netMET - Network's METrology

Outils et fonctionnalités disponibles

netMET
Alexandre SIMON

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

Prérequis netMET

- 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

Outils et fonctionnalités disponibles

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

netMET
Network's METrology

Le collecteur netMET

- Le collecteur netMET propose :
  - un duplicateur 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 duplicateur(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

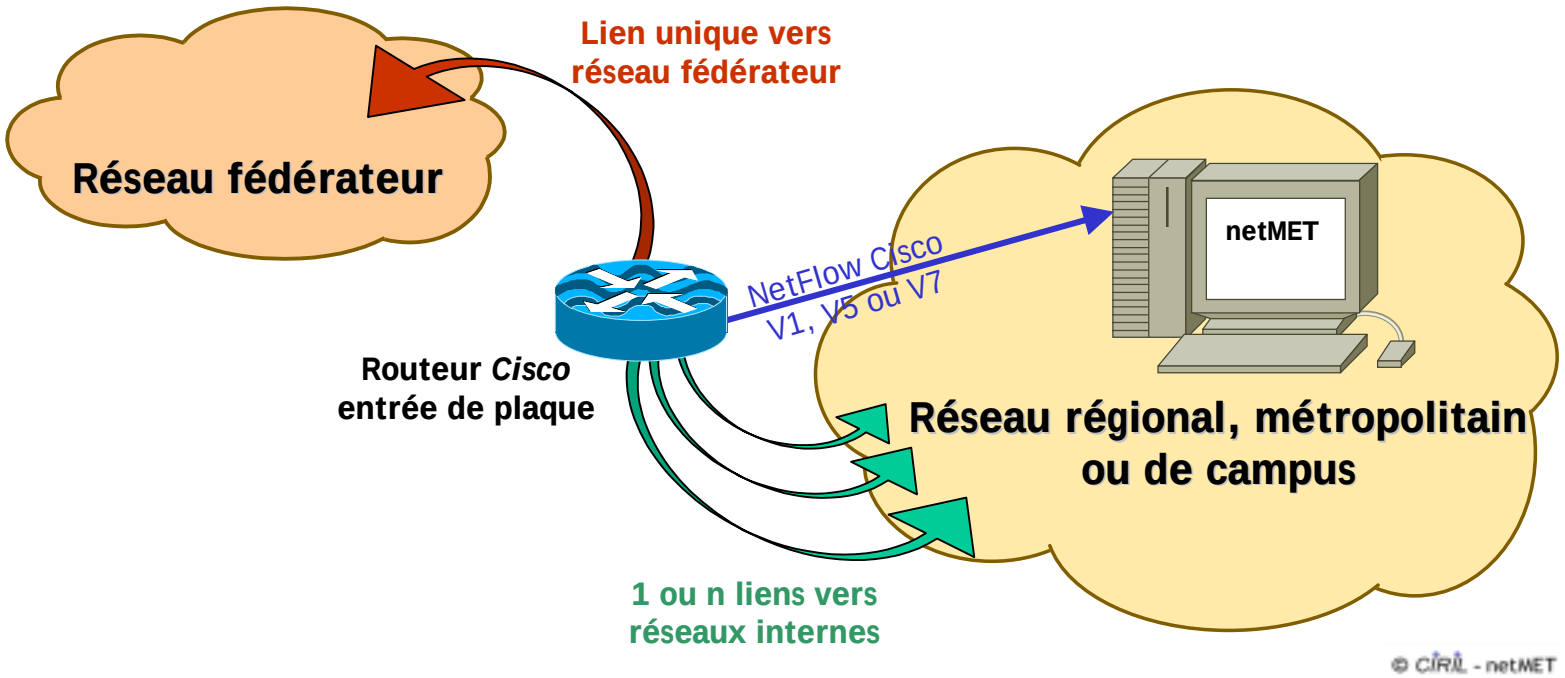
- L'exploitation netMET réalise le traitement et l'exploitation des informations collectées par le collecteur netMET, elle propose :
  - top n par machines
  - top n par organismes (ens. @IP et/ou subnet)
  - volumétrie par protocole par organismes
  - volumétrie par service/protocole par organismes
  - 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

