

netMET - Network's METrology

Outils et fonctionnalités disponibles

netMET
Alexandre SIMON

*netmet@netmet-solutions.org
Alexandre.Simon@ciril.fr*

- 1 ou n routeurs  :
 - supportant la technologie *NetFlow Cisco*
 - exportant des datagrammes *UDP NetFlow Cisco* vers 1 ou n machine(s) de métrologie *netMET*
- 1 ou n machine(s) de métrologie *netMET* sous Linux :
 - implémentant la distribution netMET (collecteur netMET de datagrammes *NetFlow Cisco* + exploitation netMET pour la métrologie et statistiques)
 - proposant l'accès à ces informations vers le web.

Outils et fonctionnalités disponibles

- 2 voies de développement netMET :
 - le **collecteur** netMET de datagrammes *UDP NetFlow Cisco*
 - l'**exploitation** netMET des informations collectées
- La **distribution** netMET regroupe ces 2 voies de développement, ainsi :
 - le collecteur netMET reste utilisable sans l'exploitation (collecte simple dans des fichiers brutes)
 - l'exploitation ne peut fonctionner qu'avec les données fournies par le collecteur netMET

Distribution netMET

- **Collecteur & Exploitation** netMET
- mise à jour du système
- script et documentation d'installation
- documentation d'aide à l'administration de la station

Collecteur netMET

- duplicateur de datagrammes *UDP NetFlow Cisco*
- collecteur & accounting des datagrammes *UDP NetFlow Cisco*
- transcription et pré-traitement des informations collectées

Exploitation netMET

- traitement & exploitation des informations collectées
- top n par machines
- top n par organismes (ens. @IP et/ou subnet)
- volumétrie par protocole par organismes
- volumétrie par service/protocole par organismes
- statistiques type *MRTG* par organismes
- informations en entrée et sortie (top, volumétrie, ...)
- outil de consultation et recherche sur critères
- détection de scan
- détection de problèmes de sécurité
- publication des rapports sur le Web
- archivage des rapports et données brutes

- Le collecteur netMET propose :
 - un dupicateur de datagrammes *UDP NetFlow Cisco*
 - duplication/répartition de charge vers n collecteur(s), duplication vers collecteur de test, ...
 - un collecteur et accounting des *flows NetFlow Cisco*
 - collecteur : alimenté directement par 1 ou n routeur(s), ou 1 ou n dupicateur(s)
 - accounting : gestion de compteurs selon le "concept" netMET
 - un outil de transcription et pré-traitement des informations collectés
 - transcription binaire/ascii
 - pré-traitement accéléré

- Collecteur générique utilisable pour d'autres problématiques que pour "l'exploitation netMET"

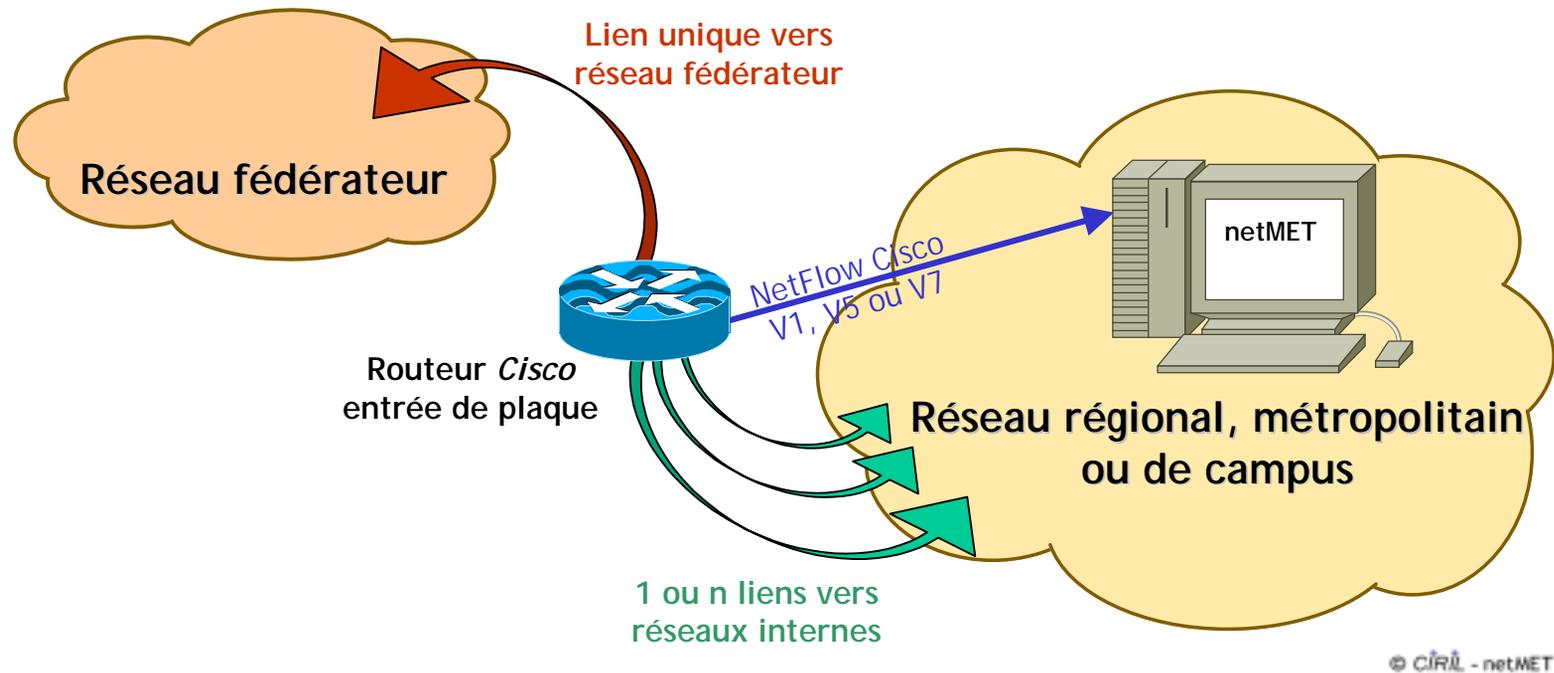
- L'exploitation netMET réalise le traitement et l'exploitation des informations collectées par le collecteur netMET, elle propose :
 - top n par machines
 - top n par organismes (ens. @IP et/ou subnet)
 - volumétrie par protocole par organismes
 - volumétrie par service/protocole par organismes
 - statistiques type *MRTG* par organismes
 - outil de consultation et recherche sur critères
 - détection de scan
 - détection de problèmes de sécurité
 - publication des rapports sur le Web
 - archivage des rapports et données brutes

