Network Problem Diagnosis with OSA Examples

David J Cheng

Applied Expert Systems, Inc.

davec@aesclever.com

March 3, 2011, 1:30PM
Session 8200

Agenda

- z/OS: CTRACE
  - Packet Trace
  - OSAENTA
- Linux, Unix/AIX: tcpdump
- TCP/IP
- Sample Cases
  - OSA
    - Excessive / Dropped packets, addressing errors
    - Checksum offloading
  - FTP – flow analysis
  - AT-TLS – flow analysis

Copyright © 2011 Applied Expert Systems, Inc.

How to Take a Packet Trace?

z/OS CTRACE:

- SYSTCPDA - Packet Trace; scope is the TCP/IP stack
- SYSTCPOT – OSAENTA; scope is LPAR or CHPID

- Set up an External Writer Proc

E.g., SYS1.PROCLIB(AESWRT):

```
//IEFPROC EXEC PGM=ITTTRCWR,REGION=0K,TIME=1440,DPRTY=15
//TRCOUT01 DD DISP=SHR,DSN=trace.dataset
```

- Set up tracing parameters

E.g., SYS1.PARMLIB(CTAESPRM):

```
TRACEOPTS ON WTR(AESWRT)
```


Copyright © 2011 Applied Expert Systems, Inc.

z/OS CTRACE: SYSTCPDA

- *To Start Tracing:*

```
TRACE CT,WTRSTART=AESWRT
V TCPIP,,PKT,CLEAR
V TCPIP,,PKT,LINKN=<link>,ON,FULL,PROT=TCP,IP=<ip addr>
TRACE CT,ON,COMP=SYSTCPDA,SUB=(TCPIP),PARM=CTAESPRM
```

- *To Stop Tracing:*

```
V TCPIP,,PKT,OFF
TRACE CT,OFF,COMP=SYSTCPDA,SUB=(TCPIP)
TRACE CT,WTRSTOP=AESWRT,FLUSH
```

- *To View Tracing Status:*

```
D TRACE,WTR=AESWRT
```

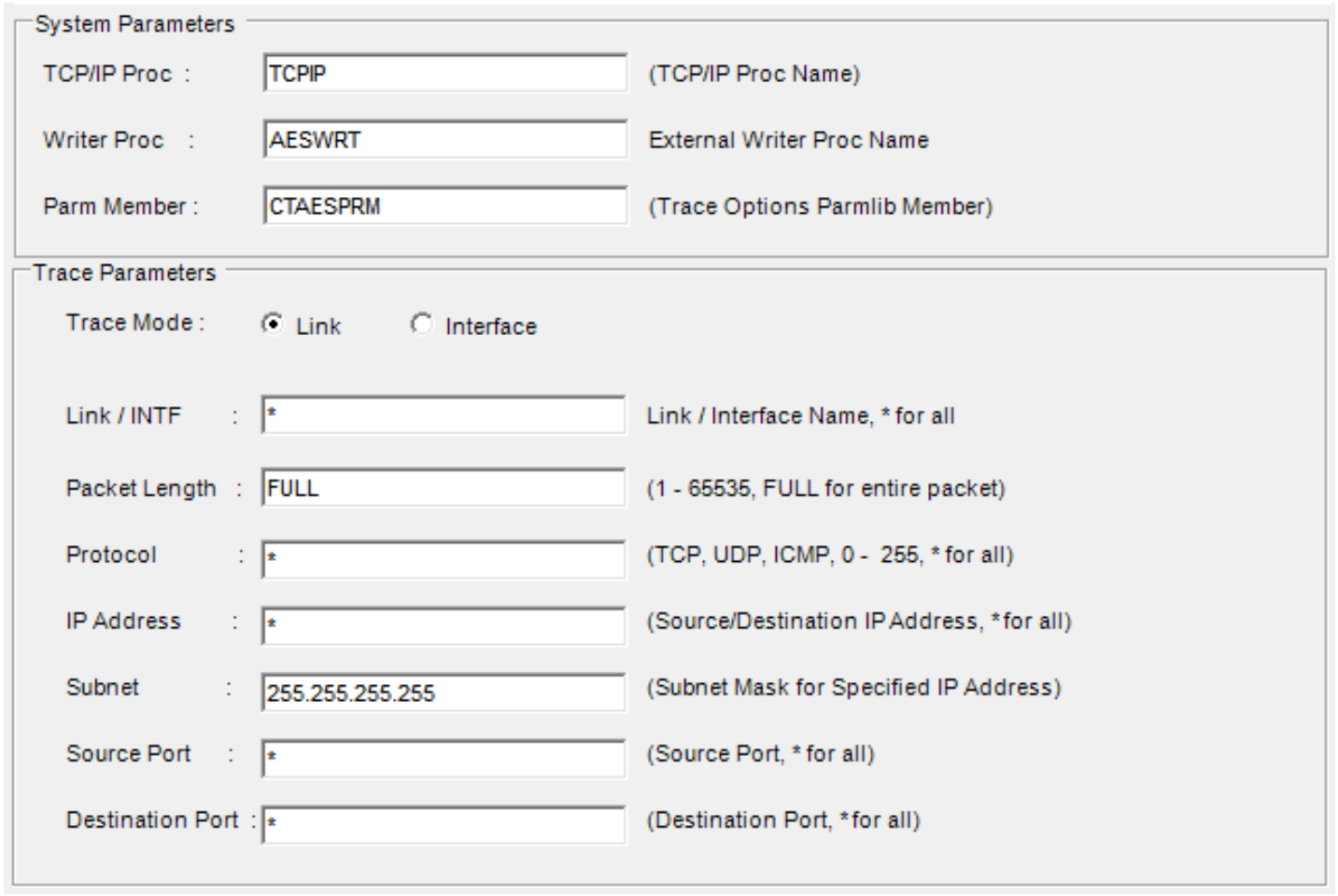
Verify that the external writer is active

```
D TCPIP,,NETSTAT,DE
```

Verify that **TrRecCnt** is non-zero and incrementing

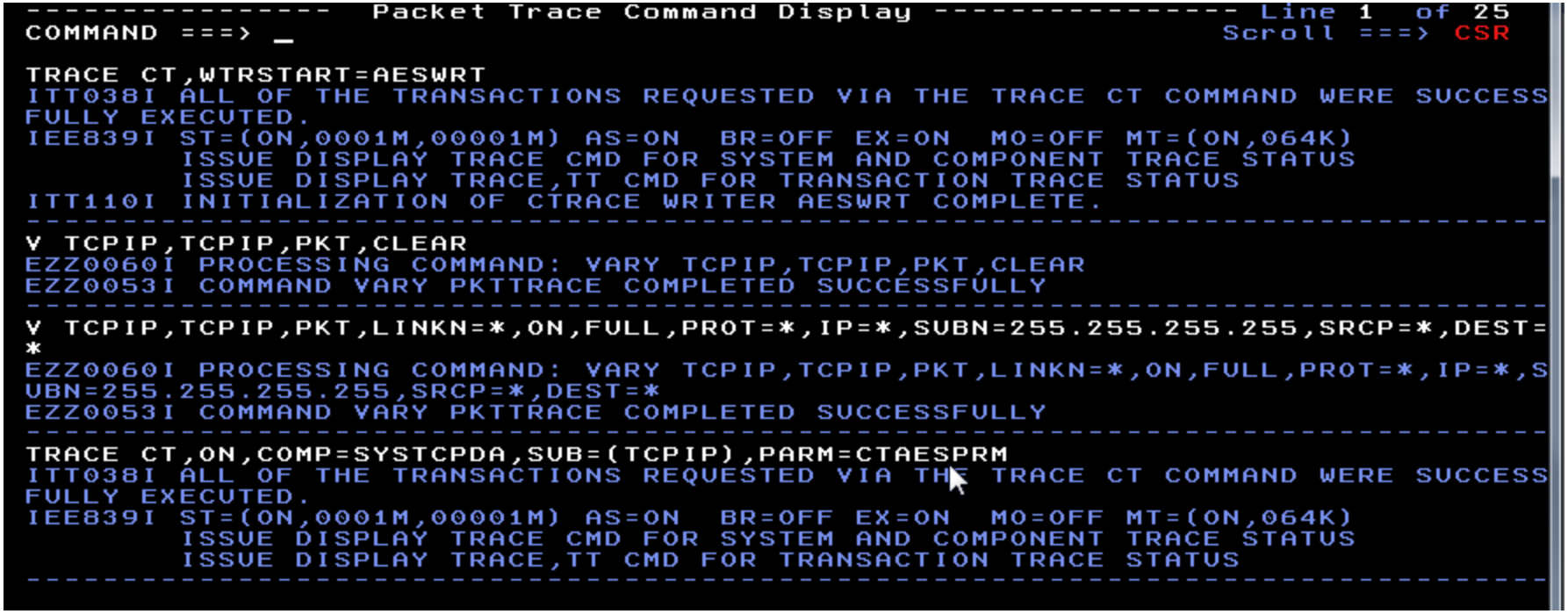
Copyright © 2011 Applied Expert Systems, Inc.

z/OS CTRACE: SYSTCPDA Parameters



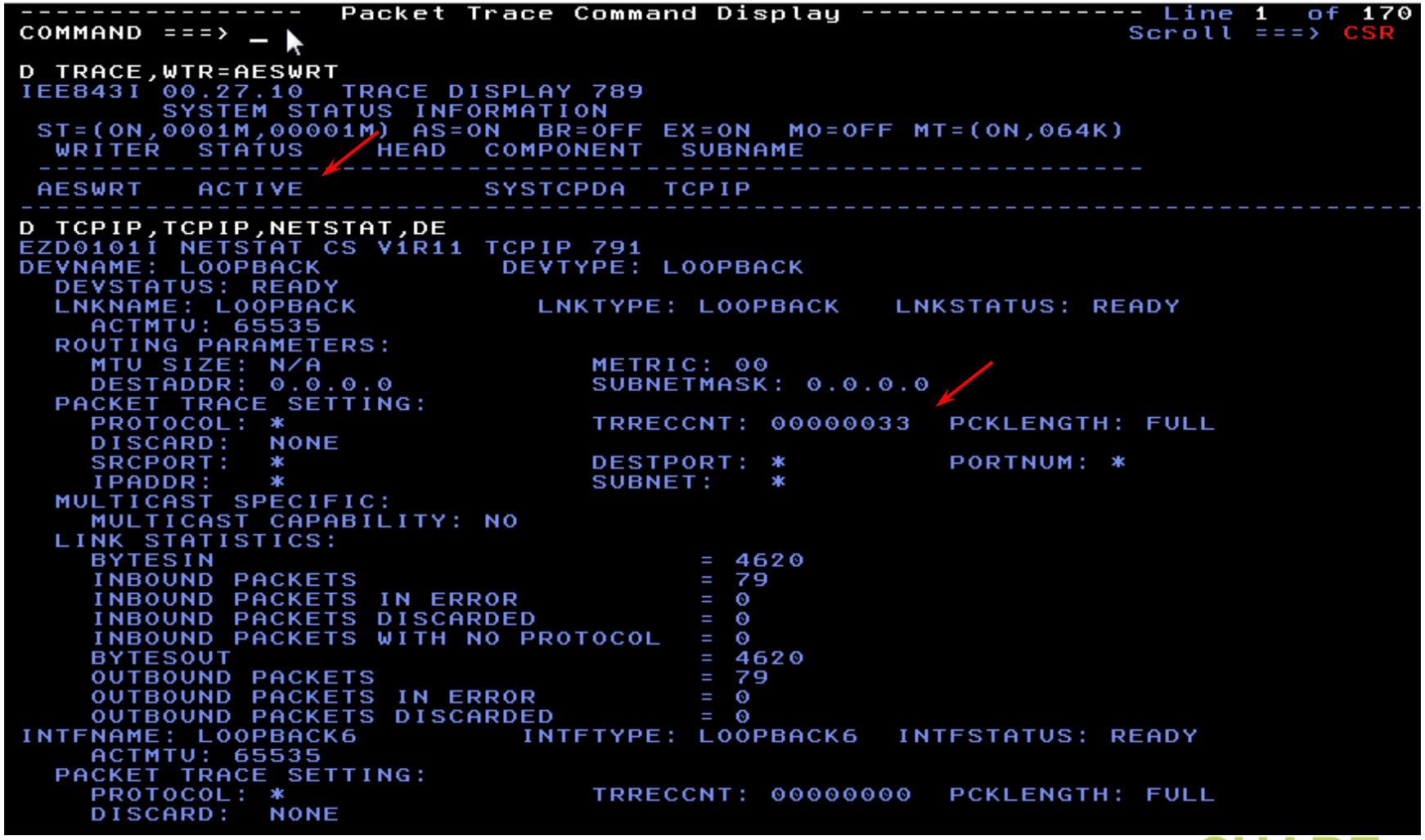
Copyright © 2011 Applied Expert Systems, Inc.

z/OS CTRACE: SYSTCPDA
Starting a Trace



Copyright © 2011 Applied Expert Systems, Inc.

z/OS CTRACE: SYSTCPDA
Checking Trace Status



Copyright © 2011 Applied Expert Systems, Inc.

z/OS CTRACE: SYSTCPDA
Stopping a Trace

```
---------------  Packet Trace Command Display ---------------- Line 1  of 19
COMMAND ===> _                                                Scroll ===> CSR

V TCPIP,TCPIP,PKT,OFF
EZZ0060I PROCESSING COMMAND: VARY TCPIP,TCPIP,PKT,OFF
EZZ0053I COMMAND VARY PKTTRACE COMPLETED SUCCESSFULLY
--------------------------------------------------------------------------------
TRACE CT,OFF,COMP=SYSTCPDA,SUB=(TCPIP)
ITT038I ALL OF THE TRANSACTIONS REQUESTED VIA THE TRACE CT COMMAND WERE SUCCESS
FULLY EXECUTED.
IEE839I ST=(ON,0001M,00001M) AS=ON  BR=OFF EX=ON  MO=OFF MT=(ON,064K)
        ISSUE DISPLAY TRACE CMD FOR SYSTEM AND COMPONENT TRACE STATUS
        ISSUE DISPLAY TRACE,TT CMD FOR TRANSACTION TRACE STATUS
--------------------------------------------------------------------------------
TRACE CT,WTRSTOP=AESWRT,FLUSH
ITT038I ALL OF THE TRANSACTIONS REQUESTED VIA THE TRACE CT COMMAND WERE SUCCESS
FULLY EXECUTED.
IEE839I ST=(ON,0001M,00001M) AS=ON  BR=OFF EX=ON  MO=OFF MT=(ON,064K)
        ISSUE DISPLAY TRACE CMD FOR SYSTEM AND COMPONENT TRACE STATUS
        ISSUE DISPLAY TRACE,TT CMD FOR TRANSACTION TRACE STATUS
ITT111I CTRACE WRITER AESWRT TERMINATED BECAUSE OF A WTRSTOP REQUEST.
--------------------------------------------------------------------------------
```


Copyright © 2011 Applied Expert Systems, Inc.

z/OS CTRACE: SYSTCPOT

- OSA-Express Network Traffic Analyzer (OSAENTA)
  - Trace data is collected (by the device drivers of OSA) as frames enter or leave an OSA adapter for a connected host
  - The host can be an LPAR with **z/OS, z/VM** or **Linux**
  - ARP packets, MAC headers (w/VLAN tags)
  - The trace function is controlled by z/OS Communication Server, while the data is collected in the OSA at the network port

- Pre-Reqs:
  - Required the microcode for the OSA (2094DEVICE PSP and the 2096DEVICE PSP).
  - Update the OSA using the Hardware Management Console (HMC) to:

    Define more data devices to systems that will use the trace function.

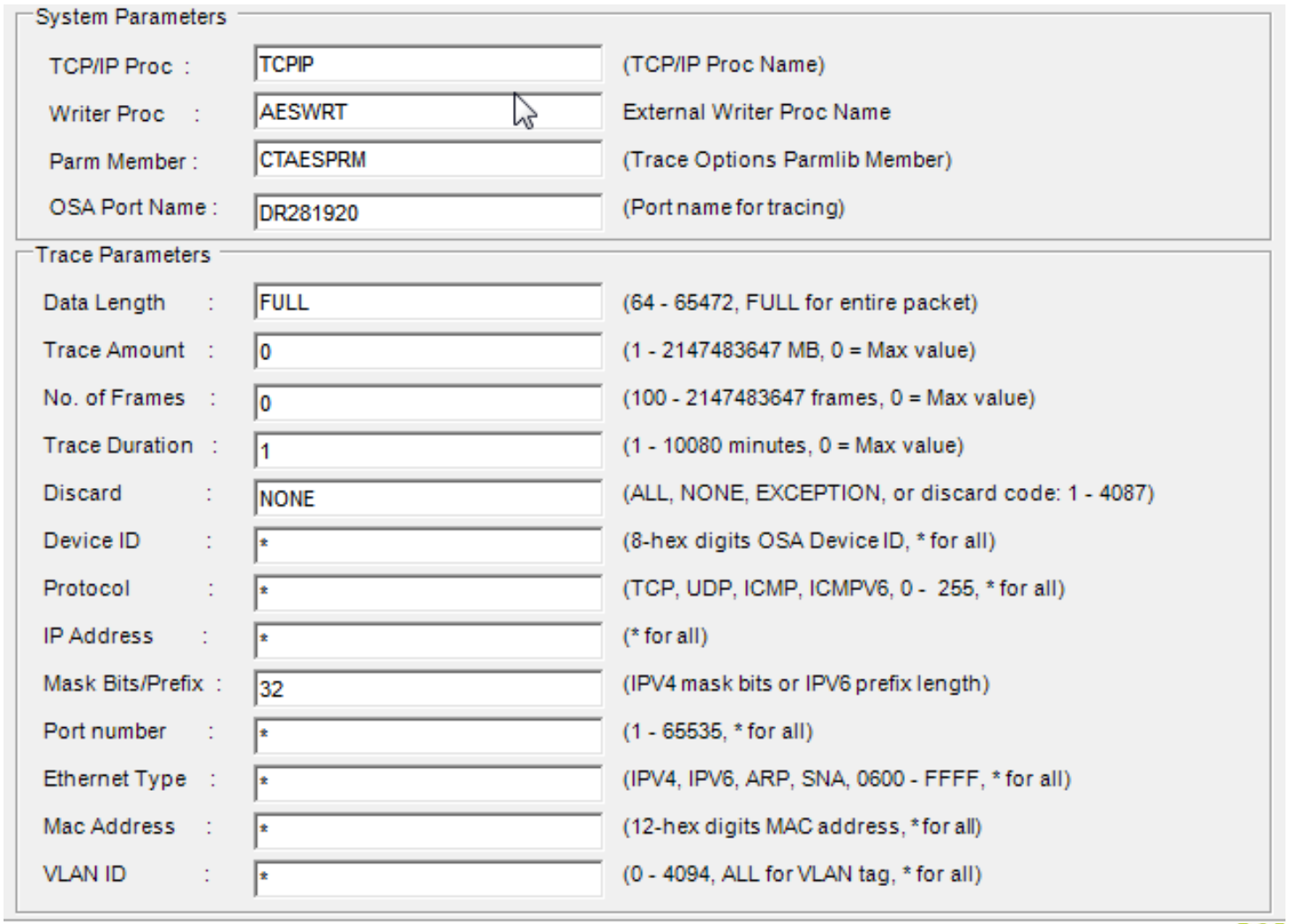
    Set the security for the OSA:

    LOGICAL PARTITION - Only packets from the LPAR

    CHPID - All packets using this CHPID
  - Verify the TRLE definitions for the OSA that it has one DATAPATH address available for tracing. Note that **two** DATAPATH addresses are required – one for data transfers and the other for trace data.

