



Table Of Contents

1. The Prefix List - A Network Fable - Ethan Banks
2. Tech Blogs: How To
3. Learn Stuff! June 6th Virtual Design Clinic
4. Tech Blogs: Opinion
5. The Lulz
6. IT News
7. New Products & Industry Takes
8. New Whitepaper For Premium Ignition Members
9. Got A Tech Tip?

The Prefix List - A Network Fable

By Ethan Banks

You log into the router for the first time. The router is configured, running, and happily doing its job. As far as you know, it's never crashed. No one complains of performance problems. Routing adjacencies are stable. The router is clearly modeled in the NMS. You've noticed traps and log events coming in. All seems well.

Quiet stability is one reason you've ignored this router. Since the acquisition, you've focused on the "squeaky wheels", and the acquired WAN wasn't one of them. But with grease liberally applied to the squeaky bits, it's time to get a handle on the rest.

show run

As you parse the output, you notice a prefix list. You didn't expect that based on the documentation you'd reviewed.

You scan the list, trying to make sense of it. What's using the prefix list? Ah, a BGP neighbor. Filtering a couple of inbounds. Hmm. Why bother with that? This was a dead simple WAN according to the doc.

You examine the router's BGP neighbors and find the one the docs say should be there. And...there's also a second

neighbor. You review the BGP config stanza, and sure enough--two neighbors configured. Why is the prefix list applied to one and not the other? Seems like a needlessly complex configuration, code from back in the day that probably someone forgot to clean up.

The prefixes in the list don't look familiar, although in fairness you haven't audited the IPAM system yet. Still. Like many engineers, you're slightly OCD, and useless config scraps bother you. Your gut tells you that this is one of those situations.

You begin writing the "no" commands in your head to remove the prefix list and clean up the BGP neighbor config. You know you shouldn't just edit the config midday, because that's not standard procedure.

But you keep thinking about it. And thinking about it. Finally, you talk yourself into it. No one's likely to notice the config diff in the morning report anyway, because you're the only one who reads it.

You execute your negation plan. You clean up the BGP config section, removing references to the prefix list. Then, you wipe out the prefix list itself.

You hold your breath for a moment. You're still on the router. You still have CLI control. Nothing went red on the NMS. And hey, you didn't think it would. You're a pro. Time to save your fine work and move on. You'll investigate that second, undocumented BGP neighbor another day.

write mem

You smile that the ancient way of committing config to NVRAM still works, and continue poking at other network devices. The afternoon wears on. You go home.

The next morning, the help desk overnight shift is getting ready to head out. You check in with them, as you usually do. Somebody pipes up "Yeah, we had a weird one overnight nobody could figure out. That company we acquired has a B2B partner that called the NOC to complain. Something about overlapping IPs. The problem got punted to us, but we have no idea. Take a look?"

"Sure," you say. "Forward me the ticket."

Two IP prefixes stand out in the ticket. Despite being alone in your cubicle, you sink lower in your seat. Your face flushes red and hot.

Now you know who the second BGP neighbor was, and what the prefix list was for. After your so-called clean-up, that router was announcing IP blocks to the B2B partner that it shouldn't have, and that B2B partner network was confused.

Ouch. Thankfully, you log all your console sessions, so you pull up the session from yesterday where you "fixed" that router. You put everything back the way it was and save the config.

You make a note in the help desk ticket. "Discovered acquired network was incorrectly announcing two IP prefixes to partner network. Added route filter. Problem should be resolved."

Which is true...but not entirely. The whole truth is a little too hard to record in the ticket. Your pride wounded, you resolve to leave configs alone until you truly understand them.

Just because you didn't build the config doesn't make it wrong.

