Human Infrastructure 115: For And Against Shutting Down Unused Ports

PACKET PUSHERS
Human Infrastructure Magazine
A Newsletter About a Life in Networking

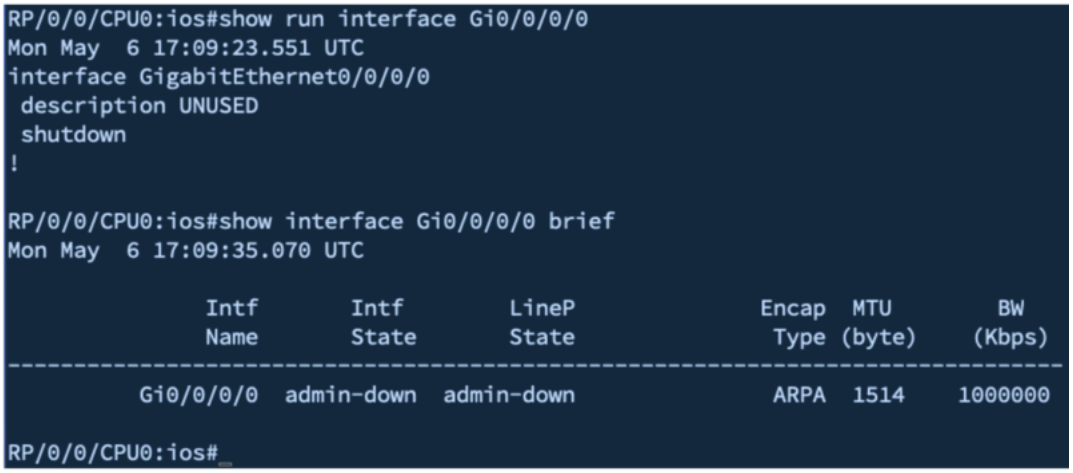
## Table Of Contents

# For And Against Shutting Down Unused Ports

### By Ethan Banks

As the tech lead on ‘new-to-me’ networks, my first task is to bring order to chaos. My process includes deep discovery of the existing network, configuration standardization, management plane security, support contract auditing, and so on.

A favorite step in bringing network order is administratively disabling unused ports.



```
RP/0/0/CPU0:ios#show run interface Gi0/0/0/0
Mon May  6 17:09:23.551 UTC
interface GigabitEthernet0/0/0/0
 description UNUSED
 shutdown
!

RP/0/0/CPU0:ios#show interface Gi0/0/0/0 brief
Mon May  6 17:09:35.070 UTC

               Intf       Intf        LineP              Encap  MTU        BW
               Name       State       State               Type (byte)    (Kbps)
--------------------------------------------------------------------------------
          Gi0/0/0/0  admin-down  admin-down               ARPA  1514     1000000

RP/0/0/CPU0:ios#_
```

For IT shops not used to this practice, shutting down unused ports feels harsh. Some engineers might complain “I should just be able to plug into the network and go. You just want to control everything.”

Yes, I do want to control everything, because I believe in network stability. Network stability comes, in part, through predictable, controlled interactions with edge devices. An unconfigured port waiting for anyone to plug in helps neither predictability nor control.

But is this approach too harsh? Let’s think through the pros and cons in an enterprise context.

## The Case For And Against Shutting Down Unused Ports

**Security.** Shutting down unused ports gives you better control of device access. For example, leaving idle ports lit in common areas is a no-no. Folks walking in off the street could plug in and gain network access. Employees with personal devices could also attach to the network, bringing their malware with them.

Network access control (802.1x) is another way to combat this, and is appropriate in many cases. But sometimes shutting ports down is the best--or only available--step.

*On the other hand*, you can make extra work for yourself if you are shutting down ports too aggressively. For example, conference room jacks should be lit, configured, and ready to go. Do you really want to be lighting up ports every time a meeting is scheduled or someone uses the room unannounced?

**Interaction.** When people have to make a help desk request to light up a port, you have the chance to interact with them. Why do they need the port? What are they going to use it for? Is there a better way to meet their need?

For example, I once discovered developers installing extra machines under their desks for testing--an early form of shadow IT. This went against corporate policy. Discovery caused a wholesale change in how developers performed testing.