Copyright © 2011 Applied Expert Systems, Inc.

z/OS CTRACE: SYSTCPOT Parameters



Copyright © 2011 Applied Expert Systems, Inc.

z/OS CTRACE: SYSTCPOT

- *To Start Tracing*:

```
TRACE CT,WTRSTART=AESWRT
V TCPIP,,OSAENTA,PORTNAME=<port>,CLEAR
V TCPIP,,OSAENTA,PORTNAME=<port>,ON,NOFILTER=ALL
TRACE CT,ON,COMP=SYSTCPOT,SUB=(TCPIP),PARM=CTAESPRM
```

- *To Stop Tracing*:

```
V TCPIP,,OSAENTA,PORTNAME=<port>,OFF
TRACE CT,OFF,COMP=SYSTCPOT,SUB=(TCPIP)
TRACE CT,WTRSTOP=AESWRT,FLUSH
```

- *To View Tracing Status*:
  - `D TRACE,WTR=AESWRT` to verify that the external writer is active
  - `D TCPIP,,NETSTAT,DE` to check status

Copyright © 2011 Applied Expert Systems, Inc.

z/OS CTRACE: SYSTCPOT

- To View Tracing Status (continued):

```
D TCPIP,,NETSTAT,DE
 OSA-EXPRESS NETWORK TRAFFIC ANALYZER INFORMATION:
   OSA PORTNAME: DR281920           OSA DEVSTATUS:     READY
     OSA INTFNAME: EZANTADR281920   OSA INTFSTATUS:    READY
     OSA SPEED:    1000             OSA AUTHORIZATION: LOGICAL PARTITION
     OSAENTA CUMULATIVE TRACE STATISTICS:
       DATAMEGS:   1                  FRAMES:          3625
       DATABYTES:  1641283            FRAMESDISCARDED: 0
       FRAMESLOST: 0
     OSAENTA ACTIVE TRACE STATISTICS:
       DATAMEGS:   0                  FRAMES:          23
       DATABYTES:  6148               FRAMESDISCARDED: 0
       FRAMESLOST: 0                  TIMEACTIVE:      2
     OSAENTA TRACE SETTINGS:          STATUS: ON
       DATAMEGSLIMIT: 2147483647      FRAMESLIMIT:     2147483647
       ABBREV:        480             TIMELIMIT:       10080
       DISCARD:       NONE
     OSAENTA TRACE FILTERS:           NOFILTER: ALL
       DEVICEID: *
       MAC:      *
       VLANID:   *
       ETHTYPE:  *
       IPADDR:   *
       PROTOCOL: *
       PORTNUM:  *
```


Copyright © 2011 Applied Expert Systems, Inc.

Linux, Unix and AIX: tcpdump

- Requires root authority; use the “su” command first
- Output is formatted trace (default) or written to a pcap file
- tcpdump –w xyz.pcap
- tcpdump –v (sample output from SLES 11 on System z)

```
16:23:18.803265 IP (tos 0x10, ttl 64, id 63277, offset 0, flags [DF], proto TCP
(6), length 40) etpglsj.dal-ebit.ihost.com.ssh > 172.29.96.42.56570: ., cksum 0x
96e2 (correct), ack 2111375775 win 158
16:23:18.805880 IP (tos 0x10, ttl 64, id 63278, offset 0, flags [DF], proto TCP
(6), length 172) etpglsj.dal-ebit.ihost.com.ssh > 172.29.96.42.56570: P 0:132(13
2) ack 1 win 158
16:23:18.806155 IP (tos 0x0, ttl 64, id 51563, offset 0, flags [DF], proto UDP (
17), length 71) etpglsj.dal-ebit.ihost.com.33031 > ns.dfw.ibm.com.domain: 56736+
 PTR? 42.96.29.172.in-addr.arpa. (43)
16:23:18.808816 IP (tos 0x0, ttl 26, id 23382, offset 0, flags [none], proto UDP
 (17), length 148) ns.dfw.ibm.com.domain > etpglsj.dal-ebit.ihost.com.33031: 567
36 NXDomain 0/1/0 (120)
16:23:18.858199 IP (tos 0x0, ttl 127, id 1215, offset 0, flags [none], proto UDP
 (17), length 78) 172.29.96.56.netbios-ns > 172.29.191.255.netbios-ns: NBT UDP P
ACKET(137): QUERY; REQUEST; BROADCAST
16:23:18.858309 IP (tos 0x0, ttl 126, id 1215, offset 0, flags [none], proto UDP
 (17), length 78) 172.29.96.56.netbios-ns > 172.29.191.255.netbios-ns: NBT UDP P
ACKET(137): QUERY; REQUEST; BROADCAST
16:23:18.858548 IP (tos 0x0, ttl 64, id 51568, offset 0, flags [DF], proto UDP (
17), length 71) etpglsj.dal-ebit.ihost.com.55971 > ns.dfw.ibm.com.domain: 64720+
 PTR? 56.96.29.172.in-addr.arpa. (43)
16:23:18.859303 IP (tos 0x0, ttl 125, id 1215, offset 0, flags [none], proto UDP
 (17), length 78) 172.29.96.56.netbios-ns > 172.29.191.255.netbios-ns: NBT UDP P
```

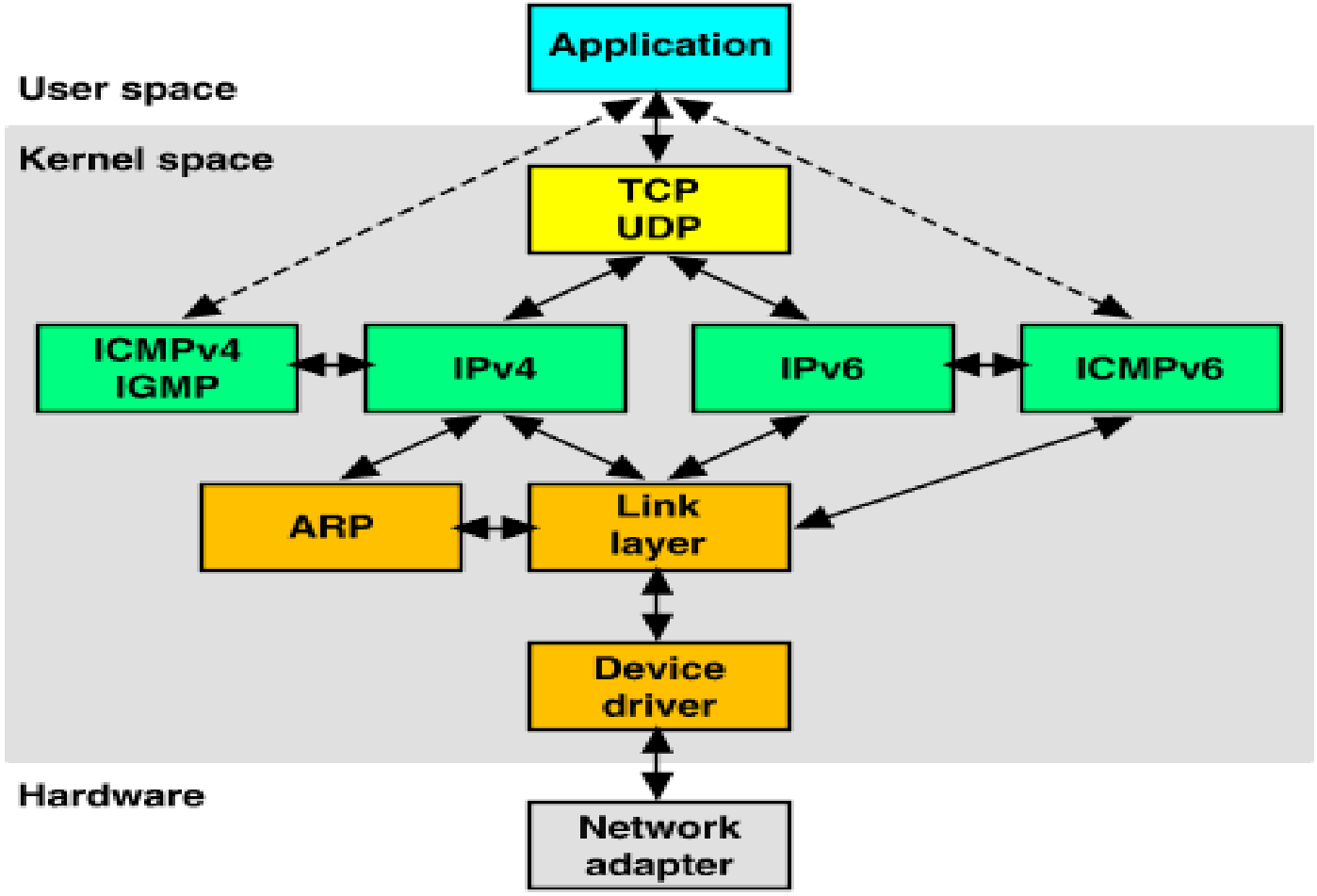

Copyright © 2011 Applied Expert Systems, Inc.

Know Your Protocols and Applications - TCP

- TCP Functions
  - Establish Connections
  - Manage Connections
  - Terminate Connections
  - Handling and Packaging Data
  - Transferring Data
  - Providing Reliability
  - Flow Control and Congestion Avoidance

Copyright © 2011 Applied Expert Systems, Inc.

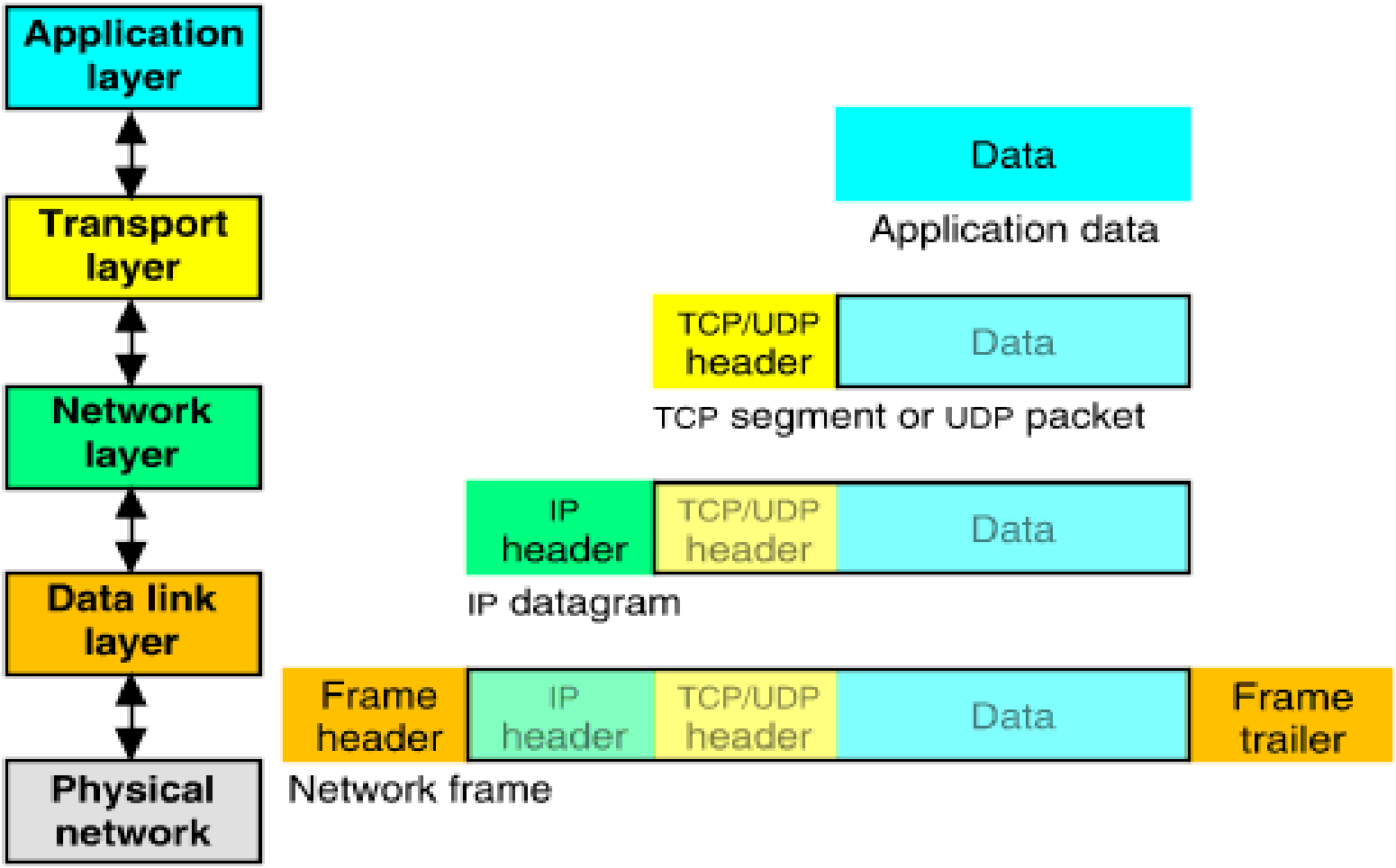
Networking Stack Support for TCP/IP



Source: http://uw713doc.sco.com/en/NET_tcpip/tcpN.tcpip_stack.html

Copyright © 2011 Applied Expert Systems, Inc.

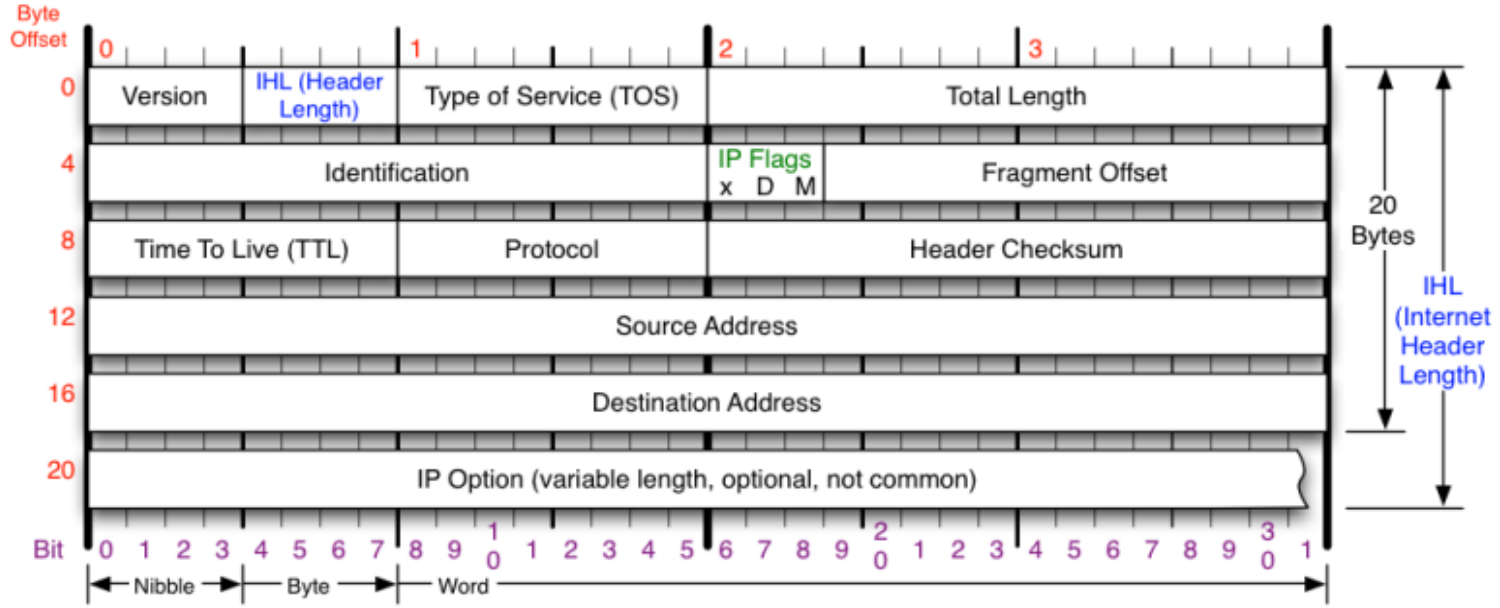
Encapsulation of Application Data within a Network Stack



Source: http://uw713doc.sco.com/en/NET_tcpip/tcpN.tcpip_stack.html

Copyright © 2011 Applied Expert Systems, Inc.

IP Header Format



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

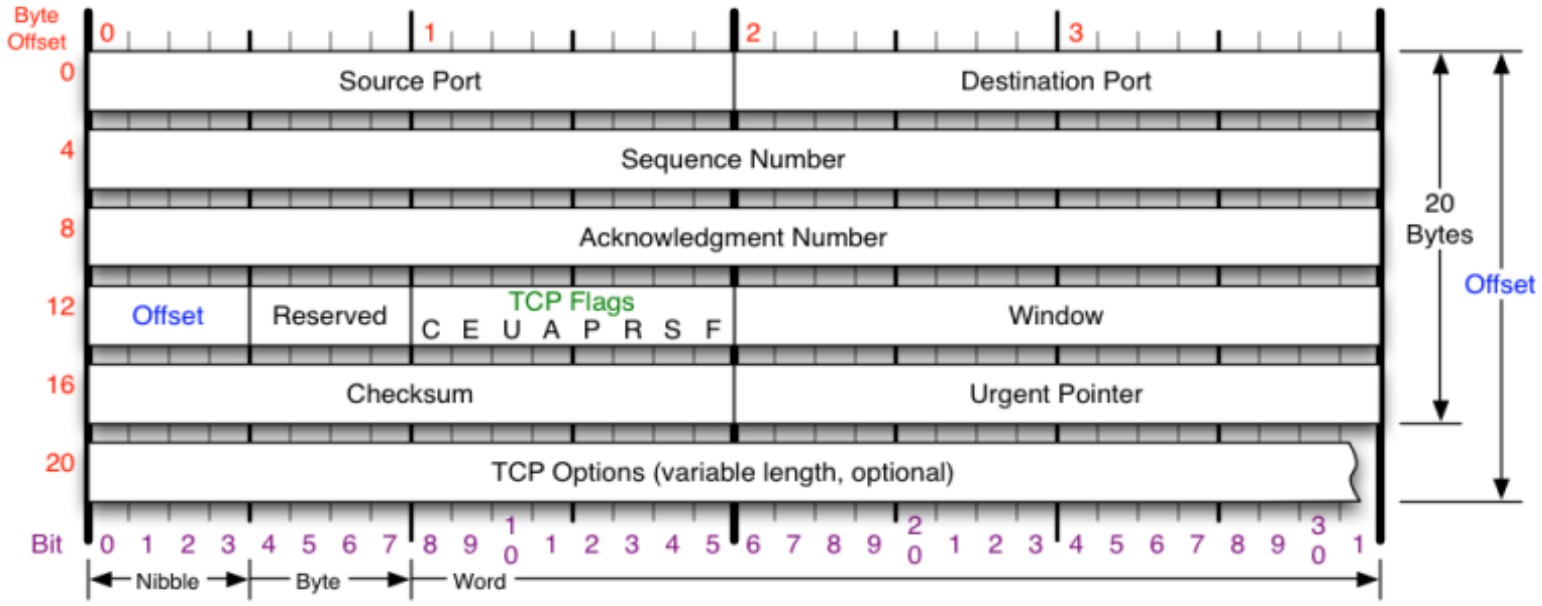
RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

Source: http://nmap.org/book/images/hdr/MJB-IP-Header-800x576.png

Copyright © 2011 Applied Expert Systems, Inc.

TCP Header Format



TCP Flags

C E U A P R S F

Congestion Window

C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

Offset

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

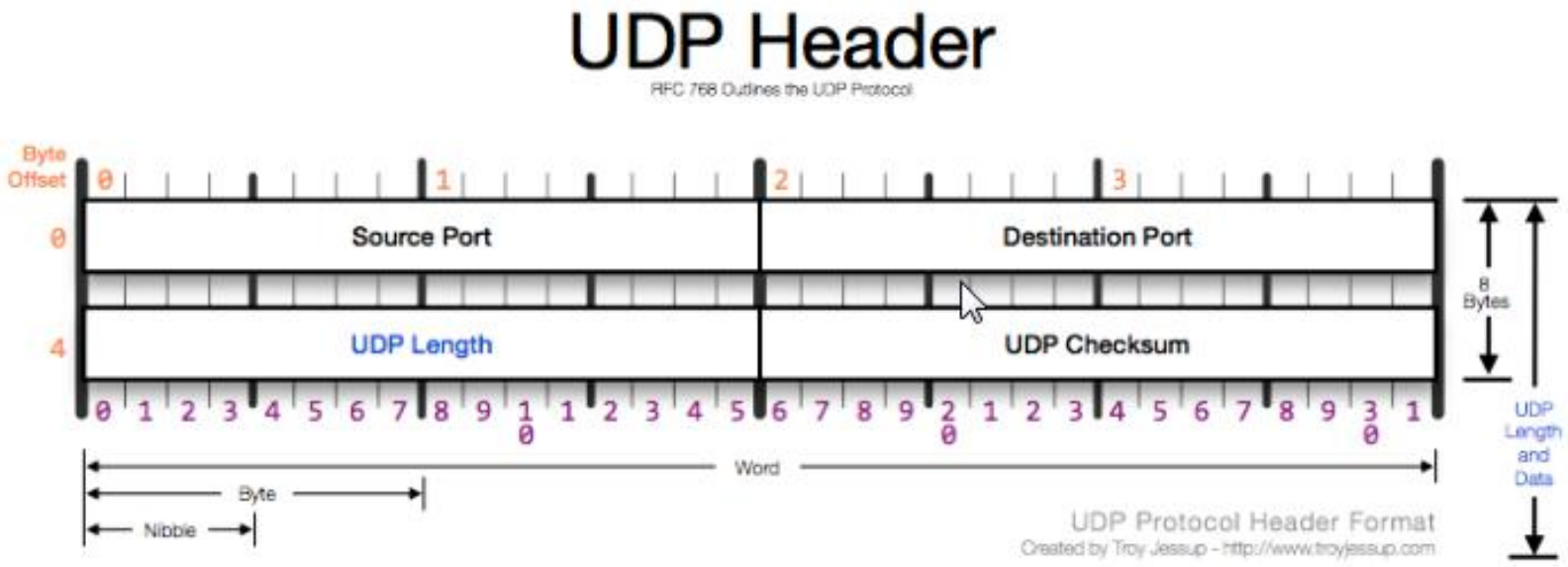
RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

Source http://nmap.org/book/images/hdr/MJB-TCP-Header-800x564.png

Copyright © 2011 Applied Expert Systems, Inc.

