netMET LookUp

Outil de recherche multicritères

Avant-propos

A. Objet

Ceci est la documentation de l'outil de consultation *netMET LookUp*.

Il est destiné à un large public, et constitue à la fois une aide pour les utilisateurs de *nmlookup*, ainsi qu'une documentation technique pour les développeurs.

B. Structure de la documentation

La documentation est découpée en deux grandes parties :

- le chapitre 2 présente les fonctionnalités de l'outil; cette section est destinée à tous ceux qui découvrent *nmlookup* et qui désirent acquérir rapidement toutes les finesses de l'outil.
- le chapitre 3 et le chapitre 4 sont quant à elles destinés à toutes les personnes soucieuses de comprendre le fonctionnement de *nmlookup*; cette partie constitue la documentation technique du produit.

C. Quelques mots sur le projet *netMET LookUp*

netMET LookUp a vu le jour un certain mois de juillet 2000; les circonstances de cette apparition restent encore vagues, mais aux dernières nouvelles, il semblerait que l'outil ait été développé par un stagiaire du CIRIL, alors fasciné devant la puissance de *netMET* et par la motivation de son créateur, le célébre Alexandre Simon. Certains prétendent qu'il est iranien; d'autres, qu'il raffolait d'une certaine friandise appelée "tapis rouge", alors commercialisée sous le nom "LookOLook", et que l'origine même du nom *netMET LookUp* viendrait de là. A l'heure actuelle, le mystère persiste encore.

Le présent document est une compilation de l'ensemble des notes trouvées sur son plan de travail. Comme tout travail de mémoire, des erreurs peuvent exister; n'hésitez pas à lui faire part de vos critiques : certains prétendent qu'il répond à ses mails...

Visite guidée de *netMET LookUp*

Ce chapitre présente toutes les fonctionnalités de *nmlookup*. Vous y apprendrez comment utiliser l'outil, et comment tirer profit de ses nombreuses possibilités.

A. *nmlookup* : un outil de recherche multicritère multicession

netMET LookUp se lance depuis le browser de n'importe quel poste client ayant accès au serveur web de la machine *netMET*.

C'est un outil de consultation multicritère permettant de formuler des requêtes d'une grande variété. Cette variété vient du fait qu'il est possible de demander pour une période donnée, l'ensemble des flux vérifiant une ou plusieurs des propriétées suivantes :

- précision d'une machine ou d'un ensemble de machines en source et/ou en destination,
- utilisation d'un service particulier,
- utilisation d'un service particulier dans une quantité donnée,
- utilisation d'au moins un service dans une quantité donnée,
- quantité de trafic total compris dans un intervalle donné.

La requête formulée par l'utilisateur est communiquée au serveur par un *CGI*, et y est exécuté. Il est donc possible à plusieurs utilisateurs d'utiliser *nmlookup* en même temps. Mais il est également possible pour un utilisateur de lancer plusieurs recherches simultanément.

netMET LookUp permet de résoudre toutes les requêtes formulées grâce à la liste des contraintes que nous avons précédemment citées. Mais aucune information n'est donnée quant à la durée que cette recherche peut prendre! Il est ainsi très facile de formuler des requêtes d'une grande compléxite (Exemple *(soyons fou!)* : rechercher toutes les communications comprises entre 50 Octets et 1000 Octets pour le mois de Juillet 2000), qui mettront beaucoup de temps à s'exécuter.

Vous devrez donc savoir plus ou moins évaluer la compléxité d'une requête pour utiliser efficacement l'outil; de façon générale, sachez que

... une recherche prendra du temps ...

- si elle est effectuée sur plusieurs périodes et que les résultats sont cumulés
- si des quantités sont recherchées

... sera rapide ...

- si la source ou la destination sont spécifiées
- si un service est spécifié

Ceci étant dit, vous pouvez tout à fait lancer des recherches très complexes. Soyez juste conscient du temps de calcul que cela peut représenter!

B. La 1ère étape de la recherche : la saisie des périodes de recherche

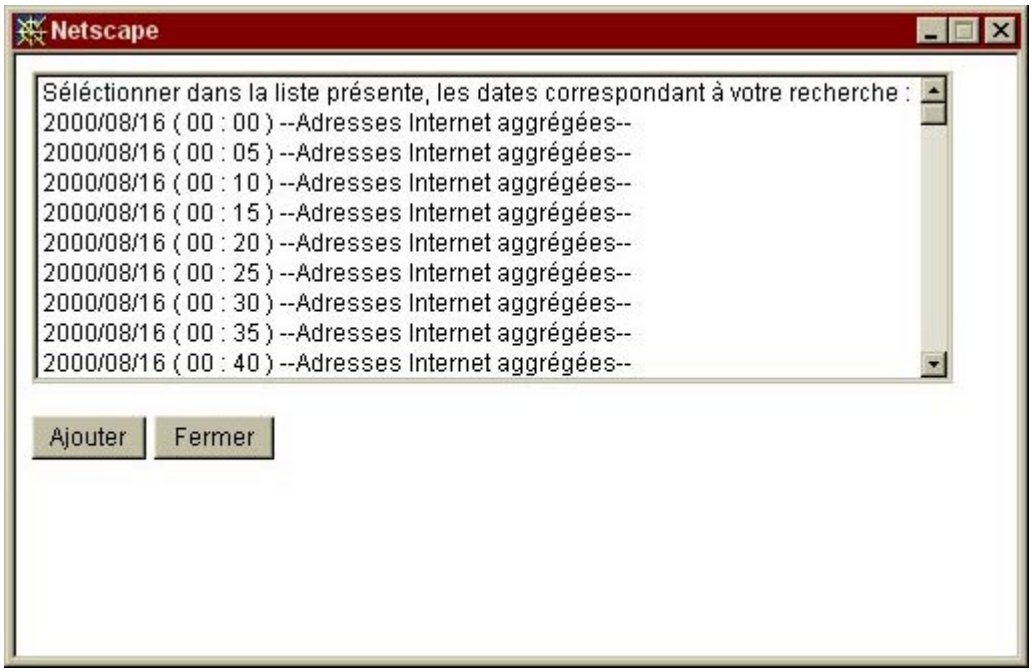
Une recherche s'applique avant tout à une période. La section consacrée à la sélection des périodes de recherche se présente ainsi :

L'ensemble des dates prises en compte pour la recherche seront celles qui se trouvent dans la zone blanche. On peut y ajouter des dates, et en supprimer, en utilisant les deux boutons qui se trouvent à sa droite.

Deux granularités différentes existent à l'heure actuelle : l'utilisateur a le choix entre des périodes longues correspondant à une journée, et des périodes plus courtes de l'ordre d'une dizaine de minutes. Et pour chacune d'elle, il peut choisir d'activer l'aggrégation des adresses de l'Internet; ceci donne ainsi quatre choix de dates possibles, qui sont :

- les tranches horaires de 24h, avec aggrégation des adresses extérieures au site,
- les tranches horaires de 5 minutes, avec aggrégation des adresses extérieures au site,
- les tranches horaires de 24h, avec le détail de toutes les adresses,
- les tranches horaires de 10 minutes, avec le détail de toutes les adresses.

Suivant le choix effectué et des informations fournies sur l'année, le mois et dans certains cas, le jour, un script *CGI* est lancé sur le serveur afin de rechercher le fichiers de données disponibles; les résultats sont affichés dans une fenêtre similaire à celle-ci. On peut alors choisir une ou plusieurs dates à rajouter (utilisez la touche <*CTRL* pour en sélectionner plusieurs).



