Verkon analysointi – kuunteluohjelma Ethereal

Sisällys

1 Johdanto

Ethereal- ohjelmalla voi selata verkon liikennettä eli se on nk. "snifferi" Unixille ja Unixin kaltaisille käyttöjärjestelmille. Etherealilla antaa hyödyllistä tietoa verkon tapahtumista ja sen avulla on helppo oppia käytännössä tietoliikenteen perusteita, erityisesti protokollista sekä kehyksistä.

Tämä tutkielma on tehty harjoitustyönä Liisa Marttisen keväällä 2001 luennoimalle Tietoliikenne II –kurssille Tietojenkäsittelytieteen laitoksella. Tätä työtä ei ole tarkoitettu jaettavaksi kurssin ulkopuolelle. Kirjoittaja ei ota vastuuta lukijan mahdollisesta omatoimisesta ohjelman käytöstä tai siihen opastamisesta.

Koska ohjelmaa voi käyttää myös tietomurtojen apuvälineenä, sen käyttöön on pyydettävä lupa verkon ylläpitäjältä. Ota huomioon, että ilman lupaa käytettynä Etherealin käyttö voi johtaa oikeudellisiin toimiin.

Lisäoppia verkon kuuntelusta löytyy internetistä ja kurssikirjojen lisäksi esimerkiksi Esa Kerttulan kirjasta Tietoverkkojen tietoturva [Ker98].

2 Ohjelman käyttötarkoitus

Ethereal on verkkoprotokollien analysointiohjelma [Eth01]. Etherealilla on mahdollista testata verkon turva-aukkoja, napata tietoa kuten käyttäjätunnuksia, salasanoja, käytettyjä protokollia ja minkä tyyppistä tietoa verkossa kulkee ja minkä verran. Analysointi on suhteellisen yksinkertaista jo Tietoliikenne I-kurssin käyneille.

Ethereal mahdollistaa pakettien selaamisen reaaliaikaisesti verkosta. Katselu tapahtuu sieppaustiedostosta (capture), johon on talletettu tapahtumat. Etherealille ei tarvitse määritellä, minkä tyyppistä tiedostoa luetaan, koska se osaa itse päätellä tiedostomuodon. Tiedot napataan avonaisesta verkkoyhteydestä.

Ethereal on yksi monipuolisimmista verkon kuunteluohjelmista (beta –ohjelma), joka on käyttökelpoinen jo nyt. Se ei ole täydellinen, mutta virheitä korjataan ja uusiin versioihin lisätään ominaisuuksia koko ajan. Ethereal on Open Source –ohjelmisto, joka on julkaistu GNU:n (General Public License [GNU01]) luvalla. Käyttäjä joutuu luopumaan oikeuksistaan (ns. Disclaimer-ehto), koska ohjelman kehittäjät eivät – tietenkään - anna tuotteeseen minkäänlaista takuuta, ei eksplisiittistä tai implisiittistä. Ohjelmaa voi käyttää vain omalla vastuulla.

Wiretap-kirjaston avulla Ethereal voi lukea useita tiedostotyyppejä. Ethereal pystyy lukemaan siepattua tietoa seuraavilta :

- tcpdump (libpcap, Ethernet)
- NAI's Sniffer (compressed and uncompressed)
- Sniffer Pro
- NetXray
- Snoop, Atmsnoop
- LANalyzer
- Shomiti
- AIX's iptrace
- MS Network Monitor
- Novell's LanAlyzer
- RADCOM's WAN/LAN Analyzer
- HP-UX nettl, ISDN4BSD "i4btrace" utility
- Cisco Secure Intrustion Detection System iplogging sekä
- the pppd-okit (pppdump-muotoiset tiedostot)

