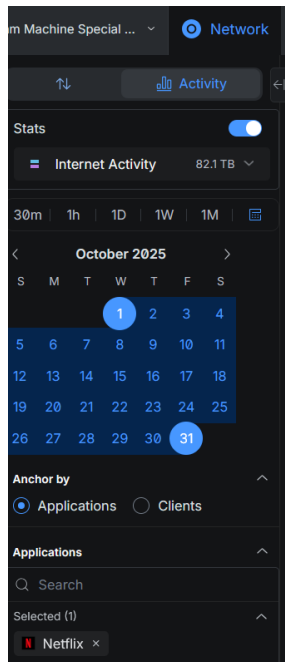


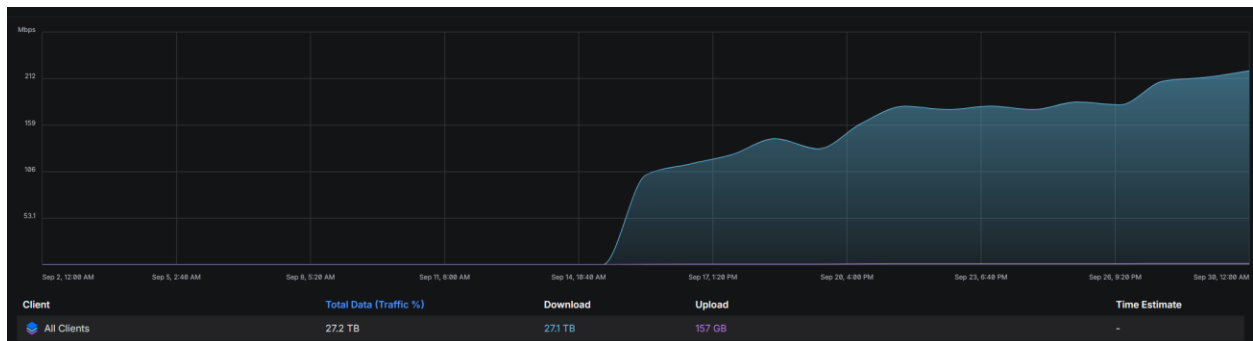
The Dish Netflix App Investigation

Timeline:

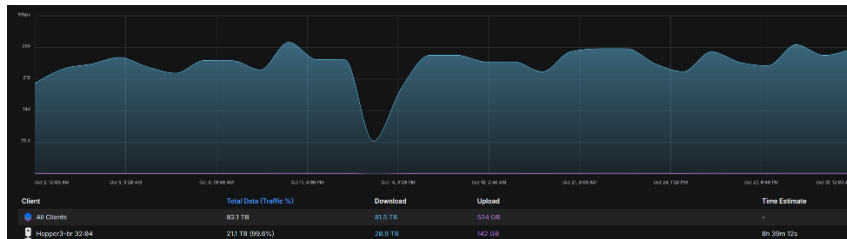
Pictures below come from Unifi's activity logs, with the filters set to just look at the Netflix app's traffic:



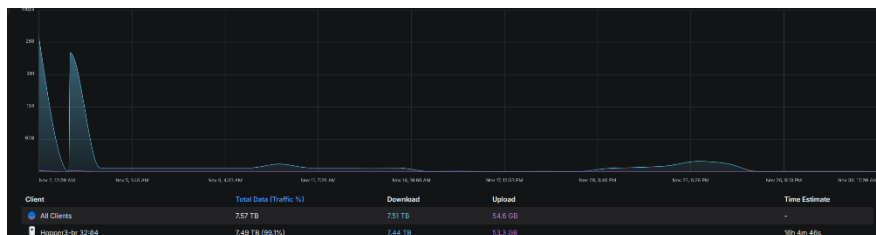
Starting September 15th, we saw a massive spike in downloads, upwards of 27.2TBs.