Shutting down ports seems adversarial, but it can encourage a team mindset. At an old job I had, people would put in a ticket requesting that network ports be provisioned before they brought up a new machine. Networking was a part of the process.

This interaction can uncover other lurking issues. For example, you might find a VLAN running out of address space, or an access list requiring an update to handle a new machine. Perhaps a firewall policy needs a touch to allow for smooth communication.

*On the other hand*, you can be too heavy-handed, getting in the middle of things you don't need to be in the middle of. Sometimes it's okay to just give folks what they need and not ask too many questions.

**Documentation.** When bringing a port online, the time is right to update the port description to help identify what's on the other end of the link. The description field appears in network management systems, and can be helpful when troubleshooting.

*On the other hand*, manual port descriptions are just that--manual. Anything manual tends to fall out of date. LLDP is your friend, and a great many hypervisors and operating systems support it.

**Lifecycle management.** If you're in the habit of shutting down unused ports, port monitoring can flag when a port that was once in use goes down and stays down. Folks retiring equipment often forget to notify the networking team that the port is no longer being used. Even with excellent IT lifecycle processes, people forget this step. Monitoring port status lets you reclaim a port that's been decommissioned surreptitiously.

*On the other hand*, you need to have a good process for monitoring ports. Even in small environments, switch port density can quickly climb into the thousands of managed objects. A periodic, automated report that highlights port status changes is key.

**Stability.** Folks who plug in personal network switches can sometimes cause bridging loops by plugging two jacks at their desk into their switch. While protections such as bpduguard can help prevent loops, this doesn't always work in my experience. Similar loop issues can arise with misconfigured servers.

*On the other hand*, network stability is overrated. Everyone needs some excitement in their day now and then. There's nothing like a bridging loop to get the blood pumping!

## Parting Thoughts

On the whole, I've found that enabling ports in response to requests has led to better team relationships, a more predictable network, and opportunities for network design discussions. Other IT people have an excuse to talk to you. You miss out on those opportunities if people can just "plug 'n' go."

If you handle those interactions well, the result is a win for the business. Networking is included in IT planning discussions. There are fewer calls from panicked folks who can't get a server talking even though the link light is up.

You move towards a network that is intentional. Controlled. Predictable. Stable.

# Tech Blogs: How To

## I'll show you mine if you show me yours, investigating OSPF's "B" bit - Router# show ip int bri

https://showipintbri.blogspot.com/2019/05/ill-show...

Tony E. came across a lab task while studying for the CCIE that puzzled him: "How can you exchange prefixes across multiple areas in an OSPF domain when there is not an Area 0?" This post is his answer, which goes into very useful detail, and also serves as a reminder that reading RFCs can be useful when troubleshooting or problem-solving network issues. - Drew

## Free 2D symbols for computer network diagrams - GitHub

https://github.com/ecceman/affinity

You can get free symbols for network diagrams in this GitHub repository from ecceman (who calls Westeros home). This person writes “I wanted modern, crisp, pixel-perfect, printable, manufacturer independent symbols for computer-network topology that does not look they were made in the 80s.” There you go. - Drew

## Exploding Juniper Devices with NAPALM – The Networker

https://basimaly.wordpress.com/2018/01/08/exploding-juniper-devices-with-napalm/

“In this multi-posts series, We will deep dive into Juniper network automation and how to automate both configuration and operation for Juniper devices using different tools available such as PyEZ, NAPALM and Ansible.” The post is a little bit older, but still valuable. - Ethan

## 50 days from zero to hero with Kubernetes - Microsoft Azure Blog

https://azure.microsoft.com/mediahandler/files/resourcefiles/kubernetes-learning-path/Kubernetes%20Learning%20Path%20version%201.0.pdf

This PDF is a structured list of Kubernetes-related material curated by Microsoft. The idea is to take 50 days to work through the information. I like this approach. Don't rush. Learning isn't accomplished by blasting through material. Learning is accomplished through deep understanding of topics mastered over time by ponderance and practice. This "50 days" course might be what you're looking for to get a handle on Kubernetes, especially if you're also interested in Azure. - Ethan

