Overzicht Ntop (Network Top)

Article · January 2000

CITATIONS
0

READS
10

3 authors, including:

João Paulo A. Almeida
Universidade Federal do Espírito Santo
148 PUBLICATIONS **1,550** CITATIONS
SEE PROFILE

Aiko Pras
University of Twente
247 PUBLICATIONS **2,365** CITATIONS
SEE PROFILE

4.5.1 Overzicht Ntop (Network top)

SAMENVATTING

Netwerkmanagement wordt steeds complexer en de menselijke inspanningen hebben nu geautomatiseerde ondersteuning nodig. De bedoeling van dit artikel is netwerkmanagers en -operators informatie aan te reiken over het gebruik van Ntop. Ntop is een eenvoudig, gratis, en breed inzetbaar instrument voor het meten en observeren van netwerkverkeer. Het ondersteunt diverse beheersactiviteiten, waaronder optimalisatie en planning van het netwerk, en het waarnemen van inbreuken op de beveiliging van het netwerk. Dit artikel geeft een korte beschrijving van het gebruik van Ntop, de installatie en voorbeelden van het gebruik. Alternatieven voor netwerkmonitoring worden ook besproken.

Ntop heeft bewezen waardevol te zijn als eerste stap richting netwerkmonitoring. Het heeft een gemakkelijk te gebruiken geïntegreerde web interface en lage systeemvereisten. Een netwerkmanager kan het gebruiken met een minimale inspanning en kosten voor wat betreft de installatie en opleiding, in tegenstelling tot kostbare en complexe (maar ook geavanceerde en flexibele) managementplatforms.

1 INLEIDING

Netwerkmanagement wordt steeds ingewikkelder door de verschillende netwerktypes en integratie van verschillende netwerkmedia. De kosten van netwerkmanagement nemen toe, naarmate netwerken groter, complexer en heterogener worden. De menselijke inspanningen moeten dan ook worden ondersteund door geautomatiseerde instrumenten, die informatie verzamelen over de toestand en het gedrag van de netwerkelementen. Volgens [Stallings] is netwerkmonitoring het meest fundamentele aspect van geautomatiseerd netwerkmanagement.

Dit artikel is bedoeld als inleiding op het gebruik van Ntop door netwerkmanagers en -operators. Ntop [Ntop] is een eenvoudig, gratis en breed inzetbaar instrument voor het meten en bestuderen van netwerkverkeer. Het werd oorspronkelijk bedacht door Luca Deri en Stefano Suin om problemen met de prestaties van het campusnetwerk van de Universiteit van Pisa in Italië aan te pakken.

De ontwikkelaars hadden een eenvoudig stuk gereedschap nodig om de belangrijkste gebruikers (de *top users*, vandaar Ntop) van het netwerk te bepalen, zodat de hosts die het grootste deel van de netwerk-resources gebruiken snel herkend konden worden. (Wat dit betreft lijkt Ntop op het Unix top-tool, dat informatie levert over het CPU-gebruik door processen.) Ntop werd later ontwikkeld tot een flexibeler en krachtiger instrument [DeriSuin00a, DeriSuin99,

Deri98], op basis van het open source-softwareconcept [OpenSource]. De huidige versie van Ntop heeft zowel command line- als web-gebruikersinterfaces en is beschikbaar voor Unix en Win32 platforms. Ntop concentreert zich op:

- verkeersmeting;
- verkeersmonitoring;
- netwerkoptimalisatie en -planning;
- het waarnemen van inbreuken op de netwerkbeveiliging.

Dit artikel is als volgt opgebouwd: hoofdstuk 2 bespreekt de hierboven genoemde functies nader, hoofdstuk 3 beschrijft de installatie, hoofdstuk 4 geeft een voorbeeld van het gebruik van Ntop, en hoofdstuk 5 behandelt andere opties voor netwerkmonitoring.