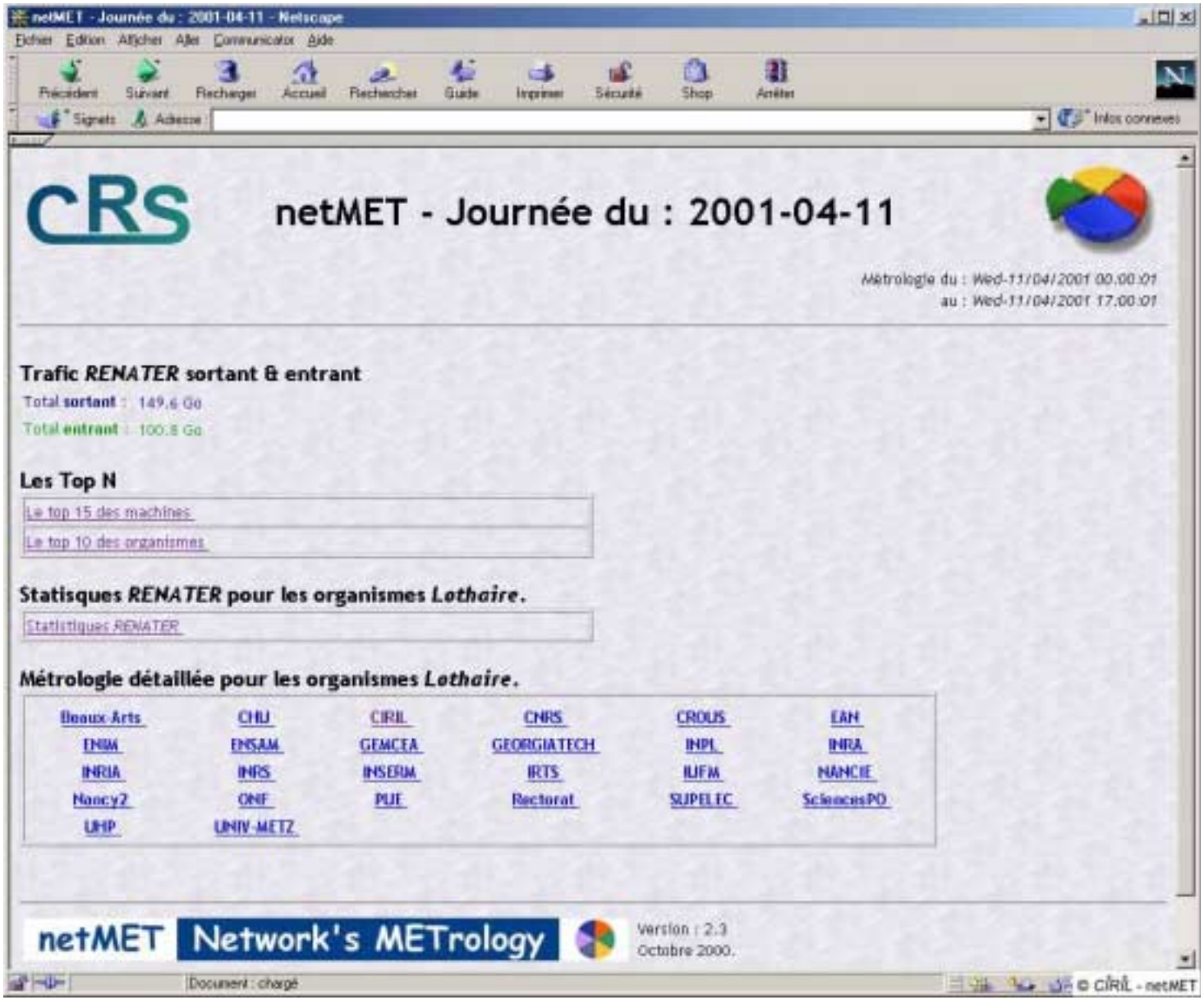
- L'exploitation netMET est orientée :
  - mesure d'un réseau régional, métropolitain ou de campus vers un réseau fédérateur (Renater par ex.) connecté par un lien unique
  - mais elle peut être facilement dérivée et adaptée pour d'autres problématiques