Tech Blogs: How To

Where Is Your Configuration Source Of Truth? - SolarWinds Thwack Geek Speak Blog

<https://thwack.solarwinds.com/community/solarwinds-community/geek-speak/blog/2018/10/25/where-is-your-configuration-source-of-truth>

John Herbert challenges us to rethink how network configurations are managed. He points out that the device configuration itself is not a source of truth, as it does not necessarily reflect how the device should be configured. Merely how it is configured. John introduces the idea of a source of truth and how automation tools such as Puppet would use that source to ensure that the network configuration is aligned with operator intent. - Ethan

How to: Deploying DNSSEC with BIND and Ubuntu Server - APNIC Blog

<https://blog.apnic.net/2019/05/23/how-to-deploying-dnssec-with-bind-and-ubuntu-server/>

This piece is exactly what it says in the title, demonstrating key generation, zone signing, chain of trust establishment, and more for BIND 9. The piece is also recruits you to sign up for a free APNIC Academy webinar for even moar DNSSEC, but don't be offended. I didn't know there was such a thing as the APNIC Academy. Probably there's some good info there. - Ethan

For ESXi: Realtek NICs Are Awful And Don't Use Them - DataCenter Overlords

<https://datacenteroverlords.com/2019/05/24/for-esxi-realtek-nics-are-awful-and-dont-use-them/>

Quick and to the point. "For this particular question (Realtek or buy another NIC) there's only right right answer: Buy another NIC. Realtek NICs suck. They don't perform well, they're a pain to work with for ESXi, so just buy a NIC." More advice from Tony Bourke on what NIC to get for your home lab when you click through. - Ethan

Love Your Job? Someone May be Taking Advantage of You - Duke's Fuqua School of Business

<https://www.fuqua.duke.edu/duke-fuqua-insights/kay...>

People who are 'passionate' about their jobs are easily exploited. Employers will certainly take advantage of this and will encourage you to 'love your work, love your company'. Of course, it's a simple way to get more work for less money. And you will probably sacrifice your personal life at the same time. - Greg

Learn Stuff! June 6th Virtual Design Clinic

[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:

Human Infrastructure 116: The Prefix List - A Network Fable

- 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



PACKET PUSHERS
VIRTUAL DESIGN CLINIC

The Packet Pushers' Virtual Conference

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.

Special Guests: Tom Ammon & Lee Badman

Sponsored by

anuta networks

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

[register now](#)



Tech Blogs: Opinion

Engineering Unplugged - Bytes of Cloud

<https://www.bytesofcloud.net/2019/05/engineering-unplugged/>

Ethan Gleason, son of network engineer Brian, talks about why, after lots of CCNA study, network engineering isn't for him. - Ethan

Does Security Belong Near Endpoints? - NetCraftmen

<https://www.netcraftsmen.com/does-security-belong-...>

Pete Welcher considers the firewall scale up vs. scale out problem, looking at the pros and cons of traditional big firewall approaches as compared to modern microsegmentation and container sidecar approaches. A thoughtful read that poses excellent questions in a space where there is no one right answer. - Ethan

Sales Ethics - Nick Russo

<http://njrusmc.net/blog/2019/05/29-sales-ethics.html>

Nick shares thoughts about how his ideal salesperson would act in a situation where a warranted customer network consolidation would result in a 70% loss of revenue to the vendor. I like his conclusion, and wish more salespeople were like Nick's ideal. - Ethan

Incompetent, privileged individuals are more likely to act smart — and get away with it - MarketWatch

<https://www.marketwatch.com/story/incompetent-peop...>

This article has me reconsidering my advice of 'fake it until you make it' because it might work for people from a privileged background but not for others. The closely related 'move fast and break things' mantra works as long as there is permission or forgiveness to break things. History is recorded by the winner; if incompetence is winning more often, then normalization happens. - Greg

The Lulz

He's got a point...



Via @NickSherman

IT News

Chrome to limit full ad blocking extensions to enterprise users - 9to5Google

<https://9to5google.com/2019/05/29/chrome-ad-blocking-enterprise-manifest-v3/>

“Back in January, Google announced a proposed change to Chrome’s extensions system, called Manifest V3, that would stop current ad blockers from working efficiently. In a response to the overwhelming negative feedback, Google is standing firm on Chrome’s ad blocking changes, sharing that current ad blocking capabilities will be restricted to enterprise users.” Doesn’t mean ad blockers have been outlawed in the Chrome ecosystem, but does mean they won’t work well. - Ethan

Confusion Reigns Over One of Huawei’s Wors[t] Weeks - SDxCentral

<https://www.sdxcentral.com/articles/news/confusion-reigns-over-one-of-huaweis-worse-weeks/2019/05/>

If you're not aware of just how difficult life is becoming for Huawei, have a read. From what several insiders have shared with me, their difficulties have been a long time coming and are justified. Don't shed any tears for Huawei.

