# SHARKFEST 2015 WIRESHARK DEVELOPER AND USER CONFERENCE

#### COMPUTER HISTORY MUSEUM

# Visualizations and Correlations in Troubleshooting

Kevin Burns Comcast

kevin\_burns@cable.comcast.com

### **Comcast Technology Groups**

- Cable CMTS, Modem, Edge Services
- Backbone Transport, Routing
- Converged Regional Area Networks
- Metro Ethernet Services
- National Data Center
- Digital Voice Services (CDV)
- Domain Name / DHCP Services
- Product Engineering / Development
- Home Services (TV, Internet, Security)
- Business / Commercial Services (L2VPN, MPLS, etc)

### How Do It Know ???

- HINT: It don't.
- Computers only know as much as <u>YOU</u> do.
- We can only apply what <u>WE</u> know.
- How do we get from "I don't know" to solving the problem??

ヽ (ツ) /

### Why am I talking about Visualization?

- Troubleshooting is more of an art than a science. This presentation is about how I describe my own "art". Everyone will develop their own art (ie: methodologies).
- Nobody can teach you this. They can only help you learn to how to incorporate ideas and techniques into your own art.
- A lot can be gained from looking at different types of thinking and methods to incorporate into your own set of tools and techniques.
- Visualizing problems is the most common process people are involved in during a troubleshooting effort.
- To be a successful problem solver you need to understand how the components of visualization fit together.

### **Understanding Visualization Components**

- In order to visualize a problem we must:
  - Be able to recognize how a problem <u>manifests</u> itself to it's users, engineers and inside of packet captures.
  - <u>Categorize</u> the problem based on it's manifestation <u>behavior</u> to users and protocol interactions
  - Determine what <u>technical indicators</u> exist that allow us to <u>correlate</u> information to visualize the problem.
  - Understand the <u>impact</u> of various technical indicators.
- The goal of visualization is to determine how a problem <u>manifests</u> itself and <u>correlate</u> it's <u>technical indicators</u> to produce a <u>diagnosis</u>.
- Visualization is about seeing and recognizing patterns on several different levels.
- Problem solving is about utilizing visualization techniques to resolve an issue.

# **Components of Visualization**

- Problem Manifestation
  - The outward or perceptible indication of a problem.
  - Determine how the problem manifests inside of a packet capture.
  - Categorize of the problem and it's behavior.
- Technical Indicators
  - Characteristics of a problem's manifestation.
  - Identify a problem's technical indicators
- Correlation
  - Correlation of various technical indicators.
  - Correlate technical indicators with a problem's manifestation
  - Look for repeatable patterns.
- Diagnosis
  - The foundation of a definitive diagnosis is based on correlation of a problem's manifestation and it's technical indicators.

### **Problem Solving Cycle**



#### **Problem Manifestation**

- How is it known the problem exists?
- How is the problem viewed?
  - By users
  - By engineers
  - By management
  - In packets
- What technical indicators does the problem manifest itself through?
  - Retransmissions
  - Time-outs, Delays
  - Application Messages
- What tools can help you uncover more methods of how the problem manifests itself?
- What techniques can you use to look for patterns?
- Understand how different technical indicators relate to impact !!

perspectives (at first)

**Often different** 

### **Problem Categorization by OSI Model**

- Problems will manifest themselves in one or more layers of the OSI Model.
- Problems are almost always isolated to a single layer.
- The first and most important step in troubleshooting is to determine what layer of the OSI model the problem lives in. If you don't want to understand the OSI model at least understand the protocol dependancies you are dealing with
- OSI teaches us about dependancies, that is why it's useful.



# **Problem Categorization by Type**

- Loss of Connectivity
  - Complete and total loss of end to end connectivity at one or more layers.
  - Application failures, TCP Resets, Ping failures
- Intermittent Connectivity
  - Inconsistent end to end connectivity at one or more layers.
  - Dropped packets, sessions
- Degraded Performance
  - End to end connectivity is good but performance over the connection is suffering
  - Low Throughput, Latency impact
- Unknown
  - Technical indicators are unknown (concentrate on changes in state).

### **Case Study: Manifestation of Server Delay**

#### Application

Remedy Ticketing System

#### Symptoms

- User experiencing minute long delays when performing lookups.
- Network path appears to be clean. No loss or latency.

#### Manifestation

- Problem manifests as delay
- Delay is obvious in the packets

#### **Case Study: Manifestation of Server Delay**

No.	61 I	delta.t	Destination	Source	Protocol	Info
	1	0.000000	172.30.1.134	172.29.4.89	TCP	s1p > 36504 [PSH, ACK] Seq=1 Ack=1 win=17520 Len=224
	2	0.095926	172.29.4.89	172.30.1.134	TCP	36504 > slp [ACK] Seq=1 Ack=225 Win=8760 Len=0
	3	79.318670	172.29.4.89	172.30.1.134	TCP	36504 > slp [ACK] Seq=1 Ack=225 win=8760 Len=1460
	-4	0.007840	172.29.4.89	172.30.1.134	TCP	36504 > slp [PSH, ACK] Seq=1461 Ack=225 Win=8760 Len=
17	5	0.000035	172.30.1.134	172.29.4.89	TCP	slp > 36504 [ACK] Seq=225 Ack=2921 Win=17520 Len=0
	6	0.007812	172.29.4.89	172.30.1.134	TCP	36504 > slp [PSH, ACK] Seq=2921 Ack=225 Win=8760 Len=
	7	0.187247	172.30.1.134	172.29.4.89	TCP	slp > 36504 [ACK] Seq=225 Ack=4381 win=17520 Len=0
	8	0.369366	172.29.4.89	172.30.1.134	TCP	36504 > slp [PSH, ACK] Seq=4381 Ack=225 Win=8760 Len=
	9	0.131341	172.30.1.134	172.29.4.89	TCP	slp > 36504 [ACK] Seq=225 Ack=5841 win=17520 Len=0
	10	0.045120	172.29.4.89	172.30.1.134	TCP	36504 > slp [PSH, ACK] Seq=5841 Ack=225 win=8760 Len=
	11	0.000036	172.29.4.89	172.30.1.134	TCP	36504 > slp [PSH, ACK] Seq=7301 Ack=225 Win=8760 Len=
	12	0.000028	172.30.1.134	172.29.4.89	TCP	slp > 36504 [ACK] Seq=225 Ack=7357 Win=17520 Len=0
	13	0.888008	172.30.1.134	172.29.4.89	TCP	slp > 36504 [P5H, ACK] Seq=225 Ack=7357 win=17520 Len
	14	0,167088	172.29.4.89	172.30.1.134	TCP	36504 > slp [ACK] Seq=7357 Ack=501 win=8760 Len=0
	15	0.237163	172.29.4.89	172.30.1.134	TCP	36504 > s1p [PSH, ACK] Seq=7357 Ack=501 Win=8760 Len= *
4	15			ш.,	118592	
(41)	Fr	ame 3: 1514	bytes on wir	e (12112 bits)	1514	bytes captured (12112 bits)
100	Et	hernet II.	Src: Cisco_41	:d4:09 (00:07:4	f:41:d	4:09), Dst: Dellcomp_02:fb:d0 (00:b0:d0:02:fb:d0)
(#)	In	ternet Prot	cocol version	4. 5rc: 172.30.	1.134	(172, 30, 1, 134), Dst; 172, 29, 4, 89 (172, 29, 4, 89)
THE	Tr	ansmission	Control Proto	col. Src Port:	36504	(36504), DST PORT: slp (1605), Seg: 1, Ack: 225, Len: 1460
(E)	Da	ta (1460 by	/tes)			
00	00	00 b0 d0	02 fb d0 00 0	7 4f 41 d4 09	08 00	45 00E.
00	20	05 GC 9a	e/ 40 00 TD 0	o 81 19 ac 1e	7F 46	
00	30	22 38 1b	fd 00 00 80 0	1c b8 76 41	7b 42	00 00 "8
00	40	00 01 00	00 00 00 00 00	00 00 00 00 00	00 00	00 00
00	50	10 00 01	Ar 56 12 20 A	7 7F 12 6h 67	75 77	6a 72 V ve clebuene

What do you see as the manifestation of the problem? Does it correlate with the user experience?

#### **Client to Server Visualization**

No.	delta.t Dest	tination	Source	Protocol	Info	tcp.seq	tcp.ack	tcp.len r	rpc,xid
1	0.000000 17.	2.30.1.134	172.29.4.89	RPC:390620	V8 proc-94 call (Reply In 11)		1	1 224	0x76417b42
2	0.095926 177	2.29.4.89	172.30.1.134	TCP	36504 > slp [ACK] seq=1 Ack=27	25 Win-	1 2	25 0	
3	79.318670 172	2.29.4.89	172.30.1.134	TCP	[TCP segment of a reassembled	PDU]	1 2	25 1460	
4	0.007840 17.	29.4.89	172.30.1.134	TCP	[TCP segment of a reassembled	PDU] 1	461 23	25 1460	
5	0.000035 172	2. 38. 1. 134	172.29.4.89	TCP	s1p > 36504 [ACK] Seq=225 Ack-	-2921 W	225 293	21 0	-
6	0.007812 177	2.29.4.89	172.30.1.134	TCP	[TCP segment of a reassembled	PDU] 2	921 23	25 1460	13
7	0.187247 172	2.30.1.1.1	172.29.4.89	TCP	s1p > 36504 [ACK] Seq=225 Ack-	=4381 W	225 43	81 0	
8	0.369366 177	2,29.4.89	172.30.1.134	TCP	[TCP segment of a reassembled	PDU] 4	381 23	25 1460	
9	0.131341 177	2.30.1.134	172 29.4.89	TCP	s1p > 36504 [ACK] seq=225 Ack-	-5841 W	225 58	1 0	
10	0.045120 172	2.29.4.89	172.30 1.134	TCP	[TCP segment of a reassembled	POU] 5	841 2	25 1460	and the second s
11	0.000036 177	2.29.4.89	172.30.1.134	RPC:390620	V8 proc-94 Reply (Call In 1)	7	301 2	25 56	0x76417b42
12	0.000028 172	2.30.1.134	172.29.4.89	TCP	s1p > 36504 [ACK] Seq=225 Ack-	-7357 W	225 73	57 0	
13	0.888008 173	2.30.1.134	172.29.4.89	RPC:390620	V8 proc-5 Call (Reply In 15)		225 73	57 276	0x75417b42
14	0.167088 172	2.29.4.89	172.30.1.134	TCP	36504 > s1p [ACK] Seq=7357 Act	c=501 W 7	357 50	01 0	
15	0.237163 172	2.29.4.89	172.30.1.134	RPC:390620	V8 proc-5 Reply (Call In 13)	7	357 50	180	0x75417b42
16	0.004846 177	2.30.1.134	172.29.4.89	RPC:390620	v8 proc-5 call (Reply In 18)		501 75	37 256	0x74417b42
17	0.171415 177	2.29.4.89	172.30.1.134	TCP	26504 > slp [ACK] seq=7537 Ack	(=757 W 7	537 7	57 0	
18	0.000020 177	2.29.4.89	172.30.1.134	RPC:390620	v8 proc-5 Reply (call to 16)	7	537 7	57 284	0x74417b42
19	0.000364 177	2.30.1.134	172.29.4.89	RPC:390620	V8 proc-1 call (R				
20	0.086031 177	2.29.4.89	172.30.1.134	RPC:390620	V8 proc-1 Reply (				1
21	0.001777 177	2.30.1.134	172.29.4.89	RPC:390620	v8 proc-94 sall ( VVNV IS I	there a 79	second r	Jause bet	ween
22	0.036926 177	2.29.4.89	172.30.1.134	RPC:390620	V8 proc-94 Reply				
23	0.163806 177	2.30.1.134	172.29.4.89	TCP	s1p > 36504 [ACK] the clien	nt request.	and serv	er respon	se?
74	0 011284 177	7 20 1 124	177 70 4 90	00/11200620	WR pror_77 call (	it i oquoot		or roopon	
1 in					Take no	ote of the T	CP Dela	ved ACK	as well.

#### Visualization Techniques:

Protocol Decode (forced to RPC) TCP SEQ+LEN=ACK Application Transaction ID Column

#### **Technical Indicators:**

TCP ACK TCP Delayed ACK Application Delay

#### **Server to Backend DB Visualization**

No.	delta.t	Destination	Source	Protocol	Info	tcp.seq	tcp.ack	tcp.len	4
	1 0.000000	172.30.0.71	172,30,1,134	TNS	Request, Data (6), Data		1 1	91	
	2 0.001004	172.30.1.134	172.30.0.71	TNS	Response, Data (6), Data[Packet	51	1 92	788	
	3 0.001222	172.30.0.71	172.30.1.134	TNS	Request, Data (6), Data	9	2 789	60	
	4 0.000980	172.30.1.134	172,30.0.71	TNS	Response, Data (6), Data	78	9 152	16	
	5 0.098316	172.30.0.71	172,30.1.134	TCP	43660 > ncube-lm [ACK] Seq=152 A	ck 15	2 805	0	
	6 0.024814	172.30.1.134	172.30.0.71	TNS	Response, Data (6), Data[Packet	si	1 1	708	
	7 0.002122	172.30.0.71	172.30.1.134	TNS	Request, Data (6), Data		1 709	60	
	8 0.001190	172.30.1.134	172.30.0.71	TNS	Response, Data (6), Data	70	9 61	16	
	0.007618	172.30.0.71	172.30.1.134	TCP	47944 > ncube-lm [ACK] Seq=61 Ac	k= 6	1 725	0	E
1	b) 59.780412	1 2.30.0.71	172.30.1.134	TNS	Request, Data (6), Data		1 1	. 251	
1	0.002740	172.30.1.134	172.30.0.71	TNS	Response, Data (6), Data[Packet	si	1 252	540	
	2 0.002730	172.30.0.71	172.30.1.134	TNS	Request, Data (6), Data[Packet s	12	1 1	1155	
	.3 0.001092	172.30.0.71	172.30.1.134	TNS	Request, Data (6), Data	25	2 541	60	
	4 0.000490	172.30.0.71	172.30.1.134	TNS	Request, Data (6), Data		1 1	. 322	
	5 0.000006	172.30.1.134	172.30.0.71	TNS	Response, Data (6), Data	54	1 312	16	
	6 0.001036	172.30.0.71	172.30.1.134	TNS	Request, Data (6), Data	6	1 725	246	
1	7 0.000260	172.30.0.71	172.30.1.134	TNS	Request, Data (6), Data	31	557	245	
	0.001092	172.30.0.71	172.30.1.134	TNS	Request, Data (6), Data		1 1	151	-
1									

#### **Technical Indicators:**

Delay TCP SEQ+LEN=ACK Application Request/Response <u>Behavior</u> Why does the Remedy Server stop talking to the Database for 59 seconds after ACKing all responses???

