Colasoft®
Maximize Network Value

Capsa

Real-time Portable Network Analyzer

Whitepaper

(Professional Edition)

Colasoft reserves the right to make changes in the product design without reservation and without notification to its users.

Contact Us

Sales
sales@colasoft.com

Technical Support
support@colasoft.com

Website
http://www.colasoft.com/

Contents

Introduction

This chapter describes the background, the system architectures, and the principle that how Capsa works.

Background

The rapid popularization and wide application of network, including various E-Commerce, E-Government, network office and other uses of modern information, offers opportunities of faster development to enterprises. However, while people are enjoying convenience and profits brought by network, they also have to suffer its low efficiency, troubles and even breakdown, which may cause damages to enterprises/organizations' operation and result in incalculable loss.

As security management and performance maintenance are becoming more and more important, network engineers and administrators are facing the problem of how to improve network speed and efficiency. On the other hand, due to network infrastructure being more complex and network technology being developing amazingly fast, it is more difficult than ever before to implement network maintenance and network arrangement. Therefore, efficient network management solutions are very important for to administrators find and solve network problems.

Capsa, provided by Colasoft, is such a solution. It captures original packets in real-time, decodes, and analyzes captured packets, and then displays the results in straightaway views, visualized charts and structured reports, to thereby get the network administrators to know the network status comprehensively and quickly.

Working principle

In actual network communications, all data are sent and received by network adapters. By default, a network adapter only receives unicast packet traffic matching its MAC address and broadcast traffic on the network. If we put the network adapter in promiscuous mode, it will receive all traffic through it, regardless of the destinations.

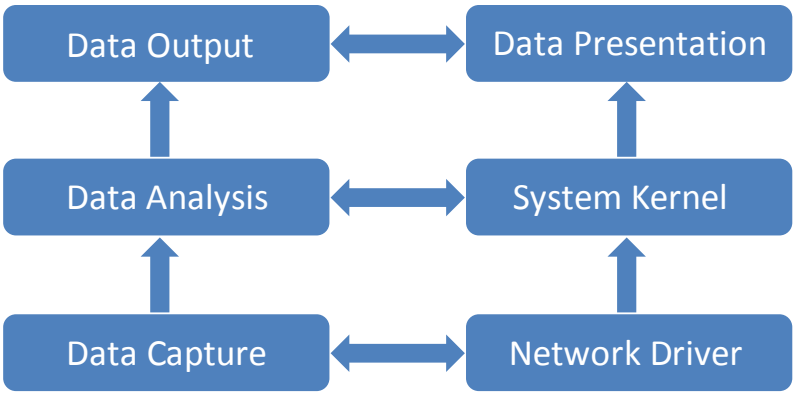
Colasoft Capsa utilizes such a mechanism to capture packets. It takes every network element, such as IP addresses, MAC addresses, protocols, packets, as a network object, and integrates them into a project. Therefore, every tiny change on the network will be monitored and analyzed to the project.

Based on Ethernet sniffer technology, Capsa captures traffic via bypass access. It first puts the network adapter of the computer on which Capsa is installed in promiscuous mode to capture all packets over the network, then delivers captured packets to analysis modules for analyzing, and at last displays the result on the screen.

System architecture

To analyze the traffic over the network, the traffic must first be captured. The network drivers at the bottom-level are the core module for detecting and capturing the data transmitted. And then all data are forwarded to high-level modules to be analyzed, summarized and outputted on screen. The architecture of Capsa is described as Figure 1.

Figure 1 Capsa Architecture



1. Network drivers are responsible for network traffic capture and ensure the data is accurate and complete.
2. All captured data is delivered to analysis modules for real-time analysis, such as statistic modules and packet decoding module, and other analysis modules.
3. Finally the analysis results are outputted to user interface and/or to hard disk.

