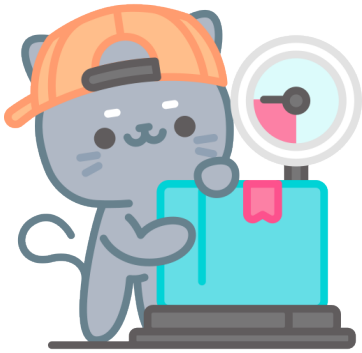
C’est quoi le MTU ?

Introduction

Quand on parle de réseau, on imagine souvent que les données partent d’un ordinateur et arrivent directement à un serveur, un peu comme une lettre envoyée par la poste. En réalité, les données ne voyagent pas en un seul gros bloc. Elles sont découpées en petits morceaux, appelés des paquets.



Définition du MTU

Le **MTU**, pour **Maximum Transmission Unit**, correspond à la taille maximale qu’un paquet peut avoir pour passer sur un réseau.

Dit plus simplement : le MTU, c’est la **taille maximale d’un paquet réseau** avant qu’il ne soit trop gros pour passer correctement.

Une analogie simple

On peut l’imaginer comme une limite de taille pour un colis. Si le colis est assez petit, il passe normalement dans le camion, dans les machines de tri, puis arrive à destination. S’il est trop gros, il faut soit le découper en plusieurs colis, soit il risque d’être refusé quelque part sur le trajet.

En réseau, c’est un peu pareil. Si un paquet est trop gros pour un équipement ou une liaison, il peut être découpé, ralenti, ou parfois même bloqué.

Valeur classique du MTU

Sur un réseau Ethernet classique, la valeur de MTU la plus courante est :

```
1500 octets
```

Cela veut dire qu'un paquet IP peut avoir une taille maximale de 1500 octets sur ce réseau. Ce n'est pas énorme, mais c'est largement suffisant pour transporter les données petit bout par petit bout.

Le MTU dans la pratique

Quand on charge une page web, qu'on regarde une vidéo, qu'on télécharge un fichier ou qu'on se connecte en VPN, beaucoup de paquets circulent en arrière-plan. On ne les voit pas, mais ils sont

là, et le MTU définit la taille maximale de ces petits morceaux.

Le souci, c'est que tous les réseaux ne permettent pas forcément de faire passer des paquets de la même taille. Un réseau local peut accepter 1500 octets, mais dès qu'on ajoute certains éléments comme un VPN, du PPPoE, du tunnel GRE, de l'IPsec, du WireGuard ou d'autres encapsulations, une partie de la place disponible est utilisée pour ajouter des informations supplémentaires autour du paquet.

C'est comme si on mettait un colis dans une boîte, puis cette boîte dans une autre boîte. Le contenu n'a pas changé, mais l'emballage prend plus de place.

Résultat : un paquet qui passait très bien sur un réseau classique peut devenir trop gros une fois encapsulé dans un tunnel VPN.

Exemples de valeurs de MTU

C'est pour ça qu'on voit parfois des MTU plus petits, par exemple :

```
1500 → Ethernet classique
1492 → connexion PPPoE
1420 → souvent utilisé avec WireGuard
1400 → valeur prudente pour certains VPN ou tunnels
```

Ce ne sont pas des règles absolues, mais ça donne une idée. Plus il y a de couches autour du paquet, plus il faut parfois réduire le MTU pour éviter les problèmes.

Symptômes d’un MTU mal configuré

Quand le MTU est mal adapté, les symptômes peuvent être très étranges. Ce n’est pas forcément une panne franche où “rien ne marche”. Parfois, certaines choses fonctionnent très bien, et d’autres non.

Par exemple, on peut avoir Internet qui fonctionne, mais certains sites ne chargent pas. Une page peut commencer à s’afficher, puis rester bloquée. Un VPN peut se connecter, mais certains services derrière ne répondent pas. Une connexion SSH peut marcher, mais un transfert de fichier peut échouer. Un site peut être accessible depuis un réseau, mais pas depuis un autre.

C’est le genre de problème qui donne envie d’accuser le DNS, le pare-feu, le navigateur, le serveur, la météo, et probablement aussi l’imprimante du bureau. Pourtant, parfois, le coupable est simplement un MTU trop grand quelque part sur le chemin.