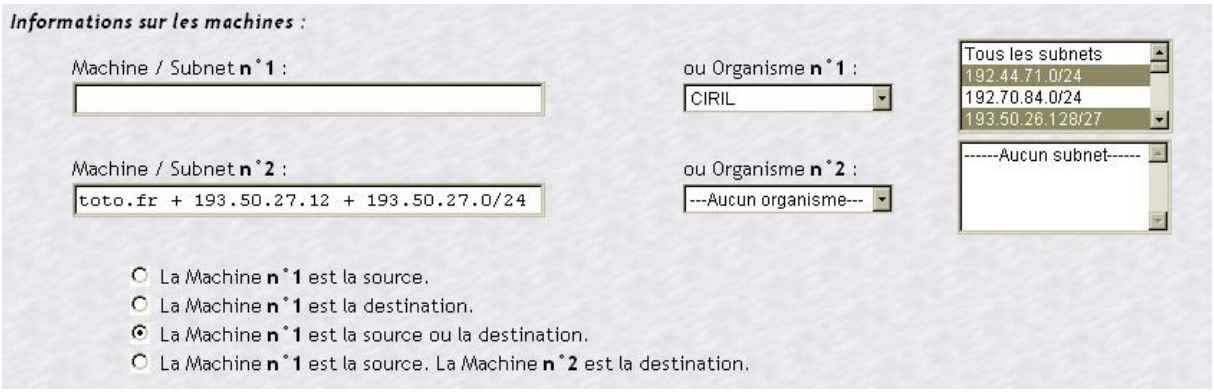
L'option *"Cumuler les résultats si plusieurs dates sont sélectionnées"* vous permet de lancer votre recherche, soit séparément sur chacune des périodes sélectionnées, soit sur leur totalité. Il est à noter que le temps de calcul est plus long dans le cas du cumul.

C. La 2ème étape de la recherche : le choix des critères

Les données générées par *netMET* sont considérablement importantes et riches; l'objectif de *netMET LookUp* est de permettre la recherche d'informations parmi ces données. Pour celà, il suffit de renseigner les critères correspondant à la recherche que l'on veut faire. On peut ainsi rechercher tous les flux

- ayant en source une certaine machine ou ensemble de machines,
- ayant en destination une certaine machine ou ensemble de machines,
- ayant utilisé un service particulier,
- ayant utilisé un service particulier dans une quantité donnée,
- ayant utilisé au moins un service dans une quantité donnée,
- et enfin, dont le cumul en octets est compris dans un intervalle donné.

C.1. La recherche de machines en source, en destination



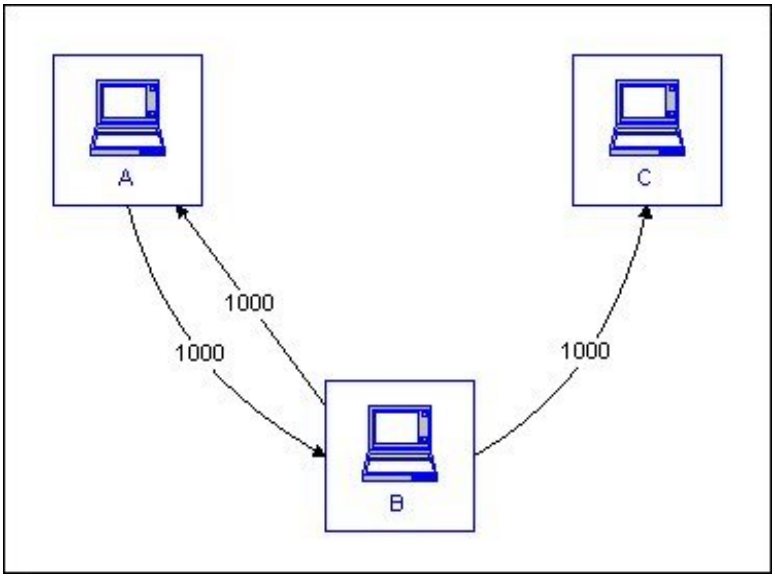
Afin de spécifier les machines qui sont en source et les machines qui sont en destination, vous disposez de deux ensembles de machines, celles portant le numéro 1 et celles portant le numéro 2, et de cases à cocher donnant le sens de communication entre ces entités. Bien sûr, les machines n°2 ne sont prises en comptes que si la quatrième option est choisie.

Pour choisir les machines, on peut :

- soit saisir leurs adresses à la main dans le champs prévu à cet effet; dans ce cas, on peut taper soit l'adresse symbolique, soit l'adresse IP, soit l'adresse en notation *CIDR* (xxx . xxx . xxx . xxx/nn) dans le cas d'un subnet. Si plusieurs adresses sont saisies, elles doivent être séparées par des '+'; ces machines seront alors considérées comme une seule et même entité.

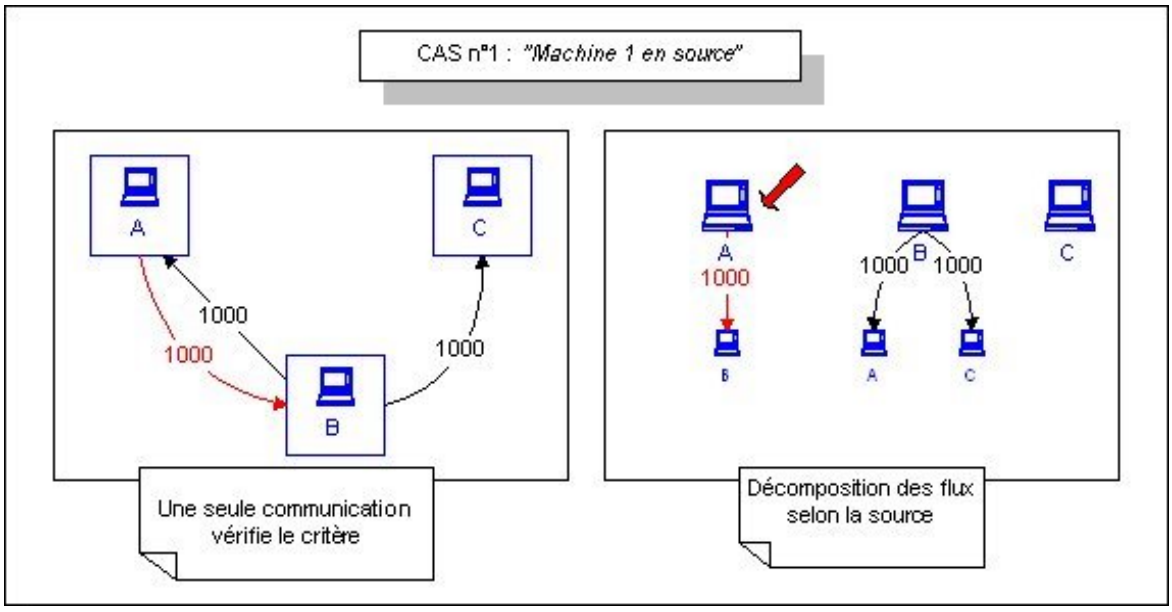
- soit sélectionner dans les listes déroulantes, un ou plusieurs des subnets d'un organisme connu de *netMET*. Si vous désirez séléctionner tous les subnets d'un organisme, vous pouvez soit choisir *"Tous les subnets"* dans la liste donnant les subnets, soit ne sélectionner aucun des subnets de l'organisme : *nmlookup* prendra par défaut l'organisme en entier. Notez que ces données ne sont prises en compte que si aucune adresse de machine(s) ou de subnet(s) n'est saisie comme spécifié dans le premier cas.