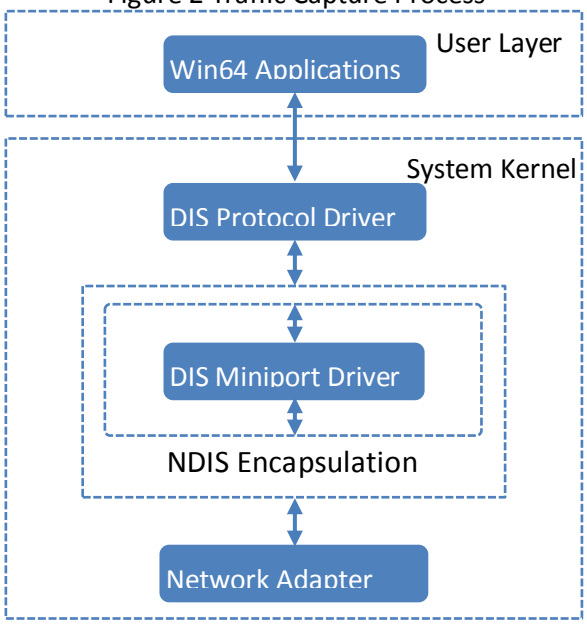
Data capture

Capsa can capture packets by the following two methods:

1. With Colasoft NDIS Protocol Driver on Windows, capture packets by network adapters.
2. With Colasoft NDIS Intermediate Driver on Windows, capture packets by network adapters.
3. With Colasoft TDI Driver on Windows, capture local loop packets without network adapters.

By default, Capsa collects traffic via Colasoft NDIS Protocol Driver and Colasoft TDI Driver. The following figure outlines the data capture process for Capsa.

Figure 2 Traffic Capture Process

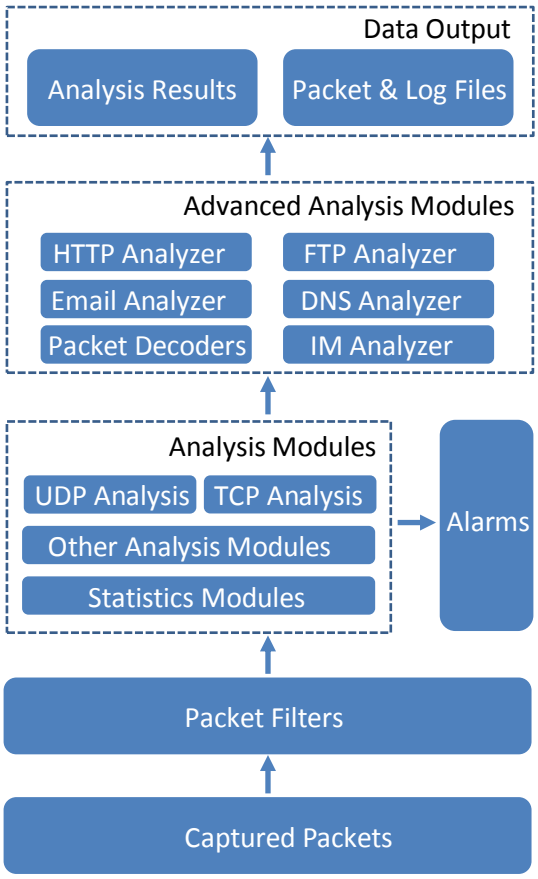


The efficiency of data capture at the bottom level is crucial to the following analysis missions. Thus, filters are implemented on this level to filter out the irrelevant packets so as to avoid the waste of the resource due to data transfer from driver level to application level.

Data analysis

When the driver gets a packet matching filtering conditions, it immediately delivers the packet to the system kernel for further analysis. The analysis includes statistics, in-depth packet inspection, packet decoding and protocol analysis. The following flowchart shows the packet analysis process of Capsa.

Figure 3 Packet Analysis Diagram



Data output and presentation

After packet analysis, all analysis results and statistics are presented in the form of charts, lists and reports on the screen. The analysis contents presented including packet decoding, nodes, protocols, IP flow, TCP flow, conversations and logs. In addition, these lists, reports and logs can be exported for further use according to the need.