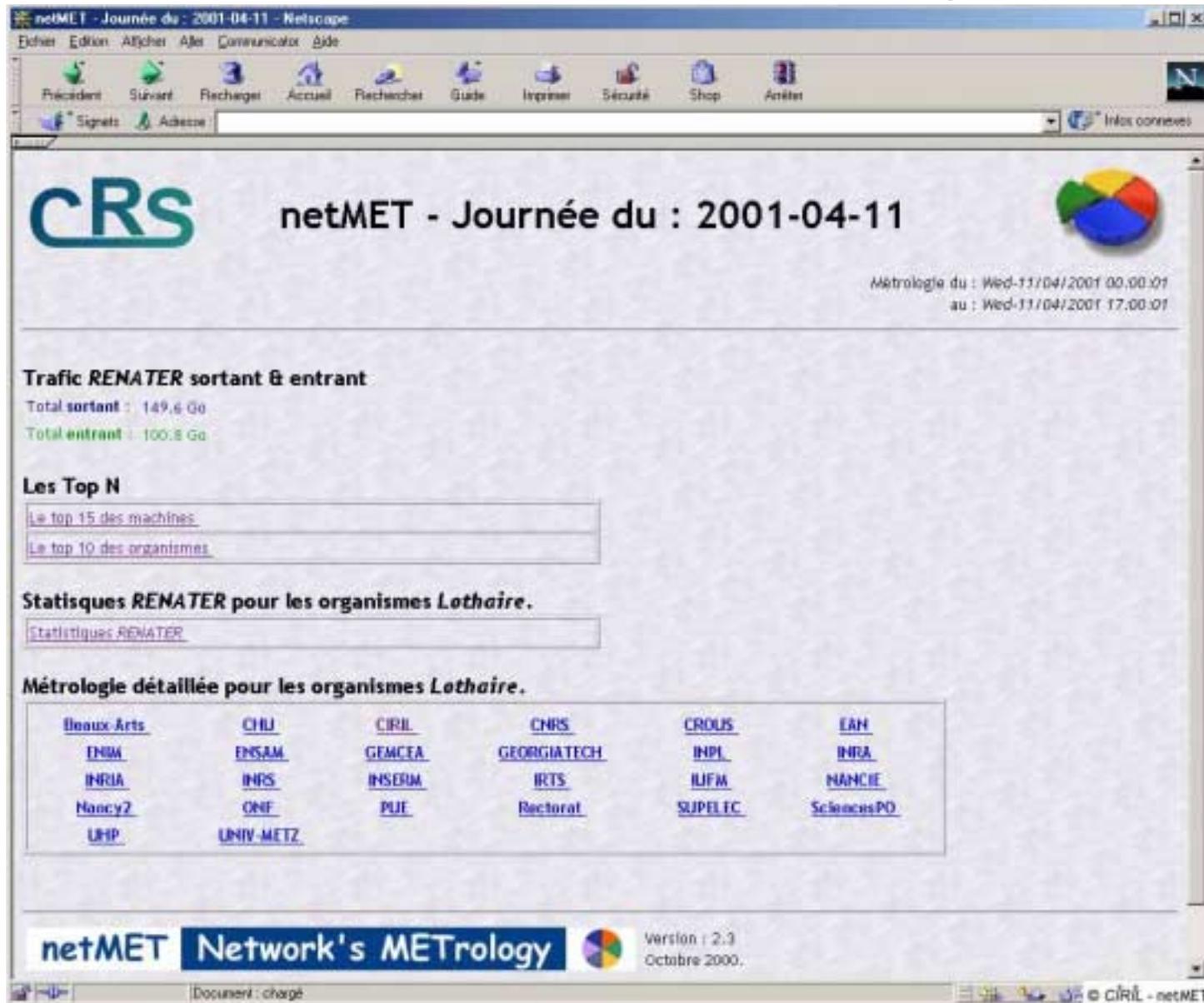
L'exploitation netMET

- L'exploitation netMET est orientée :
 - mesure d'un réseau régional, métropolitain ou de campus vers un réseau fédérateur (Renater par ex.) connecté par un lien unique
 - mais elle peut être facilement dérivée et adaptée pour d'autres problématiques

L'exploitation netMET

- Schéma *typique* d'utilisation de l'exploitation netMET :





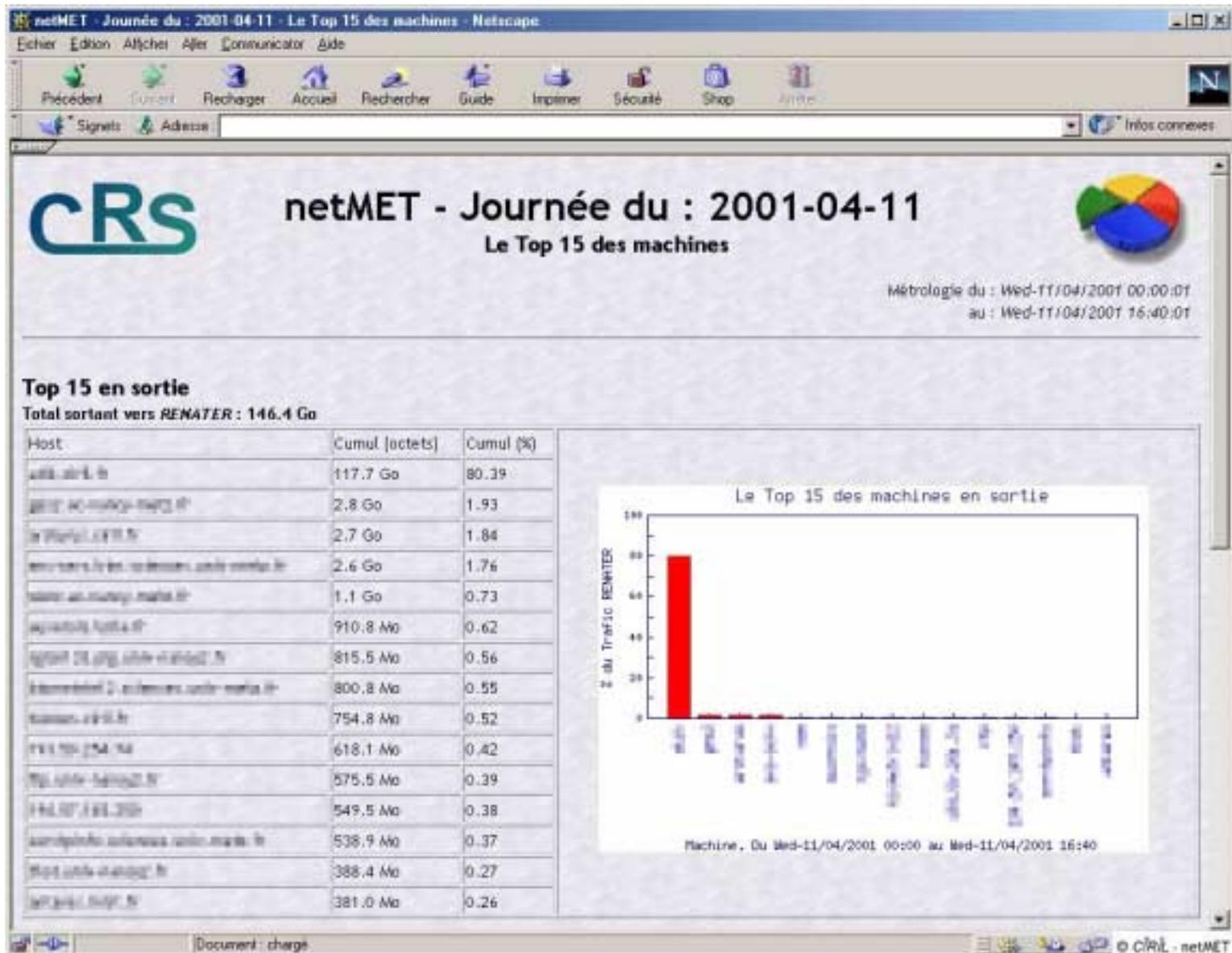
The screenshot shows the netMET web application running in a Netscape browser window. The browser title is "netMET - Journée du : 2001-04-11 - Netscape". The interface includes a menu bar (Fichier, Edition, Affichage, Aller, Communicator, Aide), a toolbar with icons for navigation and actions, and a search bar. The main content area features the "cRS" logo, the title "netMET - Journée du : 2001-04-11", and a date range for metrology data: "Métrologie du : Wed-11/04/2001 00:00:01 au : Wed-11/04/2001 17:00:01".

