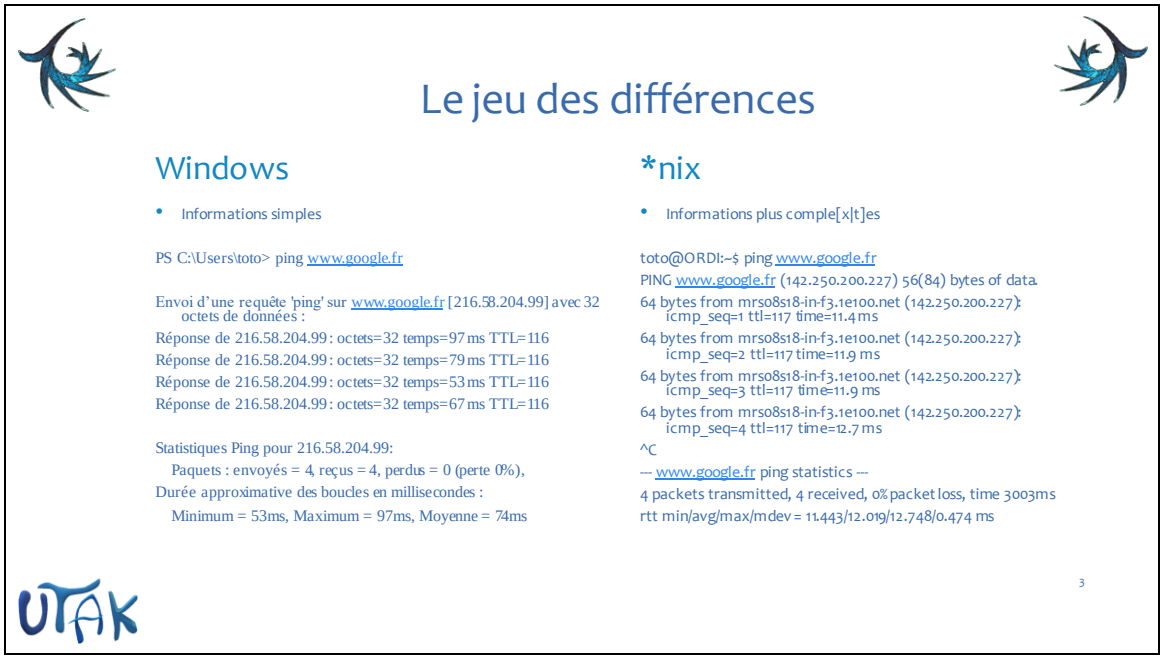
ICMP

- Protocole spécifique allant jusqu'à la couche 3 du modèle ISO
- Le protocole :
  1. Porte plusieurs types d'actions
     - Demande/réponse @IP, demande/réponse heure, demande/réponse de masque sous-réseau, demande/réponse d'écho, ...
  2. Véhicule de la donnée "aléatoire"
- Commande "ping" :
  - Demande d'écho et réponse d'écho

UTAK

2

Malgré le titre de l'article, celui-ci est complet et source d'informations : Le ping pour les débutants | IT-Connect



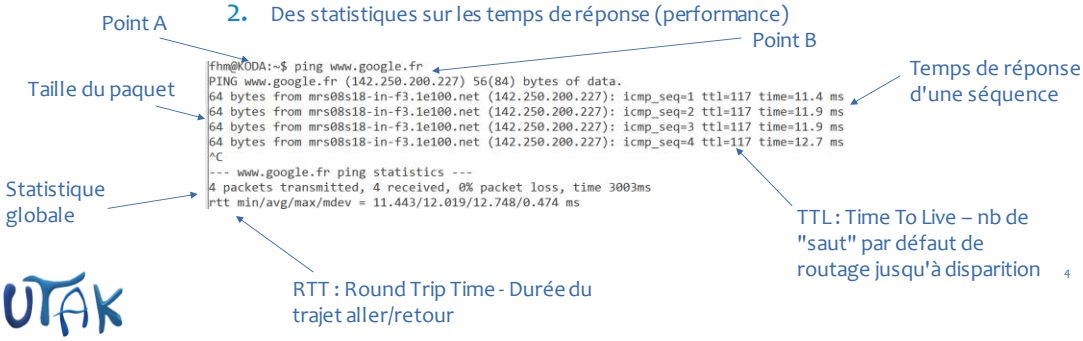
La déclinaison du protocole se retrouve basiquement dans la commande "ping". Son implémentation sur les différents systèmes d'exploitation diffère comme nous le voyons dans cette planche.