## A Kompromat Mystery - thaddeus t. grugq

https://medium.com/@thegrugq/a-kompromat-mystery-29caa1fd94a2

Release of material that compromises a ruling politician in Austria when forces resignation and subsequent election. This post is deep dive into attribution and dissecting of who would release this material. For me, this is a learning experience in the difficulty of attribution in the cybersecurity space. - Greg

## AWS Transit Gateway Routing in Multiple Accounts - Driven By Code via Medium

https://medium.com/driven-by-code/aws-transit-gateway-routing-in-multiple-accounts-713b10ca7b34

TrueCar describes how they simplified their VPC routing & security environment using Transit Gateway. "AWS released the Transit Gateway product, which allowed us to remove the dependency on our legacy routers and Direct Connect links so that we could tie all our environments together in one place without creating a mesh of peers. We could also create routing policies for each of our types of environments..." Several diagrams scattered throughout, along with code blocks. - Ethan

### Remote Development with Visual Studio Code - Microsoft

https://code.visualstudio.com/blogs/2019/05/02/rem...

The folks at Visual Studio Code write “Today we're excited to announce the preview of three new extensions for Visual Studio Code that enable seamless development in Containers, remotely on physical or virtual machines, and with the Windows Subsystem for Linux (WSL). You can get started right away by installing the Remote Development Extension Pack.” - Drew

## Virtual Design Clinic June 6th

Register now to join the Packet Pushers online for our next Virtual Design Clinic on June 6th.

This live, online event includes 3 Ask Me Anything sessions with a panel of experts where you can get your networking, IT, and design questions answered.

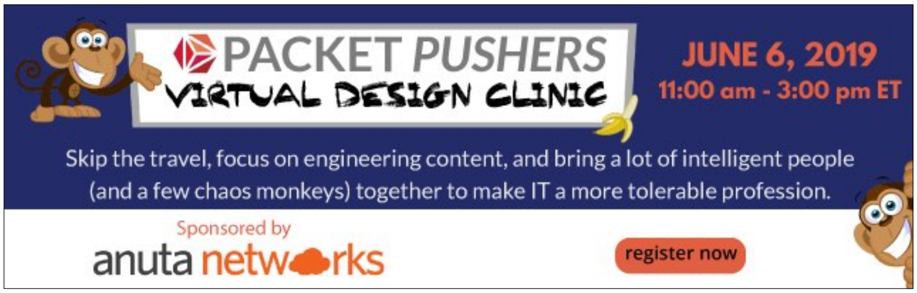
The VDC also features two tech presentations:

- Wi-Fi 6 Is Knocking. Are You Ready To Let It In? - Lee Badman
- The Art of Network Maintenance: A Practical Guide - Tom Ammon

Plus a sponsored presentation on network automation:

- Anuta ATOM: Assurance, Telemetry, and Orchestration for Multi-Vendor Networks - Anuta Networks

We hope to see you there!



PACKET PUSHERS
VIRTUAL DESIGN CLINIC

JUNE 6, 2019
11:00 am - 3:00 pm ET

Skip the travel, focus on engineering content, and bring a lot of intelligent people (and a few chaos monkeys) together to make IT a more tolerable profession.

Sponsored by
anuta networks

register now

# Tech Blogs: Opinion

## The Wi-Fi 6 elephant in the room - Sam's WiFi space

https://sc-wifi.com/2019/05/18/the-wi-fi-6-elephant-in-the-room/

Sam Clements thinks Cisco's new Wi-Fi 6 AP's are gonna be great. Why? They've gotten past this single threaded OS problem, among other challenges. "Cisco is an organization comprised of people, and people are fallible, but my personal experience with the Wi-Fi 6 (802.11ax) platforms from Cisco have been nothing short of rock-solid." Many of you out there tell us that new Cisco gear, software especially, suffers from quality problems. So, I hope Sam is right. - Ethan

## 9 Things to Consider When Estimating Time - packetmischief

https://www.packetmischief.ca/2019/05/21/9-things-to-consider-when-estimating-time/