Enfin, il va de soit que si la requête porte sur toutes les machines, il suffit de ne sélectionner aucun adresse. Par contre, les trois premières options donnant la direction de communication pour la machine n°1 gardent encore leur sens dans le cas où un critère quantitatif est saisi (il pourra s'agir d'une quantité de service, ou d'une quantité de tafic global). Vous allez très vite comprendre pourquoi sur un exemple; soit la configuration suivante :

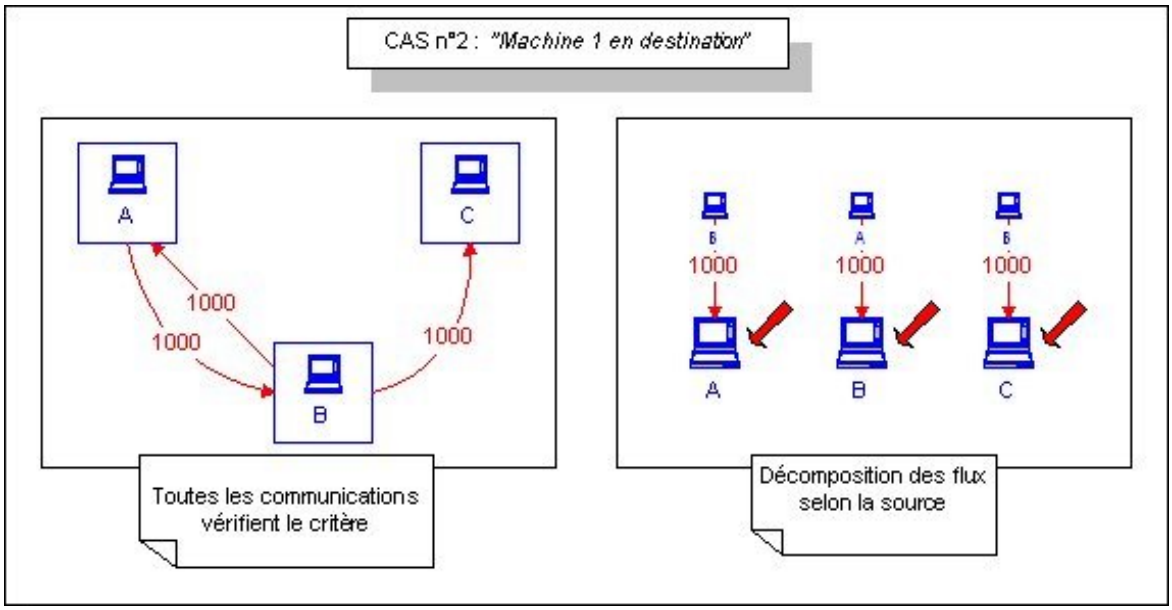


Comme on peut le voir, il ne revient pas au même de rechercher ...

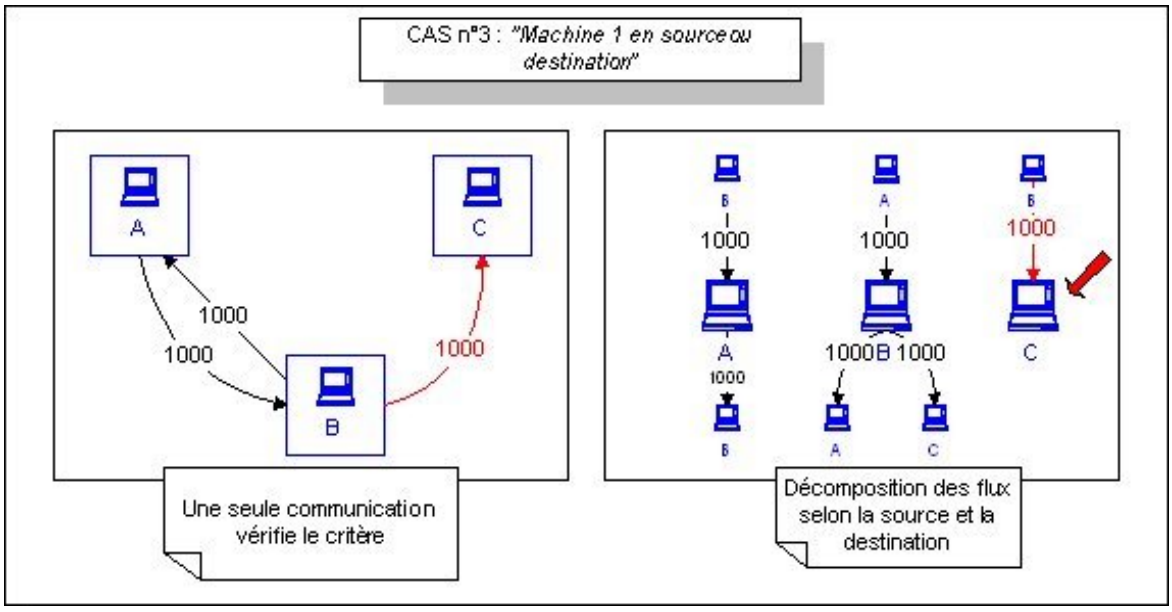
- *1er cas :* tous les flux pour lesquels la machine en source émet globalement 1000 Octets



- *2ème cas :* tous les flux pour lesquels la machine en destination reçoit globalement 1000 Octets



- *3ème cas :* tous les flux pour lesquels une machine, en source ou en destination, réalise un trafic global de 1000 Octets

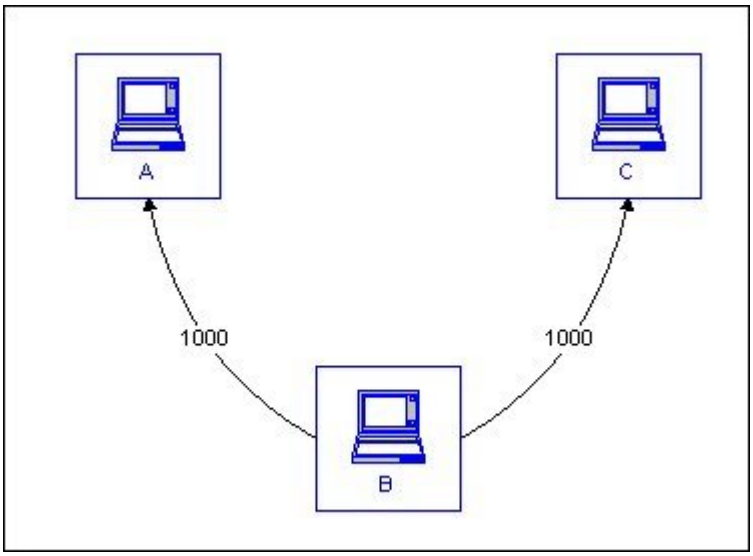


C.2. La recherche d'un service, d'une quantité de service

Il vous est possible de rechercher les flux :

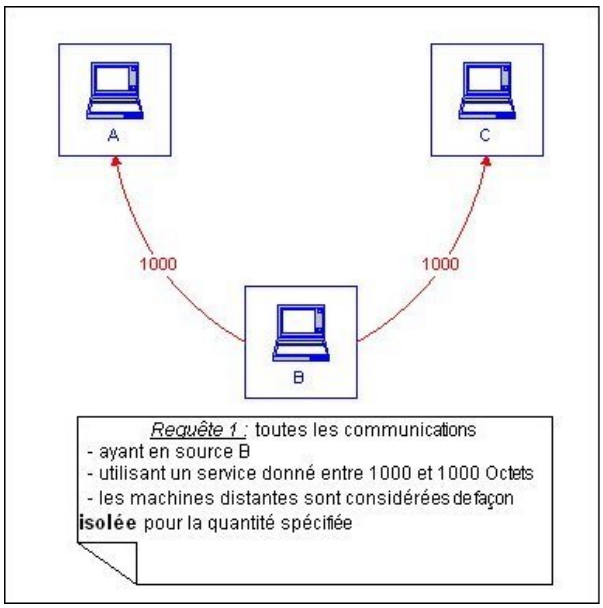
- qui utilisent un service particulier; le format de saisie est le suivant : *"port utilisé par le service / protocole"*. Par exemple, il faudra taper "80/6" pour le *web*, ou "20/6" pour *ftp*. La liste des services connus par *netMET* (fichier /etc/services) est également proposée.
- qui utilisent un service particulier dans une quantité donnée; les quantités seront saisies dans les deux champs prévus à cet effet.
- dont au moins un service est utilisé dans une quantité donnée; il suffit dans ce cas de ne pas remplir le champ "service".