2 Functies

2.1 Verkeersmeting

Verkeersmeting omvat het meten van relevante gebruiksactiviteiten. Ntop observeert het gebruik van het netwerk en houdt statistieken bij voor alle hosts op het locale subnetwerk, en voor het subnetwerk als geheel. De benodigde informatie wordt verzameld vanaf de host waar Ntop op draait, door het verkeer op het netwerk te observeren. De verwerking wordt zo verschoven van de operationele nodes naar

Tabel 1
Door Ntop voor iedere host verzamelde informatie

Data sent/received	*Het totale verkeer (volume en aantal packets) van of naar de host. Gesorteerd op het netwerkprotocol (IP, IPX, AppleTalk, enz.) en IP-protocol (FTP, HTTP, NFS, enz.)*
Used bandwidth	*Huidige, gemiddelde en piekbandbreedte.*
IP multicast	*Totaal volume multicast-verkeer verzonden of ontvangen door de host.*
TCP sessions history	*Actieve TCP-sessies die door de host zijn opgezet of geaccepteerd en de bijbehorende verkeersstatistieken.*
UDP traffic	*Totaal volume UDP-verkeer, per poort.*
TCP/UDP used services	*Lijst van op IP gebaseerde diensten (b.v. open en actieve poorten) verleend door de host, met een lijst van de laatste vijf hosts waardoor ze werden gebruikt.*
Traffic distribution	*Lokaal (subnetwerk) verkeer, lokaal vergeleken met remote (buiten het gespecificeerde of lokale subnetwerk), remote vergeleken met lokaal.*
IP traffic distribution	*UDP- en TCP-verkeer, verdeling van de IP-protocollen op basis van de hostnaam.*

de Ntop-host. Alle packets op het subnetwerk worden afgevangen en in verband gebracht met een zender / ontvanger-paar. Zo kan van iedere host alle verkeersactiviteiten worden gevolgd.

Tabel 2 beschrijft de informatie die Ntop voor iedere host bijhoudt.

Ntop levert ook algemene verkeersstatistieken, zoals:

Traffic distribution	*Lokaal (subnetwerk) verkeer, lokaal vergeleken met remote (buiten het gespecificeerde of lokale subnetwerk), remote vergeleken met lokaal.*
Packet distribution	*Totaal aantal packets, gesorteerd op packet size, unicast/multicast/ broadcast, en IP- en niet-IP-verkeer.*
Used bandwidth	*Huidige, gemiddelde en piekbandbreedte.*
Protocol utilisation and distribution	*Verdeling van het geobserveerde verkeer op basis van het protocol en de bron/bestemming (lokaal of remote).*
Local subnet traffic matrix	*Geobserveerd verkeer tussen alle hostparen op subnetwerk.*
Network flows	*Verkeersstatistieken voor een aantal door de netwerkmanager gedefinieerde stromen (verkeer waar de netwerkmanager speciale belangstelling voor heeft).*

TABEL 2
ALGEMENE STATISTIEKEN VERZAMELD DOOR NTOP

Naast de in de tabellen genoemde informatie, kan de huidige versie van Ntop ook worden voorzien van plug-in's, die gedetailleerde statistieken bijhouden over protocollen die niet worden ondersteund door de standaardversie. De NFS en NetBIOS plug-in's zijn hier voorbeelden van.

2.2 Verkeersmonitoring

Verkeersmonitoring is het herkennen van situaties, waarin het netwerkverkeer niet voldoet aan het gestelde beleid (policies) of als het een bepaalde grens overschrijdt. In het algemeen stelt de netwerkmanager het beleid op voor de diverse elementen van het netwerk. Het is echter mogelijk dat sommige hosts zich hier niet aan houden. Vaak zal dit worden veroorzaakt door een onjuiste configuratie van het operating system, netwerk interfaces, applicaties, enzovoort [DeriSuin00a].

Ntop kan helpen bij het onderkennen van sommige netwerkconfiguratieproblemen, zoals:

- Het gebruik van gedupliceerde IP-adressen;
- Lokale hosts in de 'miscuous mode';

- Onjuiste configuratie van applicatiesoftware;
- Misbruik van diensten. Identificeren van hosts die geen gebruik maken van de voorgeschreven proxies;
- Onjuist gebruik van protocollen. Het identificeren van hosts die onnodige protocollen gebruiken;
- Identificeren van subnetwerk-outers. Detecteren van onjuist geconfigureerde werkstations die als routers worden gebruikt;
- Te hoog gebruik van netwerkbandbreedte.

Optimalisatie en planning van het netwerk
Als de hosts niet optimaal zijn geconfigureerd, kan dit een negatief effect hebben op de netwerkprestaties in het algemeen. Met Ntop kan een netwerkmanager potentiële bronnen van onproductief gebruik van bandbreedte herkennen, men name het gebruik van onnodige protocollen en problemen met niet-optimale routing.
Op basis van de aard en verdeling van het verkeer is indirect mogelijk het beleid voor het netwerk te wijzigen, zodat de bandbreedte beter wordt gebruikt.

