IN THIS WEEK'S ISSUE: Cloud, GitHub, social media, CCIE limits, and more. And make sure you enable the images; the magazine looks a whole lot better that way!

ETHEREALMIND
Human Infrastructure Magazine
A Packet Pushers Newsletter on Life in Networking

Table of Contents
(aka The Project Plan)

Issue Number 19

11/25/2015

The "Can't Think of Anything Smart To Say" Edition

Thought For The Week:
Doing fewer things probably gets more things done.

[This channel](#) has our nerdiest shows on data networking technologies and products.

[Network Break is a weekly podcast](#) that delivers news & analysis on the networking industry in a fun, fast-paced style.

What Do Cloud, Health Care & Fast Food Have In Common?

by Greg Ferro

Lots of people complain that health care doesn't deliver a product that suits their own situation. Regardless of your country's health care system, this complaint is universal across the first word, where universal healthcare actually exists.

This problem isn't unique to health care; it's the problem of operating a large-scale, multidisciplinary, resource-intensive business model. Lets consider two other large-scale business models, Public Clouds and Fast Food.

> *I'm going to resist the urge to highlight how lucky you are to have a health care system that you can access.*

Public Clouds

Public Cloud products are never exactly what you need.

- Public Clouds offer a strictly limited set of products/services
- You have limited methods of payment [1]:
- You have limited ways of accessing the services
- Customization is limited to a narrow set of options

Cloud providers do not customize their services and their processes do not change just to "help you out." You either take or leave what they offer.

Fast Food

Consider any large-scale fast food business such as McDonald's or Starbucks.

- You can have only the food on the menu
- No serving options (wrapped in cheap grease-proof paper)
- You have limited methods of payment [1]
- Customization is limited to a narrow set of options

Large-Scale Business Models

All three of these businesses are **Large Scale, High Volume, Low Margin** models. The result is always the same:

- Strictly limited product choices
- Low or zero customization
- Limited payment options
- Low levels of customer service

None of these things are inherently bad for you as a customer. In fact, it is the customer that most often has delusions about the level of service they'll get. You won't get your choice of doctor in a hospital because 24-hour care can't be delivered by just one person. You can't get your favorite ketchup on your burger, they simply don't have it. You can't have a public cloud that operates exactly the way you want.

---

1. You can't pay on account or by company check. ↵

GitHub: Why Network Engineers Should Care
by Russ White

GitHub is the center of the open source world. It's a Web-based repository and change-tracking system for source code, and it houses a variety of open source projects.

I can already hear you saying, "I didn't sign up to be a coder! Just let me configure things, I don't want to worry about this stuff!"

To paraphrase an old saying, you might not be interested in coding, but it's certainly interested in you. From DevOps to programmable networking, the ability to create, manage, and use repositories of code is going to be a crucial networking skill in just a few years.

And the networking industry isn't walled off from the open source world. All kinds of interesting projects are afoot.

For instance, most of the YANG models being developed for routing are contained in a repository called YangModels, which can be found at https://github.com/YangModels/yang.

Quagga, a full open source routing stack that runs on many versions of Linux and OpenWRT, can be [found here](#) (for more information on Quagga check out [Open Source Routing](#)). OpenWRT, by the way, is an operating system that can be run on most small home routers.

Why is any of this important? If you really want to understand how BGP performs the bestpath calculation, you can look it up in a book, or you can look at an implementation.

While Quagga isn't the only source (each vendor has its own source), it's a good place to start. The BGP bestpath implementation in Quagga can be found in the function bgp_info_cmp in bgp_route.c.

Where do you begin with all that's available on GitHub? It just so happens the site has worked with Wheelhouse to provide free online GitHub training for "a limited time."

The training is hands-on; you'll create repositories, issues, branches, and merging branches. You'll install a local copy of Git. (I keep a local synchronized copy of Quagga on my laptop for quick reference using Git). You'll edit files, commit changes, and all the rest. It's all covered using a very simple project through this tutorial.

If you're a GitHub beginner, [this free training](#) is hard to beat.

Sponsor: Riverbed

also delivers the unique ability to instantly provision new services, and entirely new branches, as well as recover from remote outages, all from the central data center. Learn more at riverbed.com.

Places The CCIE Can't Take Me
by Ethan Banks

I've been a CCIE since 2008, maintaining my active status via a recertification cycle that comes around every 2 years. While the CCIE certification undoubtedly changed my life, there are places the CCIE program can't take me now.

The CCIE program, much like other certification systems, is limited by being vendor-specific. It's a Cisco program, no matter what general networking skills you might gain.