L'exploitation netMET

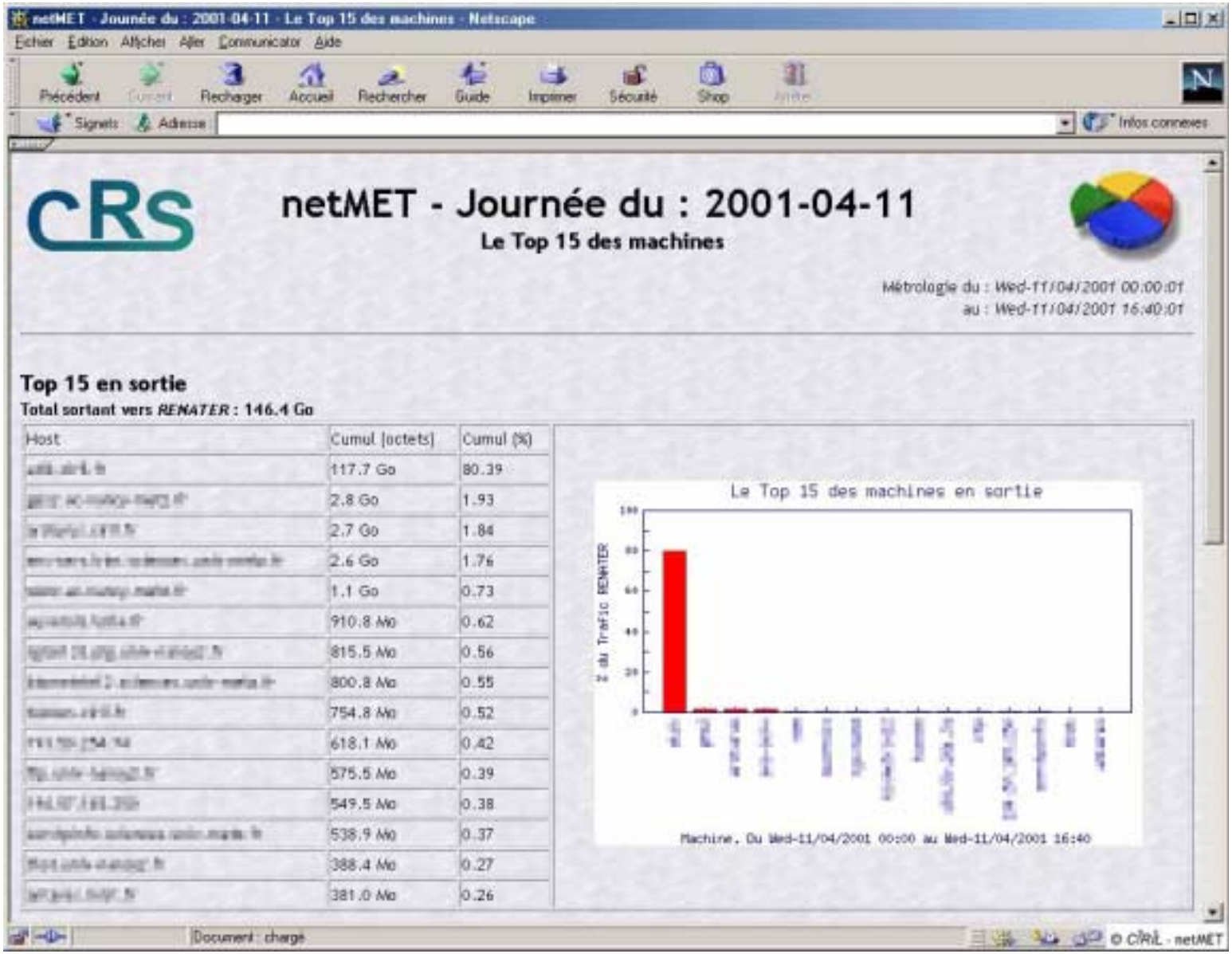
- Schéma *typique* d'utilisation de l'exploitation netMET :



Index de l'exploitation netMET



Top n par machines



Top n par organismes

netMET - Journée du : 2001-04-11 - Le Top 10 des organismes - Netscape

Fichier Edition Afficher Aller Communicator Aide

Précédent Suivant Recharger Accueil Rechercher Guide Imprimer Sécurité Shop Arrêter

