IN THIS WEEK'S ISSUE: Proof Of Concept testing means vendors sell bad products; what to do after you screw up; and a parable about a salesperson and an engineer. Please remember to enable the images; the magazine looks a lot better that way!

Table of Contents
(aka The Project Plan)

Issue Number 30

04/26/2016

The "Interop is next week so we better get started on our slide deck" issue.

Thought For The Week:

Act your age and not your shoe size.
- Prince

1. Proof Of Concept Testing Should Never Happen

by Greg Ferro

It's a "best practice" to assume that IT vendor products are faulty, have serious bugs, and will fail in normal operation at any time. Thus, customers are forced to run proof of concept (POC) tests before they can use these products. There's something wrong with an industry that produces unreliable technology and customers that buy it on that basis.

You Need A POC To Prove It Works

- We accept this requirement because we've been told that networking is complex technology and cannot be bug free. (Why not?)
- We've also been told that every customer is unique--even though every customer uses exactly the same products.
- If I am buying top-quality equipment, why should I have to prove it works as advertised before I deploy it?

But POCs Don't Prove Anything

- POCs can test, *at best*, 50% of a real deployment.
- Completing a vendor POC project provides zero guarantees that it will work in real life.
- **There are NO circumstances in which the vendor will accept legal or financial liability for its products in normal operation**.

So why are we told that Proof Of Concept testing is necessary for large projects?

POC Value (For Who?)

A POC test needs large amounts of OpEx to define and execute the testing: typically on the order of 400–800 hours of preparation by the customer to

execute a medium-sized engagement. (This doesn't include travel expenses.)

Do you get any benefits from conducting a POC test?

- Training on product and forced education on technology through actual hands-on work
- Insights into troubleshooting and operating the technology after the deployment
- A reduction of the impact of the learning curve after deployment
- **A (false) sense of confidence that the solution works** since there are no actual vendor guarantees

Now consider just how many benefits the vendor gets out of your POC test: Bug testing, product validation, user feedback, training for their POC engineers, and professional services revenue.

If you're paying a vendor for “high-quality, reliable and market-proven" technology then a POC/Test/Validation should not be required. Caveat: There *are exceptions,* but they should be rare, not the norm.

Vendors have big profit margins, and those profits aren’t put back into reliable, quality products. They are given to shareholders instead of delivering customer value. (Sales is well funded, perhaps to overcome objections to poor-quality products). Vendors have no incentive to produce high-quality products because all responsibility and risk is accepted by the customer.

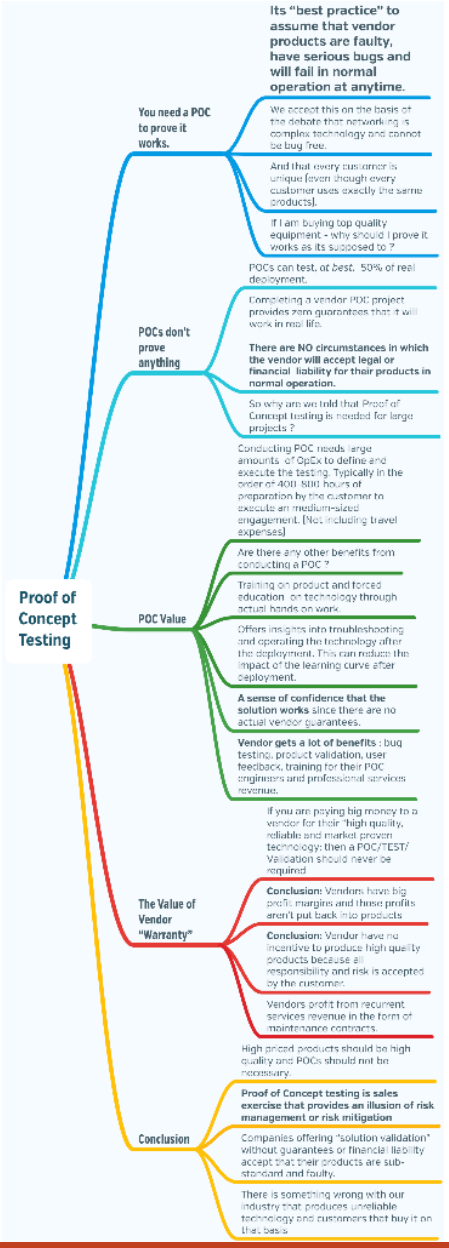
Conclusion

- High-priced products should be high quality, and POCs should be unnecessary in the majority of cases.
- POC testing is a sales exercise that provides the illusion of risk management or risk mitigation.
- Vendors profit from recurrent services revenue in the form of maintenance contracts.
- Vendors profit from creating an environment of fear, uncertainty, and doubt to encourage customers to buy maintenance contracts.
- The same fear drives POC testing because no other option exists.