The CCIE is also silo-specific. It goes deep on networking...and that's it. It doesn't teach you how to stand up all of the silos in a data center and deliver business applications. You learn how to provision infrastructure with the CCIE program -- how to twist the nerd knobs. Yes, there's crossover into storage and collaboration, but what I think needs to be learned is how to be an application

delivery engineer.

The term I've heard applied to this brave new IT staffer is the "full-stack engineer" - someone who understands infrastructure, applications, a bit about development, and lot about automation and orchestration systems that deliver applications.

To the full-stack engineer, developers are not the enemy, but rather consumers of infrastructure you work with closely as applications are created and deployed.

Neither the CCIE nor any other certification program can make you a full-stack engineer. Might they help? Yes. Certification programs can teach you about a technology and perhaps enable basic competence in a silo.

But full-stack engineering is a complex, interdependent set of disciplines that's not only about skills. It's also about understanding IT as a system -- about seeing the forest for the trees.

Is this approach being taught anywhere, even in our college and university computer science programs? I'm not sure. The best teaching I'm aware of right now might just be from the community.

Sponsor: Viptela

Viptela's hybrid SD-WAN technology unifies your MPLS, Leased Line, and Internet-based WAN infrastructure. It's packaged with centralized administration, real-time visibility, and policy control for precise and measurable application performance. A Viptela SD-WAN lets you build flexible, multi-segmented topologies. Your branch sites can have guest WiFi, video collaboration, PCI, and so on, with each application on different segments, and possibly with a different topology for each. Viptela is already deployed at thousands of sites across more than fifteen Fortune 500 companies in retail, healthcare, and more. Get more details at Viptela.com.

How Social Networking Enhances My Technical Skills

by Lee Badman

In the early days of social media, I was a skeptic that it had any value as a professional tool. I got onto Facebook so I could see what my kids were up to (me and Mom had to be their Facebook friends or they weren't allowed to have accounts), and I still keep Facebook reserved for family interactions.

Twitter hit my radar when a coworker opened a Pandora's Box by letting our network clients tweet their complaints instead of opening trouble tickets.

It started as a procedural mess, and I was fairly disgusted that users were grousing about network trouble at 2 a.m. behind bogus names—but I learned quickly that this wasn't going away.

We successfully figured out how to use Twitter to augment the helpdesk, and then I had an epiphany: There are some really smart people sharing a lot of good information on the likes of Twitter and LinkedIn.

The more I looked, the deeper the hook was set. Within a few months, I was regularly interacting with hundreds of IT types that I'd normally have to hope to meet up with at conferences.

I've discussed network problems and solutions, gotten wind of new tools and vendors, and have learned to do a little bit of people-networking every day. I've gotten job offers and writing gigs over social media. Most importantly, I've expanded my circle of friends and like-minded professionals.

Corny as it may sound, social media has made me a better networker, both personally and professionally.

Technology, Terrorism & Surveillance
By Drew Conry-Murray

In response to the recent terrorist attacks in Paris, law enforcement, intelligence agencies, and politicians in the United States are condemning the use of end-to-end encryption, and some are calling for the creation of back doors that would give government agencies access to encrypted communications.

I've been trying to reconcile my objections to government surveillance capabilities (above and beyond what are already in place) against the terrible loss of life in Paris, Beirut, and most recently Mali.

While I don't want to hamper efforts to track terrorist activities and thwart

attacks, I don't think outlawing or weakening encrypted communications would materially improve our intelligence capabilities. Here's why.

First, back doors create vulnerabilities that can be exploited by others, including criminals and spies. And while the government might pledge to implement protections for a master key, it doesn't have a great record on security.

Whatever you think of Edward Snowden, he demonstrated that even the NSA is susceptible to breaches. And then there's the Office of Personnel Management hack, in which over 21.5 million records of government officials, including Social Security numbers and fingerprints, were stolen.

Introducing back doors would expose commercial and personal information to even greater risks.

Second, even if corporations and developers were forced to implement back doors under the penalty of U.S. law, or stop using encryption altogether, that wouldn't prevent developers or organizations outside the reach of the United States from creating encrypted apps and software. Terrorist and criminal organizations could still get access to encryption tools.

Third, back doors could be misused by intelligence agencies and law enforcement to target political enemies or harass citizens.

In addition, as we learn more about the the Paris attacks, there's growing evidence that encrypted communications played [very little role in their planning and execution](#).