2.4 Detecteren van inbreuken op de netwerkbeveiliging

In netwerken komen de meeste inbreuken vanuit het netwerk zelf. Ntop voorziet dan ook in mogelijkheden om aanvallen te volgen en om mogelijke zwaktes in de beveiliging op te sporen. Deze mogelijke zwaktes omvatten onder andere: IP spoofing, netwerkkaarten in de promiscuous mode, denial-of-service-aanvallen, Trojan horses (die bekende poorten gebruiken) en port scan-aanvallen.

Nadat er een inbreuk op de beveiliging of een onjuiste configuratie van het netwerk is opgemerkt, kan Ntop worden gebruikt om een alarm te sturen naar de netwerkoperator (via e-mail, SNMP traps of Short Messaging Systems) en om, waar van toepassing, bepaalde acties te ondernemen om de aanval te blokkeren. Ntop wordt ook gebruikt om verkeersinformatie op te slaan in een database.
Deze informatie kan dan worden gebruikt om de aanval te bestuderen en in de toekomst te voorkomen. Voor nadere informatie over het gebruik van Ntop voor beveiliging wordt u verwezen naar [DeriSuin00b]. Men dient er wel rekening mee te houden dat Ntop, net zoals andere monitoringinstrumenten, zelf de beveiliging kan beïnvloeden als het niet juist is geïnstalleerd en geconfigureerd.

3 INSTALLATIE

De huidige versie van Ntop is 1.3. Het wordt gedistribueerd onder de GNU General Public Licence [FSF] en kan gratis worden opgehaald van de officiële homepage van Ntop [Ntop] en andere mirrors op het internet. De platforms, media en protocollen die Ntop ondersteunt staan in Tabel 3.

Platforms	*UNIX, Win32*
Media	*Ethernet, Token Ring, PPP, FDDI, Raw IP, Loopback*
Protocollen	*IP, IPX, NeTBIOS, OSI, AppleTalk, DecNet, DLC*
IP protocollen	*Geheel door de gebruiker instelbaar (NFS, HTTP, X11, DNS, FTP, SMTP, POP, IMAP, SNMP, Telnet, enz.)*

TABEL 3
PLATFORMS, MEDIA EN PROTOCOLLEN, ONDERSTEUND DOOR NTOP

Alvorens de software op te halen, moet u eerst kiezen op welke pc Ntop wordt geïnstalleerd. Deze host moet een interface hebben met het te bewaken netwerk, omdat alleen het verkeer, afgevangen via deze interface, kan worden geanalyseerd. In netwerken met switches of bridges moet u er bij het kiezen van de Ntop-host aan denken, dat alleen het segment waar de host in geïnstalleerd is zal worden bewaakt. Met moderne switches (switching hubs) is het echter mogelijk het gehele netwerkverkeer (of virtuele LAN's) naar een geselecteerde poort van de switch te spiegelen (mirroring). Ntop kan dan draaien op een host die aan een dergelijke poort is gekoppeld. Dit is helaas niet mogelijk bij meerdere LAN's die door middel van routers zijn gekoppeld, bijvoorbeeld in een IP-internetwerk.

Na het kiezen van de pc die als Ntop-host zal dienen, moet het geschikte download-formaat worden gekozen. De volgende formaten zijn beschikbaar:

- Broncode (kan gecompileerd worden op bijna ieder Unix- of Win32-platform);
- Applicatie binary of binary package, voor diverse Unix-versies (Linux, IRIX 6.2, Solaris 2.7 i386/SPARC, HP-UX 11.X, FreeBSD 3.X, AIX 4.1);
- Binary demonstratieversie voor Windows 95/98/Ntop (beperkt tot het afvangen van 1000 packets).

Zowel de Unix- als Win32-versies zijn ontwikkeld op dezelfde basis en hebben de libcap library nodig die ook van de officiële homepage kan worden opgehaald.

Bij Unix moet de Ntop-broncode worden opgehaald en de libcap library worden geïnstalleerd. Ntop moet dan worden gecompileerd en geïnstalleerd:

```
# cd /ntops-directory/ntop-1.3
# sh ./configure
# make
# make install
# exit
```

Als een Ntop-binary is opgehaald hangt de installatieprocedure af van de gebruikte package-manager.

