



# Testing Darwinsim: The History and Evolution of Network Resiliency

**Mike Hamilton**  
**Ixia Communications**

Session ID: SPO-210

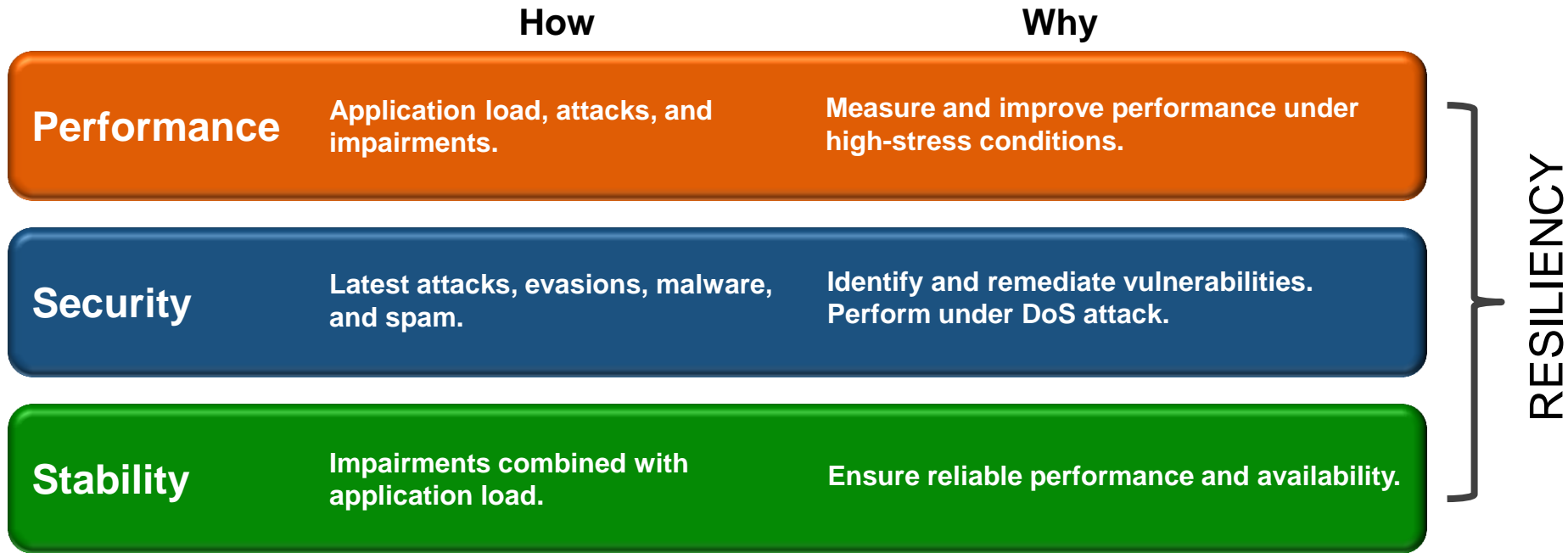
Session Classification: General Interest

**RSACONFERENCE**  
**EUROPE 2012**

# Why Should I Care?



# Defining Resiliency



# Performance

**How**

**Why**

**Performance**

Application load, attacks, and impairments.

Measure and improve performance under high-stress conditions.





# The Datasheet Game - Carrier Class Firewall

Metric	Firewall A	Firewall B	Firewall C
Throughput (Max)	150 Gbps	560 Gbps	640 Gbps†
*3WHS+D+3WC	**Derived from PPS	†Connectivity	‡Stated as Application



# The Datasheet Game - Carrier Class Firewall

Metric	Firewall A	Firewall B	Firewall C
Throughput (Max)	150 Gbps	560 Gbps	640 Gbps†
Throughput (IMIX)	37.8 Gbps	560 Gbps	135 Gbps‡
*3WHS+D+3WC	**Derived from PPS	†Connectivity	‡Stated as Application