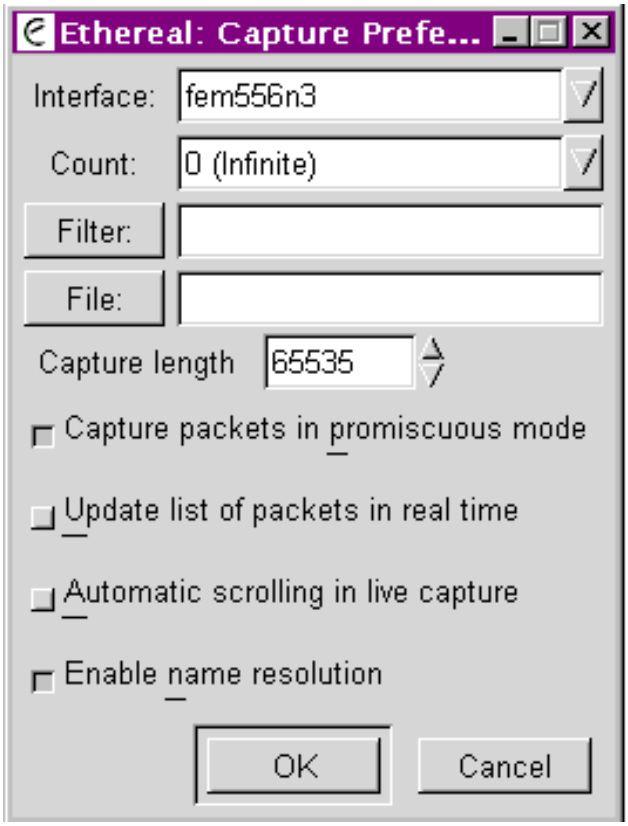
Ethereal voi seurata jälkiä myös Lucent/Ascend (access) WAN reitittimistä ja Toshiban ISDN-reitittimistä. Mikä tahansa näistä tiedostoista voidaan kompressoida gzipillä ja Ethereal purkaa ne lennosta.

Reaaliaikaista dataa voi lukea Ethernet-, FDDI-, PPP-, Token-ring-, X.25- tai Classical IP-verkoista ATM-rajapinnan (Asynchronous Transfer Mode) kautta. Siepattua verkon tietoa voi selata GUI- (Graphical User Interface) tai TTY-muodossa (Teletype) Tethereal –ohjelman avulla (Etherealin ’sisarohjelma’ [Tet01]). Sieppaustiedostoja voi ohjelmoimalla muuttaa tai konvertoida komentorivin kautta Editcap-ohjelmalla [Edi01].

Etherealin tulospääikkuna näyttää kolme näkymää paketeista: yhteenvetorivi kuvaa lyhyesti, mikä paketti on. Protokollapuu antaa näkyviin protokollan tai kentän, josta käyttäjä on kiinnostunut. Hexadesimaali-dumppi näyttää tarkasti, miltä paketti näyttää kun se menee verkossa. Verrattuna muihin verkon analysointiohjelmiin Etherealilla on paljon muokattavia filttereitä. Lisäksi Ethereal osaa koota paketit TCP kommunikoinnista ja näyttää ne ASCII:na.

3 Mitä ohjelmalla voi tehdä

Paketin jäljittämiseen on tehty apuvälineeksi mahdollisuus suodattaa lopputuloksiin vain tiettyjä protokollia. Tämä vaikuttaa lopputulosrivien määrään. Filtteröinnillä (ks. kaavio 3.1) voi protokollan kenttiä verrata tiettyyn haluttuun arvoon, kenttiä keskenään tai tarkistaa tiettyjen kenttien tai protokollien olemassaolo.



