Packet analyzer

From Wk ped a the free encycloped a

Th s art c e **needs additional citations for verification**. P ease he p mprove th s art c e by add ng c tat ons to re ab e sources. Unsourced mater a may be cha enged and removed. *(March 2013)*

A **packet analyzer** (a so known as a **network analyzer**, **protocol analyzer** or **packet sniffer**, or for part cu ar types of networks, an **Ethernet sniffer** or **wireless sniffer**) s a computer program or a p ece of computer hardware that can ntercept and og traff c pass ng over a d g ta network or part of a network.[1] As data streams f ow across the network, the sn ffer captures each packet and, f needed, decodes the packet's raw data, show ng the va ues of var ous fe ds n the packet, and ana yzes ts content accord ng to the appropr ate RFC or other spec f cat ons.

Packet capture s the process of ntercept ng and ogg ng traff c.

Contents [hide]

Capabilities [ed t]

On w red broadcast LANs, depend ng on the network structure (hub or sw tch), one can capture traff c on a or just parts of the network from a s ng e mach ne w th n the network; however, there are some methods to avo d traff c narrow ng by sw tches to ga n access to traff c from other systems on the network (e.g., ARP spoof ng). For network mon tor ng purposes, t may a so be des rab e to mon tor a data packets n a LAN by us ng a network sw tch w th a so-ca ed *monitoring port*, whose purpose s to m rror a packets pass ng through a ports of the sw tch when systems (computers) are connected to a sw tch port. To use a network tap s an even more re ab e so ut on than to use a mon tor ng port, s nce taps are ess ke y to drop packets dur ng h gh traff c oad.

On w re ess LANs, one can capture traff c on a part cu ar channe , or on severa channe s when us ng mu t p e adapters.

On w red broadcast and w re ess LANs, to capture traff c other than un cast traff c sent to the mach ne runn ng the sn ffer software, mu t cast traff c sent to a mu t cast group to wh ch that mach ne s sten ng, and broadcast traff c, the network adapter be ng used to capture the traff c must be put nto prom scuous mode; some sn ffers support th s, others do not. On w re ess LANs, even f the adapter s n prom scuous mode, packets not for the serv ce set for wh ch the adapter s conf gured w usua y be gnored. To see those packets, the adapter must be n mon tor mode.[*citation needed*]

When traff c s captured, e ther the ent re contents of packets can be recorded, or the headers can be recorded w thout record ng the tota content of the packet. Th s can reduce storage requ rements, and avo d ega prob ems, but yet have enough data to revea the essent a nformat on requ red for prob em d agnos s.

The captured nformat on s decoded from raw d g ta form nto a human-readab e format that perm ts users of the protoco ana yzer to eas y rev ew the exchanged nformat on. Protoco ana yzers vary n the r ab t es to d sp ay data n mu t p e v ews, automat ca y detect errors, determ ne the root causes of errors, generate t m ng d agrams, reconstruct TCP and UDP data streams, etc.[*citation needed*]

Some protoco ana yzers can a so generate traff c and thus act as the reference dev ce; these can act as protoco testers. Such testers generate protoco -correct traff c for funct ona test ng, and may a so have the ab ty to de berate y ntroduce errors to test for the DUT's ab ty to dea w th error cond t ons.[*citation needed*]

Protoco Ana yzers can a so be hardware-based, e ther n probe format or, as s ncreas ng y more common, comb ned w th a d sk array. These dev ces record packets (or a s ce of the packet) to a d sk array. Th s a ows h stor ca forens c ana ys s of packets w thout the users hav ng to recreate any fau t.[*citation needed*]

Uses [ed t]

The versat ty of packet sn ffers means they can be used to:[*citation needed*]

- Ana yze network prob ems
- Detect network ntrus on attempts
- Detect network m suse by nterna and externa users
- Document ng regu atory comp ance through ogg ng a per meter and endpo nt traff c
- Ga n nformat on for effect ng a network ntrus on
- Iso ate exp o ted systems
- Mon tor WAN bandw dth ut zat on
- Mon tor network usage (nc ud ng nterna and externa users and systems)
- Mon tor data- n-mot on
- Mon tor WAN and endpo nt secur ty status
- Gather and report network stat st cs

EXHIBIT F

- F ter suspect content from network traff c
- Serve as pr mary data source for day-to-day network mon tor ng and management
- Spy on other network users and co ect sens t ve nformat on such as og n deta s or users cook es (depend ng on any content encrypt on methods that may be n use)
- Reverse eng neer propr etary protoco s used over the network
- Debug c ent/server commun cat ons
- Debug network protoco mp ementat ons
- Ver fy adds, moves and changes
- Ver fy nterna contro system effect veness (f rewa s, access contro , Web f ter, spam f ter, proxy)

Packet capture can be used to fu f a warrant from a aw enforcement agency (LEA) to produce a network traff c generated by an nd v dua . Internet serv ce prov ders and VoIP prov ders n the Un ted States must comp y w th CALEA (Commun cat ons Ass stance for Law Enforcement Act) regu at ons. Us ng packet capture and storage, te ecommun cat ons carr ers can prov de the ega y requ red secure and separate access to targeted network traff c and are ab e to use the same dev ce for nterna secur ty purposes. Co ect on of data from a carr er system w thout a warrant s ega due to aws about ntercept on.

Notable packet analyzers [ed t]

For a more comprehensive list see Comparison of packet analyzers

- Capsa Network Ana yzer
- Ca n and Abe
- Carn vore (FBI)
- dSn ff
- ettercap
- F dd er
- Lanmeter
- M crosoft Network Mon tor
- NarusIns ght
- NetScout Systems nGen us Inf n stream
- ngrep, Network Grep
- Omn Peek
- SkyGrabber
- snoop
- tcpdump
- W reshark (former y known as Etherea)
- Xp co Open source Network Forens c Ana ys s Too

See also [ed t]

- Bus ana yzer
- Log c ana yzer
- Network detector
- Network ntrus on detect on system
- Network tap
- Packet generat on mode
- pcap
- S gna s nte gence

References [ed t]

1 ^ Kevn J Connolly (2003) *Law of Internet Security and Privacy* Aspen Publ shers p 131 SBN 978 0 7355 4273 0

External links [ed t]

- Protoco Ana yzers on the Open D rectory Project
- ow-to Packet Sn ff
- The Mak ng of a Profess ona cTrace Packet Ana yzer (You must f a "Down oad request form" to access th s document)
- Packet Sn ff ng FAQ by Robert Graham
- A Qu ck Intro to Sn ffers
- Mu t -Tap Network Packet Capture
- M crosoft Message Ana yzer

Wikimedia Commons has media related to *Computer data network analyzers*

Wikiversity has learning materials about *Packet analyzer*

Categor es: Network ana yzers | Packets (nformat on techno ogy) | W re ess network ng | Computer network secur ty | Deep packet capture