Human Infrastructure is a magazine-style newsletter from Packet Pusher with News, Views and Opinions on being a human in IT Infrastructure. Hit the signup page to subscribe and join 5,013 subscribers.

View this email in your browser

ETHEREALMIND

Human Infrastructure Magazine

A Newsletter on a Life in Networking

Issue Number 13

08/10/2015

The Making Websites Is Hard Edition

Thought For The Week:

It's six am. Just tell me those 3 words I am dying to hear: "The meeting's cancelled."

This Week: Packet Pushers Next Generation

I've been head down on the long overdue migration of **PacketPushers.net** migration to a new platform for quite some time. At last, it has reached the Internet and I can get back to writing and research.

The Packet Pushers website has a totally new look, colour scheme, logos and fonts. Go and look, revel in the glory of a web page that doesn't have popups, minimal analytics, simple banner ads and clean modern look.

The Hurting

Managing a website is relatively simple but time consuming work. And time is what Ethan & I don't have. We want to spend our time researching, writing and speaking to vendors & clients. So we moved our website onto a platform managed and operated by a company that is dedicated to Wordpress hosting. The good news - security, updates, CDN, performance and space are all managed items.

The bad news ? Someone else does all the custom configuration work via a helpdesk. Their helpdesk was pretty good but work was always done at a pace that suited them, when it was explained to them in terms that they could understand.

Which is the problem with technical support everywhere.

RSS Feeds and iTunes

It would have been fine if we were just pushing web content but Packet Pushers is mostly about podcasts. The new platform changes the way we publish podcasts so all of the RSS feeds for the podcasts had to change.

While I was preparing the testing plan I discovered that Packet Pushers already has

more 40 RSS URLs that we have collected over the last five years. And all of them needed 301 redirection so that your favourite podcatcher would continue to work. Painful.

Anyway, hope you like the new website and on with this Issue of Human Infrastructure.

Subception: Why Is Network Monitoring Done Badly ? Because Moral Hazards and Crumple Zones.

Software Defined Networking & self-driving cars are closely related because they are automated systems. When automated systems go wrong who takes responsibility ?

Declarative and Imperative Confusion

Networks operate in declarative mode. We configure policy (declare) into our various devices and then let the automated systems do the rest. This “hands off” approach is quite different from the imperative model used elsewhere in IT of “do exactly this and nothing else”. I wonder if this basic difference is why network technology is poorly understood by others. And the reverse direction is also true.

More importantly, this gap leads to Moral Hazard around network monitoring. An an industry, networking does monitoring badly.

Moral Hazard and Network Monitoring

The most pervasive problem with network management is that operators don’t install tools to validate the integrity of the network.

Running an autonomous data network is a calculated risk. The automation systems of BGP, OSPF, STP, TRILL are highly unreliable. Eventually consistent, prove to loops, detection of state changes is poor etc, etc. Each protocol has a specific purpose and a network must run multiple autonomous systems to provide a complete solution. The interoperation of each autonomous system requires deep expertise to consider the impact

Why ? Partly because they are based on assumptions made 30 years ago and partly because building distributed autonomous systems is very hard. Computer science has advanced to make distributed systems easier with new languages and programming models but networking has been slow, incredibly slow, to adopt new technology preferring to rely on “proven reliable” protocols developed in a different era.

With imperative mode systems, monitoring and operations is somewhat simpler. Because each configuration is explicitly defined or deliberately executed then the system is in a known (or better known) state. Thus configuring operating systems and storage arrays requires less monitoring. With declarative mode systems, we enter the realm of moral hazard.

> Moral hazard occurs when one person takes more risks because someone else bears the burden of those risks. **Moral hazard - Wikipedia**

The most common form of moral hazard is in car insurance. Drivers without insurance drive much more carefully and have less accidents than drivers with insurance. The very act of insurance means that majority of the impact of an accident is transferred to insurance company who will pay for damage to your car and any third party. Its proven that car insurance increasing driving accidents and this creates adverse outcomes.