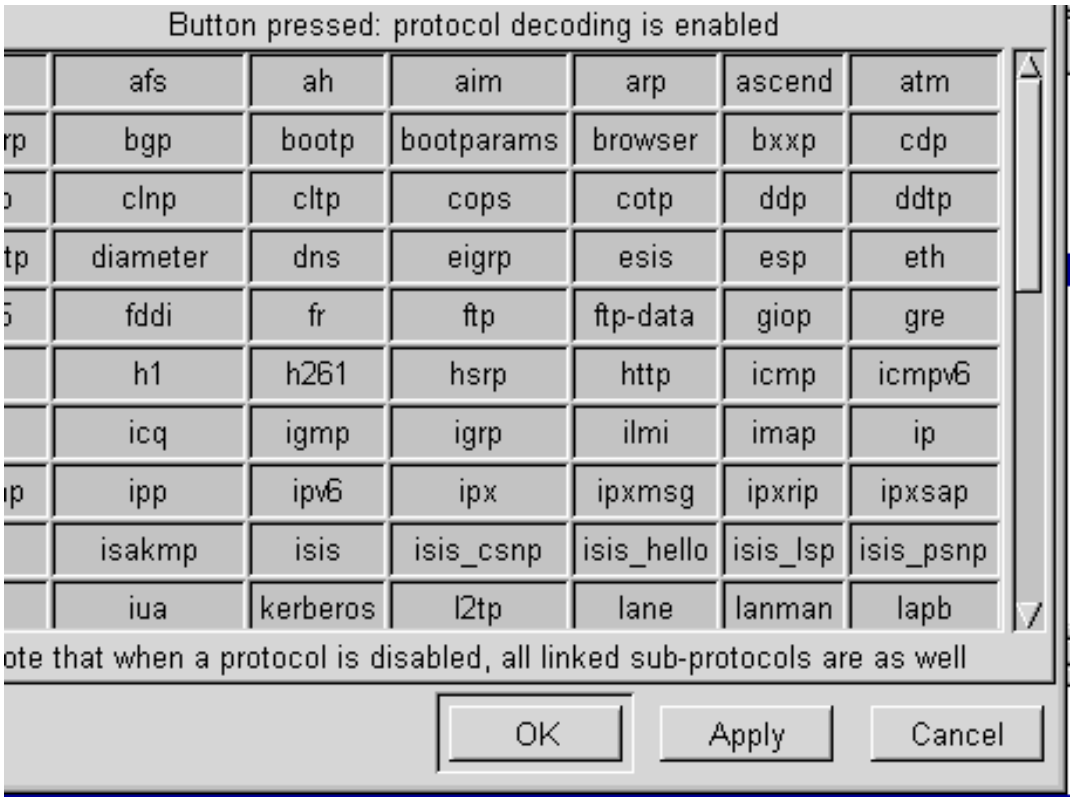
Kaavio 3.1 Etherealin käytön aloitus

Vertailuoperaattorit ovat eq **==** yhtä suuri (EQual), ne **!=** erisuuri (Not Equal), gt **>** suurempi kuin (Greater than), lt **<** pienempi kuin (Less Than), ge **>=** suurempi tai yhtä suuri kuin (Greater than or Equal to) sekä le **<=** pienempi tai yhtä suurikuin (Less than or Equal to).

Ethereal tukee seuraavia rajapintoja ja pakettityyppejä:

AARP, AFS, AH, AIM, ARP, ASCEND, ATM, AUTO_RP, BGP, BOOTP, BOOTPARAMS, BROWSER, BXXP, CDP, CGMP, CLNP, CLTP, COPS, COTP, DATA, DDP, DDTP, DEC_STP, DIAMETER, DNS, EIGRP, ESIS, ESP, ETH, EX.25, FDDI, FR, FRAME, FTP, FTP-DATA, GIOP, GRE, GVRP, H1, H261, HSRP, HTTP, ICMP, ICMPV6, ICP, ICQ, IGMP, IGRP, ILMI, IMAP, IP, IPCOMP, IPP, IPV6, IPX, IPXMSG, IPXRIP, IPXSAP, IRC, ISAKMP, ISIS, ISIS_CSNP, ISIS_HELLO, ISIS_LSP, ISIS_PSNP, ISL, IUA, KERBEROS, L2TP, LANE, LANMAN, LAPB, LAPBETHER, LAPD, LDAP, LDP, LLC, LPD, M3UA, MAILSLOT, MALFORMED, MAPI, MIP, MOUNT, MP, MPLS, MSPROXY, NBDGM, NBIPX, NBNS, NBP, NBSS, NCP, NETBIOS, NETLOGON, NFS, NLM, NNTP, NTP, NULL, OSPF, PIM, POP, PORTMAP, PPP, PPPOED, PPPOES, PPTP, Q2931, Q931, QUAKE, RADIUS, RIP, RIPNG, RLOGIN, RPC, RSH, RSVP, RTCP, RTMP, RTP, RTSP, RX, SAP, SCTP, SDP, SHORT, SIP, SLL, SMB, SMTP, SMUX, SNA, SNMP, SOCKS, SPX, SRVLOC, SSCOP, STAT, STP, SYSLOG, TACACS, TCP, TELNET, TEXT, TFTP, TIME, TNS, TPKT, TR, TRMAC, UDP, V120, VINES, VINES_FRP, VINES_SPP, VLAN, VRRP, VTP, WAP-WSP, WAP-WSP-WTP, WCCP, WHO, WLAN, X.25, X11, XOT, YHOO, YPBIND, YPSERV, YPXFR, ZEBRA

Protokollat valitaan sieppauksen alussa (ks. kaavio 3.2).