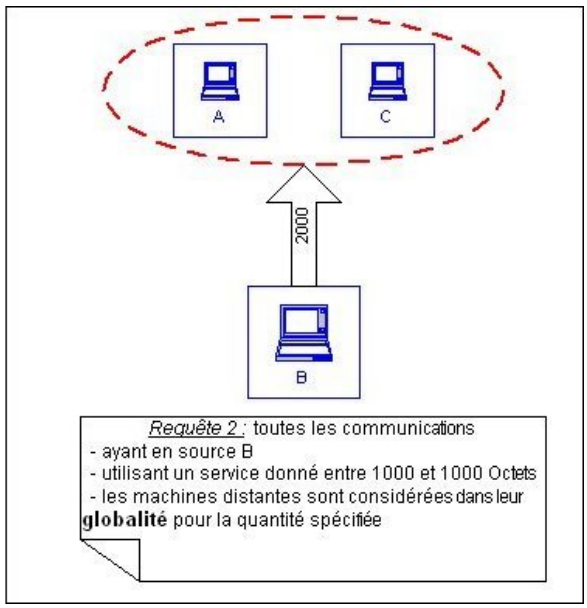
L'option qui se situe au bas de cette rubrique et qui s'intitule *"Les machines distantes sont considérées dans leur globalité"* permet de préciser si les quantités saisies concernent l'ensemble des machines distantes ou si elles les concernent chacune séparément. Un exemple vous permettra de mieux comprendre cette différence; soit la configuration suivante :



Si vous recherchez toutes les communications
- ayant en source la machine B et
- correspondant à 1000 Octets pour un service donné,

aucune des deux communications n'est affichée si la case est cochée, alors que les deux seront affichées si la case n'est pas cochée.





Pour finir, notez que le choix du sens de la communication (Machine n°1 en source, Machine n°1 en destination, Machine n°1 en source ou destination) a son importance lorsqu'une recherche concerne une quantité de service. Reportez-vous pour plus d'informations à la section explicant la différence entre ces trois choix.

C.3. La recherche d'une quantité totale de flux

Le dernier critère concerne la quantité totale d'octets transmis entre deux machines ou ensemble de machines. Les quantités sont à spécifier dans les champs prévus à cet effet.

De même que pour les quantités de service, une option permet de spécifier si les machines distantes sont à considérer dans leur globalité ou non.

Je rappelle enfin que le choix du sens de communication effectué dans la section "Informations sur les machines" a également son importance pour ce critère. Reportez-vous aux explications concernant ces choix pour plus d'informations.

D. Affichage des résultats

A chaque fois qu'une requête est lancée, une nouvelle fenêtre de navigation est créée pour afficher les résultats. Et cette fenêtre est subdivisée en autant de parties qu'il y a de recherche sur des périodes distinctes.

Une récapitulation de la requête est faite avant l'affichage de chaque résultat; elle permet notamment de vérifier l'exactitude de la saisie. Les communications entre les machines sont affichés les unes après les autres, dans un ordre quelconque. Par contre, les services sont triés pour chacun des flux suivant leur importance en terme de quantité.

Et Dieu créa netMET

Ce chapitre a pour objet de résumer les connaissances qu'il faut avoir sur *netMET* afin de comprendre les choix effectués lors de la conception de *netMET LookUp*. Les personnes connaissant bien *netMET* peuvent sauter ce chapitre et passer directemnt au suivant.

A. Divers types d'informations générées par netMET

netMET est un outil de métrologie qui offre à l'heure actuelle trois services :

- la métrologie générale,
- la métrologie pour les statistiques,
- la métrologie orientée sécurité.

Chacun de ces services possède ses caractéristiques propres, et correspond à un usage bien particulier.

La métrologie générale :

Les données de la métrologie générale sont générées tous les 24 heures. L'ensemble des machines extérieures au site sont vues comme une seule et même entité : c'est ce que l'on appelle plus communément le "Trou Renater".

Ces mesures présentent l'intérêt d'être suffisamment générales pour effectuer des recherches très "grossières"; les informations qu'elles contiennent sont déjà très riches et permettent de guider l'utilisateur dans une recherche plus approfondie.

La métrologie pour les statistiques :

Les données de cette métrologie sont quant à elles générées toues les 5 minutes. L'aggrégation des adresses Internet en un "Trou Renater" est toujours activée.

Le principal avantage que possède cette métrologie sur la métrologie générale est de donner, à 5 minutes près, l'heure à laquelle une communication a eu lieu. Cette information est d'autant plus importante que le service de sécurité est en place.

La métrologie orientée sécurité :

Ce service présente les mêmes caractéristiques que les deux précédents services, à la seule différence que l'aggrégation des adresses Internet n'est pas faite : il est ainsi possible de précisément voir l'adresse des machines avec lesquelles les ordinateurs du site ont communiquées.

Les mesures effectuées par ce service sont les plus fines qui soient, et sont répertoriées dans des fichiers générées tous les 10 minutes, ainsi que dans des fichiers journaliers de 24 heures.

B. Archivage des données

Les fichiers de données correspondant à chacun des services sont rangés dans des répertoires précis. Les noms de répertoire, ainsi que les noms des fichiers de données sont configurables à partir du fichier *"~netmet/netMET/etc/explt.conf"*.

Avec les paramètres par défaut, on obtient :

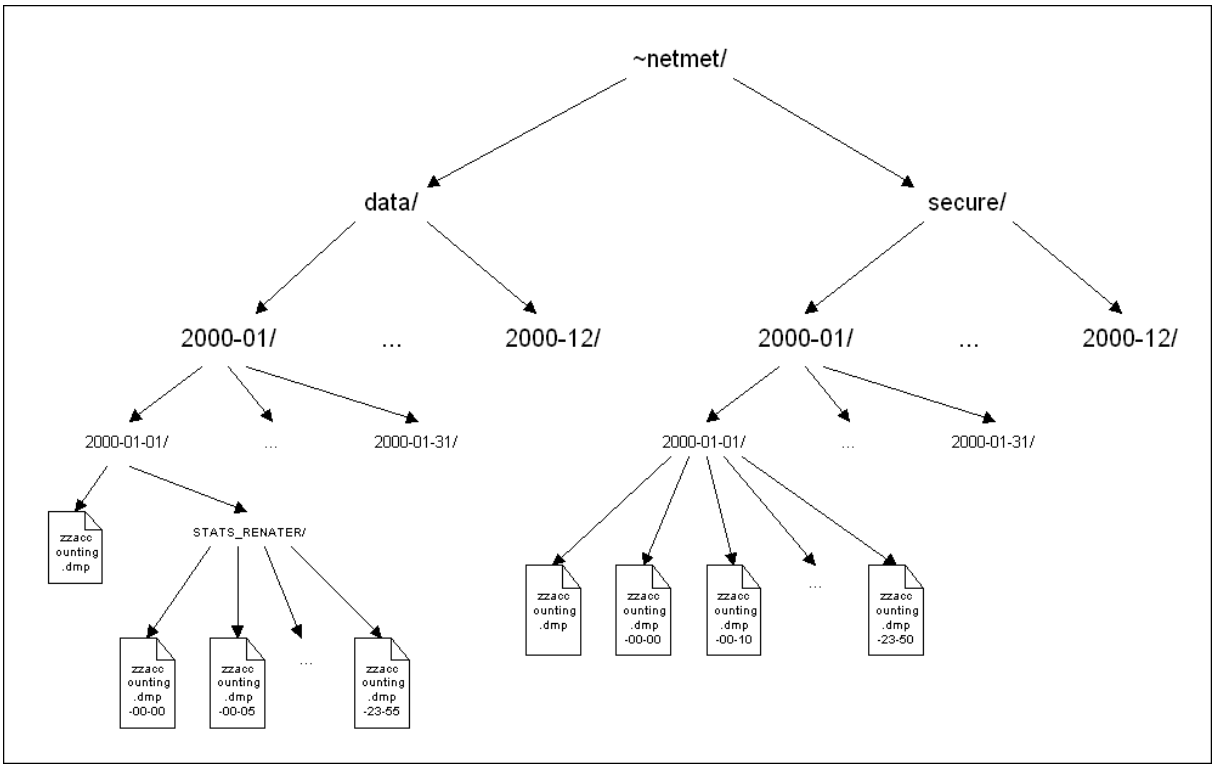
- un répertoire *"~netmet/data"*, qui comprend l'ensemble des données relatives à la métrologie générale et à la métrologie pour la sécurité.