Signets Adresse : Infos connexes

netMET - Journée du : 2001-04-11

Le Top 10 des organismes

Métrologie du : *Wed-11/04/2001 00:00:01*
au : *Wed-11/04/2001 16:50:00*

Top 10 en sortie

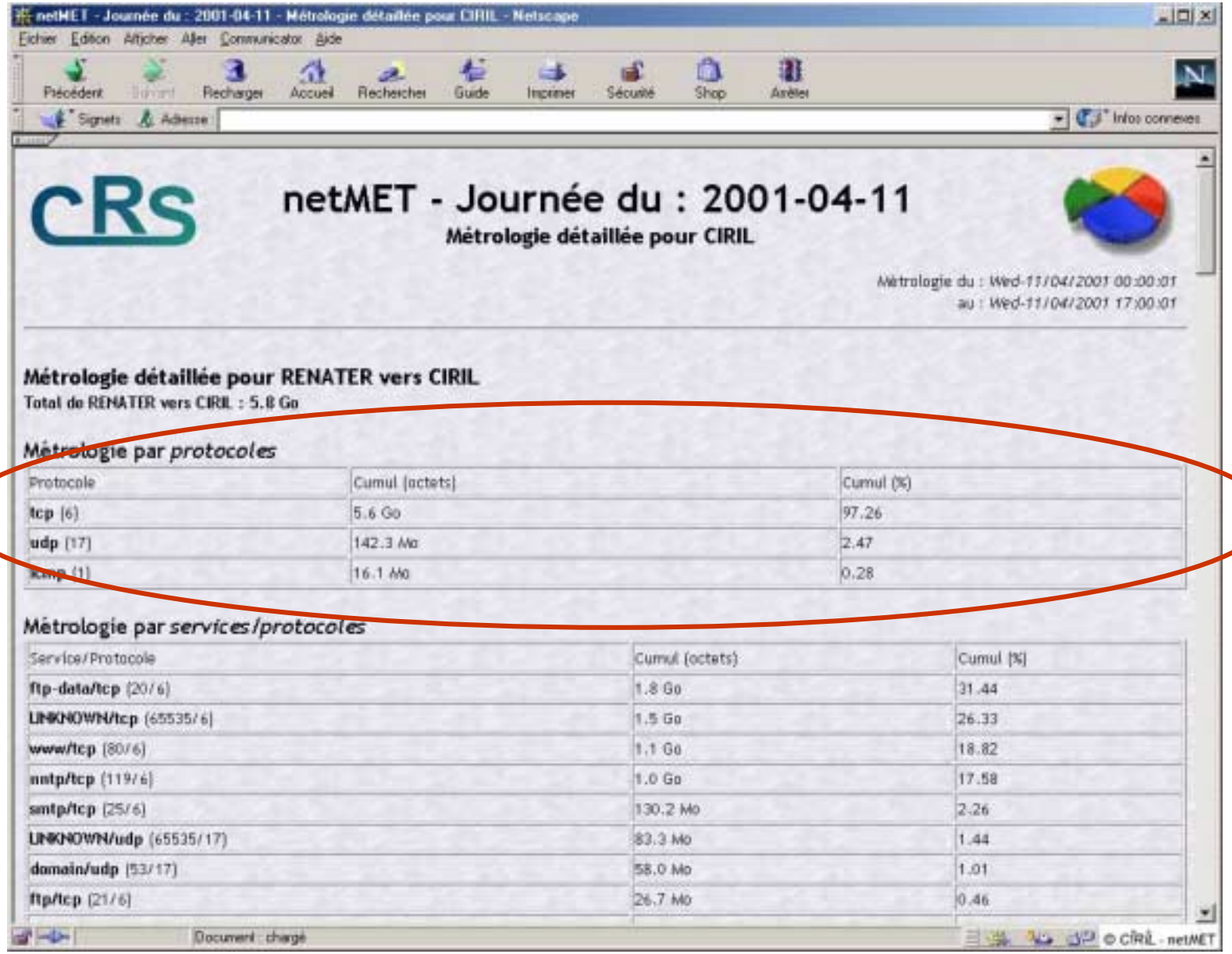
Total sortant vers *RENATER* : 148.1 Go

Organisme	Cumul (octets)	Cumul (%)
CIRIL	122.6 Go	82.87
UNIV-METZ	7.1 Go	4.77
Rectorat	4.3 Go	2.92
UHP	3.5 Go	2.36
Nancy2	2.6 Go	1.78
INRIA	2.0 Go	1.33
INPL	1.7 Go	1.15
CNRS	1.2 Go	0.82
INRS	899.9 Mo	0.61
INRA	418.2 Mo	0.28