Le jeu des différences :

- 4 envois par défaut sur Windows vs l'envoi permanent jusqu'à interruption par l'utilisateur avec la séquence de caractère Ctrl C
- La taille des paquets : 32 octets sur Windows vs 58(84) octets côté *nix
- Présentation du numéro de séquence dans le cadre des systèmes d'exploitation *nix
- Présentation du temps global de la commande (time 3003 ms) dans le cadre des systèmes d'exploitation *nix
- Présentation de l'écart-type (mdev 0.474 ms) dans le cadre des systèmes d'exploitation *nix
- Le TTL, le temps de vie sur le réseau de la trame ICMP, diffère également très légèrement. 116 côté Windows, 117 côté *nix

ICMP

- Le protocole permet fonctionnellement :
  1. Le contrôle de la disponibilité de la carte réseau d'un équipement
  2. D'obtenir des symptômes sur la qualité du réseau d'un point A à un point B par :
     1. Des statistiques sur le nombre de trame perdu (fiabilité)
     2. Des statistiques sur les temps de réponse (performance)



Il faut savoir situer ce protocole dans le modèle OSI (***O**pen **S**ystems **I**nterconnection* - cf. Modèle OSI — Wikipédia (wikipedia.org))
Ce protocole reste dans les couches basses du modèle, couches labelisées "matérielles" dans le modèle (niveau 3).
La limite de ce contrôle sera donc le fait que votre système d'exploitation pourrait être figé (hang) et pourtant, la carte réseau détenant l'adresse IP sera a même de répondre au "ping".


Statistique (1/4)

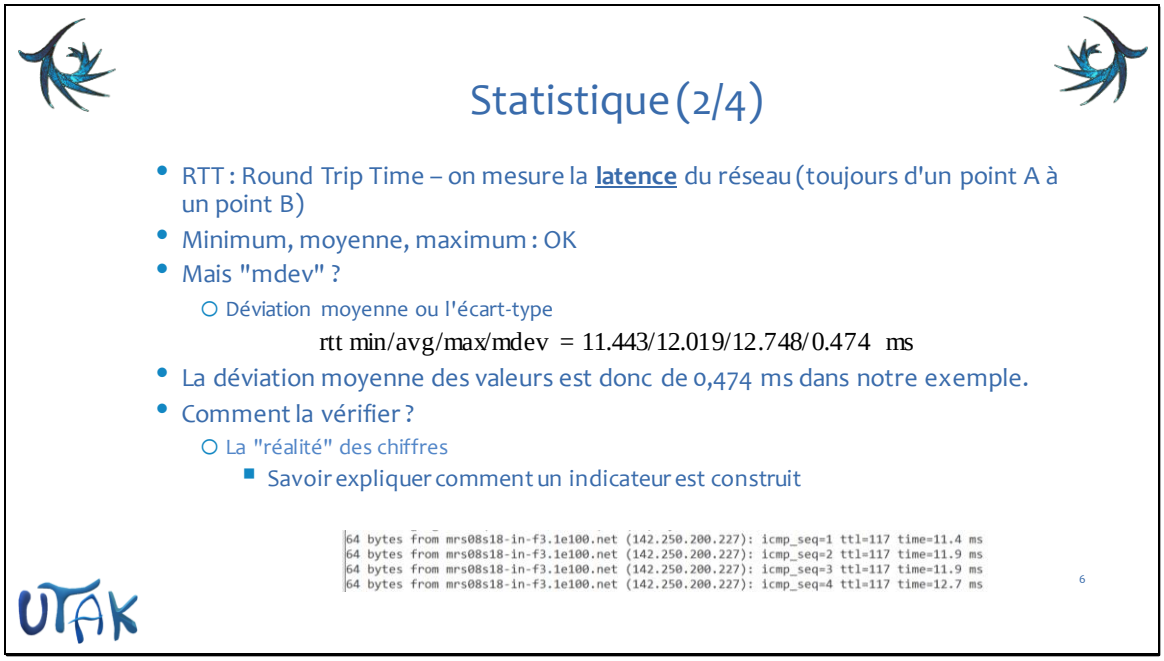
4 packets transmitted, 4 received, 0% packet loss, time 3003ms