De Win32-versie is gratis beschikbaar als demonstratieprogramma met een beperkte capture-capaciteit. De volledige versie is tegen betaling verkrijgbaar en volledige snapshot-versies zijn beschikbaar op de Ntop FTP-site: ftp://ftp.ntop.org/pub/local/ntop/snapshots/.

Na installatie moet Ntop worden gestart door een gebruiker met super-user-toegang, en zal dan beginnen met het afvangen van de packets op het netwerk. Als Ntop wordt opgestart in de webmode heeft het een interne webserver. Bij het opstarten wordt deze op een bepaalde poort ingesteld. De software kan dan via een web-browser worden gebruikt via URL http://hostname:portnumber/.

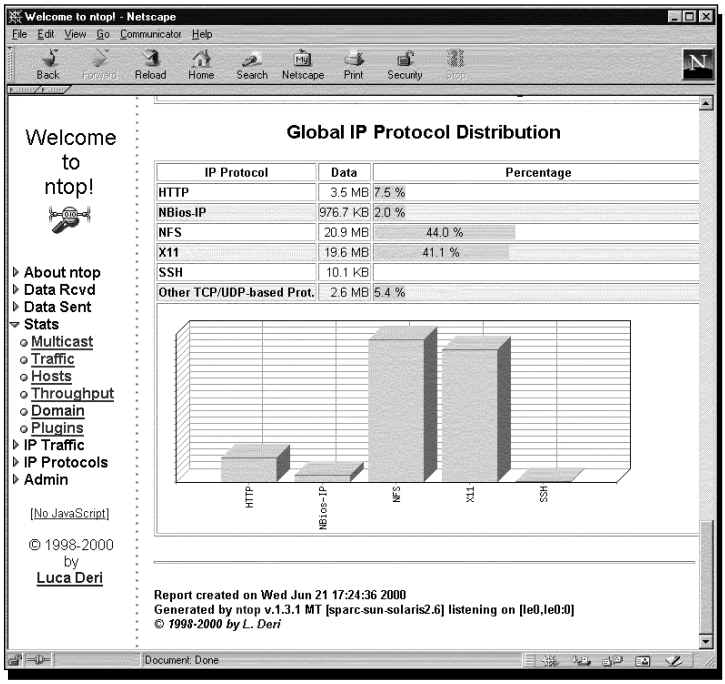
De huidige versie van Ntop ondersteunt plug-ins voor uitbreidingen. De netwerkmanager kan de functionaliteit van Ntop zo uitbreiden. Enkele voorbeelden hiervan zijn ICMP, ARP/RARP en WAP-plug-ins. Deze kunnen naar keuze worden geïnstalleerd en selectief worden gestart tijdens de initialisatie van Ntop.

4 Gebruiksvoorbeelden

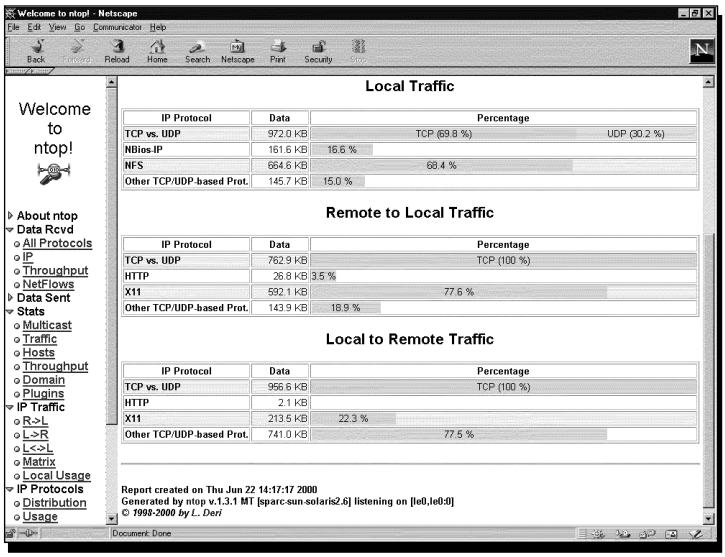
In dit hoofdstuk worden enkele voorbeelden van de mogelijkheden van Ntop gegeven. De onderstaande schermafbeeldingen zijn gebaseerd op de webmode.