Ce dossier est organisé de la façon suivante : chaque fichier de données de la métrologie générale est rangé dans un répertoire correspondant au jour où il a été généré, ce répertoire étant lui-même rangé dans un répertoire correspondant à son mois.

Les fichiers de la métrologie pour les statistiques sont juste séparés des fichiers de la métrologie générale par un répertoire nommé *"STATS_RENATER"*. Le nom de ces fichiers est suffixé par leur heure de génération, ce qui permet de les distinguer.

- un répertoire *"~netmet/secure/"* qui comprend l'ensemble des données relatives à la métrologie orientée sécurité. L'organisation est identique au précédent, à la différence que tous les fichiers sont rangés dans le même répertoire.

Pour résumer tout celà, voici un petit schéma :



Remarquons une chose importante : les fichiers des divers services sont générés à des heures précises de la journée, et paradoxalement, il peut arriver que les données qu'ils contiennent ne représentent pas nécessairement l'ensemble des communications qui ont eu lieu dans l'intervalle de temps qui suivait la pécédente génération. Un cas de figure typique où cela arrive est lorsque la métrologie est arrêtée pendant un certain temps : les fichiers de 24 heures ne contiennent alors des mesures que sur quelques heures.

Cette précision étant faite, nous confondrons dorénavant les noms de fichiers et la durée qu'elles sont censées représenter : ainsi, le fichier *"~netmet/secure/2000-07/2000-07-13/zzaccounting.dmp-14-20"* représentera les données recueillies pour la tranche horaire 14h20 - 14h30.

C. Exploitation des données

L'exécutable *netMETexp* permet de déchiffrer les infromations contenues dans les fichiers de données. Plusieurs options existent; nous allons détailler celles qui nous intéressent particulièrement :

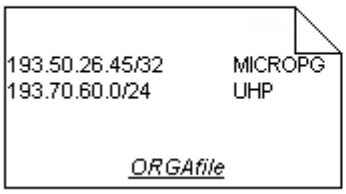
- l'option ***-H*** *(--HOSTaccprint __zzaccounting_file__)* permet l'affichage détaillé de toutes les mesures effectuées. Les résultats sont affichés ligne par ligne selon le format suivant :

@Source @Destination [service/protocole](taille en octets) ... [service/protocole](taille en octets)

Cette option est particulièrement intéressante pour faire des recherches exhaustives, et répondre à des questions du type : "*Quelles sont les machines qui ont fait .... ?*"

- l'option ***-O*** *(--ORGAaccprint __zzaccounting_file__)* et ***-f*** *(--ORGAfile __ORGAfile_)* permettent l'affichage de toutes les communications qui ont eu lieu entre une communauté restreinte de machines. Ces machines sont définies dans le fichier *"ORGAfile"* passé en paramètre de l'option *-f* , la notation utilisée étant la notation CIDR. Voici un exemple de fichier, ainsi que le résultat renvoyé :

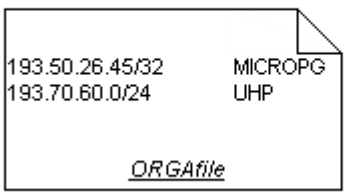
Fichier *ORGAfile* et résultat de l'appel de netMETexp avec les options -o et -f



MICROPG	UHP	[80/6](2500)[21/6](2000)
UHP	MICROPG	[80/6](2500)[21/6](2000)

Par ailleurs, une option supplémentaire ***-a*** *(--ALLtraffic)* donne la possibilité d'afficher sans restriction, tous les trafics qui ont concérné l'ensemble des machines sélectionnées.

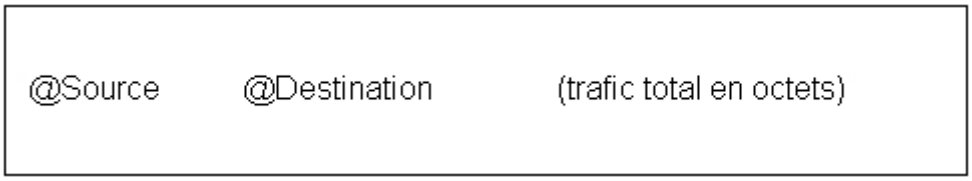
Fichier *ORGAfile* et résultat de l'appel avec l'option -a



MICROPG	UHP	[80/6](2500)[21/6](2000)
UHP	MICROPG	[80/6](2500)[21/6](2000)
MICROPG	194.214.110.110	[80/6](2500)[21/6](2000)
UHP	194.214.110.110	[80/6](2500)[21/6](2000)

La combinaison de ces trois options est particulièrement intéressante pour rechercher les trafics concernant, soit une machine précise, soit un subnet, soit un ensemble de subnets (un organisme par exemple);

- enfin, l'option ***-c*** *(--CUMULaccprint)*, combiné aux options -O et -H, permet d'afficher les résultats de façon cumulée; le format d'affichage est le suivant :



Cette option sera utile pour quantifier un trafic. Elle permettra de répondre aux questions du type : *"Quelles sont les communications comprises entre tant et tant d'octets?"*

Notez enfin qu'il est possible de passer en paramètre de la fonction *netMETexp*, plus d'un fichier de données; dans ce cas, les résultats seront cumulés.

D. Pourquoi *nmlookup*?

Un outil de consultation tel que *nmlookup* s'est avéré nécessaire pour plusieurs raisons.

Tout d'abord, les recherches faites *à la main* ne pouvaient s'effectuer que sur des critères relatifs aux machines et aux services; il suffisait dans ce cas de *piper* le résultat de la fonction *netMETexp* sur un *grep.* Toutes les recherches concernant les quantités de service, et les quantités de trafic globaux étaient alors impossibles.

Ensuite, il était nécessaire d'avoir accès au compte *netmet* pour pouvoir consulter les données. Par conséquent, il n'était pas possible de gérer les droits d'accès de telle façon que tout le monde ne puisse avoir accès à certaines donnnées comme la sécurité. Le fait de passer par un serveur web *Apache* nous ouvre la porte à de très nombreuses possibilités, en ce qui concerne les droits d'accès.

Enfin, on ne disposait d'aucun outil permettant de formuler des requêtes génériques et de formater leurs résultats de telle façon que l'on puisse facilement rechercher une information, et la comparer avec d'autres.