- Companies offering “solution validation” without guarantees or financial liability accept that their products are sub-standard and faulty.

Somehow, the enterprise IT industry has convinced customers that it's acceptable to buy expensive, unreliable technology, and that the burden of getting it to work is the customer's responsibility. That's wrong.

Post Mind Map - Click for Full Size



Sponsor: Viptela

Eat, Drink, And SD-WAN With The Packet Pushers At Interop!

Come and join the Packet Pushers team for a merry evening of food, drinks, and conversation on Monday May 2nd at the Skyfall Lounge in Mandalay Bay.

You can chat with attendees from the Future of Networking Summit, and meet Greg and Ethan live and in person. And if you've got questions about SD-WAN, network architects from some of the largest SD-WAN deployments in banking, retail, and healthcare will be there to talk shop and share their experiences.

Register here for The Big SD-WAN Mixer with the Packet Pushers!

Skyfall Lounge, which offers amazing views of the Vegas skyline, is located in the Delano Las Vegas (formerly THEhotel) in the Mandalay Bay resort complex. See you there!

2. You Screwed Up, And It Was Bad. What Next?

by Ethan Banks

Let me tell you a story. This one time, I typed “debug ip packet” on a production Cisco 7206VXR router with an NPE-400. If I remember right, the box was a campus WAN gateway with a busy T3 as well as few 100Mbps Ethernet segments. Nearly 3,000 people relied on this router. And even though TAC had told me to do it while troubleshooting a problem, typing “debug ip packet” was an incredibly stupid thing to do.

The 7206 was configured to log all debug events to a remote syslog, as well as the physical serial console. As soon as I entered the debug command, the router bricked. The CPU just couldn’t handle the load. It become unresponsive to remote SSH, lost all routing adjacencies, and IOS died a horrible death. I could smell the smoke from across town, and many green lights went red in our HP OpenView console.

I hastily explained to my boss that I needed to go across town RIGHT NOW, and buzzed over there. After power cycling the 7206, life went back to normal. And then I changed my soiled shorts.

Most network engineers have stories like this. We’ve typed the wrong thing, typed the right thing on the wrong device, unplugged the wrong cable, or bumped a power switch. The question then becomes...how do you deal with this situation? As the engineer, you’re probably the only one who knows what really happened.

1. **Knowing the technical truth is critical to IT operations.** When application delivery is affected because the network is down, preventing that outage in the future is a big deal. Should the system be redesigned? Is there a redundant configuration we could add? If the outage is caused by sausage fingers, the “how to prevent in the future” conversation is very different.

2. **Avoid the instinct to “CYA.”** Yes, you want to cover up. The shame of a screw-up can hit hard for those of us who take pride in our technical chops. That shame might be compounded by fear if we think we could lose our job for the screw-up. Fair enough. But lying about what really happened doesn’t resolve the point above.

   And to the managers out there, a special note: Protect your normally competent staff. One mistake should never put anyone in peril of their job. Foster an atmosphere of technical honesty.

3. **Admit failure factually, not emotionally.** I recommend you come clean with your mistake, but come clean to the right person. You don’t need to fall on your sword in an e-mail addressed to everyone, where you share the sad tale of your sleepless night caring for a teething toddler and the following morning where you left your wallet at the coffee shop, your car got a flat, and you were just so stressed out, you didn’t notice you were on the core switch when you typed “no router ospf 100”.

   Not everyone wants or needs to know the background. Just calmly tell your technical superior what happened so that the outage is analyzed properly. Allow them to disseminate a postmortem to the rest of the team if that’s appropriate. Minimize the drama.

The end of an embarrassing mistake should be that you learn something. What is it you will do to prevent yourself from making a business-impacting screw-up

in the future?

For example, some people will create colored terminal sessions as a visual aid. The red screens are production systems. The green screens are lab systems. Did you trip a power switch accidentally? Put a protective shield over the switch, or gently remind the boss that it's time to fund the RPS project.

Think about what happened, and how you could prevent it next time. Take definitive action if at all possible. Prevention is far better than making the same mistake a second time.

3. The Salesperson And The Engineer: A Parable

by Phil Gervasi

A couple of years ago, one of the top salespeople in our company was sitting across from me. He was working with a major school system interested in a large hardware refresh, including a new wireless and VoIP infrastructure.