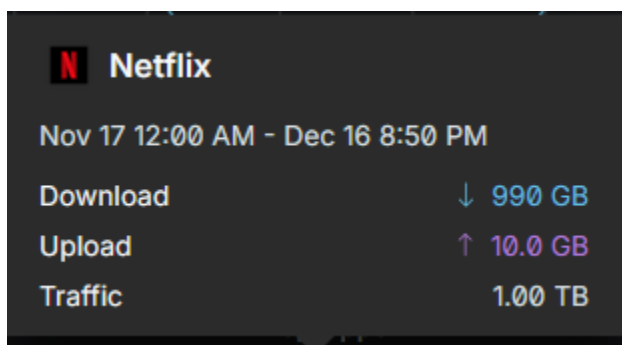
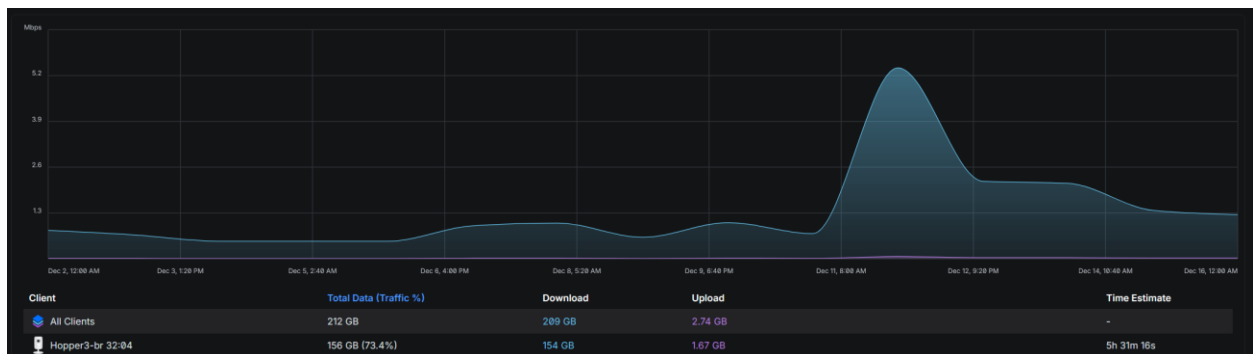
In October, this increased to 82.1TBs.



In November, this dropped to 7.57TBs due to the use of firewall rules to block Netflix on the Hopper device.



December – Continued use of rules and extensive monitoring. Traffic is down from terabytes to just a few hundred gigabytes:



The Problem:

Since September, I have observed odd communications from our Dish Hopper receiver and what appears to be a log collection server for Netflix on Dish's side. This communication was happening exclusively through the Netflix app until yesterday. Since yesterday I have started to observe that this same communication is now happening outside of the Netflix app through the Dish receiver itself.

In the following logs we can observe two different devices reporting this block, Hopper3 and ZiP-br0. The naming are the defaults provided by Unifi in the router as it appears that dish receiver is not a common device. To my understanding, due to how a Dish Hopper (Hopper3) and Dish Joey (ZiP-br0) work, these are effectively the same device. The Hopper is the "main" device, and the Joey is just a relay that works off the main Hopper. If you install Netflix, this must be done on the Hopper which then allows the Joey to access Netflix.

I have created rules to block this communication which is appearing in the logs here:

Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 34.210.171.252 by the dish ssl Firewall Policy.	---	Today at 6:27:40 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 3.230.116.16 by the dish ssl Firewall Policy.	---	Today at 6:22:14 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 8.39.224.113 by the dish ssl Firewall Policy.	---	Today at 6:17:11 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 8.39.224.113 by the dish ssl Firewall Policy.	---	Today at 6:17:11 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 151.101.46.68 by the dish ssl Firewall Policy.	---	Today at 6:16:56 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 44.253.138.236 by the dish ssl Firewall Policy.	---	Today at 6:11:52 AM
Firewall	Blocked by Firewall	ZiP-br0 32:04 was blocked from accessing 54.68.231.241 by the dish ssl Firewall Policy.	---	Today at 6:06:43 AM
Firewall	Blocked by Firewall	ZiP-br0 32:04 was blocked from accessing 52.24.234.236 by the dish ssl Firewall Policy.	---	Today at 6:01:17 AM
Firewall	Blocked by Firewall	ZiP-br0 32:04 was blocked from accessing 52.24.234.236 by the dish ssl Firewall Policy.	---	Today at 6:01:17 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 45.57.90.1 by the dish netflix Firewall Policy.	---	Today at 5:59:46 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 45.57.90.1 by the dish netflix Firewall Policy.	---	Today at 5:59:46 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 52.7176.80 by the dish ssl Firewall Policy.	---	Today at 5:56:17 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 3.129.196.255 by the dish netflix Firewall Policy.	---	Today at 5:51:56 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 151.101.46.68 by the dish ssl Firewall Policy.	---	Today at 5:51:14 AM
Firewall	Blocked by Firewall	ZiP-br0 32:04 was blocked from accessing 13.57.63.231 by the dish ssl Firewall Policy.	---	Today at 5:47:00 AM
Firewall	Blocked by Firewall	ZiP-br0 32:04 was blocked from accessing 45.57.90.1 by the dish netflix Firewall Policy.	---	Today at 5:46:53 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 3.230.116.16 by the dish ssl Firewall Policy.	---	Today at 5:46:11 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 3.16.62.20 by the dish netflix Firewall Policy.	---	Today at 5:41:53 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 54.224.145.4 by the dish netflix Firewall Policy.	---	Today at 5:41:51 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 13.57.63.231 by the dish ssl Firewall Policy.	---	Today at 5:41:51 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 54.221.40.48 by the dish ssl Firewall Policy.	---	Today at 5:41:11 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 54.189.223.155 by the dish ssl Firewall Policy.	---	Today at 5:35:56 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 44.253.138.236 by the dish ssl Firewall Policy.	---	Today at 5:30:14 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 52.24.234.236 by the dish ssl Firewall Policy.	---	Today at 5:28:21 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 44.253.138.236 by the dish ssl Firewall Policy.	---	Today at 5:25:13 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 54.189.223.155 by the dish ssl Firewall Policy.	---	Today at 5:19:56 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 54.189.223.155 by the dish ssl Firewall Policy.	---	Today at 5:19:56 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 8.39.224.113 by the dish ssl Firewall Policy.	---	Today at 5:17:11 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 8.39.224.113 by the dish ssl Firewall Policy.	---	Today at 5:12:13 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 52.85.31.112 by the dish ssl Firewall Policy.	---	Today at 5:06:56 AM
Firewall	Blocked by Firewall	ZiP-br0 32:04 was blocked from accessing 44.242.17.57 by the dish ssl Firewall Policy.	---	Today at 5:01:23 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 54.68.231.241 by the dish ssl Firewall Policy.	---	Today at 4:56:21 AM
Firewall	Blocked by Firewall	Hopper3-br 32:04 was blocked from accessing 54.189.223.155 by the dish ssl Firewall Policy.	---	Today at 4:50:10 AM
Firewall	Blocked by Firewall	ZiP-br0 32:04 was blocked from accessing 52.85.31.33 by the dish ssl Firewall Policy.	---	Today at 4:44:03 AM
Firewall	Blocked by Firewall	ZiP-br0 32:04 was blocked from accessing 52.85.31.33 by the dish ssl Firewall Policy.	---	Today at 4:44:03 AM

Netflix App

IP	Link	Notes
45.57.90.1:443	occ.a.nflxso.net	
3.16.62.20:80	appboot.us-east-2.origin.prod.a.netflix.com	
18.116.209.101:80	pushy-prod-nlb1-shard2-61b6e2f158c74469.el	
45.57.90.1	assets.nflxext.com	
3.16.62.20	appboot.us-east-2.origin.prod.a.netflix.com	
13.59.96.40		
3.138.232.98		
45.57.41.1		
3.17.233.126		
100.28.13.17		
18.223.242.221:443	logs.netflix.com	
13.216.189.215:443	api-global.netflix.com	