# The Datasheet Game - Carrier Class Firewall

Metric	Firewall A	Firewall B	Firewall C
Throughput (Max)	150 Gbps	560 Gbps	640 Gbps†
Throughput (IMIX)	37.8 Gbps	560 Gbps	135 Gbps‡
Throughput (64B)	7.7 Gbps**	560 Gbps	31 Gbps**
*3WHS+D+3WC	**Derived from PPS	†Connectivity	‡Stated as Application





# The Datasheet Game - Carrier Class Firewall

Metric	Firewall A	Firewall B	Firewall C
Throughput (Max)	150 Gbps	560 Gbps	640 Gbps†
Throughput (IMIX)	37.8 Gbps	560 Gbps	135 Gbps‡
Throughput (64B)	7.7 Gbps**	560 Gbps	31 Gbps**
Connections per Second*	380,000	3.29M	320,000
*3WHS+D+3WC	**Derived from PPS	†Connectivity	‡Stated as Application



# The Datasheet Game - Carrier Class Firewall

Metric	Firewall A	Firewall B	Firewall C
Throughput (Max)	150 Gbps	560 Gbps	640 Gbps†
Throughput (IMIX)	37.8 Gbps	560 Gbps	135 Gbps‡
Throughput (64B)	7.7 Gbps**	560 Gbps	31 Gbps**
Connections per Second*	380,000	3.29M	320,000
Concurrent Connections	20M	280M	100M
*3WHS+D+3WC	**Derived from PPS	†Connectivity	‡Stated as Application



# The Datasheet Game - Carrier Class Firewall

The screenshot shows a Wireshark capture of a network session between 1.1.148.13 and 1.2.39.43. The packet list table is as follows:

No.	Size	Source	Destination	Protocol	Info
1	60	1.1.148.13	1.2.39.43	TCP	35672 > http [SYN] Seq=0 Win=5792 Len=0 MSS=1460
2	60	1.2.39.43	1.1.148.13	TCP	http > 35672 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
3	60	1.1.148.13	1.2.39.43	TCP	35672 > http [ACK] Seq=1 Ack=1 Win=5792 Len=0
4	60	1.1.148.13	1.2.39.43	HTTP	Continuation or non-HTTP traffic[Malformed Packet]
5	60	1.2.39.43	1.1.148.13	TCP	http > 35672 [ACK] Seq=1 Ack=4 Win=7252 Len=0
6	60	1.2.39.43	1.1.148.13	HTTP	Continuation or non-HTTP traffic[Malformed Packet]
7	60	1.1.148.13	1.2.39.43	TCP	35672 > http [ACK] Seq=4 Ack=4 Win=7252 Len=0
8	60	1.2.39.43	1.1.148.13	TCP	http > 35672 [FIN, ACK] Seq=4 Ack=4 Win=7252 Len=0
9	60	1.1.148.13	1.2.39.43	TCP	35672 > http [FIN, ACK] Seq=4 Ack=5 Win=7252 Len=0
10	60	1.2.39.43	1.1.148.13	TCP	http > 35672 [ACK] Seq=5 Ack=5 Win=7252 Len=0

The packet details pane for packet 4 shows:

```

HTTP
  Continuation or non-HTTP traffic[Malformed Packet]
  
```

The status bar at the bottom indicates the file path: "/Users/mhamilton/Downloads/Slot2Port0.1346946381660.pc..." and the current packet is 4.

# The Datasheet Game - Carrier Class Firewall

Metric	Firewall A	Firewall B	Firewall C



# The Datasheet Game - Carrier Class Firewall

Metric	Firewall A	Firewall B	Firewall C
Throughput (64B)	7.7 Gbps	560 Gbps	31 Gbps



# The Datasheet Game - Carrier Class Firewall

Metric	Firewall A	Firewall B	Firewall C
Throughput (64B)	7.7 Gbps	560 Gbps	31 Gbps
CPS	380,000	3.29M	320,000



# The Datasheet Game - Carrier Class Firewall

Metric	Firewall A	Firewall B	Firewall C
Throughput (64B)	7.7 Gbps	560 Gbps	31 Gbps
CPS	380,000	3.29M	320,000
Worst-case Throughput	1.8 Gbps	15.8 Gbps	1.5 Gbps



# The Datasheet Game - Carrier Class Firewall

Metric	Firewall A	Firewall B	Firewall C
Throughput (64B)	7.7 Gbps	560 Gbps	31 Gbps
CPS	380,000	3.29M	320,000
Worst-case Throughput	1.8 Gbps	15.8 Gbps	1.5 Gbps
Worst-case Goodput	6 Mbps	52 Mbps	5.1 Mbps





# Performance

**How**

**Why**

**Performance**

Application load, attacks, and impairments.