De verkeerstatistieken geven algemene informatie over het waargenomen verkeer. Het verkeer wordt in zijn algemeenheid bekeken en er wordt geen informatie weergeven over specifieke hosts. Figuur 1 laat de ‘Global IP Protocol Distribution’-tabel en -grafiek zien. De door Ntop verzamelde gegevens laten zien dat de NFS- en X11-protocollen verantwoordelijk zijn voor het grootste deel van de huidige bandbreedtebezetting van het netwerk. Samen zorgen zij voor 85,1 procent van het verkeer. Deze statistieken zijn van belang voor de netwerkmanager om het verkeer te kunnen begrijpen en in verband te leggen met specifieke applicaties. Zo kan de beschikbare bandbreedte beter worden gebruikt.

De tabellen in figuur 2 geven statistische informatie over lokaal verkeer, verkeer van remote hosts naar de lokale hosts, en van de lokale hosts naar remote hosts. Een host is lokaal als deze hoort bij het opgegeven subnetwerk van de netwerkkaart of het subnetwerk(en)



FIGUUR 1
GEBRUIK VAN DE VERSCHILLENDE IP-PROTOCOLLEN

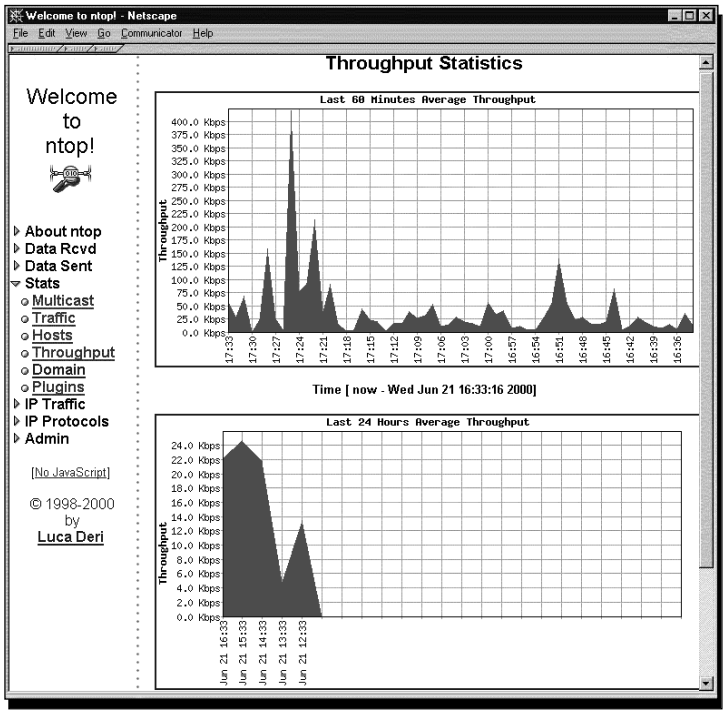


FIGUUR 2
DIVERSE VERKEERSSTATISTIEKEN

wordt opgegeven bij de initialisatie van Ntop [Deri98]. De local traffic-tabel bevat informatie over de data die wordt uitgewisseld tussen de lokale hosts. In dit voorbeeld wordt NFS gebruikt voor 68,4 procent van het lokale verkeer. De remote to local traffic-tabel

betreft het binnenkomende verkeer van remote (niet-lokale) hosts. In dit geval worden er lokale X11-servers gebruikt door hosts buiten het netwerksegment. Met behulp van deze informatie kan de netwerkmanager het beleid over het toegestane remote-gebruik van X-Windows bijstellen. De local-to-remote-tabel betreft het verkeer dat verder gaat dan de het lokale netwerk.

FIGUUR 3
DOORVOERSTATISTIEKEN



Figuur 3 laat de doorvoerstatistieken zien, een andere vorm van algemene verkeersstatistieken. Deze grafieken laten de ontwikkeling zien van de doorvoer door het netwerk. Er zijn verschillende tijdschalen die de doorvoer in de laatste 60 minuten en 24 uur aangegeven. Deze statistieken worden gebruikt om de piek- en dalperioden te bepalen. Hierdoor kan de netwerkmanager activiteiten die veel netwerkverkeer opleveren of het netwerk verstoren (fysiek onderhoud aan het netwerk, configuratie van switches, dataverkeer met een lage prioriteit, enzovoort) beter inplannen. Het is ook de moeite waard onverwachte pieken in de doorvoer te identificeren. Deze kunnen wijzen op een overmatig gebruik van de netwerkresources door een gebruiker of groep gebruikers, of ander afwijkend gedrag.