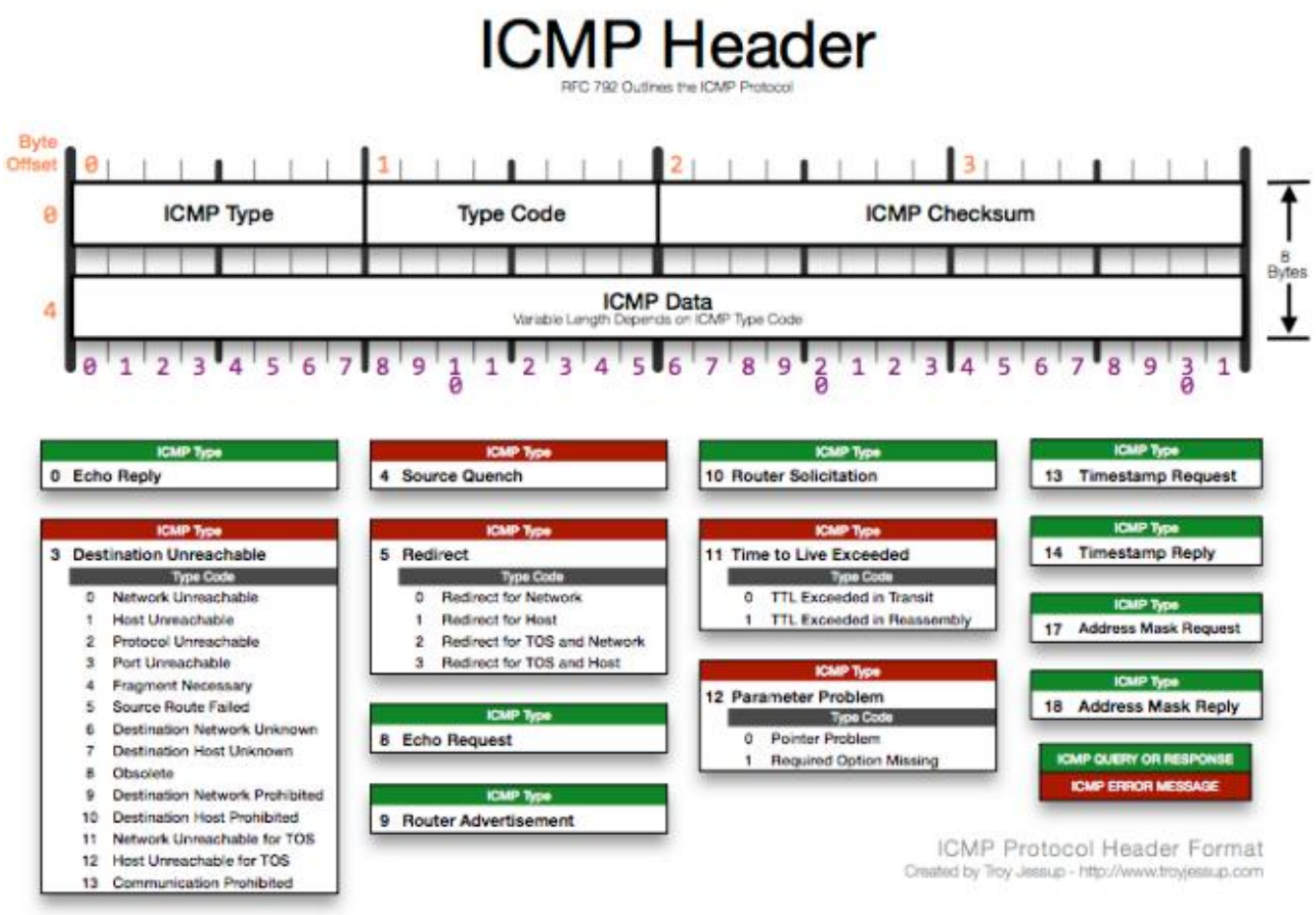
UDP Header Format



Source http://www.troyjessup.com/headers/UDP_Header.png

Copyright © 2011 Applied Expert Systems, Inc.

ICMP Header Format



Source http://www.troyjessup.com/headers/ICMP_Header.png

Copyright © 2011 Applied Expert Systems, Inc.

TCP Flags Explained

- ACK – Acknowledge receipt of the packet
- PSH – Push – Send the data (flush TCP buffer) immediately
- SYN – Synchronize Seq. Num. – Establish a connection
- FIN – Finish – Terminate the connection
- RST – Reset – Abnormal Session Disconnection
- URG – Urgent – Tell Receiver to process immediately

Copyright © 2011 Applied Expert Systems, Inc.

Sliding Window Acknowledgement

- **Advertised window size -** This field contains the amount of data that may be transmitted into the buffer.
- **Sequence number** – Identifies the first byte of data in this segment.
- **Acknowledgment number** – Identifies the next byte of data that a recipient is expecting to receive.
- With this information, a sliding-window protocol is implemented.

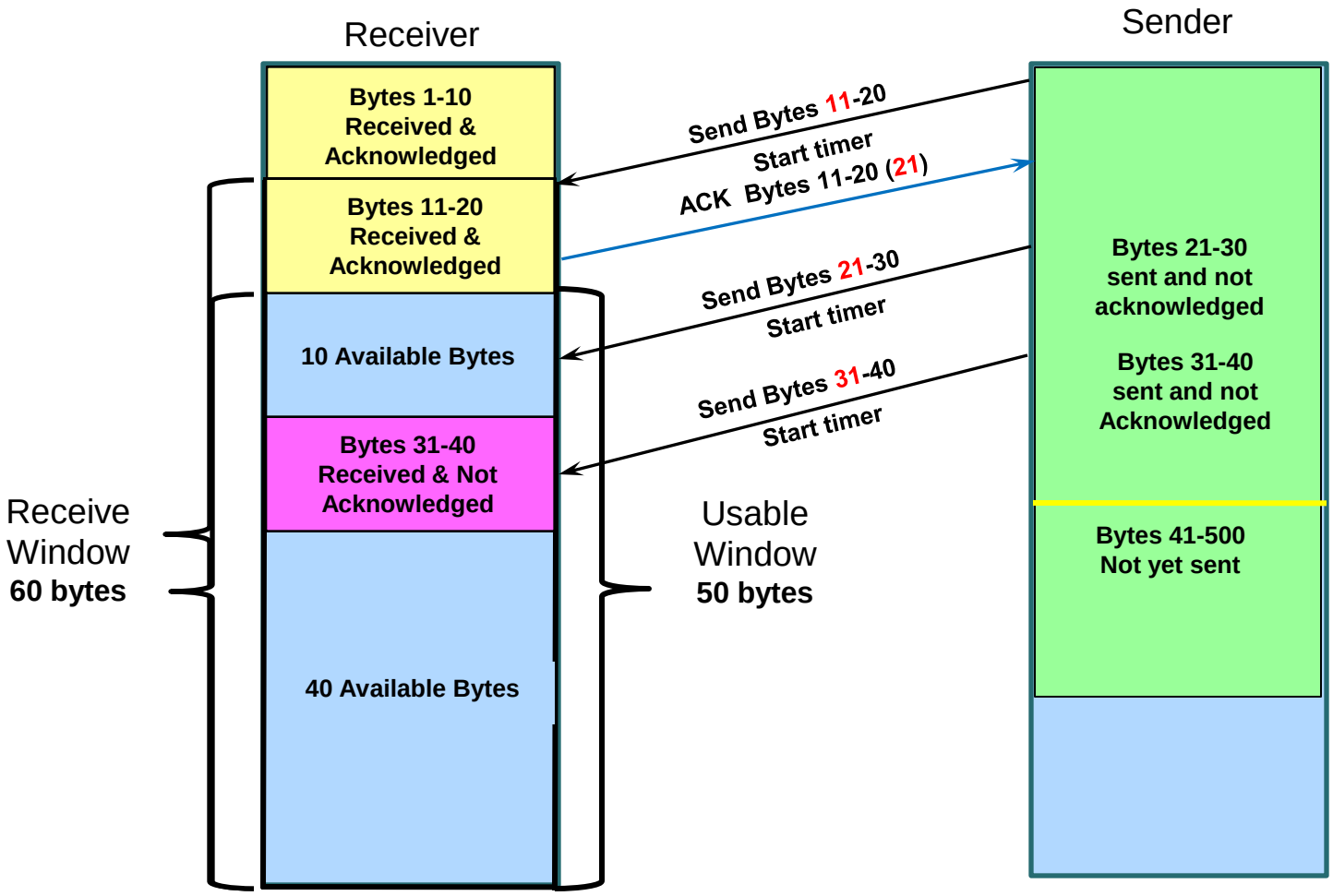
Copyright © 2011 Applied Expert Systems, Inc.

Sliding Window Acknowledgement

- Transmit categories
  1. Bytes Sent And Acknowledged
  2. Bytes Sent But Not Yet Acknowledged
  3. Bytes Not Yet Sent For Which Recipient Is Ready
  4. Bytes Not Yet Sent For Which Recipient Is Not Ready
- Receive categories
  1. Bytes Received And Acknowledged. This is the receiver's complement to Transmit Categories #1 and #2.
  2. Bytes Not Yet Received For Which Recipient Is Ready. This is the receiver's complement to Transmit Category #3.
  3. Bytes Not Yet Received For Which Recipient Is Not Ready. This is the receiver's complement to Transmit Category #4.

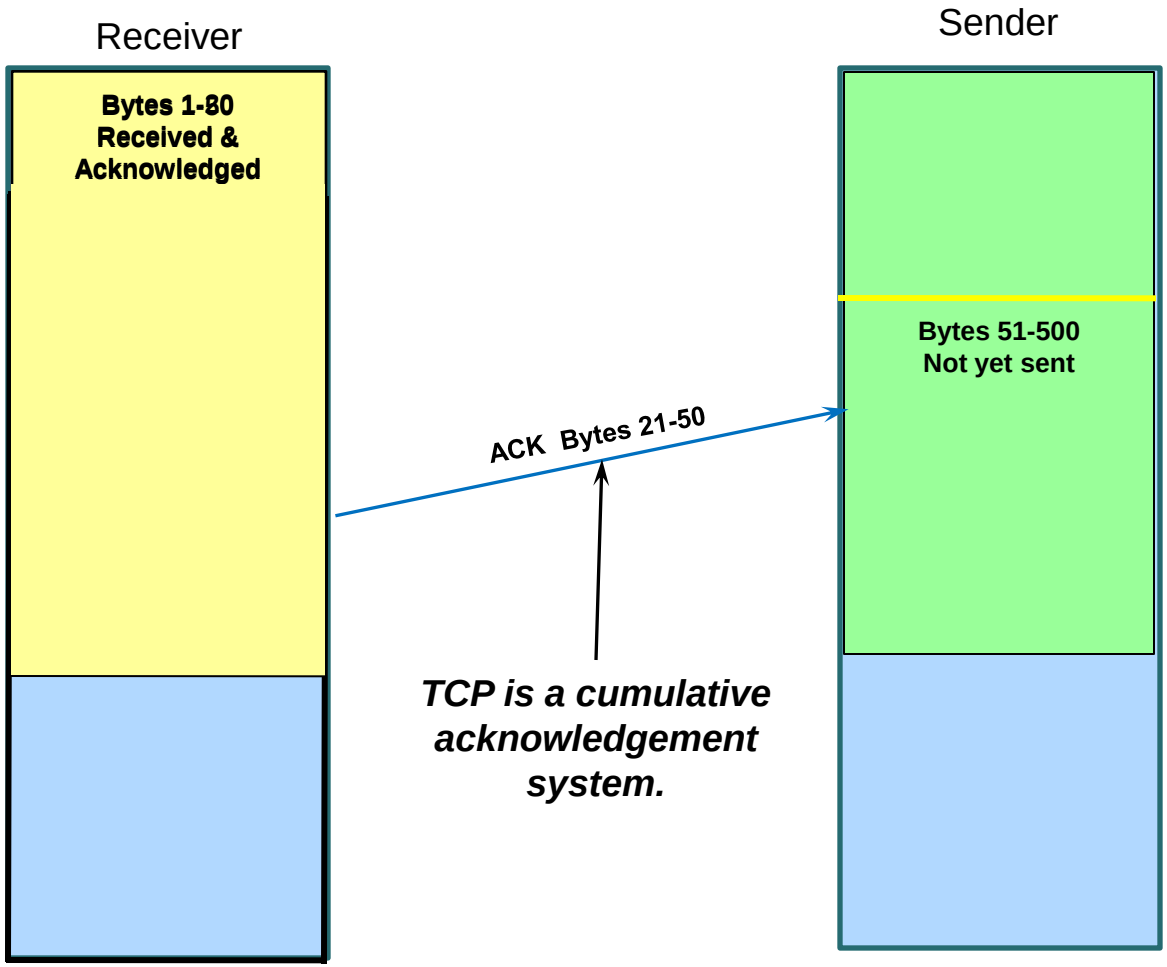
Copyright © 2011 Applied Expert Systems, Inc.

Sliding Window Acknowledgement



Copyright © 2011 Applied Expert Systems, Inc.

Sliding Window Acknowledgement



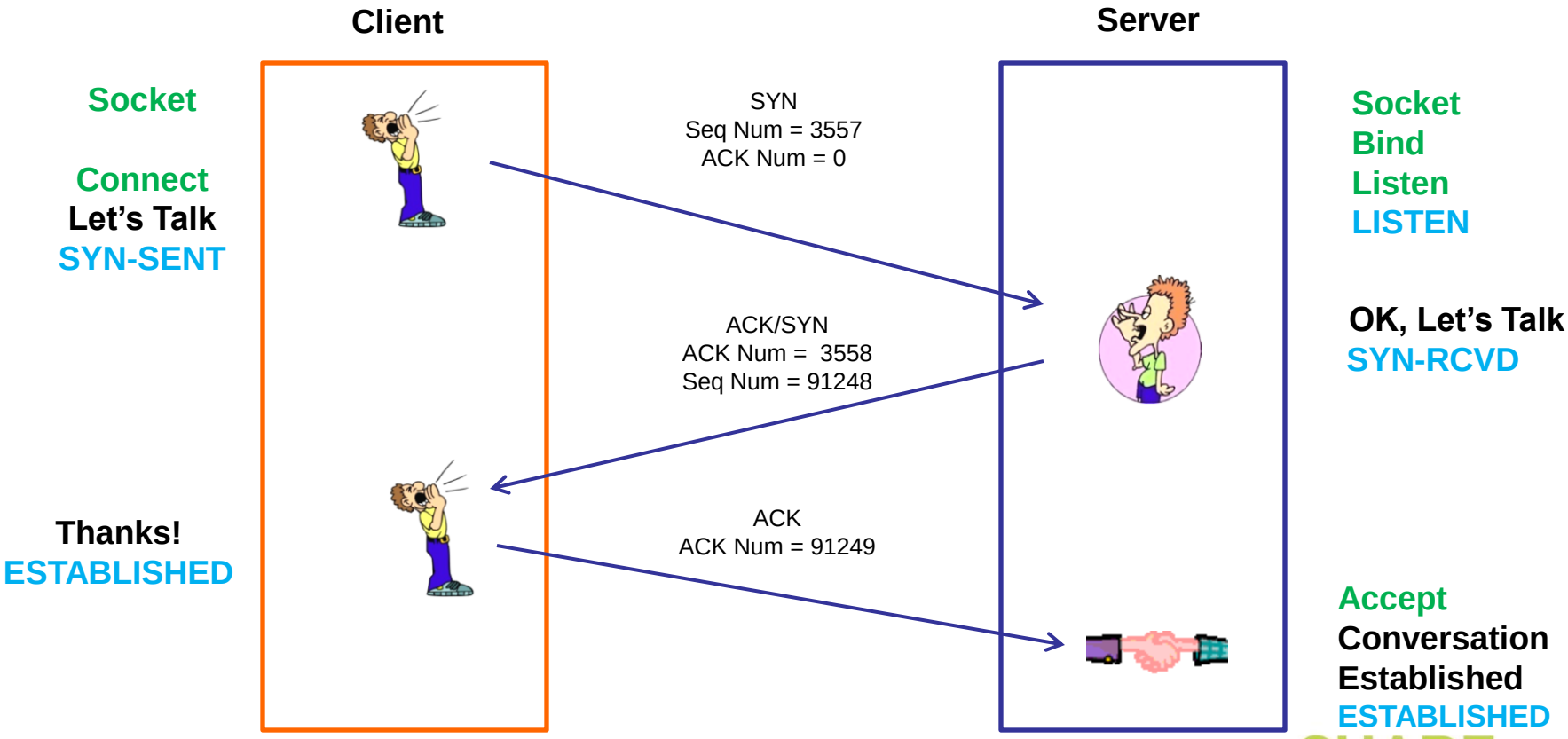
Copyright © 2011 Applied Expert Systems, Inc.

TCP Sequence of Events

- Establishing a connection
- Data transfer
- Termination

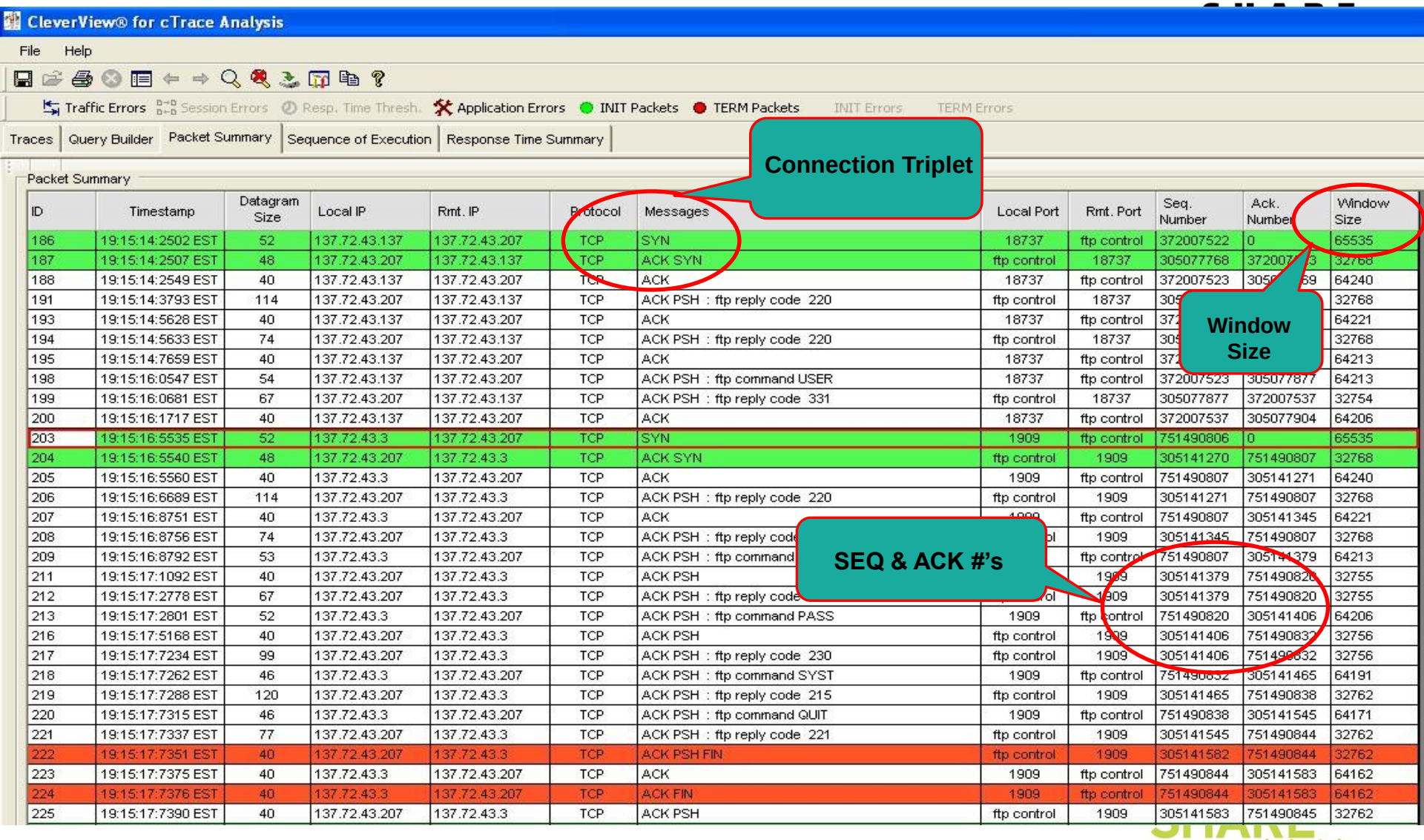
Copyright © 2011 Applied Expert Systems, Inc.