Measure and improve performance under high-stress conditions.



# Security

**How**

**Why**

**Performance**

Application load, attacks, and impairments.

Measure and improve performance under high-stress conditions.

**Security**

Latest attacks, evasions, malware, and spam.

Identify and remediate vulnerabilities. Perform under DoS attack.



# Does Mark the Spot?



# IPS - Imprecise Performance Systems

	Firewall A	Firewall B	Firewall C
Throughput (64B)	7.7 Gbps	560 Gbps	31 Gbps
CPS	380,000	3.29M	320,000
Worst-case Throughput	1.8 Gbps	15.8 Gbps	1.5 Gbps
Worst-case Goodput	6 Mbps	52 Mbps	5.1 Mbps
IPS Throughput	26 Gbps	131.6 Gbps	40 Gbps



# DDoS - Are You Ready?

## Largest Bandwidth Attacks Reported

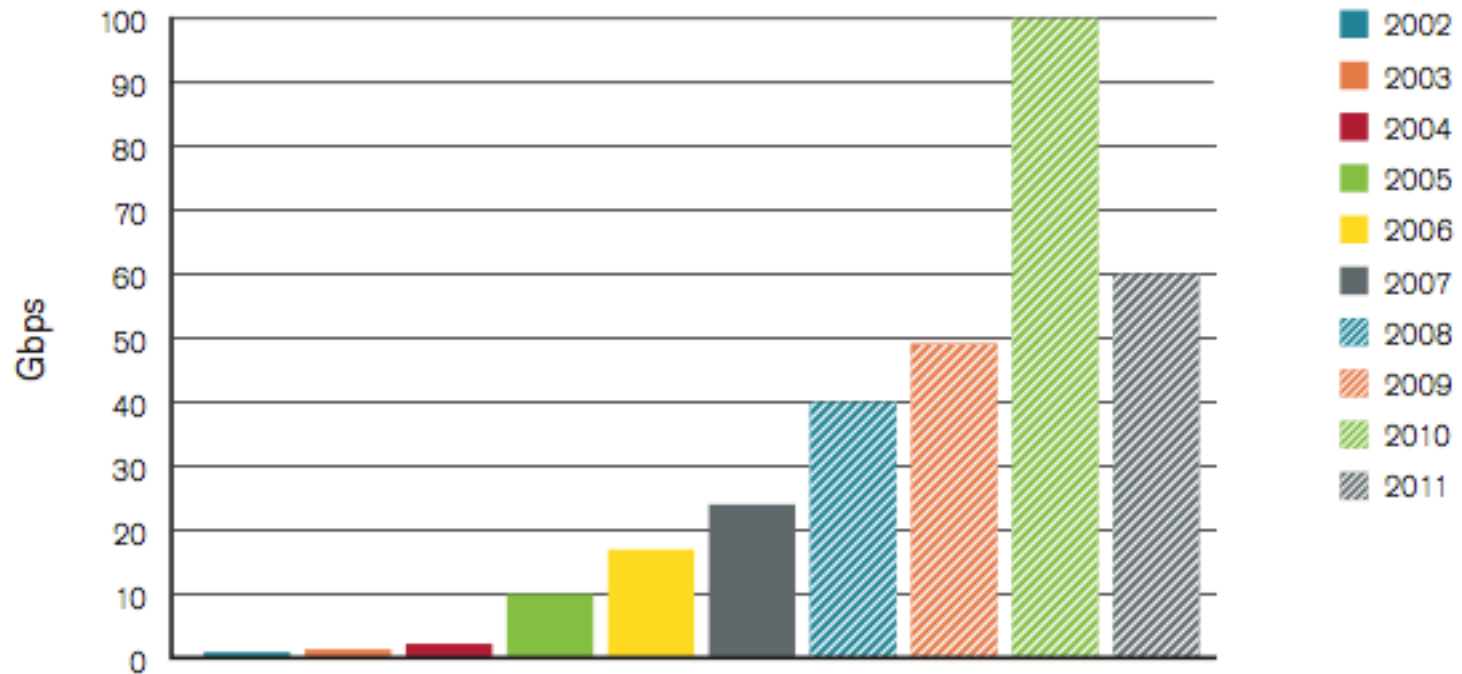


Figure 15 Source: Arbor Networks, Inc.



# Why Should I Care?

- "Approximately \$250,000 USD/incident."
- "\$8,000 USD/incident."
- "Approximately 1,000EUR/incident."
- "Roughly \$1M USD to \$1.5M USD/incident."
- "\$300,000 USD/incident."
- "\$1M USD/incident."
- "More than \$100,000 USD/month."
- "Net revenue-generator—we offer commercial DDoS mitigation services."

