Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Ethereal: Mucho más que un sniffer (111831 lectures)

Per **Carlos Cortes Cortes**, ***carcoco*** (http://bulma.net/~carcoco/)

Creado el 10/09/2002 20:54 modificado el 10/09/2002 20:54

Ethereal es un **potente analizador libre** de **protocolos** de **redes**, para máquinas **Unix** y **Windows**. Nos permite capturar los datos directamente de una red o obtener la información a partir de una captura en disco (puede leer más de **20** tipos de formato distintos ;-). Destaca también por su impresionante soporte de más de **300 protocolos**, gracias sin duda a la licencia **GPL** y sus más de **200 colaboradores** de todo el mundo ;-) ...

"Ethereal is a free network protocol analyzer for Unix and Windows. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session."

Una de las cosas que más cuesta entender cuando uno comienza con **ethereal** es la utilización de los **filtros** a la hora de capturar datos (el típico error: *Unable to parse filter string (parse error)*, puesto que utiliza un sistema para **visualizar los datos** y otro totalmente diferentes e incompatible para realizar las **capturas** (tcpdump), por lo que os voy a dejar unos sencillos ejemplos de unos **filtros de captura de datos** de **Ethereal**:

```
src host 127.0.0.1

host linuxalcoy and 192.168.0.1

tcp port 23 and host 10.0.0.5

tcp port 23 and not host 10.0.0.5

ip.src eq 127.168.0.55

less 50000

ip.addr eq 127.168.0.5 and ip.addr eq 127.168.0.47

(ip.addr eq 127.168.0.5 and ip.addr eq 127.168.0.47)
 and (tcp.port eq 21210 and tcp.port eq 1032)
```

Teneís más información en esta página[1] y consultando la ayuda del propio **tcpdump**: (*man tcpdump*).

La potencia y posibilidades del **Ethereal** son realmente impresionantes como podemos apreciar a continuación:

Protocolos soportados:
802.11, 802.11 MGT, 802.11w, AARP, AFP, AFS, AFS (RX), AH, AIM, AODV, AODV ARP/RARP, ARP, ASAP, ASP, ATM, ATM LANE, ATP, AppleTalk, Auto-RP, BACapp, BACnet, BEEP, BGP, BOOTP, BOOTP/DHCP BOOTPARAMS, BROWSER, BVLC, CDP, CGMP, CHDLC, CLNP, CLTP, CONV, COPS, COSEVENTCOMM COSNAMING, COTP, CUPS, DCCP, DCE RPC, DCERPC, DDP, DDTP, DEC spanning tree, DEC_STP, DFS, DHCPv6, DIAMETER, DLSw, DNS, DSI, DSI DVMRP, DVMRP, Data, Diameter, EAP, EAP/ EAPOL, EAPOL, EIGRP, EPM, ESIS, ESP, Ethernet, FDDI, FR, FTP, FTP-DATA, Frame GIOP, GIOP, GMRP, GNUTELLA, GRE, GTP, GTPv0, GTPv1, GVRP, Gryphon, H.261, H1, HCLNFSD, HMIPv6, HSRP, HTTP, IAPP, IAPP ICAP, ICMP, ICMPv6, ICP, ICQ, IEEE 802.11, IEEE spanning tree, IGMP, IGRP, ILMI, IMAP, IP, IPComp, IPP, IPX, IPX MSG, IPX RIP, IPX SAP, IPv6, IRC, IS-IS, ISAKMP, ISIS, ISL, ISUP, IUA, KLM, KRB5, L2TP, LANMAN, LAPB, LAPBETHER LAPD, LAPD, LDAP, LDP, LLAP, LLC, LMI, LMP, LPD, LSA, Lucent/Ascend, M2PA, M2TP,