TCP - Establishing a Connection
The 3 Way Handshake



Copyright © 2011 Applied Expert Systems, Inc.

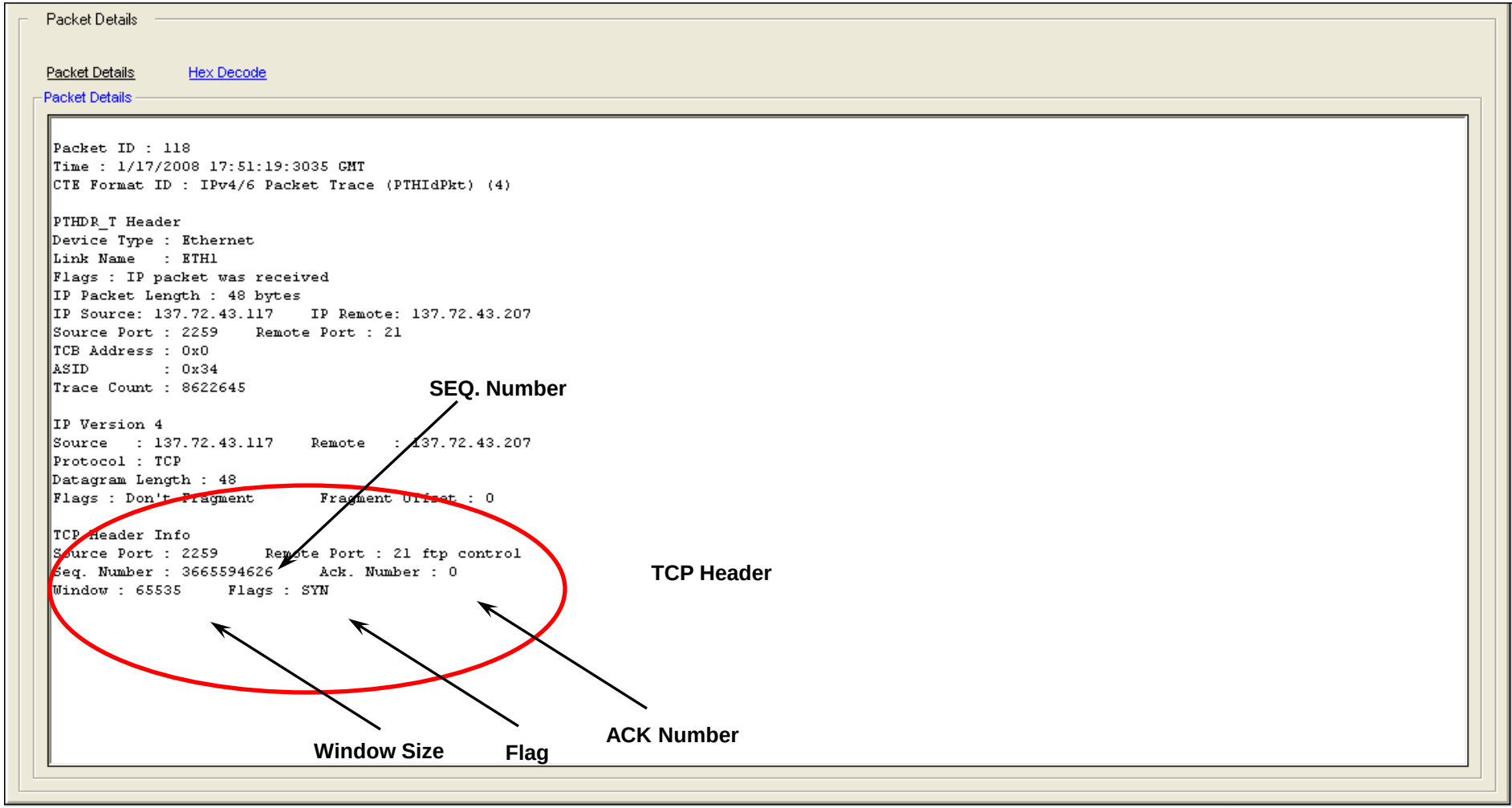
TCP - Establishing a Connection
The 3 Way Handshake



ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
186	19:15:14:2502 EST	52	137.72.43.137	137.72.43.207	TCP	SYN	18737	ftp control	372007522	0	65535
187	19:15:14:2507 EST	48	137.72.43.207	137.72.43.137	TCP	ACK SYN	ftp control	18737	305077768	372007523	32768
188	19:15:14:2549 EST	40	137.72.43.137	137.72.43.207	TCP	ACK	18737	ftp control	372007523	305077769	64240
191	19:15:14:3793 EST	114	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 220	ftp control	18737	305		32768
193	19:15:14:5628 EST	40	137.72.43.137	137.72.43.207	TCP	ACK	18737	ftp control	372		64221
194	19:15:14:5633 EST	74	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 220	ftp control	18737	305		32768
195	19:15:14:7659 EST	40	137.72.43.137	137.72.43.207	TCP	ACK	18737	ftp control	372		64213
198	19:15:16:0547 EST	54	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command USER	18737	ftp control	372007523	305077877	64213
199	19:15:16:0681 EST	67	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 331	ftp control	18737	305077877	372007537	32754
200	19:15:16:1717 EST	40	137.72.43.137	137.72.43.207	TCP	ACK	18737	ftp control	372007537	305077904	64206
203	19:15:16:5535 EST	52	137.72.43.3	137.72.43.207	TCP	SYN	1909	ftp control	751490806	0	65535
204	19:15:16:5540 EST	48	137.72.43.207	137.72.43.3	TCP	ACK SYN	ftp control	1909	305141270	751490807	32768
205	19:15:16:5560 EST	40	137.72.43.3	137.72.43.207	TCP	ACK	1909	ftp control	751490807	305141271	64240
206	19:15:16:6689 EST	114	137.72.43.207	137.72.43.3	TCP	ACK PSH : ftp reply code 220	ftp control	1909	305141271	751490807	32768
207	19:15:16:8751 EST	40	137.72.43.3	137.72.43.207	TCP	ACK	1909	ftp control	751490807	305141345	64221
208	19:15:16:8756 EST	74	137.72.43.207	137.72.43.3	TCP	ACK PSH : ftp reply code	ol	1909	305141345	751490807	32768
209	19:15:16:8792 EST	53	137.72.43.3	137.72.43.207	TCP	ACK PSH : ftp command		ftp control	751490807	305141379	64213
211	19:15:17:1092 EST	40	137.72.43.207	137.72.43.3	TCP	ACK PSH		1909	305141379	751490820	32755
212	19:15:17:2778 EST	67	137.72.43.207	137.72.43.3	TCP	ACK PSH : ftp reply code	ol	1909	305141379	751490820	32755
213	19:15:17:2801 EST	52	137.72.43.3	137.72.43.207	TCP	ACK PSH : ftp command PASS	1909	ftp control	751490820	305141406	64206
216	19:15:17:5168 EST	40	137.72.43.207	137.72.43.3	TCP	ACK PSH	ftp control	1909	305141406	751490832	32756
217	19:15:17:7234 EST	99	137.72.43.207	137.72.43.3	TCP	ACK PSH : ftp reply code 230	ftp control	1909	305141406	751490832	32756
218	19:15:17:7262 EST	46	137.72.43.3	137.72.43.207	TCP	ACK PSH : ftp command SYST	1909	ftp control	751490832	305141465	64191
219	19:15:17:7288 EST	120	137.72.43.207	137.72.43.3	TCP	ACK PSH : ftp reply code 215	ftp control	1909	305141465	751490838	32762
220	19:15:17:7315 EST	46	137.72.43.3	137.72.43.207	TCP	ACK PSH : ftp command QUIT	1909	ftp control	751490838	305141545	64171
221	19:15:17:7337 EST	77	137.72.43.207	137.72.43.3	TCP	ACK PSH : ftp reply code 221	ftp control	1909	305141545	751490844	32762
222	19:15:17:7351 EST	40	137.72.43.207	137.72.43.3	TCP	ACK PSH FIN	ftp control	1909	305141582	751490844	32762
223	19:15:17:7375 EST	40	137.72.43.3	137.72.43.207	TCP	ACK	1909	ftp control	751490844	305141583	64162
224	19:15:17:7376 EST	40	137.72.43.3	137.72.43.207	TCP	ACK FIN	1909	ftp control	751490844	305141583	64162
225	19:15:17:7390 EST	40	137.72.43.207	137.72.43.3	TCP	ACK PSH	ftp control	1909	305141583	751490845	32762

Copyright © 2011 Applied Expert Systems, Inc.

TCP - Establishing a Connection
Packet Details



Copyright © 2011 Applied Expert Systems, Inc.

TCP - Data Transfer

Traces | Query Builder | Packet Summary | Packet Details | Sequence of Execution | Response Time Summary | Exception Report

Seq. of Execution

Local IP: 137.72.43.207 Remote IP: 137.72.43.117 Protocol: TCP Sessions Count : 2

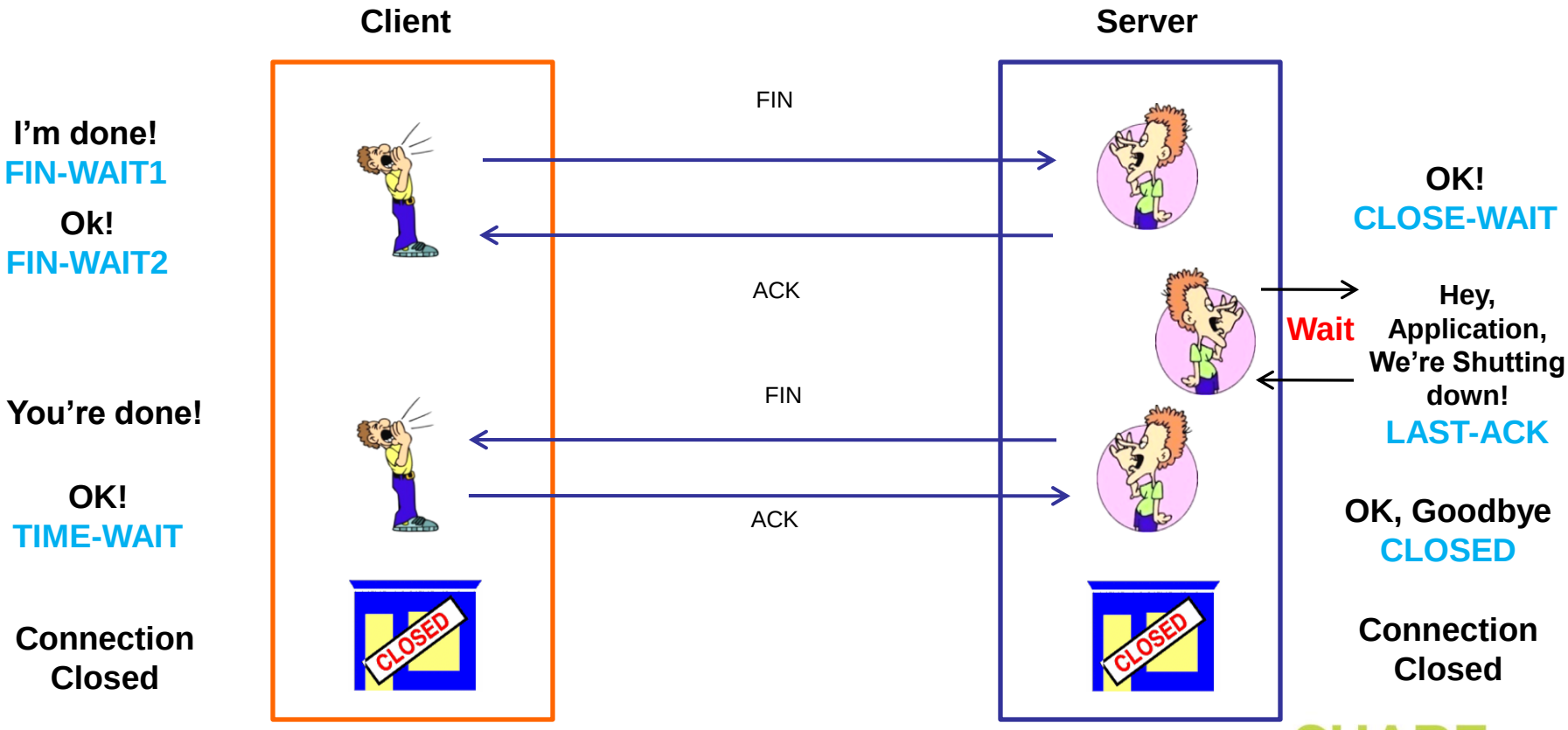
ID	Timestamp	Elapse Time (hh:mm:ss.tttt)	Datagram Size	Messages	Local Port	Direction	Rmt. Port	Seq. Number	Ack. Number	Window Size
58	17:58:55:0072 GMT	00:00:00:0000	60	SYN	ftp data	---->	2261	3004779	0	32768
59	17:58:55:0077 GMT	00:00:00:0005	60	ACK SYN	ftp data	<----	2261	2375637840	3004780	65535
60	17:58:55:0109 GMT	00:00:00:0032	52	ACK	ftp data	---->	2261	3004780	2375637841	32768
62	17:58:55:0709 GMT	00:00:00:0600	1500	ACK	ftp data	---->	2261	3004780	2375637841	32768
63	17:58:55:0712 GMT	00:00:00:0003	1500	ACK	ftp data	---->	2261	3006228	2375637841	32768
64	17:58:55:0712 GMT	00:00:00:0000	52	ACK	ftp data	<----	2261	2375637841	3007676	62639
65	17:58:55:0712 GMT	00:00:00:0000	1500	ACK PSH	ftp data	---->	2261	3007676	2375637841	32768
66	17:58:55:0714 GMT	00:00:00:0002	52	ACK	ftp data	<----	2261	2375637841	3009124	64951
67	17:58:55:0749 GMT	00:00:00:0035	1500	ACK	ftp data	---->	2261	3009124	2375637841	32768
68	17:58:55:0752 GMT	00:00:00:0003	1500	A	a	---->	2261	3010572	2375637841	32768
69	17:58:55:0753 GMT	00:00:00:0001	52	A	a	<----	2261	2375637841	3012020	62055
70	17:58:55:0753 GMT	00:00:00:0000	1500	A	a	---->	2261	3012020	2375637841	32768
71	17:58:55:0753 GMT	00:00:00:0000	1500	A	a	---->	2261	3013468	2375637841	32768
72	17:58:55:0753 GMT	00:00:00:0000	52	A	a	<----	2261	2375637841	3014916	59159
73	17:58:55:0754 GMT	00:00:00:0001	1500	ACK PSH	ftp data	---->	2261	3014916	2375637841	32768
74	17:58:55:0755 GMT	00:00:00:0001	52	ACK	ftp data	<----	2261	2375637841	3016364	62055
75	17:58:55:0757 GMT	00:00:00:0002	52	ACK	ftp data	<----	2261	2375637841	3016364	65535
76	17:58:55:0785 GMT	00:00:00:0028	1500	ACK	ftp data	---->	2261	3016364	2375637841	32768
77	17:58:55:0787 GMT	00:00:00:0002	1500	ACK	ftp data	---->	2261	3017812	2375637841	32768
78	17:58:55:0788 GMT	00:00:00:0001	52	ACK	ftp data	<----	2261	2375637841	3019260	62639
79	17:58:55:0788 GMT	00:00:00:0000	1500	ACK	ftp data	---->	2261	3019260	2375637841	32768
80	17:58:55:0789 GMT	00:00:00:0001	1500	ACK	ftp data	---->	2261	3020708	2375637841	32768
81	17:58:55:0789 GMT	00:00:00:0000	52	ACK	ftp data	<----	2261	2375637841	3022156	59743
82	17:58:55:0790 GMT	00:00:00:0001	52	ACK	ftp data	<----	2261	2375637841	3022156	63503
83	17:58:55:0791 GMT	00:00:00:0001	1500	ACK	ftp data	---->	2261	3022156	2375637841	32768
84	17:58:55:0791 GMT	00:00:00:0000	1500	ACK	ftp data	---->	2261	3023604	2375637841	32768
85	17:58:55:0791 GMT	00:00:00:0000	52	ACK	ftp data	<----	2261	2375637841	3025052	60607
86	17:58:55:0793 GMT	00:00:00:0002	1500	ACK	ftp data	---->	2261	3025052	2375637841	32768
87	17:58:55:0794 GMT	00:00:00:0001	1500	ACK PSH	ftp data	---->	2261	3026500	2375637841	32768

Ouch! A Retransmission!!

TCP parm limits bursts to two 1500 byte packets

Copyright © 2011 Applied Expert Systems, Inc.

TCP - Connection Termination



Copyright © 2011 Applied Expert Systems, Inc.

TCP - Connection Termination

Traces | Query Builder | Packet Summary | Packet Details | Sequence of Execution | Response Time Summary | Exception Report

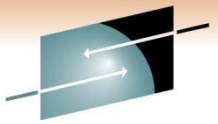
Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
439	18:15:39:7282 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598481056	1803247842	32768
440	18:15:39:7283 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598482504	59743
441	18:15:39:7283 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598482504	1803247842	32768
442	18:15:39:7283 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598483952	1803247842	32768
443	18:15:39:7283 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598485400	56847
444	18:15:39:7285 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598485400	1803247842	32768
445	18:15:39:7286 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598486848	59159
446	18:15:39:7287 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598486848	1803247842	32768
447	18:15:39:7287 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598488296	1803247842	32768
448	18:15:39:7287 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598489744	56263
449	18:15:39:7288 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598489744	1803247842	32768
450	18:15:39:7290 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598491192	1803247842	32768
451	18:15:39:7290 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598492640	53367
452	18:15:39:7291 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598492640	1803247842	32768
453	18:15:39:7292 GMT	1396	137.72.43.207	137.72.43.117	TCP	ACK PSH	ftp data	4410	3598494088	1803247842	32768
454	18:15:39:7292 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598495432	50575
455	18:15:39:7295 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598495432	56951
456	18:15:39:7300 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598495432	65535
457	18:15:39:7447 GMT	52	137.72.43.207	137.72.43.117	TCP	ACK PSH FIN	ftp data	4410	3598495432	1803247842	32768
458	18:15:39:7450 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598495433	65535
459	18:15:39:7454 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK FIN	4410	ftp data	1803247842	3598495433	65535
460	18:15:39:7491 GMT	52	137.72.43.207	137.72.43.117	TCP	ACK PSH	ftp data	4410	3598495433	1803247843	32768
461	18:15:39:7799 GMT	40	137.72.43.117	137.72.43.207	TCP	ACK	4408	ftp control	250971858	3598076766	65233
462	18:15:39:7816 GMT	78	137.72.43.207	137.72.43.117	TCP	ACK PSH : ftp reply code 250	ftp control	4408	3598076766	250971858	32754
464	18:15:39:9804 GMT	40	137.72.43.117	137.72.43.207	TCP	ACK	4408	ftp control	250971858	3598076804	65195
466	18:15:41:6117 GMT	46	137.72.43.117	137.72.43.207	TCP	ACK PSH : ftp command QUIT	4408	ftp control	250971858	3598076804	65195
467	18:15:41:6164 GMT	77	137.72.43.207	137.72.43.117	TCP	ACK PSH : ftp reply code 221	ftp control	4408	3598076804	250971864	32762
468	18:15:41:6172 GMT	40	137.72.43.117	137.72.43.207	TCP	ACK FIN	4408	ftp control	250971864	3598076841	65158
469	18:15:41:6191 GMT	40	137.72.43.207	137.72.43.117	TCP	ACK PSH	ftp control	4408	3598076842	250971865	32762
470	18:15:41:6195 GMT	40	137.72.43.207	137.72.43.117	TCP	ACK PSH FIN	ftp control	4408	3598076841	250971864	32762
471	18:15:41:6195 GMT	40	137.72.43.117	137.72.43.207	TCP	ACK	4408	ftp control	250971865	3598076842	65158

Termination Sequence

Copyright © 2011 Applied Expert Systems, Inc.