*Source: Arbor Networks, Inc.*



# \$, £, €, ¥...£

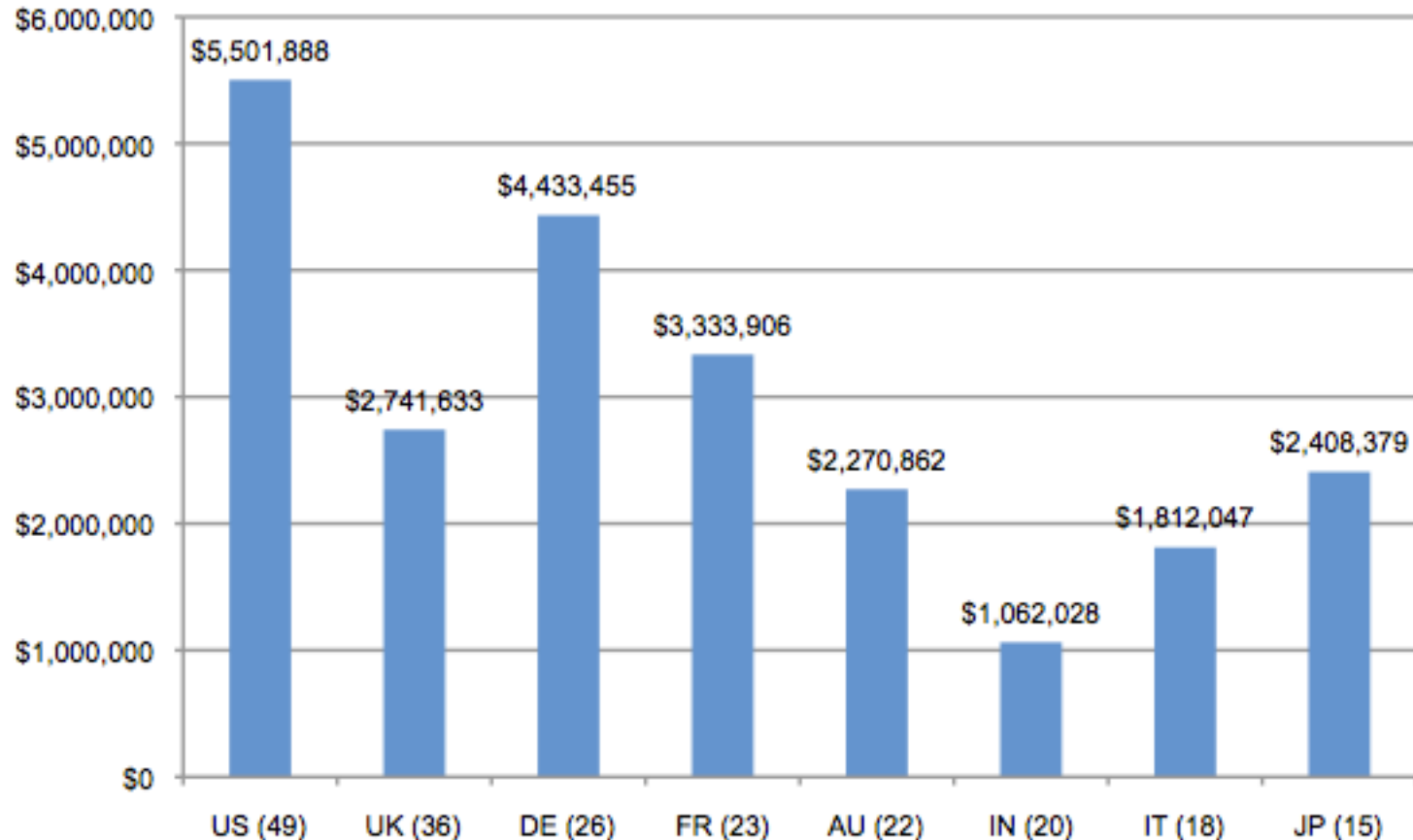


[www.jolyon.co.uk](http://www.jolyon.co.uk)



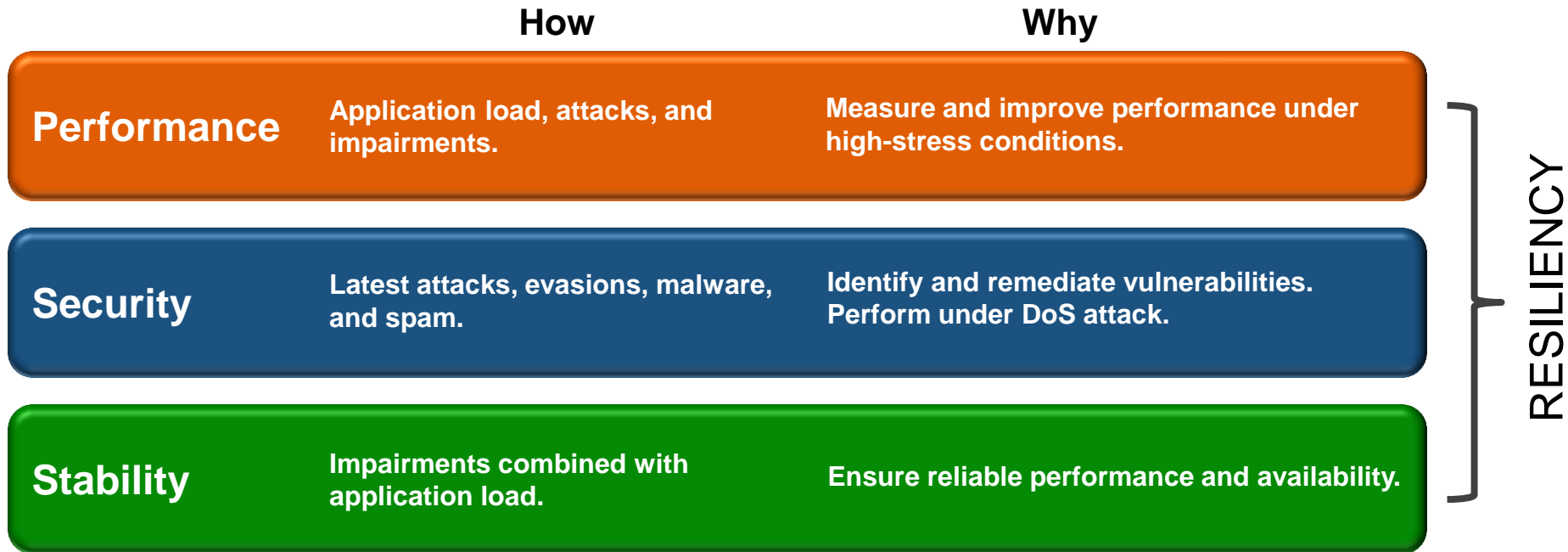
# DLP - Dollar Loss Prevention

Figure 2. The average total organizational cost of data breach






# Stability





# Stability

sta·bil·i·ty  [stuh·bil-i-tee]  [Show IPA](#)