#### **Correlation of Client/Server Visualizations**



#### What are Technical Indicators?

- Assuming the correct packets have been captured, the problem will always exist inside of the packets.
- Technical Indicators are feedback mechanisms found in packet communications. (sometimes you really have to dig for them)
- They are not symptoms.
  - I tend to avoid using the word symptom as people tend to associate it with being the cause.
- Problems will exist inside of packets in several ways
  - Explicit packet feedback mechanisms
  - Implicit packet feedback mechanisms
  - Extrapolated Data and Measurements
  - Behavior and Relationship Based (Correlation)

### **Feedback Mechanisms**

- Asssuming the correct packets have been captured, the problem will always exist inside of the packets.
- Problems will exist inside of packets in several ways
  - Explicit packet feedback mechanisms:
    - TCP (FIN, RST)
    - Application Messages
    - ICMP return types/codes.
  - Implicit packet feedback mechanisms:
    - Timing
    - Behavior
    - Other Correlative Factors
  - Extrapolated Data and Measurements
    - Latency
    - Throughtput
    - Examples, Behavior, Relationships

Complexity Increases

#### **Explicit Feedback Mechanisms**



Explicit: Application Feedback Implicit: Timing (Delay) Why is TCP waiting 3 seconds to retransmit the first lost segment?

#### **Implicit Feedback Mechanisms**

No.	rel.t	Destination	Source	Protocol	Info	tcp.seq	tcp.ack	tcp.len	
	1 0.000000	172.20.95.132	172.20.93.32	SSH	Encrypted request packet len=1460	1	1	1460	
	2 0.000004	172.20.95.132	172.20.93.32	SSH	[TCP Previous segment not captured] Encry	p 2921	1	1460	
	3 0.000010	172.20.93.32	172,20,95,132	TCP	ssh > 57648 [ACK] Seq=49 Ack=1461 win=225	5 49	1461	0	
	4 0.000017	172.20.95.132	172.20.93.32	SSH	Encrypted request packet len=1460	4381	1	1460	
	5 0.000022	172.20.93.32	172.20.95.132	TCP	[TCP Dup ACK 3#1] ssh > 57648 [ACK] Seq=4	9 49	1461	0	
	6 0.000028	172.20.95.132	172.20.93.32	SSH	Encrypted request packet len=1460	5841	1	1460	
	7 0.000034	172.20.93.32	172.20.95.132	TCP	[TCP Dup ACK 3#2] ssh > 57648 [ACK] Seq=4	9 49	1461	0	
							T		
No:	relat	Destination	Source	Protocol	Info	tcp.seq	tcp.ack	tcp.len	-
42	1 0.006996	172.20.95.132	172.20.93.32	SSH	Encrypted request packet len=1460	31098:	L 97	1460	
42	2 0.006999	172.20.93.32	172.20.95.132	TCP	[TCP Dup ACK 244#89] ssh > 57648 [ACK] 54	eq 97	1461	0	
42	3 0.007040	172.20.95.132	172.20.93.32	SSH	Encrypted request packet len=1460	312441	97	1460	(
42	4 0.007046	172.20.93.32	172.20.95.132	TCP	[TCP Dup ACK 244#90] ssh > 57648 [ACK] Se	eq 💋	7 1461	0	
42	5 0.007057	172.20.95.132	172.20.93.32	SSH	Encrypted request packet len=1460	31390	L 97	1460	5
42	6 0.007063	172.20.93.32	172.20.95.132	TCP	[TCP Dup ACK 244#91] ssh > 57648 [ACK] Se	eq 93	7 1461	0	81
42	7 0.007069	172.20.95.132	172.20.93.32	SSH	Encrypted request packet len=1460	1536	L 97	1460	
42	8 0.007073	172.20.93.32	172.20.95.132	TCP	[TCP Dup ACK 244#92] ssh > 57648 [ACK] Se	eq 97	1461	. 0	
42	9 0.007078	172.20.95.132	172.20.93.32	SSH	Encrypted request packet len=1460	31682	L 97	1460	8 1
43	0 0.007082	172.20.93.32	172.20.95.132	TCP	[TCP Dup ACK 244#93] ssh > 57648 [ACK] Se	93	7 1461	0	8
43	1 0.007085	172.20.95.132	172.20.93.32	SSH	Encrypted request packet len=712	318283	L 97	712	ŝ.,
43	2 0.007089	172.20.93.32	172.20.95.132	TCP	[TCP Dup ACK 244#94] ssh > 57648 [ACK] 50	eq 97	1461	0	6
43	3 0.009087	172.20.93.32	172.20.95.132	5SH	Encrypted response packet len=48	9	7 1461	48	
43	4 0.049168	172.20.95.132	172.20.93.32	TCP	57648 > ssh [ACK] Seq=318993 Ack=145 win-	-4 31899	3 145	0	
43	5 0.202230	172.20.95.132	172.20.93.32	SSH	[TCP Retransmission] Encrypted request pa	ac 146	1 145	1460	
43	6 0.202244	172.20.93.32	172.20.95.132	TCP	ssh > 57648 [ACK] Seq=145 Ack=14601 Win=2	2 14	5 14601	0	-
e					ш.				
Te	chnical Ind	dicators.			Why did 32 not East Petransmit a	ftor receiv	ing 3		
							ing 5		
					duplicate ACKs?				
Ev	nlicit <sup>.</sup> TCP	Retransmission							
					Why did 32 wait 200mg before re-	transmittin	a tho		
Im	plicit: Timin	ig (Delay)				uansmittin	y ne		
Ro	havior (pot	East Dotranem	itting)		lost segment?				
ре		Tast Retransm							

#### **Extrapolated Data & Measurements**

	e Channel   FD		S IPX JXTA NCP	RSVP SCTP	TCP: 2 Token I	Ring UDP US	B WLAN
			IPv4 Endpoint	ts			
Address 4 Pa	ackets 4 Bytes	<ul> <li>Tx Packet</li> </ul>	s 🖣 Tx Bytes 👎 R	x Packets 4 F	x Bytes 🔹 Lati	tude 🕈 Longiti	ude 👎
172.28.85.156	9 209 11 42	6 894 7	456 11 311 464	1 753	115 430	8	12
172.27.37.13	9 209 11 42	6 894 1	753 115 430	7 456	11 311 464	~	1
		100 - 100 - 100					and the second second
Wireshark: 216	Expert Infos	100.08.0			ang bas. No.		
Wireshark: 216 Errors: 0 (0) Wi	Expert Infos arnings: 2 (43)	Notes: 55 (168	) Chats: 4 (5) Deta	ils: 216 Pack	et Comments: 0		
Wireshark: 216 Errors: 0 (0) Wa Group 4 P	Expert Infos arnings: 2 (43) trotocol	Notes: 55 (168	) Chats: 4 (5) Deta	ils: 216 Pack	et Comments: 0	Count	
Wireshark: 216 Errors: 0 (0) Wa iroup 4 P E Sequence 1	Expert Infos armings: 2 (43) frotocol fCP	Notes: 55 (168 Summary Previous se	) Chats: 4 (5) Deta gment not captured	ils: 216 Pack (common at	et Comments: 0 ◀ capture start)	Count	

<u>Technical Indicators:</u> Lost Packets and TCP Retransmissions

Packet Loss = 0.003 (.3%)

### **Finding Round Trip Latency**

Eile E	dit <u>V</u> iew <u>G</u> o	Captu	re <u>A</u> nałyze	Statistics	Telephor	ny <u>T</u> ools	Internals	Help	No. 40. 151		
0 0	1 🔳 🔬		🖻 X 🖻	0	> 🛸 🚳	Ŧ 2		QQ	् 🖂 🛛		1 🎭 🖗 🛛 🧱
Filter:							Express	ion Cle	ar Apply	Save	
lo.	delta.t	<ul> <li>Destin</li> </ul>	ation	Source	š	Protocol	Info				
7812	0.04923629	8 172.	27.37.13	172.	28.85.15	6 TCP	46646 :	> commpl	ex-link	[ACK]	Seq=9171745 Ack=1 Win=5888 1
9086	0.04922485	3 172.	27.37.13	172.	28.85.15	6 TCP	46646 3	> commp1	ex-1ink	[ACK]	Seq=10722265 Ack=1 win=5888
8242	0.04921722	5 172.	27.37.13	172.	28.85.15	6 TCP	46646 :	> commpl	ex-link	[ACK]	Seq=9697345 Ack=1 Win=5888 1
5	0.04920387	3 172.	27.37.13	172.	28.85.15	6 TCP	46646 >	> commp]	ex-link	[ACK]	Seq=1 Ack=1 Win=5888 Len=0
21	0.04919815	1 172.	27.37.13	172.	28.85.15	6 TCP	46646	> commpl	ex-link	[ACK]	Seq=11705 Ack=1 Win=5888 Ler
63	0.04918289	2 172.	27.37.13	172.	28.85.15	6 TCP	46646	> commp1	ex-link	[ACK]	Seq=49665 Ack=1 Win=5888 Ler
7037	0.04917717	0 172.	27.37.13	172.	28.85.15	6 TCP	46646 3	> commp1	ex-link	[ACK]	5eq=8208145 Ack=1 Win=5888 1
37	0.04916954	0 172.	27.37.13	172.	28.85.15	6 TCP	46646 :	> commpl	ex-link	[ACK]	Seq=26305 Ack=1 Win=5888 Ler
81.87	0.04914856	0 172.	27.37.13	172.	28.85.15	6 TCP	46646 :	> commpl	ex-link	[ACK]	Seq=9627265 Ack=1 Win=5888 I
8933	0.04914855	9 172.	27.37.13	172.	28,85.15	6 TCP	46646	> commp]	ex-link	[ACK]	5eq=10533925 Ack=1 win=5888
7051	0.04914855	9 172.	27.37.13	172.	28.85.15	6 TCP	46646 :	> commp1	ex-link	[ACK]	Seq=8227125 Ack=1 Win=5888 1
10	0.04914474	5 172.	27.37.13	172.	28.85.15	6 TCP	46646 :	> commpl	ex-link	[ACK]	Seq=2945 Ack=1 Win=5888 Len=
9209	0.04913902	3 172.	27.37.13	172.	28.85.15	6 TCP	46646 :	> commpl	ex-link	[ACK]	5eq=10879002 Ack=2 Win=5888
8876	0.04913330	1 172.	27.37.13	172.	28.83.15	6 TCP	46646 ;	> commpl	ex-link	[ACK]	Seq=10463845 Ack=1 win=5888
8791	0.04913139	3 172.	27.37.13	172.	28.85.15	O TCP	46646	> commpl	ex-link	[ACK]	Seq=10382085 Ack=1 win=5888
9136	0.04912567	2 172.	27.37.13	172.	28.85.15	6 TCF	46646	> commp1	ex-link	[ACK]	Seq=10786505 Ack=1 win=5888 *
- Lin					m						*
	File: "\\cable\en	g-dfs\Us	ers2\kburns0	0\proj	Profile	: Default					
Toch	nical Ind	icato	re:							Roun	d Trip Latency = 49ms
			13.								
Timi	na (Pound	l Trin	Time)		Sortin	a hy Da	alta Tim	na late		tho r	ound trin latency II

# **Throughput Measurement**

#### http://www.switch.ch/network/tools/tcp\_throughput/

Maximum throughput with a <u>TCP window of 64 KByte and RTT of 49.0 ms</u> <= **10.45 Mbit/sec.** 

hernet: 2 Fibre Channel FDDJ IPv4:1 IP	v6 IPX JXTA NCP RSV	P SCTP TCP:1	Token Ring UD	P USB WLAN		
		IPv4 Conversation	ns			
idress A 🖣 Address B 🖣 bps AB 🖣 Pac	kets A+B      Buration	Bytes A+B + Pac	kets A-B 4 Byt	es A-B 4 Bytes	Rel Start < P	ackets 4 bps A-8
72.27.37.13 172.28.85.156 7127429.27	7 456 12.6963	11.311.464	1.753	115 430 11 42	894 0.000000000	9.209 7273
		m				
Name resolution 👘 Limit to display the	r'					
			10		1.1	-
Help Copy			Follow Stream	m Graph A→B	Graph 8→A	Close
3010 62						

#### Window scaling is enabled. Shouldn't it have more TCP tx buffers to use?

No	).	delta.t	Destination	Source	Protocol	Info
	1	0.000000	172.27.37.13	172.28.85.156	TCP	46646 > commplex-link [SYN] Seq=0 win=3840 Len=0 M55=1460 SACK_PERC=1 WS=128
	2	0.000086	5 172.28.85.156	172.27.37.13	TCP	commplex-link > 46646 [SYN, ACK] seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
	3	0.049204	172.27.37.13	172.28.85.156	TCP	46646 > commplex-link [ACK] seg=1 Ack=1 win=5888 Len=0

### **Useful Technical Indicators**

- Timing Based
  - Delta Time
    - Latency / Delay measurements
  - Relative Time
    - Throughput and Response Times
  - Absolute Time
    - Correlation to log files
- TCP Based
  - SYN, FIN, Reset
  - Retransmissions & Out of Order Packets
  - ACKs: Dup, Triple, Delayed, SACK
  - Windowing: Window Size & Window Full Messages

- Application Based
  - Transaction ID's
  - Control Messages
    - Open, Close, Abort
- Measurements
  - Service Response Time
  - Latency & Throughput
  - Other Delay

### **Measurement Techniques**

- Standard Columns
  - Delta Time: Sorting to find latency
  - Relative Time: Find request/response delays
- Custom Columns
  - IP: ip.ttl, ip.id
  - TCP: tcp.seq, tcp.ack, tcp.len, tcp.options.sack
  - Application Specific (transaction/message IDs)
- Service Response Times
  - Use to find application delays
- Expert
  - Best used to look for TCP behavior (reactions to conditions on the wire)

## **Protocol Layer Techniques**

- IP Based
  - Use TTL column to visualize packet flow through routers
  - Use IPID column to visualize packet loss.
- ICMP Based
  - Destination Unreachable (Fragmentation, TTL, ACL's, Host)
- TCP Based
  - Out of Order Packets: Look for SACKs in opposite direction. Indicates possible packet loss or network queuing or asynchronous routing issues.
  - ACK: Useful to prove a request arrived at a destination
  - Dup ACKs: Triple Dup ACKs indicate host not using Fast Retransmit algorithm.
  - Delayed ACKs: Indicates TCP waiting for an application.
  - Windowing: Full windows may indicate application problems or lack of TCP buffering (scaling needed).