Intelligence agencies bear the blame when terrorists launch successful attacks, so I understand why they want as many tools at their disposal as possible to find and disrupt plots. But crippling or banning the use of commercial encryption imposes unwarranted risks, including to personal liberties, without making us safer. It's not an effective or worthwhile strategy.

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.

Are Successful CEOs Just Lucky?

TLDR: Yes.

It turns out the CEOs are no different in terms of talent or intelligence from other professionals or business executives -- they just got lucky in the selection lottery.

From the **Harvard Business Review**:

"It's safe to say that CEOs are, overall, a talented bunch, but that's not what separates them from other professionals, nor is it the main reason their firms succeed or fail. Certainly it doesn't come close to explaining why they're so well paid. Put another way, CEOs matter, just less than many people think. Instead, luck, and yes, bias, play a far larger role in determining who ends up leading companies, and whether they are fired or end up industry leaders."

Don't put your CEO on a pedestal. They are ordinary people doing a job. Nor should your CEO act like they have super-powers because they don't.

LINK

A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps

From the paper **Who Knows What About Me?**

"*73% of Android apps shared personal information such as email address with third parties, and 47% of iOS apps shared geo-coordinates and other location data with third parties*"

and

"*We show that a significant proportion of apps share data from user inputs such as personal information or search terms with third parties without Android or iOS requiring a notification to the user*"

Congratulations, network professionals. Look what we helped to achieve.

LINK

The $24 Billion Data Business That Telcos Don't Want To Talk About

Carriers are building vast lakes of data about the traffic that crosses their networks and then selling that data to marketers.

From **Advertising Age**:

"*...marketers and agencies are testing never-before-available data from cellphone carriers that connects device location and other information with telcos' real-world files on subscribers. Some services offer real-time heat maps showing the neighborhoods where store visitors go home at night, lists the sites they visited on mobile browsers recently and more.*"

LINK

APNIC: IP anycast and managed DNS

From the **APNIC Blog**:

"*Here at APNIC, we use both IP anycast and managed DNS, and this article will outline how we do it.*"

LINK

BROCADE enables world's first 100 Gbps Trans-Pacific Research & Education Network

From **Brocade Networks**:

"*Brocade today announced that Corporation for Education Network Initiatives in California (CENIC) has selected Brocade network solutions in the world's first 100-Gigabit per second (Gbps) Research and Education (R&E) network link between Asia and the United States, as a part of Pacific Wave.*"

[LINK](#)

LINUX 101: Get The Most Out Of Systemd

From **LinuxVoice**:

"*Why do this?*

- *Understand the big changes in modern distros.*
- *See how Systemd replaces SysVinit.*
- *Get to grips with units and the new journal.*"

[LINK](#)

Wireshark 2.0 Is OUT!

When doing packet capture, you are using free and open source software in 2015. For which I am always thankful, since in 1995 I was using a packet sniffer that cost over $50,000 for a single physical unit. (It was [Dolch](#) hardware running Network General Sniffer).

[LINK](#)

RPC Protocol For Device Communication

This uses a bi-direction push/pull model over HTTP2. Google is backing this protocol through the OpenConfig initiative and it's likely that this will replace

SNMP for device operations and management.

Sponsor: Sonus Networks

[Sonus Networks](#) wants you to know that there is a better way to address business continuity with less cost, more flexibility, and increased management efficiency – a Software-Defined WAN (SD-WAN) powered by Sonus' NaaS IQ. Ensure you know the differences between SD-WAN business connectivity and SD-WAN business continuity; visit [Sonus online](#) or reach them at 1-855-GO-SONUS and tell them you heard about them on PacketPushers.

Research Papers

Research and deep technology papers that provide deep insight or expertise.

Exploiting Web Analytics to Ensnare Victims

A PDF whitepaper from FireEye about "malicious actors" (hackers) using Web analytics and persistent Web tracking (EverCookies) to track your users as they move around the Internet. This data is then mined with analytics and machine intelligence for spearphishing attacks that are targeted at your networks and

users.

Greg says: Although the company (FireEye/Mandiant) is known for big and aggressive media stunts (like many IT security companies), this paper is a valuable read on the technology that profiles users after compromising well-known websites. That said, they still named the research project "WITCHCOVEN" like they want to pretend they are the NSA or something. Childish.

MPLS Under the Microscope: Revealing Actual Transit Path Diversity

Lots of people talk about MPLS like it is the only network technology that matters. Strasbourg University did a study into the complexity of MPLS deployments in certain telco networks to find that most have very simple deployments. The majority don't even run MPLS-TE, instead preferring to use path ECMP for performance/resilience.