SSL/TLS

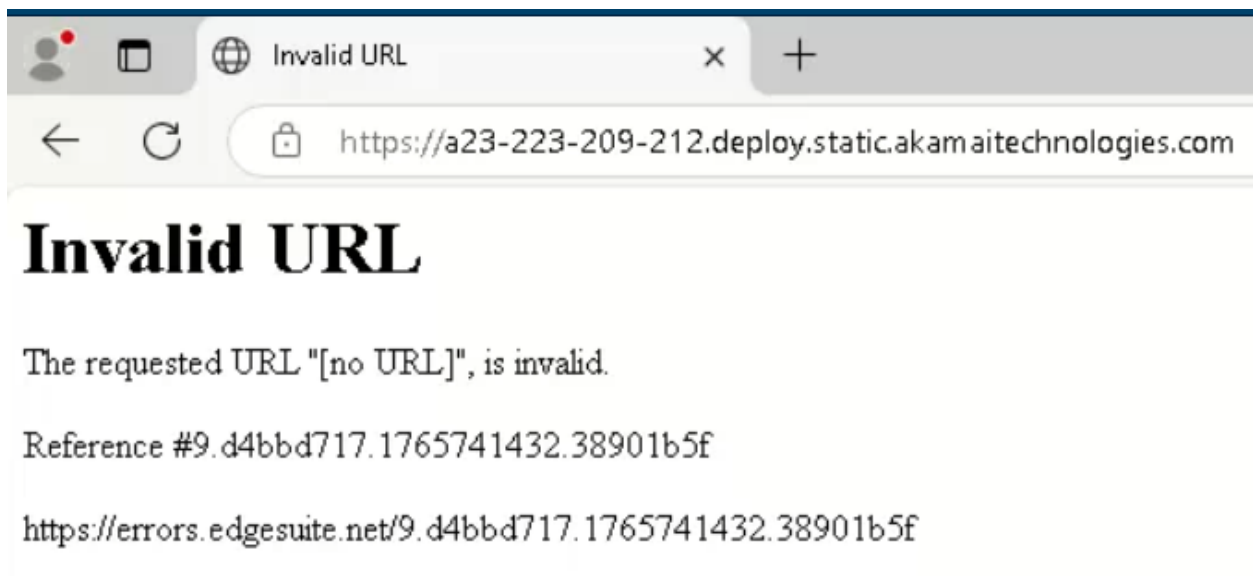
IP	Link	Notes
8.39.224.113:443	nsapi-prod.echodata.tv	
23.200.3.232:443	webapp.movetv.com	
44.253.138.236:8883	stbhlive.dishtv.technology	
34.210.171.252:443	grasshopper-rtr-logs.dishanywhere.com	
52.7.176.80:8443	grasshopper-config.dishanywhere.com	
52.85.31.112:443	mdconfig.sling.com	
13.57.63.231:443	ec2-13-57-63-231.us-west-1.compute.amazonaws.com	See images below
23.223.209.212:443	a23-223-209-212.deploy.static.akamaitechnologies.com	See images below
8.39.225.20:443	stbanalytichy.echostarbeta.com	
54.244.10.244:443	vmcollector-pvm.dish.com	

ec2-13-57-63-231.us-west-1.compute.amazonaws.com



ec2-13-57-63-231.us-west-1.compute.amazonaws.com/console

a23-223-209-212.deploy.static.akamaitechnologies.com



Hopper3-br 32:04 was blocked from accessing 23.223.209.212 by the dish ssl Firewall Policy.

Hopper3-br 32:04 was blocked from accessing 23.223.209.212 by the dish ssl Firewall Policy.

The associated IP appears twice. The first one does not display any link on Unifi's side, however the second instance has a link for webapp.movetv.com. When doing a reverse DNS

Called Netflix twice and spoke with their chat on their contact page.

1st call did not provide any useful information.

2nd call advised me to speak with their chat to provide more information.

In the chat I provided the highlighted Ips and sites associated with them which the support agent just mentioned that I should only see if I was using public wi-fi. *I'm not sure why, or if I'm supposed to be seeing any of those.*