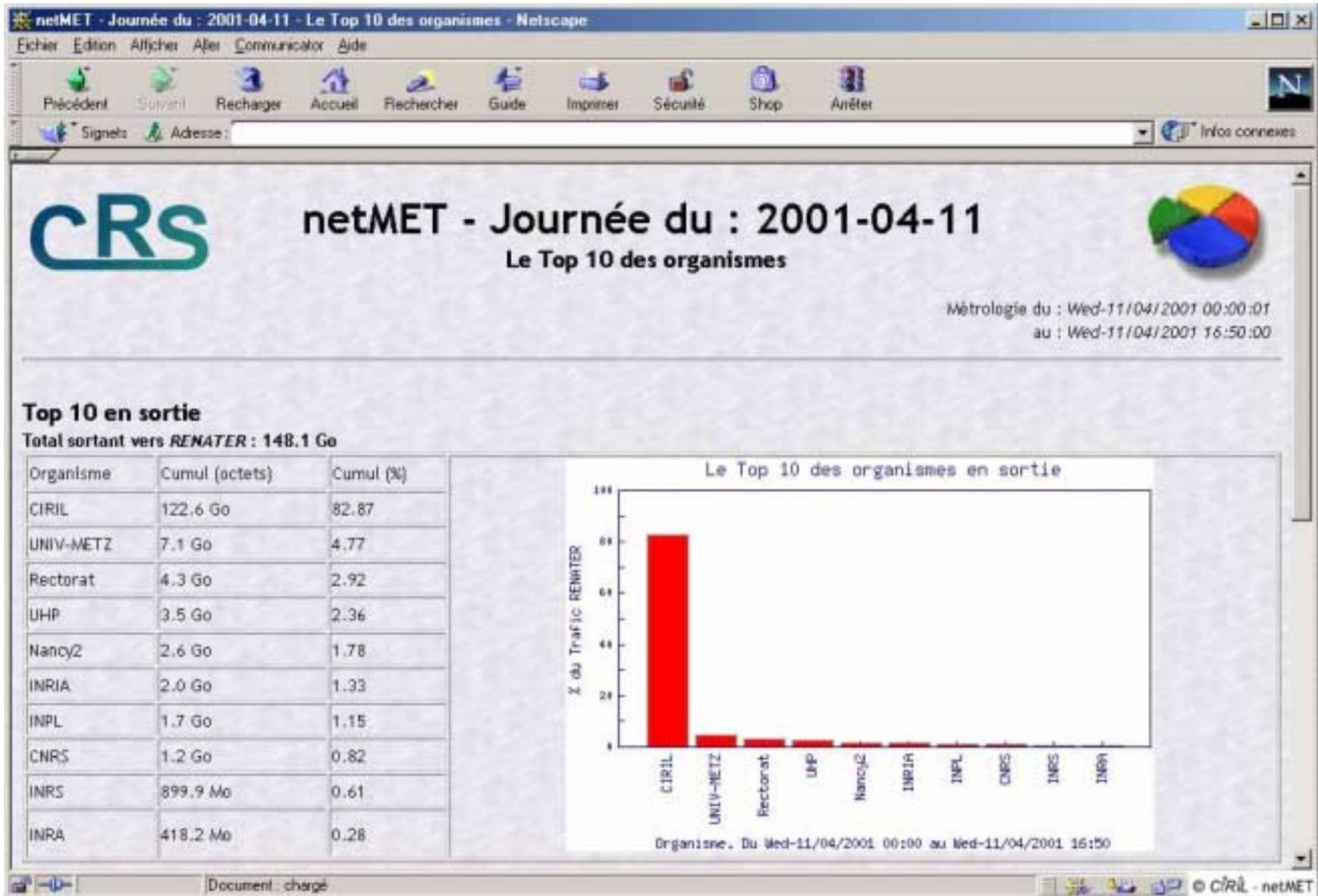
Key sections of the interface include:

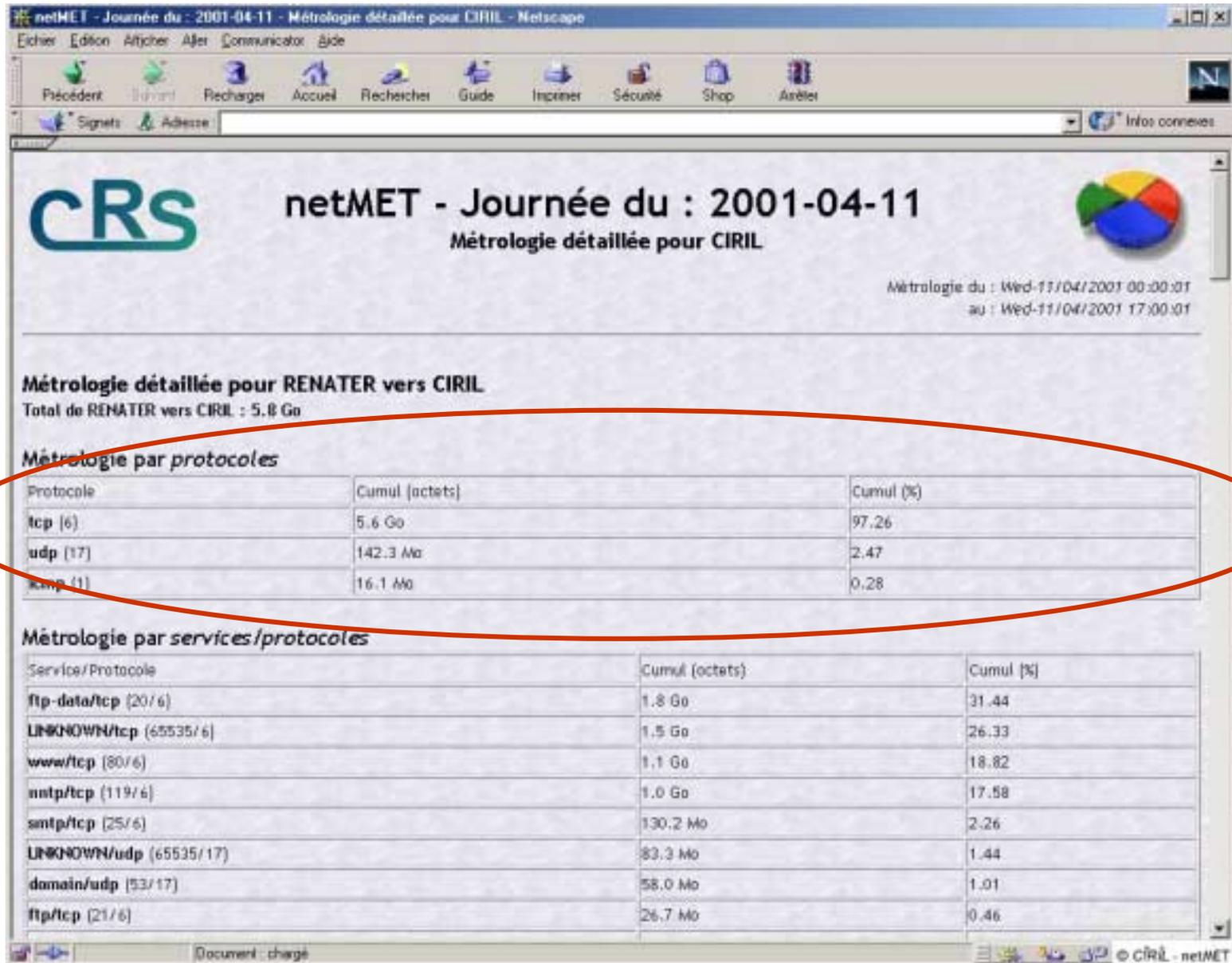
- Trafic RENATER sortant & entrant:**
 - Total sortant : 149,6 Go
 - Total entrant : 100,8 Go
- Les Top N:**
 - [Le top 15 des machines](#)
 - [Le top 10 des organismes](#)
- Statistiques RENATER pour les organismes Lorraine:**
 - [Statistiques RENATER](#)
- Métrieologie détaillée pour les organismes Lorraine:**

Beaux-Arts	CHU	CIRIL	CNRS	CROUS	EAM
ENSM	ENSAM	GEMCEA	GEORGIA TECH	INPL	INRA
INRIA	INRS	INSERM	IRTS	IJFM	NANCIE
Nancy2	ONF	PJE	Rectorat	SUPELEC	SciencesPO
UHP	UNIV-METZ				

The footer contains the netMET logo, the text "Network's METrology", the version "Version : 2.3", the date "Octobre 2000", and a copyright notice "© CIRIL - netMET".