Comparing Traces



Trace Diff

Trace 1

C:\Program Files\AES\traces\ftp_cli_1_18.mdb | Browse | Search | Run Query

Packet Summary | Packet Detail

ID	Timestamp	Datagram Size	Local IP	Rmt.
13	17:58:40:9044 GMT	48	137.72.43.117	137.7
14	17:58:40:9065 GMT	44	137.72.43.207	137.7
15	17:58:40:9065 GMT	40	137.72.43.117	137.7
29	17:58:41:0354 GMT	114	137.72.43.207	137.7
30	17:58:41:1930 GMT	40	137.72.43.117	137.7
31	17:58:41:2007 GMT	74	137.72.43.207	137.7
32	17:58:41:3936 GMT	40	137.72.43.117	137.7
35	17:58:44:5920 GMT	54	137.72.43.117	137.7
36	17:58:44:6087 GMT	67	137.72.43.207	137.7
37	17:58:44:8045 GMT	40	137.72.43.117	137.7
38	17:58:47:5682 GMT	52	137.72.43.117	137.7
39	17:58:47:8573 GMT	40	137.72.43.207	137.7
40	17:58:47:9542 GMT	101	137.72.43.207	137.7
41	17:58:48:1151 GMT	40	137.72.43.117	137.7
43	17:58:49:9270 GMT	48	137.72.43.117	137.7
44	17:58:49:9317 GMT	74	137.72.43.207	137.7
45	17:58:50:1215 GMT	40	137.72.43.117	137.7
55	17:58:54:9830 GMT	66	137.72.43.117	137.7
56	17:58:54:9880 GMT	62	137.72.43.207	137.7
57	17:58:54:9890 GMT	54	137.72.43.117	137.7
58	17:58:55:0072 GMT	60	137.72.43.207	137.7
59	17:58:55:0077 GMT	60	137.72.43.117	137.7
60	17:58:55:0109 GMT	52	137.72.43.207	137.7
61	17:58:55:0629 GMT	90	137.72.43.207	137.7
62	17:58:55:0709 GMT	1500	137.72.43.207	137.7

Trace 2

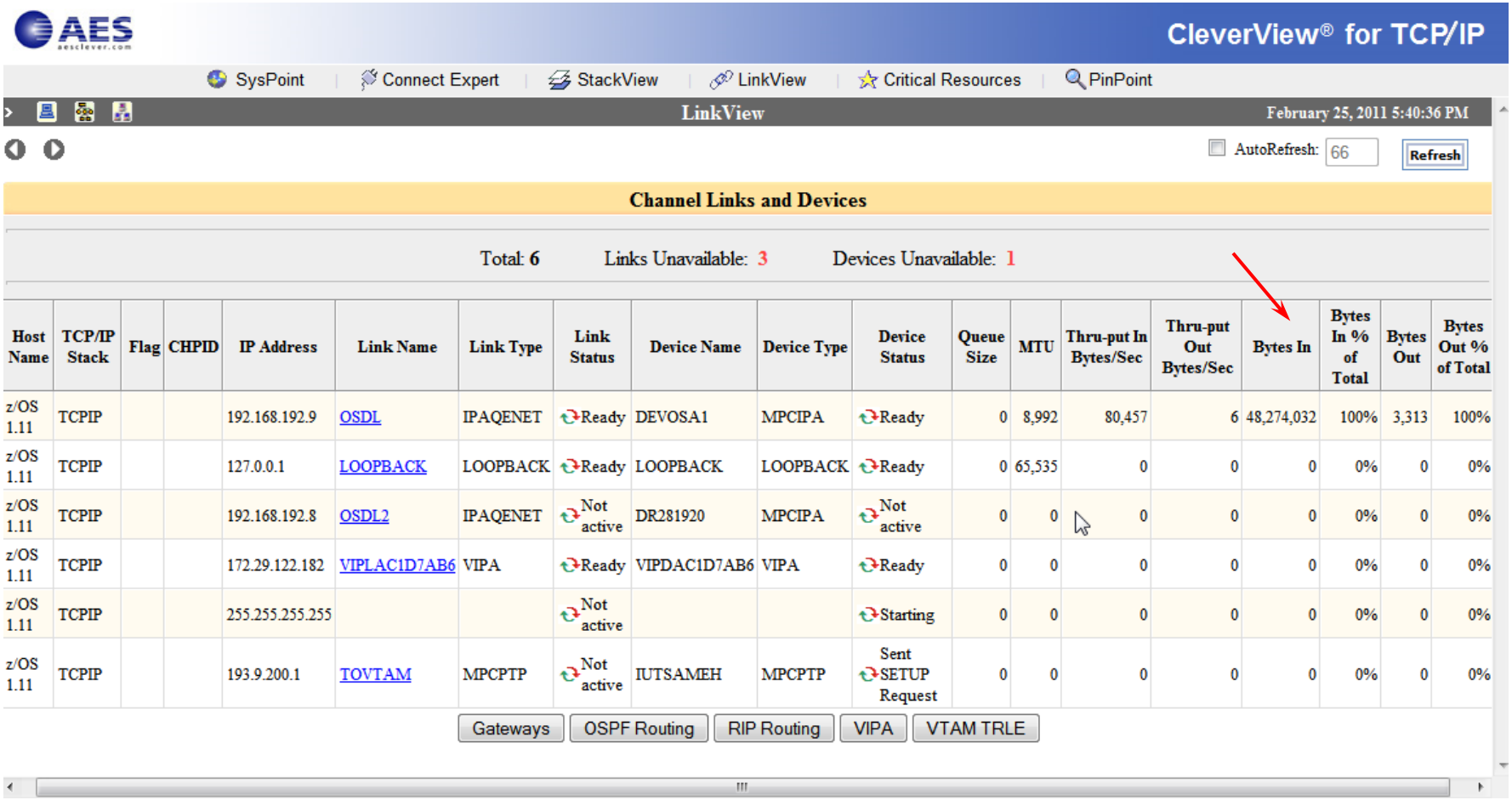
C:\Program Files\AES\traces\ftp_srv_1_18.mdb | Browse | Search | Run Query

Packet Summary | Packet Detail

ID	Timestamp	Datagram Size	Local IP	Rm
118	17:51:19:3035 GMT	48	137.72.43.117	137
119	17:51:19:3041 GMT	44	137.72.43.207	137
120	17:51:19:3053 GMT	40	137.72.43.117	137
134	17:51:19:4328 GMT	114	137.72.43.207	137
135	17:51:19:5979 GMT	40	137.72.43.117	137
136	17:51:19:5983 GMT	74	137.72.43.207	137
137	17:51:19:7930 GMT	40	137.72.43.117	137
138	17:51:22:9910 GMT	54	137.72.43.117	137
139	17:51:23:0061 GMT	67	137.72.43.207	137
140	17:51:23:2035 GMT	40	137.72.43.117	137
141	17:51:25:9671 GMT	52	137.72.43.117	137
142	17:51:26:2546 GMT	40	137.72.43.207	137
143	17:51:26:3515 GMT	101	137.72.43.207	137
144	17:51:26:5140 GMT	40	137.72.43.117	137
145	17:51:28:3258 GMT	48	137.72.43.117	137
146	17:51:28:3290 GMT	74	137.72.43.207	137
147	17:51:28:5203 GMT	40	137.72.43.117	137
156	17:51:33:3818 GMT	66	137.72.43.117	137
157	17:51:33:3852 GMT	62	137.72.43.207	137
158	17:51:33:3877 GMT	54	137.72.43.117	137
159	17:51:33:4042 GMT	60	137.72.43.207	137
160	17:51:33:4063 GMT	60	137.72.43.117	137
161	17:51:33:4081 GMT	52	137.72.43.207	137
162	17:51:33:4600 GMT	90	137.72.43.207	137
163	17:51:33:4673 GMT	1500	137.72.43.207	137

Copyright © 2011 Applied Expert Systems, Inc.

OSA – Excessive Inbound Packets in Real-Time



AES

CleverView® for TCP/IP

SysPoint | Connect Expert | StackView | LinkView | Critical Resources | PinPoint

LinkView — February 25, 2011 5:40:36 PM

AutoRefresh: 66 Refresh

Channel Links and Devices

Total: 6 Links Unavailable: 3 Devices Unavailable: 1

Host Name	TCP/IP Stack	Flag	CHPID	IP Address	Link Name	Link Type	Link Status	Device Name	Device Type	Device Status	Queue Size	MTU	Thru-put In Bytes/Sec	Thru-put Out Bytes/Sec	Bytes In	Bytes In % of Total	Bytes Out	Bytes Out % of Total
z/OS 1.11	TCPIP			192.168.192.9	OSDL	IPAQENET	Ready	DEVOSA1	MPCIPA	Ready	0	8,992	80,457	6	48,274,032	100%	3,313	100%
z/OS 1.11	TCPIP			127.0.0.1	LOOPBACK	LOOPBACK	Ready	LOOPBACK	LOOPBACK	Ready	0	65,535	0	0	0	0%	0	0%
z/OS 1.11	TCPIP			192.168.192.8	OSDL2	IPAQENET	Not active	DR281920	MPCIPA	Not active	0	0	0	0	0	0%	0	0%
z/OS 1.11	TCPIP			172.29.122.182	VIPLAC1D7AB6	VIPA	Ready	VIPDAC1D7AB6	VIPA	Ready	0	0	0	0	0	0%	0	0%
z/OS 1.11	TCPIP			255.255.255.255			Not active			Starting	0	0	0	0	0	0%	0	0%
z/OS 1.11	TCPIP			193.9.200.1	TOVTAM	MPCPTP	Not active	IUTSAMEH	MPCPTP	Sent SETUP Request	0	0	0	0	0	0%	0	0%

Gateways | OSPF Routing | RIP Routing | VIPA | VTAM TRLE

Copyright © 2011 Applied Expert Systems, Inc.

Command: Netstat Devlinks

```
DevName: DEVOSA1           DevType: MPCIPA
   DevStatus: Ready
   LnkName: OSDL              LnkType: IPAQENET   LnkStatus: Ready
     Speed: 0000001000
     IpBroadcastCapability: No
     CfgRouter: Non                    ActRouter: Non
     ArpOffload: Yes                   ArpOffloadInfo: Yes
     ActMtu: 8992
     VLANid: None                      VLANpriority: Disabled
     ReadStorage: GLOBAL (4096K)       InbPerf: Balanced
     SecClass: 255                     MonSysplex: No
   Routing Parameters:
     MTU Size: n/a               Metric: 00
     DestAddr: 0.0.0.0           SubnetMask: 255.255.255.0
   Multicast Specific:
     Multicast Capability: Yes
     Group             RefCnt        SrcFltMd
     -----             ------        --------
     224.0.0.1         0000000001    Exclude
       SrcAddr: None
   Link Statistics:
     BytesIn                           = 25081576230
     Inbound Packets                   = 194853959
     Inbound Packets In Error          = 194353459
     Inbound Packets Discarded         = 194352011
     Inbound Packets With No Protocol  = 0
     BytesOut                          = 103520236
     Outbound Packets                  = 387012
     Outbound Packets In Error         = 0
     Outbound Packets Discarded        = 0
```

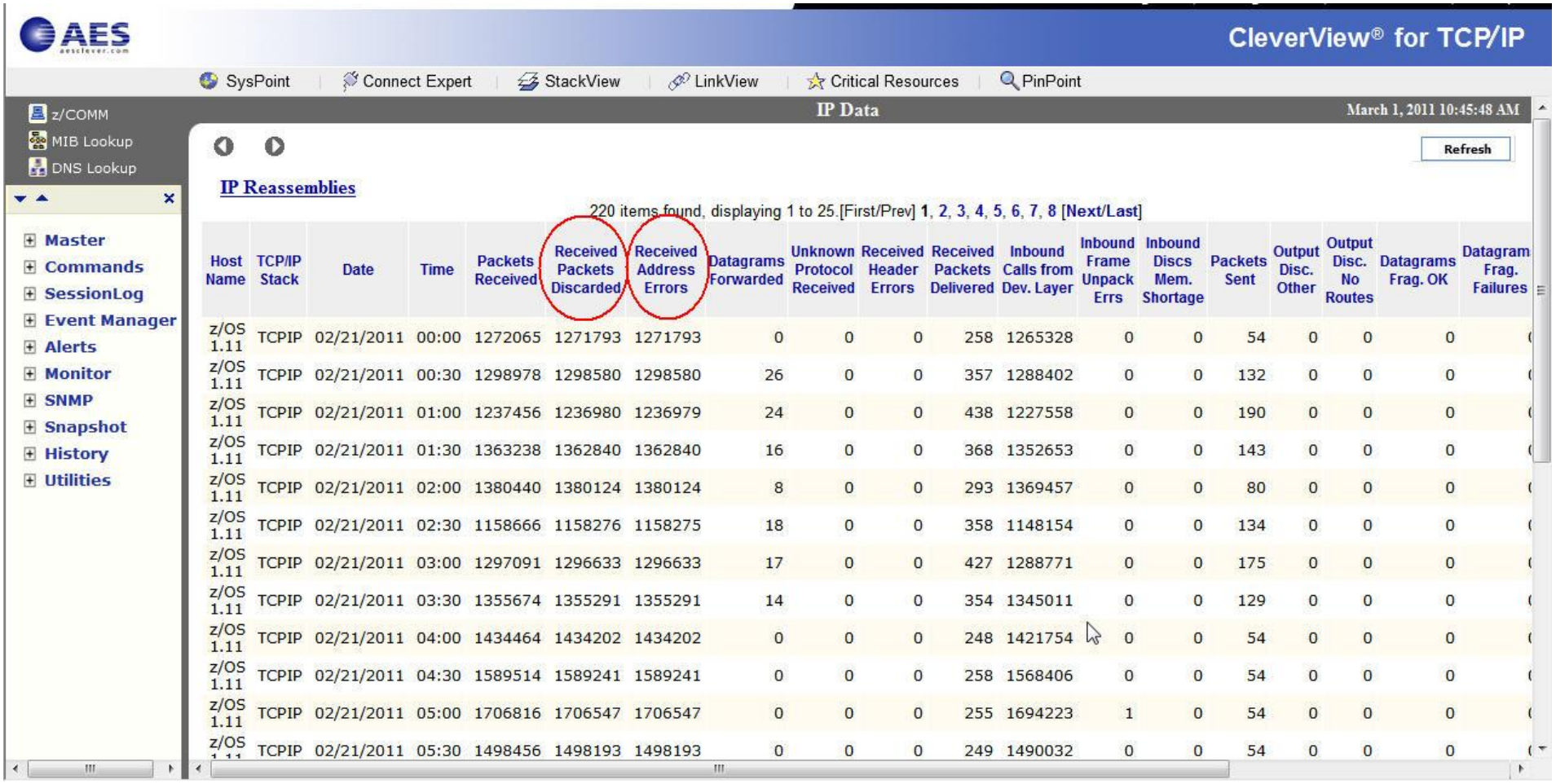

Copyright © 2011 Applied Expert Systems, Inc.

Command: Netstat Stats Proto IP

```
MVS TCP/IP NETSTAT CS V1R11       TCPIP Name: TCPIP          02:22:49
IP Statistics (IPv4)
  Packets Received                    = 194959223
  Received Header Errors              = 194429115
  Received Address Errors             = 194431079
  Datagrams Forwarded                 = 4680
  Unknown Protocols Received          = 0
  Received Packets Discarded          = 0
  Received Packets Delivered          = 523425
  Output Requests                     = 409928
  Output Discards No Route            = 0
  Output Discards (other)             = 0
  Reassembly Timeouts                 = 0
  Reassembly Required                 = 0
  Reassembly Successful               = 0
  Reassembly Failures                 = 0
  Datagrams Successfully Fragmented   = 0
  Datagrams Failing Fragmentation     = 0
  Fragments Created                   = 0
  Inbound Packets handled by zIIP     = 0
  Outbound Packets handled by zIIP    = 0
```


Copyright © 2011 Applied Expert Systems, Inc.

Check Historical Data



Host Name	TCP/IP Stack	Date	Time	Packets Received	Received Packets Discarded	Received Address Errors	Datagrams Forwarded	Unknown Protocol Received	Received Header Errors	Received Packets Delivered	Inbound Calls from Dev. Layer	Inbound Frame Unpack Errs	Inbound Discs Mem. Shortage	Packets Sent	Output Disc. Other	Output Disc. No Routes	Datagrams Frag. OK	Datagram Frag. Failures
z/OS 1.11	TCPIP	02/21/2011	00:00	1272065	1271793	1271793	0	0	0	258	1265328	0	0	54	0	0	0	0
z/OS 1.11	TCPIP	02/21/2011	00:30	1298978	1298580	1298580	26	0	0	357	1288402	0	0	132	0	0	0	0
z/OS 1.11	TCPIP	02/21/2011	01:00	1237456	1236980	1236979	24	0	0	438	1227558	0	0	190	0	0	0	0
z/OS 1.11	TCPIP	02/21/2011	01:30	1363238	1362840	1362840	16	0	0	368	1352653	0	0	143	0	0	0	0
z/OS 1.11	TCPIP	02/21/2011	02:00	1380440	1380124	1380124	8	0	0	293	1369457	0	0	80	0	0	0	0
z/OS 1.11	TCPIP	02/21/2011	02:30	1158666	1158276	1158275	18	0	0	358	1148154	0	0	134	0	0	0	0
z/OS 1.11	TCPIP	02/21/2011	03:00	1297091	1296633	1296633	17	0	0	427	1288771	0	0	175	0	0	0	0
z/OS 1.11	TCPIP	02/21/2011	03:30	1355674	1355291	1355291	14	0	0	354	1345011	0	0	129	0	0	0	0
z/OS 1.11	TCPIP	02/21/2011	04:00	1434464	1434202	1434202	0	0	0	248	1421754	0	0	54	0	0	0	0
z/OS 1.11	TCPIP	02/21/2011	04:30	1589514	1589241	1589241	0	0	0	258	1568406	0	0	54	0	0	0	0
z/OS 1.11	TCPIP	02/21/2011	05:00	1706816	1706547	1706547	0	0	0	255	1694223	1	0	54	0	0	0	0
z/OS 1.11	TCPIP	02/21/2011	05:30	1498456	1498193	1498193	0	0	0	249	1490032	0	0	54	0	0	0	0

Copyright © 2011 Applied Expert Systems, Inc.

Packet Trace – SYSTCPDA / SYSTCPOT

VARY TCPIP,*tcpipproc*,PKT,ON,DISCard=ALL

```
54550962 S0W1      PACKET    00000004 14:13:05.687445 Packet Trace
 From Interface     : OSDL              Device: QDIO Ethernet     Full=78
  Tod Clock         : 2011/01/25 14:13:05.687445                  Intfx: 9
  Discard           : 4114 (IP_MAC_BRDCST)
  Segment #         : 0                 Flags:   In Dscrd
  Source            : 172.29.96.9
  Destination       : 172.29.191.255
  Source Port       : 137               Dest Port: 137    Asid: 004F TCB: 00000000
 IpHeader: Version  : 4                 Header Length: 20
  Tos               : 00                QOS: Routine Normal Service
  Packet Length     : 78                ID Number: 78B7
  Fragment          :                   Offset: 0
  TTL               : 82                Protocol: UDP             CheckSum: 77A4 FF
  Source            : 172.29.96.9
  Destination       : 172.29.191.255
 UDP
  Source Port       : 137    (netbios-ns) Destination Port: 137    (netbios-ns)
  Datagram Length   : 58                CheckSum: 0000 6B36
Ip Header           : 20                IP: 172.29.96.9, 172.29.191.255 Offset:  0
000000 4500004E 78B70000 521177A4 AC1D6009  AC1DBFFF
Protocol Header     : 8                 Port: 137, 137            Offset: 14
000000 00890089 003A0000
Data                : 50      Data Length: 50                   Offset: 1C
000000 84E20110 00010000 00000000 20464946 |dS.............. ..............FIF|
000010 41464745 4A464345 48454A45 4F434143 |....¢.....¢.|... AFGEJFCEHEJEOCAC|
000020 41434143 41434143 41434141 41000020 |.............. ACACACACACAAA..  |
000030 0001                                |..             ..              |
```


Copyright © 2011 Applied Expert Systems, Inc.