Greg says: There are very, very few complex networks in the world and MPLS is complex, costly to buy, and costly to operate. That's why most companies deploy the simplest possible MPLS architecture - it simply isn't practical to operate it.

Conclusion:

- Most operators seem to deploy MPLS
- Usage depends on operator
    - Basic most of the time (Mono-LSP or ECMP)
    - Traffic engineering less common but well represented in some ASes
- In case of ECMP, the parallel links architecture seems predominant
- When TE is deployed, in many cases, different LSPs between the same endpoints take the same IP path
    - Bandwidth sufficiently abundant for allowing all LSPs on the same route

Intent-Based Nemo Problem Statement - draft-hares-ibnemo-overview-00

As IP networks grow more complicated, these networks require a new interaction mechanism between customers and their networks based on intent rather than detailed specifics. An intent-based protocol language is need to enable customers to easily describe their diverse intents for network connectivity to the network management systems. This document describes the problem Intent-Based Network Modeling (IB-Nemo) language is trying to solve, a summary of the use cases that demonstrate this problem, and a proposed scope of work. Part of the scope is the validation of the language as a minimal subset.

Greg says: I'm still struggling to accept that intent/promise concepts of network abstraction will work in real life. While I understand that loose abstractions scale for operating systems and applications, the lack of precision in defining network state seems to foolhardy. Networks are simple when reduced to their minimum condition of flow states in endpoints. Smarter people than me are committing vast resources, but I've also seen lots of smart people repeatedly do dumb things over the last two decades.

What do you think ? Answers on a postcard

Automated Certificate Management (ACME)

This is simply wonderful. As someone who wasted a significant part of his life managing root certs on hardware devices with pointlessly complex CLIs, this offers a ray of light that I will do something more meaningful during my work day.

Getting a certificate with ACME

1. Make an account

2. Prove that you own a domain
   3. Issue a certificate for that domain

This is the same process that I have used to validate my domains for Google Analytics/Webmaster and is widely used elsewhere on the Internet. The arcane process of using Certificate Signing Requests has become such an enormous operational risk that this is long overdue.

I can already hear the howls of pain from so-called "security experts" already that certificate issuance is a major security threat.

Note: For the video link below, the presenter wasn't able to attend. Randy Bush delivered the session instead, and it's effectively unwatchable. Mr Bush inserts pointless commentary and snark that detracts from the content.

[LINK to PDF](#)
[LINK to Video](#)
[LINK to Working Group](#)

Product News

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

Cisco IOS-XR Version 6.0

Lots of fuss was made of IOS-XR Version 6.0 without much information to explain why. This is the only document I could find that actually explained why we might care.

   1. Boots from an IOS - should improve installation and operation
   2. Streaming Telemetry - we are moving into a post-SNMP world
   3. Support for new APIs based on JSON/REST
   4. Modular software - hopefully Cisco has gotten better at this. The last fifteen years of modular software haven't gone well

5. Third-party software support - this isn't new as Cisco has been promoting this feature for three or four years. But sometime in the next year or so when IOS-XR Version 6.0 ships to customers after passing early adoption, you will get a chance to see how it actually works

So far, this release is only supported on some of Cisco's most expensive platforms (NCS5xxx) so not much of a change for most customers.

LINK

Next Evolution of VCE Vblock with Cisco ACI

From **Cisco Systems**:

"Cisco and VCE today announced the next evolution of the Vblock® System with Cisco Application Centric Infrastructure (ACI) to make it easier and faster for customers to build flexible, highly secure data centers that can rapidly adapt to changing application and business requirements."

Many people would find it surprising that VCE has taken on Cisco ACI given the competitive factors, but it's good for customers to have the choice, especially those that are more aligned to Cisco than EMC.

LINK

Q&A

People send me questions. I do my best to answer them.

Question: A quick question about a routed port on a Cisco L3 switch:
I wanted to verify that VTP and STP traffic would not cross a port configured as a routed port. I didn't think it would/could cross the layer 3 boundary, but wanted to double check.

Answer: By default, a routed/L3 physical port will not generate BPDUs or make VTP announcements. Those software threads in the operating have not been

invoked on the interface.

If you use an SVI it might (depending on code vendor/version/platform). This makes it easy to get confused.