- Statistique sur 4 paquets envoyés
  - 4 reçus sur 4 transmis : 0% de paquet perdu
- Euh, et "time" finalement ?
  - Le temps global d'exécution de la commande
  - Par défaut, un délai d'une seconde existe entre 2 transmissions
  - Ici 4 transmissions
    - T0 : 0s ; T1 : +1s ; T2 - +1s ; T3 + 1s
    - On est effectivement à un peu plus de 3 secondes en tout

UTAK

5

Le temps global est donc indiqué par le champ "time 3003ms"
Le premier contrôle se fait quasi immédiatement, juste le temps que le système d'exploitation prenne en compte la commande.
Le deuxième contrôle se fait au bout de 1 seconde : on est donc à très légèrement plus d'une seconde
On ajoute encore une seconde au troisième contrôle : on est à très légèrement plus de 2 secondes
Une nouvelle seconde en plus pour notre dernier contrôle : on est à légèrement plus de 3 secondes



On parle ici des temps de réponse aux requêtes ICMP. On parle donc de latence, voire de lag, et on attend parfois parler de gigue. Ce dernier terme est plutôt à proscrire, car la gigue est avant tout une notion électronique. Ce terme n'abonde pas les mêmes notions et peut être confusant.

Autant on comprend assez simplement les valeurs minimums, maximums et moyennes d'une série, autant le libellé "mdev" est moins parlant. Cela correspond à "Mean Deviation", à savoir une déviation moyenne. On parle également d'écart-type. Sur l'échantillon que nous avons, 4 valeurs présentes avec en moyenne pour ces 4 valeurs : 11,975.
Pour calculer cette déviation moyenne, on soustrait la moyenne à chaque valeur individuelle et on retient la valeur absolue don't on prend la moyenne.

Temps	: T0	| T1	| T2	| T3
Série de valeurs	: 11,4	| 11,9	| 11,9	| 12,7
Déviation individuelle	: 0,575	| 0,075	| 0,075	| 0,725

On en déduit la déviation moyenne : (0,575 + 0,075 + 0,075 + 0,725) / 4 = 0,3625 ms
Parfait, voyons notre "mdev" !
Gasp, cela n'a rien à voir : 0,474 ms

Pour bien repositionner le sujet, vous avez dans chaque statistique individuelle des contrôles une précision à 2 chiffres après la virgule (exemple : 11.4 ms pour le premier temps de réponse).
A contrario, la précision des statistiques globales sont, elles, à 3 chiffres après la virgule. C'est cela qui influe sur notre résultat !
Pour vérifier le fonctionnement et le calcul réalisé, 2 possibilités :
1. en ne faisant qu'un contrôle, on constate bien une déviation moyenne à 0
2. en faisant 2 contrôles, le min et le max sont forcément les valeurs appropriées pour faire le calcul et donc on peut récupérer les valeurs avec le même niveau de précision.

PING www.google.fr (142.250.74.227) 56(84) bytes of data.
64 bytes from par10s40-in-f3.1e100.net (142.250.74.227): icmp_seq=1 ttl=110 time=4.57 ms
64 bytes from par10s40-in-f3.1e100.net (142.250.74.227): icmp_seq=2 ttl=110 time=4.95 ms
^C
--- www.google.fr ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 4.573/4.763/4.953/0.190 ms

T1	T2
4,573	4,953
0,190	0,190

La déviation moyenne est bien de 0,190 ms !