To me this was a typical project, with typical hardware, typical licensing, and a typical scope. Needless to say I felt like the expert in the room.

So when the salesperson challenged me about hardware and considerations for deploying QoS policies, I was *offended*.

What did *he* know about QoS? What did *he* know about LAN switching? My solution was simple: buy Catalyst switches of varying platforms and do a huge hardware refresh.

This meant manually configuring custom QoS policies on every device. You see, the Catalyst 4500X wouldn't support auto QoS on the port-channels, so we

needed to do it all by hand.

The salesperson wouldn't buy it, though. He rolled his eyes and said there must be a better way. He mentioned some heathen brand of switch that would deploy policy throughout an entire network with a few mouse clicks.

I was outraged. As a network engineer, I *enjoyed* getting into configs. I didn't care about efficiency. I didn't care about automation. I didn't care about doing it a better way. I knew the CLI, and I knew Cisco. How dare he?

But deep down I knew he was right. Of course it was completely inefficient to configure everything by hand. Imagine how many errors my team and I would have made copying and pasting DSCP maps and AAA configurations over hundreds of switches!

And even if we didn't make many errors, accessing every device by hand would take forever. The conflict I experienced wasn't a matter of logic or reason – it was a matter of comfort level and pride.

It took me several months before I could say out loud that his approach was the way to go. But why? Network engineers generally pride themselves in learning new technology and staying flexible.

I think it was because I'd grown comfortable with a blinking cursor and a humming fan. It was safe, and it was what I knew.

I brought up my dilemma with my father-in-law, who also works in IT. He reminded me that I successfully changed careers in my mid-20s from teaching English to networking, though it took considerable effort.

Was it so difficult to believe that I couldn't change again?

The scales fell from my eyes. I needed to put in the effort to learn a better way to do networking, just like I learned how to do traditional networking 10 years ago. I knew logically that it made so much more sense, but I just needed the switch to flip in my brain.

I still see reluctance among colleagues to accept managing a LAN with

software. Whether it's a lack of skill, or a mindset that resists doing something differently, the switch hasn't flipped for some people.

As a recent convert, I embrace this new paradigm just as I would embrace a better way of doing anything. It's more efficient. It's less prone to error. It just makes sense. And as much as I hate to admit it, the sales person was right.

Research Papers

By Greg Ferro

Network Functions Virtualization: Challenges

and Opportunities for Innovations - AT&T Labs Research

Abstract: Network Functions Virtualization (NFV) was recently proposed to improve the flexibility of network service provisioning and reduce the time to market of new services. By leveraging virtualization technologies and commercial off-the-shelf programmable hardware, such as general purpose servers, storage and switches, NFV decouples the software implementation of network functions from the underlying hardware. As an emerging technology, NFV brings several challenges to network operators, such as the guarantee of network performance for virtual appliances, their dynamic instantiation and migration, and their efficient placement. In this article, we provide a brief overview of NFV, explain its requirements and architectural framework, present several use cases and discuss the challenges and future directions in this burgeoning research area.

LINK

A Systematic Analysis of the Juniper Dual EC Incident

This independent analysis from researchers at four American universities shows that anyone with knowledge could passively decode VPN traffic on a NetScreen firewall.

Abstract: In this work, we report the results of a thorough independent analysis of the ScreenOS randomness subsystem, as well as its interaction with the IKE VPN key establishment protocol. Due to apparent flaws in the code, Juniper's countermeasures against a Dual EC attack are never executed. Moreover, by comparing sequential versions of ScreenOS, we identify a cluster of additional changes that were introduced concurrently with the inclusion of Dual EC in a single 2008 release. Taken as a whole, these changes render the ScreenOS system vulnerable to passive exploitation by an attacker who selects Q. We demonstrate this by installing our own parameters, and showing that it is

possible to passively decrypt a single IKE handshake and its associated VPN traffic in isolation without observing any other network traffic.

LINK

Website-Targeted False Content Injection by Network Operators

ISPs are injecting their own traffic into users' sessions to hijack ads. But malware networks are using the same technique.