Good thinking on the process of calculating hours required to deliver a work package. It's hard to learn how to budget time for projects because much is based on experience plus trial and error. This could be helpful in getting your thinking started right. - Greg

## Rubrik's Build is all about education - Ned In The Cloud

https://nedinthecloud.com/2019/05/07/rubriks-build-is-all-about-education/

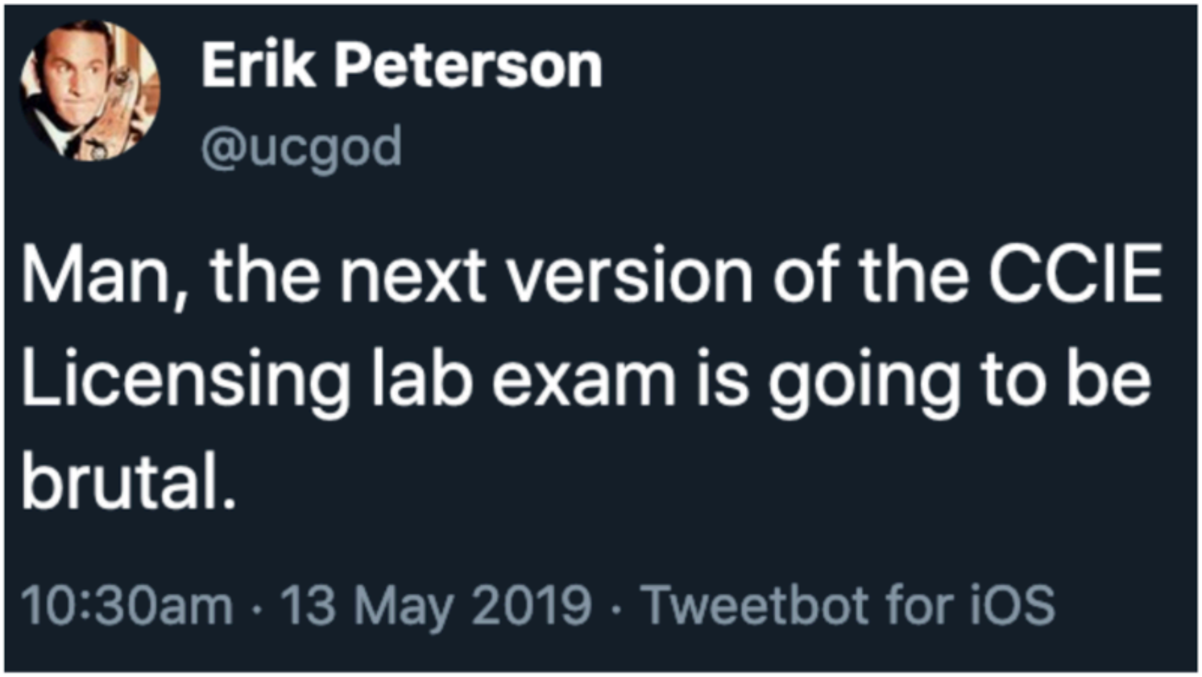
Ned Bellavance explains the motivations behind Build, an open-source project from Rubrik meant to help people get comfortable with Rubrik's APIs and automation capabilities. After seeing a presentation on Build at a Cloud Field Day, Ned says he wasn't quite sure what it was for. Now he's got a better idea; get IT admins who haven't ever touched an API to get comfortable with essential automation constructs. Yes, it's a little self-serving in addition to being educational, but Ned writes, "I'm glad that Rubrik is doing this. I'm also glad that companies like Juniper have the NRE labs to help network engineers on their journey. In an industry that experiences as much change as ours, education is paramount. I'm glad that some vendors see it that way too. - Drew

## Don't Base Your Design on Vendor Marketing - IP Space

https://blog.ipspace.net/2019/05/dont-base-your-de...

Ivan Pepelnjak does some blogging triage on an Arista-based DCI design that went sideways. The headline pretty much says it all, but you can read the blog for the gory details. - Drew

# The Lulz



Erik Peterson
@ucgod

Man, the next version of the CCIE Licensing lab exam is going to be brutal.