### **Case Study: Assisting the Manifestation Process**

#### Application

Radius authentication was suffering due to "perceived" packet loss

#### Symptoms

- WIFI clients were unable to authenticate through a specific site/router
- Network path appears to be clean. No obvious loss or latency.

#### Manifestation

- Problem manifests as loss of connectivity
- Location of problem local to a single site.

### **Case Study: Radius Authentication Failures**

No.	del.t	rel.t	Destination	Source	Protocol Info
1	0.000000	0.000000	172.30.16.147	69.252.208.133	RADIUS Accounting-Request(4) (1d=118, 1=463
2	0.000008	0.000008	172.30.16.147	69.252.208.133	RADIUS Accounting-Request(4) (id=118, 1=463)
3	0.000013	0,000021	172.30.16.147	69.252.208.133	RADIUS Accounting-Request(4) (id=118, 1=463)
4	0.000759	0.000780	69.252.208.133	172.30.16.147	RADIUS Accounting-Response(5) (id=118, 1=20)
5	0.000029	0.000809	69.252.208.133	172.30.16.147	RADIUS Accounting-Response(5) (id=118, 1=20)
б	1.454033	1.454842	172.30.16.147	69.252.208.133	RADIUS Accounting-Request(4) (id=118, 1=510)
7	0.000013	1.454855	172.30.16.147	69.252.208.133	RADIUS Accounting-Request(4) (id=118, 1=510)
8	0.000012	1.454867	172.30.16.147	69.252.208.133	RADIUS Accounting-Request(4) (id=118, 1=510)
9	0.000698	1.455565	69.252.208.133	172.30.16.147	RADIUS Accounting-Response(5) (id=118, 1=20)
10	0.673942	2.129507	172.30.16.147	69.252.208.133	RADIUS Accounting-Request(4) (id=118, 1=491)
11	0.000012	2.129519	172.30.16.147	69,252,208,133	RADIUS Accounting-Request(4) (id=118, 1=491)
12	0.000015	2.129534	172.30.16.147	69.252.208.133	RADIUS Accounting-Request(4) (id=118, 1=491)
13	0.011410	2.140944	69.252.208.133	172.30.16.147	RADIUS Accounting-Response(5) (id=118, 1=20)
14	0.000028	2.140972	69.252.208.133	172.30.16.147	RADIUS Accounting-Response(5) (id=118, 1=20)
15	1.354180	3.495152	172.30.16.147	69.252.208.133	RADIUS Accounting-Request(4) (id=118, 1=510)
16	0.000017	3.495169	172.30.16.147	69.252.208.133	RADIUS Accounting-Request(4) (id=118, 1=510)
17	0.000004	3.495173	172.30.16.147	69.252.208.133	RADIUS Accounting-Request(4) (id=118, 1=510)
18	0.001219	3.496392	69.252.208.133	172.30.16.147	RADIUS Accounting-Response(5) (id=118, 1=20)
19	1.693790	5.190182	172.30.16.147	69,252,208,133	RADIUS Accounting-Request(4) (id=118, 1=534)
20	0.000013	5.190195	172.30.16.147	69.252.208.133	RADIUS Accounting-Request(4) (id=118, 1=534)
21	0.000004	5.190199	172.30.16.147	69.252.208.133	RADIUS Accounting-Request(4) (id=118, 1=534)
22	0.000813	5.191012	69.252.208.133	172.30.16.147	RADIUS Accounting-Response(5) (id=118, 1=20)
23	0.892666	6.083678	172.30.16.147	69.252.208.133	RADIUS Accounting-Request(4) (id=118, 1=506)
24	0.000015	6.083693	172.30.16.147	69.252.208.133	RADIUS Accounting-Request(4) (id=118, 1=506)
25	0.000017	6.083710	172.30.16.147	69.252.208.133	RADIUS Accounting-Request(4) (id=118, 1=506)
26	0.000820	6.084530	69.252.208.133	172.30.16.147	RADIUS Accounting-Response(5) (id=118, 1=20)
27	0.000052	6.084582	69.252.208.133	172.30.16.147	RADIUS Accounting-Response(5) (id=118, 1=20)

How do we find and visualize packet loss?

#### **Case Study: Visualize Sessions**

No.	del.t	rel.t	Destination	Source	dst.port	src.port	Protocol	Info
	1 0.000000	0.000000	172.30.16.147	69.252.208.133	181	1 21503	RADIUS	Accounting-Request(4) (id=118,
	2 0.000008	0.000008	172.30.16.147	69.252.208.133	1813	3 21503	RADIUS	Accounting-Request(4) (id=118,
3	3 0.000013	0.000021	172.30.16.147	69.252.208.133	1813	3 21503	RADIUS	Accounting-Request(4) (id=118,
24	4 0.000759	0.000780	69.252.208.133	172, 30, 16, 147	21503	3 1813	RADIUS	Accounting-Response(5) (id=118
	5 0.000029	0.000809	69.252.208.133	172.30.16.147	21503	3 1813	RADIUS	Accounting-Response(5) (id=118
	6 1.454033	1.454842	172.30.16.147	69.252.208.133	1813	3 21502	RADIUS	Accounting-Request(4) (id=118,
34	7 0.000013	1.454855	172.30.16.147	69.252.208.133	1813	3 21502	RADIUS	Accounting-Request(4) (id=118,
1.0	8 0.000012	1.454867	172.30.16.147	69.252.208.133	1813	3 21502	RADIUS	Accounting-Request(4) (id=118,
3	9 0.000698	1.455565	69.252.208.133	172.30.16.147	21502	2 1813	RADIUS	Accounting-Response(5) (id=118
1	0.673942	2.129507	172.30.16.147	69.252.208.133	1813	3 21504	RADIUS	Accounting-Request(4) (id=118,
1	1 0.000012	2.129519	172.30.16.147	69.252.208.133	1813	3 21504	RADIUS	Accounting-Request(4) (id=118,
1	2 0.000015	2,129534	172.30.16.147	69.252.208.133	1813	3 21504	RADIUS	Accounting-Request(4) (id=118,
1	3 0.011410	2.140944	69.252.208.133	172.30.16.147	21504	1813	RADIUS	Accounting-Response(5) (id=118
1.	4 0.000028	2.140972	69.252.208.133	172.30.16.147	21504	1813	RADIUS	Accounting-Response(5) (id=118
1	5 1.354180	3.495152	172.30.16.147	69.252.208.133	1813	3 21502	RADIUS	Accounting-Request(4) (id=118,
1	5 0.000017	3.495169	172.30,16.147	69.252.208.133	1813	3 21502	RADIUS	Accounting-Request(4) (id=118,
1	7 0.000004	3.495173	172.30,16.147	69.252.208.133	1813	3 21502	RADIUS	Accounting-Request(4) (id=118,
1	8 0.001219	3.496392	69.252.208.133	172.30.16.147	21502	2 1813	RADIUS	Accounting-Response(5) (id=118
1	9 1.693790	5.190182	172.30.16.147	69.252.208.133	1813	3 21501	RADIUS	Accounting-Request(4) (id=118,
21	0.000013	5.190195	172.30.16.147	69.252.208.133	1813	3 21501	RADIUS	Accounting-Request(4) (id=118,
2	1 0.000004	5.190199	172.30.16.147	69.252.208.133	1813	3 21501	RADIUS	Accounting-Request(4) (id=118,
2	2 0.000813	5.191012	69.252.208.133	172.30.16.147	21501	1813	RADIUS	Accounting-Response(5) (id=118
2	3 0.892666	6.083678	172.30.16.147	69.252.208.133	1813	3 21503	RADIUS	Accounting-Request(4) (id=118,
24	4 0.000015	6.083693	172.30.16.147	69.252.208.133	1813	3 21503	RADIUS	Accounting-Request(4) (id=118,
2	5 0.000017	6.083710	172.30.16.147	69.252.208.133	1813	3 21503	RADIUS	Accounting-Request(4) (id=118,
21	6 0.000820	6.084530	69.252.208.133	172.30.16.147	21503	1813	RADIUS	Accounting-Response(5) (id=118
2	7 0.000052	6.084582	69.252.208.133	172.30.16.147	21503	1813	RADIUS	Accounting-Response(5) (id=118

#### **Technical Indicator**

Number of packets in each session.

#### <u>Technique</u>

Use Columns to Visualize Sessions

#### **Case Study: Filter to Single Session**

No.	de	el.t	rel.t	Destination	Source	dst.port	src.port	Protocol	Info
	1 (	0.000000	0.000000	172.30.16.147	69.252.208.133	1813	21501	RADIUS	Accounting-Request(4) (id=118,
	2 (	0.000013	0.000013	172.30.16.147	69.252.208.133	1813	21501	RADIUS	Accounting-Request(4) (id=118,
2	3 1	0.000817	0.000830	69.252.208.133	172.30.16.147	21501	1813	RADIUS	Accounting-Response(5) (id=118
24	4 7	2.015653	2.016483	172.30.16.147	69.252.208.133	1813	21501	RADIUS	Accounting-Request(4) (id=118,
	5 (	0.000012	2.016495	172.30.16.147	69.252.208.133	1813	21501	RADIUS	Accounting-Request(4) (id=118,
	6 (	0.000637	2.017132	69.252.208.133	172.30.16.147	21501	1813	RADIUS	Accounting-Response(5) (id=118
0	7 (	0.000028	2.017160	69.252.208.133	172.30.16.147	21501	1813	RADIUS	Accounting-Response(5) (id=118
1	8 4	4.499100	6.516260	172.30.16.147	69.252.208.133	1813	21501	RADIUS	Accounting-Request(4) (id=118,
3	9 (	0.000027	6.516287	172.30.16.147	69.252.208.133	1813	21501	RADIUS	Accounting-Request(4) (id=118,
1	0 (	0.000715	6.517002	69.252.208.133	172.30.16.147	21501	1813	RADIUS	Accounting-Response(5) (id=118
1	1	2.027109	8.544111	172.30.16.147	69.252.208.133	1813	21501	RADIUS	Accounting-Request(4) (id=118,
1	2 (	0.000014	8.544125	172.30.16.147	69.252.208.133	1813	21501	RADIUS	Accounting-Request(4) (id=118,
1	3 (	0.001001	8.545126	69.252.208.133	172.30.16.147	21501	1813	RADIUS	Accounting-Response(5) (id=118
1.	4 1	6.732012	15.277138	172.30.16.147	69.252.208.133	1813	21501	RADIUS	Accounting-Request(4) (id=118,
1	5 (	0.000007	15.277145	172.30.10 147	69.252.208.133	1813	21501	RADIUS	Accounting-Request(4) (id=118,
1	6 (	0.000786	15.277931	69.252.208.133	172.30.16.147	21501	1813	RADIUS	Accounting-Response(5) (id=118
1	7 7	2.035259	17.313190	172.30.16.147	69.252.208.133	1813	21501	RADIUS	Accounting-Request(4) (id=118,
1	8 1	0.000002	17.313192	172.30.16.147	69.252.208.133	1813	21501	RADIUS	Accounting-Request(4) (id=118,
1	9 (	0.001446	17.314638	69.252.208.133	172.30.16.147	21501	1813	RADIUS	Accounting-Response(5) (id=118
2	0 0	6.735149	24.049787	172.30.16.147	69.252.208.133	1813	21501	RADIUS	Accounting-Request(4) (id=118,
2	1 (	0.000016	24.049803	172.30.16.147	69.252.208.133	1813	21,501	RADIUS	Accounting-Request(4) (id=118,
2	2 (	0.000738	24.050541	69.252.208 133	172.30.16.147	21501	1813	RADIUS	Accounting-Response(5) (id=118
2	3 (	0.000032	24.050573	69.252.208.133	172.30.16.147	21501	1813	RADIUS	Accounting-Response(5) (id=118

Notice the 2 second delays manifest themselves after packets are filtered down to a single session!