netMET - Journée du : 2001-04-11 - Métrologie détaillée pour CIRIL - Netscape

netMET - Journée du : 2001-04-11
 Métrologie détaillée pour CIRIL

Métrologie du : Wed-11/04/2001 00:00:01
 au : Wed-11/04/2001 17:00:01

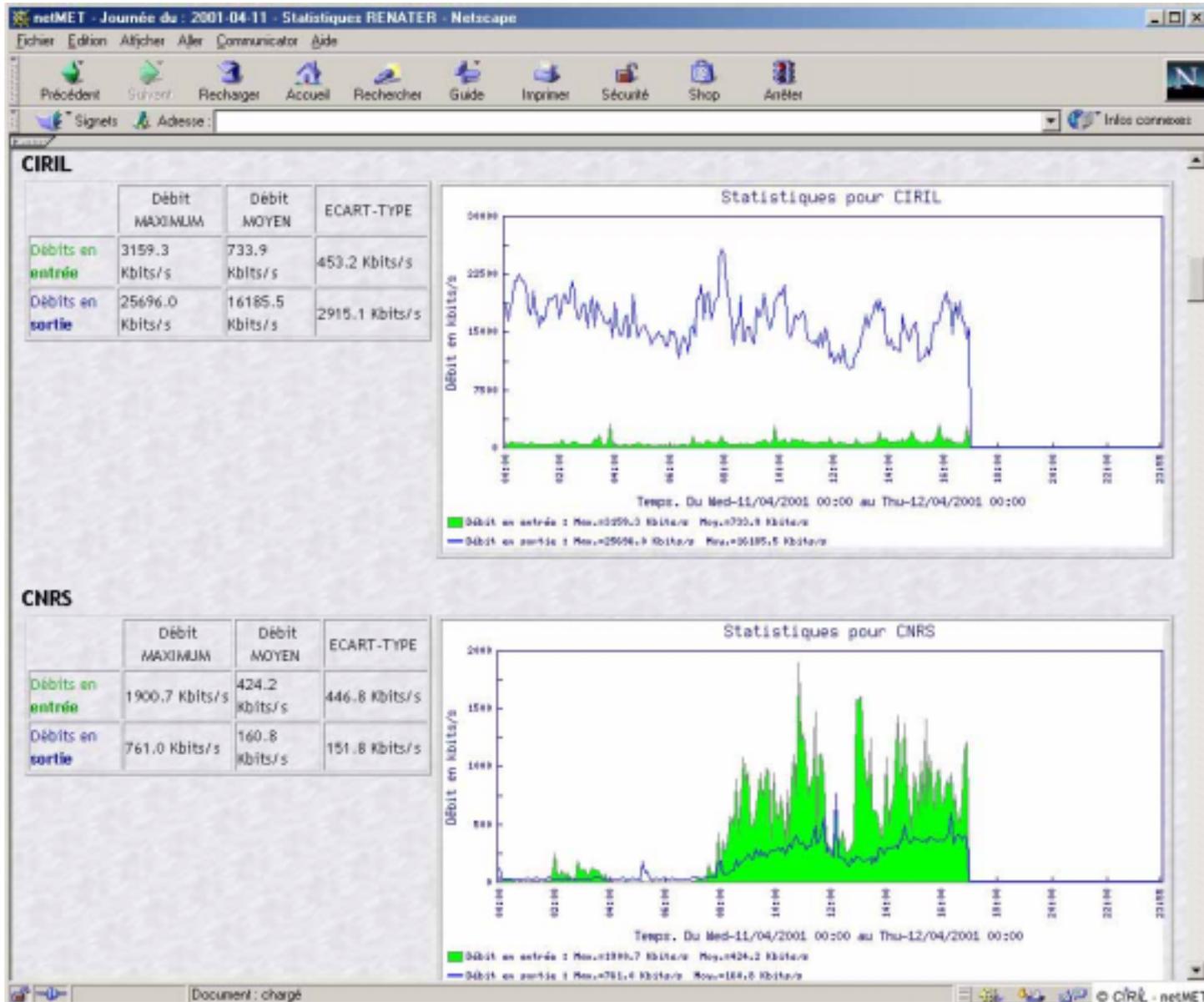
Métrologie détaillée pour RENATER vers CIRIL
 Total de RENATER vers CIRIL : 5.8 Go