10:30am · 13 May 2019 · Tweetbot for iOS

# IT News

## Intel Gives Moore’s Law A Makeover - The Next Platform

https://www.nextplatform.com/2019/05/13/intel-gives-moores-law-a-makeover/

This piece shows exactly where Intel is at in their 14nm, 10nm, and 7nm fabrication plans. It’s been a rough ride getting from 14 to 10, and some shareholders are grumpy. The future seems to be picking back up for Intel, though. - Ethan

## Comcast is working on an in-home device to track people's health - CNBC

https://www.cnbc.com/2019/05/21/comcast-working-on-home-health-device-similar-to-amazon-echo.html

“The device will monitor people’s basic health metrics using ambient sensors, with a focus on whether someone is making frequent trips to the bathroom or spending more time than usual in bed.” Fantastic--sensors that monitor, among other things, when I use the bathroom. Just stop. How can they even pretend their vision is altruistic? This isn’t what we built the Internet for. We built it for cat videos. Let’s keep that in mind. 😹 - Ethan

## FCC Chief Backs T-Mobile-Sprint Merger With Concessions - SDxCentral

https://www.sdxcentral.com/articles/news/fcc-chief-backs-t-mobile-sprint-merger-with-concessions/2019/05/

Sprint & T-Mobile have cleared a major hurdle in their merger aspirations--the FCC. That doesn’t mean the merger is a done deal, but the chances of final approval have increased substantially. In theory, the combined carrier would compete more effectively with VZW & AT&T. My understanding is that Pink SprinT will have enough spectrum to build out a competitive 5G network, and their overall network coverage should improve. Generally, I’m against behemoth “too big to fail” companies, but in this specific scenario, I like the idea of a real contender joining the fray against the big two in the US market…so far. - Ethan

## Open19 Hardware in PoCs With ‘Mega Data Center Operators’ - SDxCentral

https://www.sdxcentral.com/articles/news/open19-hardware-in-pocs-with-mega-data-center-operators/2019/05/

Open19 is a standard for racks and the form factors of gear you stuff into them. Apparently, enough big-time buyers have expressed an interest that Open19 felt compelled to talk about it. I want to care, but…it’s complicated. There is conflict between Open19 and OCP’s Rack & Power spec. Besides that, most of us don’t have the ability to buy equipment compatible with either spec anyway, even though these specs have been in development for years. I’m bored with the waiting. - Ethan

## Yes, Americans can opt out of airport facial recognition. Here’s how - TechCrunch

https://techcrunch.com/2019/05/13/americans-opt-out-facial-recognition-airport/

I can’t quite articulate why facial recognition at the airport unnerves me, other than it feels like a further step toward pervasive video surveillance, which makes my tinfoil hat itch. In any case, this piece from Tech Crunch tells you how you can opt out. I’ve got some travel coming up, so I think I’m going to try it and see what happens. - Drew

## AT&T promised 7,000 new jobs to get tax break—it cut 23,000 jobs instead - Ars Technica

https://arstechnica.com/tech-policy/2019/05/att-promised-7000-new-jobs-to-get-tax-break-it-cut-23000-jobs-instead/

Seriously, do the executives sit around twirling their mustaches and chortling while they do stuff like this? - Drew

# New Products & Industry Takes

## A year later – updating Container Attached Storage - CNCF Blog

https://www.cncf.io/blog/2019/05/16/a-year-later-u...

Container Attached Storage (CAS) is rapidly evolving as container use cases expand. This article discusses where CAS is at and where it's going. Not sure why you care? All this container-related storage traffic is likely running across the network. Having at least a basic understanding of CAS is a good idea. - Ethan

## A Brief History of OpenTelemetry (So Far) - CNCF Blog

https://www.cncf.io/blog/2019/05/21/a-brief-history-of-opentelemetry-so-far/

Cloud native applications are complex. Lots of possible inputs and outputs. Lots of possible paths through the infrastructure that any given transaction could take. Troubleshooting is difficult, because no amount of human familiarity is enough to intuit what's happening when the system is slow...or broken. OpenTelemetry aims to help, and is a joining of the OpenTracing and OpenCensus projects. - Ethan