Key Features

Capsa provides many powerful features, including some unique features different from other network sniffer products.

Colasoft Packet Analysis Engine (CSPAE) II

The 2nd generation of Colasoft Packet Analysis Engine (CSPAE), powered by the innovative Colasoft dynamic object model (CSDOM), greatly improves analysis efficiency and performance under heavy traffic networks. The following new technologies are applied to Capsa.

- Multi-thread analysis
  - Upgrade single-thread analysis to multi-thread analysis technology, which take full advantage of the processing ability of multi-core CPU.
- Multiple Cycle Buffer (MCB)
  - Recycle multiple cache buffers
  - Parallelize data analysis and data accessing to avoid latency from analysis and data query
  - Decrease memory fragmentation
- Direct Memory Access (DMA)
  - Bypass kernel-level to transmit data directly to user-level
  - Speed up data transmission
- Protocol dynamic creation
  - Dynamically create protocol tree structure
  - Effectively identify protocol and sub-protocol types
  - Support custom protocol definition

Directive analysis guide

An easy-to-use Start Page is provided to guide users to start an analysis project. Usually an analysis project can be started within four simple steps:

1. Select an analysis mode: real-time monitor or replay captured packets.
2. Select the network adapters for capturing packets and then select a network profile, or select the packet files to be replayed.
3. Select an appropriate analysis profile.
4. Click to start an analysis project.

Network profile

Colasoft Capsa can be installed on a laptop and then you can use the laptop to access any networks. Every network has its own network structure and properties. Network profile is defined to save the general properties for different networks, including network bandwidth, network structure, name table, and alarm settings. When you need to analyze the network of the same type, you just load the network profile of that network.

Analysis profile

Capsa defines analysis profile as a container of different analysis modules to provide flexible, extensible and effective analysis performance. You can combine different analysis modules together to create your own analysis profile that focusing on certain applications. Generally speaking, an analysis profile includes the settings for analysis modules, analysis object, analysis views, packet buffer, packet filters, log output and packet output. The following table describes the default analysis profiles.

Analysis Type	Analysis Profile	Description
Basic Analysis	Traffic Monitor	Provides analysis for large traffic network or traffic monitor.
	Full Analysis	Provides comprehensive analysis of all traffic and applications.
Application Analysis	HTTP Analysis	Analyzes the HTTP traffic and provides traffic statistics of clients and servers, and logs of HTTP activities.
	FTP Analysis	Analyzes the FTP traffic and provides statistics on uploading, downloading, and logs of FTP activities.
	Email Analysis	Analyzes the SMTP/POP3 traffic and provides statistics on email communications, duplicating emails and logs of email activities.
	DNS Analysis	Analyzes the DNS traffic and provides statistics on DNS queries, and logs of DNS activities.
	IM Analysis	Provides instant messenger analysis.
Built-in Analysis	TCP Flow Analysis	Analyzes the TCP transactions and provides detailed information of the transaction procedures.

Node Explorer window

A Node Explorer window is provided to let users view the analysis and statistics of a specific node, a network segment or a protocol, conveniently. It is functionally a powerful filter and includes three types of node explorers: protocol node explorer for hierarchically displaying the protocols on the network, MAC explorer for users to view the communications between MAC addresses, and IP node explorer for providing analysis and statistics about IP nodes.

Powerful dashboard

Various charts and graphs can be defined to visualize the network traffic just by a few clicks, not only on the whole network but down to a specific node. In addition, top statistics can be displayed in charts to display the traffic of the network in real-time to get you know the network status directly and comprehensively.

Traffic analysis

With traffic analysis, the host with largest communication volume can be located easily and quickly. You can sort the nodes according to bytes, packets, bit rate, TCP conversation quantity, and many other parameters. Furthermore, the host with largest sending traffic, the host with largest receiving

traffic, the host with largest broadcast volume, and the network segment with largest internal traffic can be located easily.

