How to Gain More Performance Out of Today's Networks

Laura Chappell

Sr. Protocol/Security Analyst

Protocol Analysis Institute, LLC

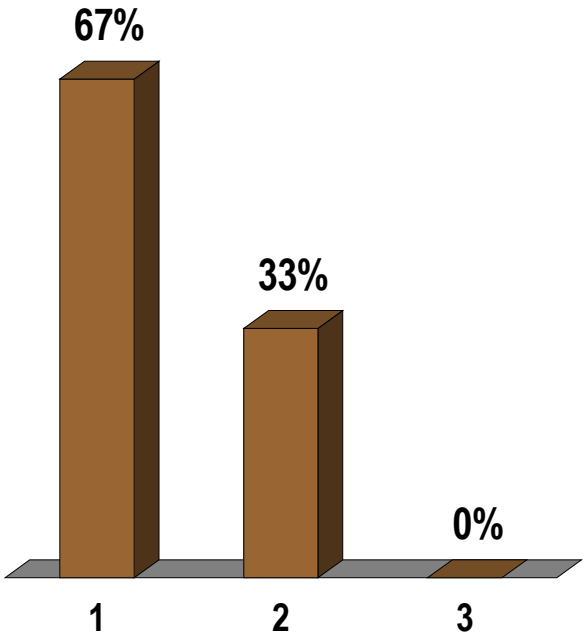
www.packet-level.com

Topics

- **The framework for managing the network**
- **Common causes of performance problems**
- **What three things can you do to improve performance?**

Have you heard the dreaded "the network is slow" complaint in the last 30 days?