- Ethan

Taking A Hard Line On Fraud - ARIN Blog

<https://blog.apnic.net/2019/05/22/taking-a-hard-line-on-fraud/>

Don't screw around when it comes to IPv4 resources, folks. ARIN is not amused. This article shares some details of a substantial fraud court case ARIN has won. Expect more IPv4-related fraud as the value per address increases in the face of v4 scarcity. Don't be a victim. -

Ethan

Five questions you can use to cut through the AI hype - MIT Technology Review

<https://www.technologyreview.com/s/613535/five-questions-you-can-use-to-cut-through-ai-hype/>

Everyone and their brother with a tech product to sell makes liberal use of the terms “AI” and “machine learning” in their marketing materials. How do you know what’s real and what’s wishful thinking? This piece from MIT Technology Review offers five questions you can use to help sort fact from fiction. My favorite is question 3, which tackles data labeling, but I also find question 5 compelling: Is this a problem that should be solved with ML? That gets into the moral and ethical issues around ML. - Drew

New Products & Industry Takes

<rant>The Packet Pushers receive pitches from PR firms daily. This week, we heard about newly published reports. Most industry reports are marketing tools designed to drive readers into a sales funnel. Some reports have good data, but be wary. We heard about some awards, too. Industry awards are often given by groups you haven’t heard of based on criteria you don’t know in competitions where the competitor list is hidden. Don’t be impressed by awards. **</rant>** - Ethan

Segment Routing: Policies, Paths and Segments - Juniper J-net Industry Solutions & Trends Blog

<https://forums.juniper.net/t5/Industry-Solutions-and-Trends/Segment-Routing-Policies-Paths-and-Segments/ba-p/463023>

A quick overview of what a segment is, and how a segment routed packet makes its way through the network. Part of a series on SR Juniper is releasing week by week. - Ethan

Notifying administrators about unhashed password storage - Inside Google Cloud

<https://cloud.google.com/blog/products/g-suite/not...>

“Google’s policy is to store your passwords with cryptographic hashes that mask those passwords to ensure their security. However, we recently notified a subset of our enterprise G Suite customers that some passwords were stored in our encrypted internal systems unhashed. ... To be clear, these passwords remained in

our secure encrypted infrastructure. This issue has been fixed and we have seen no evidence of improper access to or misuse of the affected passwords.” Um, okay. I guess. Thanks for the heads up. - Ethan

Certified Kubernetes Administrator (CKA) Certification is Now Valid for 3 Years - Cloud Native Computing Foundation

<https://www.cncf.io/blog/2019/05/28/certified-kube...>

This cert only used to be valid for 2 years. Now it's 3. I have mixed feelings about this. As rapidly as K8s is advancing, does 3 years make sense? On the other hand, a 2 year recert cycle sucks pretty hard. I lived that pain for a long time. - Ethan

Infoblox Unveils Simplified Security Platform to Detect and Stop Threats in Today's Borderless Networks - Infoblox

<https://www.infoblox.com/company/news-events/press...>

Infoblox is rebranding a pair of existing offerings as BloxOne Threat Defense. The rebranding puts its ActiveTrust and ActiveTrust Cloud DNS security offerings under one umbrella. The gist of the offering is to leverage DNS as a security tool. If Infoblox sees a device trying to reach an address that it knows is bad (for example, a malware command-and-control server), it can block, quarantine, or send an alert. You can get this DNS security service on premises. For remote workers or road warriors, you can install an agent on their mobile devices that resolves any and all DNS queries to an Infoblox cloud service first. Infoblox isn't the only company that offers this kind of security offering, but if you've got DDI infrastructure in place already, this is a useful extension. - Drew

Hey Premium Members: Get Your New IBN Whitepaper

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?

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 underappreciated 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 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.

Copyright © 2018 Packet Pushers Interactive LLC, All rights reserved BUT feel free to share this email with ALL YOUR FRIENDS. They would love it, right? Just don't change it. Send it because it's beautiful.

[Unsubscribe From This List](#) | 95 Hidden Lane, Northfield, NH
03276