Protocol analysis

Capsa hierarchically presents the protocols according to actual encapsulation order of network protocols, with the traffic statistics of each protocol node, including the packets statistics, bytes statistics, bit rate, and traffic percentages. With protocol analysis, you can easily find the applications with largest traffic volume so as to assist you in troubleshooting the network.

Process analysis

Capsa provides a Process view, which provides traffic statistics for local processes, including total bytes, packets, Bps, bps, pps, path, etc. You can double-click a process to view all packets for that process. Also a Process Explorer is provided to group the processes, listing the process name and process ID in a tree-like structure. A Process column is provided for TCP Conversation view and UDP Conversation view to show the process name of that TCP/UDP conversation, which helps users troubleshoot quickly.

Application analysis

The application analysis is able to show all the traffic statistics for applications, including total bytes, packets, Bps, bps, pps, etc. Once an application is selected, the lower pane will show protocol and conversation information related to that application. Double-click an application, the Packet Decoding window will open to show packets related to that application.

Conversation analysis

Capsa provides four types of conversation analysis: MAC conversation which is conversation between MAC addresses, IP conversation, TCP conversation, and UDP conversation. Each type of conversation is provided with source address, destination address, packets as well as bytes for the conversation, start time as well as end time, and conversation duration.

TCP transaction analysis

Capsa presents a comprehensive high-level overview of health of applications on your network. From TCP transaction analysis, you can drill down to access more detailed information, including TCP server/client response time, delay, retransmissions, and further down to the server flow to observe the actual content of the flow. This unparalleled level of control and visibility speeds time to application problem resolution and minimize overall network downtime.

Detailed decoding

A decoding view is provided to display the detailed decoding information of all packets, including summary decoding, field decoding, hexadecimal decoding, ASCII and EBCDIC decoding. With the decoding information, you can know the original data transmitted over the network.

Flexible reports

A report contains the statistic information of summary statistics, protocol statistics, and top 10's traffic. In addition, you can make a report not only on the whole network but also on a specific node.

Real-time alarms

Alarms can be defined to inform you network anomalies based on various traffic parameters, including the traffic, the packet size, the utilization, protocols, conversations, applications, and many other parameters. In addition, the alarms can be defined both on the global network and on a specific node. When the alarms are triggered, a notification pops up and a sound generates to get you know the anomalies immediately. Besides, the triggered alarms can be notified with emails to get you know the details even if you are not around the computer.

Log analysis

Network communications analyzed by advanced analysis modules can be recorded and displayed in a form of logs, including HTTP request and reply logs, DNS query logs, email sending and receiving logs, FTP file transfer logs, and instant messenger information logs. Furthermore, the Email logs can not only record the sending and receiving actions but save the copies of the email content, including its body and all the attachments. In addition, all the logs can be saved automatically, into one file or multiple files according to time length or the size.

HTTPS decryption

Capsa enables users to decrypt the HTTPS message with the right configuration of key file. There are three common decryption method: RSA, PSK, and (P)MS log file. Capsa support all of these three methods. Users could choose either to edit the RSA key list, to use a PSK, import a (P)MS log file, or even use them all at the same time for the decryption.

Protocol customization

Capsa recognizes more than 1,700 protocols and sub-protocols. You can easily create signatures to recognize new protocols to your specific needs. You can customize protocols by Ethernet type, IP encapsulated protocol ID, TCP port and UDP port.

Application customization

Capsa has more than 1,800 system applications. Capsa also allows you to create signatures to identify new applications to your specific needs. You can customize applications by protocol, port, pattern, IP address, IP address pair, IP address + protocol, address + port, client + server, and address + port + pattern.

Port number based statistics

A Port view is provided to present traffic statistics based on TCP/UDP port numbers. This feature is useful when you want to analyze a specific application. The port numbers are provided with above layer protocol, packets, bytes, average packet size, and common application. All TCP and/or UDP conversations are recorded for selected port number.

Easy-to-use display filter

Besides the capture filter, Capsa provides display filters to display interested items. The simple display filter is based on the field columns on the statistical views. An advanced display filter is available for the Packet view to display-screen out uninterested packets based on the protocol fields of a packet. The advanced display filter can even display the packets of specified time range.