Kaavio 3.2 Protokollien valinta

Ethereal käyttää GTK+ -graafista käyttöliittymäkirjastoa ja libpcap –pakettikaappausta sekä protokollien filtteröintikirjastoa. Jos haluat katsota esimerkiksi kaikki paketit, jotka sisältävät ARP-osoitteenmuunnosprotokollan (Address Resolution Protocol), filtteri on ARP ja vastaavasti liitteen 1 luettelon mukaan.

4 Syntaksi

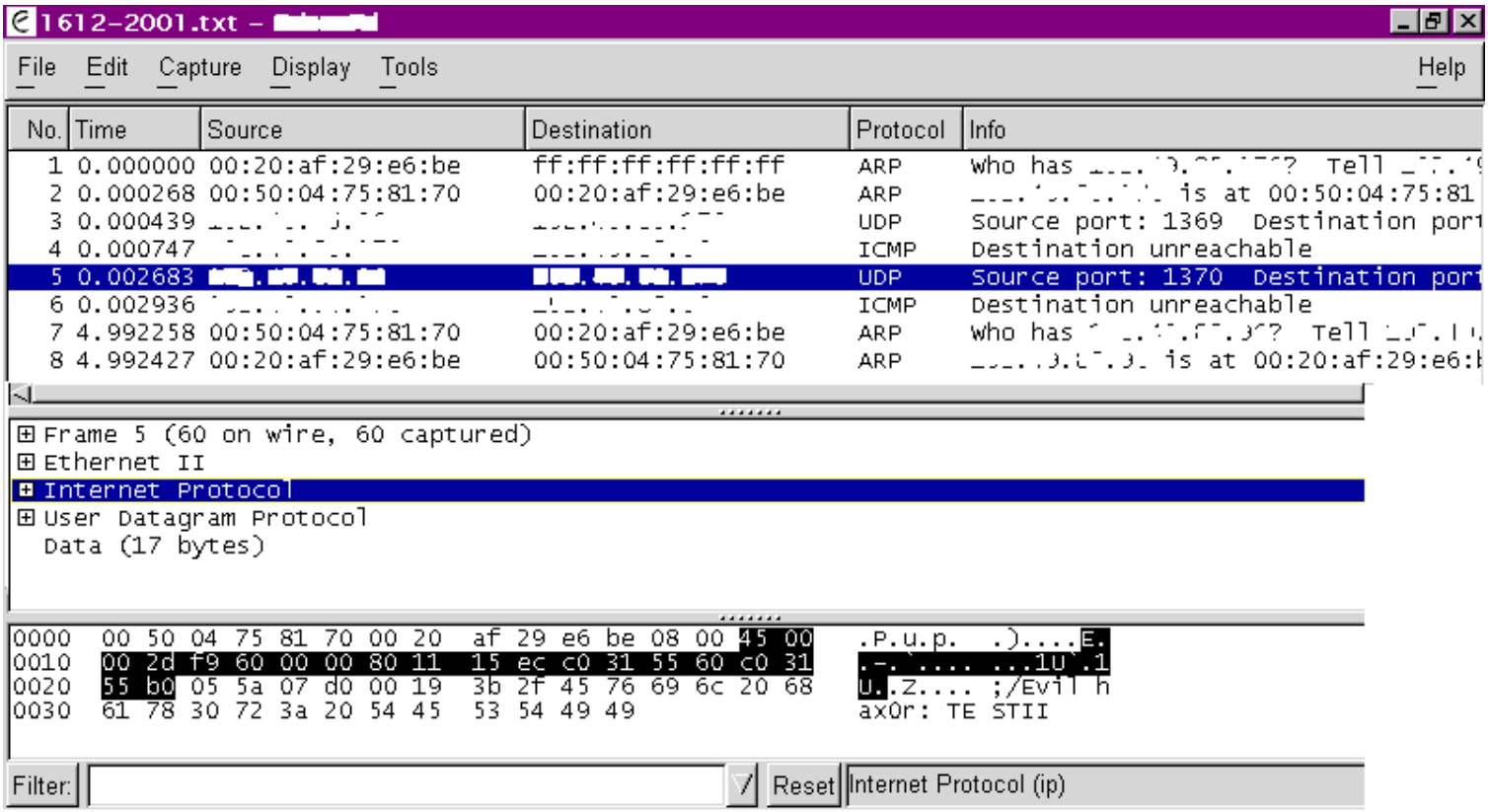
Kaaviossa 4.1 on Ethereal -ohjelman syntaksi. Katso lisätietoja man-komennolla tai readme-tiedostosta.

