

Dictionnaire de filtres

Ce document est réalisé dans le cadre de l'unité d'enseignement « Réseaux » dispensée par la faculté des Sciences de Sorbonne Université.

1. Préambule

Le visualisateur de flux de trafic réseau permet l'analyse du flux en fonction de certaines données. Cette analyse spécifique peut être réalisée à l'aide des filtres décrits ci-dessous.

Attention : Lors de l'utilisation des filtres, veuillez veiller à ne pas mettre d'espaces. Les caractères doivent être écrits les uns à la suite des autres.

2. Commandes supportées par le visualisateur

Commande	Objectif
ip	Filtrer avec l'adresse IP
ipsrc	Filtrer avec l'adresse IP de la source
ipdst	Filtrer avec l'adresse IP de la destination
proto	Filtrer par protocole (Ethernet, IPV4, TCP ou HTTP)
pt	Filtrer avec le numéro de port
ptsrc	Filtrer avec le numéro de port de la source
ptdst	Filtrer avec le numéro de port de la destination

3. Exemples de requêtes

Requête	Résultat
ipsrc==255.255.255.255	Trames ayant pour adresse IP source 255.255.255.255
ipdst==255.255.255.255	Trames ayant pour adresse IP de destination 255.255.255.255
proto==TCP	Trames ayant pour protocole TCP
ptsrc==80	Trames ayant pour numéro de port source 80)
Ptdst==80	Trames ayant pour numéro de port de destination 80