System Specifications

Capsa is a network management solution which integrates traffic capture, analysis and statistics, and performance evaluation, to thus help network administrators troubleshoot the network, ensure the network security, enhance the network performance, and maximize the network value. The following lists describe the main system specifications.

Comprehensive traffic statistics

- Total network traffic summary
- Total network traffic volume
- Broadcast traffic volume
- Multicast traffic volume
- Internal traffic volume
- Traffic volume of an IP address
- Traffic volume of a MAC address
- Traffic volume of a segment
- Traffic volume of a VLAN
- Traffic volume of an application (protocol)
- Downlink traffic volume
- Uplink traffic volume
- Downlink packets quantity
- Uplink packets quantity
- Total packets quantity
- Physical layer conversation statistics
- IP layer conversation statistics
- TCP conversation statistics
- UDP conversation statistics
- Packets per second (pps) statistics
- Inbound/outbound traffic
- Inbound/outbound packet ratio
- IP country group
- Alarms on traffic, protocols
- Port based statistics
- Top domain name statistics

Protocol analysis

- Identify user-defined protocol
- Identify network service
- Analyze network service
- Analyze bandwidth consumption
- Summarize application packets
- Locate hosts running a specific service
- Decode protocol with Hex, ASCII and EBCDIC
- Identify abnormal protocol
- Identify packets with forged data
- Display protocol in OSI 7 layer structure

Conversation analysis

- Conversation between MAC addresses
- Conversation between IP addresses
- TCP conversation
- Reconstruct TCP communication
- TCP transactions
- UDP traffic
- BitTorrent traffic
- Network communication in matrix map
- TCP time sequence diagram

Performance evaluation

- Evaluate outbound bandwidth demand
- Evaluate outbound bandwidth utilization
- Evaluate internal bandwidth usage
- Evaluate packet size distribution
- Evaluate network upgrade performance
- Analyze TCP transaction performance
- Evaluate critical business traffic and non-business traffic
- Evaluate network transmission performance
- Baseline network performance
- In-depth analysis of application performan

Product Specifications

Supported network types

- Ethernet
- Fast Ethernet
- Gigabit Ethernet

Supported network adapters

- 10/100/1000 Mbps Ethernet adapters

System requirements

Operating systems

- Windows Server 2008 (64-bit)
- Windows Server 2012 (64-bit)*
- Windows Vista (64-bit)
- Windows 7 (64-bit)
- Windows 8/8.1 (64-bit)
- Windows 10 Professional (64-bit)

*indicates that Colasoft Packet Builder is not compatible with this operating system.

Minimum

- CPU: P4 2.8 GHz
- RAM: 4 GB
- 100 MB free disk space
- Internet Explorer 6.0

Recommended

- CPU: Intel Dual-Core 3.2 GHz
- RAM: 8 GB or more
- 10 GB additional space for packet files and logs
- Internet Explorer 8.0 or higher

Supported packet file formats

Supported packet file formats to replay

- Accellent 5Views Packet File (*.5vw)
- Colasoft Packet File (*.cscpkt; *rapkt; *.rawpkt; *.cacproj)
- EtherPeek Packet File (V7/V9) (*.pkt)
- HP Unix Nettl Packet File (*.TRCO; TRC1)
- Libpcap (Wireshark, Tcpdump, Ethereal, etc.) (*.cap; *pcap)
- Wireshark (Wireshark, etc.) (*.pcapang; *pcapang.gz; *.ntar; *.ntar.gz)

- Microsoft Network Monitor 1.x 2.x (*.cap)
- Novell LANalyer (*.tr1)
- Network Instruments Observer V9.0 (*.bfr)
- NetXRay 2.0, and Windows Sniffer (*.cap)
- Sun_Snoop (*.Snoop)
- Visual Network Traffic Capture (*.cap)