De voorgaande voorbeelden betroffen het gebruik van Ntop om algemene verkeersinformatie te verzamelen. Figuur 4 laat Ntop-informatie zien voor een afzonderlijke host.

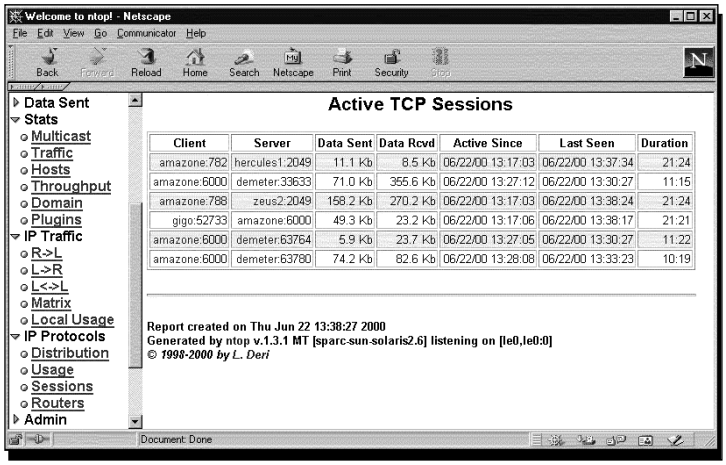
FIGUUR 4
HOST-INFORMATIE

De lijst omvat het IP-adres, MAC -adres en fabrikant van de netwerkkaart (alleen voor lokale hosts), statistieken over de totaal verzonden en ontvangen data (lokaal en remote verkeer), verzonden broadcastpackets, enzovoort. De IP Protocol Distribution-tabel bevat informatie over de diverse protocollen waarbij het IP-verkeer wordt onderverdeeld in de bekende hoog-niveau protocollen. De Last Contacted Peers-tabel bevat de hosts, waar de betreffende host het laatst informatie mee heeft uitgewisseld. De informatie over een host kan een netwerkmanager helpen bij de configuratie en onderhoud van afzonderlijke elementen van het netwerk. Hosts kunnen ook in verband staan met afzonderlijke gebruikers. Deze statistieken kunnen dan informatie geven over hun gedrag.

Ntop kan ook afzonderlijke afgevangen IP-packets analyseren en ze in verband brengen met de actieve TCP-sessies. Dit is mogelijk omdat Ntop de TCP Protocol-Machine implementeert [Deri 98]. Figuur 5 laat de Active TCP Sessions-tabel zien, met informatie over iedere actieve verbinding. Zo kunnen afzonderlijke stromen en hun verkeer worden herkend. De informatie omvat de aangeroepen en aanroepende host-adressen, de verzonden en ontvangen data, verbindingstijd, en lengte van de sessie.

Zoals al besproken in paragraaf 3 kan de functionaliteit van Ntop worden uitgebreid met plug-ins. Figuur 6 laat zien hoe toegang tot

FIGUUR 5
ACTIEVE TCP-SESSIES



FIGUUR 6
DE NTOP WAP-PLUG-IN, INFORMATIE OVER DE TOP RECEIVERS OP EEN WAP-TOESTEL

Ntop wordt verkregen via een WAP-toestel. (Voor dit voorbeeld werd een WAP-emulator [Gelon] gebruikt.) Dit wordt mogelijk gemaakt door de installatie en activatie van een WAP-plug-in [Deri00c], die de presentatie van de statistieken in het WAP-formaat verzorgt.

Figuur 7 laat de interactieve mode van Ntop zien, deze is ook bekend onder de naam Intop. De gegevens worden gepresenteerd in tekstformaat, in de vorm van tabellen. In dit voorbeeld kan de list van hosts die data verzonden of ontvangen hebben worden bekeken. De andere kolommen geven de host-activiteit weer (specifiek de ontvangen en verzonden data), TCP-, UDP- en ICMP-data. Voor een grondige, zij het verouderde, bespreking van de gebruikersinterface van Intop wordt u verwezen naar de *Ntop User Guide* [Deri98].