Discarded Packets

- **Discard Reason Code**
  - *Comm Server IP & SNA Codes:*

Discard Reason Code	Category
1 – 4095	OSA
4096 – 8191	Interface and IP layer
8192 – 12287	TCP layer
12288 – 20479	Reserved

  - 4114 (IP_MAC_BRDCST):
    The MAC broadcast packet not accepted.
- Destination IP = 172.29.191.255 ?

Copyright © 2011 Applied Expert Systems, Inc.

Discarded Packets - continued

- The drop reason code 4114 usually indicates that the packet has a non-broadcast destination IP address and a broadcast media header (the broadcast indicator is on in the media header). This is likely to be caused by an invalid locally administered MAC address.
- Big switched LAN => broadcast flood; use VLAN to preserve bandwidth
- **netbios-ns**
  - NetBIOS Name Service (over UDP port 137)
  - Similar to DNS
  - Name Query request

Copyright © 2011 Applied Expert Systems, Inc.

OSA Checksum Offload Verification

- Packet Trace
  - Checksum field = 0 indicates checksum offload is in effect
  - Exceptions
    - Packets that go directly to another stack that shares the same OSA-Express feature
    - IPSec-encapsulated packets
    - Fragmented and reassembled packets
    - Outbound multicast and broadcast packets
    - Outbound TCP packets that contain only a TCP header
    - When multipath is in effect (unless all interfaces in the multipath group support

Copyright © 2011 Applied Expert Systems, Inc.

OSA Statistics from SNMP MIBs

- IOBSNMP SNMP sub-agent, OSNMPD
- Performance data is available from all LPARs
- **Channel** - PCI bus and processor utilizations (1 min/5 min/1 hr), etc.
- **Ethernet** – Active MAC address, in/out packets and frames, etc.
- "**LPAR**" (CSS/Image ID) - Data transfer rate (1 min/5 min/1 hr), processor utilization (1 min/5 min/1 hr)

Copyright © 2011 Applied Expert Systems, Inc.

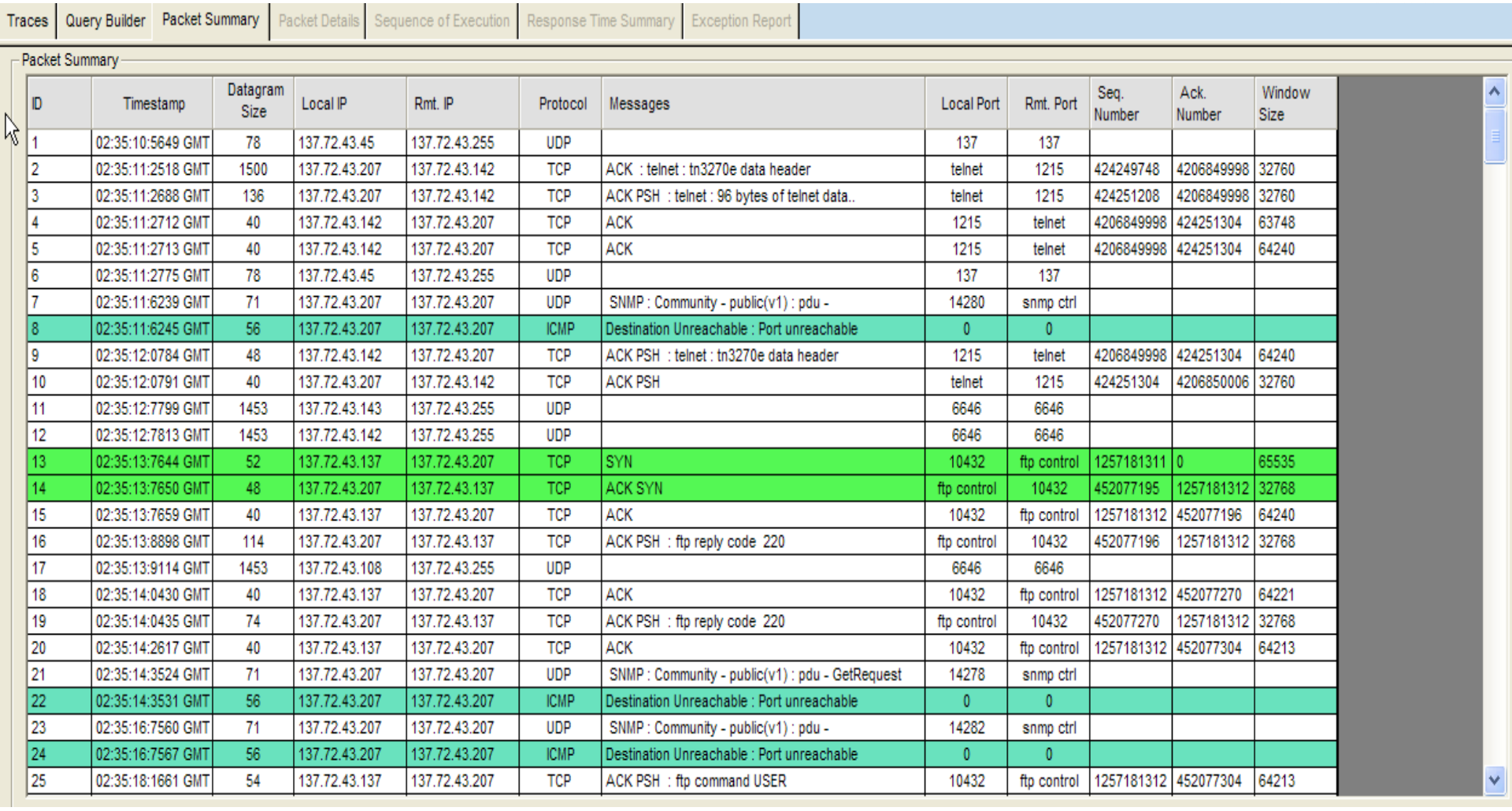
Display OSAINFO Command (z/OS V1R12)
General OSA and active protocols info

DISPLAY TCPIP,*tcpproc*,OSAinfo,INTFName=*interface*

```
EZD0031I TCP/IP CS V1R12 TCPIP Name: TCPCS 15:14:15
Display OSAINFO results for IntfName: LNK29D
PortName: DEV29D PortNum: 01 Datapath: 3902 RealAddr: 0002
PCHID: 0451 CHPID: 29 CHPID Type: OSD OSA code level: 6760
Gen: OSA-E3 Active speed/mode: 1000 mb/sec full duplex
Media: Singlemode Fiber Jumbo frames: Yes Isolate: No
PhysicalMACAddr: 643B88F30000 LocallyCfgMACAddr: 000000000000
Queues defined Out: 4 In: 3 Ancillary queues in use: 2
Connection Mode: Layer 3 IPv4: Yes IPv6: No
SAPSup: 00010293 SAPEna: 00010293
IPv4 attributes:
VLAN ID: N/A VMAC Active: No
Defined Router: Non Active Router: No
AsstParmsEna: 00215C66 OutCkSumEna: 00000000 InCkSumEna: 00000000
Registered Addresses:
IPv4 Unicast Addresses:
ARP: Yes Addr: 10.10.10.10
Total number of IPv4 addresses: 1
IPv4 Multicast Addresses:
MAC: 01005E000001 Addr: 224.0.0.1
Total number of IPv4 addresses: 1
Ancillary Input Queue Routing Variables:
Queue Type: BULKDATA Queue ID: 2 Protocol: TCP
Src: 11.1.1.11..100
Dst: 12.12.12.12..100
Src: 13.3.3.13..101
Dst: 14.14.14.14..101
Total number of IPv4 connections: 2
Queue Type: SYSDIST Queue ID: 3 Protocol: TCP
Addr: 10.10.10.10
Total number of IPv4 addresses: 1
```


Copyright © 2011 Applied Expert Systems, Inc.

FTP Diagnosis



Traces | Query Builder | Packet Summary | Packet Details | Sequence of Execution | Response Time Summary | Exception Report

Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
1	02:35:10:5649 GMT	78	137.72.43.45	137.72.43.255	UDP		137	137			
2	02:35:11:2518 GMT	1500	137.72.43.207	137.72.43.142	TCP	ACK : telnet : tn3270e data header	telnet	1215	424249748	4206849998	32760
3	02:35:11:2688 GMT	136	137.72.43.207	137.72.43.142	TCP	ACK PSH : telnet : 96 bytes of telnet data..	telnet	1215	424251208	4206849998	32760
4	02:35:11:2712 GMT	40	137.72.43.142	137.72.43.207	TCP	ACK	1215	telnet	4206849998	424251304	63748
5	02:35:11:2713 GMT	40	137.72.43.142	137.72.43.207	TCP	ACK	1215	telnet	4206849998	424251304	64240
6	02:35:11:2775 GMT	78	137.72.43.45	137.72.43.255	UDP		137	137			
7	02:35:11:6239 GMT	71	137.72.43.207	137.72.43.207	UDP	SNMP : Community - public(v1) : pdu -	14280	snmp ctrl			
8	02:35:11:6245 GMT	56	137.72.43.207	137.72.43.207	ICMP	Destination Unreachable : Port unreachable	0	0			
9	02:35:12:0784 GMT	48	137.72.43.142	137.72.43.207	TCP	ACK PSH : telnet : tn3270e data header	1215	telnet	4206849998	424251304	64240
10	02:35:12:0791 GMT	40	137.72.43.207	137.72.43.142	TCP	ACK PSH	telnet	1215	424251304	4206850006	32760
11	02:35:12:7799 GMT	1453	137.72.43.143	137.72.43.255	UDP		6646	6646			
12	02:35:12:7813 GMT	1453	137.72.43.142	137.72.43.255	UDP		6646	6646			
13	02:35:13:7644 GMT	52	137.72.43.137	137.72.43.207	TCP	SYN	10432	ftp control	1257181311	0	65535
14	02:35:13:7650 GMT	48	137.72.43.207	137.72.43.137	TCP	ACK SYN	ftp control	10432	452077195	1257181312	32768
15	02:35:13:7659 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077196	64240
16	02:35:13:8898 GMT	114	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 220	ftp control	10432	452077196	1257181312	32768
17	02:35:13:9114 GMT	1453	137.72.43.108	137.72.43.255	UDP		6646	6646			
18	02:35:14:0430 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077270	64221
19	02:35:14:0435 GMT	74	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 220	ftp control	10432	452077270	1257181312	32768
20	02:35:14:2617 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077304	64213
21	02:35:14:3524 GMT	71	137.72.43.207	137.72.43.207	UDP	SNMP : Community - public(v1) : pdu - GetRequest	14278	snmp ctrl			
22	02:35:14:3531 GMT	56	137.72.43.207	137.72.43.207	ICMP	Destination Unreachable : Port unreachable	0	0			
23	02:35:16:7560 GMT	71	137.72.43.207	137.72.43.207	UDP	SNMP : Community - public(v1) : pdu -	14282	snmp ctrl			
24	02:35:16:7567 GMT	56	137.72.43.207	137.72.43.207	ICMP	Destination Unreachable : Port unreachable	0	0			
25	02:35:18:1661 GMT	54	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command USER	10432	ftp control	1257181312	452077304	64213

Copyright © 2011 Applied Expert Systems, Inc.

FTP Diagnosis – zoom in on FTP ports: Control connection vs. Data connection

Traces | Query Builder | Packet Summary | Packet Details | Sequence of Execution | Response Time Summary | Exception Report

Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
13	02:35:13:7644 GMT	52	137.72.43.137	137.72.43.207	TCP	SYN	10432	ftp control	1257181311	0	65535
14	02:35:13:7650 GMT	48	137.72.43.207	137.72.43.137	TCP	ACK SYN	ftp control	10432	452077195	1257181312	32768
15	02:35:13:7659 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077196	64240
16	02:35:13:8898 GMT	114	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 220	ftp control	10432	452077196	1257181312	32768
18	02:35:14:0430 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077270	64221
19	02:35:14:0435 GMT	74	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 220	ftp control	10432	452077270	1257181312	32768
20	02:35:14:2617 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077304	64213
25	02:35:18:1661 GMT	54	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command USER	10432	ftp control	1257181312	452077304	64213
26	02:35:18:1790 GMT	67	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 331	ftp control	10432	452077304	1257181326	32754
27	02:35:18:3075 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181326	452077331	64206
33	02:35:20:6157 GMT	55	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command PASS	10432	ftp control	1257181326	452077331	64206
34	02:35:20:8732 GMT	40	137.72.43.207	137.72.43.137	TCP	ACK PSH	ftp control	10432	452077331	1257181341	32753
36	02:35:21:3641 GMT	101	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 230	ftp control	10432	452077331	1257181341	32753
37	02:35:21:4799 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181341	452077392	64191
41	02:35:23:5899 GMT	48	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command TYPE	10432	ftp control	1257181341	452077392	64191
42	02:35:23:5935 GMT	83	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077392	1257181349	32760
43	02:35:23:7760 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181349	452077435	64180
61	02:35:29:5343 GMT	67	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command PORT	10432	ftp control	1257181349	452077435	64180
62	02:35:29:5379 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741
65	02:35:30:3898 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741
68	02:35:32:1407 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741
74	02:35:35:5118 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741
75	02:35:42:2300 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741
99	02:35:55:6398 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741
166	02:36:22:7005 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741
257	02:37:16:9704 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741

Copyright © 2011 Applied Expert Systems, Inc.

FTP Diagnosis – Analyze the PORT command

Traces | Query Builder | Packet Summary | Packet Details | Sequence of Execution | Response Time Summary | Exception Report

Packet Details

Packet Details Hex Decode

Packet Details

```
Packet ID : 61
Time : 2/28/2009 02:35:29:5343 GMT
CTE Format ID : IPv4/6 Packet Trace (PTHIdPkt) (4)

PTHDR_T Header
Device Type : Ethernet
Link Name   : ETH1
Flags : Record Size adjust by +1
        IP packet was received
IP Packet Length : 67 bytes
IP Source: 137.72.43.137    IP Remote: 137.72.43.207
Source Port : 10432    Remote Port : 21
TCB Address : 0x0
ASID        : 0x35
Trace Count : 191128

IP Version 4
Source    : 137.72.43.137    Remote    : 137.72.43.207
Protocol : TCP
Datagram Length : 67
Flags : Don't Fragment       Fragment Offset : 0

TCP Header Info
Source Port : 10432     Remote Port : 21 ftp control
Seq. Number : 1257181349     Ack. Number : 452077435
Window : 64180     Flags : ACK PSH

FTP Data
Command : PORT
Parameters : 137,72,43,137,40,196
```


Copyright © 2011 Applied Expert Systems, Inc.

FTP Diagnosis – Analyze the PORT command continued

PORT 137,72,43,137,40,196

- Specifies that the FTP Server will initiate the data connection
- Client's IP Address: 137.72.43.137
- Client's Port: 40 * 256 + 196 = 10436
- Expect to see a SYN packet:
  - from server (137.72.43.207)
  - to client (137.72.43.137)

Copyright © 2011 Applied Expert Systems, Inc.

FTP Diagnosis – check the equivalent Sniffer trace

Traces | Query Builder | Packet Summary | Packet Details | Sequence of Execution | Response Time Summary | Exception Report

Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
10	02:42:00:5115 GMT	52	137.72.43.137	137.72.43.207	TCP	SYN	10432	ftp control	1257181311	0	65535
11	02:42:00:5130 GMT	48	137.72.43.207	137.72.43.137	TCP	ACK SYN	ftp control	10432	452077195	1257181312	32768
12	02:42:00:5130 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077196	64240
13	02:42:00:6380 GMT	114	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 220	ftp control	10432	452077196	1257181312	32768
14	02:42:00:7886 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077270	64221
15	02:42:00:7916 GMT	74	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 220	ftp control	10432	452077270	1257181312	32768
16	02:42:01:0073 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077304	64213
17	02:42:04:9129 GMT	54	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command USER	10432	ftp control	1257181312	452077304	64213
18	02:42:04:9278 GMT	67	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 331	ftp control	10432	452077304	1257181326	32754
19	02:42:05:0542 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181326	452077331	64206
20	02:42:07:3607 GMT	55	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command PASS	10432	ftp control	1257181326	452077331	64206
21	02:42:07:6216 GMT	40	137.72.43.207	137.72.43.137	TCP	ACK PSH	ftp control	10432	452077331	1257181341	32753
22	02:42:08:1125 GMT	101	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 230	ftp control	10432	452077331	1257181341	32753
23	02:42:08:2261 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181341	452077392	64191
24	02:42:10:3368 GMT	48	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command TYPE	10432	ftp control	1257181341	452077392	64191
25	02:42:10:3419 GMT	83	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077392	1257181349	32760
26	02:42:10:5229 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181349	452077435	64180
30	02:42:16:2812 GMT	67	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command PORT	10432	ftp control	1257181349	452077435	64180
31	02:42:16:2865 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741

Copyright © 2011 Applied Expert Systems, Inc.

FTP Diagnosis

Sniffer trace shows the PORT command was sent to the server but there was no SYN packet coming in – SYN packet was “lost”

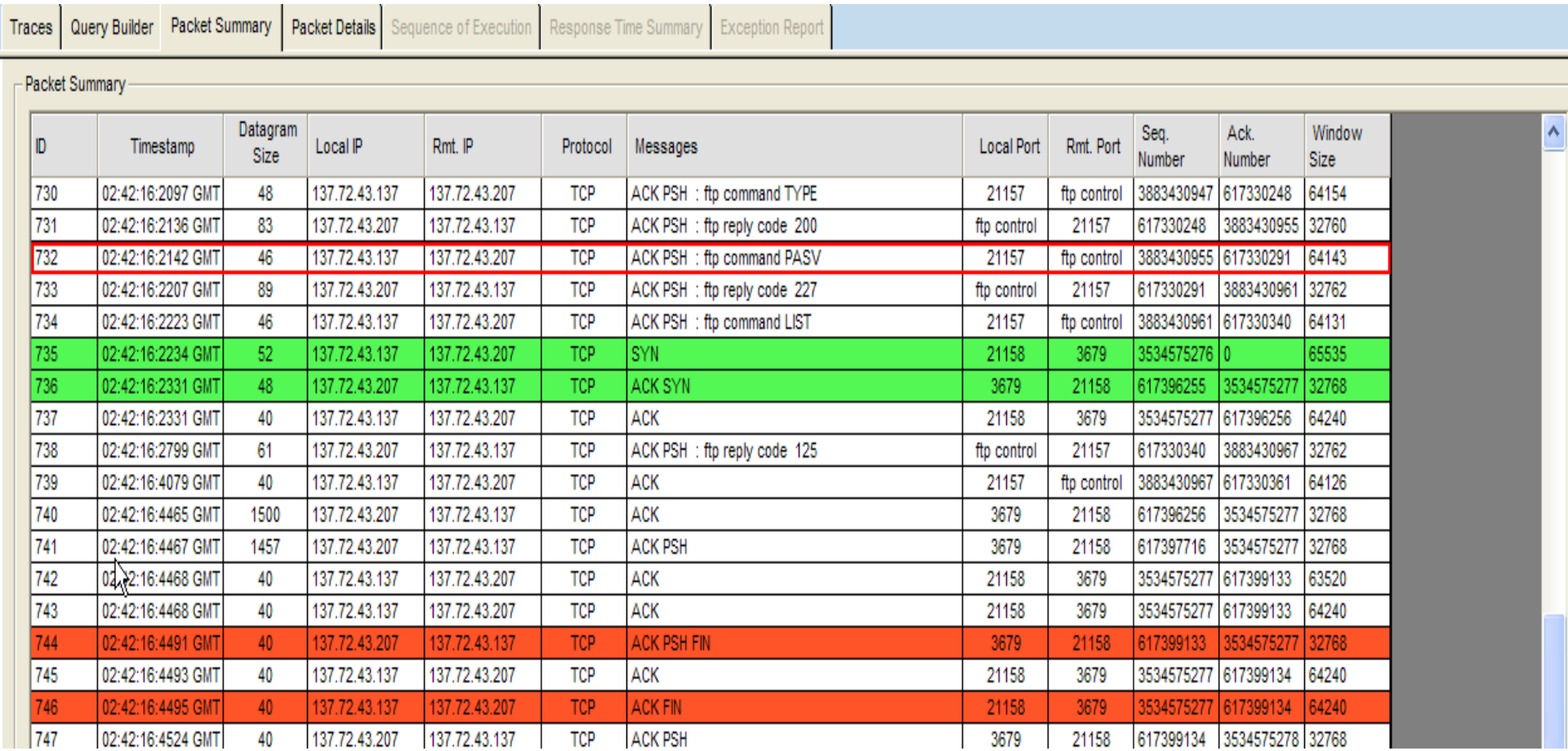
Might be related to firewall issues - check firewall setting, FTP.DATA and TCP PROFILE settings.