#### **Case Study: Visualization of Packet Loss**

No.	del	.t rel.t	Destination	Source	ip.id	ip.ttl	Protocol	Info
	1	0.000000 0.000000	172.30.16.147	69.252.208.133	0x0000 (0)	64	RADIUS	Accounting-Request(4)
	2	0.000013 0.000013	172.30.16.147	69,252,208,133	0x0000 (0)	63	RADIUS	Accounting-Request(4)
	3	0.000817 0.000830	69.252.208.133	172.30.16.147	0xce54 (52820)	255	RADIUS	Accounting-Response(5)
	4	2.015653 2.016483	172.30.16.147	69.252.208.133	0x0000 (0)	64	RADIUS	Accounting-Request(4)
	5	0.000012 2.016495	172.30.16.147	69.252.208.133	0x0000 (0)	63	RADIUS	Accounting-Request(4)
	6	0.000637 2.017132	69.252.208.133	172.30.16.147	0xd25f (53855)	255	RADIUS	Accounting-Response(5)
	7	0.000028 2.017160	69.252.208.133	172.30.16.147	Oxd25f (53855)	254	RADIUS	Accounting-Response(5)
	8	4.499100 6.516260	172.30.16.147	69.252.208.133	0x0000 (0)	64	RADIUS	Accounting-Request(4)
	9	0.000027 6.516287	172, 30, 16, 147	69,252,208,133	0x0000 (0)	63	RADIUS	Accounting-Request(4)
1	0	0.000715 6.517002	69.252.208.133	172.30.16.147	0xdc44 (56388)	255	RADIUS	Accounting-Response(5)
1	1	2.027109 8.544111	172.30.16.147	69.252.208.133	0x0000 (0)	64	RADIUS	Accounting-Request(4)
1	2	0.000014 8.544125	172.30.16.147	69.252.208.133	0x0000 (0)	63	RADIUS	Accounting-Request(4)
1	3	0.001001 8.545126	69.252.208.133	172.30.16.147	0xe0f6 (57590)	255	FADIUS	Accounting-Response(5)
1	4			1.208.133	0x0000 (0)	64	RADIUS	Accounting-Request(4)
1	5		ited european	fully .208.133	0x0000 (0)	63	RADIUS	Accounting-Request(4)
1	б	IFID-55655 100	lieu succes	Siully .16.147	0xeee4 (61156)	255	RADIUS	Accounting-Response(5)
1	7	$(TTI_{-1})$		.208.133	0x0000 (0)	64	RADIUS	Accounting-Request(4)
1	8	(     -   )		. 208.133	0x0000 (0)	63	RADIUS	Accounting-Request(4)
1	9			0.16.147	0xf301 (62209)	255	RADIUS	Accounting-Response(5)
2	0	6.735149 24.049787	172.30.16.147	69.252.208.133	0x0000 (0)	64	RALIUS	Accounting-Request(4)
2	1	0.000016 24.049803	172.30.16.147	69.252.208.133	0x0000 (0)	63	RADIUS	Accounting-Request(4)
2	2	0.000738 24.050541	69.252.208.133	172.30.16.147	0x0043 (67)	255	RADIUS	Accounting-Response(5)
2	3	0.000032 24.050573	69.252.208.133	172.30.16.147	0x0043 (67)	254	RADIUS	Accounting-Response(5)
2	4	4.592564 28.643137	172.30.16.147	69.252.208.133	0x0000 (0)	64	RADIUS	Accounting-Request(4)
2	5	0.000009 28.643146	172.30.16.147	69.252.208.133	0x0000 (0)	63	RADIUS	Accounting-Request(4)
2	6	0.000725 28.643871	69.252.208.133	172.30.16.147	0x0a38 (2616)	255	RADIUS	Accounting-Response(5)
2	7	2.044703 30.688574	172.30.16.147	69.252.208.133	0x0000 (0)	64	RADIUS	Accounting-Request(4)
2	8	0.000013 30.688587	172.30.16.147	69.252.208.133	0x0000 (0)	63	RADIUS	Accounting-Request(4)
2	9	0.000860 30.689447	69.252.208.133	172.30.16.147	0x0e2f (3631)	255	RADIUS	Accounting-Response(5)

<u>Technique</u> Use IP ID and TTL to track packet flow through a router TTLs allow us to see packet loss inside of the router. IPID=56388 is never shown with TTL=254

### **Case Study: Correlating for Visibility**

No.	del.t	16	sht	Destination	Source	ip.id	ip.ttl	Protocol	Info	rad.auth
	1	*REF* *	REF*	172.30.16.147	69.252.208.133	0x0000 (0)	64	RADIUS	Accounting-Request(4)	82824cacba68d89773cedc14b49c95dc
	2	0.000013 0	0,000013	172.30.16.147	69.252.208.133	0x0000 (0)	63	RADIUS	Accounting-Request(4)	82824cacba68d89773cedc14b49c95dc
13	3	0.000817 0	0.000830	69,252,208,133	172.30,16.147	Oxce54 (52820)	255	RADIUS	Accounting-Response(5)	5e1df93fe640b0a8fb828d7442aaa970
2	4	2.015653 2	.016483	172.30.16.147	69.252.208.133	0x0000 (0)	64	RADIUS	Accounting-Request(4)	82824cacba68d89773cedc14b49c95dc
	5	0.000012 2	.016495	172.30,16.147	69.252.208.133	0x0000 (0)	63	RADIUS	Accounting-Request(4)	82824cacba68d89773cedc14b49c95dc
	6	0.000637 2	2.017132	69.252.208.133	172.30.16.147	0xd25f (53855)	255	RADIUS	Accounting Response(5)	5e1df93fe640b0a8fb828d7442aaa970
	7	0.000028 2	.017160	69.252.208.133	172.30.16.147	Oxd25f (53855)	254	RADIUS	Accounting-Response()	5e1df93fe640b0a8fb828d7442aaa970
	8	"REF" "	REF*	172.20.16.147	69.252.208.133	0x0000 (0)	64	RADIUS	Accounting-Request(4)	b7998507e20561f4fda2f1ae4a1dbbae
귛	9	0.000027 0	.000027	172.30.15.147	69.252.208.133	0x0000 (0)	63	RADIUS	Accounting-Request(4)	b7998507e20561f4fda2f1ae4a1dbbae
1	0	0.000715 0	.000742	69.252.208.133	172.30 16 147	Dudess (SE288)	255	RADIUS	Accounting-Response(5)	66fc7f51f11c0ff79dc7557f879f6a9a
1	1	2.027109 2	. 027851	172.30.16.147	69.25		64	RADIUS	Accounting-Request(4)	b7998507e20561f4fda2f1ae4a1dbbae
1	2	0.000014 2	. 027865	172.30.16.147	2 sec a	oplication	153	RADIUS	Accounting-Request(4)	b7998507e20561f4fda2f1ae4a1dbbae
1	3	0.001001 2	. 028866	69.252.208.133	172.3		255	RADIUS	Accounting-Response(5)	66fc7f51f11c0ff79dc7557f879f6a9a
1	4	*REF* *	REF*	172.30.16.147	69.25: recove	rv	64	RADIUS	Accounting Request(4)	8834e60cedca56b69201cb3e95a2165d
1	5	0.000007 0	. 000007	172 30.16.147	69.25.	· )	63	RADIUS	Accounting-Request(4)	8834e60cedca56b69201cb3e95a2165d
1	6	0.000786 0	0.000793	69.252.208.133	172.30.10.147	OXECC4 (01130)	255	RADIUS	Accounting Response(5)	258c36cca1b?f4bd8ceba7419bba2289
1	7	2.035259 2	. 036052	172.30.15.147	69.252.208.133	0x0000 (0)	64	RADIUS	Accounting-Request(4)	8834e60cedca56b69201cb3e95a2165d
1	8	0.000002 2	. 036054	172.30.16.147	69.252.208.133	0x0000 (0)	63	RADIUS	Accounting-Request(4)	8834e60cedca56b69201cb3e95a2165d
1	9	0.001446 2	.037500	69.252.208.133	172.30 16 247	0-6203 (62200)	255	RADIUS	Accounting-Response(5)	258c36cca1b7f4bd8ceba7419bba2289
2	0	*REF* *	REF*	172.30.16.147	09,252		64	RADIUS	Accounting-Request(4)	de1a9d53830d05e2f4d694233477133c
2	1	0.000016 0	0.000016	172.30.16.147	Recove	erv packet		RADIUS	Accounting-Request(4)	de1a9d53830d05e2f4d694233477133c
2	2	0.000738 0	. 000754	69.252.208.133	172.30		255	RADIUS	Accounting-Response(5)	817d06f882f9152042d65fa89333723e
2	3	0.000032 0	.000786	69.252.208.133	172.30 droppe	D	254	RADIUS	Accounting-Response(5)	817d06f882f9152042d65fa89333723e
2	4	*REF* *	REF*	172.30.16.147	69.252		64	RADIUS	Accounting-Request(4)	2d\$036c584ceae8155341c0a24e9b676
2	5	0.000009 0	. 000009	172.30.16.147	69.252.208.133	0x0000 (0)	63	RADIUS	Accounting-Request(4)	2d5036c584ceae8155341c0a24e9b676
2	6	0.000725 0	0.000734	69.252.208.133	172.30.16.147	0x0a38 (2616)	255	RADIUS	Accounting-Response(5)	fc0b45c796f0fc744741b6fd36ceb309
2	7	2,044703 2	. 045437	172.30.16.147	69.252.208.133	0x0000 (0)	64	RADIUS	Accounting-Request(4)	2d5036c584ceae8155341c0a24e9b676
2	8	0.000013 2	. 045450	172.30.16.147	69.252.208.133	0x0000 (0)	63	RADIUS	Accounting-Request(4)	2d5036c584ceae8155341c0a24e9b676
2	9	0.000860 2	1.046310	69.252.208.133	172.30.16.147	0x0e2f (3631)	255	RADIUS	Accounting-Response(5)	fc0b45c796f0fc744741b6fd36ceb309

#### **Technique**

Correlation of data from different columns in Wireshark allows us to visualize the packet loss inside the router and the attempts by the application to recover from it.

### **Extrapolation Techniques**

- Application Based
  - Always attempt to decode the application layer.
  - Look for hints in the packet hex bytes that may indicate what the protocol is.
  - Look for explicit messages that indicate application behavior or reactions to conditions on the wire.
  - Find protocol fields that allow you to track requests and responses.
  - Associate application messages and behavior to reactions and recovery mechanisms in the transport layer (ie: TCP).

# **Case Study: Manifestation of Server Delay**

#### Application

Performance degredation with database transactions.

#### Symptoms

- Transactions which should take less than one second are taking up to (5) seconds causing the application to disconnect.
- Network path appears to be clean. No obvious loss or latency.

#### Manifestation

- Problem manifests as delay
- Location of Delay uncertain.

up Protocol Summury Sequence TCP Duplicate ACK (#1) Sequence TCP Retransmission (suspected)	Count •		
Help	Slose IDAP Service Resp	oonse Time statistics slow, Idap_bransactions.pcap	
		LDAP Service Response Time statistics Filter	
	Index 4 Descenture	LDAP Commends	
Technical Indicators:			
Expert shows no obvious or relevant indicators found.			
		Close	

The	Edit View Go	Sapture Analyze	Statistics Telephony	Iools Interna	als Help			
0	ð 🛋 🔳 🖉		Q + + 4	7 2 0			📓 🕅 🍕 🗱	
Filter:				- Ex	pression Clear	Apply	Save	
lo.	delta.t	Destination	Source	Protocol Inf	0			
58	8 0.000025	76.96.31.11	24.40.31.172	TCP 38	488 > 11539	[ACK]	5eg-82 Ack-15 win-52528 Len-0	.0
59	9 0.000388	76.96.31.11	24.40.31.172	TCP 38	3510 > 11539	[PSH,	ACK] Seq=1 Ack=1 Win=51456 Len=81	
60	0.011199	24.40.31.172	76.96.31.11	TCP 11	1539 > 38859	[ACK]	Seq=1 Ack=82 win=13936 Len=0	
61	0.066221	24.40.31.172	76.96.31.11	TCP 11	1539 > 38510	[ACK]	5eq=1 Ack=82 win=48695 Len=0	
62	2 0.784925	24.40.31.172	76.96.31.11	TCP 11	1539 > 38598	[PSH,	ACK] Seq=103 Ack=325 Win=48695 Len=34	
6	3 0.000169	76.96.31.11	24.40.31.172	TCP 38	1598 > 11539	[PSH,	ACK] Seq=325 Ack=137 Win=53600 Len=81	
64	4 0.077834	24.40.31.172	76.96.31.11	TCP 11	1539 > 38598	[ACK]	Seq=137 Ack=406 Win=48695 Len=0	
65	5 0.011217	24.40.31.172	76.96.31.11	TCP 11	1539 > 38598	[PSH,	ACK] Seq=137 Ack=406 win=48695 Len=34	
68	5 0.000122	76.96.31.11	24.40.31.172	TCP 38	3598 > 11539	[PSH,	ACK] Seq-406 Ack-171 win-53600 Len-81	
67	7 0.116289	24.40.31.172	76.96.31.11	TCP 11	1539 > 38598	[ACK]	Seq=171 Ack=487 Win=48695 Len=0	
- 61	8 0.749313	24.40.31.172	76.96.31.11	TCP 11	.539 > 38598	PSH.	ACK] Seq=171 Ack=487 Win=48695 Len=34	-
< Lim								1
) (E)	Checksum: Oxo [SEQ/ACK ana]	3c4 [validati lysis]	on disabled]					
- Da	ta (34 bytes) Data: 3012020 [Length: 34]	) 013c640d04096f	3d436f6d63617374	3000300c020	1			-
			OF FF 20 00 08	00 45 00		E.		
0000 0010 0020 0030 0040 0050	ac 16 2d a6 00 4a 36 68 1f ac 2d 13 be 37 c3 c4 3d 43 6f 66 07 04 01 00	5 30 80 00 17 8 40 00 30 06 9 96 c6 16 ef 90 00 30 12 63 61 23 74 94 00 04 00	70 87 40 60 1f 91 78 04 a9 62 02 01 30 64 0d 30 00 30 0c 02	0b 18 28 97 50 18 04 09 61 01 3c 65	.36.0.0, p.1	b.P.		

**Technique** 

Look in Hex Data for a hint on what the protocol may be.

	LDAP Service Response Time statistics Filter: LDAP Commands		
Index   Procedure	Calls ▼ Min SRT ◀ Max SRT ◀ Avg SRT		
3 Search	502 0.080458 2.034575	0.113035	
	<u>Close</u>	and to L DAP)	

📕 si	ow_b	ind_sessions.po	cap [Wireshark 1.10.	7 (v1.10.7-0-g6b931a	1 from ma	ster-1.10)]					×
Eile	Edit	t <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>Analyze</u>	Statistics Telephon	<u>y</u> <u>I</u> ools	Internals <u>H</u>	<u>l</u> elp				
0	۲	A # #	🖻 ն 🗶 🖉	1 🔍 🗢 🗢 🥥	香 生		QQQE	1 📓 🗹 !	8 💥 i 🙀		
Filte	r:					• Expressi	on Clear Appl	ly Save			
No.	de	elta.t	Destination	Source	Protocol	src.port to	o.dst Info			messageID	
	1	0.000000	76.96.31.11	24.40.31.172	TCP	39003	11539 3900	03 > 11539	[SYN] Seq=0 Win	₩Ē	
	2	0.079642	24.40.31.172	76.96.31.11	TCP	11539	39003 115	39 > 39003	[SYN, ACK] Seq=	0	
	3	0.000015	76.96.31.11	24.40.31.172	TCP	39003	11539 3900	03 > 11539	[ACK] Seq=1 Ack	=1	
	4	0.000298	8 76.96.31.11	24.40.31.172	LDAP	39003	11539 bind	dRequest(1)	) "cn=pcsAppUser	, c	1
	5	0.076998	24.40.31.172	76.96.31.11	TCP	11539	39003 1153	39 > 39003	[ACK] Seg=1 Ack	<b>-</b> Ε	
	6	4.837878	24.40.31.172	76.96.31.11	LOAP	11539	39003 bin	dResponse()	<ol> <li>success</li> </ol>		1
	7	0.000256	76,96,31,11	24.40.31.172	TCP	39003	11539 3900	03 > 11539	[ACK] Seg=85 AC	k=	
	8	0.000138	3 70.06.31.11	24.40.31.172	LDAP	39003	11539 sear	chRequest	(2) "ou=mailedge	pa	2
	9	0.076977	24,40,31,172	76.96.31.11	TCP	11539	39003 115	39 > 39003	[ACK] Seg=15 AC	k=	
1	10	0.009529	24.40.31.172	76.56.31.11	LDAP	11539	39003 sear	chResDone	(2) success [0	re	2
1	11	0.039927	76.96.31.11	24.40.31.1/2	TCP	39003	11539 3900	03 > 11539	[ACK] Seq=221 A	ck	-
4						10					*

Why does it take the LDAP server nearly 5 seconds to respond to the Bind request??