---

ethereal [**-B** bittinäkymän korkeus alaruudussa] [**-c** pakettilaskuri] [**-f** filtterin kuvaus] [**-h** versio ja optiot] [**-i** verkon rajapinta] [**-k** istunnon aloitus välittömästi] [**-m** kirjasintyyppi tekstille] [**-n** estää name resolutionin (esim. host, TCP- ja UDP -porttien nimet)] [**-o** asetukset esim. halutut arvot] ... [**-p** satunnaisen tilan esto] [**-P** pakettilistan korkeus yläruudussa] [**-Q** lopetus istunnon jälkeen] [**-r** lukee paketit tiedostosta] [**-R** filtterin kuvaus] [**-S** määrittelee paketin sieppauksen erilliseksi prosessiksi] [**-s** sieppausotoksen pituus bitteinä] [**-T** puunäkymän korkeus keskiruudussa] [**-t** paketin aikaleiman muoto pakettilistassa] [**-v** versio] [**-w** talletettava tiedosto]

Kaavio 4.1 Etherealin syntaksi

5 Ohjelman ulkoasu



Kuva 5.1 Lopputulokset, näkyvillä ovat kaikki kolme ruutua.

Pääikkuna (ks. kuva 5.1) on jaettu kolmeen ruutuun, joiden kokoa voi muuttaa.

Yläruutu sisältää listan verkkopaketeista, rivejä voi selata. Jokaisesta paketista näytetään oletuksena pakettinumero, paketin aikaleima, lähdeosoite ja kohdeosoite, protokolla sekä kuvaus paketista.

Paketti merkitään klikkaamalla hiirellä riviä. Sarakkeita voi valita järjestettäväksi minkä tahansa otsikon mukaan. Muutokset asetuksiin löytyvät ylävalikosta Preferences.

Kerätty tieto näytetään mahdollisimman ylhäällä protokollapinossa esimerkiksi IP-osoitteet näytetään IP-paketteina, mutta MAC-kerroksen osoitteet näytetään tuntemattomana pakettityyppinä.

Keskiruutu sisältää protokollapuun valituille paketeille. Puu näyttää jokaisen kentän ja sen arvon jokaisesta pinon protokollaotsakkeesta.

Alaruutu sisältää heksadesimaalidumpin todellisesta paketin datasta. Valittu protokollapuun kenttä näyttää vastaavat jakson bitit.

Kun protollapuusta on valittu kenttä, vastaavat tämän jakson biti korostuvat. Käytetty filtteri näkyy alareunassa, esimerkiksi filtteri HTTP, HTTPS ja DNS:

```
tcp.port == 80 || tcp.port == 443 || tcp.port == 53
```

6 Ohjelman käyttö

Ethereal -analysaattori tarvitsee käyttöjärjestelmän mukaisen Winpcap-pakettiajurin asentamisen asennushakemistoon. Muuten ohjelma asentui melkein ensi yrittämällä. Ethereal on käännettävissä ja suoritettavissa seuraavissa järjestelmissä:

- Linux (2.0.x, 2.1.x, 2.2.x, 2.3.x, 2.4.x)

- Solaris (2.5.1, 2.6, 7)

- FreeBSD (2.2.5, 2.2.6, 3.1, 3.2, 3.3)

- Sequent PTX v4.4.5

- Tru64 UNIX (entinen Digital UNIX) (3.2, 4.0)

- Irix (6.5)

- AIX (4.3.2, with a bit of work) sekä

- Win32 (NT, 98)

Ohjelman pitäisi olla suoritettavissa muissakin Unix-ish järjestelmissä. Asentamisohjeet löytyvät Etherealin Install-tiedostosta, eri käyttöjärjestelmille löytyy vieläpä erilliset Readme -tiedostot.