Passive FTP:

- Client initiates the data connection.
- Check to reply to the PASV command to determine the IP address and Port number of the server for the data connection.

Copyright © 2011 Applied Expert Systems, Inc.

FTP Diagnosis – Passive FTP



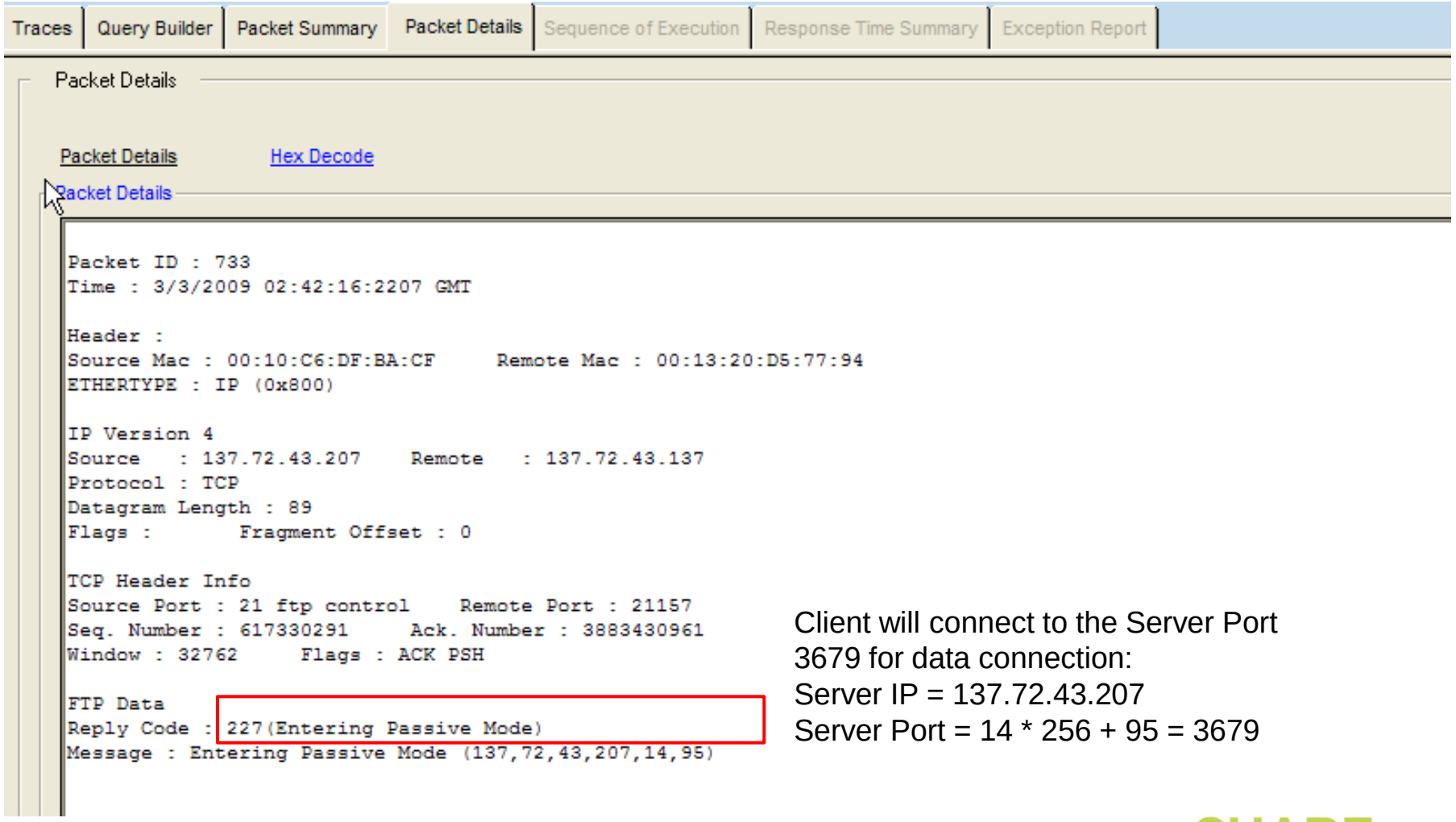
Traces | Query Builder | Packet Summary | Packet Details | Sequence of Execution | Response Time Summary | Exception Report

Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
730	02:42:16:2097 GMT	48	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command TYPE	21157	ftp control	3883430947	617330248	64154
731	02:42:16:2136 GMT	83	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	21157	617330248	3883430955	32760
732	02:42:16:2142 GMT	46	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command PASV	21157	ftp control	3883430955	617330291	64143
733	02:42:16:2207 GMT	89	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 227	ftp control	21157	617330291	3883430961	32762
734	02:42:16:2223 GMT	46	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command LIST	21157	ftp control	3883430961	617330340	64131
735	02:42:16:2234 GMT	52	137.72.43.137	137.72.43.207	TCP	SYN	21158	3679	3534575276	0	65535
736	02:42:16:2331 GMT	48	137.72.43.207	137.72.43.137	TCP	ACK SYN	3679	21158	617396255	3534575277	32768
737	02:42:16:2331 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	21158	3679	3534575277	617396256	64240
738	02:42:16:2799 GMT	61	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 125	ftp control	21157	617330340	3883430967	32762
739	02:42:16:4079 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	21157	ftp control	3883430967	617330361	64126
740	02:42:16:4465 GMT	1500	137.72.43.207	137.72.43.137	TCP	ACK	3679	21158	617396256	3534575277	32768
741	02:42:16:4467 GMT	1457	137.72.43.207	137.72.43.137	TCP	ACK PSH	3679	21158	617397716	3534575277	32768
742	02:42:16:4468 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	21158	3679	3534575277	617399133	63520
743	02:42:16:4468 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	21158	3679	3534575277	617399133	64240
744	02:42:16:4491 GMT	40	137.72.43.207	137.72.43.137	TCP	ACK PSH FIN	3679	21158	617399133	3534575277	32768
745	02:42:16:4493 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	21158	3679	3534575277	617399134	64240
746	02:42:16:4495 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK FIN	21158	3679	3534575277	617399134	64240
747	02:42:16:4524 GMT	40	137.72.43.207	137.72.43.137	TCP	ACK PSH	3679	21158	617399134	3534575278	32768

Copyright © 2011 Applied Expert Systems, Inc.

FTP Diagnosis – Analyze the PASV Reply



Client will connect to the Server Port 3679 for data connection:
Server IP = 137.72.43.207
Server Port = 14 * 256 + 95 = 3679

Copyright © 2011 Applied Expert Systems, Inc.

TLS/SSL
https (Port 443), AT-TLS (appl. port)

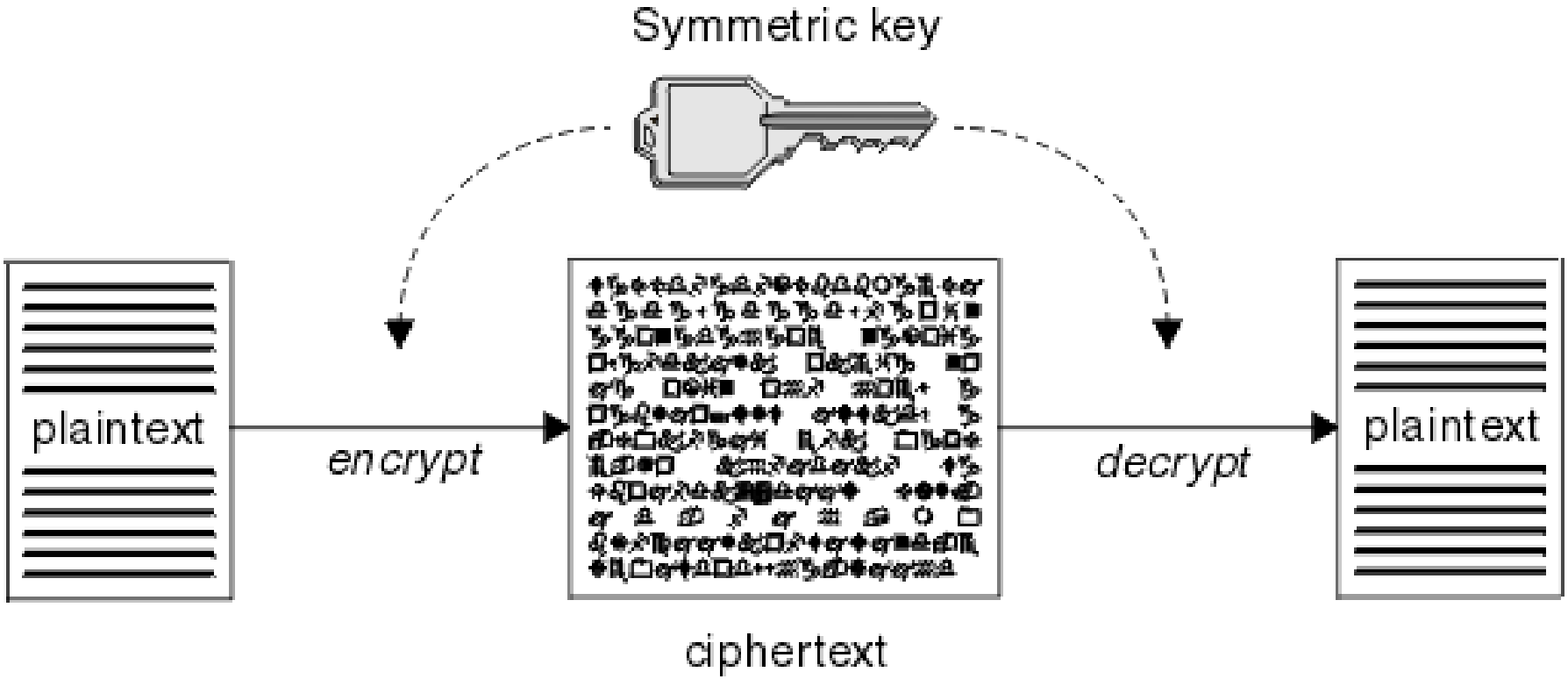
- Transport Layer Security provides security for communications over networks by encrypting the segments at the transport layer end to end.

- TLS V1.0 (RFC 2246) is based on SSL V3.0.

- It does not require the client and the server to arrange for a secret key to be exchanged *before* the transaction.
  - Asymmetric keys (public/private) for handshaking and secret key exchange.
  - Secret key (symmetric) mechanism for subsequent communication.

Copyright © 2011 Applied Expert Systems, Inc.

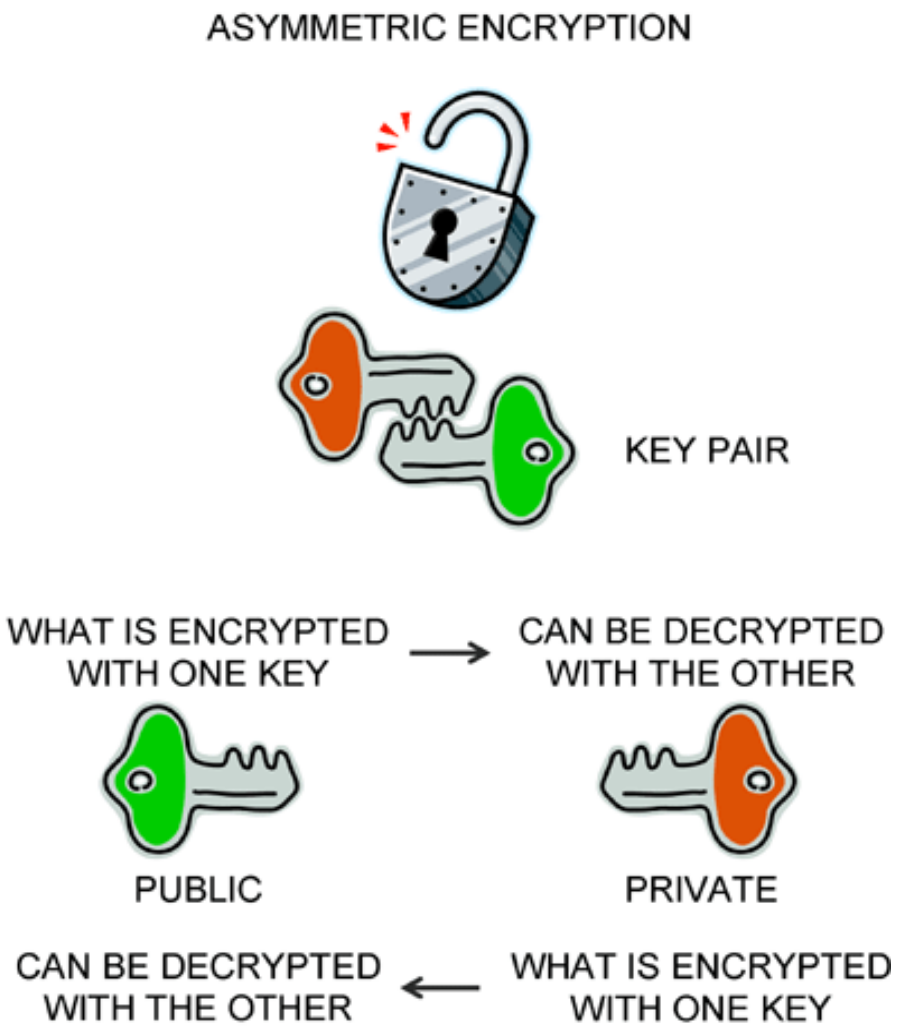
TLS/SSL, AT-TLS – Secret Key (Symmetric)



Source: http://middleware.its.state.nc.us/middleware/Documentation/en_US/htm/csqzas00/csq01skc.gif

Copyright © 2011 Applied Expert Systems, Inc.

TLS/SSL, AT-TLS – Public/Private Keys



Source: http://www.teracomtraining.com/tutorials/teracom-tutorial-asymmetric-encryption.gif

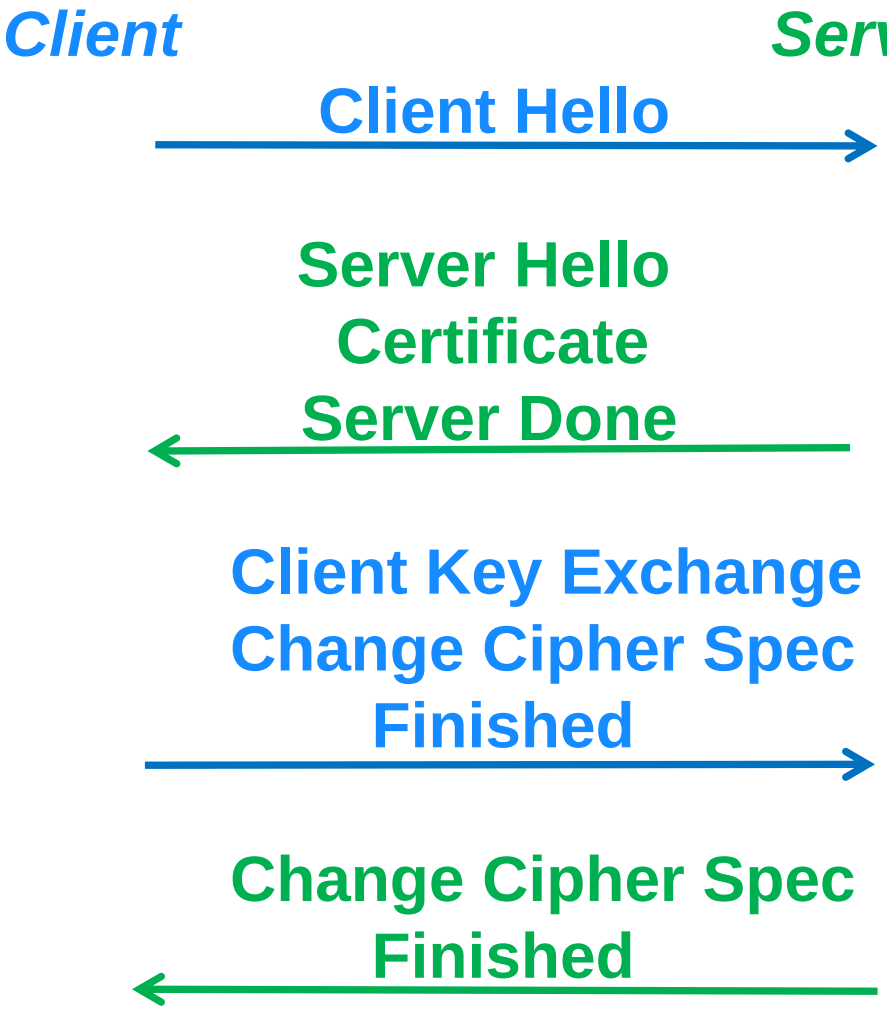
Copyright © 2011 Applied Expert Systems, Inc.

TLS/SSL Basic Flow

- Negotiate cipher suites and compression algorithms.
- Authenticate the server (and optionally the client) through certificates and public/private keys.
- **Server -> Client:** The server uses its private key to encrypt and the client uses the public key to decrypt.
- **Client -> Server:** the client uses the public key to encrypt and the server uses its private key to decrypt.
- Exchange random numbers and a pre-master secret, which is used with other data to create a shared secret key – the **Master Secret** is used to encrypt/decrypt the data.

Copyright © 2011 Applied Expert Systems, Inc.

TLS/SSL Handshake – Server Authentication



Hello
Highest SSL/TLS version supported
Ciphers and Compression Method
Session ID
Random data for key generation

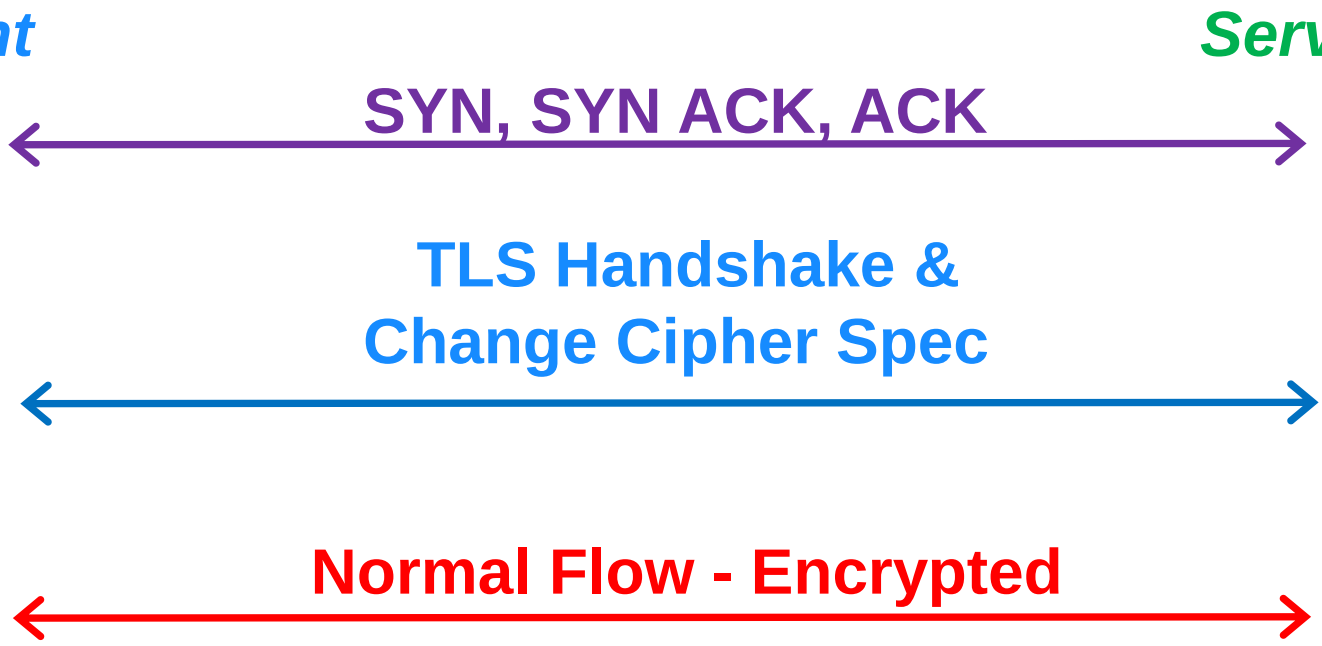
Certificate:
Server Certificate – contains server's public key.