# **Case Study: Manifestation of Client Delay**

#### Application

UNIX servers and VMs.

#### Symptoms

- UNIX admins are reporting very slow response times running SUDO level commands.
- Network path appears to be clean. No obvious loss or latency.

#### Manifestation

- Problem manifests as delay
- Location of Delay uncertain.

### **Case Study: Sudo Command Slow**



### **Case Study: Sudo Command Slow**

0 0	🔺 🖩 🖉 🛛		् 🗢 🗢 🎝 🏹	2	III Q Q Q 🗹 👹 🖬 🍋 % 🔛
Filten					Expression Clear Apply Save
lo.	delta.t 🔹 🔻	Destination	Source	Protocol	Info
329	97.721841812	172.28.154.19	172.27.16.205	LDAP	unbindRequest(5)
12	0.0329/0880	172.28.154.19	172.27.16.205	LDAP	<pre>searchRequest(3) "ou=sudoers,dc=comcast,dc=com" i</pre>
15	0.000589371	172.27.16.205	172.28.154.19	LDAP	searchResEntry(4) "cn=SEO_Unix_ESP_Nonprod#SEO_U
9	0.000459671	172.27.15.205	172.28.154.19	LDAP	<pre>searchResEntry(2) "cn=defaults,ou=sudoers,dc=com</pre>
13	0.000423432	172.27.16.205	172.28.154.19	LDAP	searchResDone(3) success [0 results]
22	0.000282288	172.27.16.205	172.28.154.19	LDAP	searchResEntry(4) "cn=SEO_Unix_MD5_NonProd#SEO_U
20	0.000268937	172.27.16.205	172,28,154,19	LDAP	searchResEntry(4) "cn=SE0_Un1x_MDS_NonProd#SE0_U
2076	0.000265121	172.27.16.205	172.28.154.19	LDAP	searchResEntry(4) "cn=W_DIV_CRAN_TWIN_XOCROUTER_0
184	0.000265121	172.27.16.205	172.28.154.19	LDAP	searchResEntry(4) "cn=SEO_Unix_AppMgmt_Prod#SEO_!
18	0,000244141	172.27.16.205	172.28.154.19	LDAP	searchResEntry(4) "cn=SEO_Unix_SBSS_Infrastructu
3292	0:000244140	1/2.27.16.205	1/2.28.154.19	TCP	Idap > 52603 [FIN, ACK] Seq=2875094 ACK=285 WIN=
24	0.000244140	1/2.2/.16.205	1/2.28,154.19	LDAP	searchResEntry(4) cn=SEO_Unix_SiteMinderCA_NonPi
2264	0.000226974	1/2.27.16.205	172.28.154.19	DAP	searchResentry(4) cn=crs_test#cRAN_ROUTER_WRITE
3111	0.000198364	1/2.2/.16.205	1/2.28.154.19	LDAP	searcnResEntry(4) cn=w_DIV_CRAN_CAL_XOCROUTER_C
1037	0.000190/35	1/2.2/.16.205	1/2.28.154.19	LDAP	searchResentry(4) Ch=DEVICES_NETSD_BBONE_ROUTER:
3039	0.000186920	1/2.2/.16.205	172.28.154.19	LDAP	SearchkesEntry(4) Ch=C_DIV_CRAN_AIL_XOCROUTER_C
2005	0.000186920	1/2.27.10.205	172.28.104.19	LDAP	SERFCHRESENERY(4) CH=NE_DIV_CRAN_WNE_XOCROUTER_(
293	0.000183012	1/2.2/.10.205	172.28.104.19	LUAP	searchkesenery(4) cn=seo_app11cationsD_S1K#Seo_1
1000	0.000181108	172.27.10.203	172.20.134.19	LDAP	SearchResentry(4) CH=C_DIV_CRAN_ATL_XOCROUTER_C
5074	0.000101198	1/2.2/.10.205	1/2.20,104,19	LUAP	Sear CHRESENERY(4) CHMNE_DIV_CRAN_BELT_ROCROUTER +
10000				m	
	File: "E:\sharkfest\s	udo_issue\sudo_slow.p	pca Packets: 3296 -	Displaye	Profile: Default

Large delay seen in delta time

#### **Case Study: Sudo Command Slow**

No. +	delta.t	rel.t	Destination	Source	Protocol	Info	
3277	0.000009537	0.124540329	172.28.154.19	172.27.16.205	TCP	52603 > 1dap [ACK] 5eq=277 Ack=2870966 W	in=
3278	0.000017166	0.124557495	172.27.16.205	172.28.154.19	LDAP	searchResEntry(4) "cn=EBDP_Platform_Node	s_P
3279	0.000024796	0.124582291	172.27.16.205	172.28.154.19	LDAP	searchResEntry(4) "cn=EBDP_Platform_Node	S_N
3280	0.000005722	0.124588013	172.28.154.19	172.27.16.205	TCP	52603 > 1dap [ACK] Seq=277 Ack=2871855 W	in=
3281	0.000020981	0.124608994	172.27.16.205	172.28.154.19	LDAP	searchResEntry(4) "cn=EBDP_Platform_Node	S_N
3282	0.000022888	0.124631882	172.27.16.205	172.28.154.19	LDAP	searchResEntry(4) "cn=EBDP_Edge_Nodes_Pr	od#
3283	0.000005722	0.124637604	172.28.154.19	172.27.16.205	TCP	52603 > 1dap [ACK] Seq=277 Ack=2872732 W	in=
3284	0.000019073	0.124656677	172.27.16.205	172.28.154.19	LDAP	searchResEntry(4) "cn=EBDP_Edge_Nodes_Pr	od#
3285	0.000024796	0.124681473	172.27.16.205	172.28.154.19	LDAP	searchResEntry(4) "cn=EBDP_Edge_Nodes_No	nPr
3286	0.000017166	0.124698639	172.28.154.19	172.27.16.205	TCP	52603 > 1dap [ACK] Seq=277 Ack=2873597 W	in=
3287	0.000007630	0.124706269	172.27.16.205	172.28.154.19	LDAP	searchResEntry(4) "cn=EBDP_Edge_Nodes_No	nPr
3288	0.000036239	0.124742508	172.27.16.205	172.28.154.19	LDAP	searchResEntry(4) "cn=TempAccess_gdavi10	01#
3289	0.000007630	0.124750138	172.28.154.19	172.27.16.205	TCP	52603 > 1dap [ACK] Seq=277 Ack=2874595 W	in=
3290	0.000026702	0.124776840	172.27.16.205	172.28.154.19	LDAP	searchResEntry(4) "cn=Devices_Labops_Uni	X_I
3291	0.000001908	0.124778748	172.27.16.205	172.28.154.19	LDAP	<pre>searchResDone(4) success [445 results]</pre>	
3292	0.000011444	0.124790192	172.28.154.19	172.27.16.205	TCP	52603 > 1dap [ACK] Seq=277 Ack=2875094 W	in=
3293	97.721841812	97.846632004	172,28.154.19	172.27.16.205	LDAP	unbindRequest(5)	
3294	0.000021796	97.846656800	172.28.154.19	172.27.16.205	TCP	52603 > 1dap [FIN, ACK] Seq=284 Ack=2875	094
3295	0.000244140	97.846330940	172.27.16.205	172.28.154.19	TCP	Idap > 52603 [FIN, ACK] Seq=2875094 Ack=	285
3296	0.000009537	97.846910477	172.28.154 19	172.27.16.205	TCP	52603 > 1dap [ACK] 5eq=285 Ack=2875095 W	in= -
4							
0.11	Eiler "E/\chaddentic	de incue\cude de	Backeter 2206	Dicolayed 3206 (100	Death		

#### **Technical Indicators**

LDAP Unbind Time is very slow.

Client waits 97 seconds before unbinding the LDAP connection.

### What is Correlation?

- The goal of correlation is to map the problem's method of manifestation to what is happening in the packets !!
- The process of correlating technical indicators must be understood, <u>you cannot</u> <u>automate anything you have never done manually</u>.
- You need to understand the protocols and the tools, know how Wireshark thinks !!!





#### **Correlation Best Practices**

- The correlation process starts by understanding how a problem manifests itself.
- Get as much information from the users and technical staff as possible.
- Ask how it is known the problem actually exists.
- Always analyze from the client's perspective first.
- Look for small patterns that can represent the problem as a whole.
  - A complex problem can often be represented by 10 packets or less.
- Visualize and understand requests and responses. Be the app!!
  - You cannot automate this part unless you understand how to do it manually.
- Understand the relationship between different technical indicators.
- Use visualization techniques for large amounts of packets.
  - Graphs, expert, column sorting.

#### **Packet Based Correlations**

No.	del	ita.t	Destination	Source	Protocol	Info	L.A
	1	0.000000	68.85.204.170	76.96.35.70	TCP	40335 > afs3-vlserver [SYN] Seq=0 Win=5840 Len=0 MSS=1460	
	2	0.000019	76.96.35.70	68.85.204.170	TCP	afs3-vlserver > 40335 [SYN, ACK] 5eq=0 Ack=1 win=5840 Len	=
	3	0.001153	68.85.204.170	76.96.35.70	TCP	40335 > afs3-vlserver [ACK] Seq=1 Ack=1 Win=6144 Len=0	
	4	0.000018	68.85.204.170	76.96.35.70	TCP	[TCP segment of a reassembled PDU]	
	5	0.000015	76.96.35.70	68.85.204.170	TCP	afs3-vlserver > 40335 [ACK] Seq=1 Ack=257 Win=6912 Len=0	1
	6	0.000014	76.96.35.70	68.85.204.170	TCP	[TCP segment of a reassembled PDU]	
	7	0.000014	76.96.35.70	68.85.204.170	TCP	[TCP segment of a reassembled PDU]	6H I
	8	0.999760	76.96.35.70	68.85.204.170	HTTP	HTTP/1.1 100 Continue	ΞU.
	9	0.000019	76.96.35.70	68.85.204.170	TCP	afs3-vlserver > 40335 [RST, ACK] Seq=27 Ack=257 Win=6912	1
	10	0.000311	68.85 204.170	76.96.35.70	TCP	[TCP Dup ACK 4#1] 40335 > ats3-vlserver [ACK] 5eq=257 Ack	ē., -
4.1						m	

**Technical Indicators** 

TCP Reset Delay (delta time)

TCP Reset correlates to a 1 second time out !

#### **Behavior Based Correlations**

**Relative** Time

🧲 cops_disc.pcap [Wi	reshark 1.10.7 (v1.10.	7-0-g6b931a1 from m	naster-1.10	)]	-			3			
<u>File Edit View Go</u>	Capture Analyze	Statistics Telephon	n <u>y T</u> ools	Internals Help							
0 0 🖌 🔳 🖉	🗎 🎥 🗶 🔁	🔍 🍲 🏟 🥥	T 4	। 🔲 🖬 🔍 Q 🔍 🖉 🕷 🕷	M 🛃 💥	11					
Filter:				Expression Clear Apply Save							
No. rel.t	Destination	Source	Protocol	Info	tcp.seq	tcp.ack	tcp.len				
1 0.000000	67.178.2.242	68.87.8.74	COPS	COPS Keep-Alive (KA)		1	1	8			
2 0.003990	68.87.8.74	67.178.2.242	COPS	COPS Keep-Alive (KA)		1	9	8			
3 0.203947	67.178.2.242	68.87.8.74	TCP	pktcable-cops > 51454 [ACK]	Sec	9	9	0			
4 2.873947	76.96.180.242	68.87.8.74	COPS	COPS Keep-Alive (KA)		1	1	8			
5 2.875502	68.87.8.74	76.96.180.242	COPS	COP5 Keep-Alive (KA)		1	9	8			
6 3.072271	76.96.180.242	68.87.8.74	TCP	pktcable-cops > 54298 [ACK]	Sec	9	9	0			
7 4.256548	67.178.2.242	68.87.8.74	COPS	COPS Keep-Alive (KA)		9	9	8			
8 4.260500	68.87.8.74	67.178.2.242	COPS	COPS Keep-Alive (KA)		9	17	8			
9 4.460304	67.178.2.242	68.87.8.74	TCP	<pre>pktcable-cops &gt; 51454 [ACK]</pre>	SAC	17	17	0			
10 10.004980	67.178.2.242	68.87.8.74	COPS	COPS Client-Close (CC)		17	17	16			
11 10.005114	67.178.2.242	68.87.8.74	TCP	petcapie-cop: > 51454 [FIN,	PSF	37	17	0			
12 10.009087	68.87.8.74	67.178.2.242	TCP	51454 > pktcable_cops [FIN,	ACK	17	33	0			
4 L								Ŀ,			
Tochnical Indi	catore		C								
				TCP columns allow us to prove all keepalives							
				were received yet the application still times out							

after 10 seconds and closes the connection.