C'est pour répondre à tous ces besoins que nmlookup a été conçu. Dans la suite, nous détaillerons les choix effectués lors de la conception et la structure de l'outil.

netMET LookUp vu de l'intérieur

Ce chapitre constitue la documentation technique de *nmlookup.* Y sont exposés les grandes idées sur la manière dont l'outil est conçu. Aucun détail n'est donné quant au code source, mais vous n'aurez pas de mal à le comprendre après avoir pris connaissance de ce qui suit.

A. Conception générale

Perl, a "Practical Extraction and Report Language" :

Comme l'indique sa définition, Perl est un langage de programmation qui a été créé pour permettre de parcourir des fichiers textes, d'en extraire des informations et de générer un rapport sur les données extraîtes. Cette description correspondant très précisément à ce que nous voulons faire, c'est le *Perl* qui a été choisi comme langage de programmation.

Un souci permanent d'efficacité :

Les données sur lesquelles sont appliquées les requêtes sont importantes; il convient donc d'être efficace en ce qui concerne l'ordre dans lequel les critères sont appliqués. Voici l'ordre choisi :

- en premier, la recherche des machines;
- en deuxième, la recherche du service;
- en troisième, la recherche de la quantité de service;
- en quatrième, la recherche du cumul.

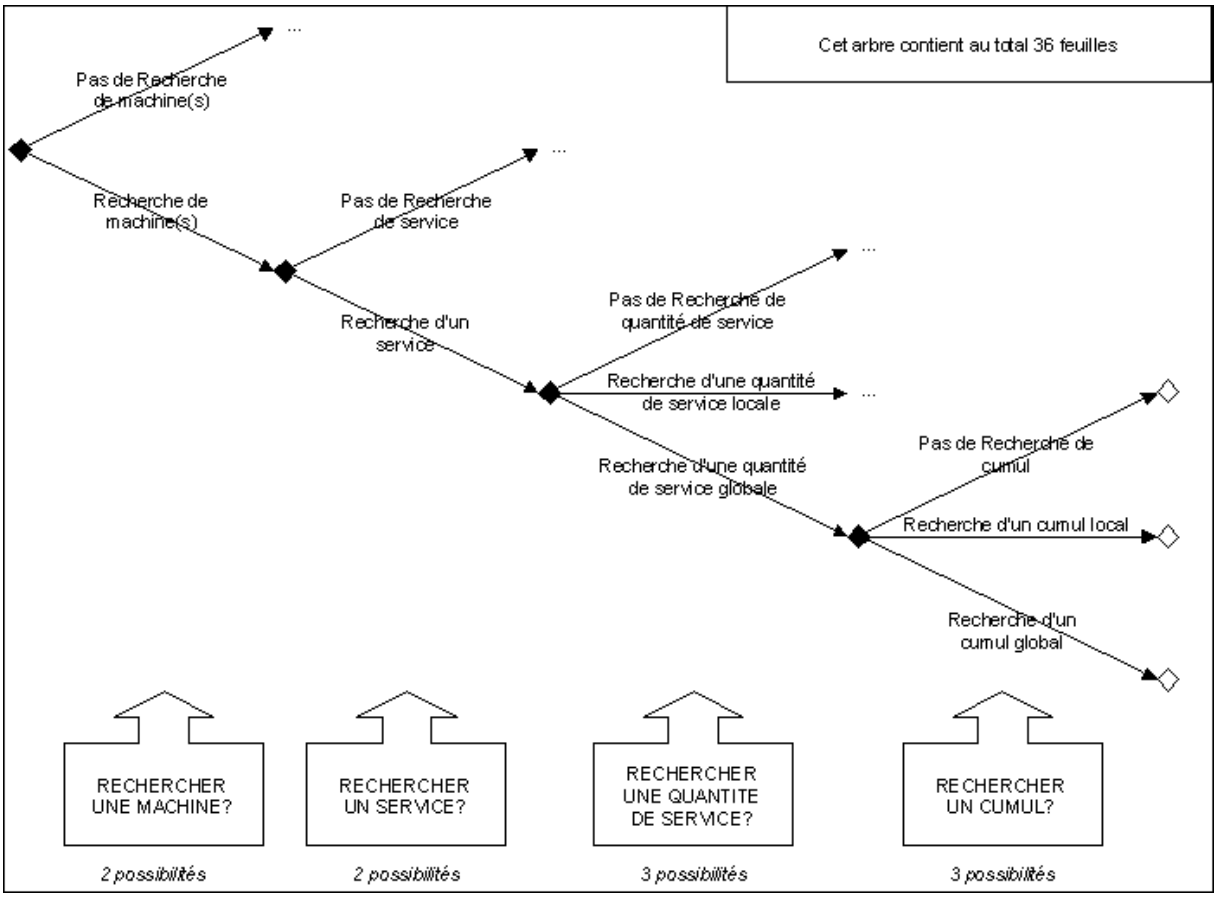
Cet ordre a été établi de telle façon que lorsque l'on arrive aux traîtements les plus complexes (recherche d'une quantités), la quantité de données à traîter soit la plus petite possible.

On utilise également le plus possible les mécanismes puissants d'Unix. Ainsi, pour la recherche des machines source et/ou destination, on utilise la fonction *"grep"* en ligne de commande.

Compléxité du problème :

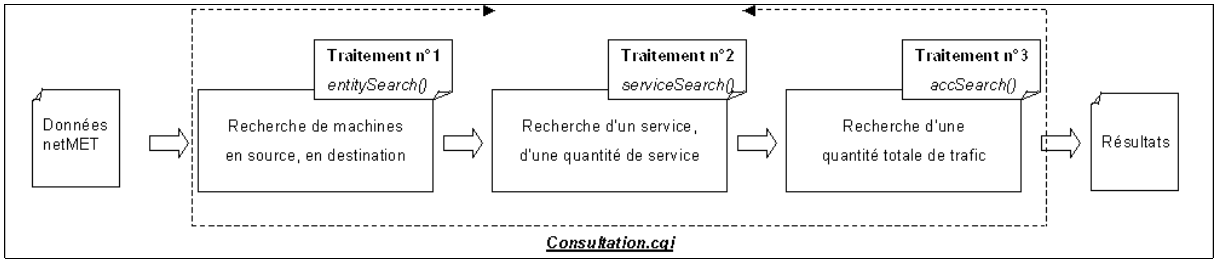
La principale difficulté que l'on rencontre lors de l'élaboration d'un tel outil est de pouvoir prendre en compte l'ensemble des requêtes que l'on peut formuler grâce à un certain nombre de critères. C'est comme si on simulait en fait l'interrogation d'une base de données relationnelle par une requête *SQL*.

On peut résumer la situation sous la forme d'un arbre :



Il est clair que l'on ne va pas écrire 36 sous-fonctions différentes pour traîter chaque cas de figure. On va plutôt utiliser l'une des grandes forces du langage *Perl* que constitue la manipulation des fichiers.