**noun, plural sta·bil·i·ties.**

1. the state or quality of being stable.
2. firmness in position.
3. continuance without change; permanence.
4. *Chemistry* . resistance or the degree of resistance to chemical change or disintegration.
5. resistance to change, especially sudden change or deterioration: *The stability of the economy encourages investment.*

sta·ble<sup>2</sup>  [stey·buhl]  [Show IPA](#) *Dictionary.com Unabridged*

**adjective, sta·bler, sta·blest.**

1. not likely to fall or give way, as a structure, support, foundation, etc.; firm; steady.
2. able or likely to continue or last; firmly established; enduring or permanent: *a stable government.*
3. resistant to sudden change or deterioration: *A stable economy is the aim of every government.*
4. steadfast; not wavering or changeable, as in character or purpose; dependable.
5. not subject to emotional instability or illness; sane; mentally sound.



# How to Measure?



# Why Should I Care?



# Combinations and Permutations

Protocol	Header Field	Malformed %	
Total Frames		1%	
Ethernet	Destination MAC	0%	
	Source MAC	1%	
	Ethertype	1%	
	CRC	1%	
IP Version 4	Version	1%	
	IHL	1%	
	Type of Service	1%	
	Total Length	1%	
	Identification	1%	
	Flags	1%	
	Fragment Offset	1%	
	Time to Live	1%	
	Protocol	1%	
	Header Checksum	1%	
	Source Address	1%	
	Destination Address	1%	
	Options	1%	
	Padding	1%	
	UDP	Source Port	1%
		Destination Port	1%
Length		1%	
Checksum		1%	
TCP	Source Port	1%	
	Destination Port	1%	
	Sequence Number	1%	
	Acknowledgement Number	1%	
	Data Offset	1%	
	Reserved(3 bit)	1%	
	Flags(9 bit)	1%	
	Window Size	1%	
	Checksum	1%	
	Urgent Pointer	1%	
	Options(Variable Length)	1%	

$$48 + 48 + 16 + 16 + 32 = 160$$

$$4 + 4 + 8 + 16 + 16 + 3 + 13 + 8 + 8 + 16 + 32 + 32 = 160$$

$$16 + 16 + 16 + 16 = 64$$

OR

$$16 + 16 + 32 + 32 + 4 + 3 + 9 + 16 + 16 + 16 = 160$$



# Combinations

$2^{160+160+160} = 2^{480} = 3.121749 \times 10^{144}$  packets

■ On a 10 Gbps link at 15mm PPS

=  $2.08 \times 10^{137}$  seconds

=  $3.46 \times 10^{135}$  minutes

=  $5.78 \times 10^{133}$  hours

=  $2.41 \times 10^{132}$  days

=  $6.59 \times 10^{129}$  years

=  $4.7 \times 10^{119}$  lifetimes of the Universe



# Why Should I Care?



# Combinations and Permutations

Protocol	Header Field	Malformed %	
Total Frames		1%	
Ethernet	Destination MAC	0%	
	Source MAC	1%	
	Ethertype	1%	
	CRC	1%	
IP Version 4	Version	1%	
	IHL	1%	
	Type of Service	1%	
	Total Length	1%	
	Identification	1%	
	Flags	1%	
	Fragment Offset	1%	
	Time to Live	1%	
	Protocol	1%	
	Header Checksum	1%	
	Source Address	1%	
	Destination Address	1%	
	Options	1%	
	Padding	1%	
	UDP	Source Port	1%
		Destination Port	1%
Length		1%	
Checksum		1%	
TCP	Source Port	1%	
	Destination Port	1%	
	Sequence Number	1%	
	Acknowledgement Number	1%	
	Data Offset	1%	
	Reserved(3 bit)	1%	
	Flags(9 bit)	1%	
	Window Size	1%	
	Checksum	1%	
	Urgent Pointer	1%	
	Options(Variable Length)	1%	