Document : chargé

© CIRIL - netMET

Volumétrie par protocole par organismes



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

Fichier Edition Afficher Aller Communicator Aide

Précédent Recharger Accueil Rechercher Guide Imprimer Sécurité Shop Arrêter

Signets Adresse Infos connexes

CRs

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

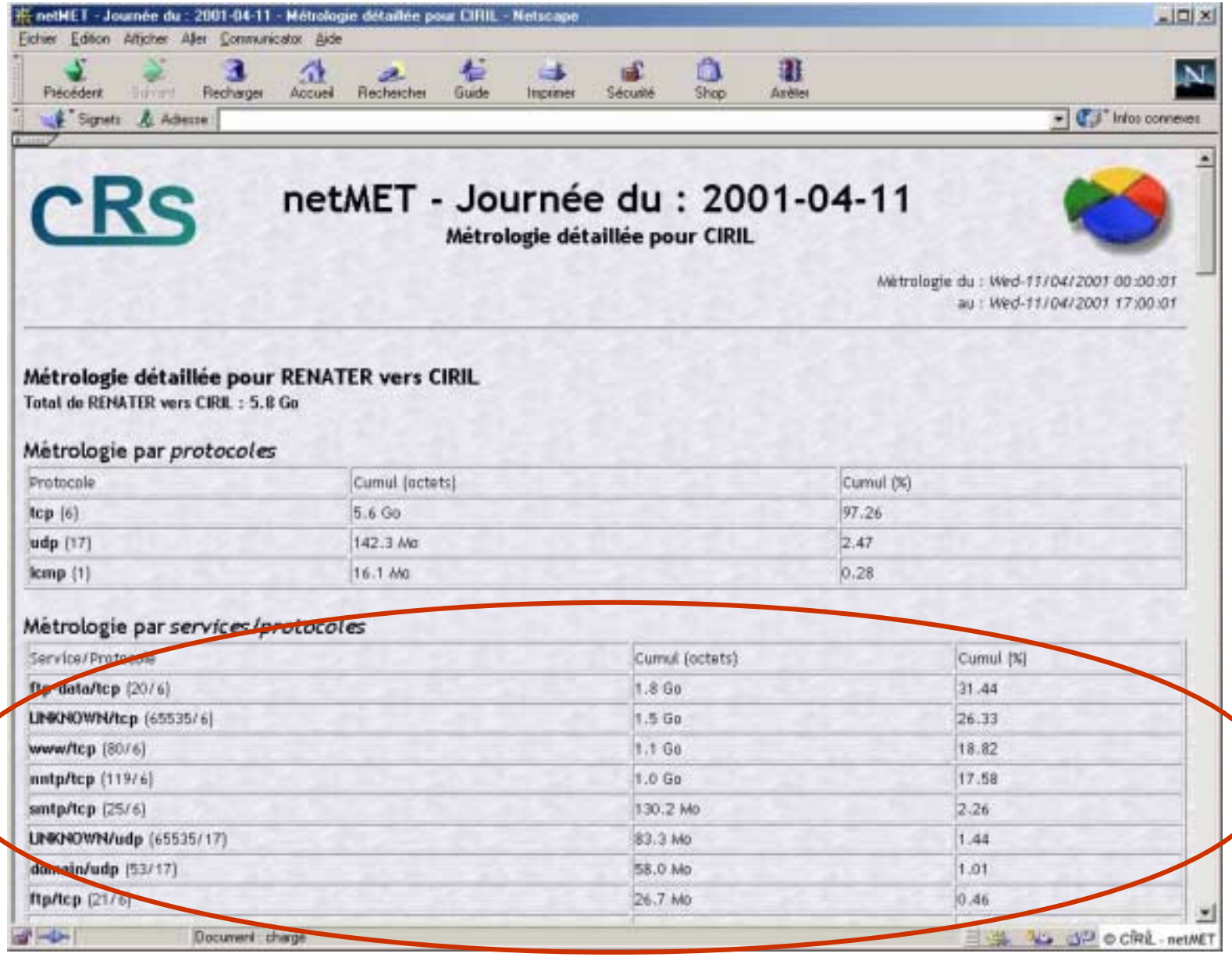
Métrologie par *services/protocoles*

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