Statistique (3/4)

- Quels cas d'usage ?
  - Construire une ligne de base (baseline)
  - Déterminer la "variation de la latence" (souvent appelée gigue ou Jitter en anglais)
  - Alerter lors d'une déviation
- On parle de dérive comportementale
- Quelle périodicité vous parait la plus appropriée pour contrôler cette variation ?

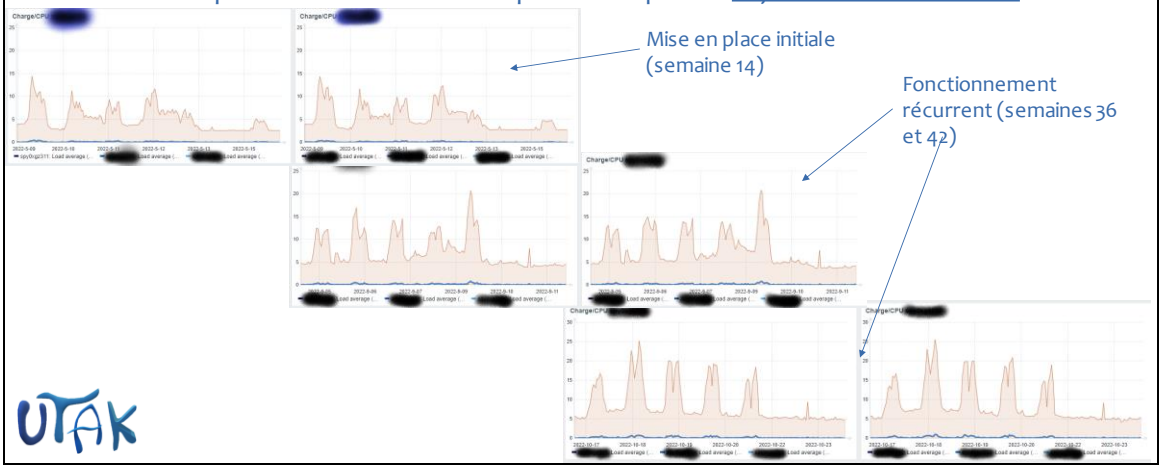
UTAK

7

La périodicité idéale est souvent le jour de la semaine. Voyons à la planche suivante le pourquoi de cette périodicité.

Statistique (4/4)

- La périodicité "standard" la plus classique est la journée de la semaine



Pourquoi ?

L'anitvirus ou la sauvegarde démarre en règle générale à des heures déterminées. Elles permettent donc de comparer des comportements. Quoi de plus classique que d'analyser le comportement de chaque jour de la semaine.

On peut bien sur définir une plage que l'on compare dans une périodicité. Par exemple, je prends une plage d'une heure entre 10h30 et 11h30 le lundi, que je compare à la même plage la semaine précédente.

Complétude

- Mais que dire des tailles véhiculées ?

```
fhm@KODA:~$ ping www.google.fr
PING www.google.fr (142.250.200.227) 56(84) bytes of data.
64 bytes from mrs08s18-in-f3.1e100.net (142.250.200.227): icmp_seq=1 ttl=117 time=11.4 ms
```

  - 64 octets envoyés à chaque transmission
  - 56 octets : volume de données arbitraites
  - 8 octets : volume de l'entête d'un "echo request"
  - 20 octets : volume de l'entête ICMP
- Quelques options :
  - -c : nombre de requête "echo request" qui sera envoyé
  - -i : intervalle de temps entre 2 envois en seconde
  - -s : taille du paquet transmis

9

Alors pour les tailles, nous avons donc sur Linux 64 octets transmis, composés de 56 octets de données quelconques incrémentés de 8 octets de l'entête du type de requête (ici Echo) et initialement, la trame ICMP a une entête de 20 octets. Nous comprenons maintenant le "56(84) bytes of data".

56 octets pour les données arbitraires

84 octets, correspondant à la somme de 56 + 8 + 20 octets, à savoir 84.