There are two parts to moral hazard - transfer of risk & adverse outcomes. The end-to-end reliability of networking is known to be poor therefore implementing redundancy is normal and most often mandatory. Indeed, redundancy is so common that the cost is rarely considered. The result is that we transferred the risk of failure to our autonomous protocols.

So now we rely on these protocols to repair and sustain the connectivity of devices - risk is transferred. The adverse impact is that we focus all our efforts on design and protocols to sustain that redundancy.

And thats why, I believe, we don’t monitor those networks. We have spent our efforts, money and time on implementing redundancy and building the illusion of imperative control.

Compounding Adverse Effects

As a side note, we further compound the adverse effects through the use of command line. In one sense, the use of the command line give our human minds an illusion of imperative control when configuring our declarative protocols and devices. This illusion is a false sense of control, experienced engineers know that an network is, at best, partially controlled. That is, you can only hope that things work as expected but there are zero assurances.

Moral Crumple Zones

The network is often blamed when there is no obvious problem elsewhere in the system or infrastructure and the lack of networking monitoring means that refutation is impractical.

It also doesn’t help that most IT professional are versed in imperative systems that “do exactly as I say and no more” do not comprehend

declarative systems. This builds misguided perception is that a complex, autonomous system is highly likely to fail.

But the most adverse effects of redundancy is there are insufficient tools deployed to provide notification of deviation, damage or defect. Instead, network operations must evaluate the autonomous systems to check their status and integrity using the crudest possible tools - literally, connecting to the command line of each device and executing dozens of complex commands to divine the reason for failure using highly detailed knowledge of

In short, we do not have the ability to immediate confirm whether the network is at fault and network engineers become__ "moral crumple zones"__. Any failure in the network is pointed to the engineer who take personal liability for the network instead of getting to the real cause. The most common causes of network failures are beyond the control of the engineer - vendor software bugs are common, hardware failures, power outages, WAN networks, faulty cables in the data centre, variable bandwidth consumption, dynamic endpoints are just some of uncontrolled factors in networking.

> Yet even while the plane is being run by software, the pilots in the cockpit are legally responsible for its operation. US Federal Aviation Administration (FAA) regulations specify this directly, and courts have consistently upheld it. So when something goes wrong, we observe pilots becoming "moral crumple zones"—largely totemic humans whose central role becomes soaking up fault, even if they had only partial control of the system.
>
> **When your self-driving car crashes, you could still be the one who gets sued - Quartz**

Most IT execs and CIOs are highly critical of their networks.

> 75 % of CIOs stated that the network is an issue that impacts their organizations ability to achieve its business goals. For almost a quarter, it is a 'significant' issue.
>
> **Brocade - press-releases**

Network Monitoring, Automation and Orchestration

The rise of Software Defined Networking(SDN) and its close companion Network Functions Virtualization(NFV) are changing the landscape for network operations and design. The primary change is that we see network devices as *software* instead of treating each network element as precious node of highly customised functionality. This software focus has renewed customer demand that network devices must be managed by software.

Software network nodes can be disposable, fungible, elastic, replaceable. SDN means using automation tools to control devices and perform path management. In NFV, running network nodes in VMs mean that they can stopped, started, rolled back and upgrading with close to zero risk. These tools work for hardware devices too and vendors are racing to "software enable" their hardware products to avoid being left behind.

The current generation of technology around Network Monitoring is genuinely bad. The best software standards for data interchange today are SNMP, Syslog, SSH. Vendors often use "screen scraping" of vendor consoles to get better data for the management platforms.

And I'm tired of being the "moral crumple zone" whenever someone wants to blame my network. When we say "Its Not The Network" we must have the tools to easily **prove it**. The Mean Time to Resolution to the age old question "Is The Network OK?" must be automated.

Drew-Conry Murray **Contributor**

Drew: A Bunch of Links

This week I've got a bunch of links that took my fancy in the last month or so.