45

### **Data Extrapolation Revisited**

hernet: 2 Fibre Channel FDDI IPv4	1 IPv6 IPX JXTA NCP RSVP SCTP TCP:1 Token Ring UDP USB WLAN
	IPv4 Conversations
72.27.37.13 172.28.85.156 7127429.	7 7 456 12.6963 11.311.464 1.753 115.430 11.426.894 0.00000000 9.209 727
1	
Name resolution	av filter
<u>Неір</u> <u>Сору</u>	Follow Stream Graph AB Graph 8A Close
Help Copy	Follow Stream Graph AB Graph BA Close TMb/sec with .3% packet loss
Help Copy Wireshark: 216 Expert	Follow Stream Graph A-B Graph B-A Close TMb/sec with .3% packet loss Infos 2 (43) Notes: 55 (168) Chats: 4 (5) Details: 216 Packet Comments: 0
Help Copy Wireshark: 216 Expert Errors: 0 (0) Warnings: Group • Protocol	Follow Stream Graph A-B Graph B-A Close TMb/sec with .3% packet loss Infos 2 (43) Notes: 55 (168) Chats: 4 (5) Details: 216 Packet Comments: 0 Summary Count
Help Copy Wireshark: 216 Expert Errors: 0 (0) Warnings: Group • Protocol B Sequence TCP	Follow Stream Graph AB Graph BA Close TMb/sec with .3% packet loss Infos 2 (43) Notes: 55 (168) Chats: 4 (5) Details: 216 Packet Comments: 0 Summary Count 1 Previous segment not captured (common at capture start) 29

#### **Measurement Based Correlations**



Correlation of Bytes in Flight and Receiver Window Size indicates inefficient use of available receiver buffers..... but why?

#### **Measurement Based Correlations**



#### Can you spot the correlation that visualizes the problem?

### **Correlation Techniques**

- Know where the analyzer is
  - Use TTL value to determine the location of packet collection
- Identify Client and Server
  - Always analyze from the perspective of the client first
- Identify Requests and Responses
  - Important to be able to measure transaction times and understand application behavior.
- Associate Packets to Process
  - Look for manifestation behavior in the packets
  - Utilize hex data to learn more about the application
- Look for obvious timing indicators that can be correlated with behavior. Common timers are: 1, 2, 5, 10, 30,60,120... (seconds)
- Reduce the scope of the problem to as few packets as possible.
  - Concentrate on single sessions.

# **Useful Visualizations**

#### **TCP Sequence and Acknowledgements**

No.	Destination	Source	Protocol	Info		tcp.seq	tcp.ack	tcp.len	
	1 67.178.2.242	68.87.8.74	COPS	COPS Keep-Alive (KA)			1		- 8
	2 68.87.8.74	67.178.2.242	COPS	COPS Keep-Alive (KA)			1	9	8
	3 67.178.2.242	68.87.8.74	TCP	pktcable-cops > 51454	[ACK] 5	eq=9 .	9	9	0
	4 76.96.180.242	68.87.8.74	COPS	COPS Keep-Alive (KA)			1	1	8
	5 68.87.8.74	76.96.180.242	COPS	COPS Keep-Alive (KA)			1	9	8
	6 76.96.180.242	68.87.8.74	TCP	pktcable-cops > 54298	[ACK] S	eq=9.	9	9	0
	7 67.178.2.242	68.87.8.74	COPS	COPS Keep-Alive (KA)		112	9	9	8
	8 68.87.8.74	67.178.2.242	COPS	COPS Keep-Alive (KA)			9	17	8
	9 67.178.2.242	68.87.8.74	TCP	pktcable-cops > 51454	[ACK] 5	eq=17	17	17	0
	0 67.178.2.242	68.87.8.74	COPS	COPS Client-Close (CC	)	10	17	17	16
1	1 67.178.2.242	68. 87. 8. 74	TCP	pktcable-cops > 51454	FIN, P	SH. A	33	17	0
	12 68.87.8.74	67.178.2.242	TCP	51454 > pktcable-cops	FIN. A	CK] S	17	33	0
		Sender	<sup>-</sup> (Sequ	uence + Length) = I SEQ(1) + LEN(8	Receive ) = AC	r ACK Nur <mark>K(</mark> 9)	nber		
1				m					•

TCP sequence, acknowledgement, and length fields are invaluable at proving a packet arrived at a destination.

#### **TCP Session Visualization**



#### **TCP Selective Acknowledgements**

No.	Length	del.t		Destination	Source	Protocol	Info						tcp.sack		-
27	66	0.00	0111	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	24#1]	60492 >	http	Т	rue	Ξ
28	66	0.00	0006	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	24#2]	60492 >	- http	T	rue	
62	66	0.00	0117	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	59#1]	61047 >	http	Т	rue	
63	74	0.00	0006	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	59#2]	61047 >	http	1	rue	
65	66	0.00	0283	76.96.210.8	10.19.89.39	TCP	61047	> h	ittp	[ACK]	Seq=644	4 Ack	=) (T	rue	
78	66	0.00	0209	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	76#1]	61047 >	http	. <b>T</b>	rue	
80	66	0.00	0166	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	76#2]	61047 >	http	( T	rue	
84	66	0.00	0212	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	82#1]	61047 >	http	Т	rue	
191	66	0.00	0138	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	189#1	61278	> http	р т	rue	
288	66	0.00	0003	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	280#1	61317	> http	рт	rue	
306	66	0.00	0154	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	269#1	61315	> http	рт	rue	
309	66	0.00	0028	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	269#2	61315	> http	рт	rue	
310	66	0.00	0003	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	269#3	61315	> http	рт	rue	
312	66	0.00	0173	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	280#2	61317	> http	рт	rue	
331	66	0.00	0172	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	269#4	61315	> http	рт	rue	
337	66	0.00	0033	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	293#1	61318	> http	рт	rue	
338	66	0.00	0002	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	293#2	61318	> http	р т	rue	
339	66	0.00	0001	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	293#3	61318	> http	р Т	rue	
341	66	0.00	0059	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	293#4	61318	> http	рт	rue	
349	66	0.00	0089	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	329#1	61319	> http	рт	rue	
352	66	0.00	0047	76.96.210.8	10.19.89.39	TCP	[TCP	Dup	ACK	329#2	61319	> http	рт	rue	
353	66	0 00	0002	76 96 210 8	10 19 89 39	TCP	TTCP	Dun	ACK	320#3	61319	> http	о <b>т</b>	rue	*

Filtering on TCP Selective Acknowledgement packets allows us to see the manifestation of unidirectional packet loss

#### **IP Identification Field**

Filter	ip.src==70	5.96.210.8			🔹 Exp	ression (	Clear App	oly Save
No.	Length	del.t	Destination	Source	ip.id		Protocol	Info
106	7 1434	0.000688	10.19.89.39	76.96.210.8	Oxeefd	(61181)	HTTP.	Continuation or non-HTTP traffic
370	0 1434	0.022167	10.19.89.39	76.96.210.8	0xef01	(61185)	TCP	[TCP segment of a reassembled PDU]
37:	1 1434	0.000763	10.19.89.39	76.96.210.8	0xef02	(61186)	TCP	[TCP segment of a reassembled PDU]
1169	9 1434	0.214512	10.19.89.39	76.96.210.8	0xef1a	(61210)	TCP	[TCP segment of a reassembled PDU]
176	7 1434	0.039989	10.19.89.39	76.96.210.8	0xef34	(61236)	TCP	[TCP Retransmission] [TCP segment of a
177:	1 1434	0.000892	10.19.89.39	76.96.210.8	0xef4a	(61258)	TCP	[TCP Retransmission] [TCP segment of a
341	8 1434	0.052943	10.19.89.39	76.96.210.8	0xefd1	(61393)	TCP	[TCP Previous segment not captured] [T
350	0 1434	0.000640	10.19.89.39	76.96.210.8	0xefda	(61402)	TCP	[TCP segment of a reassembled PDU]
35	1 1434	0.000029	10.19.89.39	76.96.210.8	Oxefdb	(61403)	TCP	[TCP segment of a reassembled PDU]
354	4 60	0.003135	10.19.89.39	76.96.210.8	0xeff1	(61425)	TCP	[TCP Previous segment not captured] ht
35	5 1434	0.000736	10.19.89.39	76.96.210.8	0xeff2	(61426)	HTTP	Continuation or non-HTTP traffic
79	8 1434	0.252016	10.19.89.39	76.96.210.8	0xf02e	(61486)	TCP	[TCP segment of a reassembled PDU]
1277	2 1434	0.317410	10.19.89.39	76.96.210.8	0xf084	(61572)	TCP	[TCP Retransmission] [TCP segment of a
1297	7 1434	0.113089	10.19.89.39	76.96.210.8	0xf084	(61572)	TCP	[TCP segment of a reassembled PDU]
609	9 1434	0.001170	10.19.89.39	76.96.210.8	0xf0a6	(61606)	TCP	[TCP segment of a reassembled PDU]
61(	0 134	0.000225	10.19.89.39	76.96.210.8	0xf0a7	(61607)	TCP	[TCP segment of a reassembled PDU]
614	4 1434	0.000015	10.19.89.39	76.96.210.8	0xf0c1	(61633)	TCP	[TCP segment of a reassembled PDU]
641	S 60	0.048017	10.19.89.39	76.96.210.8	0xf14b	(61771)	TCP	http > 61317 [ACK] Seq=22605 Ack=15241
1544	8 60	0.260351	10.19.89.39	76.96.210.8	Oxf15c	(61788)	TCP	http > 61540 [ACK] Seq=1 Ack=2329 win=
1549	9 1434	0.003029	10.19.89.39	76.96.210.8	Oxf18e	(61838)	TCP	[TCP segment of a reassembled PDU]
1550	0 134	0.000378	10.19.89.39	76.96.210.8	0xf18f	(61839)	TCP	[TCP segment of a reassembled PDU]
		A 000470			0	1-10103		From assessed at a second blad mould

Filtering on a single direction and sorting by the IP ID field allows us to visualize unidirectional packet loss.

#### **Validation using IP Identification**

No.	del.t	Destination	Source	ip.id	Protocol	Info	
	1.000000000	68.87.67.14	68.86,206,174	Oxe1ab (57771)	TCP	21022 > 10122 [SYN] Seq=0 Win=49640 Len=0 MSS=14	1
	2.000116348	68.86.206.174	68.87.67.14	0x6862 (26722)	TCP	10122 > 21022 [SYN, ACK] Seq=0 Ack=1 Win=49640 L	8
	3.000000000	68.86.206.174	68.87.67.14	0x6862 (26722)	TCP	[TCP Out-of-order] 10122 > 21022 [SYN, ACK] Seq=	£.
	4.000177383	68.87.67.14	68.86.206.174	Oxelac (57772)	TCP	21022 > 10122 [ACK] Seq=1 Ack=1 win=49640 Len=0	6
	5.00000000	68.87.67.14	68.86.206.174	Oxelac (57772)	TCP	[TCP Dup ACK 4#1] 21022 > 10122 [ACK] Seq=1 Ack=	=
	6.001295090	68.87.67.14	68.86.206.174	Oxe1ad (57773)	TCP	21022 > 10122 [PSH, ACK] Seq=1 Ack=1 Win=49640 L	
	7.000000000	68.87.67.14	68.86,206,174	Oxelad (57773)	TCP	[TCP Retransmission] 21022 > 10122 [PSH, ACK] Se	2
	8.000070572	68.86.206.174	68.87.67.14	0x6863 (26723)	TCP	10122 > 21022 [ACK] Seq=1 Ack=111 Win=49530 Len=	
	9.00000000	68.86.206.174	68.87.67.14	0x6863 (26723)	TCP	[TCP Dup ACK 8#1] 10122 > 21022 [ACK] Seq=1 Ack=	ŧ.
	10.004245758	68.86.206.174	68.87.67.14	0x6864 (26724)	TCP	10122 > 21022 [PSH, ACK] Seq=1 Ack=111 Win=49640	
	11.000215531	68.87.67.14	68.86.206.174	Oxelae (57774)	TCP	21022 > 10122 [ACK] Seq=111 Ack=123 Win=49640 Le	8
	12.00000000	68.87.67.14	68.86.206.174	Oxelae (57774)	TCP	[TCP Dup ACK 11#1] 21022 > 10122 [ACK] Seq=111 A	8
	13.005445480	68.87.67.14	68.86.206.174	Oxe1af (57775)	TCP	21022 > 10122 [PSH, ACK] Seq=111 Ack=123 Win=496	
	14.000082016	68.86.206.174	68.87.67.14	0x6865 (26725)	TCP	10122 > 21022 [ACK] Seq=123 Ack=117 win=49640 Le	8
	15.00000000	68.86.206.174	68.87.67.14	0x6865 (26725)	TCP	[TCP Dup ACK 14#1] 10122 > 21022 [ACK] Seq=123 A	8
	16.000795364	68.87.67.14	68.86.206.174	Oxe1b0 (57776)	TCP	21022 > 10122 [PSH, ACK] Seq=117 Ack=123 Win=496	8
	17.000095368	68.87.67.14	68.86.206.174	Oxe1b1 (57777)	TCP	21022 > 10122 [PSH, ACK] Seq=154 Ack=123 Win=496	6
	18.000001907	68.87.67.14	68.86,206.174	Oxe1b1 (57777)	TCP	[TCP Retransmission] 21022 > 10122 [PSH, ACK] Se	
	19.000076294	68.86.206.174	68.87.67.14	0x6866 (26726)	TCP	10172 > 21022 [ACK] 5ed=123 Ark=344 Win=49640 Le	12
1			WI .				

Wireshark is confused by duplicate packets and thinks there are DUP ACKs and <u>Retransmissions oc</u>curring. IP ID field allows us to see the duplicate IP packets.