Supported packet file formats to export

- Accellent 5Views Packet File (*.5vw)
- Colasoft Packet File (V3) (*.rapkt)
- Colasoft Packet File (*.cscpkt)
- Colasoft Raw Packet File (*.rawpkt）
- Colasoft Raw Packet File (V2) (*.rawpkt）
- EtherPeek Packet File (V9) (*.pkt)
- HP Unix Nettl Packet File (*.TRCO; *.TRC1)
- Libpcap (Wireshark, Tcpdump, Ethereal, etc.) (*.cap; *pcap)
- Wireshark (Wireshark, etc.) (*.pcapang; *pcapang.gz; *.ntar; *.ntar.gz)
- Microsoft Network Monitor 1.x 2.x (*.cap)
- Novell LANalyer (*.tr1)
- NetXRay 2.0, and Windows Sniffer (*.cap)
- Sun_Snoop (*.Snoop)
- Visual Network Traffic Capture (*.cap)

Supported protocols

Capsa supports 1776 protocols and sub-protocols. The following are the supported application layer protocols.

MiNT, MIPv6, MONGO, MSDP, Netsync, MSNMS, NBDS, OLSR, OMAPI, OPSI, PacketBB, PCEP, PCP, PGSQL, PKTC, PULSE, QUAKE, QUAKE2, QUAKE3, QUAKEWORLD, RDT, Rlogin, RSIP, RSYNC, SAMETIME, SCoP, SEBEK, SIGCOMP, SIR, SliMP3, SMRSE, SMUX, Socks, SoulSeek, SPDY, SRVLOC, T.38, Tetra, TFP, TNS, TPCP, TPNCP, TZSP, UDPENCAP, ULP, VICP, WASSP, WINS-Replication, WoW, WTLS, X11, XDMCP, XMPP, XOT, XYPLEX, ZEP, AllJoyn NS, MRP-MMRP, MRP-MSRP, MRP-MVRP, NSRP, ROHC, Roofnet, RTcfg, Rtmac, SERCOS III V1.1, SNAETH, TDMoE, TELKONET, TIPC, TRILL, TTE PCF, VMLAB, VNTAG, WAI, WRETH, WSMP, swIPe, UDPlite, XTP, HOPOPT, ST, BBN-RCC-MON, NVP-II, ARGUS, EMCON, XNET, MUX, DCN-MEAS, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, MFE-NSP, MERIT-INP, 3PC, IDRP-CMTP, TPPP, IL, IPv6-Route, IPv6-Frag, BNA, I-NLSP, MOBILE, IPv6-NoNxt, IPv6-Opts, AHIP, ALN, SAT-EXPAK, SAT-MON, KRYPTOLAN, RVD, IPPC, ADFS, VISA, IPCU, CPNX, CPHB, WSN, BR-SAT-MON, SUN-ND, WB-MON, WB-EXPAK, VMTP, SECURE-VMTP, VINES, TTP, IPTM, NSFNET-IGP, DGP, TCF, Sprite-RPC, LARP, MTP, AX.25, IPIP, MICP, SCC-SP, ENCAP, APES, GMTP, IFMP, PNNI, ARIS, SCPS, QNX, A/N, IPComp, Compaq-Peer, IPX-in-IP, 0-hop, DDX, IATP, STPoIP, UTI, SM, IS-IS over IPv4, FIRE, SSCOPMCE, IPLT, RSVP-E2E-IGNORE, Mobility Header, MPLS-in-IP, manet, Shim6, WESP, DCE, FSPFoE, IEN, DOSP, DRCP, RBCP, BSP, MVP, IETF-TRILL, HDBTCMP, HCfB, GHP, AES50-2005, TPC, ES, IN, MXSP, WIO, STISA, TEP, VNTSMP, Eth-Trunks, MEF, NN, IEEE 802.1 ECP, IPDoE, IEN LAN-to-LAN, IEEE 802.1 CFM, MPLS-LS, IS-IS, EBP, VSP, XDP, DRP, FMACS, NMCS, NSMCP, MRP, LSPP, MACSP, MISIDRP, SET,