Document : chargé

© CIRIL - netMET

Volumétrie par service/protocole par organismes



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

Fichier Edition Afficher Aller Communicator Aide

Précédent Recharger Accueil Rechercher Guide Imprimer Sécurité Shop Arrêter

Signets Adresse Infos connexes

CRs

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

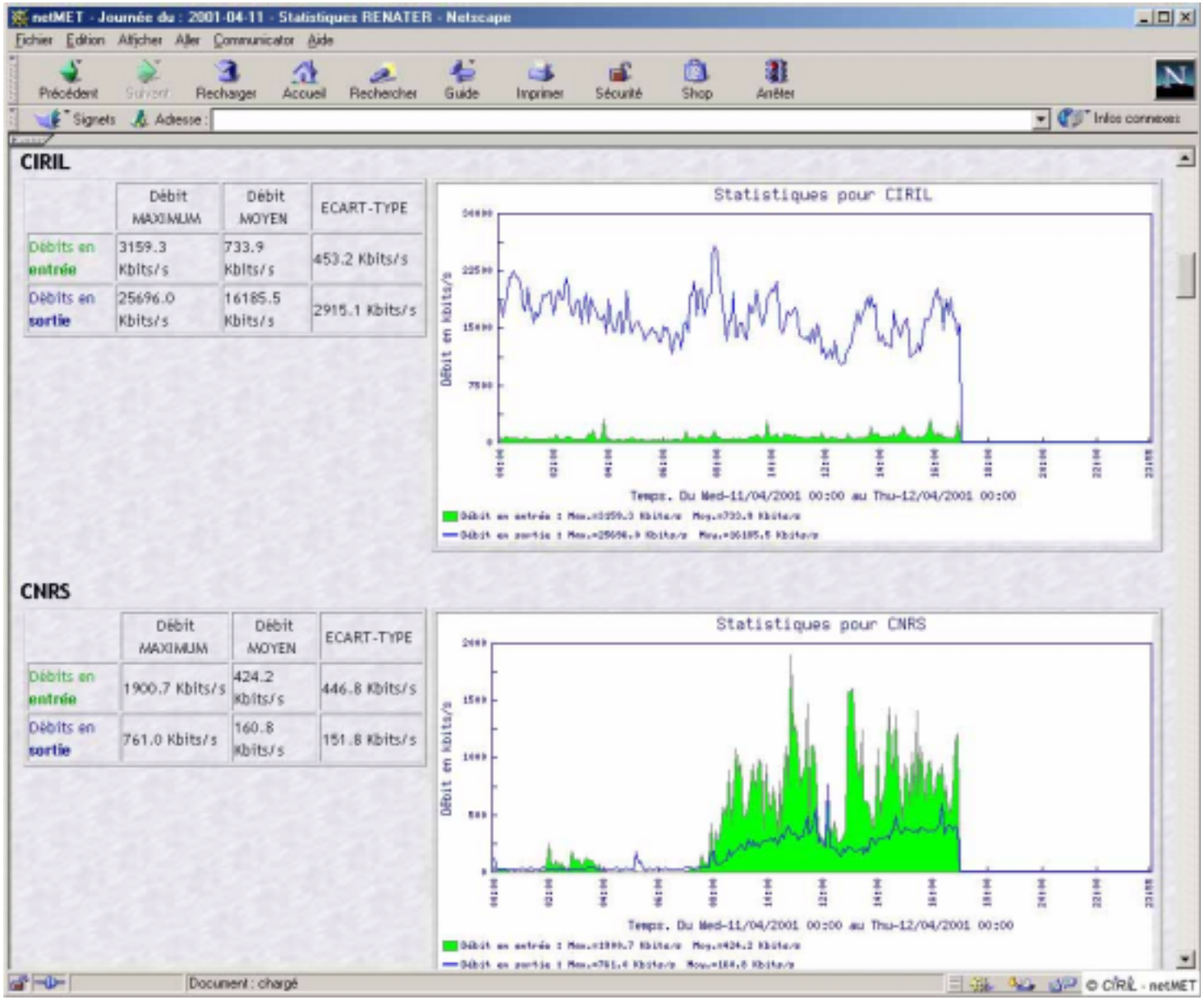
Métrologie par *services/protocoles*