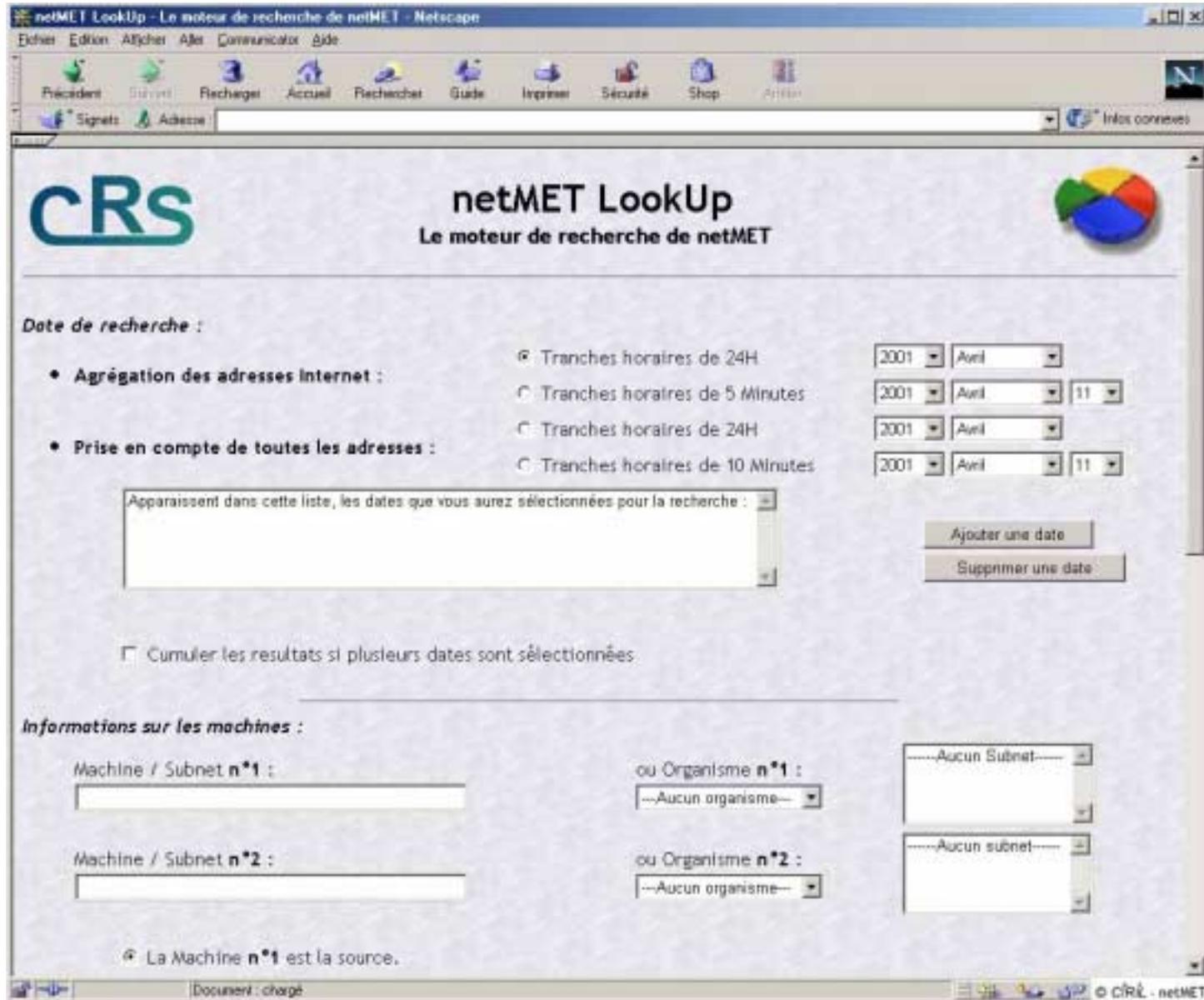
Métrologie par protocoles

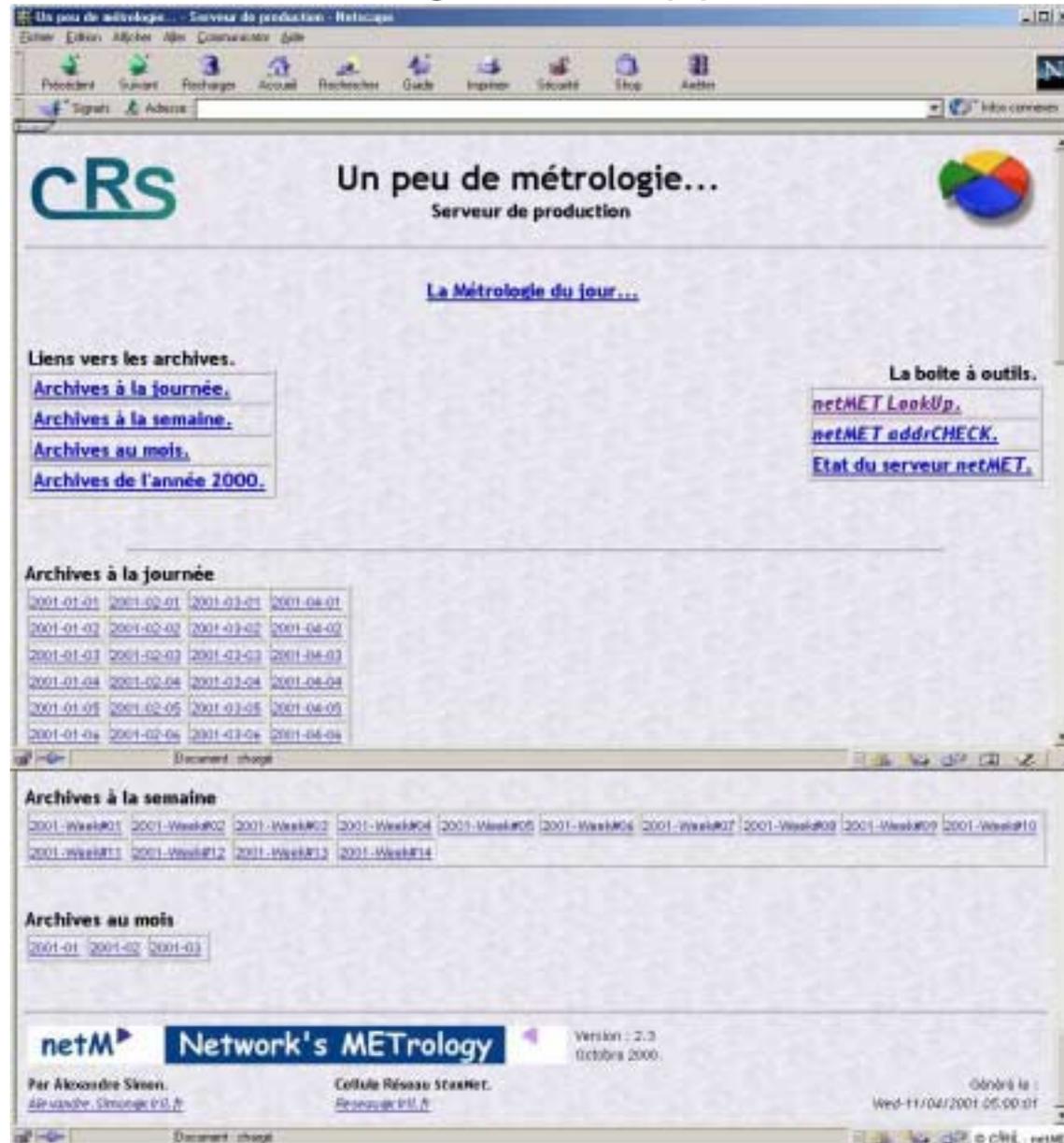
Protocole	Cumul (octets)	Cumul (%)
tcp (6)	5.6 Go	97.26
udp (17)	142.3 Mo	2.47
icmp (1)	16.1 Mo	0.28