intop 0.0.1 (May 19 2000) listening on [hme0]
6606 Pkts/770.7 Kb [IP 703.7 Kb/Other 67.1 Kb] Thpt: 211.9 Kbps/349.7 Kbp

Host	Act	-Rcvd-	Sent	TCP	UDP	ICMP
more	B	257.4 Kb	281.9 Kb	256.6 Kb	769	0
zetant	B	204.2 Kb	232.3 Kb	204.2 Kb	0	0
tar	B	42.9 Kb	19.5 Kb	42.9 Kb	0	0
ibook	B	32.7 Kb	4.7 Kb	32.7 Kb	0	0
tecserv	R	791	0	0	595	196
bugnoli	B	602	1.4 Kb	0	602	0
urano	B	496	5.1 Kb	0	496	0
utlrouter	R	98	0	0	0	98
mis	S	0	212	0	0	0
fiorella	S	0	486	0	0	0
piutltst02	S	0	1.4 Kb	0	0	0
mostardi	S	0	952	0	0	0
193.43.104.55	S	0	588	0	0	0
itest1	S	0	928	0	0	0
rolly	S	0	46	0	0	0
itin2	S	0	92	0	0	0
3comhub1	S	0	610	0	0	0
re	S	0	5.6 Kb	0	0	0
pi100	S	0	1.2 Kb	0	0	0
lcardini	S	0	546	0	0	0
mbeng	S	0	602	0	0	0
itest2	S	0	600	0	0	0
fossati-a	S	0	960	0	0	0
hpwsutl	S	0	3.1 Kb	0	0	0
catlc	S	0	120	0	0	0
aut01b	S	0	243	0	0	0
biu	S	0	542	0	0	0
artico2	S	0	226	0	0	0

FIGUUR 7
INTOP - NTOP IN DE INTERACTIEVE TEKST-MODE [DERI98]

5 ANDERE OPTIES VOOR NETWERKMONITORING

Er zijn ook eenvoudige alternatieven voor netwerkmonitoring, zoals packet tracers en decoders, die vaak bekend staan als network sniffers. Enkele voorbeelden hiervan zijn tcpdump [Jacobson et al] en snoop [Sun]. Deze tools zorgen voor het afvangen van de packets op het netwerk. Er is dan vaak een off line analyse-tool nodig voor de correlatie van de data en het bepalen van de netwerkstromen. Sniffers geven meestal informatie over de packet-activiteit, maar niet over het netwerk in zijn geheel [DeriSuin99]. Protocol-analysers, zoals Ethereal [Ethereal], concentreren zich meestal op de inhoud van afzonderlijke packets op het netwerk en niet op de netwerkactiviteit als geheel. Deze oplossingen geven geen ondersteuning op hoog niveau aan de beheersactiviteiten.

Meer geschikte en geavanceerde alternatieven zijn de RMON (Remote Network Monitoring)-platforms [Stallings]. Bij deze platforms worden de probes en managers gescheiden. Probes verzamelen informatie van het netwerk en de managers zijn applicaties, die nuttige informatie op een hoger niveau leveren voor de operator. RMON-managers kunnen worden beschouwd als data analysers maar kunnen de probes ook configureren en de verzamelde gegevens ophalen door middel van SNMP. De flexibiliteit van RMON is gebaseerd op modulariteit en standaardisatie. De MIB (Management Information Base) van RMON is gedefinieerd in RFC's [STD0059].

Aangezien de probes en managers bij RMON niet nauw gekoppeld zijn kan er meer dan één probe per manager zijn. Het is dan ook mogelijk grotere netwerken te analyseren. Bij Ntop zijn de probe en

de analyser nauw gekoppeld en er is dan ook een één-op-één relatie. Daardoor is het niet mogelijk gegevens te analyseren over diverse subnetwerken. De beperkingen van Ntop worden duidelijk als het te bewaken netwerk niet gemonitord kan worden vanuit een enkel punt. Dit is het geval bij concernnetwerken die door routers verbonden zijn, waar Ntop alleen het verkeer van één subnetwerk kan afvangen.

Omdat de RMON-definitie alleen de informatie vastlegt die wordt uitgewisseld tussen probes en managers, is het in principe mogelijk managers uit te breiden met nieuwe specialistische functies, bijvoorbeeld voor het detecteren van inbreuken op de netwerkbeveiliging. Omdat Ntop is ontwikkeld als een complete tool, kunnen specialistische functies alleen worden toegevoegd in nieuwe versies of als optionele plug-in's.