Abstract: It is known that some network operators inject false content into users' network traffic. Yet all previous works that investigate this practice focus on edge ISPs (Internet Service Providers), namely, those that provide Internet access to end users. Edge ISPs that inject false content affect their customers only. However, in this work we show that not only edge ISPs may inject false content, but also core network operators. These operators can potentially alter the traffic of all Internet users who visit predetermined websites. We expose this practice by inspecting a large amount of traffic originating from several networks. Our study is based on the observation that the forged traffic is injected in an out-of-band manner: the network operators do not update the network packets in-path, but rather send the forged packets without dropping the legitimate ones. This creates a race between the forged and the legitimate packets as they arrive to the end user. This race can be identified and analyzed. Our analysis shows that the main purpose of content injection is to increase the network operators' revenue by inserting advertisements to websites. Nonetheless, surprisingly, we have also observed numerous cases of injected malicious content. We publish representative samples of the injections to facilitate continued analysis of this practice by the security community.

LINK

Internets Of Interest

A collection of pre-loved links that might interest you. "Pre-loved" because I liked them enough to put into this newsletter. It's not *true* love.

By Greg Ferro and Drew Conry-Murray

With cloud, anything goes, apparently

This article highlights that all possible choices for IT infrastructure architecture are on the table. **It's the smartest piece on cloud I've read in a long time.** Go and read it.

From **CIO.com:** *Is it better to rideshare, take a taxi, or rent, lease, finance, or outright purchase a car? Should it be a convertible, coupe, or sedan? The answer, of course, is "it depends"—on a variety of factors, which vary among customers and over time. Similar variability of deployment models and architectures occurs with the cloud, too. Here are some examples of what leading companies are doing, and their presumed or stated rationales.*

LINK

Who Doesn't Like Lock-In?

This article from Adrian Cockcroft at Battery Ventures is poking the bear that is lock-in. After years of vendor abuse, enterprises have found vendor lock-in to be a toxic business and are searching for ways out. However, every technology decision creates lock-in once any decision is made. The article gives good examples of how to choose the lock-in that suits you best.

From **Battery Ventures:** *Like a marriage, enterprise-IT lock-in—or using only one vendor's product for key functions, such as outsourced cloud computing—is a good thing if managed well for mutual benefit. But like a divorce, it gets ugly*

and expensive when things go wrong.

LINK

Amazon Copies Products

Part of Amazon's corporate strategy is to bring companies onto its platforms. “Amazingly,” Amazon seems to come up with products that copy successful offerings on its own platform, and then compete with its own customers.

This article from Bloomberg "*Got a Hot Seller on Amazon? Prepare for E-Tailer to Make One Too*” suggests that blatant product copying is a regular event.

And same thing applies for AWS, which often copies successful products that use AWS.

LINK

Script to Convert Google Docs to Markdown

I write in Markdown format. It's awesome. This makes it even more awesome. On Github (of course).

From **Mangini:** *A simple Google Apps script to convert a properly formatted Google Drive Document to the markdown (.md) format.*

LINK

Polycom Gets Bought By Mitel

The slow death of IP telephony/voice/collaboration continues. There's been a

lot of discussion recently around “bots” replacing call centers. And then Polycom, which has been rapidly shrinking for a few years now, is merging with Mitel.

From **Polycom:** *The communications and collaboration industry is undergoing a period of intense change that is rapidly redrawing the competitive landscape and breaking down barriers between previously discrete markets and technology domains. Through a series of strategic acquisitions, Mitel has successfully capitalized on changing market dynamics and transformed the company to help customers operate more efficiently and cost effectively. The combination of Mitel and Polycom will create a new industry leader leveraging Mitel’s recognized leadership as a pioneer in global communications with Polycom’s well-known premium brand and industry-leading portfolio in the conference and video collaboration market.*

LINK

Fake O'Reilly Book Cover Generator

O'Reilly technical books have a distinctive style that's immediately recognizable, including the black-and-white image of an animal and the white text on a colored block--not to mention the publisher's uncanny ability to crank out books on the tech craze *du jour*.

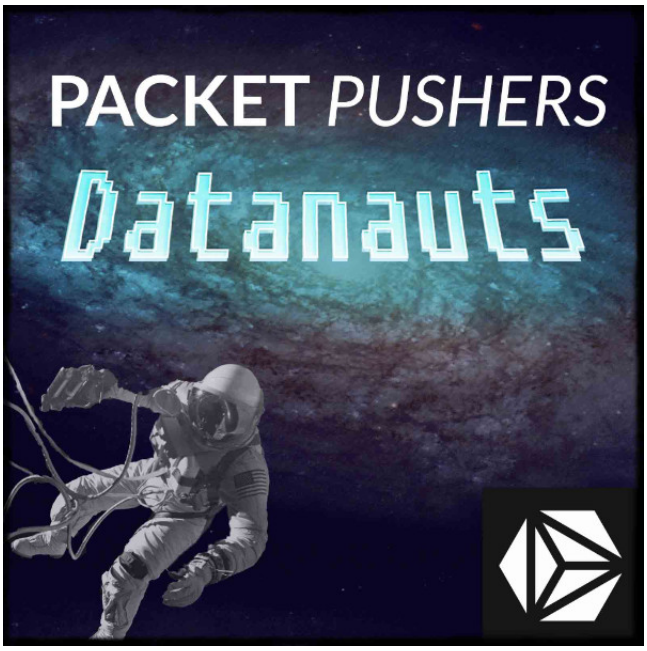
You don't have to actually write a book for O'Reilly to make up your own cover thanks to the 'O RLY Cover Generator,' a Web site that makes it easy to generate your own homage or spoof. Check it out and have some fun.

