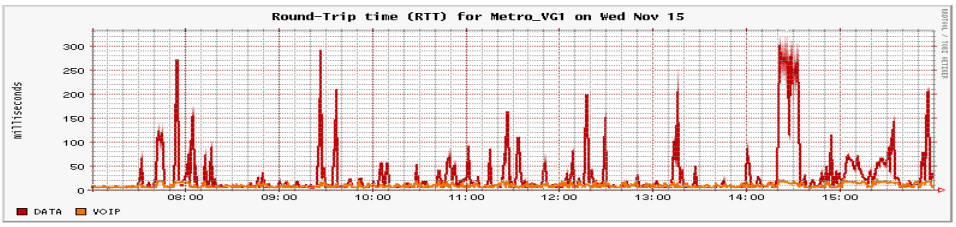
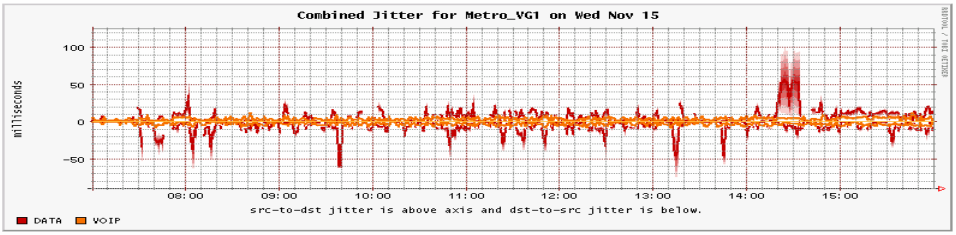
BCBS Utica Office, Nov 15 2006, 7am-4pm

IP SLA Response Times for DATA (red) and VOIP (orange)



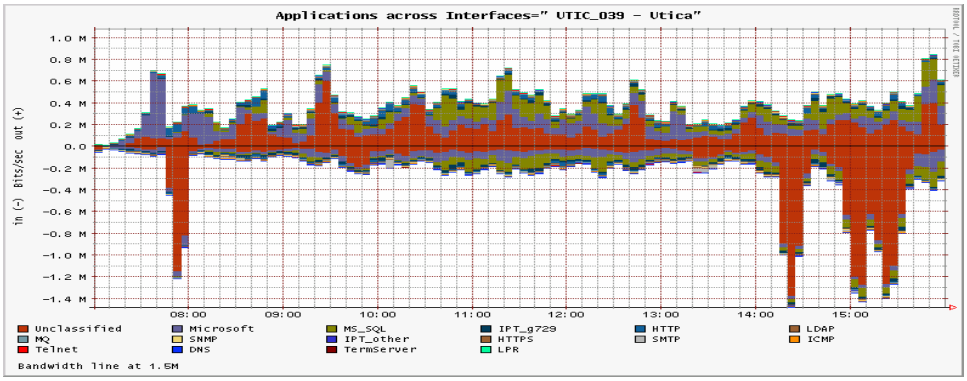
	ms			stddev		
	min	avg	max	min	avg	max
DATA	4	26	378	0	9	133
VOIP	3	9	40	0	4	8



	src-to-dst						dst-to-src					
	ms			stddev			ms			stddev		
	min	avg	max	min	avg	max	min	avg	max	min	avg	max
DATA	1	6	56	0	6	112	1	6	61	0	5	73
VOIP	0	3	11	0	2	6	1	4	9	0	3	6

Note: all VOIP values are normal and within limits. QoS is working.

NetFlow traffic breakdown



The spikes correlate to the IP SLA probe for DATA traffic. Clicking on the big inbound spikes show that:

7:50am and 3:00pm – 10.39.2.116 (w2ua52016f3) to TCP port 1299 of 10.64.80.63 (pwn401e6980)
2:25pm – 10.39.2.69 (lcnu504fnx4) from TCP port 4242 of 10.39.2.69 (no dns)

For example:

ip-src-addr	ip-src-name	ip-dst-addr	ip-dst-name	proto	src-port	dst-port	tcp-flags	dscp	packets	bytes	start-time	dur
10.39.2.116	w2ua52016f3	10.64.80.63	pwn401e6980	tcp	3520	1299	---pa-	0	2857	4281900	3:26:16 PM	62
10.39.2.116	w2ua52016f3	10.64.80.63	pwn401e6980	tcp	3520	1299	---pa-	cs1	186	278988	3:26:16 PM	62
10.64.80.63	pwn401e6980	10.39.2.116	w2ua52016f3	tcp	1299	3520	---pa-	0	1842	97656	3:26:16 PM	61
10.39.2.116	w2ua52016f3	10.64.80.63	pwn401e6980	tcp	3546	1299	---pa-	0	2665	3970188	3:26:33 PM	63
10.64.80.63	pwn401e6980	10.39.2.116	w2ua52016f3	tcp	1299	3546	---pa-	0	1754	110248	3:26:33 PM	63
10.39.2.116	w2ua52016f3	10.64.80.63	pwn401e6980	tcp	3546	1299	---pa-	cs1	167	250480	3:26:34 PM	61
10.64.80.63	pwn401e6980	10.39.2.116	w2ua52016f3	udp	37750	4916	----a-	0	1	36	3:27:06 PM	0
10.64.80.63	pwn401e6980	10.39.2.116	w2ua52016f3	tcp	1299	3520	---pa-	0	1930	102516	3:27:17 PM	65
10.39.2.116	w2ua52016f3	10.64.80.63	pwn401e6980	tcp	3520	1299	---pa-	0	2931	4385836	3:27:18 PM	64
10.39.2.116	w2ua52016f3	10.64.80.63	pwn401e6980	tcp	3520	1299	---pa-	cs1	152	227988	3:27:18 PM	64

NetFlow shows that some of these spikes are correctly being placed in the Scavenger class (DSCP CS1). This suggests that the BCBS QoS policy in place is working well.