Saadaksesi siepattua paketteja verkosta, sinun täytyy olla kirjautuneena pääkäyttäjäksi (ns. root) tai päästä verkkoon esim. jättämällä kannettavan tietokoneen kytkettynä verkkoon. Tällaisia tilanteita voi syntyä esimerkiksi kirjaston koneilla, opiskelupaikkojen tietokoneluokissa tai yritysten neuvotteluhuoneissa. Etherealin tekijät kuitenkin varoittavat Etherealin suorittamisesta setuid rootina, koska ohjelma sisältää turva-aukkoja.

7.1 IPv6

Ethereal pyrkii käyttämään reverse name resolution- mahdollisuutta IPv6-paketeille, jos käyttöjärjestelmä tulee IPv6.versiota. Jos et halua käyttää name resolution -ominaisuutta, IPv6-paketeista näkyy vain IPv6-osoitteet, mutta isäntäkoneiden nimet eivät näy.

7.2 NetWare Core Protocol

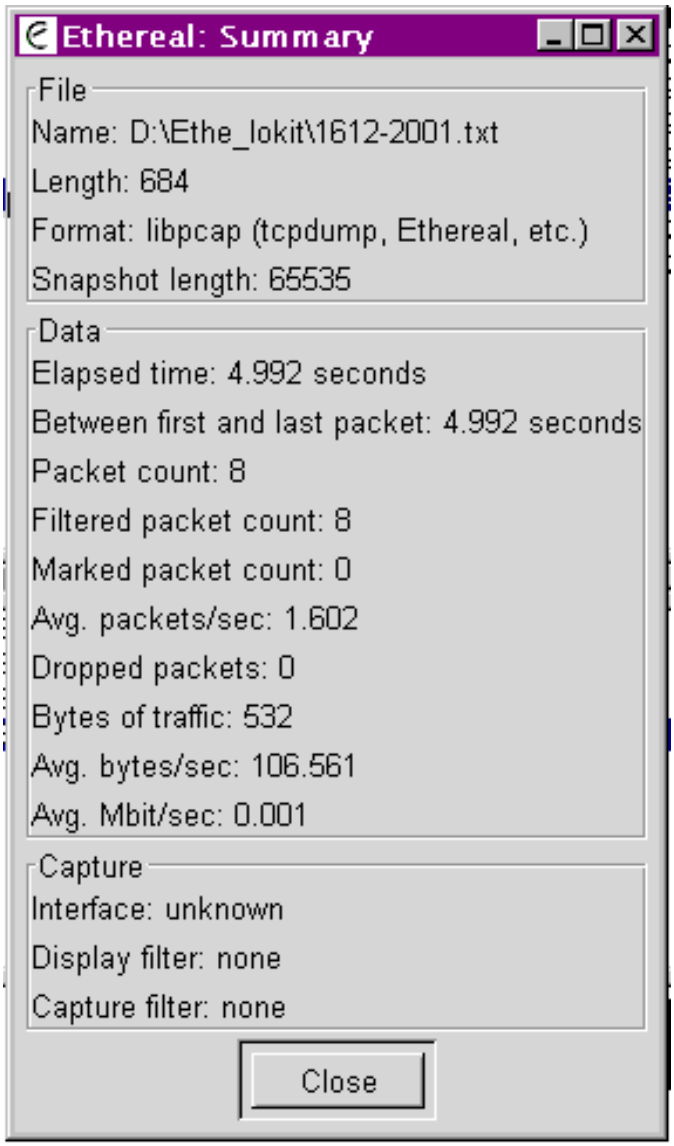
NCP-pakettityyppejä on yli 400. NCP-analysaattori ei tunne kaikkia niitä, mutta uusiin versioihin tukea lisätään vähitellen.