## Inter-RIR collaboration produces new product prototype - APNIC Blog

https://blog.apnic.net/2019/05/21/inter-rir-collaboration-produces-new-product-prototype/

"The new product — named APNIC NetOX (Network Operators ToolbOX) — is currently a working prototype. NetOX will provide whois, routing status and history, and reverse DNS information to users through a single web interface. APNIC NetOX combines information from a range of sources, for example, registry databases, Internet performance measurements, and RIPE's RIS and ATLAS services. The data will also be available via an API." - Ethan

## Stellar: Network Attack Mitigation using Advanced Blackholing - De Cix

https://www.de-cix.net/Files/2731074c857497be3827ac9537b6e486f27aa57c/Research-paper-Stellar-Network-Attack-Mitigation-using-Advanced-Blackholing.pdf

“In this paper, we propose Advanced Blackholing and its system realization Stellar. Advanced blackholing builds upon the scalability of blackholing while limiting collateral damage by increasing its granularity.” I heard this presented on at RIPE 78. Highlights just how far we are from having robust DDoS mitigation technology. Hard problem to solve, and hey--we’re making progress. - Ethan

## Teridion Announces Deep Integration with Cisco Meraki MX Security and SD-WAN Appliances to Deliver New High Performance Internet Service - BusinessWire

https://www.businesswire.com/news/home/20190523005...

Teridion, which offers a cloud-based WAN service that competes with carrier circuits, has announced a partnership with Cisco Meraki in which Teridion's service can "snap in" with Cisco MX and SD-WAN appliances to provide WAN connectivity. WAN providers such as Teridion promise better performance, visibility, and ease of use compared to traditional carrier and service provider connections, and this partnership makes sense for both vendors: Teridion gets access to Cisco Meraki's customer base, and Cisco Meraki users get more options for linking branch and remote offices. - Drew

## Mellanox Introduces Ethernet Cloud Fabric Technology based on the World’s Most Advanced 100/200/400GbE Open Ethernet Switches - Mellanox

http://www.mellanox.com/page/press_release_item?id...

Mellanox has announced new 400GbE Ethernet switches. The company writes "Spectrum-2 extends the capabilities of the first generation of Spectrum based Ethernet switches, which are deployed in thousands of data centers around the world. Spectrum enables IT managers to achieve leading performance and efficiency for 10GbE infrastructures and higher, and to effectively and economically migrate from 10 to 25, 50, and 100 Gb/s speeds." - Drew

# New Whitepaper For Premium Ignition Members

If you're a premium member of Ignition (i.e., you dropped $99 on us), we've just released a new whitepaper available for download:

Intent-Based Networking Part 2: A Deep Dive Into Network Abstraction & Continuous Validation, by Phil Gervasi.

The new whitepaper:

- Explores in technical detail how Intent-Based Networking (IBN) systems work
- Explains how IBN systems abstract network devices & configurations to build working models
- Discusses the pros and cons of different approaches to abstraction
- Reviews the closed-loop model that drives the value of IBN systems
- Provides key takeaways

Thanks to everyone who's signed on as a premium member. We'll have more premium content coming soon, including a new paper on SD-WAN, and Ethan is hard at work on a video course on QoS. We appreciate your support and patience as we build out a library worth your time and money.

# Got A Tech Tip To Share?

We've got a newsletter, you've got a tech tip. Let's get together! What do we mean by a tech tip? It could be:

1. A useful little script

2. A favorite tcpdump command line parameter

3. Screenshot of an under-appreciated feature in a GUI for some networking tool

4. A link to, and brief explanation of, a neat open source tool

5. Something else

If you've got something you'd like to share in this newsletter, drop me a line at drew@packetpushers.net. If we like it, and it's suitable for a newsletter format, we'll publish it in an upcoming issue (giving you all due credit, of course). Then you can sit back and bathe in the adulation that's sure* to follow.

**Adulation not guaranteed*

## The End Bit

Sponsorship and Advertising - Send an email to humaninfrastructure@packetpushers.net for more information. You could reach more than 6,000 subscribers.

**Human Infrastructure is 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.

Unsubscribe From This List | 95 Hidden Lane, Northfield, NH 03276