Microservices Trade-Offs

Martin Fowler writes an extensive post on the pros and cons of microservices and monolithic software architectures. Not only does he clearly and concisely describe the technical issues with both these design options, he accounts for human elements as well, including developer team dynamics and degrees of skill. Rather than pick a side and plant a flag, he advocates for sensible development using whatever methods and tools make sense.

http://martinfowler.com/articles/microservice-trade-offs.html

The Big Flowering Thing

Matt Oswalt is a network software engineer working at the cutting edge of network programmability. His most recent blog is a bit of a rant about the number of big ideas being foisted on the networking and IT industries (think SDN)—except the focus is on vendor initiatives or 'thought leadership' rather than actually helping customers. Vendor marketing and the tech press also come in for some scolding for being cheerleaders of buzzwords and hype.

By contrast, Matt wants to see more effort dedicated to 'quick wins and useful tooling.' He cites the etc project, a key-value store, as an example. It's a good read.

http://keepingitclassless.net/2015/07/big-flowering-thing/

Hybrid Cloud, Bimodal IT? Buzzwords Reflect New Ways of Building Services

I recently saw a stream of tweets about 'Bimodal IT' and I thought 'Great, another development to keep track of.' Kurt Marko's post on the definition of bimodal IT (traditional stable enterprise applications on one side, agile and iterative applications on the other) provides a clear overview and puts the

buzzword in context of the 'old vs. new' dichotomy that IT has always struggled with. What's different here is the pace: cloud services, mobility, and new app dev frameworks accelerate the rate at which new applications can be deployed. One of the tricks is how to transition iterative, fail-fast apps to the more stable enterprise core.

http://markoinsights.com/2015/06/16/bimodal-it/

Just As FBI Looks To Undermine Encryption, Federal Government Searches For Better Encryption

This TechDirt blog points up the contradictions at work in the U.S. government around encryption, with FBI chief James Comey arguing about the risks of encryption to law enforcement, while the National Institute of Standards and Technology (NIST) is stepping up efforts to bolster authentication and encryption of email. The blog is very much pro-privacy and for strong encryption.

https://www.techdirt.com/articles/20150709/07024131599/just-as-fbi-looks-to-undermine-encryption-federal-government-searches-better-encryption.shtml

7 Ways To Chop An Onion: You Suck At Cooking

This spoof of cooking how-to videos makes me laugh. I like to think it's the kind of thing I would've done if my 20s' had intersected with GoPro, inexpensive editing software, and uploadable videos. The video starts with conventional tips for cutting onions (with some explicit language), and then gets weird fast.

https://www.youtube.com/watch?v=eQgIwwKmjdo

Drew Conry-Murray
Packet Pushers

Web: **andrewconry-murray.com**
Twitter: **@Drew_CM**

Got something to say? Send your contribution to ***humaninfrastructure@packetpushers.net*** *and, if we publish it, we will pay you a pittance for it.*

You Need Business Continuity, Not Business Connectivity

Most software-defined wide area network (SD-WAN) vendors today provide an extended LAN solution to protect and connect enterprise locations. We call this business connectivity. What an enterprise really needs is an SD-WAN solution that optimizes and ensures WAN availability. We call this *business continuity*.

For organizations with customer-facing systems (Web site, customer care, sales, etc.), any application downtime has an immediate impact on revenue and customer satisfaction. From an internal IT perspective, when critical applications and data are not available, employee productivity suffers a significant reduction. Customer and employee expectations mean that critical systems now require 100 percent uptime. The key to limiting the impact of system failure is to fix the problem fast by providing rapid (sub-second) failover to alternative data center resources. How organizations achieve that is the challenge.

Access to the continuously available data center architecture relies on a high-performance, highly reliable WAN. Advances in software-defined networking (SDN) enable the network to support continuous availability via

geographically distributed data centers. **This hands-on demonstration** illustrates how Sonus' business continuity solution is helping State Street Bank and other customers keep business up and running around the clock, even in the event of disaster. Ensure you know the differences between SD WAN business connectivity and SD WAN business continuity— and why *business continuity* is a must for your network. Learn more at **www.sonus.net**.