7.3 SNMP

Ethereal osaa tehdä perusmuunnoksia SNMP-paketeille. Myös ulkoinen SNMP-kirjasto on käytettävissä vaativiin muunnoksiin. Asennuskoodi määrittelee automaattisesti mitä kirjastoa järjestelmä käyttää.

8 Raportit

Etherealista saa mielenkiintoisia ja yllättävän laajoja raportteja, joiden katseluun tosin tarvitsee itse ohjelman, ellei niitä kaappaa näytöltä. Ohjelma näyttää myös yhteenvedon siepatuista tiedoista (ks. kaavio 8.1).



Kaavio 8.1 Yhteenveto tuloksista.

Tulosteet voi joko tulostaa tai tallentaa muistiin tai tiedostoksi. Näytöllä olevaa dataa voi saada eri muodoissa käyttäen protokollasuodattimia (ks. kappaleen 3 protokollalistaus). Näytöllä voi jokaisen paketin tiedot merkata ja katsoa yhteenvedon paketeista. Kaikki siepattu tieto verkosta voidaan tallettaa tiedostoksi ((plain teksti tai PostScript®).

9 Lähteet

[Eth01] Ethereal network analyzer http://www.ethereal.com/

[Tet01] Tethereal http://www.ethereal.com/tethereal.1.html

[GNU01] GNU http://www.gnu.org/

[Edi01] Editcap http://www.ethereal.com/editcap.1.html

[Ker98] Kerttula, Esa, Tietoverkkojen tietoturva, Edita, Helsinki, 1998.

Liite 1 Protokollaluettelo

Ethereal -verkkoanalysaattorin ymmärtämät protokollat.

AARP Appletalk Address resolution protocol

AFS Andrew file system

AH Authentication header

AIM AOL Instant Messanger

ARP Address Resolution Protocol

ASCEND Lucent/Ascend debug output

ATM Asyncronous Transfer Mode

LANE ATM LAN Emulation

VINES_FRP Banyan Vines Fragmentation Protocol

VINES_SPP Banyan Vines SPP

BXXP Blocks eXtensible eXchange Protocol

BOOTP bootparams Boot Parameters Bootstrap Protocol

BGP Border Gateway Protocol

AUTO_RP Cisco Auto-RP

CDP Cisco Discovery Protocol

CGMP Cisco Group Management Protocol

HSRP Cisco Hot Standby Router Protocol

ISL Cisco ISL

IGRP Cisco Interior Gateway Routing Protocol

COPS Common Open Policy Service

DEC_STP DEC Spanning Tree Protocol

DATA Data

DDP Datagram Delivery Protocol

DIAMETER Diameter Protocol

DNS Domain name service

DDTP Dynamic DNS Tools Protocol

ESP Encapsulated Security Payload

EIGRP Enhanced Interior Gateway Routing Protocol

ETH Ethernet

EX.25 Extended X.25 (modulo 128)