LINK

PACKET PUSHERS

WEEKLY SHOW

Where Too Much Networking Would ***NEVER*** Be Enough



The Weekly Show channel is our one-hour deep dive on networking technology.

Datanauts Podcast: Build data centers and bust silos with Chris Wahl and Ethan Banks.

Product News

We don't often get new products worth talking about, so that makes it nice to have something to say.

Badu Networks

Badu is a startup that performs one-sided, in-line TCP optimization and claims to deliver strong benefits on Wi-Fi uplinks specifically, or other deep-buffered "last mile" networks.

From **Badu Networks:** *WarpTCP™ augments these data points by incorporating additional meta-data that allows it to further distinguish packet loss from actual congestion. Because WarpTCP™ reacts to network events in real-time and attempts to discern real congestion from loss, the technology is better able to optimize flows over typically lossy networks. Such networks are*

prevalent in the “wireless last hop or mobile last mile”.

LINK

A10 Networks Goes Bare Metal

From **A10 Networks:** *The new, high-capacity Bare Metal ADC takes a non-virtualized approach for greater agility, deployment efficiency and cost savings. Without intervening hypervisors, the Bare Metal ADC can deliver a throughput of up to 40 Gbps of L7 traffic processing. The release of Thunder ADC is representative of the current ADC market shift toward software-based solutions for greater flexibility, efficiency and cost savings.*

LINK

Midokura Goes To Version 5.0

This startup revs its SDN platform for OpenStack again. New features focus on analytics, visibility, and service chaining.

LINK

Endace Beefs Up Its Hardware

If you are into packet recorders for high-level security response, then Endace will be familiar. The company updated its hardware to hold more data.

LINK

Recent Articles

The last five articles published on EtherealMind and Packet Pushers

EtherealMind.com Latest

Logical Razors Can Take on Corporate Babble

Canned Response to BGP Networking Questions – Reddit

IETF RFC 8374 BGPsec Design Choices and Summary of Supporting Discussions

Net Neutrality Hasn't Ended, We Don't Know When

Next Market Transition ? Cheaper Buying, Less Selling

PacketPushers.net - The Last Five

Network Break 182: BGP Hijacked For Cryptocurrency Heist; Juniper, Big Switch Unveil New Products

Show 387: AWS Networking – A View From The Inside

PQ 147: Connecting Security And GDPR Compliance (Sponsored)

Datanauts 131: Masters And Mentorship

Network Break 181: Russia Accused Of Infrastructure Attacks; US Targets ZTE

Watch This!

Where we collect some videos that make us reflect, think about our inner lives, or just entertain us.

Mother's Day, Father's Day, or any time of year: Why not send bacon roses?

PACKET PUSHERS

Link Propagation Newsletter

Our weekly newsletter delivering essential headlines, announcements, and useful news to your inbox

Can't get enough newsletters? Check out Link Propagation, our newest publication. We send you a free weekly digest with tech news, interesting blogs, and industry announcements, all curated by the Packet Pushers. It's an easy way to keep up and stay informed. Subscribe at packetpushers.net/link-propagation.

Quick Poll: Single Panes Of Glass

On average, how many different "single pane of glass" network management systems do you interact with in a week?
Duh. Just 1. It's a single pane of glass
2–3
4–5
6 or more
Single pane of glass is a myth!

Did We Miss Something?

Got a link or an article to share? Email it to humaninfrastructure@packetpushers.net

The End Bit

Sponsorship and Advertising - Send an email to humaninfrastructure@packetpushers.net for more information. You could reach 5,013 people.

Human Infrastructure is bi-weekly newsletter with view, perspectives, and opinions. It is edited and published by Greg Ferro and Drew Conry-Murray from PacketPushers.net. If you'd like to contribute, email Drew at drew.conrymurray@packetpushers.net.

We don't give away your email address or personal details because that would suck.