# **Case Study: Bad TCP Stack**

#### Application

Web Server admins complaining about drop in throughput due to packet loss

#### Symptoms

- Throughput was perceived as being overly impacted due to packet loss
- Network path tested out as clean. No obvious loss or latency. Extremely minor levels of packet loss were seen (< .1%)</p>

#### Manifestation

- Problem manifests as performance degradation
- Issues appeared to be localized to a single hosting site

### Case Study: Bad TCP Stack

No.	del.t	rel.t	Destination	Source	Protocol	Info	1
1	0.000000000	8.000000000	Bad_Web_Server	Client	TCP	51669-80 [SYN] Seq=0 Win=8192 Len=6 MS5=1460 WS=256 SACK PERM=1	
2	0.060901000	0.060901000	Client	Bad_Web_Server	TCP	80-51669 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 WS=128	
3	0.000108000	0.061069000	Bad_Web_Server	Client	TCP	51669-80 [ACK] Seq=1 Ack=1 Win=65536 Len=0	
4	0.002658000	0.053727000	Bad_Web_Server	Client	HTTP	GET /download/x.bin HTTP/1.0	21
5	0.054433000	0.111160000	Client	Bad_Web_Server	TCP	80-51669 [ACK] Seq=1 Ack=205 Win=15744 Len=0	
6	0.005131000	6.1283.7000	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]	
7	0.000951000	0.121308000	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]	
8	0.000004000	8.121112000	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]	
9	0.000050000	0.121362000	Bad_Web_Server	Client	TCP	51669-B0 [ACK] Seq=205 Ack=4381 Win=65536 Len=0	
10	0.000215000	0.121577020	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]	
11	0.000002000	0.121579000	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]	21 E
12	0.000002000	0.121581000	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]	
13	0.000002000	0.121583000	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]	
14	0.000002000	0.121585000	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]	
15	0.000001000	0.121586000	Chient	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]	
16	0.000007000	0.121593000	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]	
17	0.000059000	0.121651000	Bad_Web_Server	Client	TCP	51669-80 [ACK] Seq=205 Ack=14601 Win=6 184 Len=0	
18	0.052475000	2 174126000	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]	
10	8 888666888	a theoteant a	rlint	Oad Mak Corner	Tro	ITCD common of a concrembled BDUI	•

Round Trip Time is roughly 52-60ms Web Server does not support TCP Selective Acknowledgements

#### Case Study: Bad TCP Stack (Expert)

-	dit View C	o <u>C</u> apture	Analyze Stat	listics Telepho	my Tools Intern	hals H	elp	-						
0 0	9 📶 🔳		Display Fill	ters		#	2 9 0	. 🖭 👹	M 😼 🎎 🔛					
Filter.	liter.						Apply Save							
de.	del t	rel t	Apply as C			Interes	attention last							
10.	10070	101.1	Apply its Fi	ilter	,	oroco	in minu	Inus indexes	and conturned 1772 approach of a particular	up seq in				
17329	6.000016000	0.000016000	Preparé a P	Filter		TCP	0.0.0	TOUR REGIME		10044301				
17338	8.008184000	6.000200000			-	TCP			Z. Writeshark: 3.393 Expert mitte					
17331	8.000818008	0.00821000	Enabled Pr	otocols	Shift+Ctrl+E	TUP	Terrer D	m Warning	1 (1) Notes 2286 (2286) Chate 4 (6) 0					
		6 000118100	di Decode As.			1224	Errors, u	W. warning	5. 1 (1) [Notes. 2300 (2300) [Chars. 4 (0) [D	Actana: 2000 lea				
17333	0.000001000	0.00039400	3 User Specif	fied Decodes		TCP.	Group	Protocol	Summary	Count				
17334	6.800007000	0.00040100	Sunt bes	V42-072-07-07		TCP	- Sequer	TCP	Previous segment not captured icommon	at capti				
17335	0.000007000	6.000488004	Follow TCP	Stream		TCP	Back	1722	tina mesona en la regula de la companya de la comp P	Charlotter and a state of the s				
7330	6.006162000	6.000390001	Follow UDP	Stream		TCP	Pack	1/32						
2438	0.000200000	0.000399004	Follow 551	Stream		TCB								
17339	0.000001000	0.00000000	CONTRACTOR OF A			TCP								
17348	0.000000000	0.089888001	<ul> <li>Exberr luce</li> </ul>			TCP								
17341	0.000007000	0.00081500	Conversati	ion Filter	,	TCP								
17342	8.008183000	6.000958008	12490	Client	Bad_Web_Server	TCP								
17343	6.008861008	0.000999000	14004	CLIENT	Bad_Web_Server	TEP	D Limit W	display filt	er					
and the second second	the second	8.001066000	14050	Rad_Web_Server.	Client	TCP	- Linne es	1						
17344	6,000899900		Carlow States in the second se	And the second se										
17344	0.000007000	0.001015000	14112	Bad_Web_Server	Client	TCP.	Help	1						
17344 17345 17346	0.000009000 0.000007000 0.000185000	0.001013000	14112 15626	Bad_Web_Server Client	Bad_Web_Server	TCP	Help	1						
17344 17345 17346 17342	6.000009000 6.000007000 6.000185000 6.000001000	0.001013000 0.051200000 0.001201000	14112 15626 17140	Client Client	Client Bad_Wub_Server Bud_Web_Server	TCP	Help	ent of a re	assambled PDV]	10559161				
17344 17345 17346 17347 17348	6.000000000 0.000007000 6.000185000 0.000001000 6.000011000	0.001013000 0.051200000 0.001201000 0.001212000	14112 15626 17140 17194	Bad_Whb_Server Client Client Bad_Web_Server	Client Bad_Web_Server Bud_Web_Server Client	TCP TCP TCP	Help	wnt of a re ACK 17325#5	essembled PSUI   51669-80 [ACK] Seq=205 Ack=18543101 Wim	18550161 265				
17344 17345 17346 17347 17348 17348	6 000009000 0.000007000 6.000185000 6.000001000 6.000011000 8.000011000	0.001013000 0.051200000 0.001201000 0.001212000 0.001213000	14112 15626 17140 17194 17248	Bad_Web_Server Client Client Bad_Web_Server Had_Web_Server	Client Bad_Web_Server Bad_Web_Server Client Client	TCP TCP TCP TCP	ETCP Seg LTCP Dup LTCP Dup	ent of a re ACK 1732945 ACK 1732941	MISANDIGH PDUI   51669-00 [ACK] Seq=205 Ack=18543101 Mim  ] 51669-00 [ACK] Seq=205 Ack=18543101 Mi	18559181 285 285				
17344 17345 17346 17347 17348 17348 17349 17350	6 0000000000 0 000007000 6 0000185000 6 000001000 8 000017000 0 000017000 0 000017000	0.001013000 0.001200000 0.001201000 0.001212000 0.001212000 0.001401000	14112 15636 17140 17194 17248 18762	Bad_Web_Server Client Client Bad_Web_Server Had_Web_Server Client	Client Bad Wub Server Bad Web Server Client Client Dad Web Server	TCP TCP TCP TCP TCP	Help	ent of a re ACK 17329#5 ACK 17329#1 Went of a re	assambled PDUI   51669-88 [ACK] Seq=205 Ack=18543101 Win 8] 51669-88 [ACK] Seq=205 Ack=18543101 Wi assambled PDUI	18559181 205 285 18550621				
17344 17345 17346 17342 17348 17349 17350 17351	6.0000000000 0.00007000 0.000185000 0.00001000 6.000011000 0.000012000 0.000182000 0.000019000	0.001013000 0.001200000 0.001201000 0.001212000 0.001219000 0.001401000 0.001402000	14112 15626 17140 17194 17248 18762 26276	Bad_Web_Server Client Client Bad_Web_Server Had_Web_Server Client Client	Client Bad_Wub_Server Bad_Web_Server Client Client Bad_Web_Server Bad_Web_Server	TCP TCP TCP TCP TCP TCP	Help	ent of a re ACK 1732945 ACK 1732945 Mont of a re wont of a re	assambled PDU1   51669-88 [ACK] Seq=205 Ack=18543101 Win 8] 51669-88 [ACK] Seq=205 Ack=18543101 Wi assembled PDU] assembled PDU] 1 51669 Ack [Sec:365 Ack=18543101 Wi	18559161 205 205 18560621 18560621 18562081 205				
17344 17343 17345 17346 17348 17348 17350 17350 17351 17352	0 0000000000 0 00007000 0 000185000 0 00001000 0 00001000 0 00001000 0 00001000 0 000010000 0 000010000	0.001013000 0.001200000 0.001201000 0.001212000 0.001219000 0.001401000 0.001402000 0.001412000	14112 15636 17140 17154 17248 18762 26276 20338 20338	Bad Whb Server Client Bad Web Server Had Web Server Client Client Bad Web Server Bad Web Server	Client Bud_Meb_Server Ulad_Meb_Server Client Client Bad_Meb_Server Bad_Meb_Server Client Client	TCP TCP TCP TCP TCP TCP TCP	TCP Seg TCP Seg TCP Seg TCP seg TCP seg TCP Seg	Mont of a re Ack 17329#5 Ack 17329#5 Mont of a re Wont of a re Ack 17329#1 Ack 17329#1	INSAMBLEH PDU]   S1669-B0 [ACK] Seq=205 Ack=10543101 Min    S1669-B0 [ACK] Seq=205 Ack=10543101 Min INSAMBLEH PDU] INSAMBLEH PDU]    S1669-B0 [ACK] Seq=205 Ack=10543101 Min    S1669-B0 [   S1669-B0 [  S1660 Min]    S1669-B0 [   S1660 Min]    S1660 Min]	18559161 205 285 18560621 18562083 205 385				
17344 17345 17345 17346 17349 17349 17350 17351 17352 17353 17353	0 0000000000 0 00007000 0 000010000 0 000010000 0 000010000 0 000010000 0 000010000 0 00000000	0.001013000 0.001201000 0.001201000 0.001212000 0.001219000 0.001401000 0.001402000 0.001412000 0.001412000 0.001419000	14112 15626 17140 17154 17248 18762 28276 26390 20384 21898	Bad Web Server Client Client Bad Web Server Client Client Bad Web Server Wad Web Server Client	Client Bad_Meb_Server Bad_Meb_Server Client Client Bad_Meb_Server Bad_Meb_Server Client Client Gad_Meb_Server		TCP Sep TCP Sep TCP Dup TCP Dup TCP Sep TCP Dup TCP Dup TCP Dup TCP Dup	Mont of a re Ack 17329#9 Ack 17329#9 Went of a re Went of a re Ack 17329#1 Went of a re	ISSAUDTEN PDU]   51609-00 [ACK] Seq=205 Ack=10543101 Wim 0] 51609-00 [ACK] Seq=205 Ack=10543101 Wi mosenbled PDU] 1] 51669-00 [ACK] Seq=205 Ack=10543101 Wi 205enbled PDU] 2] 51669-00 [ACK] Seq=205 Ack=10543101 Wi 205enbled PDU]	18559101 205 285 18560621 18562081 205 205 1855254				
17344 17345 17345 17346 17349 17349 17350 17351 17352 17353 17354	0 0000000000 0 00001000 0 00001000 0 00001000 0 00001000 0 00011000 0 000110000 0 000010000 0 000001000 0 00000000	0.001011000 0.001200000 0.001210000 0.001212000 0.001401000 0.001402000 0.001402000 0.001412000 0.001412000 0.001412000 0.001412000 0.001412000	14112 15626 17140 17194 17248 18762 26276 20330 20386 21896 21896	Bad_Wob_Server Client Client Bad_Web_Server Rid_Web_Server Client Bad_Web_Server Client Client	Client Bad Web_Server Bad_Web_Server Client Client Bad_Web_Server Client Client Bad_Web_Server Bad Web_Server Bad Web_Server		Help	ent of a re Ack 1732945 Ack 1732945 Ack 1732945 went of a re went of a re Ack 1732941 Ack 1732941 Ack 1732941	ISSAUBTENT PDU1   51669-80 [ACK] Seq=205 Ack=18543101 Wim   51669-80 [ACK] Seq=205 Ack=18543101 Wi ISSAUBTENT PDU] ISSAUBTENT PDU] 1 51669-80 [ACK] Seq=205 Ack=18543101 Wi 2 51669-80 [ACK] Seq=205 Ack=18543101 Wi ISSAUBTENT PDU]	18559181 205 18560621 18560621 18560623 205 205 205 205 18553541 18555901				
17344 17343 17346 17349 17348 17350 17350 17351 17353 17354 17355	6.000000000 6.00115300 6.00115300 6.000011000 6.00001000 6.00011000 6.00011000 6.00001000 6.00001000 6.00000000 6.00010000 6.00010000 6.00010000	0.001013000 0.001200000 0.001212000 0.001212000 0.001402000 0.001402000 0.001412000 0.001412000 0.001412000 0.001412000 0.001602000 0.001612000	14112 15626 17140 17154 18762 26276 26330 20394 21990 23412 23425	Bad Wob, Server Client Bad Web Server Rad Web Server Client Client Bad Web Server Client Client Client Bad Web Server Client Bad Web Server	Client Bad Meb_Server Bad Meb_Server Client Client Bad Meb_Server Client Client Bad Meb_Server Bad Meb_Server Bad Meb_Server Client		Help	Mont of a re ACK 1732945 ACK 1732945 wont of a re wont of a re ACK 1732941 ACK 1732941 ACK 1732941 wont of a re wont of a re	ISSANDLed PDU1 S1669-BE [ACK1 Seq=205 Ack=18543101 Win B 51669-BE [ACK1 Seq=205 Ack=18543101 Win ISSANDLED PDU3 IS 51669-BE [ACK] Seq=265 Ack=18543101 Win ISSANDLED [ACK] Seq=205 Ack=18543101 Win ISSANDLED PDU3 ISSANDLED PDU3 ISSANDLED PDU3 ISSANDLED PDU3 ISSANDLED PDU3 ISSANDLED PDU3	18559181 285 285 18560621 18560621 1856091 285 285 18553541 18565901 285				
17344 17343 17346 17349 17349 17350 17351 17353 17354 17355 17355 17356 17355	6 000005000 6 001067000 6 00105000 8 00001000 8 00017000 8 00012000 0 00005000 8 00010000 8 00010000 8 00010000 8 00010000 9 00010000 9 00010000	0.001013000 0.001200000 0.001201000 0.001212000 0.001401000 0.001402000 0.001402000 0.001412000 0.001412000 0.001602000 0.001602000 0.001612000 0.001612000	14112 15626 17140 17154 18762 26270 20330 20366 21898 23412 23456 23456	Bad Whb, Server Client Client Bad, Web, Server Client Client Bad, Web, Server Client Client Client Client Client Client Client Bad, Web, Server	Client Bad_Meb_Server Bad_Meb_Server Client Client Bad_Meb_Server Client Bad_Meb_Server Bad_Meb_Server Glient Client		Help	Mont of a re Ack 1732945 Ack 1732945 wint of a re wint of a re Ack 1732941 wint of a re	assambled PDU1 S1609-B0 [ACKI Seq=205 Ack=10543101 Min 1] 51669-B0 [ACK] Seq=205 Ack=10543101 Min assembled PDU1 1] 51669-B0 [ACK] Seq=205 Ack=10543101 Min 2] 51669-B0 [ACK] Seq=205 Ack=10543101 Min assembled PDU1 assembled PDU3 3] 51669-B0 [ACK] Seq=205 Ack=10543101 Min 4] 51669-B0 [ACK] Seq=205 Ack=10543101 Min 5] 51659-B0 [ACK] Seq=205 Ack=10543100 Min 5] 51659-B0 [ACK] Seq=205 Ack=1054500 Min 5] 51659-B0 [ACK] Seq=205 Ack=1054500 Min 5] 5165	18559181 285 285 18560621 18562081 285 285 18563541 18565081 285 285 285				
17344 17343 17346 17347 17348 17356 17351 17353 17354 17355 17354 17355 17356 17356 17356	6 000005000 6 000067000 6 00001000 8 00001000 8 00001000 8 00011000 8 00011000 6 00001000 6 00001000 8 00010000 8 00010000 8 00010000 8 000010000 8 000007000 8 000007000 8 000007000 8 000007000	0.001013000 0.05120000 0.00120000 0.001212000 0.001401000 0.001401000 0.001402000 0.001412000 0.001412000 0.001612000 0.001612000 0.001612000 0.001612000	14112 15626 17140 17194 17248 18762 26276 20306 20306 20306 21890 23412 23406 23520 2554	Bad Whb, Server Client Client Bad Web Server Riad Web Server Client Client Client Client Client Client Bad Web Server Client Bad Web Server Client	Client Bad_Mub_Server Bud_Meb_Server Client Client Bad_Meb_Server Bad_Meb_Server Bad_Meb_Server Bad_Meb_Server Client Client Client Client Bad_Mub_Server	TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	Help	Mont of a re Ack 1732945 Ack 1732945 Ack 1732945 wont of a re wont of a re Ack 1732941 Ack 1732941 Ack 1732941 Ack 1732941 Ack 1732941 Ack 1732941	INSAMBLENT PDU]   S1669-80 [ACK] Seq=205 Ack=10543101 Win 1] S1669-80 [ACK] Seq=205 Ack=10543101 Win INSAMBLED PDU] 1] S1669-80 [ACK] Seq=205 Ack=10543101 Win INSAMBLED PDU] INSAMBLED PDU] 3] S1669-80 [ACK] Seq=205 Ack=10543101 Win INSAMBLED PDU] 3] S1669-80 [ACK] Seq=205 Ack=10543101 Win INSAMBLED PDU] 3] S1669-80 [ACK] Seq=205 Ack=10543101 Win INSAMBLED PDU]	18559181 285 18560621 18560621 205 205 205 18553541 1855500 285 285 285 285 285				