$$48 + 48 + 16 + 16 + 32 = 160$$

$$4 + 4 + 8 + 16 + 16 + 3 + 13 + 8 + 8 + 16 + 32 + 32 = 160$$

$$= 96$$

$$16 + 16 + 16 + 16 = 64$$

OR

$$16 + 16 + 32 + 32 + 4 + 3 + 9 + 16 + 16 + 16 = 160$$

$$= 144$$





# Combinations

$$2^{96+144} = 2^{240} = 1.77 \times 10^{72} \text{ packets}$$

- On a 10 Gbps link at 15mm PPS

$$= 1.18 \times 10^{65} \text{ seconds}$$

$$= 1.96 \times 10^{63} \text{ minutes}$$

$$= 3.27 \times 10^{61} \text{ hours}$$

$$= 1.36 \times 10^{60} \text{ days}$$

$$= 3.73 \times 10^{57} \text{ years}$$

$$= 2.66 \times 10^{47} \text{ lifetimes of the Universe}$$



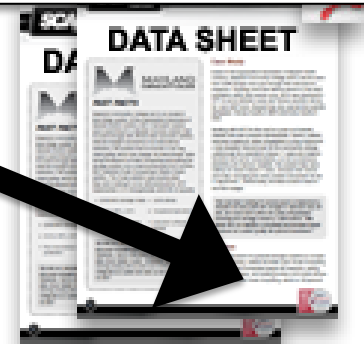
# Resiliency



# Resiliency Testing: A History Lesson

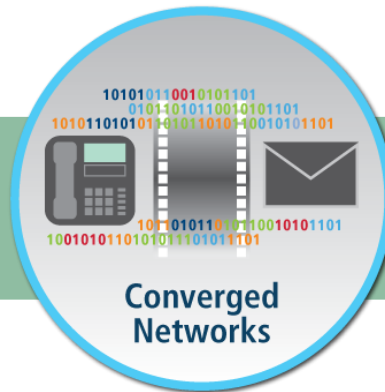
2. Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.

- Internet Growth Leads to Technology Standards
- IETF Testing Standards
  - RFC 1944
  - RFC 2544
  - RFC 3511



# RFC 2544: Right Standard, Wrong Time

- Original Goal
  - Create Vendor-Agnostic Comparisons
- 18 years later (Today)
  - Industry continues to apply RFC 2544 to next-generation and content aware devices



# RFC 3511: False Sense of Security?

- HTTP is NOT an Application

Rank	Upstream		Downstream		Aggregate	
	Application	Share	Application	Share	Application	Share
1	BitTorrent	31.7%	HTTP	19.5%	BitTorrent	20.3%
2	eDonkey	18.2%	YouTube	18.0%	HTTP	17.7%
3	HTTP	11.3%	BitTorrent	17.2%	YouTube	15.3%
4	YouTube	5.2%	eDonkey	7.0%	eDonkey	9.4%
5	Skype	2.5%	Flash Video	5.6%	Flash Video	4.7%
6	SSL	2.5%	RTMP	2.8%	RTMP	2.5%
7	Teredo	2.3%	Facebook	2.5%	Facebook	2.4%
8	Facebook	2.0%	MPEG	2.0%	SSL	1.7%
9	Flash Video	1.3%	iTunes	1.7%	MPEG	1.7%
10	BBC iPlayer	1.3%	SSL	1.5%	iTunes	1.5%
	<b>Top 10</b>	<b>78.3%</b>	<b>Top 10</b>	<b>77.8%</b>	<b>Top 10</b>	<b>77.2%</b>