CPNSH, TCN, EoIB, MDC, REAC, PACU, TLDP, CDMA-ANI, XSHD, NC-SI, E-LMI, JRC-LTP, BCN, DOCSIS, DOCSIS MAC MGMT, DOCSIS B-INT-RNG-REQ, DOCSIS BPKM-REQ, DOCSIS BPKM-RSP, DOCSIS CM-CTRL-REQ, DOCSIS CM-CTRL-RSP, DOCSIS CM-STATUS, DOCSIS DBC-ACK, DOCSIS DBC-REQ, DOCSIS DBC-RSP, DOCSIS DCC-ACK, DOCSIS DCC-REQ, DOCSIS DCC-RSP, DOCSIS DCD, DOCSIS DPV-REQ, DOCSIS DPV-RSP, DOCSIS DSA-ACK, DOCSIS DSA-REQ, DOCSIS DSA-RSP, DOCSIS DSC-ACK, DOCSIS DSC-REQ, DOCSIS DSC-RSP, DOCSIS DSD-REQ, DOCSIS DSD-RSP, DOCSIS INT-RNG-REQ, DOCSIS MAP, DOCSIS Mdd, DOCSIS REG-ACK, DOCSIS REG-REQ, DOCSIS Reg-Req-Mp, DOCSIS REG-RSP, DOCSIS Reg-Rsp-Mp, DOCSIS RNG-REQ, DOCSIS RNG-RSP, DOCSIS Sync, DOCSIS type29ucd, DOCSIS UCC-REQ, DOCSIS UCC-RSP, DOCSIS UCD, FNTP, MRME, HBLLVoE, IPMP, T-VLAN, WNSIA, N-Ring, CLP, TAEPoL, PXLVD, FCMP, APP, MMP, GAC, ZLLS, FLDP, CEC, TLP, PCCP, VARAN, RDMAoE, BTSI, 2dparityfec, EVRC, RTP PCMU, RTP LPC, RTP PCMA, RTP G.722, RTP L16, RTP QCELP, RTP CN, RTP MPA, FGP, PIPO, CALCAPP, SSP, NPMP-CONTROL, NPMP-DATA, CHARGEN, 3GPP M2AP, 3GPP RNA, 3GPP M3AP, SSHoSCTP, DSDC, DDDC, R14P, WebRTC DCEP, WebRTC String, WebRTC Binary Partial, WebRTC Binary, WebRTC String Partial, 3GPP PUA, WebRTC Binary Empty, WebRTC String Empty, 3GPP XwAP, 3GPP Xw-Control Plane, PPP ROHC-S, PPP ROHC-L, PPP OSI NL, PPP XNI, PPP DEC, PPP Appletalk, PPP IPX, PPP VJC, PPP VJU, PPP BRID, PPP STREAM, PPP Banyan Vines, PPP AppleTalk EDDP, PPP AppleTalk SB, PPP Multi-Link, PPP NETBIOS Fram, PPP Cisco Sys, PPP Ascom Timeplex, PPP LBLB, PPP SDTP, PPP DCA-RL, PPP 802.2 SNA, PPP SNA, PPP IPv6 HC, PPP KNX-BD, PPP Encryption, PPP ILE, PPP Muxing, PPP VSNP, PPP TNP, PPP SLCM, PPP CDP, PPP NTR, PPP STP, PPP EDP, PPP OSCP, PPP SNS, PPP ACSP, PPP MFTP, PPP CCCP, PPP EAP, PPP CNDP, PPP RefTek, PPP EMIT, PPP VSP, PPP TLSP, PPP OSI-NLCP, PPP ACP, PPP SPCP, PPP BVCP, PPP MLCP, PPP CSCP, PPP RLNCP, PPP SDCP, PPP ECP, PPP ILECP, PPP VSNCP, PPP TNCP, PPP SBCP, PPP CCP, PPP CDPC, PPP ACSPC, PPP SPAP, PPP POS.