Q&A: Exit Strategies

Question:

My question relates to exit strategies for Senior Network Engineers. I've been an engineer in high pressure environments for many years and I'm tired of always being answerable to someone higher. Management doesn't really interest me but what does is creating my own business. Do you think there are many avenues to exit as a network engineer into a startup? I lack programming skills and it seems the networking world is sown up by the big boys. Do you see gaps in the market that someone like me could target and create my own business?

Answer:

This is a common story. Management (bosses) doesn't want to pay engineers (workers) more than they earn themselves because they are the most valuable (important). Debates about who brings the most value are pointless (exceptions apply).

Weirdly, those same people will happily pay the same engineer ten times as much if they are a consultant who is on their payroll. For example, Cisco Professional Services have a rack rate of USD$3000 per day for each and every engineer allocated to your project. You can find people with the same competency at USD$2000 per day (like me).

There are plenty of gaps in the market for independent people to setup business and provide consulting services to companies. HOWEVER, you will need to be able to run a business, do sales and deals, accounting and many other tasks.

If you want to be in business for yourself, the best training is to work in a reseller hellhole for a couple of years. Get experience with lost of different customers and networks, learn some sales, learn some process and you should be good. You will probably hate working for a reseller (most people do) but it can be useful career progression.

> Got questions? Sure you do! Send them to **humaninfrastructure@packetpushers.net** and get answers (with no guarantee you'll like them).

Internets of Interest : Pages To See

Webpages that have caught my attention in the last couple of weeks.

StevenBlack/hosts

A single host file that collects multiple sources to build a comprehensive block list.

> Extending and consolidating hosts files from a variety of sources like mvps.org, someonewhocares.org, and potentially others.

StevenBlack/hosts

Ongoing Cisco Support Problems

Got a tip about this thread on Reddit being critical of Cisco Support program. Everything discussed here has happened to me several times. Its not a unique problem but Cisco is

> Please pardon my salt. I've been through a lot and lost my patience.
>
> Also, I am posting on a throwaway account because I don't want Cisco retaliating against me. This is the company that prosecuted Peter Adekeye, and I know from personal experience how their sales reps badmouth network engineers who go Juniper, because the've done it to me about my own staff. Far from "helping" me, I fear Cisco would want to "help" get rid of the problem as quickly as possible.

An ongoing Cisco customer support horror story : Cisco

Cisco Spark and poor quality software

Cisco Spark is yet another attempt by Cisco to remain relevant in the "collaboration" market. In particular, to build a platform that looks like Slack. At best, it is a blatant knockoff except for the fact that integrates voice & video via the Webex platform. I keep trying to use it but I find Slack actually reliably. And I use Skype or GoToMeeting for voice/video because Webex causes me great pain whenever I use it.

More importantly, it isn't supported on my Mac:

> "Safari is not yet supported for Cisco Spark for Web."
> "People using AdBlockPlus may have to disable ABP for

> web.ciscospark.com in order to load the logon screen.”

Its 2015, how the hell can you not support Safari ? Or Internet Explorer when you are a $100Billion company. I don't think Cisco is serious about this product.

Cisco Spark | Cisco Spark for Web - Known Issues

Docker Containers on the Desktop

> Most people use Docker for containing applications to deploy into production or for building their applications in a contained environment. This is all fine & dandy, and saves developers & ops engineers huge headaches, but I like to use Docker in a not-so-typical way.
>
> I use Docker to run all the desktop apps on my computers.

Jessie Frazelle’s Blog: Docker Containers on the Desktop

Change of Address - Routing Issues of Transferred IPv4 Addresses

This presentation from RIPE 70 talks about the problems of transferring blocks of IPv4 addresses. Often the IPaddresses have been sub-allocated to many other parties and subnets of sold IPv4 blocks are announced by other carriers. Are they squatters ? Can you fix this problem ?

Routing Issues of Transferred IPv4 Addresses

Introducing s2n, a New Open Source TLS Implementation

Amazon open source a TLS library. Why ?