1. **Yes**
2. **No**
3. **30 days...? Try 30 minutes!**



Think of Your Network as a Bi-directional Traffic Map

- Build a managed network

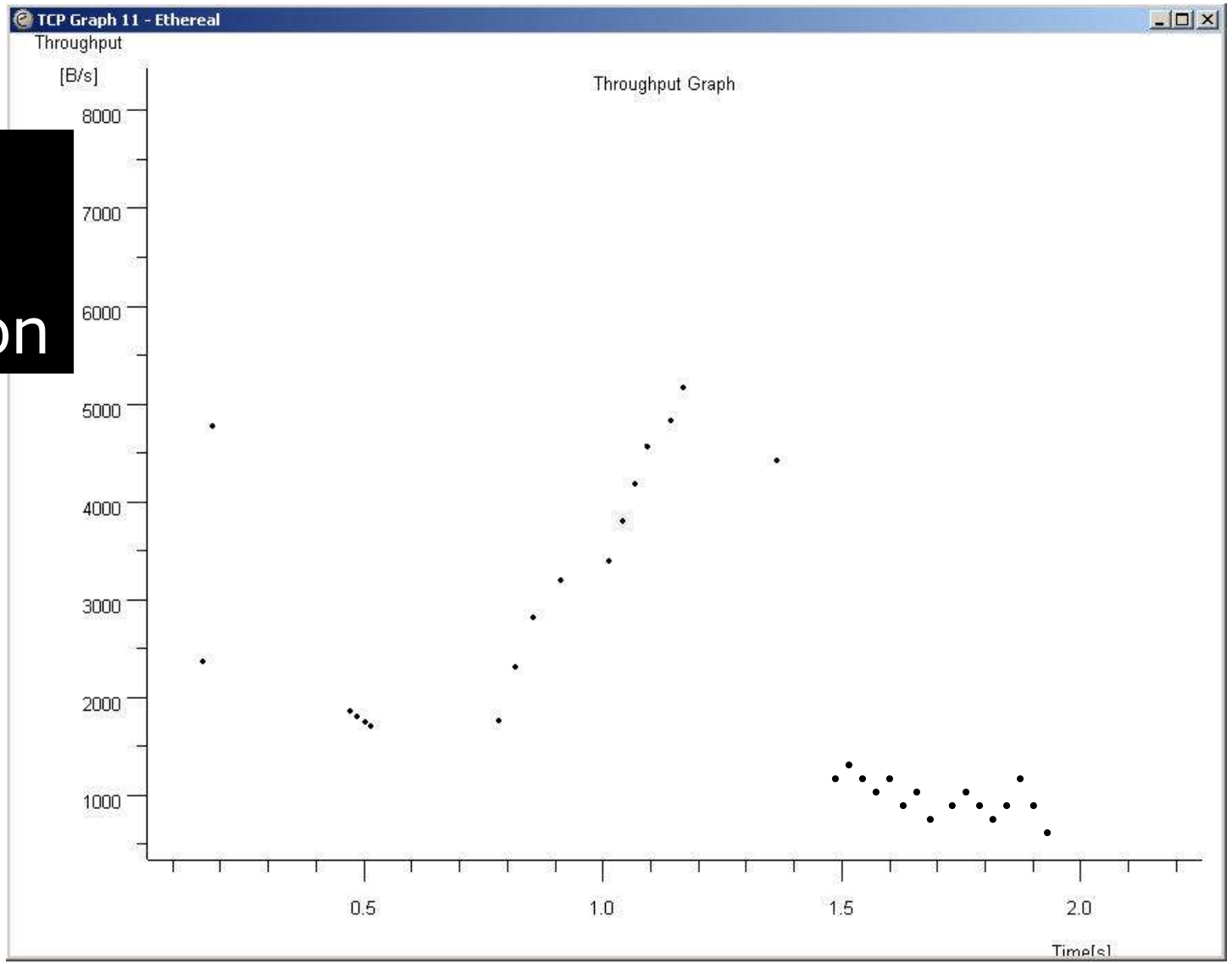
Common Causes of Performance Problems

- **Default configurations (Windows)**
- **Single points of congestion (bottleneck)**
- **Poorly written applications (repetitive dumb queries)**
- **High latency (delays along the path)**
- **Transmission/configuration faults (retransmissions)**
- **Chatty applications (Peer-to-peer)**
- **High-bandwidth applications (streaming video)**
- **High priority applications (VoIP)**
- **Security (payload inspection)**
- **Users! (We'll talk later…)**

Default Configurations

No.	Time	ourc	stinati	Protoco	Info
203	0.000248	10.1	10.0	NBNS	Name query NB SYN311<20>
204	0.750618	10.1	10.0	NBNS	Name query NB SYN311<20>
205	0.751100	10.1	10.0	NBNS	Name query NB SYN311<20>
206	0.751981	10.1	10.0	ICMP	Echo (ping) request
207	0.000068	10.1	10.0	ICMP	Echo (ping) reply
208	0.000268	10.1	10.0	NBNS	Name query NBSTAT *<00><00><00>
209	0.000046	10.1	10.0	ICMP	Destination unreachable
210	1.500956	10.1	10.0	NBNS	Name query NBSTAT *<00><00><00>
211	0.000066	10.1	10.0	ICMP	Destination unreachable
212	1.502146	10.1	10.0	NBNS	Name query NBSTAT *<00><00><00>
213	0.000068	10.1	10.0	ICMP	Destination unreachable

Single Points of Congestion



Calculating Maximum Throughput

Let's start with a 100 Mbps link.

1. Convert data rate down to bits

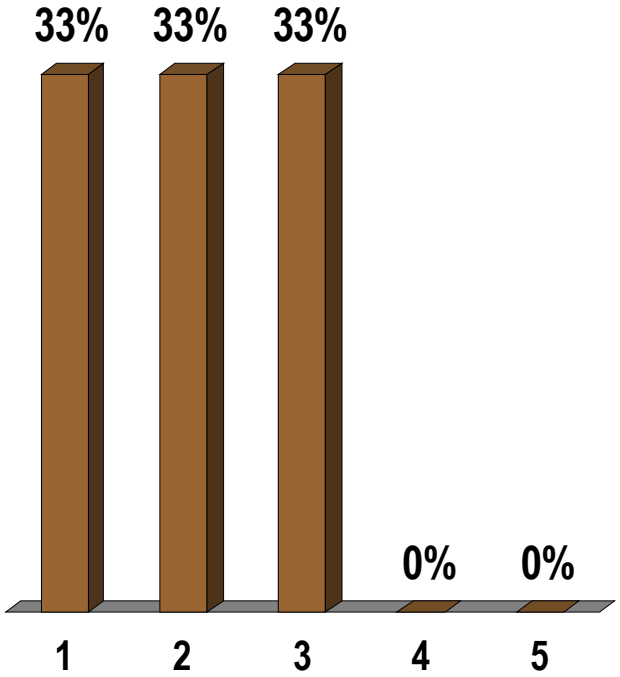
   100 Mbps = 100,000,000 bits per second

2. Convert **data rate over to bytes**

   100,000,000/8 = 12,500,000 bytes per second

Which is an acceptable round trip latency time for traffic that crosses one 100 Mbps network?