Un module différent pour chaque critère :

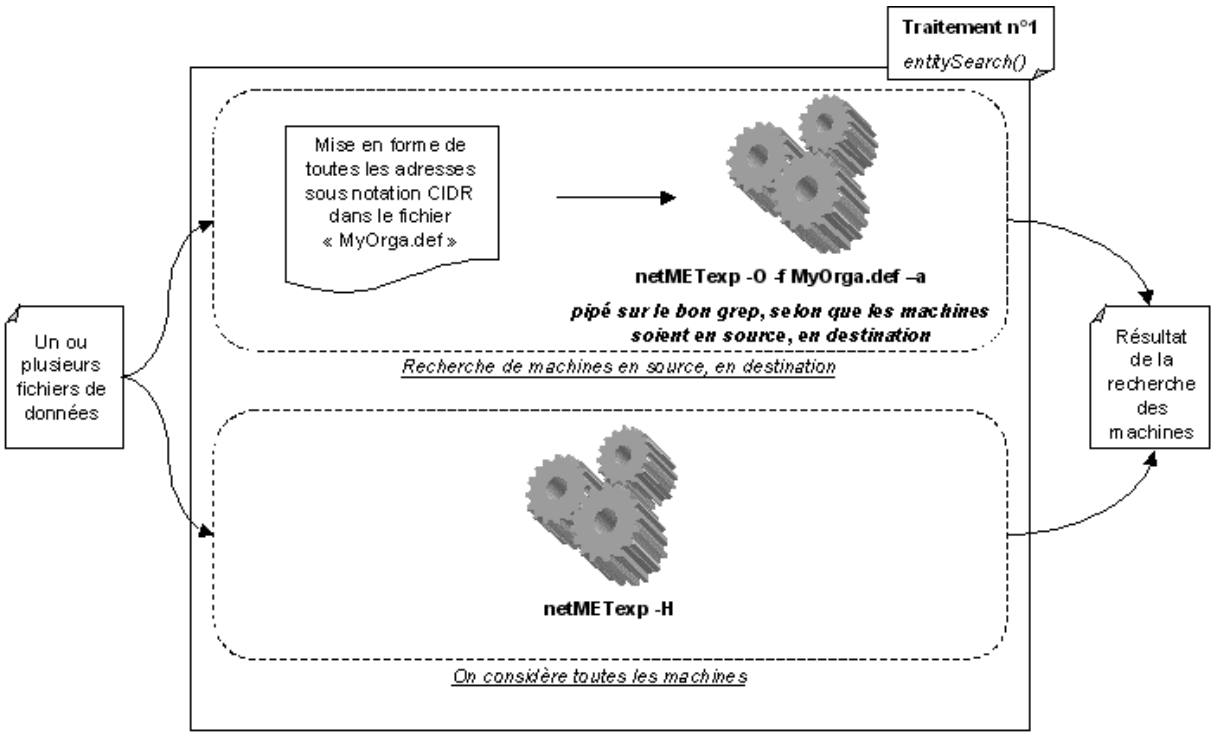


L'application est découpée en trois sous-fonctions, qui ont chacune un objectif précis : rechercher les données vérifiant un critère donné; ainsi,

- la première sous-fonction cherche parmi les données netMET à consulter, l'ensemble de celles qui vérifient le critère concernant les machines; elle les renvoie à la seconde sous-fonction;
- la deuxième sous-fonction recherche parmi les données qu'elle a reçue, l'ensemble des flux respectant le critère des services et quantité de service, qu'elle renvoie à la troisième sous-fonction;
- enfin, la dernière sous-fonction recherche les données vérifiant le critère du cumul, et les affiche en tant que résultat.

La communication des données entre les diverses sous-fonctions est faite grâce à des fichiers.

B. Recherche de machines, de subnets ou d'organismes



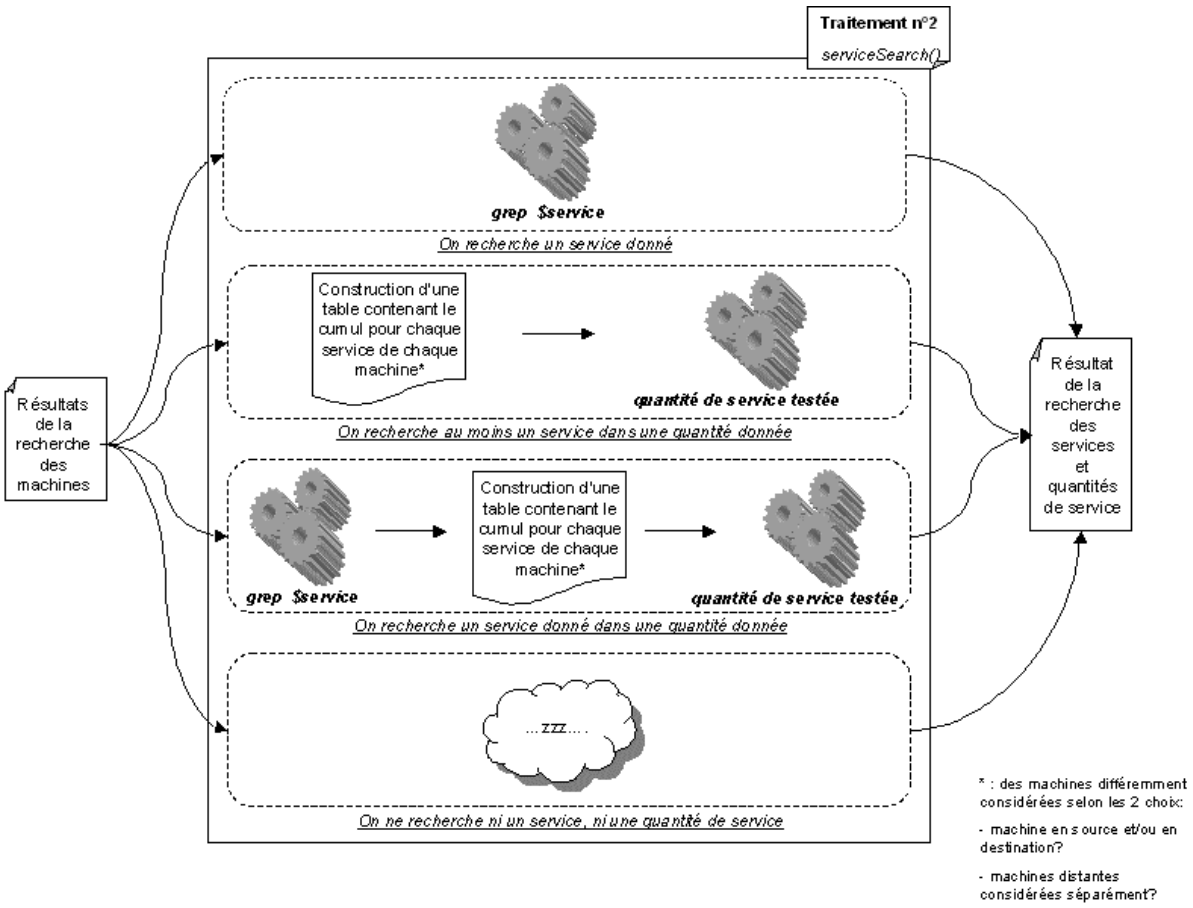
Deux types de traîtement différents peuvent être effectués par la fonction *"entitySearch()"*, selon que l'on recherche ou non des machines.

- Si on ne recherche aucune machine en particulier, alors on appelle l'exécutable *netMETexp* avec l'option *-H (--HOSTaccprint*), en lui passant en paramètre les fichiers correspondant aux périodes spécifiées.

- Si une machine ou un ensemble de machines est spécifié, c'est l'option *-O (--ORGAaccprint) qui est utilisé.* On crée ainsi un fichier temporaire contenant l'ensemble des machines à rechercher, et on le passe en paramètre de l'option *-f (--ORGAfile)*. Enfin l'option *-a (--ALLtraffic)* nous permettra de connaître tous les traffics relatifs à ces machines.

Le résultat de cette fonction est un descripteur de fichier correspondant à la commande appelée.

C. Recherche d'un service, d'une quantité de service



La fonction *"serviceSearch()"* effectue quatre types de traîtements, suivant que le service soit spécifié ou non, et qu'une quantité de service soit spécifiée ou non.

- Le cas le plus simple est bien sûr lorsque l'on ne demande rien en terme de service et quantité de service : il suffit de renvoyer le descripteur de fichier obtenu par l'appel de la précédante fonction *"entitySearch()"*.

- Dans le cas où un service est spécifié, il suffit de retenir les flux qui contienne ce service : on lit ainsi le fichier généré par *"entitySearch()"* ligne par ligne, et on ne garde que celles qui nous intéresse.