### **Case Study: Web Server Bad RTO**

No.	del.t	rel.t	Destination	Source	Protocol	Info
17327	0.000001000	2.124852000	Client	Bad Web Server	TCP	[TCP regnent of a rearreshled PDU]
17328	*REF*	*REF*	Client	Bad_Web_Server	TCP	[TCP Previous segment not captured] [TCP segment of a reass
17329	0.000016000	0.000016000	Bad_Web_Server	Client	TCP	01009-80 [ALK] Seq=205 7 K=18543101 W1N=5845032 Len=0
17330	0.000184000	0.000200000	Client	Bad Web Server	TCP	[TCP segment of a reassembled PDU]
17331	0.000010000	0.000210000	Bad_Web_Server	Client	TCP	[TCP Dup ACK 17329#1] 1669-80 [ACK] Seq=205 Ack=18543101 W
1						
					3844,484)	
No.	del.t	rel.t	Destination	Source	Protocol	Info
22078	0.000000000	0.259707000	Bad Web Server	Client	TCP	[TCP Dup ACK 1732942374] 51669-80 [ACK] Seq=205 Ack=1854310
22079	0.000006000	0.259713000	Bad Web Server	Client	TCP	[TCP Dup ACK 17329 2375] 51669-80 [ACK] Seq=205 Ack=1854310
22080	0.000359000	0.260072000	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]
22081	0.000007000	0.260079000	Bad_Web_Server	Client	TCP	[TCP Dup ACK 1732#2376] 51669-80 [ACK] Seq=205 Ack=1854310
22082	0.000357000	0.260436000	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]
22083	0.000001000	0.260437000	Client	Bad Web Server	TCP	[TCP segment of a reassembled PDU]
22084	0.000007000	0.268444880	Bad_Web_Server	Client	TCP	[TCP Dup ACK 17 29#2377] 51669-B0 [ACK] Seq=205 Ack=1854310
22685	8.000006000	0.260450000	Bad_Web_Server	Client	TCP	[TCP Dup ACK 17329#2378] 51669-80 [ACK] Seq=205 Ack=1854310
22086	0.000181000	0.260631000	Client			
22087	0.000007000	0.260638000	Bad_Web_Ser	262ms he	ofore re	etransmitting the lost segment??
22088	0.000182000	0.260820000	Client			
22089	0.000008000	0.260828000	Bad_Web_Server	CLient	TCP	[TCP Dup ACK 17329#2380] 51669-80 [ACK] Seq=205 Ack=1854310
22090	0.000180000	0.261008000	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]
22091	0.000007000	0.261015000	Bad_Web_Server	Client	TCP	[TCP Dup ACK 17329#2381] 51669-80 [ACK] Seq=205 Ack=1854310
22092	0.000359000	0.261374000	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]
22093	0.000001000	0.261375000	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]
22094	0.000006000	0.261381000	Bad Web Server	Client	TCP	[TCP Dup ACK 17329#2382] 51669-80 [ACK] Seq=205 Ack=1854310
22095	0.000007000	0.261388000	Bad_Web_Server	Client	TCP	[TCP Dup ACK 17329#2383] 51669-80 [ACK] Seq=205 Ack=1854310
22896	0.000423000	0.261811000	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]
22097	0.000007000	8.761010000	Mad_Web_Server	Client	TCP	[TCP Dup ACK 17329#2384] 51669-80 [ACK] 5eq=205 Ack=1854310
22098	0.000359000	0.262177000	Client	Bad_Web_Server	TCP	[TCP Fast Retransmission] [TCP segment of a reassembled PDU
22000	A AAAATFOAAA A	AUDITERC A	Rad Woh Sorvar	Client	TIP	51660 88 [AP#1 Son-785 Ark-37831503 Win-3764515 Jan-8
-						3+

### **Case Study: Bad Web Server Performance**



Web Server does not appear to react very well to any level of packet loss

# How should TCP recover from packet loss?

No.	del.t	rel.t	Destination	Source	Proto	ocol	Info									
1	0.00000000	0.0880000	00 Good Web Ser	ver Client	TC	P.	50086 8	O [SYN]	Seg=	0. Win=01	92 Lenet	M55=142	0 WS=256	SACK PER	RM=1	
1 F 3	0.04449400	ST GNORED IN	00 Climt	COST MID STY	1000 TX	1	EB MOOR	3 6507	ALC: NO	Red A	Real WID	=5840 Lat	LIO NOSTE	ALC DE LA	SHURLS.	5
3	0.00000000	0.0445600	00 Good Web Ser	ver Client	TC	P.	50096-8	D TACK	Seq=	1 Ack=1 1	rin=6656	0 Len=0				
	Constant Constant			anna annann			an an an Anna Anna An	Sen denned	-	119.1796.5cet0ful	area resultation	ntsdenteant				1
-		=	CONTROL (0)		_				-							
	0.0	001 - Number	No. Oneration (	NOP) (1)												
þ	TCP SACK P	ermitted Opti	on: True													
4	1				-									· · · ·		_
No.	del.t	rel.t	Destination	Source	Protocol	Info								tcp.sac	.k	1
5785	0.808812	0.043399	Good Web Server	Client	TCP	[TCP	Dup ACK	5491#1	471 50	896-98 [4	CK1 Seq-	359 Ack=5	146317 W:	in	True	
\$786	0.000175	0.043574	Client	Good_Web_Server	TCP	[TCP	segnent	ofar	eassee	bled PDU)	1					
5787	0.000018	0.043592	Good_Web_Server	Client	TCP	[TCP	Dup ACK	5491#1	48] 50	006-80 [4	CK) Seq=	:359 Ack=5	146317 Wi	LR	True	61
5788	0.000508	0.044200	Client	Good_Web_Server	TCP	[TCP	segnent	of a r	eassen	bled PDU]	Harry H					
5789	0.000033	0.044233	Good_Web_Server	Client	TCP	[TCP	Dup ACK	5491#1	491 50	006-00 [/	CK1 Seq:	:359 Ack=5	146317 W	in	True	£1
5790	0.006313	0.044546	Client	Good Web_Server	TCP	[TCP	segnent	ofar	eassee	bled PDU]	6					
5791	0.000037	0.044583	Good_Web_Server	Client	TCP	ETCP	Dup ACK	5491#1	501 50	086.00 [/	CK] Seq	359 Ack+5	146317 W	LITS	True	
5792	0.000026	0.044609	Client	Good_Web_Server	TCP	[TCP	segnent	ofar	easser	bled PDU]	Sector sector					
5793	0.000014	0.044623	Good_Web_Server	Client	TCP	[ TCP	Dup ACK	5491#1	51) 50	886-80 IA	CK] Seq:	359 Ack=5	146317 Wi	LR	True	
5794	0.000895	0.044718	Client	Good_Web_Server	TCP	[TCP	segnent	of a r	easser	bled PDU)	Jan					
5.745	8.900017	Contraction of the local division of the loc	Good_Neb_Server	<b>Client</b>	for	True	Dup ACK	-44	527 56	065-84 [/	CKI Seg-	35+ Ack=5	Lapater as	in.	Tran	
5796	0.000095	01044830	Client	Good_Web_Server	TCP	[TCP	Fast Re	transm	\$5100]	[TCP set	ment of	a reassem	bled PDU)			
5797	0.000134	0.044664	Good_Web_Server	Client	TCP	5008	5-80 [AC	K] Seq=	359 Ac	k=536499)	Win=335	9488 Len=	0			
5798	0.000063	0.045027	Client	Good_Web_Server	TC#	[TC#	segnent	of a r	eassen	bled POU	0					
5799	0.000064	0.045091	Client	Good_Web_Server	TCP	[ TCP	segment	ofar	035540	bled PDU)	E.					
5000	0.000015	0.045106	Good_Web_Server	Client	TCP	5008	6-80 [AC	KI Seq=	359 Ac	k=536783)	Win=335	6672 Len=	0			
· —								)								•
10	alculated wi	ndow 5128: 357	18.3681													1
IW	indow size s	caling factor:	256]													
D Ch	ecksum: 0xd3	Se [correct]														
Ur	gent pointer	: 0		<b>–</b>												
\$ Op	tions: (12 b	ytes), No-Oper	ation (NOP), No-(	peration (NOP), 3	SACK											
D C	And Distances in the local distance of the l	144		State of the second second												5

TCP should enable and use SACK to send/receive better feedback about performance. Retransmissions should occur as close to the RTT as possible.

# Good TCP Recovery vs Bad TCP Recovery

#### Good Web Server transmits 87292 bytes at RTT (44ms) during recovery

No.	del.t	rel.t	CumBytes	Destination	Source	Protocol	Info
5880	0.000021000	0.041703000	84284	Good_Web_Server	Client	TCP	50086-80 [ACK] Seq=359 Ack=5443097 Win=33497(
5881	0.000271000	0.041974000	85758	Client	Good_Web_Server	TCP	[TCP segment of a reassembled PDU]
5882	0.003003000	0.044977000	87232	Client	Good_Web_Server	TCP	[TCP segment of a reassembled PDU]
5683	0.000059000	0.045036000	87292	Good_Web_Server	Client	TCP	50006-80 [ACK] Seq=359 Ack=5445937 Win=33466
5884	0.000066000	0.045102000	88766	Client	Good_Web_Server	TCP	[TCP segment of a reassembled PDU]
Enne	0 000717000		00040	Clinet.	Food Mak Former	TCD	ITTO reamont of a passrouhlad DOUL
4							)+

#### Bad Web Server only transmits 7678 bytes at RTT (60ms) during recovery

No.	del.t	rel.t	CumBytes D	estination	Source	Protocol	Info	4
22096	0.000423000	2.386664000	23213546	client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]	
22097	0.000007000	2.386671000	23213600 Ba	ad_Web_Server	Client	TCP	[TCP Dup ACK 17329#2384] 51669-80 [ACK] Seq=205 Ack=1	8
22098	*REF*	*REF*	1514	Client	Bad_Web_Server	TCP	[TCP Fast Retransmission] [TCP segment of a reassembl	1
22099	0.000931000	0.000931000	1568 84	ad_Web_Server	Client	TCP	51669-80 [ACK] Seq=205 Ack=22021593 Win=3264512 Len=0	Ê.
22106	0.054327000	0.055258000	3082	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]	8
22181	0.000324000	0.055582000	4596	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled POU]	1
22102	0.000032000	0.055614000	4650 Ba	ad_Web_Server	Client	TCP	51669-80 [ACK] Seq=205 Ack=22024513 Win=3452672 Len=0	1
22103	0.000969000	0.056583000	6164	Client	Bad_Web_Server	TCP	[TCP segment of a reassembled PDU]	1
22104	0.050569000	0.107152000	7678	Client	Bad_Web_Server	TCP	(TCP segment of a reassembled PDU)	12
22105	0.000047000	0.107199000	7732 Ba	ad_Web_Server	Client	TCP	51669-80 [ACK] Seq=205 Ack=22027433 Win=3449856 Len=0	
•					)		3+	1

### Good TCP Recovery Visualization (I/O Graph)



### **Bad TCP Recovery Visualization (I/O Graph)**



#### **Bad TCP Stack Recovering with Slow Start**



Bad TCP stack using slow start instead of congestion control after packet loss.

# Thank You !! Questions?

(feel free to email me at kevin\_burns@cable.comcast.com