1. **46 milliseconds**
2. **46 microseconds**
3. **246 milliseconds**
4. **246 microseconds**
5. **Hunh? I don't know**



Calculating One-Way Latency Values

1. **Ethernet 1518 + 20 bytes (8 byte preamble and 12 byte Interpacket gap time) = 1538**

2. **Now – what can the network hold in 100 Mbits/second – 100? 12,500,000 bytes/second**

3. **Divide your packet size by the bytes/second rate.**

   1538/12,500,000= .00012304 or 123 microseconds

Poorly Written Applications

No.	Time	Source	stinati	rotoco	Info
45	0.000315	10.16	10.1	NCP	C Read From File - 0x0000B6FB0000
46	0.000031	10.16	10.1	NCP	R OK
47	0.000034	10.16	10.1	NCP	C Read From File - 0x0000B6FB0000
48	0.000284	10.16	10.1	NCP	R OK
49	0.000032	10.16	10.1	NCP	C Read From File - 0x0000B6FB0000
50	0.000034	10.16	10.1	NCP	R OK
51	0.000286	10.16	10.1	NCP	C Read From File - 0x0000B6FB0000
52	0.000032	10.16	10.1	NCP	R OK
53	0.000031	10.16	10.1	NCP	C Read From File - 0x0000B6FB0000
54	0.000033	10.16	10.1	NCP	R OK

90-byte packets; duplicate requests = lousy throughput

High Latency Causing Retransmissions

No. .	Time	ourc	stinati	rotoco	Info
7	1.000070	67.:	204.	DNS	Standard query A www.google.com
8	2.000380	67.:	204.	DNS	Standard query A www.google.com
9	0.081667	204	67.1	DNS	Standard query response CNAME www.google.

Transmission/Configuration Faults

No. .	Time	ource	stinati	Protoco	Info
311	0.000307	10.1	10.C	DNS	Standard query response A 10.0.0.18
406	6.783527	10.1	10.C	DNS	Standard query A SJ-SQL2000.corp.abc.com
407	0.000380	10.1	10.C	DNS	Standard query response, No such name
408	0.000008	10.1	10.C	DNS	Standard query A SJ-SQL2000.abc.com
411	1.001459	10.1	67.1	DNS	Standard query A SJ-SQL2000.corp.abc.com
412	0.016817	67.1	10.C	DNS	Standard query response, No such name
413	0.000256	10.1	10.C	DNS	Standard query A SJ-SQL2000.corp.abc.com
414	0.000321	10.1	10.C	DNS	Standard query response, No such name

Chatty Applications

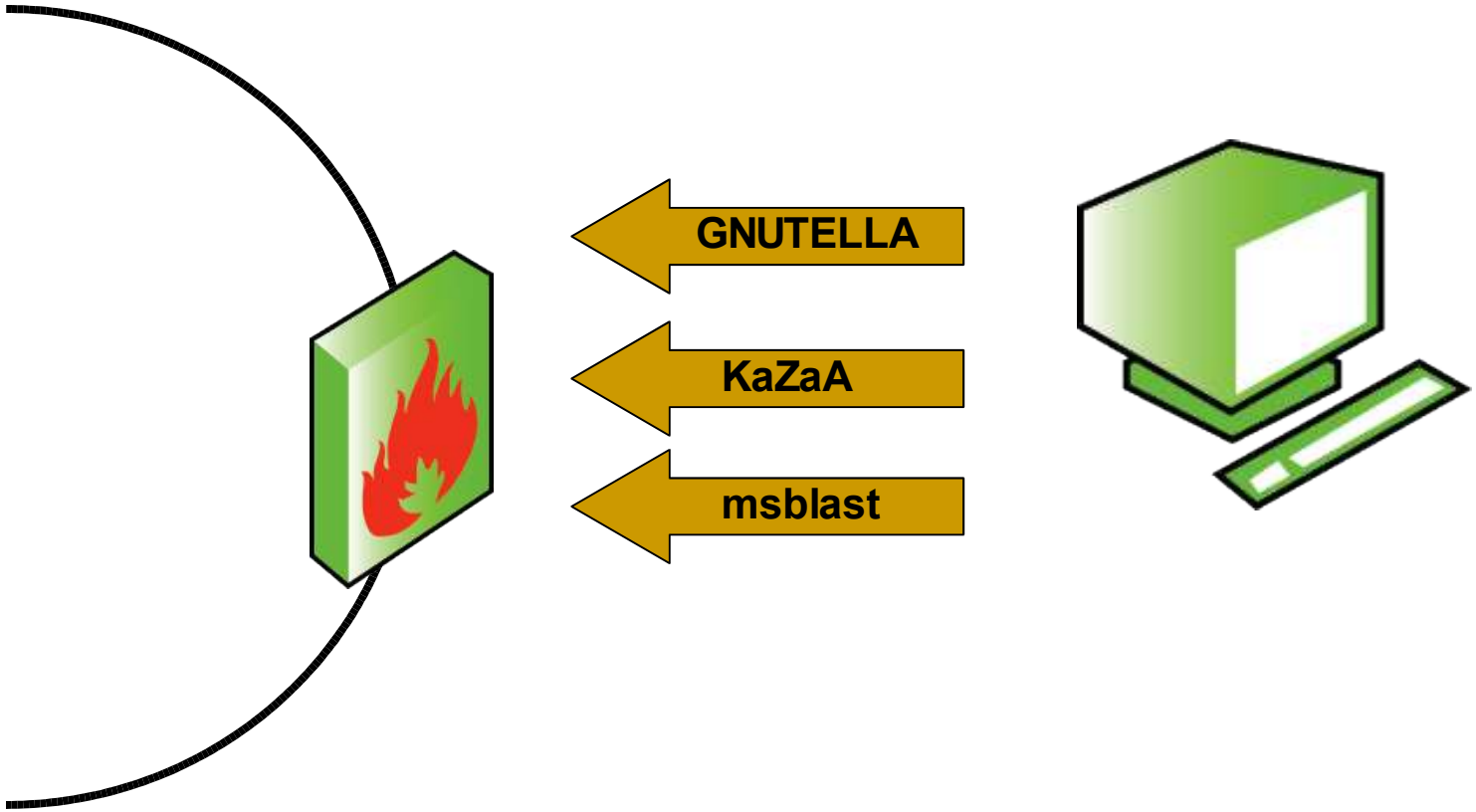
No.	Time	ource	stinati	Protoco	Info
1	0.000000	10.:	66.6	TCP	3663 > 6346 [SYN] Seq=58393422 Ack=0
2	0.028257	10.:	198.	TCP	3684 > 6346 [SYN] Seq=58414377 Ack=0
3	0.032574	198	10.1	TCP	6346 > 3684 [RST, ACK] Seq=0 Ack=584
4	0.439063	10.:	198.	TCP	3684 > 6346 [SYN] Seq=58414377 Ack=0
5	0.031318	198	10.1	TCP	6346 > 3684 [RST, ACK] Seq=0 Ack=584
6	0.468750	10.:	198.	TCP	3684 > 6346 [SYN] Seq=58414377 Ack=0
7	0.030630	198	10.1	TCP	6346 > 3684 [RST, ACK] Seq=0 Ack=584
8	0.055866	10.:	65.1	TCP	3685 > 6346 [SYN] Seq=58415434 Ack=0