Oplossingen op basis van RMON zijn vaak krachtig maar hebben helaas geavanceerde SNMP-managers nodig die de probes kunnen configureren en voor het analyseren van de verzamelde statistieken over het netwerk. Vanwege de complexiteit en kosten van oplossingen op basis van RMON worden deze voornamelijk gebruikt door ervaren netwerkmanagers bij grote instellingen.

Tools voor netwerkmonitoring zoals NeTraMet [Brownlee] en NFR [Nfr] hebben geavanceerde programmeertalen voor het analyseren van de verkeerstromen op het netwerk en het opslaan van statistische informatie over de gebeurtenissen [DeriSuin99]. Deze talen zijn van belang voor ervaren netwerkmanagers en zijn niet opgenomen in Ntop, ter wille van de eenvoud.

Ntop heeft zichzelf bewezen als een waardevol stuk gereedschap om direct te kunnen beginnen met netwerkmonitoring, met een eenvoudig te gebruiken webinterface, minimale vereisten en beperkt gebruik van de CPU. Het is voor netwerkmanagers beschikbaar tegen minimale kosten en inspanning om het te leren gebruiken en installeren, in tegenstelling tot de kostbare en complexe, maar ook geavanceerde en flexibele, managementplatforms.

LITERATUUR

[Stallings] Stallings, *W. SNMP, SNMPv2, SNMPv2 and RMON 1 and 2*, Third Edition, Addison Wesley, Sept. 1999.

[ntop] Deri, L., Suin, S. and Carbone, R. *Ntop - Network Top*, beschikbaar op: http://www.ntop.org/

[DeriSuin00a] Deri, L. and Suin, S., 'Effective Traffic Measurement using ntop', In: *IEEE Communications Magazine*, 38(5), pp 138-145, May 2000.

[DeriSuin99] Deri, L. and Suin, S., 'Ntop: beyond Ping and Traceroute'. In*: Proceedings of the DSOM'99*, Zürich, Switzerland, October 1999.

[Deri98] Deri, L. *NTOP User's Guide - Network Usage Monitor for Unix Systems*, Centro Serra, University of Pisa, Italy. Beschikbaar op:
ftp://ftp.unipi.it/pub/local/ntop/snapshots/NTOP.pdf.gz
[OpenSource] *The Open Source Page.* Beschikbaar op: http://www.opensource.org/
[DeriSuin00b] Deri, L. and Suin, S., 'Improving Network Security Using Ntop'. In*: Proceedings of the RAID 2000 - Workshop on the Recent Advances in Intrusion Detection*, Toulouse, France, verschijnt oktober 2000.
[STD0059] Waldbusser, S., *Remote Network Monitoring Management Information Base*, IETF STD 0059, May 2000.
[FSF] Free Software Foundation, *GNU General Public License*. Beschikbaar op:
http://www.gnu.org/copyleft/gpl.html
[Deri00c] Deri, L. *Beyond the Web: Mobile WAP-based Management*, Centro Serra, University of Pisa, Italy. Beschikbaar op: http://jake.unipi.it/~deri/WAP.pdf.gz
[Jacobson et al] Jacobson, V., Leres, C., and McCanne, S. *tcpdump*, Lawrence Berkeley National Labs, Beschikbaar op: ftp://ftp.ee.lbl.gov/
[Sun] Sun Microsystems, Inc. *Snoop UNIX man pages (SunOS 5.6).*
[Ethereal] Combs, G. et al. *The Ethereal Network Analyzer*, beschikbaar op:
http://ethereal.zing.org/
[Brownlee] Brownlee N. *NeTraMet 4.2 Users' Guide*, Information Technology Systems & Services, The University of Auckland, New Zealand, August 1998.
Available at http://www.auckland.ac.nz/net/Accounting/usguide.pdf
[Nfr] Network Flight Recorder, Inc. *Network Flight Recorder*. Beschikbaar op:
http://www.nfr.net

OVER DE AUTEURS:
Joao Paulo Andrade Almeida en Yohannes Ramlie volgen de internationale M.Sc. telematica-opleiding aan de Universiteit Twente (UT). Aiko Pras is senior researcher bij het Centrum voor Telematica en Informatie Technology (CTIT) van de UT.

Het artikel is vertaald uit het Engels door Hans van Bemmelen.