SOURCE: SANDVINE NETWORK DEMOGRAPHICS



Table 1: Top Peak Period Applications by Bytes - Europe, Fixed Access



# Mobility in Action

## North America Mobile

Rank	Upstream		Downstream		Aggregate	
	Application	Share	Application	Share	Application	Share
1	HTTP	20.52%	YouTube	27.17%	YouTube	24.99%
2	Facebook	20.46%	HTTP	19.90%	HTTP	19.97%
3	SSL	10.66%	Facebook	8.67%	Facebook	10.02%
4	YouTube	8.06%	MPEG Streaming	7.18%	MPEG Streaming	6.58%
5	Skype	2.32%	Pandora Radio	5.40%	SSL	5.49%
6	Google Talk	2.07%	SSL	4.83%	Pandora Radio	5.00%
7	Pandora Radio	1.90%	Google Market	3.51%	Google Market	3.23%
8	MPEG Streaming	1.89%	Netflix	2.24%	Netflix	2.06%
9	Gmail	1.38%	Flash Video	1.74%	Flash Video	1.58%
10	BitTorrent	1.32%	Windows Update	1.68%	Windows Update	1.54%
	<b>Top 10</b>	<b>70.58%</b>	<b>Top 10</b>	<b>82.32%</b>	<b>Top 10</b>	<b>80.46%</b>

SOURCE: SANDVINE NETWORK DEMOGRAPHICS



# Moving Ahead: Evolving Testing Standards

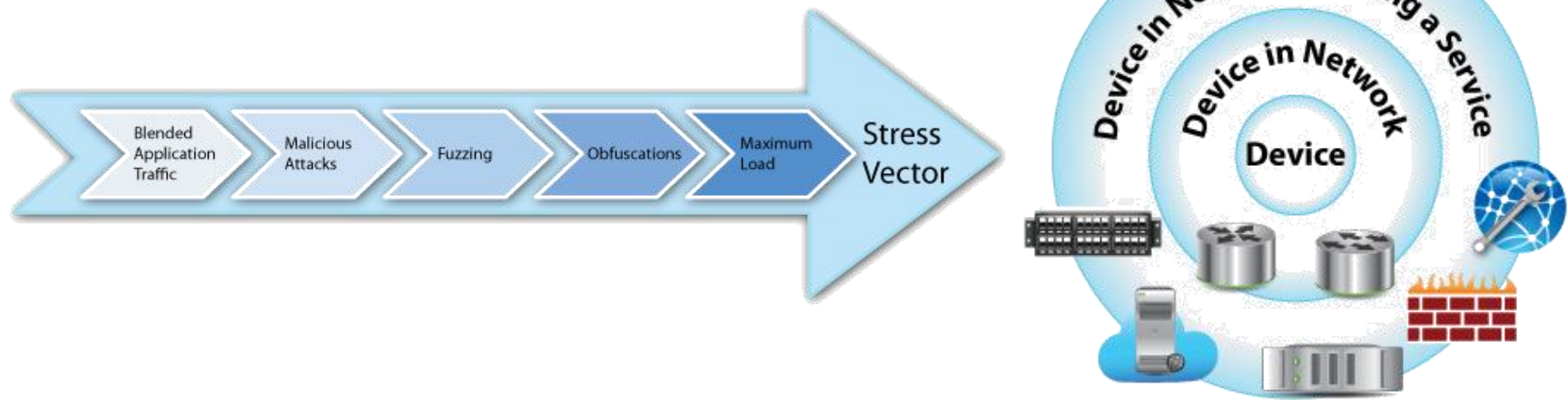
- IETF
  - Benchmarking Working Group
  - Content-aware device methodology
- Industry consortiums
  - DPIbench





# Resiliency = Battle-Tested

- Apply emerging standards today
  - Download the most recent work
- Understand your network traffic
  - Enterprise, service provider, government, etc.





# Apply: Takeaways

- Ask your vendor\*:
  1. Are you keeping up with emerging testing standards?
  2. What application mixes and weights do you use during testing?
  3. Do you combine applications and high-stress user load during testing?
  4. What have the results been when you have tested using malformed traffic?
  5. How does the device perform against application-layer attacks?
  6. Can I test your product with my unique network, application, and user conditions?

\*Vendors, ask yourself the same questions.



# Apply: Final Thoughts

- Read between the lines
- Money matters
- Just because code hasn't been touched doesn't mean it is not the problem
- Never leave a test port idle
- Utilize industry resources



# Questions?

- \$,£,€,¥...£
- Contact information:
  - Mike Hamilton
  - Director of Global Systems Engineering
  - BreakingPoint Systems
  - [mhamilton@breakingpoint.com](mailto:mhamilton@breakingpoint.com)