High-Bandwidth Applications

- **Video**
- **Audio**
- **Games**
- **P2P**

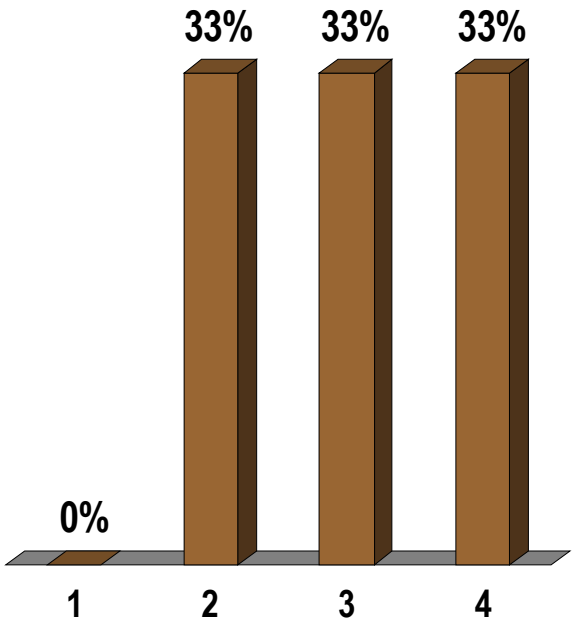
Security

Deep-Packet Inspection



How have your users affected network performance?

1. **Loading their own lousy applications on the network**
2. **They browse the Internet and download (or attempt to download) large files all day**
3. **They launch their own little servers and cause network havoc**
4. **They do other bad stuff to my network**



What Can You Do to Optimize Performance?

- **Learn**
- **Fix**
- **Enhance**

What Can You Do to Optimize?

#1: Learn

- **Put an analyzer on the cable**
- **Learn what the latency times should be**
- **Learn where the bottlenecks are**
- **Learn what's traveling over the wire**
- **Understand normal and enhanced TCP/IP communications**

What Can You Do to Optimize?

#2: Fix

- **Remove network faults – They induce delays**
- **Remove bottlenecks through redistribution, prioritization or removal of applications**
- **Remove unnecessary traffic**

What Can You Do to Optimize?

#3: Enhance

- **Remove any hubs left in the organization**
- **Consider prioritizing traffic (queuing) on internal links**
- **Consider VLANs for group**
- **Consider caching servers**
- **On long fat networks, consider enhancing TCP's buffer size**
- **Consider packet shaping on WAN links**