FTP-DATA FTP Data

FDDI Fiber Distributed Data Interface

FTP File Transfer Protocol

FRAME Frame

FR Frame relay

GVRP GARP VLAN Registration Protocol

GIOP General Inter-ORB Protocol

GRE Generic Routing Encapsulation

HTTP Hypertext Transfer Protocol

ICQ Protocol

WLAN IEEE 802.11 wireless LAN

IPCOMP Payload Compression

IPXMSG Message

IPXRIP IPX Routing Information Protocol

IUA ISDN Q.921-User Adaptation Layer

ISIS HELLO isis_hello

ISIS_CSNP ISO 10589 ISIS Complete Sequence Numbers Protocol Data Unit

ISIS ISO 10589 ISIS InTRA Domain Routeing Information Exchange Protocol

ISIS_LSP ISO 10589 ISIS Link State Protocol Data Unit

ISIS_PSNP ISO 10589 ISIS Partial Sequence Numbers Protocol Data Unit

COTP ISO 8073 COTP Connection-Oriented Transport Protocol

CLNP ISO 8473 CLNP ConnectionLess Network Protocol

CLTP ISO 8602 CLTP ConnectionLess Transport Protocol

ESIS ISO 9542 ESIS Routing Information Exchange Protocol

H261 ITU-T Recommendation H.261

ICP Internet Cache Protocol

ICMP Internet Control Message Protocol

ICMPv6 Internet Control Message Protocol v6

IGMP Internet Group Management Protocol

IMAP Internet Message Access Protocol

IPP Internet Printing Protocol

IP Internet Protocol

IPv6 Internet Protocol Version 6

IRC Internet Relay Chat

ISAKMP Internet Security Association and Key Management Protocol

IPX Internetwork Packet eXchange

KERBEROS Kerberos

LDP Label Distribution Protocol

L2TP Layer 2 Tunneling Protocol

LDAP Lightweight Directory Access Protocol

LPD Line Printer Daemon Protocol

LAPB Link Access Procedure Balanced

LAPBETHER Link Access Procedure Balanced Ethernet

LAPD Link Access Procedure, Channel D

SLL Linux cooked-mode capture

LLC Logical-Link Control

ASCEND Lucent/Ascend debug output

MAPI Mail/Messaging Applications Programming Interface [Microsoft]

MSPROXY MS Proxy Protocol

M3UA MTP 3 User Adaptation Layer

MALFORMED Malformed Frame

BROWSER Microsoft Windows Browser Protocol

LANMAN Microsoft Windows Lanman Protocol

NETLOGON Microsoft Windows Logon Protocol

MIP Mobile IP

MOUNT Mount Service

MPLS MultiProtocol Label Switching Header

NBP Name Binding Protocol

NETBIOS Netbios

NBDGM NetBIOS Datagram Service

NBNS NetBIOS Name Service

NBSS NetBIOS Session Service

NBIPX NetBIOS over IPX

NCP NetWare Core Protocol

NFS Network File System

NLM Network Lock Manager Protocol

NNTP Network News Transfer Protocol

NTP Network Time Protocol

NULL Null/Loopback

OPSF Open Shortest Path First

MP PPP Multilink Protocol

PPPOED PPP-over-Ethernet Discovery

PPPOES PPP-over-Ethernet Session

PPP Point-to-Point Protocol

PPTP Point-to-Point Tunnelling Protocol

PORTMAP Portmap

POP Post Office Protocol

PIM Protocol Independent Multicast

q.2931 q.2931

q931 q931

QUAKE Quake Network Protocol

RIPNG RIPng

RX RX Protocol

RADIUS Radius Protocol

RTSP Real Time Streaming Protocol

RTP Real-Time Transport Protocol

RTCP Real-time Transport Control Protocol

RPC Remote Procedure Call

RSH Remote Shell

RSVP Resource ReserVation Protocol

RLOGIN Rlogin Protocol

RIP Routing Information Protocol

RTMP Routing Table Maintenance Protocol

SMB Server Message Block Protocol

MAILLOT SMB MailSlot Protocol

SMUX SNMP Multiplex Protocol

SSCOP sscop

SPX Sequenced Packet eXchange

IPXSAP Service Advertisement Protocol

SRVLOC Service Location Protocol

SAP Session Announcement Protocol

SDP Session Description Protocol

SIP Session Initiation Protocol

SHORT Short Frame

SMTP Simple Mail Transfer Protocol

SNMP Simple Network Management Protocol

H1 Sinec H1 Protocol

SOCKS Socks Protocol

STP Spanning Tree Protocol

STAT Status Service

SCTP Stream Control Transmission Protcol

SYSLOG Syslog message

SNA Systems Network Architecture

Tacacs Tacacs

TPKT Tpkt

TELNET telnet

TIME Time Protocol

TR Token-Ring

TRMAC Token-Ring Media Access Control

TCP Transmission Control Protocol

TNS Transparent Network Substrate Protocol

TFTP Trivial File Transfer Protocol

UDP User Datagram Protocol

VRRP Virtual Router Redundancy Protocol

VTP Virtual Trunking Protocol

WCCP Web Cache Coordination Protocol

WHO Who

WAP-WSP Wireless Session Protocol

WAP-WSP-WTP

Wireless Transaction Protocol

x.25 x.25

XOT xot

x11 x11

YHOO Yahoo Messenger Protocol

YBIND Yellow Pages Bind

YPSERV Yellow Pages Service

YPXFR Yellow Pages Transfer

ZEBRA Zebra Protocol