- C'est dans le cas où une quantité de service est spécifiée que le traîtement est un peu plus long : il faut lire une fois le fichier de données, créer à partir de ce dernier une table contenant les informations sur les quantités de services, puis relire une seconde fois le fichier de données pour ne retenir que les lignes qui conviennent.

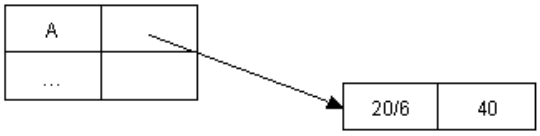
La structure de donnée utilisée est une table de hachage, dont chaque élément pointe vers une table de hachage. Les clés de la

première table sont des adresses de machines; celles de la seconde sont des services. Le choix des clés pour la première table dépend évidemment du sens de la communication et de l'option *"Les machines distantes sont considérées dans leur globalité"*. Voici un exemple pour vous en convaincre :

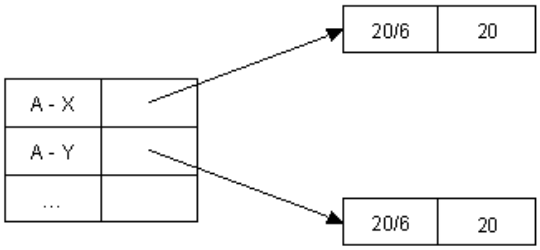
Données :

A	X	[20/6](20)
A	Y	[20/6](20)
…	…	…

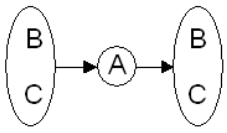
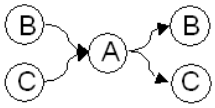
Cas n°1 : Les flux telles que :
- on ait **A** en source,
- utilisant au moins un service entre *tant* et *tant* d'octets,
- les machines distantes soient vues dans **leur globalité**.



Cas n°2 : Les flux telles que :
- on ait **A** en source,
- utilisant au moins un service entre *tant* et *tant* d'octets,
- les machines distantes soient vues **séparément**.



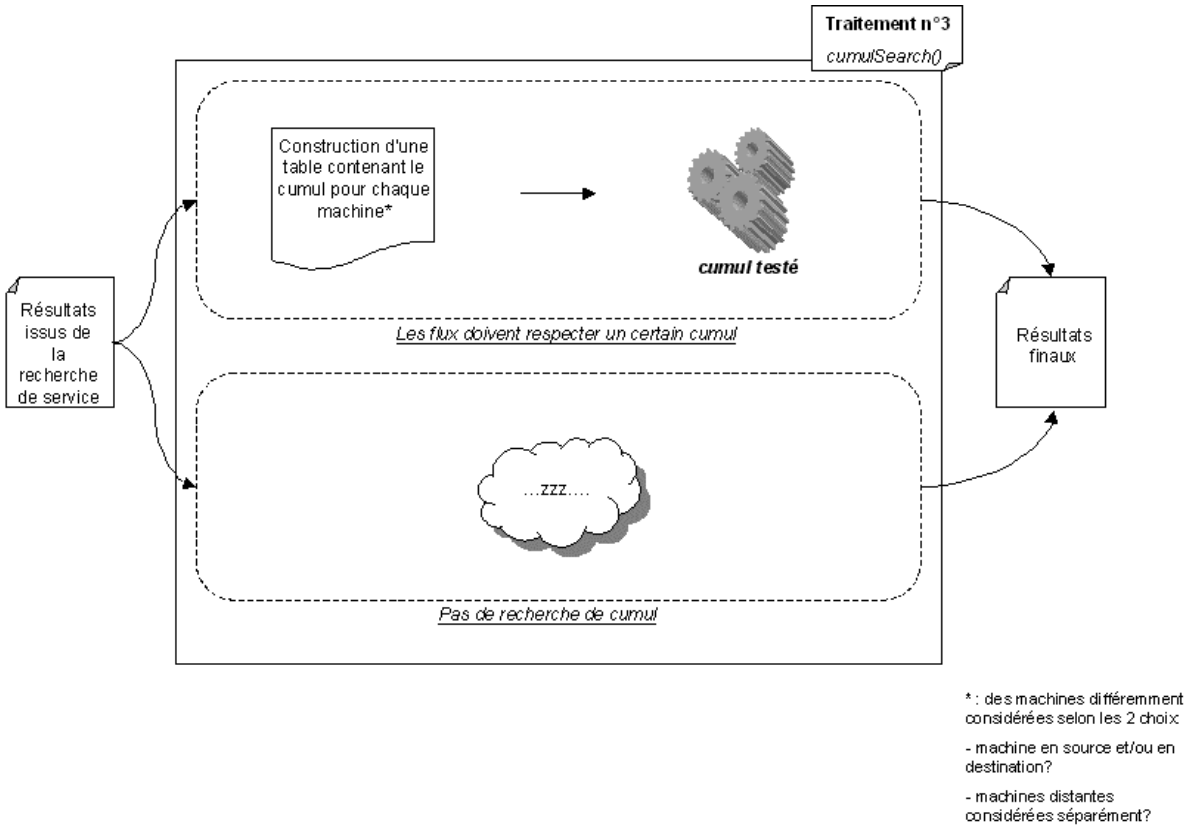
Le tableau ci-dessous indique comment se fait le choix de la clé pour la première table :

Choix des clés suivants les options cochées : *Légende :* ☐ *correspond à la clé choisie;* ↻ *indique qu'il faut inverser l'ordre.*	 Machines distantes considérées globalement	 Machines distantes considérées séparément
A est la source 	[A] B … B A … [A] C … C A …	[A B] … B A … [A C] … C A …
A est la destination 	A B … B [A] … A C … C [A] …	A B … [B↻A] … A C … [C↻A] …
A est la source ou la destination 	A [B] … [B] A … A [C] … [C] A …	[A B] … [B↻A] … [A C] … [C↻A] …
A est la source et B la destination 	[A B] … B A … A C … C A …	[A B] … B A … A C … C A …
On demande les machines en source 	[A] B … [B] A … [A] C … [C] A …	[A B] … [B A] … [A C] … [C A] …
On demande les machines en destination 	A [B] … B [A] … A [C] … C [A] …	[A↻B] … [B↻A] … [A↻C] … [C↻A] …
On demande les machines en source ou en destination 	[A] B … [B] A … [A] C … [C] A … *et* A [B] … B [A] … A [C] … C [A] …	[A B] … [B A] … [A C] … [C A] … *et* [A↻B] … [B↻A] … [A↻C] … [C↻A] …

- Pour ce qui est enfin du cas où un service est spécifié dans une quantité précise, il suffit de combiner les deux précédentes opérations; la seule différence qui existe est que l'on ne contabilise les quantités de service que pour le service recherché, et non pour tous les services. C'est d'ailleurs pour cette raison que le traîtement relatif aux services et aux quantités de service a été fusionné.

La fonction génère un fichier temporaire dans le repertoire "/tmp", qui sera utilisé par la fonction suivante, et qui sera supprimée lorsque la recherche sera achevée.

D. Recherche d'une quantité de trafic



La fonction *"accSearch()"* effectue quant à elle deux types de traîtement :

- elle ne fait rien si aucune demande de recherche sur la quantité totale de trafic n'est formulée;

- si une quantité de trafic est spécifiée, elle effectue des opérations similaires à la partie de la fonction *"serviceSearch()"* chargée de trouver les trafics vérifiant une quantité de service donnée. Elle crée ainsi une table de hachage cette fois-ci simple contenant le cumul des trafics à partir des résultats fournis par l'appel de la fonction *netMETexp* avec l'option *-c (--CUMULaccprint)*.

Le résultat de la fonction est finalement formatée, puis affichée.