M2UA, M3UA, MAPI MGCP, MGMT, MIP, MMSE, MOUNT, MPEG1, MPLS, MRDISC, MS Proxy, MSDP, MSNIP, MTP2, MTP3, Mobile IP Modbus/TCP, NBDS, NBIPX, NBNS, NBP, NBSS, NCP, NDMP, NETLOGON, NFS, NFSACL NFSAUTH, NIS+, NIS+ CB, NLM, NMPI, NNTP, NTP, NetBIOS, New dissectors include DHCPv6, Null, ONC RPC, OSPF, OXID, PCNFSD, PFLOG, PGM PIM, PIM, POP, PPP, PPP BACP, PPP BAP, PPP CBCP, PPP CCP, PPP CHAP, PPP Comp, PPP IPCP, PPP LCP, PPP MP PPP PAP, PPP PPPMux, PPP PPPMuxCP, PPP VJ, PPPoED, PPPoES, PPTP, Portmap, Prism, Q.2931, Q.931, QLLC QUAKE, QUAKE2, QUAKE3, QUAKEWORLD, RADIUS, RANAP, RARP, REG, REMACT, RIP, RIPng, RPC, RPC RQUOTA, RSH, RSTAT, RSVP, RTCP, RTMP, RTP, RTSP, RWALL, RX, Raw, Raw IP, Rlogin, SADMIND, SAMR, SAMR SAP, SCCP, SCSI, SCTP, SDB, SDP, SIP, SKINNY, SLARP, SLL, SMB, SMB Mailslot, SMB Pipe, SMB/CIFS, SMPP, SMTP, SMUX SNA, SNA over Ethernet and HiPath HDLC, SNAETH, SNMP, SOCKS, SPOOLSS, SPOOLSS RPC, SPRAY, SPX, SRVLOC, SRVSVC, SSCOP, SSL, STAT, STAT-CB, STP SUA, Skinny, SliMP3, Socks, Syslog, TACACS, TACACS+, TCP, TELNET, TFTP, TIME, TNS, TPKT, TR MAC, TSP, TSP Token-Ring, UCP, UDP, V.120, VJ, VLAN, VRRP, VTP, Vines, Vines FRP, Vines SPP, WCCP, WCP, WHO WKSSVC, WSP, WTLS, WTP, WebDAV (HTTP), X.25, X11, XDMCP, XOT, YHOO, YP, YPBIND, YPPASSWD, YPSERV, YPXFR , ZEBRA, Zebra, iSCSI, iSCSI/SCSI, ypbind.

Formatos de captura de datos:

- libpcap (tcpdump -w, etc.) - este es el formato nativo de Ethereal.
- snoop and atmsnoop
- Shomiti/Finisar Surveyor
- Novell LANalyzer
- Network General/Network Associates DOS-based Sniffer
- Microsoft Network Monitor
- AIX´s iptrace
- Cinco Networks NetXRray
- Network Associates Windows-based Sniffer
- AG Group/WildPackets EtherPeek/TokenPeek/AiroPeek
- RADCOM´s WAN/LAN Analyzer
- Lucent/Ascend access products
- HP-UX´s nettl
- Toshiba´s ISDN routers
- ISDN4BSD "i4btrace" utility
- Cisco Secure Intrustion Detection System iplogging facility
- pppd logs (formato pppdump)
- VMS´s TCPIPtrace utility
- DBS Etherwatch for VMS
- Traffic captures from Visual Networks´ Visual UpTime
- CoSine L2 debug output
- CheckPoint Firewall-1
- Sniffer 4.6 wireless captures

Soporte para:

- Ethernet
- FDDI
- PPP
- Token-Ring
- IEEE 802.11 (redes inalambricas)
- Classical IP over ATM
- loopback interfaces

Ethereal
http://www.ethereal.com(2)

La ultima versión disponible es la 0.9.6[3], que corrige muchos problemas encontrados en la versión anterior como podemos comprobar en el fichero **ChangeLog**, por lo que os recomiendo que os actualiceís a esta versión lo antes posible ;-)

Enlaces relacionados:

- **Ethereal**
  http://www.samag.com/documents/s=1441/sam0111a/0111a.htm[4]
- **Filtering while capturing**
  http://www.ns.aus.com/ethereal/user-guide/ch03capfilt.html[1]
- **Tcpdump**
  http://www.tcpdump.org/[5]
- Skirting common **Samba problems**
  http://www.linuxworld.com/linuxworld/lw-2000-11/lw-11-samba.html[6]
  http://www.linuxworld.com/linuxworld/lw-2000-11/lw-11-samba.html[6]

--
$ alias **carcoco=**"echo Carlos Cortes"
http://bulma.net/todos.phtml?id_autor=132[7]

Lista de enlaces de este artículo:

1. http://www.ns.aus.com/ethereal/user-guide/ch03capfilt.html
2. http://www.ethereal.com
3. ftp://ftp.ethereal.com/pub/ethereal/ethereal-0.9.6.tar.bz2
4. http://www.samag.com/documents/s=1441/sam0111a/0111a.htm
5. http://www.tcpdump.org/
6. http://www.linuxworld.com/linuxworld/lw-2000-11/lw-11-samba.html
7. http://bulma.net/todos.phtml?id_autor=132

E-mail del autor: carcoco _ARROBA_ gmail.com
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=1498