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

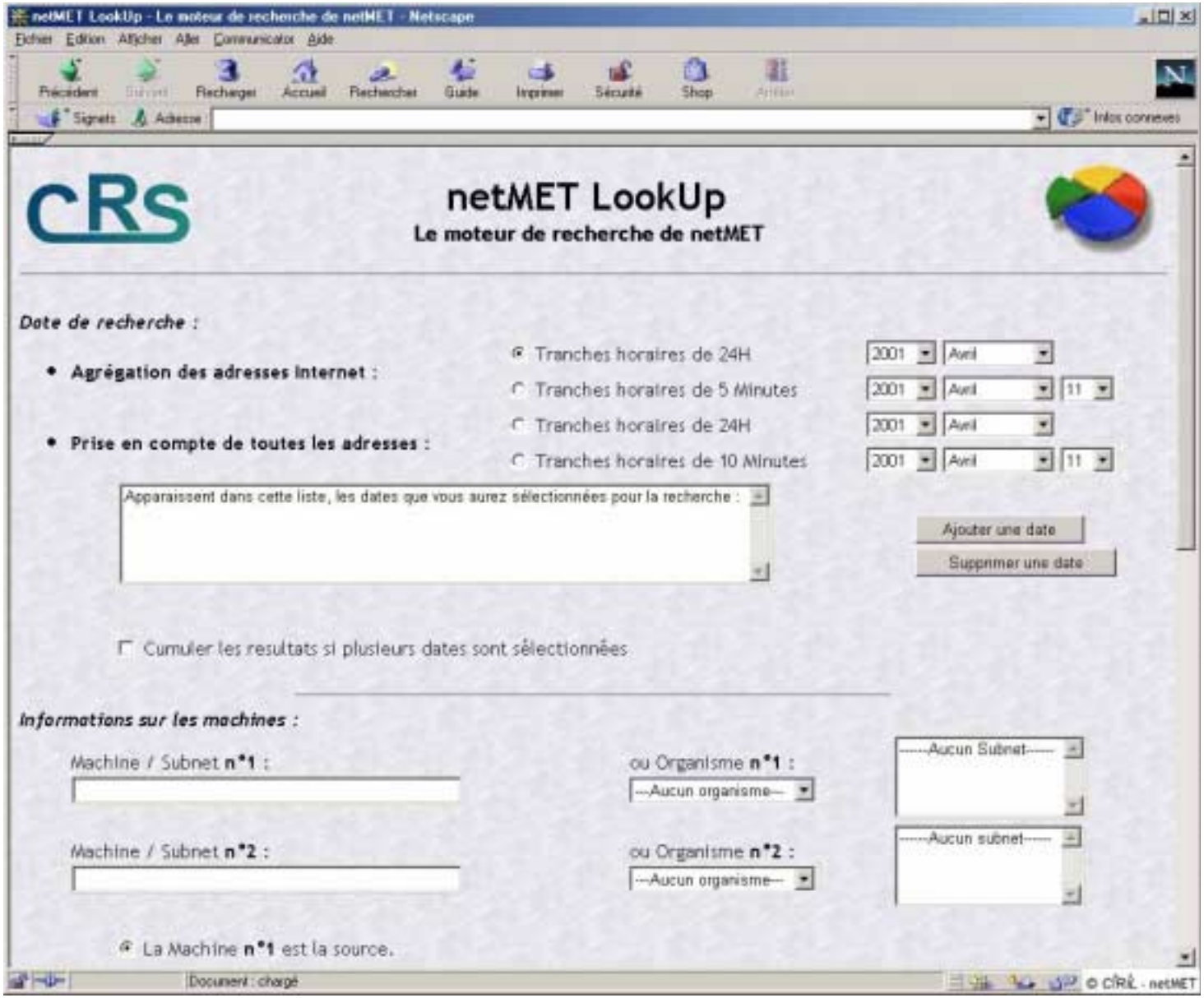
Document : charge

© CIRIL - netMET

Statistiques type *MRTG* par organismes



Outil de consultation et recherche sur critères



Archivage des rapports et données brutes

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 sécurité

  sont actuellement en développement...

La distribution netMET

- 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