Path MTU Discovery

Normalement, les équipements réseau savent gérer ce problème grâce à un mécanisme appelé **Path MTU Discovery**. Le principe est assez simple : la machine essaie de découvrir la taille maximale des paquets qui peuvent passer jusqu’à la destination. Si un paquet est trop gros, un équipement réseau devrait répondre avec un message ICMP pour dire quelque chose comme : “ce paquet est trop gros, il faut envoyer plus petit”.

Le problème, c’est que ces messages ICMP sont parfois bloqués par des pare-feu mal configurés. Et là, la machine continue d’envoyer des paquets trop gros, sans comprendre pourquoi ça ne passe pas. On parle parfois de “black hole MTU (Le trou noir MTU)”, parce que les paquets disparaissent silencieusement.

Tester le MTU avec ping

Pour tester un problème de MTU, on peut utiliser la commande `ping` avec une taille précise et demander à ne pas fragmenter le paquet.

Sous Linux

On peut faire par exemple :

```
ping -M do -s 1472 exemple.fr
```

Pourquoi `1472` et pas `1500` ? Parce qu’il faut ajouter les en-têtes IP et ICMP, qui prennent 28 octets. Donc :

```
1472 + 28 = 1500
```

Si ça passe, cela veut dire qu’un paquet de 1500 octets passe correctement jusqu’à la destination. Si ça ne passe pas, on peut réduire progressivement la taille.

Par exemple :

```
ping -M do -s 1400 exemple.fr
ping -M do -s 1380 exemple.fr
ping -M do -s 1360 exemple.fr
```

L’idée est de trouver la plus grande taille qui passe encore correctement.

Sous Windows

On peut faire un test similaire avec :

```
ping exemple.fr -f -l 1472
```

Ici, `-f` indique qu’on ne veut pas fragmenter le paquet, et `-l` permet de choisir la taille des données envoyées.

Si le test échoue, on peut réduire la valeur :

```
ping exemple.fr -f -l 1400
ping exemple.fr -f -l 1380
ping exemple.fr -f -l 1360
```

Une fois qu'on trouve la plus grande valeur qui fonctionne, il faut ajouter 28 pour obtenir le MTU approximatif.

Par exemple, si cette commande fonctionne :

```
ping exemple.fr -f -l 1392
```

Alors le MTU correspondant est environ :

```
1392 + 28 = 1420
```

C'est pour ça qu'on retrouve souvent `1420` dans des configurations VPN comme WireGuard.

Bonnes pratiques

Il faut quand même rester prudent : modifier le MTU au hasard n'est pas toujours une bonne idée. Le réduire trop bas peut fonctionner, mais ce n'est pas forcément optimal. Des paquets plus petits peuvent entraîner un peu plus de surcharge, car il faudra envoyer plus de paquets pour transporter la même quantité de données.

Le but n'est donc pas de mettre une valeur minuscule "pour être tranquille", mais de trouver une valeur adaptée au chemin réseau utilisé.

Dans un réseau classique, on laisse généralement le MTU par défaut à `1500`. Si on utilise un VPN, un tunnel ou une connexion particulière, il peut être nécessaire de descendre un peu. Dans beaucoup de cas, une valeur autour de `1400` ou `1420` peut résoudre des comportements bizarres liés aux tunnels.

Conclusion

Le MTU est donc un petit réglage discret, mais il peut avoir un gros impact. Quand il est bien configuré, on ne pense jamais à lui. Quand il est mal adapté, il peut provoquer des problèmes vraiment trompeurs : des sites qui chargent à moitié, des VPN instables, des connexions lentes ou des services accessibles uniquement dans certains cas.

En résumé, le MTU correspond à la taille maximale des paquets qui peuvent circuler sur un réseau. Si les paquets sont trop gros pour passer quelque part, ils doivent être fragmentés ou réduits. Et si le réseau ne gère pas correctement cette situation, certaines connexions peuvent se comporter bizarrement.

C’est un peu comme essayer de faire passer un meuble dans un couloir trop étroit. Si on peut le démonter proprement, tout va bien. Si personne ne dit qu’il bloque, on reste devant la porte à se demander pourquoi ça n’avance pas.

Révision #2
Créé 2026-07-09 05:10:33 UTC par Renard
Mis à jour 2026-07-11 15:11:14 UTC par Renard