Recent Articles
The last five articles published on EtherealMind and Packet Pushers

EtherealMind.com Latest

Logical Razors Can Take on Corporate Babble - Link
Canned Response to BGP Networking Questions – Reddit - Link
IETF RFC 8374 BGPsec Design Choices and Summary of Supporting Discussions - Link
Net Neutrality Hasn't Ended, We Don't Know When - Link
Next Market Transition ? Cheaper Buying, Less Selling - Link

PacketPushers.net - The Last Five

Network Break 182: BGP Hijacked For Cryptocurrency Heist; Juniper, Big Switch Unveil New Products - Link
Show 387: AWS Networking – A View From The Inside - Link
PQ 147: Connecting Security And GDPR Compliance (Sponsored) - Link
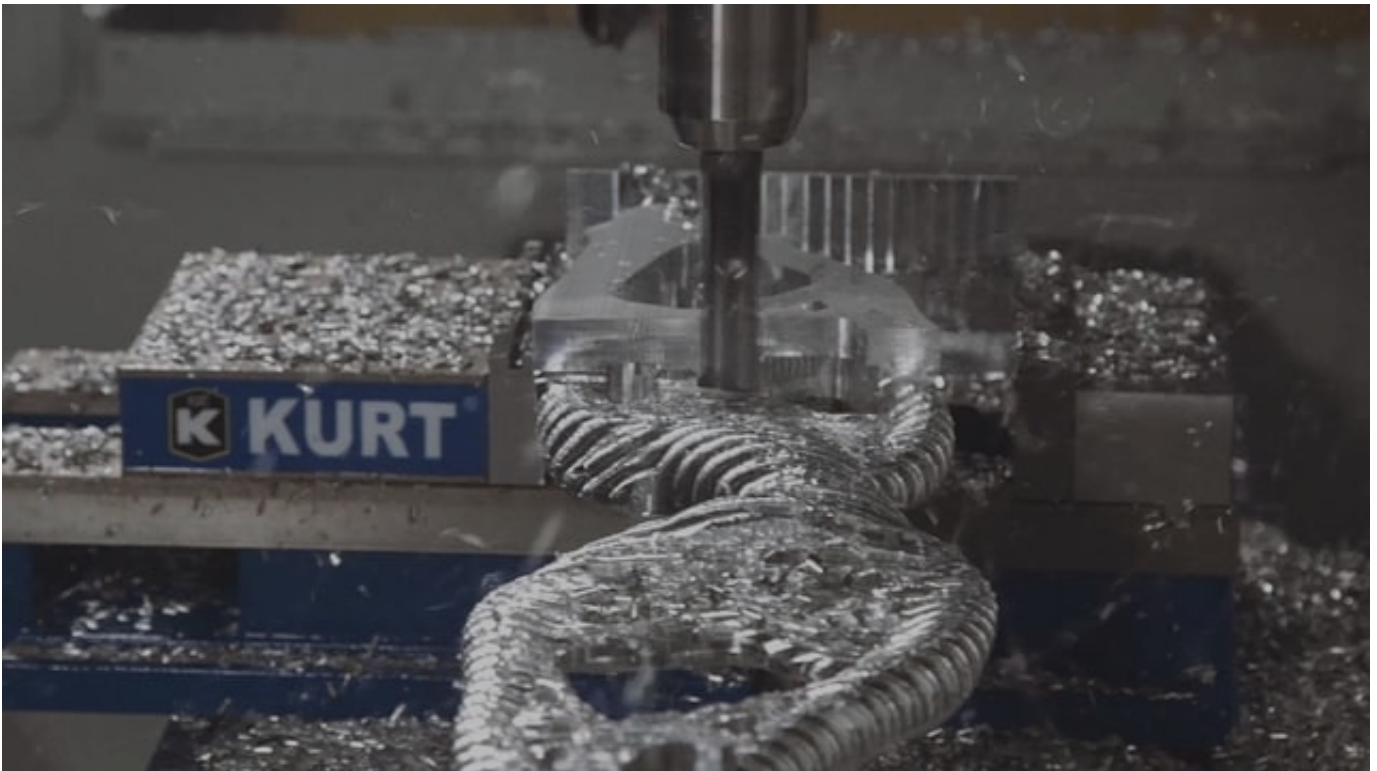Datanauts 131: Masters And Mentorship - Link
Network Break 181: Russia Accused Of Infrastructure Attacks; US Targets ZTE - Link

Watch This!

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

Slow-motion video of a fire tornado a couple of guys made for Youtube fun.

The Optimal - An Olympic Recurve Bow Created with Generative Design.

A software program generated the final shape of the device to meet the designer's criteria. Machine-designed hardware?

Hail Robot Overlords!

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](#).

The End Bit