Métrologie par services/protocoles

Service/Protocole	Cumul (octets)	Cumul (%)
ftp-data/tcp (20/6)	1.8 Go	31.44
UNKNOWN/tcp (65535/6)	1.5 Go	26.33
www/tcp (80/6)	1.1 Go	18.82
nntp/tcp (119/6)	1.0 Go	17.58
smtp/tcp (25/6)	130.2 Mo	2.26
UNKNOWN/udp (65535/17)	83.3 Mo	1.44
domain/udp (53/17)	58.0 Mo	1.01
ftp/tcp (21/6)	26.7 Mo	0.46







The screenshot shows a web browser window displaying the netMET application. The page title is "Un peu de métrologie... Serveur de production". The main content area is titled "La Métrologie du jour...". Below this, there are two sections: "Liens vers les archives." and "La boîte à outils.". The "Liens vers les archives." section contains four links: "Archives à la journée.", "Archives à la semaine.", "Archives au mois.", and "Archives de l'année 2000.". The "La boîte à outils." section contains three links: "netMET LookUp.", "netMET addrCHECK.", and "Etat du serveur netMET.". Below these sections, there are three tables of links for "Archives à la journée", "Archives à la semaine", and "Archives au mois".

Liens vers les archives.

- [Archives à la journée.](#)
- [Archives à la semaine.](#)
- [Archives au mois.](#)
- [Archives de l'année 2000.](#)

La boîte à outils.

- [netMET LookUp.](#)
- [netMET addrCHECK.](#)
- [Etat du serveur netMET.](#)

Archives à la journée

2001-01-01	2001-02-01	2001-03-01	2001-04-01
2001-01-02	2001-02-02	2001-03-02	2001-04-02
2001-01-03	2001-02-03	2001-03-03	2001-04-03
2001-01-04	2001-02-04	2001-03-04	2001-04-04
2001-01-05	2001-02-05	2001-03-05	2001-04-05
2001-01-06	2001-02-06	2001-03-06	2001-04-06

Archives à la semaine

2001-Week#01	2001-Week#02	2001-Week#03	2001-Week#04	2001-Week#05	2001-Week#06	2001-Week#07	2001-Week#08	2001-Week#09	2001-Week#10
2001-Week#11	2001-Week#12	2001-Week#13	2001-Week#14						

Archives au mois

2001-01	2001-02	2001-03
-------------------------	-------------------------	-------------------------

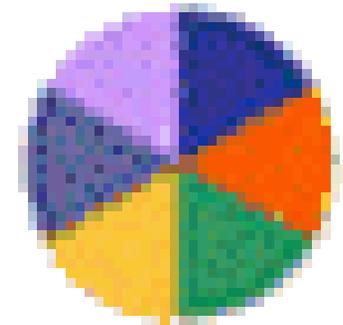
netM Network's METrology Version : 2.3
© octobre 2000.
Par Alexandre Simer. [Site web de Simerologie S.I.S.](#)
Cellule Réseau STANET. [Recherche S.I.S.](#)
Généré le : Wed-11/04/2001 05:00:01

Approche sécurité avec netMET

- L'outil de consultation et recherche sur critères est une première approche sécurité à base de netMET
- Les points
 - détection de scan
 - détection de problèmes de sécuritésont actuellement en développement...

- La **distribution** netMET regroupe le collecteur et l'exploitation netMET pour Linux
 - sous forme d'un package comprenant :
 - des mises à jour du système hôte Linux
 - un ensemble de collecteurs netMET
 - un ensemble de scripts pour l'exploitation
 - fichiers de configuration
 - disponibilité des diverses documentations
 - d'installation de la distribution
 - configuration distribution et exploitation
 - configuration générique du collecteur netMET

netMET



Network's METrology