Client Key Exchange
Premaster secret encrypted by server's public key. Both the client and the server generate the Master Secret key (symmetric) on their own using the pre-master secret and the random data that is generated from the SERVER_HELLO and CLIENT_HELLO commands.

Change Cipher Spec
Indicates that all subsequent data will be encrypted.

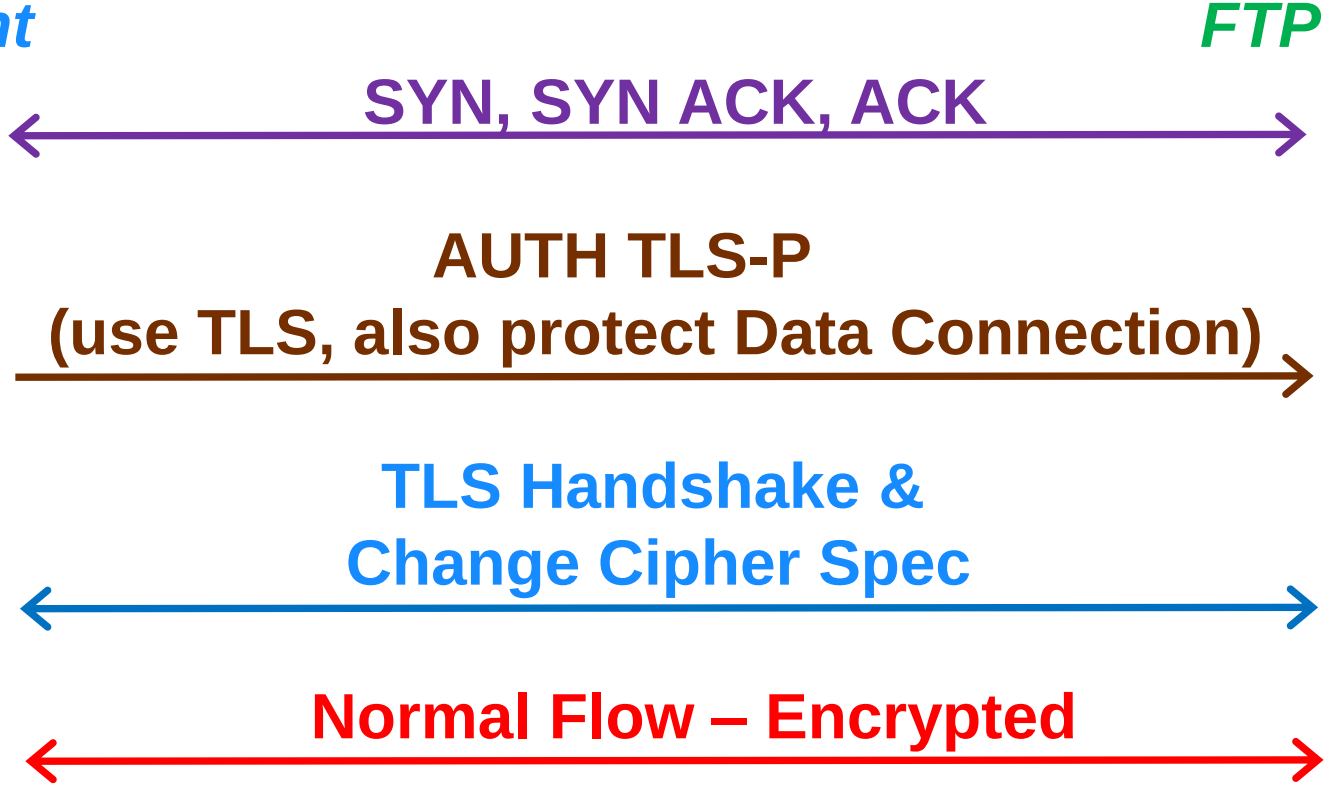
Copyright © 2011 Applied Expert Systems, Inc.

AT-TLS Flow



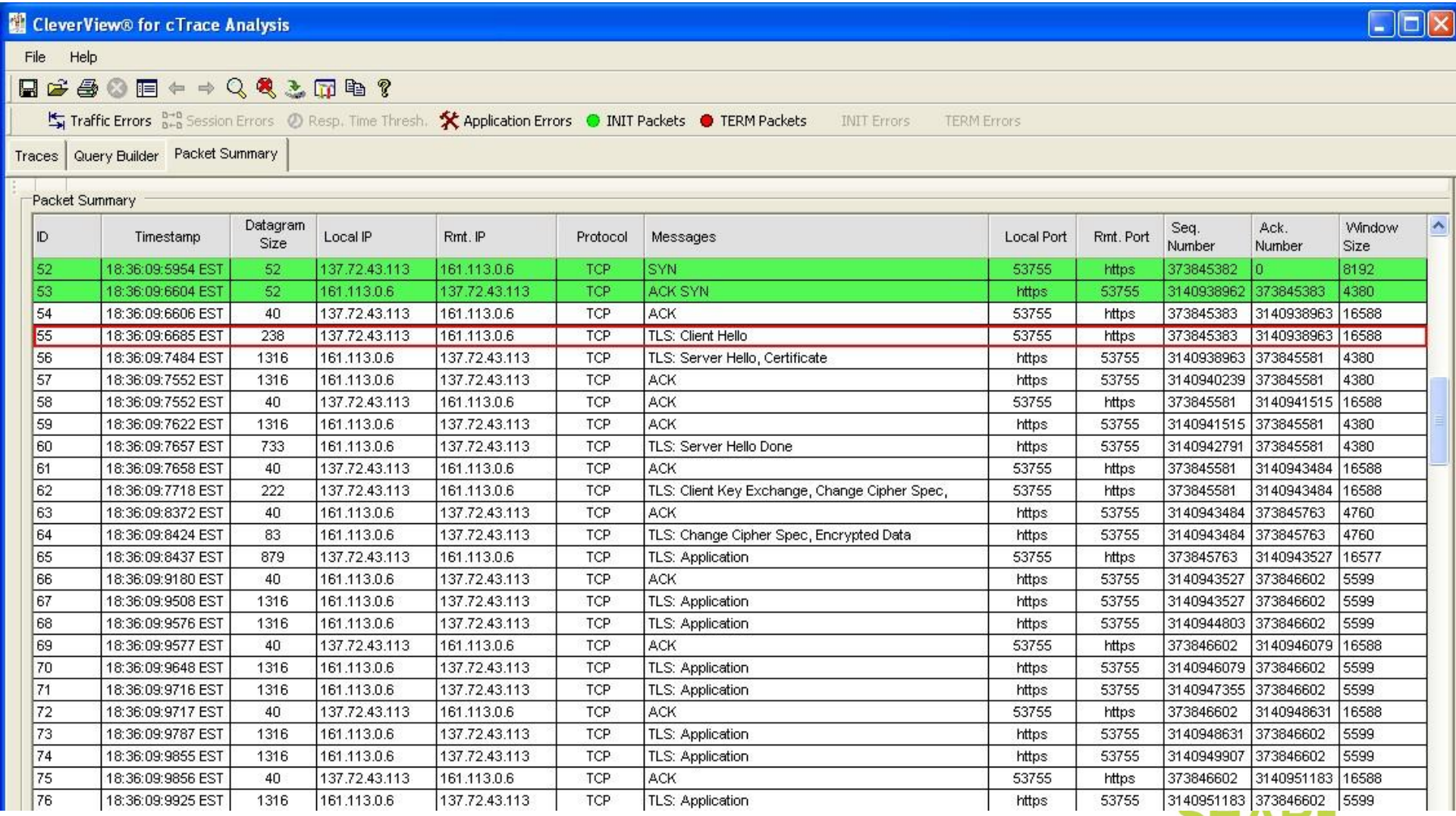
Copyright © 2011 Applied Expert Systems, Inc.

FTPS – FTP w/SSL Control Connection



Copyright © 2011 Applied Expert Systems, Inc.

HTTPS (Port 443)

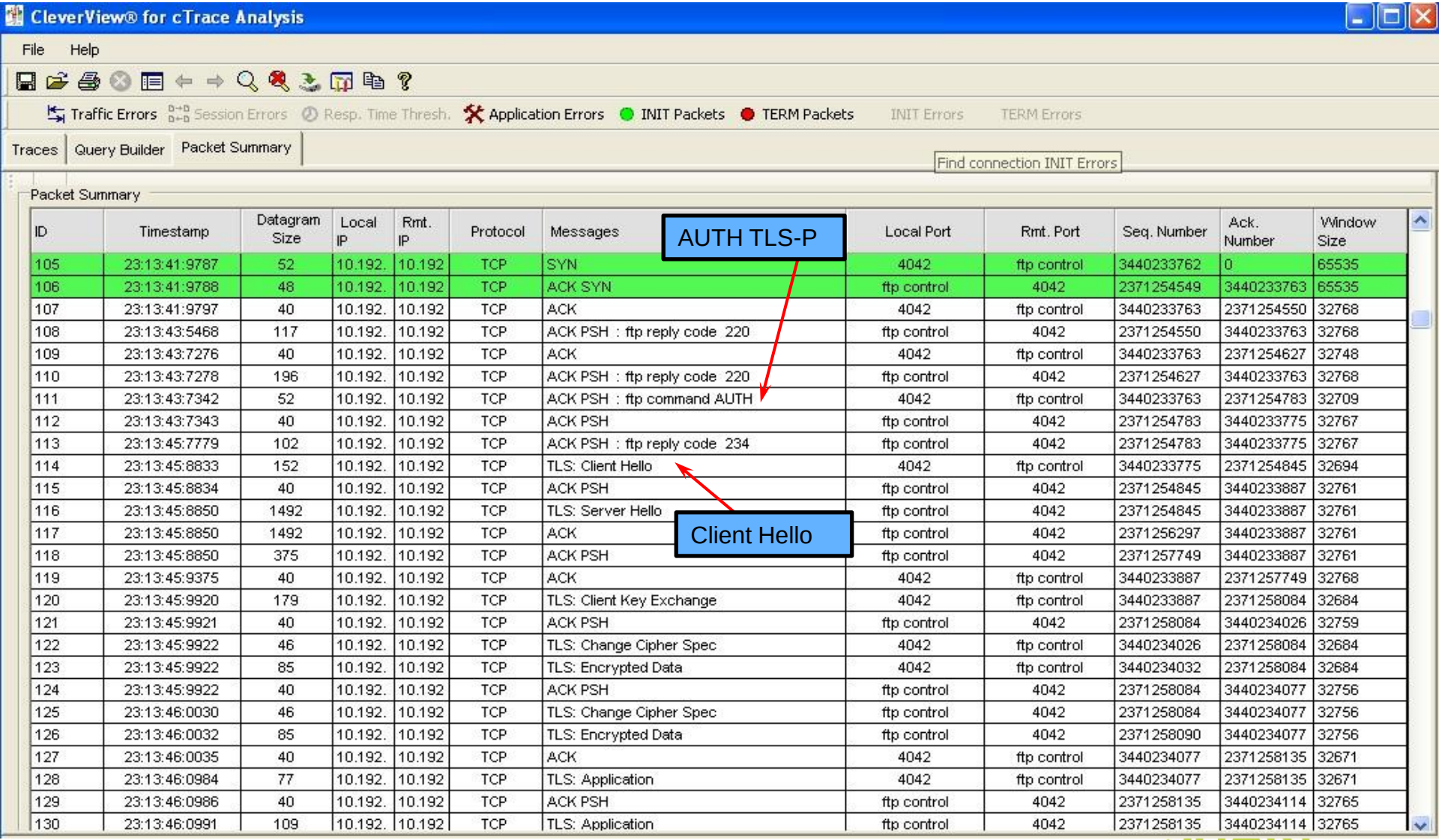


Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
52	18:36:09:5954 EST	52	137.72.43.113	161.113.0.6	TCP	SYN	53755	https	373845382	0	8192
53	18:36:09:6604 EST	52	161.113.0.6	137.72.43.113	TCP	ACK SYN	https	53755	3140938962	373845383	4380
54	18:36:09:6606 EST	40	137.72.43.113	161.113.0.6	TCP	ACK	53755	https	373845383	3140938963	16588
55	18:36:09:6685 EST	238	137.72.43.113	161.113.0.6	TCP	TLS: Client Hello	53755	https	373845383	3140938963	16588
56	18:36:09:7484 EST	1316	161.113.0.6	137.72.43.113	TCP	TLS: Server Hello, Certificate	https	53755	3140938963	373845581	4380
57	18:36:09:7552 EST	1316	161.113.0.6	137.72.43.113	TCP	ACK	https	53755	3140940239	373845581	4380
58	18:36:09:7552 EST	40	137.72.43.113	161.113.0.6	TCP	ACK	53755	https	373845581	3140941515	16588
59	18:36:09:7622 EST	1316	161.113.0.6	137.72.43.113	TCP	ACK	https	53755	3140941515	373845581	4380
60	18:36:09:7657 EST	733	161.113.0.6	137.72.43.113	TCP	TLS: Server Hello Done	https	53755	3140942791	373845581	4380
61	18:36:09:7658 EST	40	137.72.43.113	161.113.0.6	TCP	ACK	53755	https	373845581	3140943484	16588
62	18:36:09:7718 EST	222	137.72.43.113	161.113.0.6	TCP	TLS: Client Key Exchange, Change Cipher Spec,	53755	https	373845581	3140943484	16588
63	18:36:09:8372 EST	40	161.113.0.6	137.72.43.113	TCP	ACK	https	53755	3140943484	373845763	4760
64	18:36:09:8424 EST	83	161.113.0.6	137.72.43.113	TCP	TLS: Change Cipher Spec, Encrypted Data	https	53755	3140943484	373845763	4760
65	18:36:09:8437 EST	879	137.72.43.113	161.113.0.6	TCP	TLS: Application	53755	https	373845763	3140943527	16577
66	18:36:09:9180 EST	40	161.113.0.6	137.72.43.113	TCP	ACK	https	53755	3140943527	373846602	5599
67	18:36:09:9508 EST	1316	161.113.0.6	137.72.43.113	TCP	TLS: Application	https	53755	3140943527	373846602	5599
68	18:36:09:9576 EST	1316	161.113.0.6	137.72.43.113	TCP	TLS: Application	https	53755	3140944803	373846602	5599
69	18:36:09:9577 EST	40	137.72.43.113	161.113.0.6	TCP	ACK	53755	https	373846602	3140946079	16588
70	18:36:09:9648 EST	1316	161.113.0.6	137.72.43.113	TCP	TLS: Application	https	53755	3140946079	373846602	5599
71	18:36:09:9716 EST	1316	161.113.0.6	137.72.43.113	TCP	TLS: Application	https	53755	3140947355	373846602	5599
72	18:36:09:9717 EST	40	137.72.43.113	161.113.0.6	TCP	ACK	53755	https	373846602	3140948631	16588
73	18:36:09:9787 EST	1316	161.113.0.6	137.72.43.113	TCP	TLS: Application	https	53755	3140948631	373846602	5599
74	18:36:09:9855 EST	1316	161.113.0.6	137.72.43.113	TCP	TLS: Application	https	53755	3140949907	373846602	5599
75	18:36:09:9856 EST	40	137.72.43.113	161.113.0.6	TCP	ACK	53755	https	373846602	3140951183	16588
76	18:36:09:9925 EST	1316	161.113.0.6	137.72.43.113	TCP	TLS: Application	https	53755	3140951183	373846602	5599

Copyright © 2011 Applied Expert Systems, Inc.

AT-TLS - FTP w/SSL



ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
105	23:13:41:9787	52	10.192.	10.192	TCP	SYN	4042	ftp control	3440233762	0	65535
106	23:13:41:9788	48	10.192.	10.192	TCP	ACK SYN	ftp control	4042	2371254549	3440233763	65535
107	23:13:41:9797	40	10.192.	10.192	TCP	ACK	4042	ftp control	3440233763	2371254550	32768
108	23:13:43:5468	117	10.192.	10.192	TCP	ACK PSH : ftp reply code 220	ftp control	4042	2371254550	3440233763	32768
109	23:13:43:7276	40	10.192.	10.192	TCP	ACK	4042	ftp control	3440233763	2371254627	32748
110	23:13:43:7278	196	10.192.	10.192	TCP	ACK PSH : ftp reply code 220	ftp control	4042	2371254627	3440233763	32768
111	23:13:43:7342	52	10.192.	10.192	TCP	ACK PSH : ftp command AUTH	4042	ftp control	3440233763	2371254783	32709
112	23:13:43:7343	40	10.192.	10.192	TCP	ACK PSH	ftp control	4042	2371254783	3440233775	32767
113	23:13:45:7779	102	10.192.	10.192	TCP	ACK PSH : ftp reply code 234	ftp control	4042	2371254783	3440233775	32767
114	23:13:45:8833	152	10.192.	10.192	TCP	TLS: Client Hello	4042	ftp control	3440233775	2371254845	32694
115	23:13:45:8834	40	10.192.	10.192	TCP	ACK PSH	ftp control	4042	2371254845	3440233887	32761
116	23:13:45:8850	1492	10.192.	10.192	TCP	TLS: Server Hello	ftp control	4042	2371254845	3440233887	32761
117	23:13:45:8850	1492	10.192.	10.192	TCP	ACK	ftp control	4042	2371256297	3440233887	32761
118	23:13:45:8850	375	10.192.	10.192	TCP	ACK PSH	ftp control	4042	2371257749	3440233887	32761
119	23:13:45:9375	40	10.192.	10.192	TCP	ACK	4042	ftp control	3440233887	2371257749	32768
120	23:13:45:9920	179	10.192.	10.192	TCP	TLS: Client Key Exchange	4042	ftp control	3440233887	2371258084	32684
121	23:13:45:9921	40	10.192.	10.192	TCP	ACK PSH	ftp control	4042	2371258084	3440234026	32759
122	23:13:45:9922	46	10.192.	10.192	TCP	TLS: Change Cipher Spec	4042	ftp control	3440234026	2371258084	32684
123	23:13:45:9922	85	10.192.	10.192	TCP	TLS: Encrypted Data	4042	ftp control	3440234032	2371258084	32684
124	23:13:45:9922	40	10.192.	10.192	TCP	ACK PSH	ftp control	4042	2371258084	3440234077	32756
125	23:13:46:0030	46	10.192.	10.192	TCP	TLS: Change Cipher Spec	ftp control	4042	2371258084	3440234077	32756
126	23:13:46:0032	85	10.192.	10.192	TCP	TLS: Encrypted Data	ftp control	4042	2371258090	3440234077	32756
127	23:13:46:0035	40	10.192.	10.192	TCP	ACK	4042	ftp control	3440234077	2371258135	32671
128	23:13:46:0984	77	10.192.	10.192	TCP	TLS: Application	4042	ftp control	3440234077	2371258135	32671
129	23:13:46:0986	40	10.192.	10.192	TCP	ACK PSH	ftp control	4042	2371258135	3440234114	32765
130	23:13:46:0991	109	10.192.	10.192	TCP	TLS: Application	ftp control	4042	2371258135	3440234114	32765

Copyright © 2011 Applied Expert Systems, Inc.

TLS Header

Offset	Length	Description	Decimal Value	Meaning
0	1	Content Type	20 (0x14)	Change Cipher Spec
			21 (0x15)	Alert
			22 (0x16)	Handshake
			23 (0x17)	Application
1	2	Version		
1	1	Major Version	3	
2	1	Minor Version	0	SSLv3
			1	TLS 1.0
			2	TLS 1.1
			3	TLS 1.2
3	2	Length	N	The length of the Protocol Message
5	N	Protocol Message		

Copyright © 2011 Applied Expert Systems, Inc.

Sample TLS/SSL Decoding

Hex Data:
16 03 01 00 C1 01 00 00 BD 03 01 4B 71 F1 69 DA 10 ….

Secure Socket Layer
- TLSv1 Record Layer: Handshake Protocol: Client Hello
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 193
  - Handshake Protocol: Client Hello
    - Handshake Type: Client Hello (1)
    - Length: 189
    - Version: TLS 1.0 (0x0301)
    - Random
      - GMT Unix Time: Feb 9, 2010 15:36:09.0000000000
      - Random Bytes: DA10 …
    - Session ID Length: 32
    - Session ID: 2D585DAEF198D9BB951DD9F58D7766465B88A493B98ACC3C...
    - Cipher Suites Length: 70
    - Cipher Suites (35 suites)
      - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
      - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
      - Cipher Suite: …….

28 Random Bytes - to be used with the premaster secret to generate the symmetric key.

Ciphers are listed in order of preference – from the strongest to the weakest

Copyright © 2011 Applied Expert Systems, Inc.