1. They need high quality encryption inside their data centre to protect against attackers.

2. Amazon is massive target for threat actors with thousands of companies holding data and systems in their systems. They must maintain highest levels of security and may have lost faith in OpenSSL.
3. Because its cheaper to get open source to validate the code than doing it themselves.

> s2n isn't intended as a replacement for OpenSSL, which we remain committed to supporting through our involvement in the Linux Foundation's Core Infrastructure Initiative. OpenSSL provides two main libraries: "libssl", which implements TLS, and "libcrypto," which is a general-purpose cryptography library. Think of s2n as an analogue of "libssl," but not "libcrypto."

Introducing s2n, a New Open Source TLS Implementation - AWS Security Blog

Things On My Mind

On My Mind: No Servers. At All.

Use No Servers, Need No Devops

The operating system has the absolute core of IT infrastructure since the dawn of IT. CPU, memory, networking, storage, applications, databases are all fungible parts of the system but the operating system was the one thing that we built on above or below.

Now public clouds are moving to offer applications only. Instead of standing up a server, simply drop your application code in the right place and run it.

*This **jaws-stack/JAWS** project uses AWS services to build applications using Javascript.*

> *The Goals Of JAWS Are:*
>
> - ***Use No Servers:** Never deal with scaling/deploying/maintaing/monitoring servers again.*
> - ***Isolated Components:** The JAWS back-end is comprised entirely of AWS*
> - ***Lambda Functions.** You can develop/update/configure each separately without affecting any other part of your application. Your app never goes down… only individual API routes can go down.*
> - ***Scale Infinitely:** A back-end comprised of Lambda functions comes with a ton of concurrency and you can easily enable multi-region redundancy. Be Cheap As Possible: Lambda functions run only when they are called, and you only pay for when they are run.*

Think about the impact to a development team. No servers, no monitoring, no spin up, no storage provisioning or network configuration. NO DEVOPS.

All provided by a cloud platform.

Instant Reaction: "How is your career planning ?"

Here are the last five articles from the EtherealMind and Packet Pushers blog.

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

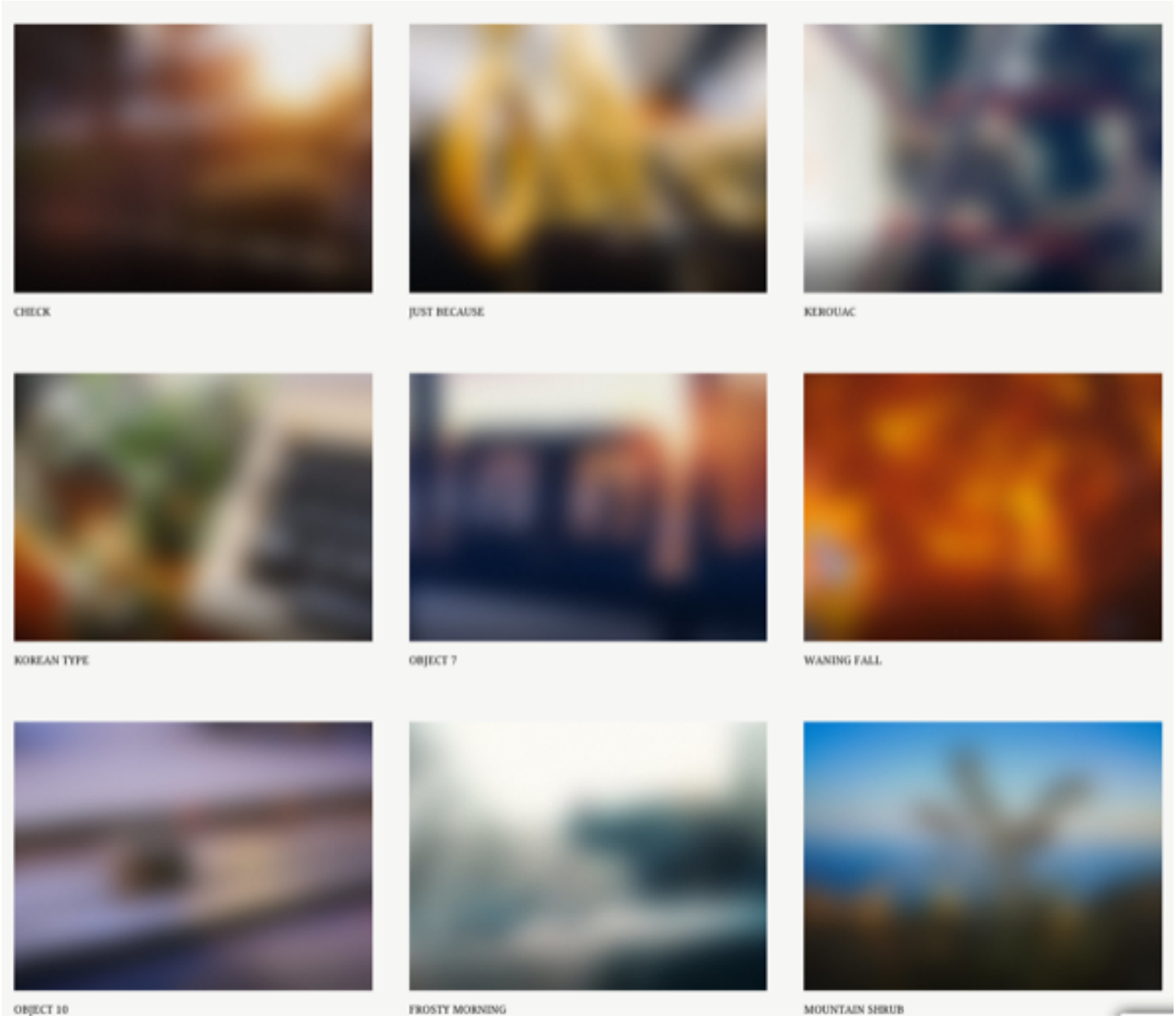
Network Break 182: BGP Hijacked For Cryptocurrency Heist; Juniper, Big Switch Unveil New Products - **Link**
Show 387: AWS Networking – A View From The Inside - **Link**
PQ 147: Connecting Security And GDPR Compliance (Sponsored) - **Link**
Datanauts 131: Masters And Mentorship - **Link**
Network Break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

I welcome your feedback, questions, and corrections. Send an email to **humaninfrastructure@packetpushers.net** and we'll get things sorted out.

Still Here?

Screen Backgrounds are a personal choice for many people. I like to have a very dark background. Mac OS X doesn't work with a black background because it needs some drop shadows to highlight icons. Here is the snap shot of my background, its a fabric style image that I never see because I don't use the Desktop.
I mean, who does that ?

But this site has some of the best backgrounds I have seen. They aren't "photos" but more abstract colour renderings.



Download them from here : **http://www.joedarnell.com/focus**

Sponsorship and Advertising - Send an email to humaninfrastructure@packetpushers.net *for more information.*

About Piece of A Human Infrastructure

A strongly curated newsletter produced by Greg Ferro that contain observations and thoughts on IT Infrastructure with a networking focus that he has seen, done, discussed, reviewed or just simply found on the Internet.

The format is structured but flexible (like any magazine) and will change over time as I settle into a routine of capturing ideas, topics that seem relevant and ultimately finding patterns that seem to be interesting to you. Your feedback will drives changes so don't hesitate to email with feedback or ask followup questions for the next edition.

About Greg Ferro

Greg is a co-host of the Packet Pushers Podcast a weekly podcast on Data Networking which has over 8000 subscribers. He blogs regularly at EtherealMind.com for the last eight years and is pretty well known these days. He also write as an analyst for Network Computing and Gigaom Research. He speaks at major events on Data Centre Design, SDN and life in technology. He moderates panels, advises customers and technology companies.

He works as a part-time network engineer in the UK on a freelance basis. Because real work configuring routers and switches remain not only a passion but important to keeping touch with the industry.